A FRAMEWORK FOR PRESERVING PRIVACY IN E-GOVERNMENT

Haya Abdullah A. Almagwashi

July 2014

Cardiff University
School of Computer Science & Informatics

A thesis submitted in partial fulfilment of the requirement for the degree of Doctor of Philosophy

Declaration

This work has not been submitted in substance for any other degree or award at this or any other university or place of learning, nor is being submitted concurrently in candidature for any degree or other award.

Signed Haya Almagwashi (candidate) Date 30-06-2014

STATEMENT 1

This thesis is being submitted in partial fulfilment of the requirements for the degree of PhD.

Signed Haya Almagwashi (candidate) Date 30-06-2014

STATEMENT 2

This thesis is the result of my own independent work/investigation, except where otherwise stated.

Other sources are acknowledged by explicit references. The views expressed are my own.

Signed Haya Almagwashi (candidate) Date 30-06-2014

STATEMENT 3

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed Haya Almagwashi (candidate) Date 30-06-2014

Summary

This research investigates the problem of preserving privacy in an e-government context. Due to the multidisciplinary, complex nature of the problem, Soft Systems Methodology (SSM) was used to understand the concepts relevant to e-government, and privacy preservation in the context of e-government. Using SSM, Conceptual Models (CMs) relevant to the concepts under investigation were developed and used to review and identify the limitations of existing frameworks in the literature and to determine the requirements for preserving privacy in an e-government context. A system thinking framework for Privacy REquirements in E-GOVernment (PRE_EGOV) was developed informed by the developed CMs. The proposed approach aims to enable the users of e-government services to have control over information about them and considers the perspectives of involved stakeholders and the impact of social, cultural and political environmental factors. The PRE_EGOV framework was validated using a survey distributed in different countries and the framework was applied on a real world case study to evaluate its applicability and usefulness. The survey findings and the feedback gained from the analysis of the case study showed that the proposed framework can enable preserving privacy in e-government services and that its application can increase users' trust in using e-government services. Also, it showed that the holistic approach used to tackle such complex, multi-disciplinary problem can result in a promising solution that is more likely to be accepted by the involved stakeholders.

Abstract

Today the world is relying heavily on the use of Information and Communication Technologies (ICT) in performing daily tasks and governments are no exception. Governments around the world are utilising latest ICT to provide government services in the form of electronic services (e-services) in a phenomena called the electronic government (e-government). These services vary from providing general information to the provision of advanced services. However, one of the major obstacles facing the adoption of e-government services is the challenging privacy issues arising from the sharing of user's information between government agencies and third parties. Many privacy frameworks have been proposed by governments and researchers to tackle these issues, however, the adoption of these frameworks is limited as they lack the consideration of users' perspective. This thesis uses Soft Systems Methodology (SSM) to investigate the concepts relevant to e-government, and preserving privacy in the context of e-government. Using SSM, Conceptual Models(CMs) relevant to the concepts under investigation were developed and used to review and to identify the limitations of existing frameworks in the literature and to determine the requirements for preserving privacy in an e-government context. A general framework for Privacy REquirements in E-GOVernment (PRE_EGOV) is proposed based on the developed CMs. The proposed framework considers the perspectives of relevant stakeholders and the ownership rights of information about users. The CM relevant to preserving privacy and the elements of the PRE_EGOV framework were evaluated against stakeholders' perspectives using a survey. The applicability of the proposed framework is demonstrated by applying it on a real world case study. The insight gained from the analysis of the case study and the survey's results increased confidence in the usefulness of the proposed framework and showed that a system thinking approach to tackle such complex, multi-disciplinary problem can result in a promising solution that is more likely to be accepted by involved stakeholders. The work in this research has been published in three full papers and a poster. The developed Conceptual Models and proposed framework have found acceptance in E-government research community [1, 2, 3, 4] as well as in other research communities [5].

Dedication

To my role models, the best teachers and mentors I have ever known, my mother Noura Alsaleehi and my father Abdullah Almagwashi.

To my beloved husband, Abdullah.

To my little angels, Sulaf, Faisal, Feras and Suhail

I hope I made you proud.

Acknowledgments

I would like to thank all those who have made this thesis possible. First and foremost, I would like to thank my supervisor, Prof. Alex Gray, for his advice and unlimited support throughout the research. I want also to thank him for giving me the space to experiment my own ideas and for all his time and effort which helped me tackle the challenges of this research. Also, I wish to thank Mr. Jeremy Hilton, for his advice and constructive comments and helpful discussion. I am also appreciative to Mr. Steve McIntosh, for his valuable thoughts at the early stages of this research. I am also grateful to Prof. Omar Rana and Dr.Wendy Ivins for their feedback and comments throughout the research.

Special thanks to Dr. Anas Tawileh, for his helpful feedback and comments which provided me with confidence in my work.

I would like to extend my thanks to my sponsor in Saudi Arabia, King AbdulAziz University (KAU), for the scholarship and the continuous support throughout the years of my study. I am also thankful to my friends and colleagues in the Faculty of Computing and Information Technology at KAU for their encouragement and friendship. Also, special thanks and appreciation go to the UK Saudi Arabian Cultural Bureau for their help and support.

I am also grateful to all the staff at the School of Computer Science & Informatics for their unconditional help whenever it is needed. Special thanks to Dr. Rob Davies, Dr. Pam Munn and Mrs Helen Williams

Also, I wish to thank my fellow doctoral students—those who have moved on, those in the quagmire, and those just beginning—for their support, feedback, and precious friendship. Your kindness and support is appreciated. Thanks to Hanaa Aldahawi, ,Eyman Altuwajiri, Soha Ali, Liqa Nawaf Yulia Cherdantseva, Fatma Alrayes, Neelam Memon, Aseelah Alharthi and Shahad Alahdal. I wish you the best in your research.

I would like to thank all my friends for believing in me and accepting nothing less than completion from me. Special thanks to Dr. Asma AL-Saidi for her treasurable friendship and support; my lovely friends Dr. Shada Alsalamah and Faten Kareem who were always there for me and my friend Dr. Hessah Alsalamah for her positive thoughts.

I would like to extend my thanks to Cardiff people, for their smiles and friendliness and to my neighbours, for their kindness and care and special thanks goes to Hend Aba Alkheel and her family for being a great neighbours and dear friends.

My deep gratitude goes to my family, especially my parents who believed in me, my sisters and brothers, Mezna, Ali, Alhassan, Sumayah, Sawsan, Bushra, Basmah, Abdulrahman, Mohamad and Tasneem, for their support throughout this journey. Also, I am thankful to my bigger family, especially my brothers and sisters in law. Special thanks to Huda, Hend, Heyam, Lolwah, Muna, Hana and Majdah.

Last but not least, I owe my deepest gratitude to my beloved husband Dr. Abdullah Almuhaisen for his endless support, encouragements and love and to my children for their patience and understanding. Thanks to all of you, your support made my dream come true.

Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Name	First appeared
APEC	Asia Pacific Economic Cooperation	*Ch V,p.65*
CATWOE	C=Customer, A=Actor, T=Transformation, W=World view, O=Owner, E= Environmental constraints	*ChII, p.13*
CM	Conceptual Model	*Ch I, p.5*
CMRPP	Conceptual Model Relevant to Preserving Privacy in e-government	*Ch I, p.6*
CPTM	Consensus Primary Task Model	*Ch II, p.12*
CS	Computer Science	*Ch I, p.5*
DG	Digital Government	*Ch I, p.5*
e-authentication	Electronic Authentication	*Ch IV, p.37*
EC	European Commission	*Ch V, p64*
EDA	Exploratory Data Analysis	*ChVII, p.99*
E-government	Electronic government	*ChI,p.1*
EGR	Electronic government research	*Ch I, p.5*
EMA	Enterprise Model Assembly	*Ch II,p.*
e-services	Electronic services	*Ch V,p.74*
EU	European Union	*Ch V, p64*
FR	Functional Requirement	*Ch IX,p.170*
FSM	Formal Systems Model	*Ch II, p.15*
G2B	Government-to-Business	*ChIII,p.24*
G2C	Government-to-Citizen	*ChIII,p.24*
G2G	Government–to-Government	*ChIII,p.24*
HAS	Human Activity System	*Ch II, p.15*
HE	Higher Education	*Ch IX,p.154*
ICT	Information and Communications Technologies	*ChI,p.1*
IEE	Internal Efficiency and Effectiveness	*ChIII,p.24*
ISR	Information Systems Research	*Ch I, p.5*
L	Linking system	*ChII ,p.12*
LoA	Level of Assurance	*Ch IV,p.39*
NCR	National Research Council	*Ch IV,p.42*
NHS	National Health Service	*ChII, p.16*
NIST	National Institute of Standards and Technology	*Ch IV,p.39*
OECD	Organisation for Economic Co-operation and Development	*Ch IV,p.40*

Acronym	Name	First appeared
OMB	Office of Management and Budget	*Ch IV p.52*
OR	Operational Research	*Ch II p.16*
PDR	Privacy Design Requirement	*Ch IX,p.172*
PET	Privacy Enhancing Technologies	*Ch VIII ,p.134*
PIA	Privacy Impact Assessment	*Ch V,p.72*
PII	Personal Identifiable Information	*Ch VIII ,p.135*
PMC	Planning, Monitoring and Control system	
PR	Privacy Requirement	*Ch IX,p.168*
PRE_EGOV	Privacy REquirements in E-GOVernment	*Ch I, p.5*
Pub Domain	Public Administration research	*Ch I, p.5*
Q	Question	*ChVI,p.89*
QR	Quick Respond code	*Ch IV, p.94*
RD	Root Definition	*ChII ,p12*
S	Supporting system	*ChII ,p12*
SA	Saudi Arabia	*Ch VI,p.85*
SD	System Dynamics	*Ch II, p.16*
SODA	Strategic Options Development and Analysis	*ChII,p.17*
SR	Security Requirement	*Ch IX,p.170*
SSM	Soft Systems Methodology	*Ch I, p.5*
T	Transformation process	*ChII ,p12*
UK	United Kingdom	*Ch IV,p51*
UN	United Nations	*Ch IV,p51*
US	United States	*Ch IV,p51*

List of Publications

1. Almagwashi, H,Gray, A," Citizens' Perceptions and Attitudes Towards Preserving Privacy and Trust in E-government Services: A Cross-sectional Study", I n the Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance – ICEGOV2014, Guimarães, Portugal, October, 2014.
2. Almagwashi, H.," Preserving Privacy in E-government: A System Approach", In the joint proceedings of On-going Research and Projects of IFIP EGOV2012 and IFIP E-Part 2012 conference, Kristiansand, Norway, 2012.
3. Almagwashi, H., Gray, A. and Hilton, J., "Privacy Requirements Elicitation in E-government: A Systems Approach", for the Security and Privacy in Collaborative Working workshop, presented at the UK All Hands Meeting (AHM) conference, Cardiff , UK ,2010.
4. Almagwashi, H., Gray, A.,"E-government Authentication Frameworks: a Gap Analysis", In the Proceedings of the 5th International Conference on e-Government (ICEG2009),Boston,US,2009.
5. Almagwashi, H., McIntosh, S., "Understanding the Government to E-government Transition Using a Soft Systems Approach: What is E-government Supposed to do?", In the Proceedings of the 9th European Conference on Electronic Government (ECEG2009),London,UK.,2009.
6. Tawileh, A., Almagwashi, h. and McIntosh,S.,2008, "A System Dynamics Approach to Assessing Policies to Tackle Alcohol Misuse" In the Proceedings of the 26th System Dynamics Conference, Athens, Greece, 2008.

Chapter One

I. Introduction

I.1 Overview

Since the introduction of the Internet and the associated vast advance in Information and Communications Technologies (ICTs), governments around the world are changing their ways of providing information and public services and their ways of interaction with those who benefits from these services. In almost every region in the globe from developing countries to industrial ones, governments on a local and national scale are putting important information on the Internet, automating their large and small processes and interacting electronically with their citizens. This phenomenon is called digital government or electronic government (e-government)[6] However, the development and deployment of e-government has faced many obstacles and security and privacy issues are one of the major obstacles which are the focus of much research in the area [6], [7] and [8]. The main security and privacy issues related to e-government services are verification and authentication of users' identities, maintaining data confidentiality, integrity, and availability and protecting users' privacy. These are also issues with web applications but with a different level of impact than in e-government applications [9]. With the increase in the provision of integrated advanced e-government services, and in order to provide reliable, trusted information that is secure and only accessible to authorized people, strong authentication measures are needed to verify the identities of the users of these services. These authentication measures require the user to share identifiable information with the government sites in order to benefit from the integrated services. However, the use of these authentication methods for verifying the identities of users when providing them with e-government services and the possibility of sharing their data between government agencies raised privacy issues for the users and has affected their adoption of e-government services [9] and [10]. This dilemma has been the subject of many efforts in the literature [11], [12], [13], [14] and [15]. The aim of this research is to provide a framework for preserving privacy in e-government

that considers the security requirements of the provided service while considering the perspectives of different stakeholders.

This chapter provides an overview of the research presented in this thesis, describes the selected approach, the main contributions achieved, and introduces the thesis structure. The next section describes the research problem and motivation while the research scope and objectives are stated in section three. The hypothesis is presented in section four with the research approach explained in section five. The main contributions of the research are presented in section six and finally the thesis structure is overviewed in section seven.

I.2 Research Problem and Motivation

I.2.1. Understanding E-government

Electronic government services were first introduced in the late 1990s by the US government [16], [17]. Since then, almost all governments around the world have established some form of electronic services. The concept of electronic government (e-government) and what e-government is supposed to provide is complex and involves different perspectives. This complexity is inherited from the complexity associated with public sector which due to the involvement of a variety of stakeholders with diverse viewpoints [18],[19]. E-government concept can be viewed as a way for providing efficient government services and enhancing the delivery of government services to the public by enhancing the quality and response time of these services. It is also considered as a way for improving democratic processes and the involvement of citizens in decision making [16],[20]. While most of the definitions found in the literature evolve around these views [16], it is important to understand how the concept is perceived by different stakeholders. Stakeholders can be identified according to their role in the provision of e-government services. The most frequently recognised roles in the literature are: users, government representatives, services providers and services developers [19]. Another important role is the government's partners and third parties who support the provision of the services[21]. Figure I.1 shows some of the main stakeholders involved in the provision of e-government services. Users are the main stakeholders and they

are the customers of e-government services. Users can be individuals including citizens, non-citizens, government employees or groups including profit and non-profit organisations and business firms and government departments. Another important stakeholder is government body representatives; such as government leaders, politicians and policy makers who represent the government on decisions related to the provision of e-government services. E-government services providers include government agencies providing e-services and their employees, and the developers of e-government services also are important stakeholders in the provision of e-government services. The identification of stakeholders and their roles is discussed in detail in this research in sectionII.12VIII.2.1. However, it is important to point out that an individual or a group might have more than one role and their perspective as stakeholders should be considered according to each role.

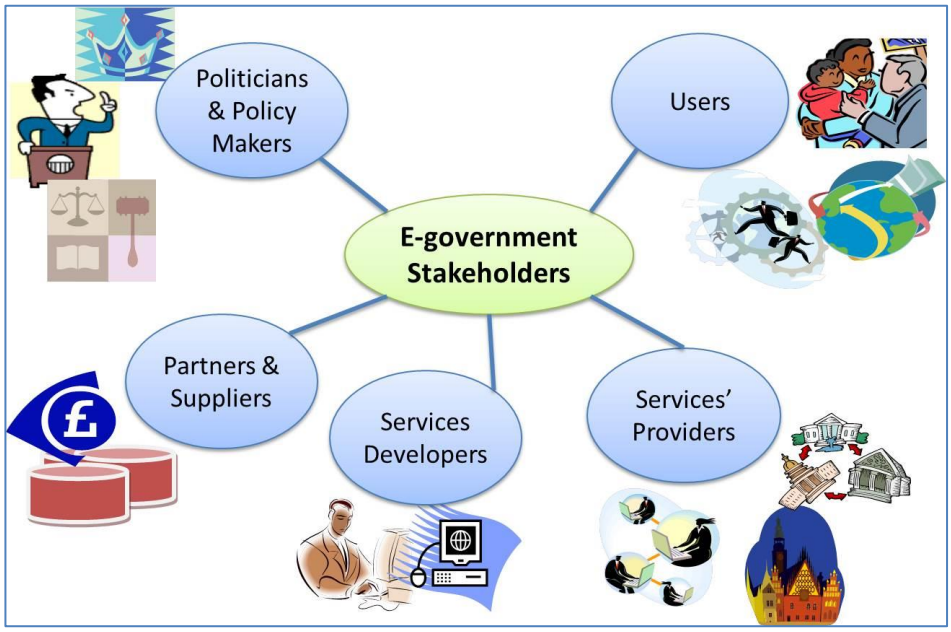


Figure I.1: E-government main Stakeholders

From the perspective of the provided electronic government services, electronic government services vary from simple provision of government information electronically to the provision of advanced integrated services, such as submitting tax return forms and paying fines electronically. Electronic government services are classified into four general categories [22]:

1. Presence: government websites are established and provide general information about public policies and regulations and information about the provided services.

2. Enhanced information services (one-way communication): government websites provide one-way communication between the users and the government, such as downloadable forms and applications for government services. The user might be required to provide a proof of identity

3. Transactional services (two-way communication): government websites provide transactional services, such as a request for licence renewal, fill and submit online tax forms and paying for services, fees and fines.

4. Connected services (e-government portal): government websites are integrated into one government portal that provides the services of all government agencies in one site. In this stage government applications are integrated and the services are provided in a citizen-centric approach. However, this means that the information about the users can be shared among government agencies.

As mentioned earlier, an individual or a group can have more than one role as a stakeholder in e-government. Also, a user of any of e-government services is not always the subject of the data processed to provide a service. In this research we differentiate the data user, from the data subject and the data owner as follows: a data subject is the individual or group who the collected data is about, while a data user is the individual or group who are using the data subject to get or provide a service. For example, an e-employee can be a data user of data that is not about him/her and he or she will use this data to provide an e-government service. In addition, the owner of the data is not always the data subject or the data user. The ownership of the data and especially personal data is argued in this research to be the right of the data subject when the data is personal and about the subject, however, other ownership rights are discussed and presented in detail in section12VIII.3.1VIII.2.1.3 as part of the novel privacy framework presented in this thesis.

I.2.2. Security and Privacy in E-government

The provision of advanced categories of e-government services, such as the transactional and connected services required the deployment of strong security measures for verifying and authenticating users' identities when requesting e-government services and for protecting their data when processed by e-government service providers. Authentication methods vary from simple user names and passwords to the use of smart cards, digital certificates and biometrics. The decision as to what type of authentication method to use when providing an e-government service is guided by an e-government authentication framework which provides government guidelines and policies that comply with relevant authentication standards and guidelines. Examples are the UK authentication framework [23], the US authentication framework [24], and the Australia Authentication framework [25]. However, many governments are aiming to integrate the provision of e-government services to achieve more efficient and effective service provision. This trend means that government agencies will share users' information, which raises many privacy concerns among users of e-government services about the amount of information shared and the way their privacy is protected. Although some of the current e-government authentication frameworks [23] and [25] acknowledge the importance of protecting users' privacy when using e-government services, the literature gap analysis presented in this thesis showed that there is a lack of detail on how users' privacy protection can be achieved when providing e-government services. Some governments provide a separate privacy framework to provide such details, such as [26]. However, these frameworks incline towards providing technical details for enhancing privacy at the implementation level and provide a limited view on how privacy is to be preserved that reflect only the service providers' perspective. In addition, there was no consideration of the perspective of the users and the influence of other environmental factors such as social, cultural and political factors on those privacy frameworks [27],[2].

Preserving privacy in e-government context is quite a complex issue as it inherits this complexity from the concept of e-government and is influenced by political, cultural, social and legal factors [28],[29]. In addition, privacy is perceived differently between stakeholders' categories and within each

category. For example, in the users category, users who are data subject would worry about the amount of personal data about them that a government department might know or share and how their personal data is protected and who is viewing it. However, a government employee who is considered a data user using e-government services systems to provide and process a service to e-government customers might worry about having missing data that will slow the provision of the service and would prefer having access to as much information might be needed as possible. Also, a government employee can be considered as a data subject who might worry about his/her identity and the protection of it to avoid unnecessary contact with e-government customers. From another perspective, the focus of government body representatives might be more on providing integrated e-government services to enhance the efficiency and reduce the cost and time needed when providing these services. However, resolving privacy issues that might arise from such integration may not be a top priority when it comes to reducing the cost and enhancing the efficiency in this perspective. In addition, sometimes opinion towards preserving privacy might differ within the same stakeholders category. For example, in the users' category, young users might tend to be less sensitive about their privacy compared to users of an older age. Also, several studies in the literature such as [27], [29] and [30], showed that e-government users who come from different social and cultural backgrounds have different views about what is considered as private personal information and how this information should be handled when using e-government services. The lack of consideration of the users' perspective of how their privacy is preserved had an impact on users' acceptance and trust in using e-government services and has been a subject of various studies and proposals by researchers in the field [13],[31],[32]. Hence, despite all these efforts, there is still a need for more detailed and easy to follow privacy frameworks that can be used by e-government service providers to determine privacy requirements from different perspectives and balance these requirements with the security requirements when providing an e-government service. This research has developed a privacy that can achieve this aim and provide a practical approach for considering the perspectives of involved parties with regard to preserving privacy framework in e-government services (see sectionVIII.3).

I.2.3. Privacy and Trust in E-government

Trust is defined as a “firm belief in the reliability, truth or ability of someone or something”[33]. Several studies showed that trust is critical for the utilisation of e-government services [27],[34] and [10]. The concept of trust in online services and mechanisms to build trust in such services have been widely discussed in e-commerce [35],[36] and in few studies in e-government research [34], [10]. Several mechanisms based in theories such as institutional-based-trust, characteristics-based-trust and process-based-trust have been suggested to help increase trust in online services [34], [37]. Trust in e-government has been linked to the intention of using e-government services and has been a subject of many studies in the literature, such as [32],[31],[38] and [10]. These studies have acknowledged the complexity of the concept of trust in e-government and have identified several factors that affect trust in using e-government services such as the perceived usefulness of e-government services [31],the quality of the provided services[38] and the relationship between users and the providers of the services [32]. The relation between the users and the providers of the services involve trusting the government and its agencies. This is affected by many factors such as the relation with the political system controlling the government, the government history with its citizens and other factors which are still the subject of research [27],[39].The protection of the privacy of personal information was among the identified factors that affect users’ trust in using e-government services[10]. Most government services require the collection of personal information from citizens in order to provide these services. Governments are expected to protect the personal information collected and to ensure it is used only for the purpose of collection. The trustworthiness of government agencies and organizations providing government services is usually assessed by the citizens’ expectations and the available knowledge about these organisations, the people working in them and the procedures followed to provide the services [27]. However, when government services are provided using the internet and other electronic means this assessment is affected by a gap of knowledge and associated speculations about how these services are provided and how personal information is protected and who is involved in providing these services. In addition, some studies suggested that privacy concerns also can be related to users not being able to have control

over their personal information when using e-government services [27] ,[34], [29], [40].

In this thesis, a novel framework for preserving privacy in e-government is presented that enables users of e-government services to have control over their personal information. The framework is evaluated and tested against the views of potential users to examine if preserving privacy using the provided novel privacy framework can increase users' trust in using e-government services.

I.3 Research Objectives and Scope

The main aim of this research is to develop a privacy framework for preserving privacy in the context of e-government which can provide a way for balancing and satisfying the security requirements of an e-government service (authentication requirements in specific) with users' privacy requirements by using a system thinking approach to understand the problem.

The research objectives can be summarised as:

- To demonstrate the usefulness of using a systems thinking approach in analysing complex concepts and problems where many aspects and perspectives are involved and need to be considered.
- To provide a rich understanding of the concepts of government and e-government and how they affect authentication in the context of e-government and preserving privacy in e-government by developing relevant conceptual models using a system thinking approach of Soft Systems Methodology (SSM).
- To develop a framework for preserving privacy in the context of e-government.

The scope of this research is limited to preserving privacy in e-government context where the privacy definition is limited to information privacy. The framework has been evaluated by stakeholders from three different countries and been applied in a case study.

I.4 Research Hypothesis

Balancing preserving privacy with the identified security requirements (authentication requirements in specific) when providing e-government services can be achieved using a privacy framework that provides a method for deriving the privacy and security requirements of a service, while considering the different perspectives of stakeholders and the influences of political, social and cultural factors and that achieving this preservation of privacy (information privacy) will increase the users' trust in using e-government services.

I.5 Research Approach

Electronic government research (EGR), which is sometimes called Digital Government (DG) research, is a relatively new field of research. This emerging multi-disciplinary research has been argued to be a non-traditional research area that spreads over a whole range of hard-pure, hard applied, soft-pure and soft applied sciences [41]. EGR mainly overlaps with Information Systems Research (ISR) and Computer Science (CS) Research and Public Administration research (Pub Admin) and shares its approaches with other disciplines' methods and research questions, in particular disciplines such as sociology and political sciences [41]. Therefore, e-government related problems are unique and complex and involve many aspects and dimensions that go beyond the scope of one specific discipline and this should be considered by researchers when deciding on an approach [41], [42]. In addition, although e-government can be similar to e-commerce in the aspect of using ICT to provide e-services to customers to increase the efficiency of these services [10], e-government still differs from e-commerce in many other aspects. These aspects include differences in the type of customers using the system, the structure of the way the e-services are provided and the way the resources should be provided to maintain the quality of the e-services [10]. In e-government, a government should target all types of customers who are benefitting from its services while in e-commerce; a firm can target only the type of customers who will bring benefit by using its services. With regard to the structure, e-commerce is more centralised while in e-government it is more distributed between government agencies. Another aspect is that in e-government the government is responsible to provide all resources in the best interest of the public while in e-commerce, a firm will provide the resources in

the interest of profiting the firm [10]. In addition, the relation between e-commerce customers and the commercial e-services providers are temporary and optional while e-government services customers have a mandatory and compulsory relationship that is not optional [37] Another difference is that e-government services are affected by political and cultural factors that have less affect in e-commerce [10], [37]. Therefore, existing solutions to the privacy problem in e-commerce cannot be used directly in e-government as the identified differences and added complexity must be considered [37].

The complex nature of the problem of preserving privacy in the e-government context and the need to consider many factors that involve human aspects make traditional approaches to tackle such problems ineffective. Thus, there was a need for a rich approach for investigating the problems and involved concepts from different perspectives. Due to the systematic characteristics of the investigated problem and the fact that the concepts involved can be perceived from different perspectives and have no exact definition, a systems thinking approach and in particular Soft Systems Methodology (SSM), as in [43], [44], was selected for investigating the problem. Using SSM, four Conceptual Models (CMs) relevant to the concepts investigated in the problem were developed and a Privacy REquirements in E-GOVernment framework (PRE_EGOV) was developed informed by these conceptual models. The developed conceptual models are relevant to the concepts of government, e-government, authentication in the context of e-government and preserving privacy in the context of e-government. These CMs were validated using SSM rules and the definitions of the concepts were verified by relevant stakeholders. Details of the research approach and the validation and evaluation of the developed CMs are provided in Chapter two.

The proposed framework was evaluated in two phases. The first phase was to evaluate if the Conceptual Model relevant to Preserving Privacy (CMRPP) in e-government and the proposed framework (PRE_EGOV) informed by the CM reflect the perspectives of relevant stakeholders. This was done using an online survey that was distributed in three countries that have some similarities and differences in their governments and national characteristics. The survey design is presented in chapter six while the survey results are discussed in chapter seven. Suggested enhancements from the survey results were used to develop

the proposed framework. Details of the developed framework (PRE_EGOV) are presented in chapter eight. The second phase was to evaluate the usability, usefulness and acceptance of this framework. This was done by applying the framework in a real world case study to demonstrate its usability and applicability. Details of the application of the case study are presented in chapter nine. Then, the usefulness and acceptance of the framework were evaluated using semi-structured interviews with relevant stakeholders as provided described in chapter ten. The evidence collected from both phases of evaluation confirmed the usability, usefulness, acceptance and validity of the work presented in this research. However, the work in this research is relevant in action research since the relevance of SSM in action research [18] is confirmed by evidence found in cases studies conducted by researchers [43],[44]. Therefore, refinements to the developed framework are devised based on the observation of the application of the framework in many case studies following an iterative process of action research. However, to generalise the framework it needs to be tested using an iterative process so that refinements that need to be made due to the observation of its application can be applied until there are no more changes, and this final version can then be used as a general framework. In this thesis, the first round of action research is presented where the framework has been tested using one case study due to limitations in time and resources. Suggestions for further enhancements are provided as future work.

I.6 Research Contributions

The main contributions of this research are:

- A novel approach to the analysis of privacy requirements when providing e-government services. The Privacy Requirements in E-GOVernment framework (**PRE_EGOV**) provides a way for deriving and balancing privacy and security requirements of an e-government service while considering the ownership right over processed information. The framework meets the identified requirements for privacy frameworks in e-government developed in this research.

- Demonstration of a structured and systematic method of modelling the systems in the domain of government and its service systems with an

emphasis on e-government, authentication and privacy preservation, using Soft Systems Methodology (SSM). To our knowledge, this approach is unique in the context of e-government research.

- Development of Conceptual Models (CMs) for the concepts of government and e-government which can be used as reference models when discussing relevant issues to the concepts and provide rich understanding of the transition from government to e-government.
- Development of CMs for the concepts of Authentication and Privacy in the context of e-government.
- Definition of requirements for privacy frameworks in the context of e-government.
- An approach for evaluating the Root Definitions (RDs) of the developed Conceptual Model CM) relevant to preserving privacy using an online survey.

I.7 Thesis Structure

This thesis is organised as follows:

Chapter One--Introduction provides an overview of the thesis, the research problem, the research approach and highlights the main contributions.

Chapter Two—Research Approach describes the research approach, provides an overview of Soft Systems Methodology (SSM) and justification for tits use. The research's logical steps and the evaluation approach are presented.

Chapter Three—Understanding Electronic Government aims to develop a rich understanding of the concepts of government and e-government. It presents and justifies two conceptual models relevant to the concepts of government and e-government that are used to develop rich understanding of the problem domain and the aspects that should be considered when investigating e-government problems.

Chapter Four—E-government Authentication Frameworks presents a conceptual model (CM) relevant to authentication in the context of e-

government which was developed using SSM. This is used for structuring the literature review of existing e-government authentication frameworks and to identify gaps and limitations in these frameworks.

Chapter Five—Preserving Privacy in the Context of E-government presents a Conceptual Model relevant to Preserving Privacy (CMRPP) in e-government developed using SSM. It is used to review and identify gaps and limitations in relevant literature and the requirements for privacy frameworks in e-government. A novel approach for preserving privacy in e-government (PRE_EGOV) is proposed.

Chapter Six—Evaluation of CMRPP-Survey Design provides details of the validation of the CMRP and the PRE_EGOV framework. It presents the design of an online survey for examining the validity of the developed CMRP and the elements of the proposed framework according to relevant stakeholders' viewpoints.

Chapter Seven— Evaluation of CMRPP-Survey Findings presents and discusses the results of the online survey in chapter six. Further requirements for preserving privacy in e-government are identified and considered as enhancements to the framework.

Chapter Eight—A Framework for Privacy REquirements in E-GOVernment (PRE_EGOV) presents and justifies details of the approach for preserving privacy in e-government (PRE_EGOV) and discusses relevant work in the literature.

Chapter Nine—Empirical Research: EduPortal Services provides a detailed description of the empirical application of PRE_EGOV framework on a real world case study. The application of PRE_EGOV is part of the evaluation of the framework.

Chapter Ten—Evaluation of the PRE_EGOV Framework, presents the evaluation strategy and details and findings of the usability and usefulness evaluation based on the selected case study.

Chapter Eleven—Conclusion and Future Work concludes the thesis by discussing the benefits of the proposed framework and the results and findings

concluded from applying the framework in the empirical case study. It summarises the main contributions of this research, and states the limitations and directions for further research.

Chapter Two

II. Research Approach

II.1 Introduction

Preserving privacy in the context of e-government is a semi-structured problematic issue as although there is a structure in the technological solutions available for preserving privacy, the issue still involves complex concepts and is affected by a large variety of influencing factors. In such situations the problems and their causes cannot be defined and described specifically but can be expressed by the perceptions of observers of the real world situation and therefore are considered 'soft' problems rather than 'hard' well defined problems [43]. Thus, such a problem situation should be considered from many perceptions or from a common agreement between different perceptions and traditional scientific approaches are not appropriate for understanding and resolving the complexity of such problems [43]. Soft systems approaches were created to address multifaceted problem situations where the problem is not clearly defined or even agreed upon by people involved in the situation and where the human factor should be considered. Soft Systems Methodology (SSM) was proposed by Checkland [43] as a general system thinking approach for tackling soft problematic situations where human activities are involved. Brian Wilson adapted SSM into a practitioner approach and introduced different methods of SSM supported with practical examples in [44]. SSM is a useful and powerful approach for exploring complex messy situations that involve divergent views[43], [44]; for this reason it was chosen as a research approach for tackling the problem of preserving privacy in the context of e-government - in particular the EMA method of SSM was selected. This chapter discusses the research approach to investigating the problem of preserving privacy in e-government, describes and justifies the methodology used and provides the research steps. An overview and justification of the research approach is presented in section two. In section three SSM and the SSM method of EMA are described. . Section four provides brief examples of using SSM in the literature and justification of the use of SSM in this research. An illustration of

the research steps, where SSM was used is provided in section five. Section six gives an overview of the evaluation approach.

II.2 System Thinking Approach

The nature of a research problem determines the selection of an approach to tackle that problem. Traditional approaches for developing information systems such as Waterfall and Rapid Application Development models [45] work well with well-defined problems that have low human/social complexity. However, in situations where the problem is ill-defined and the human/social complexity is high these approaches are limited in tackling such problems and a systems analysis approach should be applied such as a system thinking approach. Systems thinking approaches involve a set of problem analysis methods and techniques based on system analysis and defined as "a *way of thinking about, and a language for describing and understanding, the forces and interrelationships that shape the behaviour of systems[46]".* Systems thinking approaches contain hard approach and soft systems approaches. A hard system approach is used to make improvements to a defined-problem situation and to determine the how to increase the efficiency of a system based on given inputs, while a soft system approach is used to determine what needs to be done in an ill-defined problematic situation [47]. A hard system approach is used when the problem is relatively structured and the relationships between the problem variables are visible and can be expressed quantitatively. Examples of hard systems thinking methods are traditional Operational Research (OR) methods and Systems Dynamics [47]. System Dynamics (SD) involves developing simulation models related to the system that require historical data of the behaviour of the system and use internal feedback loops and time delays to understand the dynamic behaviour of the system [48] and are usually used for policy analysis and design [49]. A soft system approach is used when there is a lack of structure to the problem and a high involvement of human aspects where different stakeholders have different or even conflicting views about the problem situation. The aim of soft system methods in general is to learn about the problem situation from different perspectives and then define and bring a structure to the problem that helps gain a shared and mutual perception of the problem while considering other influencing factors. Examples of soft systems approach methods are

Strategic Options Development and Analysis (SODA)[50] and Soft Systems Methodologies (SSM) [43], [44] . Strategic Options Development and Analysis (SODA) provides cognitive mapping for eliciting individual's views and used mostly for strategic decision making, however, it does provide a general view of the systems that might be relevant to the problem [47]. Soft Systems Methodology (SSM) is a general method for system structuring and redesign which applies system thinking principles and system concepts[51]. The problem of preserving privacy in e-government has systemic characteristics as it involves many aspects and is influenced by relations with other systems. This makes a systems analysis approach such as system thinking approach an appropriate choice. It is an ill-structured problem situation and inherits the complexity of relevant concepts from government and e-government and requires the consideration of multiple perspectives of different stakeholders involved in e-government services and consideration of the influence of political, social and cultural and legal aspects as well as the involvement of the human factor. Therefore, SSM was selected for analysing this problem and relevant concepts as it uses a rich approach that takes a wide range of factors into account, e.g. social and political aspects and aims to suggest change that is meaningful and feasible in the organisational context [44].

II.3 Soft Systems Methodology (SSM)

SSM was proposed in the 1970s by Peter Checkland [43]. This was followed by a practical adaptation by Brian Wilson [44]. The basic principles of SSM involve the use of the intellectual construct of a "Root Definition" (RD) to capture the purpose of the system through a textual definition; and the use of a Conceptual Model (CM) to describe what the system must do, to be the system defined in the root definition [44]. An RD describes a transition process where the purpose will be achieved when an input is transformed to an output [44]. SSM as proposed by Checkland can be represented by the seven steps shown in Figure II.1. The main benefit of the conceptual model is that it makes the structure of the problematic situation explicit and aids in exploring the interdependencies between the system activities. An important step in using SSM is to compare the developed Conceptual Model (CM) to the real-world situation. This step improves the understanding of the problem situation and

usually leads to the identification of the changes required in order to solve the problem situation or enhance a current system.

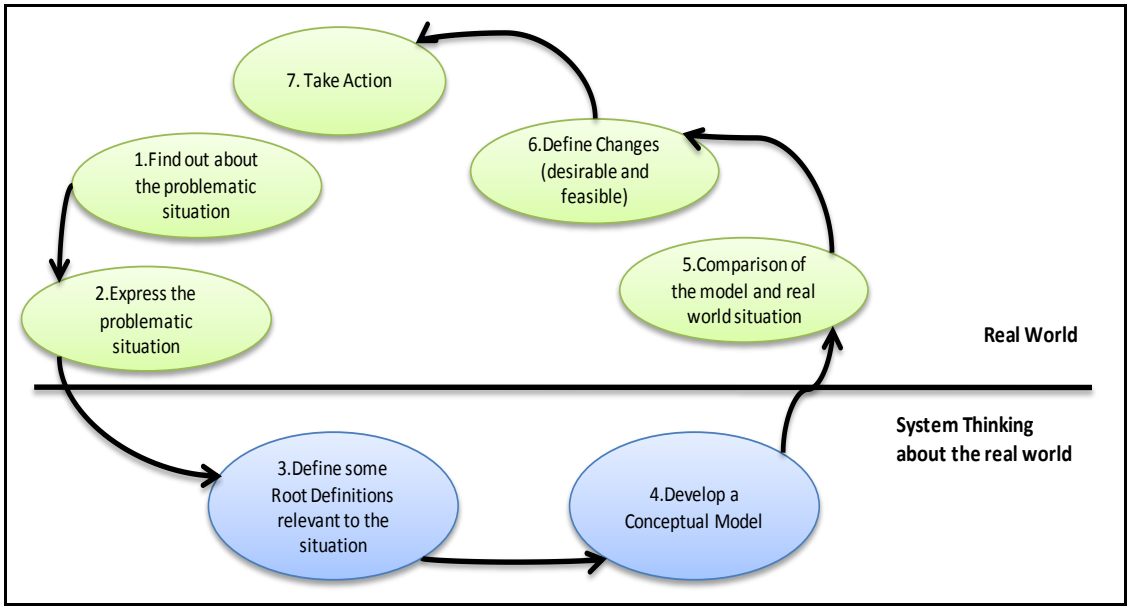


Figure II.1: SSM Steps after Checkland [44].

II.3.1 Enterprise Model Assembly (EMA) Method

The Enterprise Model Assembly (EMA) method of SSM was proposed by Wilson as a useful device for ensuring the inclusion of the total range of systems required within the developed Consensus Primary Task Model (CPTM) [44]. Enterprise modelling is a useful way of thinking and representing a high level of generality of an organization or an organisation unit while ensuring that all the required characteristics and their relations have been considered.

The CPTM is an “intellectual construct capable of representing any enterprise” [44], and describes any enterprise in terms of the four types of systems illustrated in Figure II.2. These systems are the transformation process (es) (T) which represent the core purpose of the organization; the supporting systems (S) which provide the required support to enable all activities to take place; the linking systems (L) which provide interfaces with the enterprise environment, and the planning, monitoring and control (PMC) system(s) which ensure that the enterprise is able to respond to internal and external dynamic changes [44].

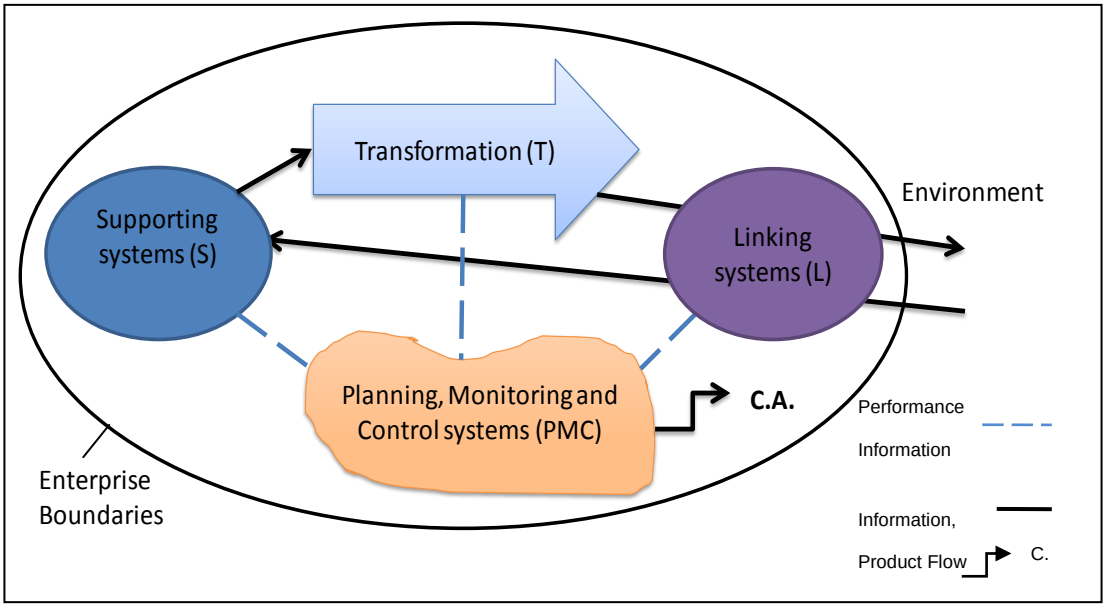


Figure II.2: The Enterprise Model Assembly (EMA) after Wilson [44].

II.3.2 Developing a Conceptual Model

II.3.2.1 Developing the Root Definitions (RDs)

The RDs are built according to the knowledge gained from capturing different perspectives and views of the problematic situation or the concepts investigated. The concepts can be expressed in pictures which can be used by the analysts when consulting involved parties to gain more knowledge about their views and opinions on the problem. In addition, the analyst understanding of the concept or the problematic situation helps in shaping the RDs that comprise the different worldviews. A RD statement should consist of at least two elements, a transformation (T) which captures the purpose of the system and a world view (W) that describes how to achieve that purpose. Other elements of CATWOE [44] can make the RD richer are the Customer (C), Actor(A), Owner(O), and Environmental constraints (E).

II.3.2.2 Developing the Consensus Primary Task Model (CPTM)

The CPTM is derived from the complete set of RDs, by logically deriving the set of activities necessary for the system described in the RD. For each part of the RD a set of activities is created to describe how that part can be achieved. In this context, the "logic" is that of the analyst, based on the identification of logical dependencies between activities and determining what "must" be done, to achieve identified outcomes. Therefore, no two analysts will develop exactly

the same activities from a given set of RDs. However, they will be similar as the aim is to express the wording in the RD. The graphic representation of an activity can be of any shape (usually a round or a cloud shape) and the relations between the activities are represented by arrows [44].There is no standard tool for CM drawings and usually CM is drawn by hand. An example of a complete CM developed in this research can be found in Appendix C.

II.3.2.3 Subsystems Decomposition

After completing the CPTM, subsystem decomposition can be used to identify related subsystems. In this decomposition, first a set of potential subsystems is derived, and then the CPTM is analysed to map activities in the model into the potential subsystems while maintaining their links with other activities. Additional subsystems are added where needed, until all the activities in the model are in subsystems. The links between the activities help in determining how the subsystems interrelate. Then the subsystems are named on the basis of the common goal of the activities within a subsystem and what they are aiming to achieve. The relations between subsystems are decided according to interdependencies between the activities. To validate this step, any subsystem must comply with “systems rules”, including the necessity to include monitoring and control activities. An additional step that helps clarifying the relations between the subsystems is to present the subsystems in a high level subsystems graph where the subsystems are grouped into levels according to their relations to each other. The highest level has the subsystems that have a relation with all the other subsystems in the CM while the second level has subsystems that have relations with some subsystems in the CM. The lowest level has the subsystems that have relations with only a few subsystems. Examples of the high level of subsystems graph can be found in **Error! Reference source not found.**and Figure III.3.

II.3.3 Validation within SSM

SSM rules are used to test the structure of the developed Root Definitions (RD) and to validate the CM. The defensible logic as illustrated by Wilson in [44] is presented in Figure II.3.

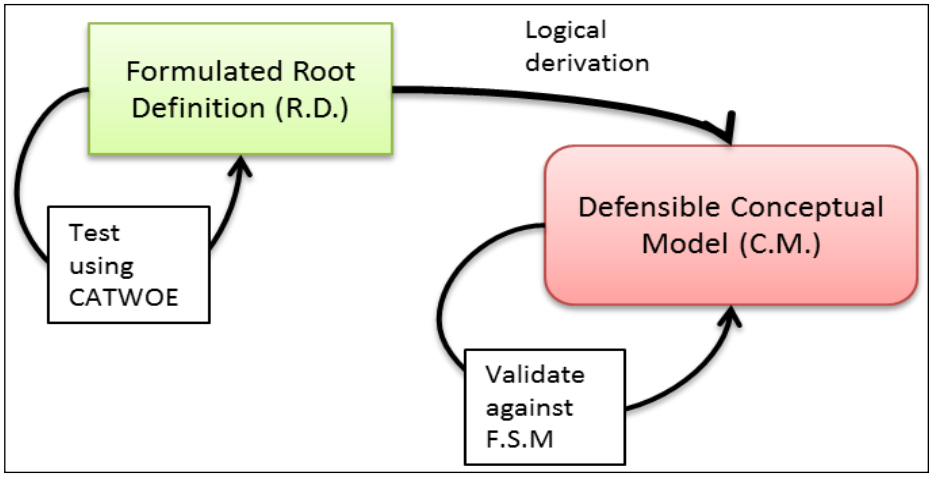


Figure II.3: The defensible intellectual relationship [44].

II.3.3.1 Root Definitions validation

SSM rules provide specific rules for testing and validating the structure of a developed RD by testing it against the mnemonic CATWOE as explained by Wilson in [44]. In brief the **CATWOE** elements are:

- **C** is for Customer of the system.
- **A** is for Actors who perform the system activities.
- **T** is for the transformation process which a RD is describing and it is a mandatory element.
- **W** is for the World View (*Weltanschauung*). It is the statement of belief on how the transformation can be achieved (also a mandatory element).
- **O** is for the Owner of the system
- **E** is for Environmental constraints that might place limitations on the system activities.

Any RD should contain a T and a W; however for a richer RD it is useful to include the other elements.

II.3.3.2 Conceptual Model validation

SSM provides a set of rules for validating a CM (detailed in [[44],p. 28]) and in brief:

- The CM should be developed based on only the relevant RD and not on other resources in the real world situation; also the CM should be checked against the relevant RD to ensure that all the words in the RD are covered.

- For each activity, sufficient words should be used to describe the transformation process in a precise way.

- Arrows in CM have logical dependencies that represent the relations between the CM activities.

- The CM should be defensible against the Formal Systems Model (F.S.M). This means that it should have connectivity, purpose, measures of performance, decision-taking processes (control), boundary, resources, hierarchy, and at least one monitor and control subsystem which are the features that should be in any model of a Human Activity System (HAS) [44].

SSM is not a technique, but a structured way of representing thinking about a particular complex problematic situation involving human activity. However, once the thinking has been made explicit, it allows the analysts to defend it. Using SSM rules makes the CMs defensible and what is left is to test if the RD reflects the views of the people involved in the problematic situation. However, possible enhancements for a developed CM lie in enhancing the RD by discussing it with different stakeholders to determine whether the CM defined "systems" reflects their views and perception of the purpose of the concept, in order to enrich the understanding of the purpose of the investigated concept and enable the deployment of a system that serves that purpose.

II.4 Research Approach Using SSM

The research aim is to create a framework for preserving privacy in e-government that balances between preserving users' privacy and maintaining security when providing e-government services. However, there are different perceptions of privacy [52] and divergent views on how privacy can be preserved in e-government [11]. What can be seen as private from the perspective of a user of e-government services might not be viewed in the same

way from the perspective of an e-government services' provider. In addition, any proposed solution or framework for preserving privacy in e-government involves human activities, and is influenced by many factors - social, cultural and political factors - should take account of relevant laws and regulations [13], [53]. Therefore, a rich approach is needed to understand the concept of privacy and identify relevant factors that should be considered when proposing a solution or a framework for preserving privacy in the e-government context. SSM is recognised as a helpful in formulating and structuring the thinking about complex messy situations that involve divergent views of the problem or purpose of a system [44] and has been used extensively in the literature to tackle similar complex concepts and messy situations, such as in [54], [55] and [56]. There are numerous practical examples of successful usage of SSM in various domains such as medical, social, and military fields. For example, the use of SSM in designing evaluation plans for the UK National Health Service (NHS) [57]. SSM is described as a learning system as the experience gained by applying SSM informs people's knowledge about their organization and based on that knowledge, changes can be made to the structures and business processes of this organization. This is supported by evidence by many practical examples published in detail by Checkland and Scholes [58] and Wilson [44]. Also, the literature reports many successful examples, where SSM proved to be a useful and powerful approach for tackling unstructured problematic situations and providing a deep understanding of complex concepts [54], [55] and [56]. Therefore, SSM was chosen to gain a better understanding of the concepts involved in preserving privacy in e-government and to develop relevant conceptual models of the problem. The EMA method of SSM [44] was used in developing relevant CMs for the concepts of government, e-government, authentication in e-government and preserving privacy in e-government. The reasons for choosing the this method are that e-government is an enterprise and maintaining security of the services and preserving privacy in e-government is a primary activity of this enterprise and not a temporary issue that needs resolution. Also, the conceptualisation of preserving privacy in e-government needs to be at a high level of generality to increase its applicability in different governments. Therefore, the EMA method was the best of SSM methods to use as it is used to create CMs al models.

II.5 Research Plan

The system thinking approach provides a rule for systems modelling, which states ” a system which serves another cannot be defined and modelled until a definition and model of the served system is available [43]”. This was detailed in [59] with examples of the SSM role in information systems development. Here, preserving privacy and maintaining security in -government are service systems and the government is the system being served by these systems. Figure II.4 shows the research plan.

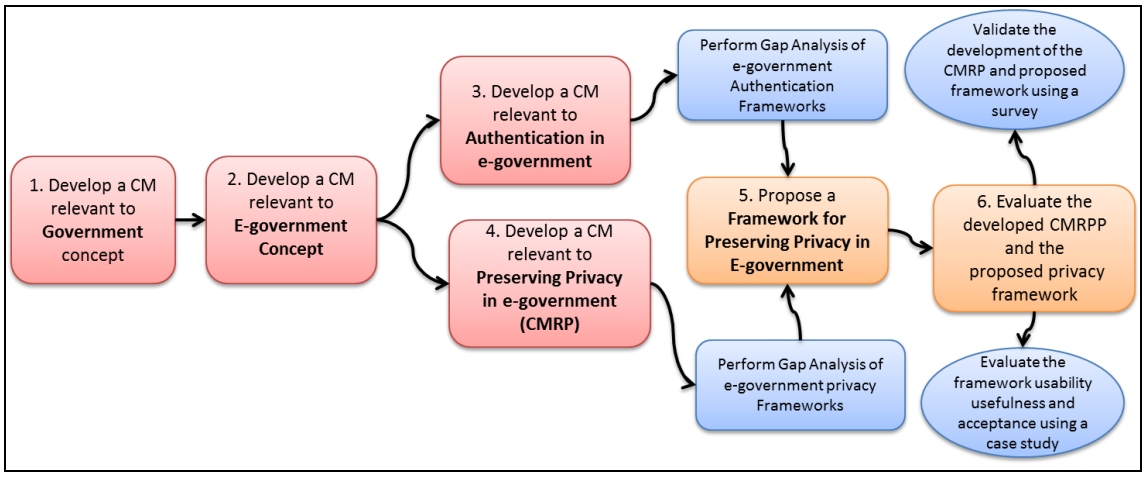


Figure II.4: Research plan steps

The first step was to develop a CM relevant to the concept of government (sectionIII.3) and a CM relevant to the concept of e-government (section III.4). The aim in developing of these CMs is to gain a deep understanding of the problem domain and the aspects that should be considered when tackling problems relevant to the domain. Next, there was a need to understand how security is maintained by governments when providing e-government services and in particular how users are authenticated and identified when requesting e-government services. E-government authentication frameworks are developed and used in e-government to describe how to authenticate users of e-government services and how to protect the security of these services. Examples of these frameworks are UK authentication framework [60], and US authentication framework [24]. SSM was used to develop a CM relevant to authentication in the context of e-government and this was used to investigate current authentication frameworks and to identify any gaps in these frameworks (section IV.7IV.3.2). Another CM relevant to preserving privacy in e-government was also developed using SSM. This was used to investigate current privacy

frameworks and methods of preserving privacy in e-government and to identify gaps and possible enhancements (section 1.1V.3.1). Based on this CM, a framework for preserving privacy in e-government was proposed (section V.5). The CM relevant to preserving privacy and the proposed privacy framework (PRE_EGOV) were evaluated using an online survey. The survey was designed to validate the CMRP and elements of the proposed framework. It was distributed in three countries and targeted users of e-government services, the services providers, developers and government representatives, who are involved in the provision of e-government services. The knowledge acquired from developing the previous CM and the feedback from the online survey on the CMRPP and the proposed PRE_EGOV framework were used to identify enhancements to the proposed framework for preserving privacy in e-government (sectionVII.8). These enhancements were considered in the final development of PRE_EGOV framework (section VIII.2). To evaluate the framework, it was applied in a case study (sectionIX.3) and the usability and usefulness of the framework was evaluated (chapter X).

II.6 Evaluation Approach

A CM developed using SSM is not a complete representation of the real world situation, but is relevant to that situation and represents the world view(W) described in the RD which the CM was derived from [44]. Therefore, a developed CM cannot be evaluated direct against the real world, but the W stated in the RD can be evaluated to see if it reflects the real world views about the situation [44]. However, in most cases of using SSM, the RDs are constructed based on the W of relevant stakeholders and the evaluation for these RDs are done by reviewing the RDs with the stakeholders to validate them. In this research, the developed CMs relevant to government, authentication in the context of e-government and preserving privacy in the context of e-government were derived from RDs, which were built on agreed definitions of the relevant concepts in the literature or definitions which are stated in relevant standards. The argument for each CM is presented as appropriate in the relevant chapter, where each developed CM is explained in detail.

The evaluation of the validity of the CM relevant to preserving Privacy in e-government (CMRPP), and the usability and usefulness of the developed PRE_EGOV framework was done in two phases. The first phase was about validating that the defined RDs in the developed CMRPP reflect the views of relevant stakeholders. However, there were no agreed definitions or relevant standards that define the purpose of preserving privacy in e-government and consider different perspectives, so the statements of the relevant RDs were validated using an online survey that was distributed in three countries. The findings of the survey are presented in sectionVII.7. The PRE_EGOV framework was also evaluated by the survey and as a result of the findings and suggestions resulted from the survey, enhancements to the framework were identified (see section VII.8). The second phase was about evaluating the usability, and usefulness of the PRE_EGOV framework. The usability of PRE_EGOV framework was evaluated by applying it in a real world case study (see section IX.3), then its usefulness was evaluated (section X.3). However, this is a one round application of the framework and a long term usefulness evaluation will require applying the framework on many cases and in different countries and for longer period to evaluate its long term usefulness and generality. This could not be done in the time frame available.

II.7 Conclusion

The research approach followed to gain an understanding of the problem of balancing preserving privacy with maintaining security in the context of e-government has been presented. Due to the unstructured nature of the research problem and the complexity of the relevant concepts, a system thinking approach was adopted to investigate the concepts relevant to the research problem. SSM and in particular, the SSM method of EMA was used to develop four CMs relevant to the concepts of government, e-government, authentication in e-government and preserving privacy in e-government. The research steps were illustrated and the evaluation approach explained. The quality of the models created in SSM relies on the expertise of the analyst and his or her ability to derive a set of RDs that capture the purpose of the system to be analysed. Following SSM rules, the developed CMs are defensible and the important step is to evaluate that the RDs) reflect the views of involved parties in the situation being addressed.

Chapter Three

III. Understanding E-government

III.1 Introduction

The deployment of e-government projects around the world has faced various obstacles and in many cases has failed to satisfy the expectations both of the government and its citizens in its delivery of government services. Maintaining the security of the provided services while preserving the privacy of the users are examples of these obstacles [61]. The concept of electronic government is complex, multi-disciplinary and influenced by a variety of perceptions from different stakeholders. Such a complex, multi-disciplinary real-world problematic situation is not amenable to traditional business analysis approaches, and instead needs a system thinking approach. Thus, SSM was used to understand the concepts of government and e-government and to explore the activities involved in order to understand the purpose of government, prior to considering where e-government might be appropriate and how to tackle the problem of preserving privacy while maintaining the security of e-government services. However, in following the systems modelling rules [43], e-government was considered as a service system to serve and support the activities of government (system served). Therefore, there was a need to explore and understand the system served (government) from different perspectives in order to understand the service system (e-government). This chapter presents the research approach used to understand the problem domain by modelling the concepts of government and e-government using the EMA method of SSM. The developed CMs can be used as reference models to give better insight into the transformation process between traditional government activities and e-government activities. Also, the developed CMs can be used to gain better understanding of the problem domain when investigating relevant research problems. The CM relevant to the concept of government covers diverse perspectives about the purpose of government and can be used to illustrate how government activities can be considered in the government to e-government transition process and how it can help to decide what e-

government is supposed to do. The CM relevant to e-government can be used as a framework for exploring various issues and obstacles facing e-government projects, as the CM provides a rich picture of the purpose of e-government and the activities that should be carried out to achieve that purpose. This chapter reviews related work to understand the concept of e-government and the transition process from government to e-government and presents the CMs relevant to government and the concept of e-government. It covers brief example of how the developed CMs can be used in practice.

III.2 E-government in the Literature

The concept of e-government appeared around 1990 when governments started to use the internet to build government websites that present information about the government and its agencies to the public and gradually developed into providing government services through electronic means [62], [6] and [20]. Since then, research has been active to investigate this new phenomenon and the past 10 years saw a fast and significant growth in published research on topics relevant to e-government. Today e-government research is recognised as a multidisciplinary area that involves many research domains [41]. E-government has been investigated from various perceptions such as business benefits, social impact, political processes, managerial issues as well as technical concerns. As the topic involves many issues, research papers vary in discussing these issues as the authors come from different perspectives and look at the domain from different aspects. However, few papers used a general approach in discussing the topic , such as [15] and [63], while the majority of studies were built on particular e-government projects, for example, [64],[65], and [66]. A recognised review of the literature was made by Heeks and Bailur [7]. They provided a content analysis for some of the current literature with an emphasis on the impact of e-government, research methodologies and the use of theory in e-government research along with practical recommendations and knowledge accumulation. Another review of e-government literature is by Yildiz who reviewed the limitations occur in e-government literature and came up with methodological and topical suggestions to be investigated [8].

Some of the key limitations inferred from these reviews are:

- Lack of a standard definition for the concept of e-government and of studies that capture various meanings of the concept of e-government.
- Lack of clarity about the methods used and the assumptions made in research.
- Lack of use of theory in research and inadequate engagement between theory and practice.

This research seeks to avoid these limitations for as possible.

III.2.1 Understanding government to e-government transition

In many cases the government to e-government transition involves enhancement and sometimes redesign of current government services. However, the decision on what government services should be provided by e-government and what e-government is expected to do is vague and involves many perspectives. There have been several efforts in the literature to analyse and understand the transition process from traditional government services to services delivered through e-government where different aspects of the e-government evolution process have been discussed [62], [6],[67] and [63]. However, evaluation of e-government overall progress and e-government maturity were the main focus of earlier research [68]. E-government models and frameworks proposed in the literature are constructed mainly according to either the development stages and/or level of communications. A framework presented by Symond [69] suggested four stages of e-government development: one-way communication, two-way communication, exchange and portals. These four development stages where recognised in the literature as a way to assess the progress of e-government, though sometimes different terms are used such: initiation, interactive, transaction and integration [70]. Layne and Lee [68] suggested a maturity model for evaluating e-government by the growth of four stages: (1) Cataloguing - there is an online presence for the government department(s), (2) Transaction – citizens are able to interact with the internal government systems, (3) Vertical integration- integration between government departments and systems in local level and (4) Horizontal integration- integration between government departments on the level of the whole government. This model is widely used to describe and evaluate the

development of e-government [70]. Belanger and Hiller [11] added a fifth stage to the Layne and Lee model which corresponds to citizen participation in politics. From the perspective of the level of communication, Brown and Brudney [71] classify e-government services into three categories depending on the level of communication with other parties. These are Government–to-Government (G2G), Government-to-Citizen (G2C), and Government-to-Business (G2B). Another category added by the US government is Intra-government Internal Efficiency and Effectiveness (IEE) which focuses on the delivery systems within the e-government system [72]. However, earlier frameworks describe the stages of e-government development as a sequential series, where each stage follows another, which is not always true in reality [8].

Other studies focused on using existing business process models, used for analysing business to e-business transition, in the context of e-government, an example is the study done by Fang [6]. Davison et al. [62] proposed a transition model which can be used to illustrate and compare the progress of an e-government project compared to other governments and to identify what developments are needed to go further. The multidisciplinary nature of e-government is only been recognised by few studies, such as the multidimensional model for e-government proposed in[15] and illustrated in [73]. This model explored different views across different abstraction layers and levels of the development process and covered a wide range of views and inter-relationships in the deployment of e-government.

From another perspective, some studies focus on the obstacles facing the development and deployment of e-government services when transferred from government services and the issues raised by the implementation of e-government, such as the social and cultural issues as well as security concerns and technical issues. Evans and Yen [72] discussed some of the social and cultural impacts associated with e-government deployment and emphasized the need to engage different stakeholders in the early stages of the implementation of e-government to avoid undesirable impacts such as resistance and lack of government employee support. On the other hand, disregarding the environmental influences has led to the failure of several e-government projects to satisfy the expectations both of the government and its citizens. For example, a study by Roa and Lee [61] showed that citizens' concerns about their privacy,

discourage them from providing terrorism investigation tips to the FBI 'Tips Online' service.

III.2.2 The concept of e-government

The concept of e-government has proven to be complex, multidisciplinary and influenced by a variety of perceptions from different stakeholders [72], [73], and [8]. The purpose and role of e-government has been the main subject of many studies and is discussed widely in e-government road mapping workshops from different perspectives, ([6], [20], [74], [63] and [75]). However, reviews of e-government literature have shown that there is a lack of a standard definition for the e-government concept, together with a lack of studies that capture the various meanings of the concept [7] and [8]. Many definitions, such as [71], [17] and [76] define e-government as the use of Information and Communications Technologies (ICT) to provide information and services from the government to the public. The main aim of deploying e-government has been seen from different perspectives. Some see e-government as a tool to improve the quality of service delivery and to allow citizens to have access to information and services wherever and whenever they need [77] and [75], while others see e-government as an opportunity to empower people through access to information and participation in public policy and decision making [6].

III.3 Developing a CM Relevant to Government

To understand the concept of e-government, there was a need to understand and analyse the concept of government itself. However, despite recognising e-government as a system to support and enhance government activities, little attention has been given to the system supported by e-government i.e. the government system. A government can be considered as a purposeful system, as it is constituted as a group of people and resources organised as a whole in order to accomplish that purpose. These characteristics fit within Peter Checkland's definition of "purposeful" Human Activity Systems (HAS) where he argues that such systems are highly unstructured and cannot be studied with the well-established methods of science [43]. Thus, the EMA method of SSM (section II.3.1) was selected to model government system in order to understand the impact of the diverse range of perceptions of its purpose.

III.3.1 Developing Root Definitions (RDs)

Developing a RD that states what government is understood to do was not a straightforward task. The purpose of government is observed differently according to stakeholders' points of view or W. Therefore, various RDs were initially developed to capture these diverse perspectives of the concept. These were built according to the knowledge gained from various definitions found in the literature which captured different perspectives of stakeholders about the concept of government. Also, the researcher's understanding of the concept and the consultation of experts in the government research field were used to shape the final set of RDs that comprise the different Ws about the concept after several iterations.

For validation, each RD has been validated using the CATWOE mnemonic for testing the structure and words chosen in the RD (section II.3.3.1). Using the EMA method, RDs were defined for four types of systems: the transformation process (T), the supporting systems (S), the linking systems (L), and the planning, monitoring and control (PMC) system(s) (see section II.3.1). We presented three root definitions for the core transformation to reflect different stakeholders' perceptions of the purpose of government. The following are the root definitions for the transformation process developed for the government enterprise model, the complete list of RDs can be found in Appendix A

RD1- Core Transformation (T1)

> *-- A system to achieve an agreed "common good" for a nation within internationally defined boundaries by instituting the necessary structures and institutions to deliver approved policies and achieve appropriate targets while constrained by political views, common beliefs, and principles.*

RD2- Core Transformation (T2)

> *A system to ensure the survival and protection of a nation welfare and strategically valuable resources and assets by taking responsibilities of detecting, deterring and defending as appropriate against externally and internally arising threats while considering performing necessary security*

measures through established structures and institutions and within constraints of relevant international agreements.

RD3- Core Transformation (T3)

-- A system to deliver those services, which are deemed to be most effectively and efficiently performed for the benefit of all the nation's people by determining the balance of advantage between public and private provision of the services, or a mixture of these while considering the needs and expectations of all the nation's people and within constraints of cultural and economic influences.

The above RDs reflect the principal aims of the purpose of a government and other aspects related to the concept are covered by the supporting RDs, Linking RDs and planning, monitoring and control RDs which can be found in Appendix A.

III.3.2 Developing the Consensus Primary Task Model (CPTM)

The Consensus Primary Task Model (CPTM) is derived from the complete set of RDs, by logically deriving the set of activities necessary for achieving the system described in the RDs. In this context, the "logic" is that of the analyst, based on the identification of logical dependencies between activities and determining what "must" be done, to achieve identified outcomes. The complete CPTM obtained, included over 500 activities and was validated by testing it against the Formal Systems Model (FSM) where the model is tested for inclusion of the following features: connectivity, purpose, measures of performance, decision-taking processes (control), boundary, resources, and hierarchy, which are the features that should be in any model of a Human Activity System (HAS) [44].

III.3.3 Subsystems Decomposition

After completing the CPTM, subsystem decomposition was performed, where the CPTM was analysed to locate subsystems and to decide how the identified subsystems are related. The relation between subsystems is identified based on how the activities in each subsystem relate to the activities in other subsystems (sectionII.3.2.3). The subsystem decomposition resulted in 31 subsystems. These subsystems were grouped into levels (sectionII.3.2.3)

based on how they relate. **Error! Reference source not found.** shows the identified subsystems and their interdependencies; note that the dotted subsystems indicate a repeat of an existing subsystem and are presented again for clarity.

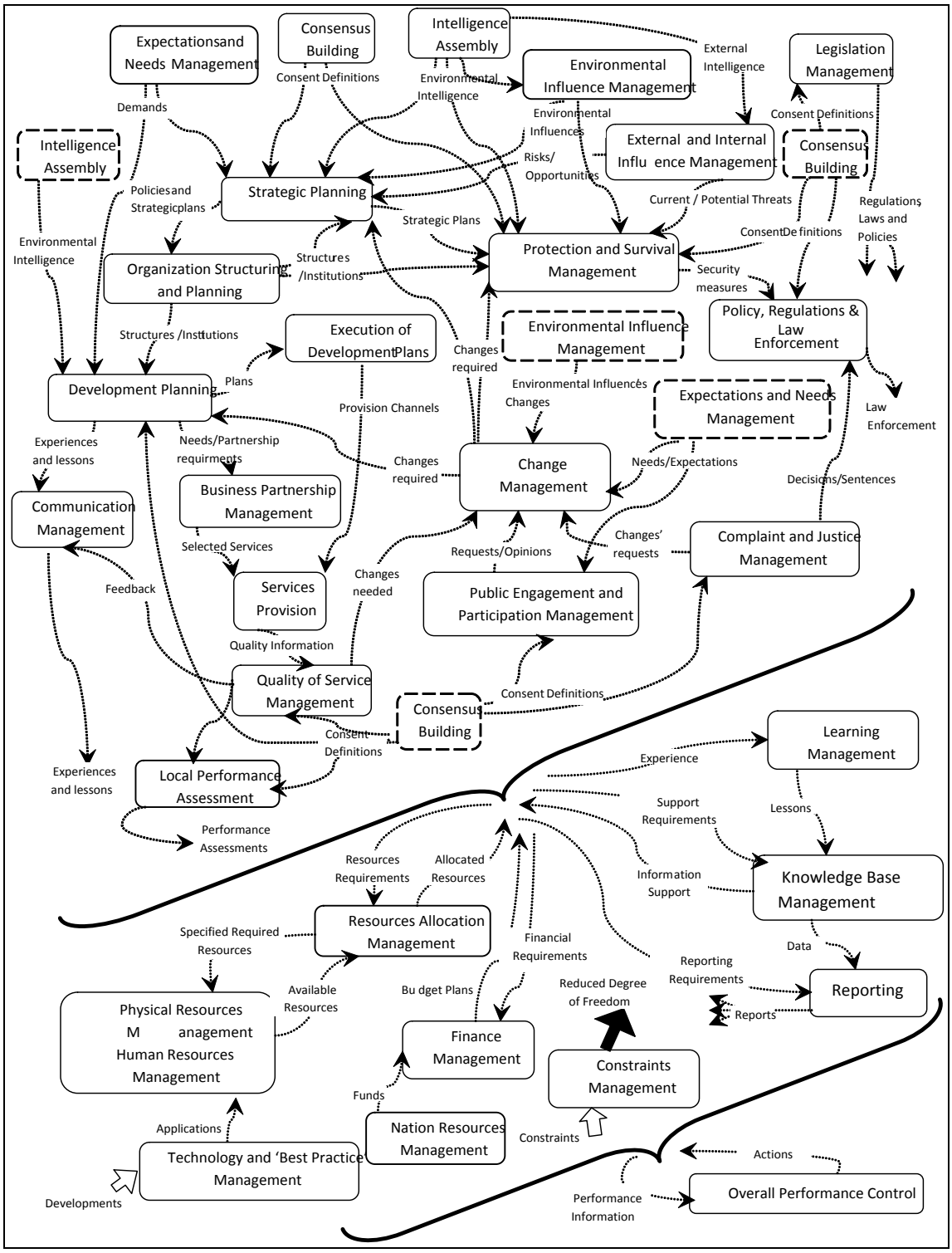


Figure III.1: High Level of Subsystems of the CM relevant to Government

The subsystems were grouped into three different levels:

- The highest level, level 1, has the Overall Performance Control subsystem which receives performance information from all other subsystems and assesses the required actions according to expectations and needs of the owner, which is here the ‘nation’.

- The next level has a group of supporting systems, (Learning Management, Knowledge Base Management, Reporting, Physical and Human resources Management systems, Nation Resources Management, Resources Allocation Management and Finance Management). These subsystems provide different types of support to the activities of the subsystems in the next level. The Constraints Management subsystem contains activities that affect the overall degree of subsystems’ freedom by the constraints placed on the system such as economic and environmental constraints.

- The third level represents the rest of the subsystems with a general description of how they relate to each other. This level contains subsystems that provide general services for other subsystems, such as the Consensus Building subsystem which contains activities that aim to build an agreement on definitions required by activities in other subsystems and the Policies, Regulations and Laws Enforcement subsystem which contains activities for enforcing defined policies, regulations and laws on the whole system of government. Figure III.2 is an expansion of the Policy, Regulations and Laws Enforcement subsystem in Figure III.1. It shows some of the main activities in the Policies, Regulations and Laws subsystem and it can be seen that the policies, regulations and laws were defined outside this subsystem by the Legislation subsystem. The activities provide general tasks for the implementation and monitoring of the application of the defined policies, regulations and activities for the assessment of the achievement of the purpose of the subsystem which is the enforcement of these policies, regulations and laws. Most of these activities were derived from RD7 in

appendix A. The assessment is done against the identified performance requirements of the owners of the system which are the nation according to RD12 in appendix A. However, when compared to the real world the empowered body of people and governors appointed by the nation, such as politicians, usually define the performance requirements for the best interest of the nation.

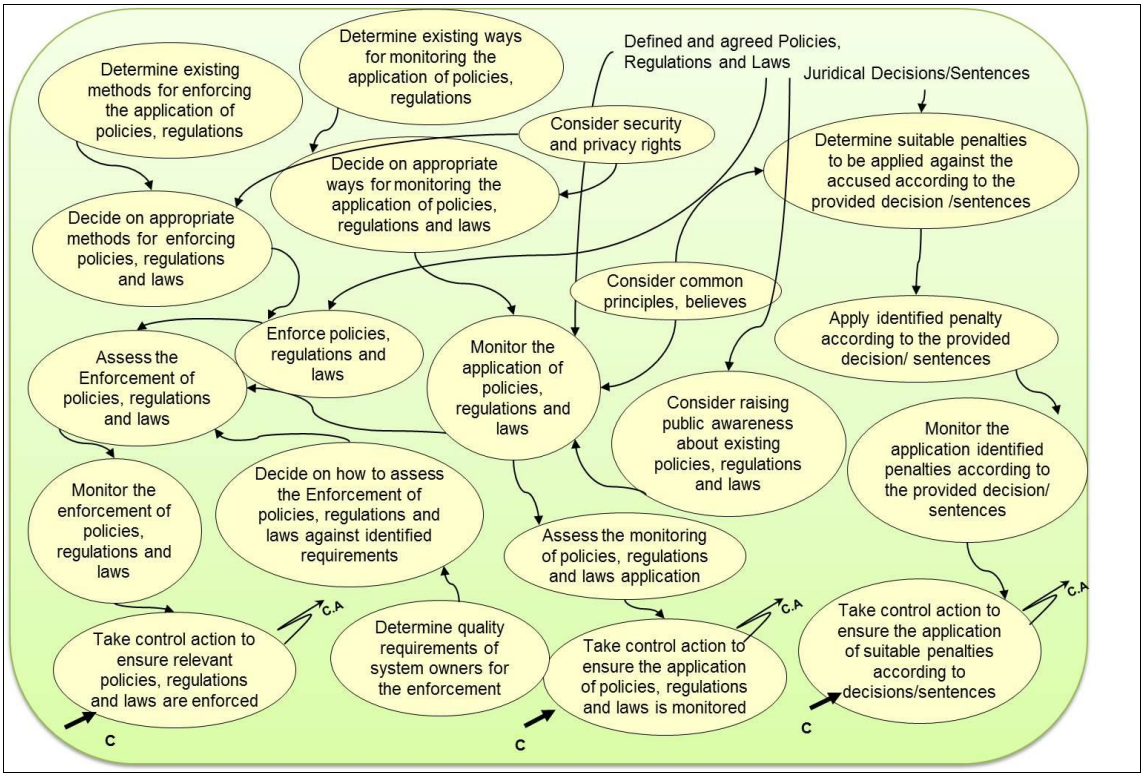


Figure III.2 Activities within Policy, Regulations and laws Enforcement subsystem

The major advantage of building CPTM is that it provides an organization structure-free description of the enterprise activities. These activities can be mapped into existing departmental roles in a real world situation or onto a potential departmental role that emerges as a result of the model [44].

III.4 Developing a CM relevant to E-government

A CM relevant to the government concept which is the system served by e-government has been developed. This section presents the CM relevant to the concept of e-government which is the service system. Due to its complexity and multidisciplinary nature and the fact that the purpose of e-government is not clearly defined, e-government is considered to be a ‘soft’ problem. The SSM

method of EMA was used to develop a CM relevant to the concept of e-government.

III.4.1 Developing Root Definitions

The purpose of e-government was considered from the following perspectives: citizen, visitors, business, government officials, government agencies and politicians. Also, e-government definitions found in the literature have been investigated, such as[42], [6], [78] and [79]. An initial set of RDs that describe the purpose of e-government from these perspectives was developed. These RDs were discussed in informal interviews that were made when attending ECEG 2009 conference with various possible stakeholders. Informed by the feedback from these discussions and the various definitions found in the literature, the following RDs were defined where e-government is an enterprise.

RD1- Core Transformation (T1)

> *-- A system owned by the government operated by skilled employees of the government or the government's partners to support the provision of new or existing internal and external government services to all government customers i.e. citizens, businesses, residents, visitors, government employees, local government agencies and other governments using efficient, effective, accessible, and secure electronic means that are available from anywhere and at any time as appropriate by utilizing current available Information and Communication Technologies (ICTs) while considering the expectations and needs of the government and its customers and constrained by relevant national regulations, policies and laws and international agreements and available resources.*

RD1- Core Transformation (T2)

> *-- A system to enable the engagement of government customers in governance by providing diverse communication means that utilize ICT to enable all eligible government customers to participate in decision making and engage in democratic dialogs between all involved parties regarding subjects and services relevant to them within a free, anonymous and trusted environment in order to enhance the relationship*

between the government and its customers while constrained by national regulations, policies and laws and available resources.

RD3- Support System (S1)

-- A system to undertake the transformation of traditional government services to electronic services by identifying necessary changes in the way traditional government services are provided in order to enhance the provision of those services and provide them in an integrated, available, secure, effective and efficient way as appropriate and possible while considering the expectations and needs of the government's customers and complying with relevant standards, guidelines and appropriate best practices.

RD4- Support System (S2)

-- A system to ensure that the physical resources available match the requirements of all activities of supporting the provision of improved government services by developing and maintaining the required infrastructure, hardware and software while exploiting the latest developments in relevant ICTs while complying with relevant standards and guidelines and constrained by available finance and resources.

RD5- Support System (S3)

-- A system to ensure that the human resources available to support all activities of supporting the provision of improved government services match the requirements of these activities, through the allocation or recruitment of personnel with appropriate capabilities that match the identified human resources' requirements to carry out those activities while taking into account the operation of proper training and education programs for developing current personnel skills and acting upon current personnel policies..

RD6- Support System (S4)

-- A system to undertake the protection of information about the government customers when using the enhanced government services provided using ICTs by the enforcement of suitable security measures and relevant defined regulations, policies and laws where appropriate

and needed while raising the awareness of involved parties about those regulations, policies and laws.

RD7- Linking System (L1)

-- A system to enable the deployment of the enhanced government services by authorizing government agencies or third parties to carry out projects to provide the identified government services using available ICTs in a secure, easy to use and integrated way while considering the expectations and needs of government customers and involved parties within constraints due to the by finance and available resources.

RD8- Linking System (L2)

-- A system to maintain a current and comprehensive knowledge base to support all activities of supporting the provision of enhanced government services using ICTs by assembling relevant knowledge about latest developments in ICTs and relevant performance measures and lessons learned from relevant 'best practice' while considering making information available as needed and providing the capability of reporting as required.

RD9- Planning, Monitoring, and Control system (PMC)

-- A system owned by the government, operated by appropriately empowered government authorities to ensure that the system activities for supporting the provision of improved government services using ICT are supported by monitoring the system activities and taking necessary actions where and when needed with consideration to the government expectations for performance while constrained by relevant standards, guidelines and best practices.

III.4.2 Developing the Consensus Primary Task Model (CPTM)

The Consensus Primary Task Model (CPTM) for the concept of e-government was derived from the complete set of Root Definitions. The complete CPTM obtained included over 200 activities and was validated by testing it against the Formal Systems Model (FSM) (section II.3.3.2).

III.4.3 Subsystems Decomposition

The subsystem decomposition resulted in 18 subsystems. Figure III.3 shows the high level of subsystems and their interdependencies.

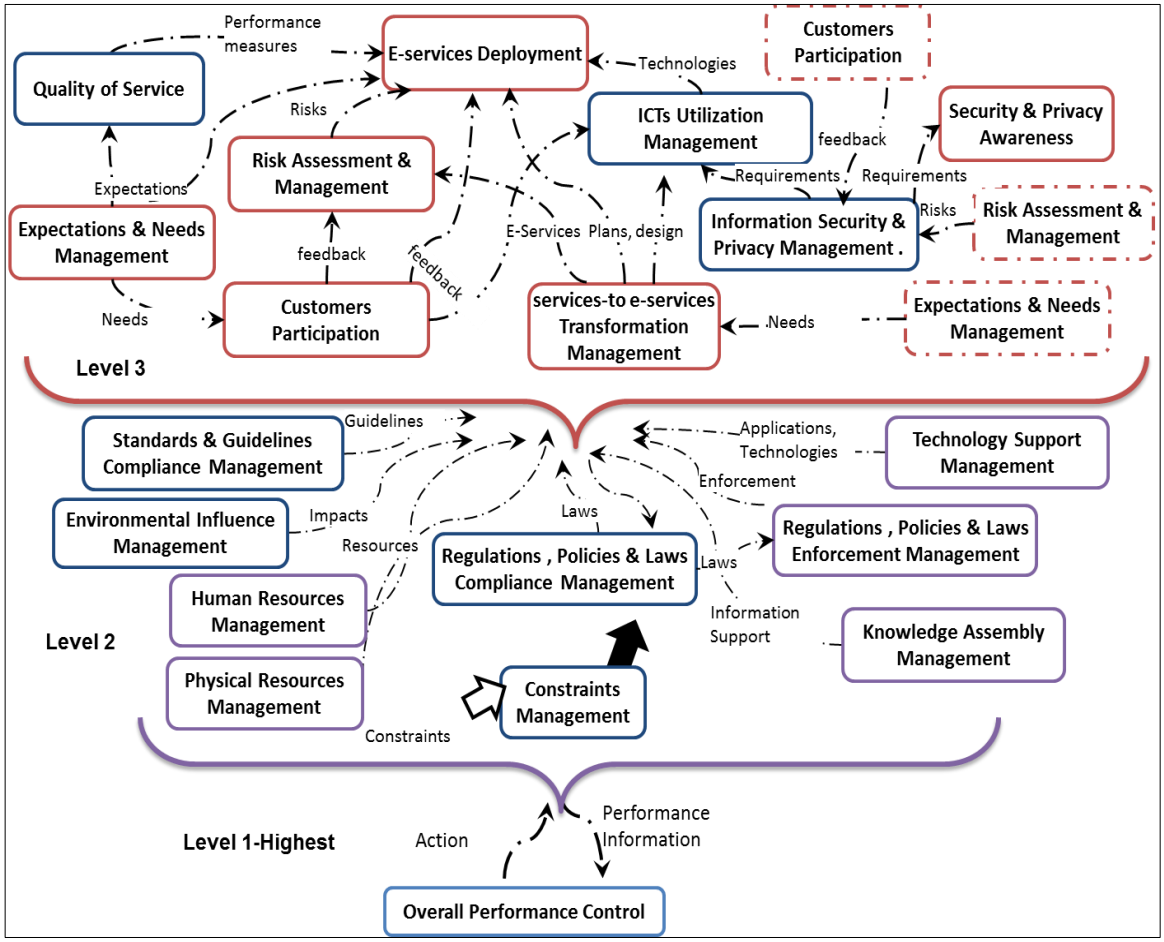


Figure III.3: High Level of subsystems of the CM relevant to E-government

The high level of subsystems shows three different levels of generality:

- The top level (Level 1) has the Overall Performance Control subsystem which receives performance information from all other subsystems and assesses the required actions according to expectations and needs of the owner, which is here the government.

- The next level (Level2) has a group of supporting systems that provide the support needed, such as human and physical resources, Knowledge, etc., to all subsystems while limiting a subsystem's freedom of choice of control action through the Constraint Management subsystem. Also, this level has subsystems which have an effect on all activities in the next level by giving technical support such as Technology support

Management or influencing the activities of the rest of the subsystems such as Environmental Influence Management and Regulations, policies & laws Management.

- The lowest level has the rest of the subsystems and the arrows show how these subsystems relate to each other in general. For example, the Services-to-E-services Transformation Management subsystem considers the expectations of both the government and its customers from the Expectations & Needs Management subsystem and the transformation plans are fed to the E-services Deployment subsystem.

One of the main advantages of the developed CPTM relevant to the e-government concept is that it can be used by e-government initiatives to work out missing activities that they might want to consider to ensure a more complete system is developed.

III.5 Discussion

This section discusses the potential benefits from using previously developed models in exploring the government to e-government transition problem. The development of the government CM has extended researcher understanding of the diverse perceptions of this concept and highlighted the interdependencies existing between government activities. To answer the question of what e-government is supposed to do, the activities in the CM relevant to Government can be considered as the “what” that a government has to undertake and e-government is a “how”. For each activity in the model, performance measures can be identified, and these measures can be used to determine where the use of ICT has the potential to increase the efficiency or effectiveness of the activities. Wilson [44] provides considerable evidence of the value of this approach in reviewing the strategic aims of an organisation, in deriving information requirements, and in process improvement. Defining the dependencies between the activities facilitates the identification of “system boundaries”, which are an essential prerequisite to defining the scope of an e-government project. To illustrate how the model can be used as a tool for exploring and researching different issues related to mapping government activities to e-government, some of the activities in the Services Provision subsystem (in CM relevant to government) (see Figure III.4) can be analysed.

Studying the activities in the view of mapping government services to e-government raises some issues concerned with how to maintain control of the performance and the quality of services for the services provided by a business partner.

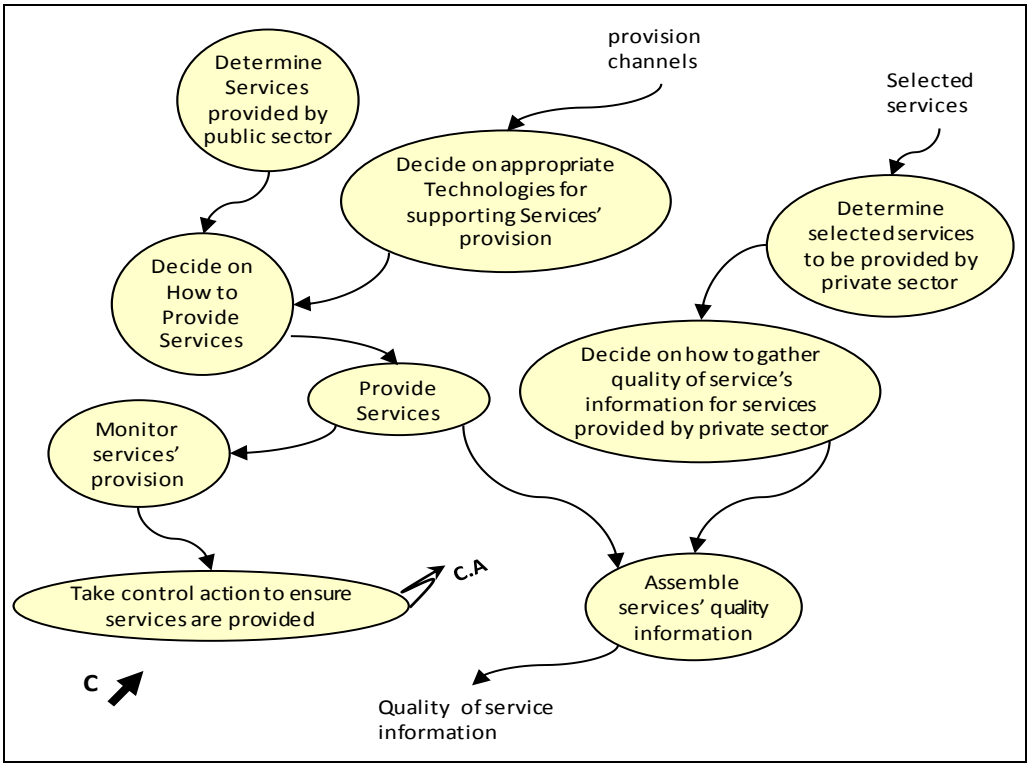


Figure III.4: Activities within the Services Provision subsystem

In addition, the impact of constraints such as the cultural and ethical influences on service provision should be noticed. Examples of questions that may be raised are:

- Does mapping a particular service to e-government serve the purposes of government?
- Do we need to apply new measures to assess the quality of service of the mapped services?
- How can we gather the quality information for the services provided by a business partner?

With regard to the e-government CM, the model can also be used as a framework for exploring various issues and obstacles facing e-government projects and those which have led to a failure of some of these projects. For example, we consider one of the findings in a study by Kolsaker and Lee-Kell [80] which indicates that the majority of citizens who responded were not

interested in using an e-government portal because it does not satisfy their expectations. The developed CM relevant to e-government acknowledges these needs. The activities in the model and in particular the activities in the Consensus Building subsystem and the Expectations and Needs Management subsystems, if considered, will encourage users to use e-government services as they will feel they were consulted and participated in the design of these services. The activities in the Consensus Building subsystem involve different stakeholders agreeing on definitions that will affect the development planning of government processes, for example, the definitions of effectiveness and efficiency from different stakeholders' points of view. The Expectations and Needs Management subsystem involves activities identifying the expectation and needs of different stakeholders and shaping the environment for accepting the government initiatives to meet these needs. The developed CM relevant to e-government was compared against some existing e-government frameworks, such as [79], [72], and [73]. The existence of similarities between the frameworks and the CM activities increased confidence in the accuracy of the CM and that it reflected the research community perspective about the purpose of e-government. The developed CMs may not be a complete representation to the concepts of government and e-government; however, these CMs gave insight into issues that should be considered when investigating problems in e-government.

III.6 Conclusion

The concept of electronic government has proven to be complex, multidisciplinary and influenced by a variety of perceptions. Therefore, the concepts of government and e-government were modelled using SSM. In the context of understanding the government to e-government transition, the CM relevant to the concept of government provided a vehicle for investigating and discussing which of the current government activities can be transformed appropriately into an e-government activity without violating the purpose of government and contributing to the overall effectiveness of government, while considering the different perspectives of stakeholders and the various environmental influences. The CM relevant to e-government helped in understanding the concept of e-government from various perspectives. Future possible usage of the e-government CM includes analysing the reasons behind

the failure of some e-government projects to derive lessons which can then contribute to the success of future efforts. The developed CMs are inherently defensible against the RDs by following the argument approach used by Brian Wilson in [44]. The core transformation RDs that represents the purpose of government and e-government were formulated based on definitions found in the literature and informal discussions with researchers in the field. The discussions and consultations were mainly about the core transformation RDs which represent the purpose of the systems. The definition of the purpose of government was based on many discussions and consultations occurred during informal meetings with Professor Brian Wilson who has more than 30 years' experience of using SSM for solving problems in both public and private sectors and is the author of an important book that provides a practical approach for building models within SSM that are relevant to real-life problems [44]. Also, another researcher, Mr. Steve McIntosh, was consulted who is an expert in system thinking approach and in particular SSM and System Dynamic (SD) and who has considerable experience with the government sector and has been involved in many government projects. The developed CM relevant to the government concept was published as a scientific paper in the proceedings of the 9th European Conference on Electronic Government (ECEG2009) [3]. At that conference, informal brief interviews were conducted with various researchers in the field to discuss their views about the purpose of e-government and the developed core transformation RD relevant to the concept of e-government. These discussions and the relevant definitions found in the literature helped to shape the RDs relevant to the concepts of government and e-government. Although the developed CMs might not be a complete representation of the concepts, they helped by shedding some light on the aspects that should be considered when investigating a problem in the domain of e-government. However, possible enhancements to the developed models lie in enhancements of the RDs by discussing them with a wider range of relevant stakeholders to determine whether the developed RDs have reflected their views and perceptions of the concepts of government and e-government. This would enrich the understanding of the concepts of government and e-government and their purposes and enable better deployment of e-government to serves these purposes.

Chapter Four

IV. E-government Authentication Frameworks

IV.1 Introduction

E-government services are provided through several electronic means, such as the internet and mobile phones. However, such services are usually accessible only to those who have the required privileges i.e. access rights to services. In order to authorise a person, a group, or even software to access a service, they must first be authenticated, i.e. their identities must be verified before allowing them access according to their assigned privileges. Authentication frameworks are used to describe the processes, guidelines and technologies used to achieve the authentication process and, sometimes, the identification processes that must be carried out prior to authentication. In the early days of e-government projects, an authentication process was either not needed or was performed in a simple way by using usernames and passwords. However, the need to define an authentication framework arose with the implementation of more advanced services that involve interaction and transmission between users and e-government agencies' websites or portals. Electronic government authentication frameworks are authentication frameworks established by governments to provide guidelines and descriptions for the processes of authentication needed and the technologies involved to achieve various trust levels required for delivering e-government services securely. However, current e-government authentication frameworks vary in the level of detail they provide and have been subject to various updates to cover new authentication requirements that arise from the deployment of more advanced services. These frameworks were updated or supported by new documents whenever a limitation was discovered or new security requirements were identified and this cause the publication of many versions and documents related to authentication framework, for example, the UK government's versions of its e-authentication framework [23] and [60]. This has led to a limited adoption of these frameworks

by government agencies. For example, the UK government authentication framework indicates that each government agency should publish its privacy policy on their website [60]. However, a study of UK e-government websites by Tolley & Mundy [81] showed that a large number of the studied websites did not have a privacy policy and that other agencies' websites have privacy policies that are inadequate and unclear to the users.

Since the aim of this research is to provide a framework for preserving privacy that balances preserving privacy with satisfying security requirements and in particular authentication requirements when using e-government services, it is essential to study and understand how the security of users' information should be protected in an e-government context and in particular how users are supposed to be authenticated when requesting e-government services as it is one of the main security measures for protecting users' information and at the same time one of the reasons for raising privacy issues from the citizen perspective. This chapter's focus is on the authentication frameworks of e-government and seeks to apply a comprehensive approach to the analysis and review of selected published e-government authentication frameworks to identify reasons that have led to the limited adoption of these authentication frameworks by government agencies and understand how privacy is considered in these frameworks. SSM is used to capture different aspects and perspectives of authentication in e-government and to identify factors that influence the authentication processes in that context. A CM relevant to authentication in the context of e-government was developed using SSM and used in studying the activities involved in the authentication processes and in capturing the interdependencies between these activities. The model was used as a comprehensive tool for analysing current authentication frameworks and to identify possible gaps and limitations in these frameworks. Section 2 provides an overview of e-government authentication frameworks and related work; it is followed by an illustration of the approach in developing a conceptual model relevant to authentication in section 3. Section 4 shows the results of the gap analysis using the model, while section 5 discusses these results.

IV.2 E-government Authentication Frameworks

Electronic government security is one of the major obstacles facing the deployment of e-government projects around the world. A fundamental aspect of e-government security is authentication, where users' identities are verified to determine if they will be granted access to the requested services. An authentication framework can be described as a group of guidelines and instructions that illustrate how the process of authentication and other related processes should be performed [12]. Most e-government services require some sort of authentication processes in order to allow access to resources and/ or perform certain actions. This has led to a need to regulate such authentication processes in an authentication framework in order to achieve a consistent online security policy between government agencies. The UK government was one of the first governments to introduce an authentication framework to regulate the authentication processes when delivering electronic services by publishing an authentication framework as part of its e-government strategy document [23]. This framework was revised in September 2002 [60]. The US government's e-authentication framework for federal agencies was issued in December 2003 [24]. With the movement of governments towards implementing more advanced applications of e-government, new security issues have arisen resulting in the updating of current e-authentication frameworks or the publishing of new guidelines that support the current e-authentication frameworks. For example, the technical guidelines for e-authentication published by the National Institute of Standards and Technology (NIST) in 2004 was revised in 2006 [82] and recently in 2013 [83]. These authentication frameworks and guidelines, especially the NIST guidelines, were widely adopted by governments around the world in their own versions of e-authentication frameworks [84]. Authentication Levels of Assurance (LoAs) are a key element in the authentication framework and defined as "measures of the authentication trustworthiness required to authorise access to services or resources" [85]. There are three levels of assurance recognised by most of the authentication frameworks in e-government. These levels are low, medium and high. However, the basis of the definition of these levels varies between authentication frameworks [85] and [84]. For example, the UK authentication framework defines four levels of assurance based on the level of control

required to minimize risk to the delivery of e-government services [60]. These vary from level 0 where no assurance is needed to level 3 where the highest level of assurance is required. The US authentication framework defines a different four levels of assurance based on the potential impact and likelihood of an authentication error when providing e-government services [24]. These levels vary from level 1 which requires minimal assurance to level 4 where the highest level of assurance of identity is required. The Organisation for Economic Co-operation and Development (OECD) authentication guidelines are followed by many countries. OECD recommended three levels of assurance (LoA) [86]:

- Low or basic level of assurance is where low confidence is required in the identity of the user of the service and a single factor authentication method can be used to verify the identity of the user, e.g. user name and password.
- Medium level of assurance is where moderate confidence is required and this is achieved by a two-factor authentication method, such as messages to a mobile phone or a one-time password generated by a given token.
- High level of assurance is where high confidence is required and this is achieved by a combination of a two- factor authentication method and the use of a hardware token.

The described Levels of Assurance (LoA) are used to control access to sensitive data and services and a risk assessment should be applied before assigning those levels.

E-government authentication frameworks are affected by differing perceptions of the purpose of authentication due to the context of e-government, the government organizational structures, the political views of the government, and the population's social and cultural values [72].There have been some efforts to investigate current e-authentication frameworks. For example, a study by Nenadic and others [84] investigated how the LoA were defined in different e-authentication frameworks. Another study by Holden and Millett [12] reviewed privacy policies and laws applied by e-authentication frameworks. However, there remains a need for a comprehensive analysis that takes into account different aspects and perspectives involved in the process of authentication in

e-government. Therefore, a system thinking approach was applied to the analysis of current e-government authentication frameworks by developing a conceptual model relevant to authentication in the context of e-government. The approach is presented and illustrated in the next section.

IV.3 Building a CM relevant to Authentication in E-Gov.

This section describes the approach followed in developing the CM relevant to authentication in e-government.

IV.3.1 Analysis approach

The e-authentication concept is complex and there are different perceptions of its purpose. This complex situation needs an analysis that accommodates different perceptions relevant to the concept in order to capture the essence of its purpose. The Soft Systems approach has been advanced as the most appropriate methodology for addressing similar unstructured and problematic situations with unresolved core purposes [87]. Therefore, SSM [43] was selected to analyse the complexity of the authentication concept in an e-government context (i.e. e-authentication). SSM helps formulate and structure thinking about complex messy situations that involve divergent views [44]. Authentication in the context of e-government is considered in this research as an enterprise (see sectionII.4). Therefore, the EMA method [44] was used to understand the core purposes of e-government and authentication in the context of e-government, and to build a relevant comprehensive CM. The aim of this CM is to capture the essence of authentication in the context of e-government by considering different aspects and perspectives that have an impact on the authentication processes. This model was then used to analyse and identify gaps in current e-government authentication frameworks.

IV.3.2 Developing the Conceptual Model (CM)

This section presents an illustration of how the model was developed and validated using SSM.

IV.3.2.1 Developing Root Definitions (RDs)

To develop the set of RDs that describe the purpose of e-authentication in the context of e-government, various definitions of e-authentication have been investigated. Authentication in general is considered to be a security measure

or function used to establish the validity of a claimed identity of a user, device, or transaction, that the identity is what it is claimed to be [24],[86]. E-authentication is defined by the NIST as "*the process of establishing confidence in user identities electronically presented to an information system"*[82]. Another definition defines e-authentication as "*the process of determining the degree of confidence that can be placed in assertions that a user or identity is who and /or what they purport to be*" [88]. These definitions are adopted by most of e-government frameworks such as [60], [88] and [89]. E-authentication in an e-government context can be considered to be a service system, and e-government to be the system served. However, e-government is a service system to support and enhance government activities (see sectionII.4). Therefore; conceptual models relevant to the concepts of government and e-government have been developed and analysed (section III.3 and section III.4). The e-government CM activities were analysed to capture the purpose of authentication in an e-government context. Those activities that might need a level of assurance that can be achieved by authentication were identified. By analysing these activities and considering different authentication definitions found in relevant standards and reports such as, the NIST guidelines for e-authentication [82], the OECD guidelines on e-authentication[86] and the National Research Council (NRC) report [90]. Also, different stakeholders' perspectives were considered based on knowledge acquired from a literature review and informal interviews and discussions with individuals representing different stakeholders, a conclusion on the core purpose of authentication in the context of e-government was derived.

The complete list of RDs is:

RD1- Core Transformation (T)

> *-- A system to establish the level of confidence required in an assertion's genuineness in order to verify the eligibility of a claimant to perform actions in the context of e-government using different channels by identifying the required levels of confidence to perform those actions and satisfy their security requirements according to the assessed risks of those actions while considering the needs and expectations of the government and its customers and the availability of alternative means*

for establishing the level of confidence in contingency situations where possible while maintaining the flexibility, ease of use and customers' rights of privacy and their right to remain anonymous when appropriate.

RD2- Support System (S1)

-- A system to define the required levels of confidence to perform actions in the context of e-government by assessing the risks from potential threats on targeted resources and assets in order to define a set of rules and definitions for each level while considering relevant rules and definitions in standards, guidelines and 'Best Practices' and the dynamic changes in potential threats and in the needs and expectations of the government and its customers.

RD3- Support System (S2)

-- A system to ensure that the human resources available to support all activities of establishing the required level of confidence in an assertion's genuineness match the requirements of those activities by the allocation or recruitment of personnel with proper capabilities that match the identified human resources requirements while considering the operation of proper relevant training and education programs for developing current relevant personnel skills in order to undertake relevant roles effectively and act upon current personnel policies.

RD4- Support System (S3)

-- A system to ensure that the physical resources available match the requirements of all activities of establishing the required level of confidence in an assertion's genuineness by developing and maintaining the required infrastructures, hardware and software while exploiting latest developments in relevant technology and considering appropriate standards ,technical, financial and environmental constraints.

RD5- Linking System (L1)

-- A system to develop and maintain a current and comprehensive knowledge base to support all activities of establishing the required level of confidence in an assertion's genuineness by assembling relevant

intelligence, knowledge about the latest developments in the means of verification and relevant security measures and lessons learned learning from relevant 'best practice' while considering making information available as needed and providing the source for reporting as required with respect to data protection and security constraints.

RD6- Linking System (L2)

-- A system to undertake the communication between the government and its customers by enabling the participation of the government's customers in policy design and decision making where relevant and appropriate in order to communicate the definitions, rules, means of verification, and relevant security measures to the government's customers and to raise their awareness and acceptance of the rules and means of verification, while considering diverse customers' needs and expectations and the appropriateness of the communication channels.

RD7- Linking System (L3)

-- A system to undertake the deployment of the identified level of confidence required for verifying the eligibility of a claimant to perform actions in the context of e-government by operating reliable, accessible and accountable means of verifications assigned to each level of confidence according to the defined security requirements of the requested actions in the context of e-government while utilising appropriate technical solutions and considering relevant standards and guidelines.

RD9- Planning, Monitoring, and Control system (PMC)

-- A system owned by the government, and operated by appropriately empowered government authorities to ensure that the activities of establishing a level of confidence in an assertion's genuineness are carried out according to the needs and expectations of the government and its customers, by monitoring these activities and taking necessary actions where and when needed, while complying with relevant standards and guidelines where possible and constrained by available

resources, finance and technologies and current legislations and policies with consideration to the impact of social, cultural and political influences.

IV.3.2.2 Developing the Consensus Primary Task Model (CPTM)

To develop the Consensus Primary Task Model (CPTM), a set of activities was derived showing what the system should do in order to be the system described in the previous RDs. The logical dependencies between these activities were identified. The final CPTM included over 200 activities. The model was validated at each step using SSM rules as illustrated in sectionII.3.3. Following the validation of the complete CPTM, subsystem decomposition was performed (see sectionII.3.2.3). The subsystem decomposition resulted in 21 subsystems. The subsystems were grouped into three levels of abstraction, the supporting systems are found in the highest and second level while the rest of the subsystems are in the lowest level.

The high level subsystems and their interdependencies are shown in Figure IV.1.

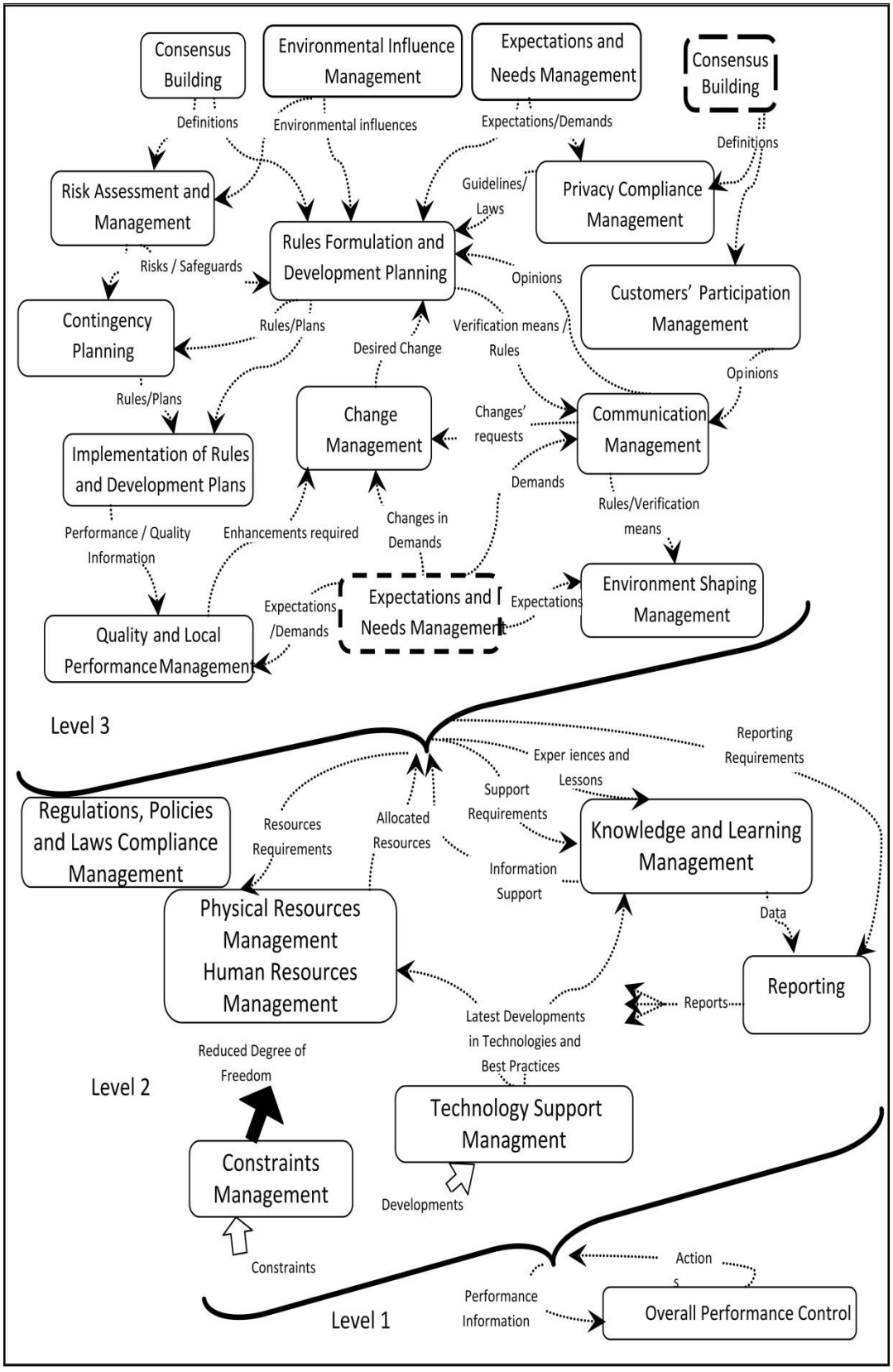


Figure IV.1: SSM high level of subsystems based on developed CPMT

The subsystems were grouped into three levels of abstraction, the supporting systems are found in the highest and second level while the rest of the subsystems are in the lowest level.

The main tasks of each subsystem at each level are:

- ***At the highest level (Level 1) is the Overall Performance control subsystem*** which has an effect on all the other subsystems. The Overall Performance Control subsystem contains activities that involve monitoring the performance of the whole system and assessing that performance using performance measures that reflect the expectations of the government and its customers. The performance information from these subsystems are passed to this subsystem for evaluation and assessment while actions decided by the evaluation are passed from this subsystem to the subsystem which need to perform an action according to the result of the assessment.
- ***The second level (Level2) contains supporting subsystems*** which support the activities of the subsystems in the next level (Level1). This level contains the following subsystems:
    - *Physical Resources Managements:* the activities in this subsystem are concerned with identifying the physical resources needed to perform other activities in the whole system and to allocate the available resources to the relevant activity as needed. These resources can include computer servers, physical places, offices, any relevant equipment and more.
    - *Human Resources subsystem*: this subsystem is concerned with identifying the human resource requirements of the system activities and allocating suitable available human resources with the required capabilities to those activities as appropriate and providing training when required.
    - *Knowledge and Learning Management*: this subsystem contains activities relevant to identifying the gaps in knowledge relevant to the system activities and identifying possible knowledge sources to determine the required knowledge while extracting lessons learned from ‘Best Practices’ relevant to authentication in the context of e-government.

- *Reporting subsystem:* provides the activities concerned with generating useful reports based on gained knowledge and provides these reports to other subsystems as required.
- *The Technology Support Management subsystem*: the main task for this subsystem is to provide other subsystems with any needed support in terms of the latest technologies relevant to their activities. Activities in this subsystem include identifying the latest technologies relevant to the system activities and assessing the possibility of using these technologies and making these technologies available to support the achievement of the system activities in an improved approach
- *The Constraint Management subsystem*: this subsystem is concerned with reducing the overall degree of a subsystem's freedom of choice by ensuring the conformance of that subsystem with constraints placed upon the system such as assigned finance and complying with regulations and laws and relevant standards and guidelines through enforcing control actions on relevant activities.
- *The Regulations, Policies and Laws Compliance Management* subsystem is concerned with monitoring the compliance of all other subsystems in the next level with the relevant established regulations, policies and laws and taking appropriate actions when a violation occurred.

- ***The lower level contains the rest of the subsystems*** which form the main activities that should be carried out to achieve the system purpose as defined in the RDs.

According to the conceptual model activities, the identified subsystems were classified into the following five stages based on their main purpose and the interdependencies between these subsystems:

1. **Preliminary Stage:** the following subsystems to be considered before and while developing plans for the authentication system are:

   - *Expectation and Needs Management:* identifies the expectations and needs of the system stakeholders and delivers these needs and expectations to the relevant subsystem and considers any

changes in the expectations and needs which are relevant to the system and manages the effect of these changes on the requirements of the system's stakeholders.

- *Consensus Building*: builds an agreement between the involved stakeholders (e.g. citizens, government agencies) on relevant definitions such as privacy and ease of use.

2. **Risk Assessment Stage:** This includes a *Risk Assessment and Management subsystem* to undertake a comprehensive risk assessment to determine potential risks on targeted assets and to identify required levels of confidence and the associated safeguards to mitigate these risks as much as possible.

3. **Development Stage:** This includes:

   - *Rules Formulation and Development Planning* subsystem to develop plans and rules for the authentication system and to define the required levels of confidence. The subsystem is responsible for designing appropriate verification methods and safeguards at each level, and for determining any pre-processes needed to enable the selected means of verification (such as identification processes).

4. **Implementation Stage:** This includes:

   - *Implementation of Rules and Development Plans* subsystem to implement the development plans and rules and the activities concerned with defining the implementation strategies and selection of the best implementation tools.

5. **Performance Assessment Stage:** This includes:

   - *Quality and Local Performance Management*: has the activities of monitoring the quality and performance of each subsystem activity and assessing these activities according to quality and performance measures set and agreed by the government and customers.

In addition, the following subsystems can be considered before, during and after the development of the e-government authentication system:

- *Contingency Planning*: identifies contingency situations and determines alternative authentication plans in contingencies situations.
- *Privacy Compliance Management*: ensures compliance of development plans with privacy laws and regulations and defines new legislation when needed for preserving users' rights of privacy and to stay anonymous when desired and appropriate.
- *Customers' Participation Management*: activities in this subsystem are concerned with providing the means for stakeholders' participation in relevant decision making and rules formulation and ensuring active communication between the government and its customers by communicating the customers' opinions to relevant subsystems and government views to the customers.
- *Environment Shaping Management:* determines strategies for raising users' awareness and the training required for government personnel.
- *Environmental Influence Management*: determines environmental influences such as political, social and cultural influences and assesses their impacts on all the activities of the authentication system in e-government.
- *Change Management:* determines changes in stakeholders' expectations, needs and changes identified as a result of quality assessment of system activities. Activities in this subsystem can be incorporated into other subsystems.
- *Communication Management:* provides activities for managing the communication between customers and the government to deliver customers' opinions with regard to the rules' designs and development plan or to communicate these rules and plan to

customers. The activities in this subsystem can be incorporated into the Customers' Participation Management subsystem.

To relate the above subsystems to real world situation, the above subsystems can be mapped into a new or existing government department or agency which can carry out the tasks identified in one or more subsystem. For example, the activities of the Overall Performance Control subsystem can be mapped to an existing government agency that is concerned about monitoring and assessing government services, so the assessment of the services concerned with authentication in e-government can be part of this general assessment. However, a new government agency to assess the services of authentication in e-government can be established to carry out the activities of the subsystem.

IV.4 Authentication Frameworks Gap Analysis

This section presents the steps and results of the gap analysis performed on selected e-government authentication frameworks. The analysis used the activities of the CM relevant to authentication in e-government to give the criteria for analysing the frameworks. The selected electronic authentication (e-authentication) frameworks for this analysis are the authentication frameworks of the United Kingdom (UK) government [60], the United State (US) government [24],[83], [82], the Australian government [88], New Zealand government [91] and Canadian government [89]. The basis of this selection was that these are leading countries in e-government development according to the United Nations (UN) report on e-government [22], and the e-authentication framework documents for these countries are publicly available in English. According to a UN report 2012 [22] the UK was ranked third, US fifth, Canada 11th position, Australia 12th, and New Zealand 13th in the UN list. In addition, the UK and US governments were the first governments to produce e-authentication frameworks and their frameworks have been widely adopted by other countries. In addition, the Australian government has established security standards in the context of e-government applications. However, the UN report [22] also shows other countries with higher rank in the development of e-government, such as the Republic of Korea who is on the top of the world in e-

government development, the Netherlands who came second in the ranking and Denmark which is in the fifth place. These countries use their own authentication and security frameworks, which unfortunately were not available publicly in English. This limits the results of the presented gap analysis as obtaining the documentation of these frameworks would have been of great value in our gap analysis of existing authentication framework, especially since these countries have different social, cultural environments. However, the results of the gap analysis are still valid for the analysed frameworks and frameworks from other countries which were developed based on them.

A brief overview on each of these frameworks is provided.

IV.4.1 E-government Authentication Frameworks: an Overview

An overview of authentication frameworks selected for the gap analysis is:

IV.4.1.1 UK Authentication Framework

The UK e-government authentication framework, “Registration and Authentication” [60] was published in 2002 as a supporting document of the e-government security framework “Security” [92]. The “Security” framework has other supporting documents, which include “Assurance”, “Business Services”, “Confidentiality”, “Network Defence”, and “Trust Services”. The Security framework complies with and references the BS EN ISO 17799 security management standard [93] and stresses that all government agencies should comply with this standard and use the risk assessment approach described in this standard when providing e-government services. The framework is aimed at any government agency or government officer who are establishing or providing e-government services.

IV.4.1.2 US Authentication Framework

The US Authentication framework was first published in 2003 by the Office of Management and Budget (OMB) in a document called “E-authentication Guidance for Federal Agencies” which later was known as document “M-04-04” [24]. This document is supported by various documents and standards issued by NIST at later dates. However, a revised version of the framework was published in 2006 in a document called “Electronic Authentication Guideline”[82]. This framework became the official version of e-government authentication framework and provided details of the levels of assurance to

be considered when designing an authentication system when providing e-government services. More supporting documents were published to support this document tackling specific issues mentioned in the framework but in greater technical details. The framework is aimed at federal agencies and federal states are encouraged to use it in their local systems so that they are able to comply with relevant federal laws and regulations. A recent version of this framework was published in 2013 [83].

IV.4.1.3 Australia Authentication Framework

The “National e-Authentication Framework “[88] is the official authentication framework for e-government in Australia published in 2009 by the department of Finance and Deregulation. The framework is aimed at use by all government bodies and agencies providing e-government services. The framework combined two earlier versions of e-authentication frameworks for Business and Individuals. It gives detailed descriptions of the risk assessment approach and assurance levels and how these should be considered by government agencies when designing authentication processes for e-government services.

IV.4.1.4 Canada Authentication Framework

The Canadian e-authentication framework ”Principles for Electronic Authentication”[94] was published in 2004 by the Authentication Principles Working Group which had representatives from industry, consumer groups and various levels of government. The framework was designed to be used as a benchmark for the development, implementation and use of authentication services in Canada. It contains six principles that address the authentication of electronic communication in its broadest sense. These principles are: responsibilities of participants, risk assessment, security, privacy, disclosure requirements and complaints handling. The framework’s aim is to provide guidelines to individuals, businesses and government bodies involved in the design and provision of authentication services. This framework was expanded and detailed in a large document “A Pan-Canadian Strategy for Identity Management and Authentication” [89] published in 2007 and supported by several separate documents to cover issues such as trust, identity, privacy and legislation. An example of these supporting documents that support the framework and give details on the assurance levels that

should be considered when providing authentication services is the document called “Pan-Canadian Assurance Model” published on 2010 [95]. Also, the Canadian government published a supporting document “Guideline on Defining Authentication Requirements” in 2012 [96]. This guideline put in practice the concepts presented in the authentication framework and the assurance model and relate the guideline to relevant standards, guidelines and laws such as” Framework for the Management of Risk” [97] and recently the Canadian government issued a “Standard on Identity and Credential Assurance” [98].

IV.4.1.5 New Zealand Authentication Framework

The current authentication framework was published in 2004 by the New Zealand government titled “Authentication for e-government, Best Practice Framework for Authentication”[99]. The framework is aimed at managers and government agencies staff who are planning or implementing government online services. The framework provides guidance to government agencies on how to determine authentication requirements and options of implementing solutions to satisfy these requirements. The framework did not include references to authentication standards, however, in recent years a set of authentication standards and guidelines have been published by the government and several guidelines have been published to help government agencies to apply and comply with these authentication standards, such as the “Guide to Authentication Standards for Online Services” [91].

In the gap analysis, the main documents on actual authentication frameworks for each country were considered in the comparison against the activities of the developed CM relevant to authentication in e-government. However, for the purpose of completeness and when gaps were identified other supporting documents were reviewed and analysed to determine if they covered the gap.

IV.4.2 Gap Analysis Results

The analysis was performed by comparing the activities identified in e-government authentication framework documents and other supporting documents against the activities in the conceptual model taking into account the interdependencies between these activities. In this analysis, the absence of activities or similar activities in the documents representing the e-government

authentication framework was considered a gap. Also, if an activity was briefly mentioned without much detail on how it could be adopted it would still be considered absent and noted as a gap. On the other hand, the existence of relevant activities that are not covered by our conceptual model was marked as an extra for the authentication frameworks and as a possible enhancement to our conceptual model, as long as these activities are relevant to the e-authentication concept. The focus of the analysis was on the procedures and guidelines that help government agencies to build their e-authentication strategy rather than the technical details. Also, it is worth mentioning that the activities of the supporting systems which appear in the developed CMs were missing in the studied frameworks. This was not considered to be a limitation as these activities usually exist as part of the supporting systems that serve government activities in general.

For example, the activities of the Human Resources Management subsystem do not exist in the studied frameworks (see Appendix B), but these activities can be found in a Human Resources government department.

A summary of the gap analysis is presented in Table IV.1, which shows the analysed frameworks compared against the CM subsystems defined in III.3.2. A detailed analysis of activity level can be seen in Appendix B. The symbol ✓ indicates that the framework had all the activities that satisfied the criteria, ☑ symbol indicates that the framework had most of the activities that partially satisfied the criteria, ☒ symbol indicates that the framework had a few activities that satisfy the criteria but with not much details and that the criteria was partially not satisfied, and ✗ symbol indicates the absence of an activity from the framework and that the criteria is not satisfied.

Criteria (CM Subsystems)	UK	US	Ca	Au	NZ
Expectations & Needs Management • Determine expectations and needs of all stakeholders. • Determine dynamic changes in expectations and needs	☑	☒	☑	☑	☒

Criteria (CM Subsystems)	UK	US	Ca	Au	NZ
Consensus Building • Determine stakeholder's perspectives on relevant terms (e.g. eligible, ease of use, reliable, accountable etc.). • Determine how to agree on relevant terms. • Define relevant terms as agreed by stakeholders.	☑	☒	☑	☑	☒
Rules Formulation and Development Planning • Define required levels of confidence and appropriate set of rules for each level. • Determine appropriate verification means for each defined level of confidence. • Determine appropriate technical solutions for selected verification means.	✓	✓	✓	✓	✓
Risk Assessment and Management • Assemble knowledge about potential threats • Asses risks associated with providing a service • Determine security requirements • Identify required levels of confidence/set of actions for satisfying identified security requirements	✓	✓	✓	✓	✓
Implementation of Rules and Development Plans • Implement selected means of verification assigned to each level of confidence. • Implement selected technical solutions and mechanisms to ensure the enforcement of rules assigned to each level of confidence. • Consider various access channels (e.g. mobile, kiosk, etc.)	☑	☑	☑	☑	☑
Privacy Compliance Management • Determine desired level of privacy in different situations • Assess the privacy impact when providing a service • Ensure the compliance of the service' implementation with relevant privacy regulations and laws and desired level of privacy	☑	☒	☑	☑	☑

Criteria (CM Subsystems)	UK	US	Ca	Au	NZ
Contingency Planning Management • Determine alternatives for currently used verification means to established the required level of confidence in contingency situations • Ensure to the application of the alternative means when needed while complying with relevant regulations and laws	☒	☒	×	☒	×
Customer's Participation Management • Ensure that government customers' participation in system activities is enabled where relevant and appropriate	☒	☒	☒	☒	×
Environment Shaping Management • Determine schemas for raising awareness and measuring customers' acceptance of the authentication systems and relevant rules. • Apply schemas for raising awareness on verification means and to communicate relevant rules and laws,	☑	☒	☑	☑	☒
Environmental Influence Management • Assemble knowledge about environmental factors (social, cultural and political) impacts on the authentication activities • Consider the impact of environmental factors when performing the system activities	☒	☒	☑	☒	☒
Quality and Local Performance Management • Determine reliability, accountability, accessibility and appropriateness measures of selected verification means • Monitor and assess the quality and performance of activities at subsystem level	☑	☑	✓	☑	☑

Table IV.1: Summary of gap analysis results

Based on our gap analysis the following gaps were noted in all the e-government authentication frameworks studied:

- **Consensus building**: Although each of the studied frameworks provided definitions for the common terms and principles, these definitions reflect the government point of view and there is a gap in establishing a consensus between the stakeholders on relevant definitions that affect the development of the system. For example, stakeholders may have

different interpretations of terms such as ‘ease of use’, ‘usefulness’ and ‘privacy’.

- **Expectations and needs management:** The expectations and needs of stakeholders were considered in some of the frameworks by consulting the stakeholders (users) and ask for their feedback about the published documents (UK, Canada and Australia authentication frameworks).

- **Environmental influence management and Environment shaping management:** Social, cultural and political impacts were not considered in the development of the system, especially when formulating relevant rules and selecting verification methods. Also raising awareness of verification means and communicating relevant rules and laws was not considered in most of the frameworks.

- **Customer’s Participation Management:** There was limited engagement of stakeholders in decision making and policy design. The only form of stakeholders’ engagement found in all the studied frameworks was the publication of the frameworks for public comments and considering changes in response to these comments. For example, the Office of e-Envoy responded to public comments on the first version of the authentication framework by a detailed document that illustrated the actions taken in response to each comment [60]. A similar approach was taken by the Canadian government to produce the final version of its authentication framework [89].

- **Privacy Compliance Management**: Although all the studied frameworks considered compliance with existing privacy laws and regulations, they did not consider the customers’ views on privacy issues that might arise from the application of authentication technologies and a customer’s right to stay anonymous if possible. For example, with regard to the privacy issue, the Australian e-Authentication framework indicates that *“The Commonwealth and each state and territory regulate the collection and handling of personal information either by legislative or administrative regimes. Agencies shall ensure that implementation meets all relevant regulatory and administrative requirements for their jurisdiction, as well as community expectations.”* [88]. Although the framework seems to

consider community expectations, there are no details on how this can be done and how these expectations can be determined. The other frameworks only emphasise compliance with existing data protection and privacy laws.

- **Implementation of Rules and Development Plans:** There is a gap in the implementation strategies used by the studied frameworks with regard to shaping the environment and change management when implementing the authentication system. In the Australian e-Authentication framework, they point out the importance of "determining awareness-raising, training and change-management requirements for agency personnel and users" as part of developing an implementation strategy [88]. However, change management and environment shaping should be incorporated as an essential part of developing and maintaining the system.

- **Quality and Local Performance Management:** There is a lack of clarity on quality and performance measures to be followed by government agencies and their business partners, and how these measures reflect the stakeholders' expectations.

- In addition, there is a lack of detail about authentication procedures for new delivery channels for e-government services (e.g. mobile phones) and for customers with special needs (e.g. disabled customers). This gap was identified as by comparing activities in the expectations and needs subsystem. However, this may be an advanced feature at this time as most current e-government services are not yet designed to cover these issues.

Though these gaps were identified, there were many good aspects in the analysed frameworks that worth mentioning; namely:

- The analysed authentication frameworks were well documented and publicly available.

- Definitions of levels of confidence were covered in all the analysed frameworks with technical details about appropriate authentication

methods for achieving each level of confidence and recommendations on when to apply them.

- The analysed frameworks presented detailed documents to help government agencies conduct their risk assessment and follow relevant standards and best practices.

- The registration phase was recognised and presented as an essential step in all the studied frameworks and its impact on defining the required level of confidence was covered in great detail in the US and the UK e-authentication frameworks.

- The overall assessment of the application of the frameworks was recommended to be carried out at different stages in the analysed frameworks. In the UK government e-authentication framework [60] it was recommended this assessment is done by an independent third party.

- The assessment of the quality and performance of the activities carried out to maintain the authentication in e-government was recognised in all the analysed frameworks and in great detail in the Canadian authentication framework [89] .

Although the developed CM relevant to authentication in e-government used in this gap analysis was developed based only on analysing existing definitions. In the literature for e-authentication, most of the identified subsystems and their activities were present in the analysed frameworks, which gave us more confidence on the relevance and accuracy of the developed CM. However, some elements were not covered by our CM such as the registration phase in the authentication frameworks and the technical details of the authentication methods for achieving the identified levels of confidence. Possible enhancements to the CM can be achieved by revising the RDs to include different stakeholders' perspectives.

IV.5 Discussion

One of the main gaps identified was understanding the expectations and needs of stakeholders and engaging them in the development of the authentication system. This gap could be reduced if the preliminary stage of our model was considered an essential step prior to the risk assessment stage, which is currently the starting point of all studied frameworks. Another important gap is in shaping the environment for accepting the system. Governments should invest more in training personnel and raising public awareness about issues relevant to applying an e-authentication system. An interesting finding of our gap analysis is that although all the studied e-authentication frameworks considered compliance with privacy laws and guidelines, there is still a gap in enforcing privacy laws and considering privacy issues from a customer's perspective in these laws as the current privacy laws do not address all these issues. This finding is in line with the McDonagh study [100] of the Australian privacy law and other similar laws, which concluded that current privacy laws and guidelines are inadequate to protect privacy in the e-government context. The results of the gap analysis reflect the analysis of the authentication frameworks versions at the time of the study. However, recent updates of these frameworks and the publishing of other supporting documents covered some of the gaps, such as a recent e-security review for the Australian government [25] which recognised the importance of establishing privacy awareness programmes and engaging consumers in e-security framework design.

The aim of developing this model was to use it as a guide to the gap analysis of current e-government authentication frameworks. However, we believe that our model can be used to enhance current e-government authentication frameworks by identifying absent activities and assessing the impact of different factors on all the activities and the interdependencies between them. In addition, the model provides a useful tool for defining quality and performance measures for an authentication system at different levels with respect to the expectations of all stakeholders.

IV.6 Conclusion

The purpose of this chapter was to investigate some existing e-government authentication frameworks in leading countries in e-government development by

analysing the core purpose of authentication in an e-government context. SSM was used to capture the essence of that purpose and to accommodate these different perspectives. Using SSM, the CPTM relevant to e-authentication was developed and used as a guide for the gap analysis. The findings of this analysis showed a gap in regard to the participation of stakeholders in the design of relevant policies and decisions, and in building consensus understanding for relevant terms and rules. It was also found that current privacy laws and regulations are inadequate and need to be revised to reflect customers' perceptions of privacy and that more effort is needed to ensure enforcement of these laws and regulations. These findings enhanced our understanding of the e-authentication concept, and the CM provided a powerful tool for investigating relevant aspects that influence the processes of authentication in e-government applications. The model can also be used to investigate details of the technical aspects of building an authentication framework.

Chapter Five

V. Preserving Privacy in the Context of E-government

V.1. Introduction

In e-government, preserving privacy is considered to be one of the main challenges facing governments when providing advanced services that require sharing, and exchanging of users' personal data with other government agencies. The results of the gap analysis (section IV.4.2) identified a lack of support for preserving privacy when providing e-government services. The studied frameworks emphasised the necessity to comply with privacy guidelines, regulations and laws but gave insufficient detail on how privacy can be preserved when designing and providing e-government services. E-government service providers have no clear guidance on how to apply privacy standards, and guidelines in the service provision level so that they comply with existing privacy regulations and laws. Without adequate details on how to preserve users' privacy when developing and providing an e-government service, e-government service providers apply their own perceptions of privacy and interpretation of the guidelines that exist in e-government frameworks. These variations in privacy perceptions leads to variations in the way privacy is preserved by different e-government services and a lack of consistency in following and complying with privacy guidelines, regulations and laws. Also, the willingness of service providers to comply with relevant existing privacy, regulations and laws is affected by the extent to which these regulations and laws are enforced. To understand different perceptions of privacy and the purpose of preserving privacy in e-government, a system thinking approach was followed using SSM approach (sectionII.2). This led to the development of a Conceptual Model Relevant to Preserving Privacy in the context of e-government (CMRPP) which is presented in section V.3. The activities of CMRPP were used to evaluate some existing privacy frameworks and to identify possible gaps or limitations in these frameworks (section V.4). Using the

results of this analysis, a privacy framework was proposed based on the CMRPP (Section V.5).

V.2. Privacy in E-government

V.2.1 Privacy Definition

Understanding the concept of preserving privacy needs an understanding and clear definition of privacy from different perspectives. Privacy has different definitions and interpretations with respect to individuals, groups and governments, and the perception of privacy is influenced by several factors, such as cultural, social and political environments. There are many definitions of privacy in the literature across different disciplines. In the Oxford dictionary, privacy is defined as *"a state in which one is not observed or disturbed by other people*"[33]. The issue of privacy has been clearly recognised by researchers for some time. Back in 1890, Warren and Brandeis defined privacy as "*the right to be left alone*" [101] . A similar definition by Byrne [102] states that privacy is "a zone of inaccessibility that surrounds a person". In another early recognition of privacy, Parker (in 1974) defined privacy as "*Privacy is control over when and by whom the various parts of us can be sensed by others* " [103]. Many other definitions support the core of this definition where privacy is seen as the ability to have control over when, how and to what extent information about someone can be accessed by others [52]. In another dimension, privacy is seen as a "*social arrangement that allows individuals to have some level of control over who is able to gain access to their physical selves and their personal information.*"[52]. Privacy concerns have increased due to the increased growth in the use of electronic services in the public and private sectors and a trend towards integrating these services, outsourcing services to third parties and the recent increase in using cloud resources to provide more efficient and cost effective services.

V.2.2 Privacy Regulations and Laws

The right to privacy is considered an essential human right [104], [103] and [52]. However, the benefits and harm of absolute privacy has been a subject of long debates [103] and [52]. From the law perspective, the first recognition of protecting privacy at a country level was the US Privacy Act of 1974 [105]. This was followed by the UK Data Protection Act 1984 and the Access to Personal

Files Act 1987 which was replaced later by the Data Protection Act 1998 [106]. In 1980, the OECD published Guidelines for the Protection of Privacy and Transborder Flows of Personal Data [104]. These international guidelines were concerned with the protection of data about an individual or group in any form and were used by OECD countries to formulate their own privacy regulations and laws. However, with the increasing use of technology and the internet in processing personal information there is a need for more specific regulations and guidelines that support the right of privacy of information when manipulated across borders. Recently the European Commission (EC) published a proposal which includes general data protection principles while considering the advancement in technologies and encouraging the development of consistent privacy laws between EU countries [107]. There are many differences between current privacy laws in different countries and sometimes a complete absence of these laws in other countries. This is a challenging issue in a world where personal information might be flowing around the world between countries.

V.2.3 Privacy Frameworks in e-government

The issue of privacy has been considered in the literature in a few proposals for e-government frameworks. These frameworks tackle the issue of preserving privacy and security from different perspectives. Belanger and Hiller proposed a framework for e-government and used it as a guide to identify privacy issues for e-government services, that would be specific for each stage of e-government [11]. Although, this framework is a tool highlighting complex issues that might occur when providing e-government services and it aids the decision making processes to resolve these issues, it was at the abstract level and did not provide details on privacy preservation at the service level. Other frameworks, such as [108] and [13], focus on considering privacy at the design and implementation stage of e-government services.

From the government perspective, security and privacy frameworks have been developed to provide processes and guidelines to be followed by e-government services providers when designing an e-government service or evaluating how privacy is preserved in an existing service. Privacy frameworks have existed in the form of standalone documents of privacy frameworks, as guideline for assessing privacy impact when providing the service, or as part of a security

framework. Examples of these frameworks are the Privacy frameworks and Privacy Impact Assessment documents of the UK [26], US[109], Canada[110], Australia [111] and the Asia Pacific Economic Cooperation (APEC) countries [112]. From a technical perspective, the framework proposed in [108] adopts multi-agent based approach for managing privacy and evaluating trust in e-government agencies. The framework provided a technical solution for enhancing and preserving privacy by following a set of identified privacy rules and information about the involved parties roles, rights and responsibilities. However, the framework did not give details on how these privacy rules were identified. Another framework proposed in [13] focuses on analysing security and privacy requirements based on *i** which is an agent-oriented requirements modelling language. The framework supports different analysis techniques such as attacker analysis, dependency vulnerability analysis and countermeasure analysis. These techniques are used for analysing security requirements and were integrated into the requirements engineering process. However, the privacy requirements were covered as part of the security requirements based on the confidentiality of the information and were not considered from the perspective of the user.

V.3. Modelling Privacy Preservation in E-government

Privacy definitions, (see section V.2.1), indicate that privacy meaning varies according to different perspectives and is influenced by many factors and accordingly the ways of preserving privacy will vary. In an e-government context preserving privacy has inherited the complexity of privacy concept as well as having the complexity associated with e-government and the influences of political, cultural and social factors inherent in the domain. Thus, SSM was chosen to develop the CMRPP in e-government. SSM and in particular the EMA method as described in sectionII.3.1, was used to build an comprehensive conceptual model that considers different perspectives with regard to preserving privacy and influencing factors associated within an e-government context.

V.3.1 Developing the Conceptual Model (CM)

V.3.1.1 Developing Root Definition(s) (RDs)

A set of RDs that describe the purpose of preserving privacy in e-government was developed. The development of these RDs was informed by the knowledge

acquired from developing CMs relevant to government, e-government and authentication in e-government. Also, the purpose of preserving privacy in existing e-government privacy frameworks found in the literature was considered. To define the purpose of preserving privacy in e-government, different definitions of privacy in the literature were analysed, such as those in [103] and [52] as well as the definitions found in e-government relevant frameworks, standards and guidelines, such as the UK privacy by design framework [26], the NIST Guidelines [109] and the OECD guidelines [104]. Based on a thorough analysis of these privacy definitions, led to the adoption in this research of the definition of privacy as "a social arrangement that allows individuals to have some level of control over who is able to gain access to their physical selves and their personal information [52]". The conclusion drawn from analysing relevant privacy frameworks and guidelines led to defining the core purpose of preserving privacy in the context of e-government as "to enable users of e-government services to have control over their information when using e-government services". Nine RDs relevant to preserving privacy in e-government were defined. These are:

RD1- Core Transformation (T)

> *-- A government owned system, operated by appropriately skilled and knowledgeable staff, to enable users of electronic government (e-government) services to have appropriate control over their owned information, by assigning appropriately defined levels of control to information owned by users when manipulated by service providers i.e. gathered, stored, accessed, shared and/or communicated between the government agencies and its partners while considering the expectations and needs of involved parties and meeting the identified security requirements of the provided services, enforcing relevant policies, regulations and laws, considering the impacts of social, cultural and political factors and complying with relevant standards and guidelines where appropriate and possible.*

RD2- Support System (S1)

> *-- A system to define ownership rights on users' information when manipulated by electronic government service providers by determining*

ownership rights for each identified type of information manipulated by the service and at each stage of manipulation while considering relevant ownership rights and laws and the dynamic changes in the expectations and needs of involved parties.

RD3- Support System (S2)

-- A system to define appropriate levels of control for information owned by users of e-government services by categorizing an appropriately selected set of controls and rules into levels according to the degree of impact of the identified risks on the users' owned information while considering relevant standards and rules and guidelines in 'Best Practices' and the dynamic changes in the needs and expectations of involved parties.

RD4- Support system (S3)

-- A system to ensure that the human resources available to support all activities enabling the users of electronic government services to have appropriate control over their owned information will match the requirements of those activities through the allocation or recruitment of staff with appropriate capabilities that match identified human resources' requirements for carrying out those activities while considering the operation of relevant training and education programmes and acting upon current personnel policies.

RD5- Linking System (L1)

-- A system to determine security requirements of a provided service by applying an appropriate requirements elicitation approach that takes into account possibly conflicting requirements of the various involved parties, applicable policies, regulations and laws while providing actionable, measurable, testable requirements that reflect relevant needs and expectations of involved parties and consider the users' ownership rights.

RD6- Linking System (L2)

-- A system to enable the deployment of levels of control over user owned information throughout any manipulation of that information when

using e-government services, by presenting those levels and types of control in a transparent ,flexible and easy to use way to all the users of electronic government services while utilizing appropriate existing technical tools and mechanisms and considering the enforcement of relevant rules and policies where possible within the limitations of current technologies and available resources.

RD7- Linking System (L3)

-- A system to ensure the compliance of involved parties with relevant regulations, policies and laws by monitoring the compliance of all involved parties when providing e-government services while considering the operation of relevant training and education programmes to for raising the public awareness about those regulations, policies and laws that affect them with consideration of common principles and 'Best Practices'.

RD8- Linking System (L4)

-- A system to undertake the enforcement of relevant policies, regulations, and laws on all involved parties by exercising authority and power to apply suitable penalties in response to any violation of relevant regulations, policies and laws when necessary while considering relevant international agreements.

RD9- Planning, Monitoring, and Control system (PMC)

-- A system owned by a government, and operated by appropriately empowered government authorities to ensure that within the provision of e-government services, appropriate controls are applied to users owned information by monitoring the system activities and taking necessary actions where and when needed, while constrained by current applied laws, regulations and policies and available resources.

V.3.1.3 Developing the Consensus Primary Task Model (CPTM)

The CPTM was developed by deriving sets of activities for each RD (section II.3.2.2). These activities show what the system should do in order to be the system described by the defined RD. Following SSM rules and using our

logic and acquired knowledge the CPTM activities were developed to determine what should be done to achieve the purpose identified in a RD and to identify dependencies between activities. These activities were revised each time the RDs were enhanced. The final version of CPTM can be found in Appendix C.

V.3.1.4 Subsystems Decomposition

The CPTM was analysed to locate potential subsystems and to decide how the identified subsystems are related to each other as described in sectionII.3.2.3. Then the resulting subsystems were grouped into levels. The grouping was based on the interdependencies and relation between the subsystems (see section II.3.2.3). The subsystems extracted from the CPTM and their interdependencies are shown in Figure V.1; note that in this figure the dotted subsystems are duplicates of other existing subsystems repeated for clarity and the interdependencies between the subsystems are illustrated by arrows.

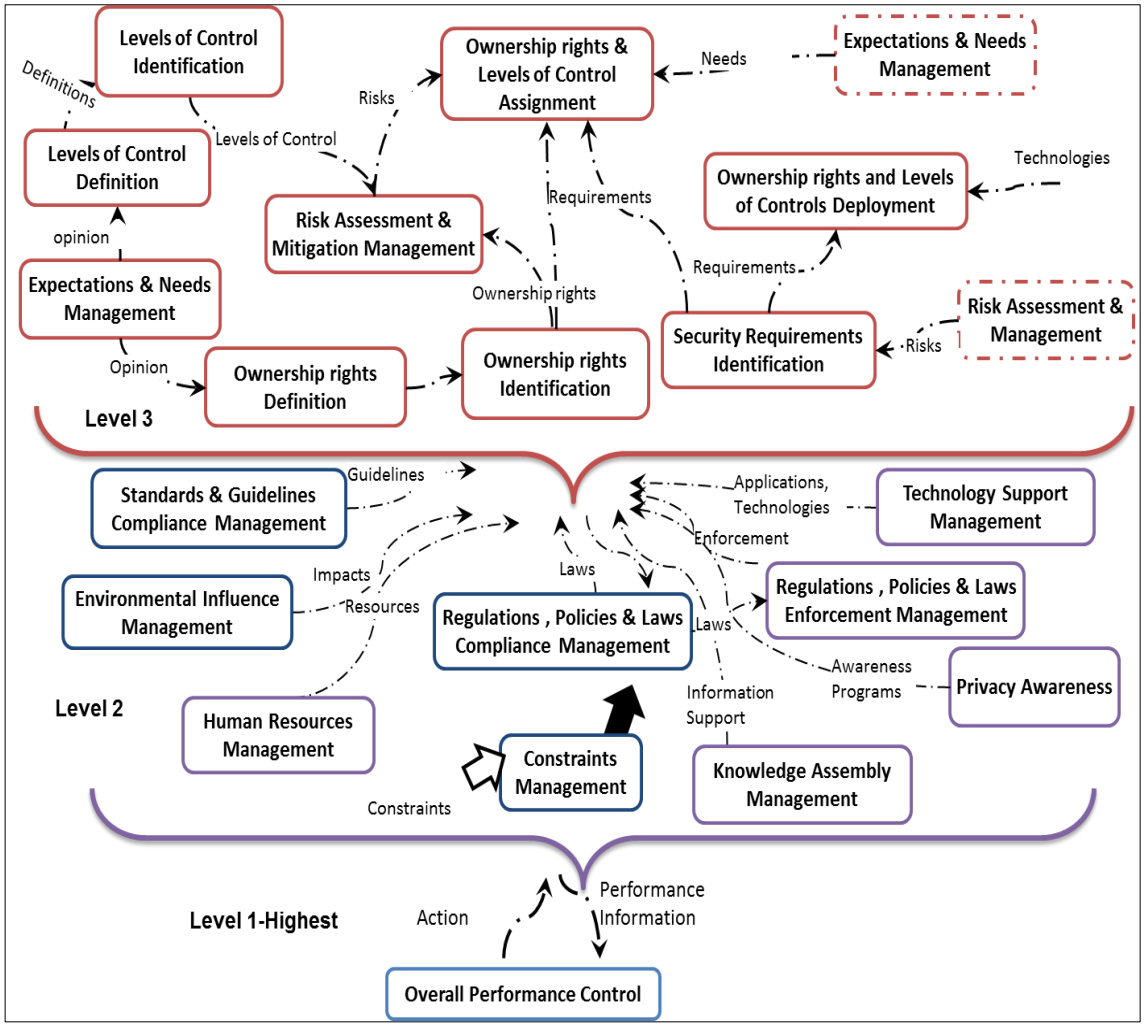


Figure V.1: High Level of subsystems of the CM relevant to Authentication

In Figure V.1, the subsystems are grouped into three levels as follows:

1. At the highest level (level1), is the overall performance control subsystem, which affects the rest of the subsystems. It includes monitoring and assessing activities for the performance of all of the subsystems and provides actions appropriate to these subsystems.

2. At level 2, there are the Knowledge Assembly Management, Constraints Managements and Human Resources Management, Standard and Guidelines Compliance Management; Regulations, Policies and Laws Compliance Management; Regulations, Policies and Laws Enforcement Management; Environmental Influence Management, Technology Support Management; and Privacy Awareness. These have activities affecting the subsystems in the next level and their affect needs to be considered when performing the activities in those subsystems.

3. At level3, remaining subsystems are shown. The dotted arrows show relations between these subsystems, which represent direct interdependencies between activities in these subsystems.

All the CPTM activities and the subsystem decomposition are in Appendix C.

V.3.2 Model Validation within SSM

The RDs and the complete CPTM were validated at each step using SSM defensible intellectual relationships (see section II.3.3).

V.3.2.1 Validating RDs

The RDs were validated using CATWOE elements (section II.3.2.1). The RDs were checked and all satisfied the requirement of having at least T (Transformation) and W (worldview) elements. The statements in each RD and in particular the T and W parts were based on knowledge gained by reviewing the literature and relevant privacy frameworks, standards, and guidelines. For example, the statement of the transformation (T) in the Core Transformation (RD1) which states “to enable users of e-government services to have control over their owned information” was based on reviewing existing privacy definitions, such as [52]and supported by privacy guidelines and standards such as [26] and [113]. The knowledge and logic of the researcher also was used to

develop the rest of elements of the RDs. Further validation for the RDs and CPTM was done through a survey to validate whether the CM reflected the stakeholders opinions or not. The survey design is presented in chapter VI while the survey findings are in chapterVII.

V.3.2.2 Validating CPTM activities

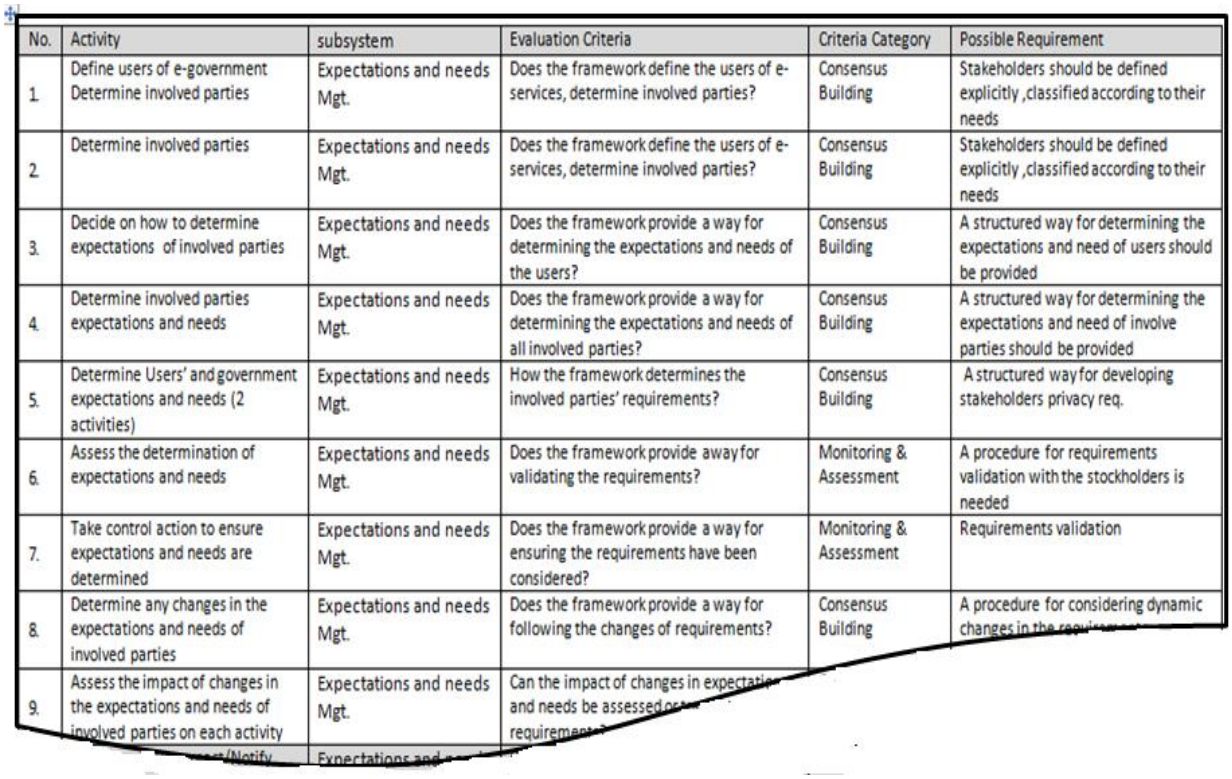
The derived activities in the CPTM were tested against each corresponding RD to ensure that each activity stems from a statement or word in the RD and describes what can be done to achieve the transformation in the corresponding RD. The logic and knowledge of the researcher was used in relating these activities to each other. The complete CPTM was validated by testing it against the Formal Systems Model (FSM) where the model is tested for its inclusion of the following features: connectivity, purpose, measures of performance, decision-taking processes (control), boundary, resources, and hierarchy, which are the features that should be in any model of a Human Activity System (HAS) [44],p. 32.

V.3.2.3 Subsystems Decomposition

For validating the subsystems created by the decomposition step, a simple rule is followed which groups all related activities that achieve a common purpose in a subsystem that can be named by the general purpose of its activities. An SSM rule is applied which states that any subsystem must satisfy the FSM requirements [44],p. 32, including the necessity for it to have monitoring and control activities.

V.4. A Gap Analysis of Current Privacy Frameworks

Our gap analysis approach was to use the CMRPP to formulate the evaluation criteria. This approach was used successfully in [54]. For each activity in the model a question was formulated. Then these questions were rephrased to formulate evaluation criteria. The resulting evaluation criteria were classified into categories according to their common purpose. Also, possible requirements which should be satisfied by any framework for preserving privacy in e-government were extracted from the CMRPP activities. Figure V.2 shows part of the table where the model activities were mapped into evaluation criteria and possible requirements of a privacy framework. The complete table is in Appendix D.



No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
1.	Define users of e-government Determine involved parties	Expectations and needs Mgt.	Does the framework define the users of e-services, determine involved parties?	Consensus Building	Stakeholders should be defined explicitly ,classified according to their needs
2.	Determine involved parties	Expectations and needs Mgt.	Does the framework define the users of e-services, determine involved parties?	Consensus Building	Stakeholders should be defined explicitly ,classified according to their needs
3.	Decide on how to determine expectations of involved parties	Expectations and needs Mgt.	Does the framework provide a way for determining the expectations and needs of the users?	Consensus Building	A structured way for determining the expectations and need of users should be provided
4.	Determine involved parties expectations and needs	Expectations and needs Mgt.	Does the framework provide a way for determining the expectations and needs of all involved parties?	Consensus Building	A structured way for determining the expectations and need of involve parties should be provided
5.	Determine Users' and government expectations and needs (2 activities)	Expectations and needs Mgt.	How the framework determines the involved parties' requirements?	Consensus Building	A structured way for developing stakeholders privacy req.
6.	Assess the determination of expectations and needs	Expectations and needs Mgt.	Does the framework provide away for validating the requirements?	Monitoring & Assessment	A procedure for requirements validation with the stockholders is needed
7.	Take control action to ensure expectations and needs are determined	Expectations and needs Mgt.	Does the framework provide a way for ensuring the requirements have been considered?	Monitoring & Assessment	Requirements validation
8.	Determine any changes in the expectations and needs of involved parties	Expectations and needs Mgt.	Does the framework provide a way for following the changes of requirements?	Consensus Building	A procedure for considering dynamic changes in the requ
9.	Assess the impact of changes in the expectations and needs of involved parties on each activity	Expectations and needs Mgt.	Can the impact of changes in expectatio and needs be assessed on requirement		
		Expectations and			

Figure V.2: A snapshot of mapping CPTM activities into evaluation criteria.

Using the these evaluation criteria, a gap analysis was performed on selected published privacy frameworks and Privacy Impact Assessment (PIA) documents relevant to e-governments in the UK [26], US [109], Canada [110], Australia [111] and APEC privacy framework [112]. The APEC privacy framework is the official document used by New Zealand as a privacy framework. These frameworks were selected as they are the leading countries using e-governance as reported by the UN report on e-government [22], and the privacy framework documents for these countries are publicly available in English. Also, these countries have established privacy laws and regulations. The selected frameworks were compared using the evaluation criteria to determine their status of preserving privacy. However, as discussed in section IV.4, there are other countries with higher rank in the UN report [22] on the development of e-government, such as the Republic of Korea who is ranked first, the Netherlands second, and Denmark fifth in the ranking. These countries have privacy frameworks that unfortunately were not available publicly in English which limits the results of the presented gap analysis. The inclusion of these frameworks would have been valuable in our gap analysis of existing privacy frameworks as

these countries have different social, cultural environments. However, the results of the gap analysis are still valid for the frameworks for the countries being analysed.

V.4.1 Evaluation Criteria

The evaluation criteria formulated using the CMRPP were grouped into categories, with names reflecting the criteria. The groups are:

1. **Consensus Building:** these evaluated: the framework's ability to handle the expectations and needs of all stakeholders; its ability to provide a way to resolve possible conflicts in the identified needs and reach an agreement on defining relevant terms and consider dynamic changes in identified requirements.
2. **Information Ownership Management (Definition, Identification):** these evaluated: the framework's ability to provide definitions of ownership rights to information about users; and to identify the ownership rights of information manipulated by electronic government service providers at different stages of manipulation.
3. **Security Requirements Elicitation**: these evaluated: the framework's approach to derive security requirements and assess and mitigate risks relevant to privacy.
4. **Rules and Controls Management (Definition, Identification and Assignment):** these evaluated: the framework's ability to provide schemas to define and assign rules and controls to protect the privacy of users' information.
5. **Rules and Controls Deployment (Presentation and Enforcement):** these evaluate: the framework's ability to present and enforce defined rules and controls.
6. **Environment Awareness:** these evaluated: the framework's ability to recognize environmental factors such as political, cultural and social factors.
7. **Privacy Awareness:** these evaluated: the framework's ability to consider raising privacy awareness between involved parties

8. **Knowledge Management:** these evaluated: the framework's ability to consider relevant knowledge about guidelines, standards and best practices.
9. **Monitoring & Assessment:** these evaluated: the framework's ability to support self-reflection and self-validation.

V.4.2 Findings

In this section we discuss the results of the gap analysis performed on the selected privacy frameworks against the identified criteria. In the analysis we considered the absence of activities or the absence of similar activities in the analysed frameworks as a gap. In addition, if an activity was mentioned without much detail on how it could be adopted it was considered to be absent and was noted as a gap. Table V.1 presents a summary of the main analysis results. This table summarises the results according to the evaluation criteria categories, while the original analysis table had all the 120 evaluation criteria listed. In the results we used the symbol ✓ to indicate that the framework had an activity that satisfied this criteria, ☑ indicates that the framework had an activity that partially satisfying the criteria, ☒ indicates that the framework had an activity but with limited details and so the criteria was not satisfied, and ✗ indicates the absence of the activity from the framework and that it is not satisfied. The gap analysis showed there were positive points in these frameworks, such as the wide recognition across the analysed frameworks of the necessity to consult stakeholders, especially users when designing a new service. Also, raising privacy awareness between users is covered briefly across the analysed frameworks. In general, the frameworks provide guidelines for government agencies or third parties to follow when providing an electronic service (e-service), though these guidelines were not detailed enough to guide service providers when developing a new service or sharing users' data between different service providers. However, the main gaps identified were ownership rights management, and enabling the user to have control over their owned data. Though, this concept was mentioned in [26] as a recommendation, no details were given on how it can be achieved. Another gap was recognizing and agreeing on levels of control and assigning these controls to users' own information and presenting and deploying these levels of controls to enable users' control over their owned information. Finally, there was a lack of

consideration of the influences of environmental factors such as political, cultural and social factors when identifying the privacy requirements of an e-government service.

Evaluation Criteria	AU	APEC	CA	UK	US
Consensus Building • Recognise stakeholders expectations and needs • Resolve conflict in needs • Consider dynamic changes in needs	☑	☑	☑	☑	☑
Information Ownership Management • Define Ownership rights and considers users views • Consider defined Ownership rights when classifying data about the user • Classify data according to sensitivity while considering users' perspective	☒	×	☒	☒	×
Security Requirements Elicitation • Assess risks on users' information • Provide ways for mitigating risks • Consider deriving security requirements	✓	✓	✓	✓	✓
Rules and Controls Management • Consider enabling users to have control over owned information • Provide ways for defining and assigning levels of control • Consider identified ownership rights and security requirements	×	×	×	☒	×
Rules and Controls Deployment • Provide ways for achieving enabling users to have control over owned information. • Deploy identified levels of control and ownership rights	×	×	×	☒	×

Evaluation Criteria	AU	APEC	CA	UK	US
Environment Awareness • Provide ways for considering impacts of social, cultural and political factors	☒	☑	☒	☒	☒
Privacy Awareness • Provide ways raising privacy awareness when applying levels of control	☑	☒	☑	☑	☒
Monitoring & Assessment • Provide ways for monitoring and assessing the applied activities	✓	✓	✓	✓	✓
Compliance with Standards and Laws • Provide guidelines to comply with relevant standards and laws • Ensure the enforcement of relevant regulations, policies and laws.	☑	☑	☑	☑	☑

Table V.1: Summary of gap analysis results

V.4.3 Requirements of Privacy Frameworks in E-government

Based on the CMRPP activities and the insight gained from performing the gap analysis, the following requirements were identified for any proposed e-government privacy framework. These requirements were derived mainly from the activities of the CMRPP and captured the best aspects found in the analysed privacy frameworks. These requirements are categorised according to the common purpose of each set of requirements:

a. Requirements related to Stakeholders Expectations and Needs:

1. A way to define all stakeholders involved in the provision of a service.
2. A structured way to determine the expectations and needs of involved parties (requirements of stakeholders).
3. Provide a way to achieve agreement on important definitions between stakeholders at an early stage of the framework.
4. Recognise the requirements of different users and their different capabilities.
5. A procedure for requirements validation with the stakeholders

6. A procedure to resolve conflicts in the expectations and needs of involved parties

7. A procedure for requirements validation with stakeholders.

8. A way to capture changes in the expectations and needs of involved parties (Stakeholders).

9. A way to consider the impact of dynamic changes in the expectations and needs on relevant activities in the system.

b. Requirements related to Information Ownership Rights:

10. Provide a structure way for determining information subject to manipulation when providing e-government services

11. Identify possible processes on user's information when providing e-government services.

12. A mechanism for classifying the sensitivity of the user's data which is subject to manipulation.

13. Provide definitions of ownership rights on information about users.

14. A mechanism for identifying ownership rights of information about users in a provided service.

c. Requirements related to Rules and Control over Information:

15. Provide definition of levels of control on users' owned information manipulated by a service.

16. A mechanism for identifying levels of control on information owned by users when using a provided service

17. Provide a way for identifying and assessing risks of potential threats on owned information.

18. Provide a way for defining an appropriate set of controls to mitigate identified risks on owned information.

19. Provide a scheme for categorising controls and rules into levels of controls.

20. Provide a way for considering security requirements when categorising control and rules into levels of control.

21. Provide guidelines for identifying appropriate control levels on user's owned information.

22. Provide a mechanism for assigning control levels to users owned information.

d. Requirements related to Rules and Control Deployment:

23. Provide a mechanism for enabling users to apply desired levels of control on their own information.

24. Consider transparency, flexibility and ease of use when designing applications to enable users to apply levels of control over owned information.

25. Provide a process for defining stakeholders' requirements when designing and deploying the levels of controls.

26. Provide a way to maintain the deployment of applied levels of control on user owned information throughout any manipulation of that information when using e-government services.

27. Provide a way to define the appropriate tools and mechanisms to be used for deploying levels of control on user owned information.

28. Provide guidelines on how to utilize appropriate tools and mechanisms when deploying levels of control over owned information.

e. Requirements related to Compliance with standards and Laws:

29. Provide guidelines for assembling relevant knowledge in 'Best Practices' and relevant standards and guidelines.

30. Provide a way to recognise and consider the impact of complying with relevant identified standards and guidelines on all activities in the framework.

31. Define measures for assessing and ensuring the compliance with relevant regulations, policies and laws.

32. Provide a way to recognise and consider the impact of relevant identified regulations, policies and laws on all activities in the framework.

33. Provide guidelines on how to comply with relevant regulations, policies and laws.

f. Requirements related to Environmental Factors Consideration:

34. Provide a way to recognise and consider the impact of political, social and cultural factors on all activities in the framework.

35. Define measures to ensure the consideration of environmental factors (Political, social, cultural factors).

36. Provide guidelines on how to act when considering environmental factors.

g. Requirements related to Privacy Awareness:

37. Provide ways to design privacy awareness programs and training to all involved parties

38. Consider best practices in raising privacy awareness

39. Implement privacy awareness programs and training

40. Provide ways to assess the privacy awareness and take required actions to ensure raising privacy awareness between all parties

h. Requirements related to Quality and Performance Assessment:

41. Provide a way to define measures for monitoring the conformance with constraints that affect system activities.

42. Provide a process to determine performance measures according to government's' performance expectations

43. Provide a way to define performance measures for assessing relevant activities according to stakeholders' expectations and needs and government's' performance expectations.

44. Provide assessment and monitoring activities over the framework activities which enable the assessment of these activities according to expectations and needs of the stakeholders and the system owner.

45. Provide a set of actions to ensure the achievement of the framework tasks and activities at each stage, in a way that satisfies the system owner expectations and the expectation and needs of stakeholders.

V.5. The Proposed Privacy Framework

The gap analysis exposed several gaps in the analysed frameworks, such as a lack of emphasis on ownership rights of processed information, and consideration of environmental factors when deriving security and privacy requirements. These gaps prove there is a need for a framework that covers these gaps while satisfying the identified requirements for a privacy framework in e-government listed in the previous section. The Privacy REquirements in E-

GOVernment (PRE_EGOV) framework was developed using the developed CMRPP and the knowledge gained from analysing existing privacy frameworks in e-government The PRE_EGOV framework addresses the identified gaps and seeks to satisfy the identified requirements. It facilitates an understanding of preserving privacy from different stakeholders' perspectives and builds a communal agreement on the privacy requirements of an e-government service. It also, considers the ownership rights over the information about the users of e-government services. An overview of the framework and its development are provided in the next sections.

V.5.1 PRE_EGOV Framework: An Overview

The proposed PRE_EGOV framework is a framework for identifying privacy requirements while considering the perspectives of the involved stakeholders and the ownership rights of information about the users. It provides a way for enabling the users of e-government services to have control over information about them. The framework consists of three main phases, namely: preliminary, the requirements elicitation and design phases. It also considers the influence of environmental factors i.e. political, social and cultural factors while performing the tasks in each phase. The impact of these factors is considered by identifying the possible factors that might affect the preservation of privacy when providing the service, and then formulating the impacts of those factors into a set of questions asked at an appropriate point in each task in the framework phases. Compliance with relevant regulations, laws and policies is also considered throughout the framework phases by identifying relevant requirements to ensure the compliance with relevant laws and regulations where possible. In addition, the importance of raising privacy awareness is recognized by the framework and incorporated within all the phases. Figure V.3 presents PRE_EGOV framework at an abstract level. The arrows in the figure illustrate the interdependencies between the phases and other elements of the framework. The dotted arrows indicate the impact of other elements of the framework on each phase while the solid arrows show the sequence and iteration between the framework phases.

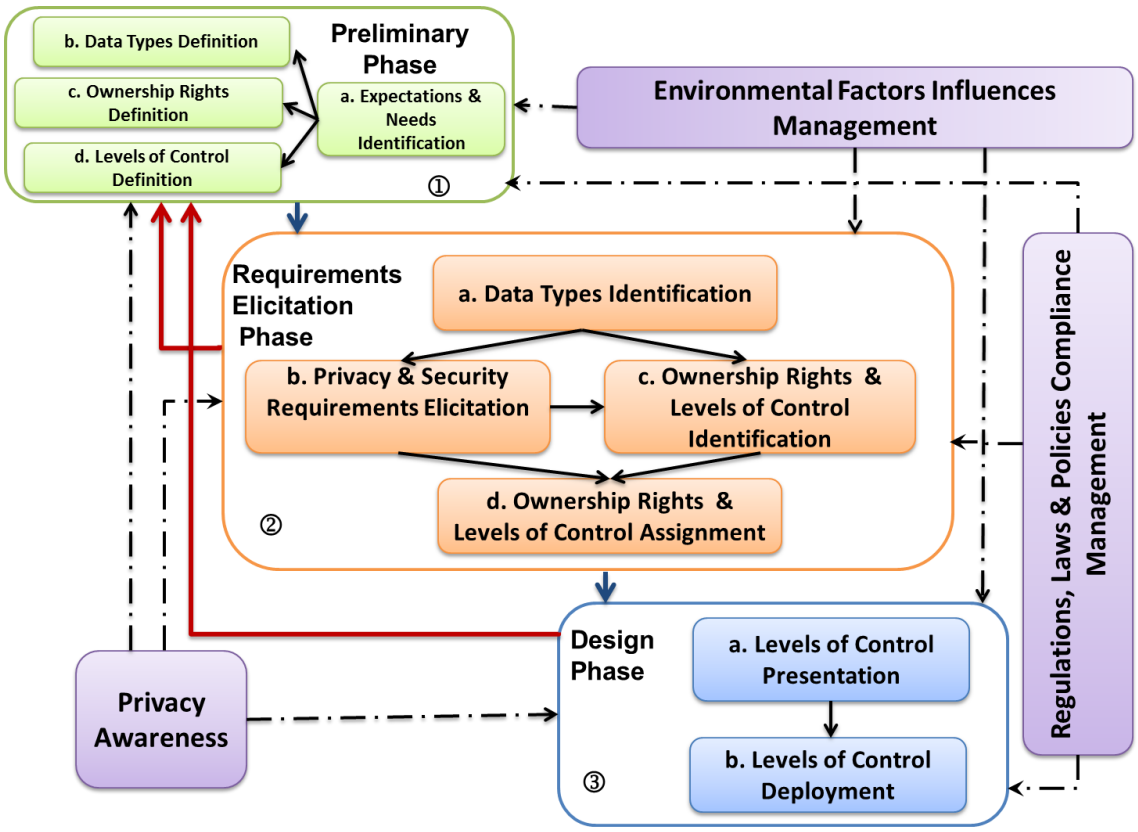


Figure V.3: PRE_EGOV Framework at an abstract level

The phases of the framework are described here in brief; however, further details are given in section VIII.2. The framework consists of:

V.5.1.1 Preliminary Phase:

This is a general phase and it has three main tasks:

a. **Expectations and Needs Management**: the main activities are building consensus between stakeholders on definitions of relevant terms such as ease of use, transparency, and flexibility, desired level of control over owned information and determining expectations and needs of stakeholders with respect to privacy and resolving possible conflicts that may arise in their expectations and needs while considering possible changes in those requirements.

b. **Data Types Definitions:** the main activities are defining data types' classification scheme for information about users according to the sensitivity of that information to the user and establishing agreement on the defined data types between stakeholders.

c. **Ownership Rights Definition**: the main activities are defining the ownership rights of information about the user and the relation between

these ownership rights and each data type of information. Also, having stakeholders' agreement on these definitions.

d. **Levels of Control Definition**: the main activities are identifying possible risks to users' information, identifying a set of appropriate rules and controls to mitigate possible risks, and categorizing identified rules and controls into levels of control of an agreed scheme.

The main deliverables of this phase are an agreed set of definitions of data types, ownership rights of information that are subject to manipulation by e-government service providers, and a set of definitions of levels of control .that enable the user to have control over their information and stakeholders requirements and preferences with regard to the whole framework of preserving privacy in the context of providing an e-government service. The phase will be reviewed while applying the framework to check for changes in expectations and needs.

V.5.1.2 Requirements Elicitation Phase

This is the main phase in the framework where the privacy and security requirements are determined while considering the ownership rights of information about users. It consists of four main tasks. Each task involves activities that describe how the task can be performed. An overview of these tasks and their activities is as follows:

a. **Data Types Identification:** the activities in this task analyse the data and processes involved in the provided e-government service, and then determine the information and data needed when providing the service and identify the types of information about users and processes involved in providing the service.

b. **Privacy and Security Requirements Elicitation: the** activities identifies potential threats to users' owned information and determines possible impacts from these threats, then identifies risks and possible rules and controls for mitigating the risks and considers the identified security requirements for providing the service. In this step, a risk assessment method and security requirements elicitation method of the government choice can be used while considering the identified expectations and needs of stakeholders and the defined definitions. Then, the privacy requirements of

the provided service are identified by analysing the information needed to provide the service and considering the defined ownership rights, levels of control and data types.

c. **Ownership Rights and Levels of Control Identification:** the activities identify ownership rights for the information types identified by assigning predefined ownership rights (as defined in the preliminary phase) to each type of information about users. Then, identify levels of control that can be assigned to information owned by the user by considering the identified risks and privacy and security requirements identified in the previous task, the user's desired level of control, and the expectations and needs of involved parties.
d. **Ownership Rights and Levels of Control Assignment:** the main activity is to assign identified levels of control from the previous task to each type of user owned information, while considering the identified security requirements.

The main deliverables of this phase are the identified data types, ownership rights and levels of control and the assignment of them to each type of information owned by a user and manipulated when a service is provided.

V.5.1.3 Design Phase

This phase presents the rules and controls so that the user can apply the assigned levels of control to owned information, while using the e-government service thereby enforcing the rules and controls in these levels. Its main tasks are:

a. **Rules and Controls Presentation:** this involves activities to identify the design requirements for presenting the levels of control, taking account of the diversity of users' capabilities and reflecting the assigned levels of controls.
b. **Rules and Controls Deployment:** these activities utilize available technology solutions to deploy the assigned levels of control and enforce relevant rules and controls when presenting these levels.

The framework also considers the influence of environmental factors such as political, social and cultural factors while performing all the phases. This is done

by formulating the impacts of those factors into a set of questions asked in each task. Compliance with relevant regulations, laws and policies is considered throughout the framework phases with an emphasis in the preliminary phase. The framework recognizes the importance of raising privacy awareness and incorporates it in all the phases especially in the requirement elicitation and design phases.

PRE_EGOV framework was described briefly. However, complete details of the proposed framework tasks and steps are provided in section VIII.2.

V.5.2 PRE_EGOV Framework Development

The framework design is informed by the developed CMRPP in sectionV.3 and it reflects users' perspectives on preserving their privacy when using e-government and the perspectives of other relevant stakeholders. The identification of the three phases and the main tasks in the framework was based on the interdependencies between the activities and the identified subsystems in the CMRPP, and on the stage these activities should be performed when developing a service. For example, the preliminary phase in the framework contains tasks that need to be performed at an early stage of development to prepare for later development and design tasks. The preliminary phase has four main tasks: the Expectations and needs identification, Data types definition, Ownership rights definition and levels of control definition. These tasks are informed respectively by the Expectations and needs management, Ownership rights definition and the Levels of control definition subsystems (see sectionV.3.1.3). The Data classification task is informed by some of the activities in the Ownership rights definition subsystem in the CMRPP (see Appendix C) Also, the task of Security requirements elicitation at the Requirements elicitation phase is informed by some activities of the developed CM relevant to authentication in e-government (see section IV.3.2.2). The activities in this task are relevant to identifying the level of confidence needed to provide a service and considered in the framework to achieve the balance between authentication and privacy requirements in the Requirements elicitation phase. Relevant privacy standards and guidelines such as [113] were also considered when developing the framework's definitions such as data classifications, levels of control and required levels of confidence.

These standards and guidelines will be referred to in the framework design where appropriate.

V.6. Conclusion

Preserving privacy is becoming a major concern in the provision of e-government services. The concept of privacy is complex and influenced by different factors. Therefore, a rich approach to understand the core purpose of preserving privacy in e-government using SSM was applied. This chapter introduced two important aspects of this research. It provided a CM using SSM which is relevant to preserving privacy in the context of e-government. Using this CM as the evaluation criteria, a gap analysis was performed on selected e-government privacy frameworks used by leading governments to develop e-government services. It also proposed a privacy framework which can be used as a powerful instrument to identify privacy requirements while considering the ownership rights associated with information about users and enabling the user to have appropriate control over owned information. The proposed framework is designed to be flexible and can be tailored to the needs of any government and service providers.

Chapter Six

VI. Evaluation of CMRPP -Survey Design

VI.1. Introduction

This chapter is about the survey to evaluate the CMRPP developed in section V.3 and the proposed framework for preserving privacy in e-government (PRE_EGOV) presented in sectionV.5. Although the CMRPP and the PRE_EGOV were developed on the basis of existing privacy definitions found in the literature and relevant standards and guidelines (see section V.3.1.1), there is a need to ensure that the CMRPP and the framework reflect the opinions of relevant stakeholders i.e. users of e-government services, services' providers, government body representatives and developers. Therefore, a rigorous approach to evaluate the RDs of the CMRPP was adopted. A survey is used to explore the opinions of relevant stakeholders from different countries to ensure the generality of the CMRPP. The survey was designed to evaluate the main core transformation statements (Ts) of the RDs and to determine if these statements reflect the actual views of respondents with different perspectives, backgrounds and environments. The survey aim was to explore the views of a wide population in the targeted countries and to study the effects of environmental factors i.e. cultural, social and political on their responses with regard to privacy issues in the context of using e-government services. Therefore, there was a need to select some countries with similar cultural, social and political environments and other countries which are different in these aspects. Due to the problems of sending the survey to targeted audience only three countries were chosen for distributing the survey. These countries were Saudi Arabia (SA), United Kingdom (UK) and Oman. Of these countries, two have similar cultural, social and political environments (Saudi and Oman), while the other (United Kingdom) has different environmental factors. This chapter describes the survey design, validation, and sampling and administration processes while the findings presented in the next chapter.

VI.2. Survey Overview, Objectives and Hypothesis

VI.2.1 An Overview

A survey is recognised as a useful instrument for collecting information about opinions, attitudes or behaviours of a targeted audience [31]. Therefore, a survey and in particular a web survey was selected to validate the CMRPP and the concept of the framework. The survey aim was to explore the views of a wide population of different people who can be considered stakeholders in e-government services in selected case studies, and to study the effects of the environmental factors i.e. cultural, social and political on their responses with regard to privacy issues in the context of using e-government services. The stakeholders were classified into four categories: users, government body representatives, services' providers and developers of e-government services. The user category includes anyone who is using or plans to use e-government services now or in the future. The government body representative category includes any person who represents a government agency and is involved in the decision process at a strategic planning level. The service provider category includes any person who works for a government agency or a third party who provides an e-government service using electronic means such as Internet, or mobile phones, under government approval, and the developer category includes any individual working for, or representing a company or group who participate in the design and technical implementation of an e-government service. To study the effect of the environmental factors on the participants' responses, there was a need to select countries which are similar in these aspects and others with differences in these aspects. The survey had a combination of closed and open-ended questions, which explored the background of the participants relevant to their relation with e-government and the use of e-government services, and explored their views on issues related to preserving privacy in e-government and on statements related to the RDs of CMRPP.

VI.2.2 Survey Objectives

The main objectives of the survey were:

- To validate the RDs of the CMRPP (sectionV.3.1.1)

- To explore participants' views with regard to the proposed framework in section V.5.
- To understand the participants' perspectives on the importance of preserving their privacy when using e-government services and its effect on their trust of the system when using e-government services.

VI.2.3 Hypothesis

The following hypotheses are tested by the survey results:

H1. There is no significant difference between the views of women and men.
H2. There are differences in the views of respondents from different age groups.
H3. There are no differences in the views of respondents from different countries with regard to the importance of preserving privacy when using e-government services.
H4. There are differences in the views of respondents from different countries towards the issues of sharing information between agencies.
H5. There is a difference in the views of respondents from different countries towards the issues of ownership rights.
H6. There are differences in the views of respondents according to their categories towards the level of control that the users should be allowed.
H7. There is high agreement between respondents on the statements in questions related to the RDs of the CMRPP.
H8. Preserving privacy in e-government services increases users' trust in using these services.

VI.3. Relevant Surveys in the Literature

There have been a few surveys of e-government that have investigated privacy issues and its effect on the use of e-government services. Some examined the relations between willingness to adopt e-government services and trust in e-government services. The issue of trust has been linked to issues of trust in the security and privacy of information systems provided in e-government systems [32] and [31]. McLeod and Pippin used open questions to explore individual perceptions of trust in e-government services. They introduced a trust model relevant to tax services and evaluated it using open questions illustrated by examples. The sample in their study was small as they had only 17 participants

and they mentioned the difficulty of having a large sample for an open-ended questions survey in a limited time [32]. Horst et al. used closed questions with one open question to investigate the perceived usefulness and trust as determinants of using e-government services [22]. Their survey suffered from missing data that affected the results of the experiment. There are also some global surveys that investigated the compliance of government websites offering e-government services with privacy laws and regulations. The WMRC Global E-Government Survey is an example of these surveys [114]. It investigated the compliance of selected e-government websites with privacy policies and compared the sites against a set of criteria and observations made were reported in the study. The survey targeted selected e-government websites and the observations were on the design of these websites and the opinions of the users of these web sites were not considered. Studying these examples gives an insight on practices to be avoided and good practices to be considered when designing a survey to explore privacy issues in this research area.

VI.4. Survey Design

In this section, the survey design is described in detail; including the data types used in the survey questions. To decide on the best survey design to fit the objectives of the survey, the lessons from previous surveys found in the literature were considered. The survey was designed to be a mix of closed and open questions using a descriptive approach (sometimes called an observational approach [115]). The essential variables and statements to be evaluated were formulated as closed questions that need to be answered and the respondents could not submit the survey without answers to them. This avoids having missing data in the survey results. However, open questions were used where needed and were optional to participants.

With regard to sampling, the survey was designed to follow a cross sectional design approach which aims to collect information on a targeted population at one point of time [115]. It uses random samples of the studied population, selected carefully to be representative of the targeted population. The reason for this is that the survey aim is to have a snapshot of the public views on privacy issues in a period of time.

VI.4.1. Data Types and Structure

The survey design followed a descriptive approach. The question order in the survey structure followed a funnel format structure [116]. Thus, general survey questions were introduced at the beginning and the questions get more specific towards the end. It had 30 questions, (25 closed questions and five open questions). An open question usually follows a closed question to gain additional feedback about the closed response. Also, in some of the closed questions, participants were given the option to add a new short answer if they wanted and if they felt that the provided answers did not cover their view. This option was called (Other) and was offered in questions (Q) Q5, Q7, Q8, Q13 (a), Q13 (b), Q15, Q16, Q17, Q24 and Q30. The types of response for closed questions were on either nominal[1] or ordinal[2] scales. The survey was developed in English and Arabic because these are the spoken languages of the targeted audience in the selected countries. The English version was developed first and pilot tested in two rounds (see section VI.8.1), then the survey was translated to Arabic and pilot tested. After validation of both versions was completed, the survey was published online and pilot tested again for a final round in both versions. The details of the validation process are presented in section VI.8.

VI.5. Writing Survey Questions

The survey followed the funnel format which aims to make the respondents comfortable with broad survey questions at the start before proceeding to specific questions. Questions 1 to 8 were designed to build background about the participant and their usage of e-government services. Some questions explored the participant's views with regard to the importance of privacy when using e-government services. Other questions explored if there is a relation between preserving privacy and an increase of trust in using e-government services. Also, there were questions exploring a participant's views about sharing user information with other agencies or third parties. There were questions about the levels of control that a user could have and who should be in charge of enabling and monitoring different tasks related to preserving privacy in e-government. These questions were aimed at gaining feedback

[1] Nominal scales or categorical scales are the scales that have no numerical value such as gender.
[2] Ordinal scales are rating scales that range from strongly disagree to strongly agree

about the CMRPP and to inform the design of the PRE_EGOV framework presented in section V.5.

VI.5.1. Survey Questions for verifying RDs

One of the main aims of the survey was to verify that the RDs of the CMRPP reflects the perspectives of a wide range of people who are involved in using, planning, providing and/or developing electronic government services. In SSM, the analyst captures the views of the stakeholders on a situation or a problem and then formulates them in a set of RDs, which are used to develop a CM for the situation or problem. These RDs of CMRPP were defined based on several definitions found in the literature and relevant privacy standards and guidelines (section V.3.1.1). However, since the RDs of the CMRPP are claimed to be general, there was a need to seek wider agreement on these RDs to ensure they reflect the different perspectives of relevant stakeholders in different countries. For that reason, the survey included questions to verify the core statements in the RDs of the CMRPP. There are two main elements in a RD which are the Transformation process (T) which represents the core purpose of the system and the World view (W). The T is the transformation process described by the main verb in the sentence and the W represents the belief of how the T can be achieved [44]. The aim of the survey questions designed to verify the RDs was to find out whether the T and W in each RD reflect the perception of the participants in the different categories. However, SSM rules for developing RDs require the use of precisely defined words and verbs to create one sentence which tends to be a long sentence. Therefore, the T and W parts of each RD were put in a list, and a question about the meaning of the T or the belief W was written in words that are easily understood without changing the meaning. However, some RDs were difficult to express in easy words with equivalent meaning, and these were stated as they were to avoid changing the meaning of the sentences. After this mapping the wording of the questions was checked by the researcher to ensure that the meaning in the original RD sentence had not been changed in the question.

There were some RDs and parts of RDs that were not covered by the survey questions for the following reasons:

- Some elements of the developed RDs (such as Owner, Actor and Constraints) were verified by a question or part of a question in the survey when possible and meaningful. The reason for this is that the focus was on covering the T and W parts of each RD, as the other elements can be verified by their logical dependence on the T or W, which was decided by the researcher. For example, the Actors in a system to preserve privacy will be government personnel and possible constraints to enabling the user to have control over his information can be complying with applied regulations and laws.
- The RD of the Supporting System (S3), (section V.3.1.1), which relates to determining security requirements, was not mapped to a question in a survey. The reason for this is that this RD provides details of how the security requirements can be determined. This is too specific for a general survey and was verified in the literature (section V.3.1).
- The RD of Supporting system (S4) section V.3.1.1), which provides details about required resources for the system was included in the first version of the survey as a question but omitted from the final version of the survey due to feedback from the pilot (see section VI.8.1). Although it is an essential RD of the CMRPP, its details were out of the scope of this research. The mapping process from parts of RDs to survey questions is in Table VI.1.

Root Definition Part	Question in the Survey
T Core Transformation RD (T) "…, to enable users of electronic government (e-government) services to have appropriate control over their owned information…"	Q11. Privacy can be preserved by enabling users to have control over their information (i.e. enabling users to decide on who can view and process their information). Please select to what extent you agree on the statement
T Core Transformation RD(W) " … by assigning identified levels of control to information owned by users when manipulated by service providers (gathered, stored, accessed, shared and /or communicated between the government agencies and its partners) and deploying these levels of controls ….."	Q16. Users can be enabled to have control over their information by allowing them to apply a desired level of control over the whole or part of their information throughout the processing of that information when using e-government services. Please select to what extent you agree on the statement

Root Definition Part	Question in the Survey
S1 Supporting System RD (W) " …, by identifying types of users' information manipulated by a service provider and determining ownership rights for each type of information and at each stage of manipulation…."	Q21. Ownership rights can be defined by identifying who own each piece of information collected about the user and specifying what can the owner do with that piece of information at each stage of processing that information. Please select to what extent you agree...
S2 Supporting System RD (W) "…, by categorising an appropriately selected set of controls and rules into levels according to the degree of impact of the identified risks on the users' owned information while considering relevant standards and rules and guidelines…"	Q18. The levels of control for enforcing the protection of users' information can be defined by grouping selected sets of security rules into levels of control based on the level of risk identified on users' information while considering relevant standards and guidelines. To what extent you agree on the statement?
L1 Linking System RD (W)"… by presenting those levels and types of control in a transparent ,flexible and easy to use way to all the users of electronic government services while utilizing appropriate technical tools and mechanisms and ensuring the relevant rules and policies are enforced within the limitations of current technologies and available resources."	Q27. In the future, a system for preserving privacy when providing e-government services should have the following features: Please rank the importance of the features to the system? (Easy to use, Transparent, Flexible, Meets the identified security requirements of the provided service, Enforces local relevant laws, policies and regulations issued by the government, Complies with relevant international standards and guidelines, Considers the impacts of social and cultural factors in the system environment, Considers the impact of political environmental factor, Cost effective)
L2 Linking System RD (W) "…..through monitoring the compliance of all involved parties and responding appropriately when there is a violation by exercising authority and power to apply the suitable penalties when necessary while educating and raising the public awareness about those policies, regulations and laws that concern them …."	Q25. The enforcement of the applications of relevant privacy regulations, policies and laws can be achieved by the following: Please select the appropriate statement(s)? (You can select more than one) By monitoring the application of relevant privacy regulations, policies and laws by all involved parties in e-government services provision. By empowering relevant authorities to respond to any violation of relevant privacy laws by applying suitable stated penalties. By educating and raising the public awareness about privacy regulations, policies and laws. No Opinion
PMC RD "…… to ensure that within the provision of e-government services, appropriate controls are applied to users owned information by placing relevant provision requirements on service providers and monitoring the system activities and taking necessary actions where and when needed …."	Q23. The government should identify and enforce requirements for preserving privacy and require all e-government service providers to satisfy those requirements to ensure that users are enabled to have control over owned information when using e-government services. To what extent do you agree ….?

Table VI.1: Mapping parts of RDs of CMRPP to survey questions

VI.6. Survey Targeted Audience

The targeted population were people in the following four categories:

1. Users of electronic government services from different ages and backgrounds.
2. People who represent government bodies.
3. Electronic government services' providers and government agencies and employers.
4. Developers of e-government services.

The targeted countries were Saudi Arabia (SA), United Kingdom (UK) (England and Wales) and Oman. These countries were selected as two of them have similar cultural, social and political environments (SA, Oman) and the other (UK) is different with regard to these factors. The aim was to explore the views of respondents from different backgrounds and environments and to investigate the effects of environmental factors - cultural, social and political factors on their responses. The survey was published online and a link to the survey was sent through different channels. A choice of "Other" in the country question was provided in the survey which allowed users from other countries to fill the survey. Although there were a few of these responses, they gave a feeling about other users views with regard to privacy issues when using electronic government services in their countries.

VI.7. Survey Administration and Sampling

The survey was designed to be self-administrated. It was published online and an email about the survey with a link to the survey (in both languages) was distributed through mailing lists, tweeted through Twitter accounts and shared through social networking sites. With regard to the sampling procedure, since the survey was an online survey, it was random by design and non-probability sampling was used. However, there was a need to ensure that the samples were random and that the percentages of the four stakeholder categories and the types of users were considered to be representative of the population to avoid any bias when distributing the survey. Therefore, the distribution channels were selected to avoid any bias and to ensure the coverage of all categories. The survey channels included universities' mailing lists (covering staff, academics and students), Twitter accounts for famous figures in the targeted

societies with large numbers of followers from different backgrounds, and ages and interests. Also, random government agencies' mailing lists were targeted to cover the categories of government body representatives, government agencies and employers. In addition, the survey was sent to companies who develop e-government services, and printed messages with a short link to the survey and the Quick Response (QR) code of the survey were distributed randomly in crowded streets, shopping centres and coffee shops. The aim was to reach out to all categories of eligible people including people who might use e-government services.

VI.8. Survey Testing and Validation

VI.8.1. Survey Pilot Test

The first round of pilot testing was the distribution of 15 printed copies of the English version to a sample of the targeted audience in the category of users from different countries. All distributed copies were filled in and returned. The high response rate for this round (100%) was due to the possibility of chasing respondents in person. The selection of participants for this round was by selecting participants from different countries in the category of users. There were 15 participants, six from UK, six from Saudi Arabia and three from other countries. In the last page of the pilot version, there were five open questions for feedback namely:

1. Did you feel that any question was a repetition of another one? If yes, which one(s)?
2. Was the questionnaire language easy to understand? (If not which part was difficult to understand?
3. Were there any questions that you felt needed some expertise to be answered? If yes, which one(s)?
4. Were there any parts of the questionnaire that were not clear and you needed more information to be able to answer them? If yes, which one(s)?
5. Please provide any extra comments you would like to add about this questionnaire?

Using the feedback from both pilot rounds and discussion with the respondents, the survey was revised and all issues raised were considered and appropriate amendments made. Both pilot and final versions of the survey are in Appendix E. Examples of feedback and the changes made as a result of the pilot rounds are presented in Table VI.2.

Feedback	Changes made
It is better to use another wording for "Do Not Know" option: in several questions	Changed to "No Opinion" in all questions
Define types of control in more details : in (Q13)in pilot version	All types of control were defined
Different remarks on Q16,Q17,Q19,Q26 in pilot version (long and a bit difficult, not clear, confusing)	Questions were revised and appropriate changes were made
Feedback on Q23 in pilot version "The question needs some expertise to answer", from many respondents	The question has been removed from the survey final version as it appeared to be out of the expertise of targeted audience as it asked about required resources for achieving the proposed system for preserving privacy.
Q24 need to be more clear in the way to rank the features	The question has been rewritten in a different way to make it easy to rank the features.
Some words were not clear(e.g. anonymous, compliance, stakeholders)	Changes were made using simpler words but with equivalent meaning or more clarification was given.

Table VI.2: Examples of feedback and changes on survey questions

The survey was then designed to be published online using Google forms[3]. This online version was tested again by a smaller sample of participants but different from the group used in the pilot round. A smaller group was used at this stage as the survey had been updated by the feedback from the pilot round and additional feedback on this version was to ensure there were no more remarks on the survey questions and that the transformation to Google forms had not introduced problems. The survey link to the online English version was sent to five respondents. Their feedback was on superficial spelling mistakes or the order of the questions with no new remarks about the questions. The feedback was analysed and the required changes were made. This version was finalised for distribution to the targeted audience. An Arabic version of the survey was then created. The translation was made by the researcher and the survey created online. The accuracy of the translation was tested by another five respondents whose first language is Arabic and are also fluent in English. These respondents saw both versions and gave feedback about the accuracy of

[3] Google forms are part of the Google Docs services which allows you to create free forms or simple surveys.

the translation and the equivalence of the meaning of statements used in both languages. The feedback covered a few spelling mistakes which were changed. The final version of the survey was sent to the ethical committee in the school of Computer Science and Informatics at Cardiff University for approval, who approved it for publishing. After both versions were finalized, all responses resulting from the online testing rounds were deleted from both of the spread sheets of the survey versions. Then, the survey was distributed online and through different channels to the targeted audience.

VI.8.2. Internal and External Validity Tests

Internal and external validity tests ensure that a survey is fit for use and that the results can be relied on. The survey design was tested using both internal and external validity tests explained in [115] and [117] and the survey design successfully passed these tests.

VI.9. Conclusion

The chapter presented a novel approach for validating RD elements using a survey. Details of the survey design were presented including the mapping of RDs into survey questions. The targeted audience were identified and justified. The survey design was validated and tested. The outcomes of the survey are presented in the next chapter.

Chapter Seven

VII. Evaluation of CMRPP -Survey Findings

VII.1. Introduction

This chapter presents the survey results and key findings are given. In addition, the implications of these findings on the CMRPP and the proposed framework are discussed and any changes required to the model as a result of the survey feedback are highlighted.

VII.2. Preparing Survey Data for Analysis

An important first step is to prepare the data for analysis. This section describes the preparation of the survey data for analysis. It includes data cleaning and validation. An additional preparation step was to combine the responses of the Arabic and English languages versions into a single data set and map the responses in Arabic to closed questions in the survey into equivalent responses in English.

VII.2.1. Combining Responses to One Data Set

The survey was distributed online in Arabic and English using Google forms [4], and the responses from both versions were originally saved in two separate spread sheets. However, the two versions of the survey were identical and had the same data structure, so they were easily combined into one spread sheet. The next step was to map all the Arabic responses to the closed questions to the equivalent responses in English.

With regard to responses to the open questions they were left untranslated at this stage. These responses will be categorised and analysed at a later stage of the data analysis. Thus, at this stage of data preparation these responses were

[4] Google Drive.2013.Creat Google available at https://www.google.com/intl/en/drive/start/apps.html

left in their original Arabic wording to minimise unintended changes in the original meaning.

This step of combining the two data sets was done before any other data preparation for better readability of the combined data sheet and to simplify the process of data validation and coding.

VII.2.2. Data Cleaning and validation

Data cleaning and validation involves inspecting the collected data for any mistakes in data entry or missing data [118]. In addition, this step involves checking the data validity for the analysis stage. This was done using the combined data held in the single data set. The single spread sheet was scanned for data entry mistakes caused by the combination step or from the mapping from Arabic to the equivalent English for the closed questions in the survey. The combined version of the data spread sheet was compared to the original spread sheets and any spotted data entry errors were corrected to the original response. This step was done in iteration, until the responses from both spread sheets were all mapped correctly in the new data set. The spread sheet was also checked for missing data or incomplete answers. However, no case was found of missing data. This was due to the survey design, as it was designed as an online survey where the respondents cannot submit the response without answering all the required questions. Also, the data set was checked for outliers[5] and incorrect values[6] in the responses to all the survey questions. However, the survey design had ensured there would be no outliers or incorrect values as the answers for the closed questions were all multiple choice. In addition, the data sheet was examined for any conflicting answers[7] and none were found. Also, any identical responses from the same person were considered a duplicate. This was verified by checking the time stamp of the response when the answers of two responses are identical. If the difference in the timestamp was a few seconds[8], then the response is considered a duplicate. There were two cases found of identical records from two

[5] Outliers are responses that are not consistent with the rest of the data set.
[6] Incorrect values are values that do not fit with the possible answers for the question.
[7] Conflicting answers happen when an answer to a question is conflicted by an answer to another question in the survey by the same respondent.
[8] The time to answer the survey is between 10-15 minutes.

respondents and it looked as if the respondents submitted the survey twice. A version of each response was kept and duplicates removed from the data set.

VII.3. Survey Data Analysis

The data analysis had two stages, Exploratory Data Analysis (EDA) and confirmative data analysis. The EDA was ongoing during the survey period and after data collection. This involved scanning the collected responses to get a general feeling about the results and spotting any potential problems in the survey. The confirmative data analysis was performed after the end of the survey period on a clean and validated data set. In this stage, a full detailed analysis is conducted to test the hypotheses and generate a summary of findings. This survey was used as an instrument to collect qualitative data about the opinions of the participants regarding different issues related to preserving privacy in an e-government context. Thus, the two stages of analysis were performed on the survey data using qualitative analysis methods. The data management and analysis was performed using two software packages Microsoft Excel 2010[9] and IBM SPSS Statistics20[10] .

VII.3.1. Exploratory Data Analysis (EDA)

VII.3.1.1 Overview

The EDA was the first stage of analysing the survey data. This analysis provides a feel for the initial results and trends in the survey. It can also show cases where additional data should be collected due to a low response rate or indications of potential bias in the characteristics of respondents. It also helps detect possible mistakes that were not spotted in the earlier stages of the survey design [119]. EDA was done during the collection of the responses. A spread sheet of the data collected from both versions of the survey was created during the stage of survey distribution and was updated with new responses frequently. In addition, summary analysis of the responses for each question was produced for the combined data. The survey was online for around two months after distribution of the survey links and sending emails to the targeted audience. EDA was performed around the middle of this collecting period. The

[9] Microsoft Excel 2010,Microsoft website at: http://office.microsoft.com/en-gb/excel-help/getting-started-with-excel-2010-HA010370218.aspx
[10] IBM SPSS Statistics 20.2013.IBM web site at: http://www-03.ibm.com/software/products/gb/en/spss-stats-standard

aim was to detect if there were any problems in the sample size or in the coverage of the targeted audience and to have a feel for the responses with regard to privacy issues in the context of e-government.

VII.3.1.2 Results with regard to the sample of the targeted audience

The targeted audience are citizens in Saudi Arabia, UK (England and Wales) and Oman. Participants from other countries were encouraged to take part in the survey. The aim was to have a representative sample of the population in each country. The latest census figures in the targeted countries are in Table VII.1, which gives the total populations and the percentages of women and men in each country.

Country	Population	Women %	Men%	Census Year
Saudi Arabia	29 million, 69% citizens(20 million)	49.5%	50.5%	2011[120]
UK(England and Wales)	56.1 million	50.8%	49.2%	2012[121]
Oman	2.77 million,68.5% citizens(1.9 million)	Not available	Not available	2010[122]

Table VII.1: Population census in surveyed countries

The Saudi and Omani censuses gave the number of citizens of the countries in the census but this was unclear in the UK census (England and Wales).

The EDA initial results analysis showed:

- There was high response from Saudi Arabia (216) and an equally low response from United Kingdom (30) and Oman (28).
- The percentages of men and women respondents were almost equal in Saudi and Oman; while in the UK men were dominant with around 74%.
- The respondents from Saudi covered all age groups, while in the UK there were no respondents under the age of 18 and in Oman there no respondent under age of 18 or over 60.

The major issue in this analysis was the low response from UK and Oman. The action taken at this point was to send the survey links to more randomly selected distribution channels such as emails to mailing lists, posts in social networks and printed short messages with a link to the survey and a QR code which is in Appendix E. The printed messages were used in the UK (Wales)

only and were distributed randomly to people in the streets, shopping centres and coffee shops. This action resulted in an increase in the UK respondents (doubling the number) and a slight increase happened in the responses from Oman. The percentage of women participating in the UK has improved slightly (by 1%). The respondents from all countries covered all the defined categories that people may fall into with regard to their relation with e-government services. The majority of respondents were users. The rest of the categories, i.e. the government body representatives, the service providers and the developers of electronic services, were represented by 8% each. Table VII.2 is a summary of the final responses from each country.

	Saudi Arabia	UK	Oman	Other	Total
No. of respondents	**228**	**61**	**36**	**20**	345
Female	50%	26%	58%	45%	46%
Male	50%	74%	42%	55%	54%
User	90%	93%	86%	80%	90%
Government body representative	8%	3%	14%	3%	8%
Electronic Services Provider	7%	3%	19%	10%	8%
Developer of electronic services	6%	5%	25%	15%	8%

Table VII.2: Summary of respondents' categories and gender

The percentages in Table VII.2, shows the sample can be considered unbiased and representative of the population of users of electronic government services in all countries, with caution about a potential bias in the Oman sample. This was due to most of the responses coming from Oman distribution channels that are used by well educated people and people working in government agencies or in developing e-government services. Although other channels have been sought to reach out to a wider part of the population, the response from these channels was low. The UK sample could also have some bias. It covers all the defined categories of stakeholders; however, the percentages of the government body representative and the electronic services provider are not high enough as the sample size was relatively small. These possible biases will be considered in the confirmative analysis.

VII.3.1.3 Summary of the Exploratory Data Analysis (EDA) Results

The EDA was performed by calculating frequencies and percentages for a combination of conditions to analyse the responses from different countries and in general. The calculated frequencies add up to 100% in most of the questions,

however, in some questions where the respondents can choose more than one answer, the accumulated percentage can add up to more than 100%. The main results of this stage were:

- There was high response from Saudi Arabia and fair responses from UK and Oman.
- Most of respondents had used e-government services (95% or over, while only 5% had never used these services). However, only 12% used e-government services very often, while 36% of respondents use them sometimes (see Figure VII.1).

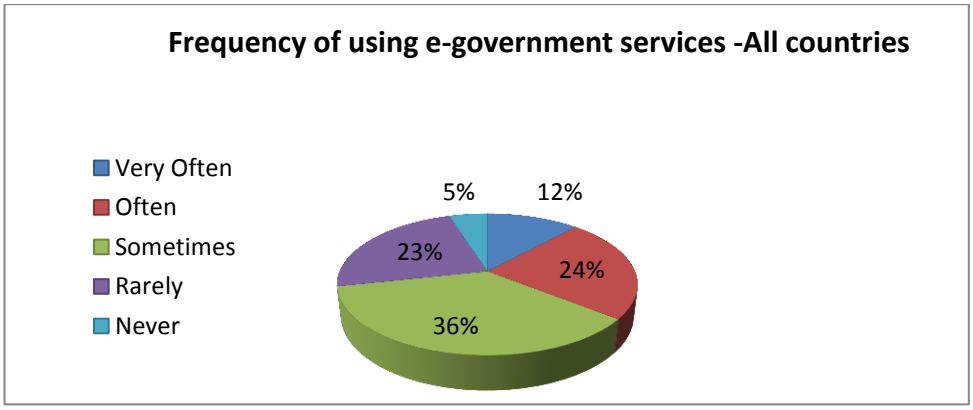


Figure VII.1: Frequency of using e-government services

- Individual personal usage is the main reason for using e-government services, while 23% have used e-government services on behalf of others and/ or used them for business and work.
- The most used e-government services are payment related services; however, percentages vary with regard to other types of services for respondents from different countries. This is due to the variation in maturity of the services provided currently in e-government portals of the targeted countries (see Figure VII.2).

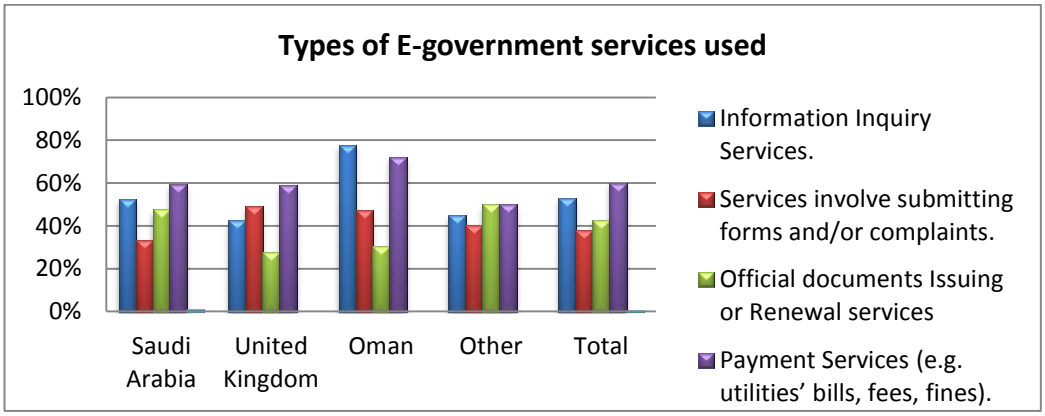


Figure VII.2: Types of e-government services used by respondents

- There is general agreement on the importance of preserving privacy among the users of e-government services (more than 90% of respondents). However, there is less agreement on how privacy can be preserved and on sharing information with other parties when using e-government services (see Figure VII.3).

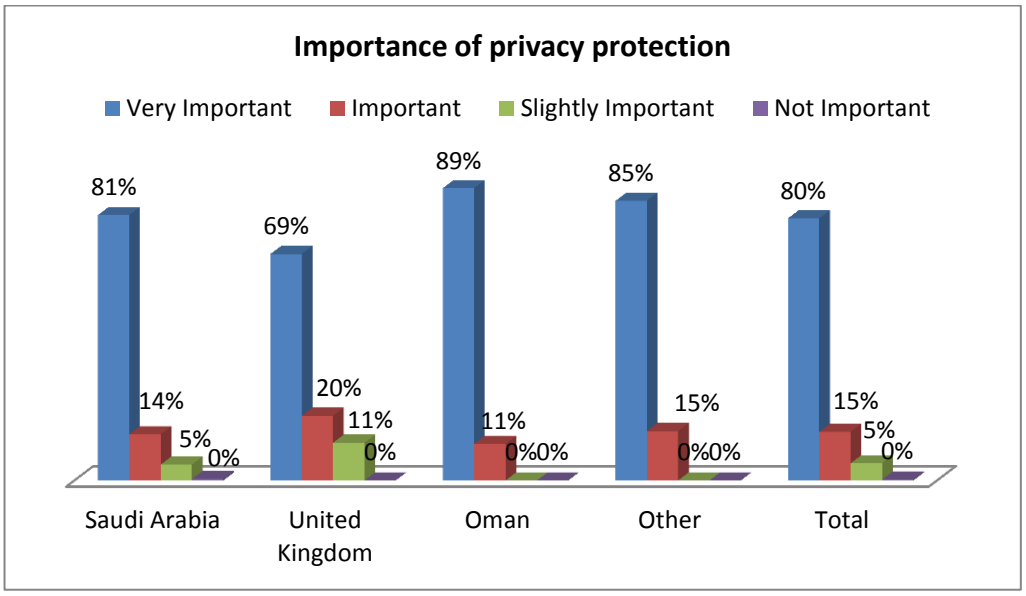


Figure VII.3: Views on the importance of preserving privacy.

- With regard to sharing users information provided in one service with other services (see Appendix F.1, Q13 (a) and (b)), more than half of the respondents (55%) favoured "sharing only information needed" to provide another service to the user by the third party, while the choice of "not sharing users' information" was favoured by 45% of respondents when the third party is not providing a service to the user. A new choice of "share with user consent" was added to the framework as a result of respondents' suggestions.
- As a response to Q 14 (Appendix F.1), 75% of respondents agreed that users should have control over their information when using e-government services, while only 17 % did not agree. However, in the UK sample, this was agreed by 92 %.
- The opinion on the extent of control that users might be given over their information (Q15, Appendix F.1) was almost evenly divided between allowing users to have full control (42%) and limited control (52%). Only 5% believed that users should not have any control over their information. However, the percentages differed between countries and

further analysis is required to investigate the views of stakeholders in each country on this (see Figure VII.4).

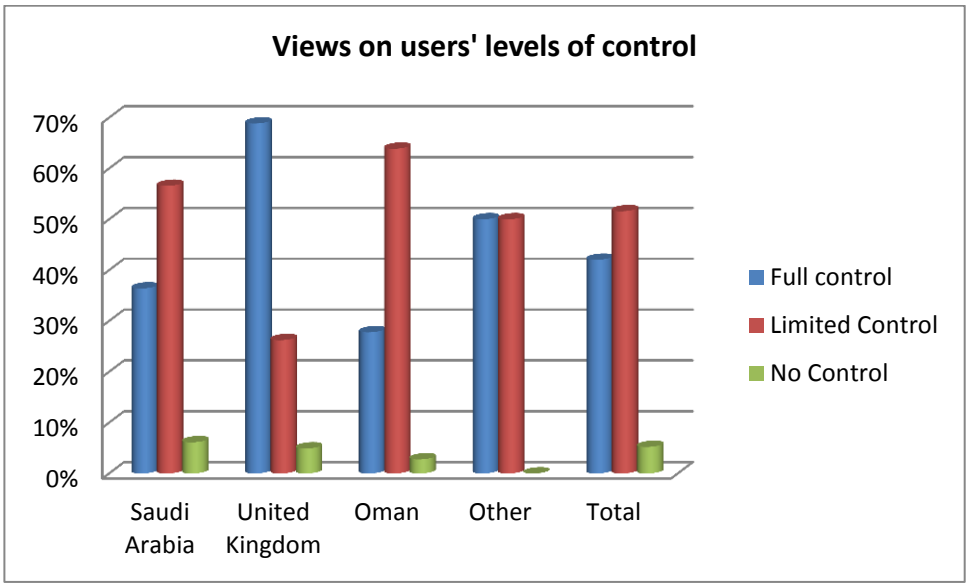


Figure VII.4: Views on extent of control over users' information.

- The majority of responses (87%) agreed that users can be enabled to have control over their information by allowing them to apply desired level of control over their information when using e-government services (Q16, Appendix F.1).
- Regarding who should be involved in defining the levels of control over information held about users(Q17, Appendix F.1), over half of respondents (52%) said the government while 41% chose the user and 33% opted for an agreement between all involved parties. This split also appeared with regard to who should define the ownership right of information about users. 53% chose the government, while 52% chose the user. These results will be analysed further in the confirmative analysis section.
- 46% chose a government body representative to be responsible for monitoring and assessing the process of preserving privacy in e-government services, while 21% chose an independent third party. These values varied a lot between countries, in the UK 41% supported an independent third party with only 7% supporting a government body representative (see Table VII.3).

Answers	SA	UK	Oman	Total
A government body representative	**58%**	7%	**42%**	**46%**
An independent third party	**16%**	**41%**	**22%**	**21%**
A representative body of the users.	9%	**13%**	3%	9%
A government body representative, An independent third party	5%	3%	11%	6%
An independent third party, A representative body of the users.	2%	10%	0%	3%
A government body representative, A representative body of the users.	8%	10%	6%	8%
A government body representative, An independent third party, A representative body of the users.	3%	0%	14%	4%

Table VII.3: Views on involvement in the monitoring and assessment

- There was a general agreement (95%) (Over 80% in all countries) that preserving privacy will increase users trust in using e-government services (see Figure VII.5).

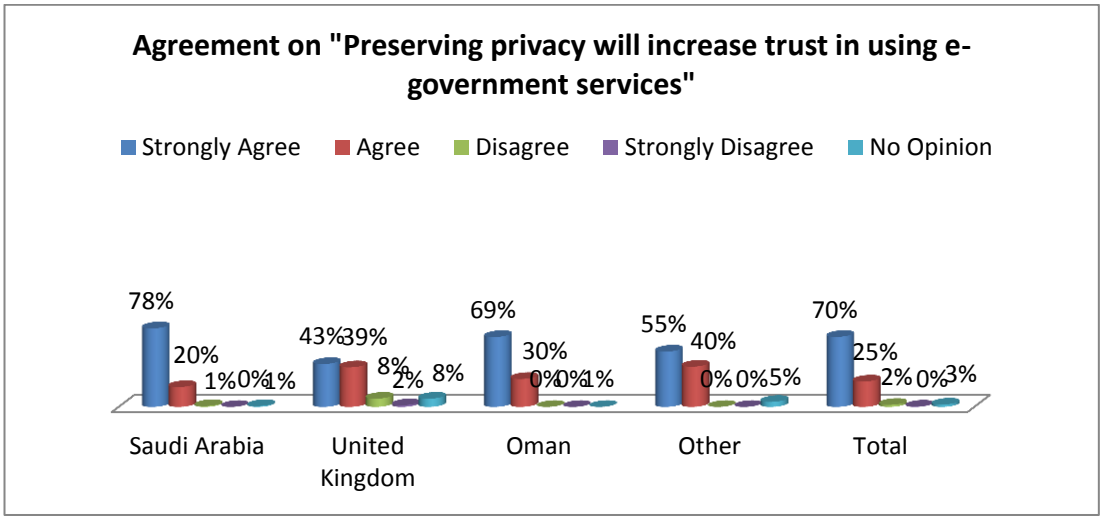


Figure VII.5: Views on preserving privacy will increase trust

- In response to Qs 16,18,21,23 and 27 which are related to evaluating statements in the RDs of the CMRPP (sectionV.3.1.1), there was general agreement between respondents on these statements (see Appendix F.1, Q16, 18, 21, 23, and 27). This is covered more fully in the Confirmative Analysis stage.

The complete results of the EDA analysis supported with tables and graphs for each question are listed in Appendix F.

The results found in this stage of analysis defined the background of the respondents and identified important factors that were used to analyse the results of the rest of the survey questions.

VII.3.2. Confirmative Analysis

The Confirmative Analysis is the detailed data analysis of the survey to realize relations between variables, draw conclusions on the analysis results, and summarise the findings. The data set used, in this stage should be complete and cleaned. This section covers this stage and analyses the effect of the independent variables on the rest of the survey questions.

The independent variables are country, age, gender, the use of e-government services and the respondents' relation type with e-government services. The four defined categories for the type of relation a respondent may have with e-government are: user, government body representative, electronic services provider and a developer of electronic services. The dependant variables are covered by the questions Q9 to Q30. The independent variables were used to predict the responses to the survey questions that were considered as dependant variables. In this analysis, pivot tables and crosstab tables were generated to analyse the differences in the answers between the groups and also the effect of these variables on the rest of the survey questions. The analysis of each independent variable effect is presented in this section.

VII.3.2.1 Analysis of effect of the independent variable Gender

The null hypothesis was that there is no significant difference in the responses to the survey's closed questions between men and women. The Independent-Samples T test was used in SPSS to test the significance of the difference where the p-value =0.05. The t-test for the difference in means is a hypothesis test that tests the null hypothesis that the means for both groups are equal, versus the alternative hypothesis that the means are not equal (2-tail) or that the mean for one of the groups is larger than the mean for the other group (1-tail) [123]. In this case we used the 2-tail test result. The significant t-test values were calculated for each closed question in the survey. The t-test value for all the closed questions varied between (0.08 and 0.98). Since the t-test values calculated were always larger than 0.05 which is the selected p-value, it means that we fail to reject the null hypothesis and that there are no significant

differences in the responses of men and women to the survey's closed questions. However, in general, women tend to choose to agree instead of strongly agree on questions whereas men choose strongly agree option.

VII.3.2.2 Analysis of effect of the independent variable Age

All age groups were covered by the survey respondents. However, the categories of "Less than 18" (3%) and "Over 60" (2%) are too small and this affects the analysis. Therefore, the effect of Age as an independent variable was excluded from the analysis.

VII.3.2.3 Analysis of effect of the independent variable Usage

Of all respondents to the survey, 90% were Users and 10% considered themselves Non-Users of e-government services. Looking at "Usage of e-government services" as an independent variable, the null hypothesis was that there is no significant difference in the responses to the survey closed questions between users and non-users of e-government services. The Independent-Samples T-test was used in SPSS to test the significance of the difference where the p-value =0.05. The t-test values were calculated for each closed question in the survey and the t-test results for all the closed questions varied between (0.07 and 0.91). Since the values were always larger than 0.05 which is the selected p-value, it means that we fail to reject the null hypothesis and that there is no significant differences in the answers to the survey questions between Users and Non-Users of e-government services. The only noticeable difference was that Non-Users tend to choose the No Opinion option in higher percentages than Users in questions Q16, 18, 21, 23, and 29(a) (see TableVII.4). However, for the other options in these questions there were no significant differences between the Non-Users and Users answers.

No Opinion %	**Q16**	**Q18**	**Q21**	**Q23**
Non Users	11.4%	20%	17%	14.3%
Users	4.8%	9.6%	8.4%	1.9%

TableVII.4: Users and Non-Users responses with "No Opinion" option

VII.3.2.4 Analysis of effect of the independent variable Country

For this independent variable, it was hypothesized there would be differences in the responses from different countries. However, no significant differences were seen in the majority of responses to the survey questions which are related to

general privacy issues. The only noticeable differences were spotted in responses to questions 13 (a),13(b), 14, 15, 17, 20, 24 25 and 27. These questions covered details of the suggested solution for preserving privacy and who should be involved in deciding on the steps of the proposed solution. The differences were:

- A slight difference between respondents from different countries towards issues of sharing information with a third party when this third party is providing a service to the user(Q13(a)) or not providing a service to the user (Q13(b)) (see Table VII.5). It can be seen that (in responses to Q13 (a)) there is almost general agreement that information can be shared in an unidentifiable form (anonymous). While responses to Q13(b) show the majority of UK respondents (70%) believe that users' information shouldn't be shared at all, and around 30% of Oman and Saudi respondents believe information can be shared but anonymously.

	SA		**UK**		**Oman**		**Total**	
Questions	**Q13 (a)**	**Q13 (b)**	**Q13 (a)**	**Q13 (b)**	**Q13 (a)**	**Q13 (b)**	**Q13 (a)**	**Q13 (b)**
Share all users' information	18%	10%	5%	2%	0%	3%	13%	7%
Share only relevant (needed) information to provide a service	12%	21%	13%	11%	25%	22%	14%	19%
Share users' information in an unidentifiable form (anonymous)	**55%**	31%	**48%**	11%	**67%**	33%	**55%**	27%
Should not share at all	13%	**38%**	28%	**70%**	6%	**42%**	15%	**45%**
Share with User Consent	1%	1%	7%	2%	3%	0%	3%	1%

Table VII.5: Summary of responses to Q13 (a) and Q13 (b)

- Q14 asked if users should have control over their information, the majority in UK answered Yes while around a quarter of the Saudi and Oman participants answered No (see Appendix F.1, Q14).
- The same difference occurred in Q15 about the extent the users should have control over their information. A high percentage (69%) of UK responses thought users should have "Full control" over their information while (26%) thought the user should have "Limited control". The Saudi Arabia and Oman responses were almost the opposite with more than half choosing "Limited control" and around a third choosing "Full control"

(see Figure VII.4) . Further analysis was made in this area to investigate the respondents' views within the four categories for each country and to see if there are any similarities between these categories across all countries, for this question (see Figure VII.6, Figure VII.7, Figure VII.8). This showed that there were no similarities between the UK respondents' views within the categories with the other respondents' views in Saudi Arabia and Oman. However, there were similarities between respondents' views within the categories between the respondents from Saudi Arabia and Oman.

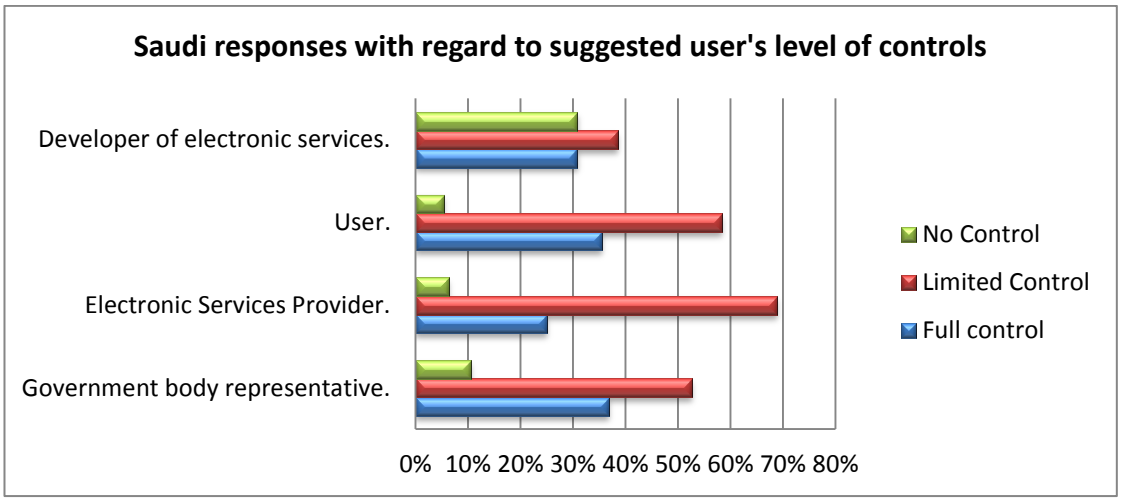


Figure VII.6: Saudi Arabia responses to suggested users' levels of control

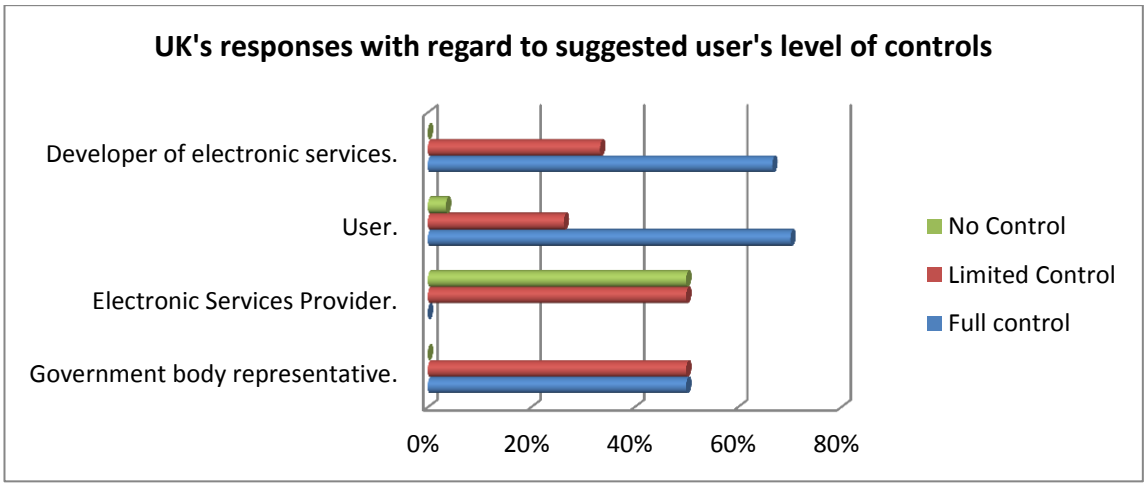


Figure VII.7: UK responses to suggested users' levels of control

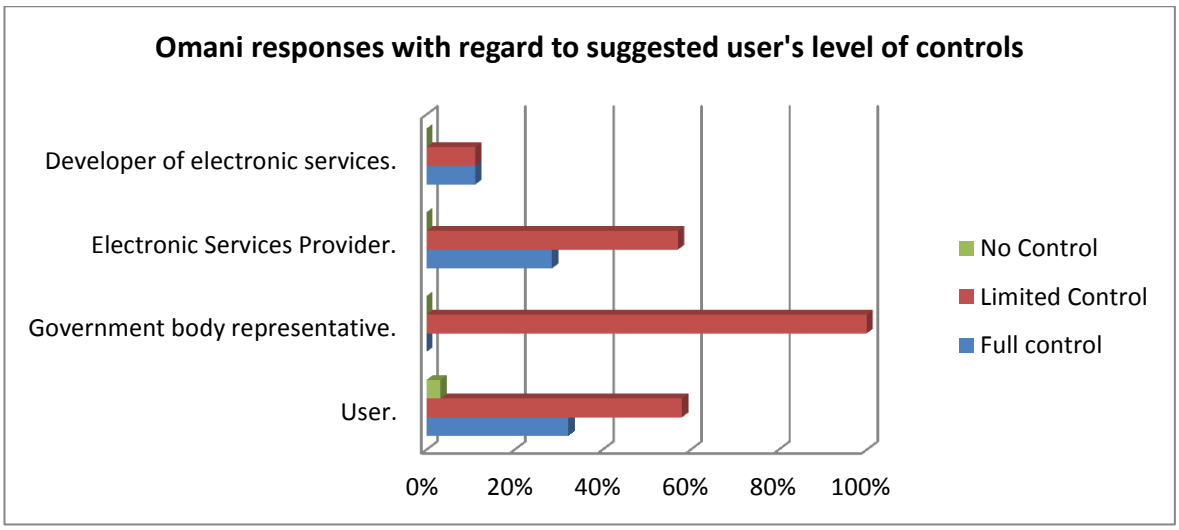


Figure VII.8: Oman responses to suggested users' levels of control

- Q17 covered who should be involved in defining the levels of control on information held about users. UK respondents chose Users first (54%) then Government (46%) while in Saudi and Oman, the Government was first choice (58% and 52% respectively), with Users as second choice (36% and 50%). In Saudi responses, the services' providers were chosen by (32%) as the third popular choice, while the third choice in Oman (44%) and UK (43%) was "By an agreement from the discussion between all involved parties". Similar results were found in Q20 about who should be involved in defining the ownership rights of information about users of e-government services (see Table VII.6). Note these percentages are accumulative as the respondents could choose more than one answer.

	SA		UK		Oman		Total	
Questions	**Q17**	**Q20**	**Q17**	**Q20**	**Q17**	**Q20**	**Q17**	**Q20**
Users	**36%**	**50%**	**54%**	**62%**	**50%**	**47%**	**41%**	**52%**
Government	**52%**	**57%**	**46%**	**34%**	**58%**	**50%**	**52%**	**53%**
Services' providers	**32%**	**25%**	18%	5%	31%	31%	30%	22%
Developers (technical developers of the services)	9%	6%	8%	3%	8%	8%	10%	6%
By an agreement from the discussion between all involved parties.	29%	18%	**43%**	**36%**	**44%**	**33%**	33%	23%
Government, Users, Services' providers	5%	6%	8%	3%	8%	11%	6%	6%

	SA		UK		Oman		Total	
Questions	**Q17**	**Q20**	**Q17**	**Q20**	**Q17**	**Q20**	**Q17**	**Q20**
Government, Users, Developers (technical developers of the services)	2%	0%	5%	3%	0%	0%	2%	1%

Table VII.6: Summary of Responses to Q17 and Q20

- Q24 was about who should monitor the process of preserving privacy, a high percentage of the responses from UK (41%) favoured an independent third party while in Saudi (58%) and Oman (42 %) responses favoured a government body representative.
- There were slight differences in the country's responses to Q25 where they selected from a list of three ways to achieve the enforcement of the application of relevant privacy regulations, policies and laws. A combination of monitoring and educating people was popular in all three countries. However, monitoring was second in the Saudi responses (28%), while a combination of all the three approaches was as a second choice for respondents in UK (31%) and Oman (44%) (See Table VII.7).

Suggest Choices in Q25	**Saudi Arabia**	**United Kingdom**	**Oman**
By monitoring the application of relevant privacy laws	**28%**	15%	11%
By empowering relevant authorities to r apply penalties.	11%	**10%**	3%
By educating and raising the privacy awareness	8%	8%	14%
Monitoring and Empowering	9%	**7%**	**8%**
Monitoring and Education	**31%**	**44%**	**50%**
Empowering and Education	3%	8%	**8%**
All the above	**21%**	**31%**	**44%**
No Opinion	11%	8%	6%

Table VII.7: Summary of responses to Q 25.

- In Q27, there were slight differences in the importance ranking for features in a future system for preserving privacy. However, the top features for all countries were Ease of Use, Transparent, Meet security requirements of the provided service, Enforce relevant privacy laws, policies and regulations issued by the government and

Flexibility. There was a noticeable difference in the responses from Oman. This could be due to a possible bias in the sample as the majority of respondents in the Oman sample were well educated and 25% of them developers of e-government services (see Table VII.8).

Feature	Saudi	UK	Oman
Ease of use	96% (1)	92%(1)	98%(3)
Transparent (i.e. users are aware of how their privacy is preserved and when and by whom it is shared)	95%(2)	91%(2)	97%(4)
Meets security requirements of the provided service	94%(3)	87%(3)	100% (1)*
Flexibility (i.e. the system is flexible to respond to dynamic changes in expectations and needs)	91% (4)	74%(6)	94%(6)
Enforces relevant laws, policies and regulations issues by the government	87% (5)	85%(4)	100%(2)
Cost effective	86%(6)*	55%(8)	71%(9)
Comply with relevant international standards & guidelines	86%(7)	80%(5)	97%(5)
Consider the impact of social &cultural factors	77%(8)	57%(7)	86%(7)
Consider the impact of political factor	70%(9)	42%(9)	83%(8)

Table VII.8: Summary of responses for ranking the future system features.

VII.3.2.5 Analysis of effect of the independent variable Respondent's Category

The relationship of participants to e-government services was defined by four categories: User, Government Body Representative, Services' Provider and Developer of e-government services. Respondents were allowed to add a new category if they felt none of these categories described their relation to e-government services, but none were defined. The effect of the category of the respondent on their answers to the questions in the survey was analysed. In general, there were no significant differences in the opinions between types of respondent, except in questions Q13, Q15, Q18, Q20, Q24 and Q27. These differences were:

- Q13 (a) and Q13 (b) asked to what extent government agencies can share user's information with another agency or a third party, when the agency or third party was providing a service to the user (Q13 (a)), or is not providing a service to the user (Q13 (b)). The opinions of developers were almost equally divided between choosing "Share all users' information" (43%) and choosing "Share only relevant (needed) information to provide a service" (43%), while in the other categories the choice "Share only relevant (needed) information to provide a service" dominated. In Q13 (b)

when the agency or third party does not provide a service to the user, the responses varied - nearly half of the users (49%) chose “Should not share at all”, while the opinions in the other categories were divided between “Share only relevant (needed) information to provide a service” and “Share users' information in an unidentifiable form” (see Table VII.9).

	Users		Government		Services' providers		Developers	
Questions	**Q13 (a)**	**Q13 (b)**	**Q13 (a)**	**Q13 (b)**	**Q13 (a)**	**Q13 (b)**	**Q13 (a)**	**Q13 (b)**
Share all users' information	**13%**	**8%**	**17%**	8%	**0%**	**0%**	**43%**	0%
Share only relevant (needed) information	**54%**	**25%**	**50%**	**50%**	**50%**	**40%**	**43%**	**43%**
Share users' information in an unidentifiable form	**15%**	**17%**	17%	25%	20%	**40%**	0%	**43%**
Should not share at all	16%	49%	8%	17%	30%	20%	14%	14%
Share with User Consent	2%	1%	8%	0%	0%	0%	0%	0%

Table VII.9: Summary of responses to Q13 (a) and Q13 (b)

- Q15 was about the control users should have over their information and gave three options of Full Control, Limited Control and No Control. Developers were divided between giving the users Full Control (43%) and No Control (43%). Government body representatives were also divided between Full Control (50%) and Limited Control (50%) while Limited Control was favoured by Services’ providers (60%) and surprisingly 53% of Users chose Limited Control while 43% chose Full Control.
- With regard to how the levels of control can be defined (Q18), only the developers’ category had a high percentage of disagreement (43%) with the statement in Q18.
- Q20 was about involvement in defining the ownership rights of information when using e-government services. More than one option could be chosen from -“Government”, “Users”, “Services’ Providers”, “Developers” and “By an agreement from the discussion between all involved parties”. The responses had a variety of combinations of these options. However, respondents from the categories of government, services’ providers and developers favoured the government only option, while the users category favoured the

combination of government and users (19%) and the option of “by an agreement between all involved parties” (18%).

- Q24 showed that apart from developers where 57% chose an independent party, the view was that the process of preserving privacy should be monitored and assessed by a government body representative.
- There were noticeable differences between the responses from all of the four categories when asked to rank the listed nine features for a future system (Q27). The developers ranked all the features as highly important (100%), while the ranking of the features varied in the other three categories. Table VII.10 shows the ranking of the features by the percentage of total importance (a sum of the percentages choosing “Very Important” and “Important”). When the percentages are the same the feature with higher percentage of “Very Important” is ranked higher and marked by an asterisk (*).

Feature	User	Services’ Provider	Government Body Representative	Developer
Ease of use	90% (3)	80%(7)	100% (1*)	100%
Transparent	93% (2)	90%(4)	100%(3)	100%
Meets security requirements of the provided service	94% (1)	100%(1)	92% (4*)	100%
Enforces relevant laws, policies and regulations issues by the government	89%(4*)	90%(3)	75% (9)	100%
Comply with relevant international standards & guidelines	86% (6)	90%(5)	100 % (2)	100%
Flexibility	89% (5)	90%(2*)	92% (5)	100%
Consider the impact of social & cultural factors	74%(8)	60%(8*)	91% (6)	100%
Cost effective	77%(7)	80%(6*)	83% (8)	100%
Consider the impact of political factor	65%(9)	60(9)	84% (7)	100%

Table VII.10: Summary of future system’s features ranking

VII.4 CMRPP Evaluation

Agreement on the statements mentioned in questions 11, 16, 18, 21, and 23 were examined, where the total percentage of agreement is the sum of the

percentages of respondents choosing “Strongly Agree” or “Agree” and the total percentage of the disagreement is the sum of “Strongly Disagree” or “Disagree” responses. Table VII.11 presents a summary of responses to these questions. The results in the table shows that there is a high percentage of agreement on the statements which mean that the statements in the relevant RDs reflect the views of a wide range of people involved in e-government services from different countries.

Question in the Survey	**Relevant RD Part**	**Total Agreement**	**Total Disagreement**
Q11. Privacy can be preserved by enabling users to have control over their information ….	Transformation RD (T) “...to enable users to have control…”	87%	10%
Q16. Users can be enabled to have control over their information by allowing them to apply a desired level of control over the whole or part of their information throughout the processing of that information when using e-government services.	T Core Transformation RD (W) “…by assigning identified levels of control to information owned by users when manipulated by service providers….”	87%	8%
Q18. The levels of control for enforcing the protection of users’ information can be defined by grouping selected sets of security rules into levels of control based on the level of risk identified on users’ information…..	S2 Supporting System RD (W) “…, by categorising an appropriately selected set of controls and rules into levels …”	86%	6%
Q21. Ownership rights can be defined by identifying who own each piece of information collected about the user and specifying what can the owner do with that piece of information	S1: Supporting System RD (W) “…,by identifying types of users’ information manipulated by a service provider and ….”	84%	7%
Q23. The government should identify and enforce requirements for preserving privacy and require all e-government service providers to satisfy those requirements to ensure that users are enabled to have control over owned information when using e-government services.	PMC RD “…to ensure that within the provision of e-government services, appropriate controls are applied … by placing relevant provision requirements on service providers and monitoring the system activities ….”	93%	4%

Table VII.11: Summary of responses on questions relevant to RDs

In Question 25 the respondent selected from three options the most appropriate way in their opinion to achieve the enforcement of applying relevant privacy regulations, policies and laws. The options were:

- By monitoring the application of relevant privacy regulations, policies and laws by all involved parties in e-government services provision.
- By empowering relevant authorities to respond to any violation of relevant privacy laws by applying suitable stated penalties.
- By educating and raising the public awareness about privacy regulations, policies and laws.
- No Opinion

This relates to the (W) in RD7 Linking System RD (L3) (see section V.3.1.1). The respondents could choose more than one option or choose the "No Opinion" option. Table VII.12 is a summary of the responses sorted according to the highest percentages. (These are accumulative as the respondents could choose more than one option).

Selected Option(s) in Q(25)	Percentage
By monitoring and education	**36%**
All the three options	**26%**
By monitoring the application of relevant privacy regulations, policies and laws by all involved parties in e-government services provision.	**23%**
By empowering relevant authorities to respond to any violation of relevant privacy laws by applying suitable stated penalties.	10%
By monitoring and empowering	8%
By educating and raising the public awareness about privacy regulations, policies and laws.	8%
By empowering and education	5%
No Opinion	10%

Table VII.12: Summary of responses to Q25

The most popular options are monitoring combined with education (36%) and applying the three approaches (26%). However, monitoring as the only approach was still popular (23%) and came third. The results did differ slightly between the three countries (see sectionVII.3.2.4).

In Q (27) the respondents ranked a set of features that should be in a future system to preserve privacy in e-government. This question relates to the (W) in RD6- Linking System (L2) (section V.3.1.1). These features are ranked by their importance to the respondents in descending order from the highest to lowest

importance. The total important percentage is the sum of “Very Important” and “Important” percentages. Table VII.13 shows the ranking of the features by all respondents, where the percentages are the same the feature with higher percentage in “Very Important” is ranked higher and asterisked (*).

Feature	Rank	Percentage
Ease of use	1	95%
Transparent (i.e. users are aware of the way their privacy is preserved and when and by whom their information is shared)	2*	94%
Meets security requirements of the provided service	3	94%*
Flexibility (i.e. the system is flexible enough to respond to dynamic changes in stakeholders’ expectations and needs)	4	89%
Enforces relevant laws, policies and regulations issues by the government	5	88%
Comply with relevant international standards & guidelines	6	86%
Cost effective	7	78%
Consider the impact of social &cultural factors	8	75%
Consider the impact of political factor	9	68%

Table VII.13: Ranking the importance system features by all respondents

There were slight differences in this ranking from one country to another (see sectionVII.3.2.4).

The” No Opinion” option was low for most of the questions. However, in Q18 (11%), Q21 (9%) and Q25 (10%) it was relatively high compared to the rest of questions. This might be due to the level of details in these questions about how the levels of control and the ownership rights can be defined and how to achieve the preservation of privacy in e-government.

VII.5 Hypotheses Testing

A list of hypotheses were given in the previous chapter, section VI.2.3. These have been tested by the survey data analysis, as follows:

- H1*: There is no significant difference between the views of women and men*. The null hypothesis was rejected as no significant difference was found between the views of women and men in any of the survey questions. The only difference which was not significant was that women tend to choose “Agree” instead of “Strongly Agree” where men will choose “Strongly Agree” (see section VII.3.2.1).
- H2: *There are differences in the views of respondents from different age groups.* This hypothesis could not be tested by the survey data results

due to limitation in the size of the sample of age groups (see section VII.3.2.2).

- H3*: There are no differences in the views of respondents from different countries with regard to the importance of preserving privacy when using e-government services*. According to the survey data analysis the null hypothesis was rejected as there was general agreement among respondents from all countries on the importance of preserving privacy when using e-government services. Results from the survey that supports this verification can be found in the EDA analysis (section VII.3.1.3).
- H4: *There are differences in the views of respondents from different countries towards the issues of sharing information between agencies*. According to the results of analysis in section VII.3.2.4 and Table VII.5 the null hypothesis was rejected as there were some differences in the views of respondents from different countries with regard to issues of sharing users' information.
- H5: *There is a difference in the views of respondents from different countries towards the issues of ownership rights*. The null hypothesis was rejected according to the results presented in section VII.3.2.4 where differences were found in the views of respondents from different countries towards ownership issues.
- H6*: There are differences in the views of respondents according to their categories towards the level of control that the users should be allowed.* The null hypothesis was rejected as the results in section VII.3.2.5 showed that there were some differences between the views of respondents from different categories.
- H7: *There is high agreement between respondents on the statements in questions related to the RDs of the CMRPP.* The total agreement from all respondents was calculated and the results in section VII.4 show there is a high agreement among respondents on the responses to questions that were related to the statements in the RDs of the CMRPP.
- H8*: Preserving privacy in e-government services increases users' trust in using these services.* This hypothesis was tested by a direct question (Question 30) to respondents. The responses to this question presented

in section VII.3.1.3 and Figure VII.5 showed that respondents think that preserving privacy in e-government will increase users' trust in using e-government services. As a result the hypothesis was verified and the null hypothesis was rejected.

VII.6 Open Questions' Responses Analysis

There were five optional open questions in the survey Q19, Q22, Q26, Q28 and Q29 (b). The number of responses to these questions varied from 6 to 114. They were all analysed and categorised according to the aim of the responses and the meaning relevant to the question asked. Requirements mentioned on many occasions in different open questions and by different respondents from different countries have been highlighted in bold to emphasise their importance. Each comment is referenced by the question number and its number as listed in Appendix F.2

VII.6.1 Question 19

Q19:If you have other alternative suggestions for how the levels of control on users' information can be defined, please state it below:

The comments were mainly about **who** can be involved in defining the levels of control and **how** these levels of control can be defined. Users were seen as the most important party that should be involved in deciding on what is important and private for them and what is not and that the dynamic changes in their needs and desire should be considered (see Appendix F.2,(Q19:14),(Q19:16)). An agreement between government and users was mentioned with a need for experts to define the security and privacy requirements for a service and a consultation with services' providers to be accepted when needed. It was suggested that a legislative authority that represents the users should agree on the defined levels of control. Table VII.14 shows a summary of the feedback and comments to Q19, note all the comments references are in Appendix F.2.

Who should define the levels of Control	How the levels of control can be defined
Users Only[Q19:14,Q19:16]	Categorise government services and divide information according to what they need to be able to provide a service [Q19:8, 9].
By negotiating between users and the government only and services providers are consulted only when needed [Q19:5]	Consider meeting security requirements for the service [Q19:3].

Who should define the levels of Control	How the levels of control can be defined
Experts to define Security requirements from users[Q19:6]	Provide a way for monitoring the access to prevent corruption [Q19:7].
A legislative authority that represent the users and unbiased [Q19:1],[Q19:17]	Easy to access and to use [Q19:7].
Users Only[Q19:14,Q19:16]	The default settings should be set to a restricted level of control (High control). [Q19:2]
By negotiating between users and the government only and services providers are consulted only when needed [Q19:5]	Users should be educated to raise their level of privacy awareness [Q19:2].
Experts to define Security requirements from users[Q19:6]	**Users should be aware of the levels of control and their meanings before using the service[Q19:15]**

Table VII.14: Summary of feedback on Q19

The last requirement in bold "Users should be aware of the levels of control and their meanings before using the service**"** was mentioned several times in different open questions and by different respondents from different countries, this comment was covered in general by the model and can be considered as a possible enhancement for the proposed framework.

VII.6.2 Question 22

Q22:If you have other alternative suggestions for how ownership rights of information about users of e-government services can be defined, please state it below:

Feedback and comments on how the ownership rights should be defined:

- Only users should own information [Q22:3]
- Legal conditions should be applied on services providers in favour of the users[Q22:4,5]
- **Users should be aware about ownership rights and its meanings before using the service[Q22:6]**

VII.6.3 Question 26

Q26:If you have alternative suggestions for how privacy regulations, policies and laws can be enforced, please state it below:

Comments on this question were concerned with **who** should be responsible for enforcing the application of privacy laws, regulations and **how** it can be enforced. Table VII.15 show a summary of the feedback.

Who should enforce privacy regulation, policies and laws	How privacy regulations, policies and laws can be enforced
A third party for monitoring the compliance with privacy regulations and laws who has authority and is able to investigate and take action against people responsible for privacy violation [Q26:2]	By establishing mature privacy laws at a national level that protect users' rights of privacy in the country and comply with international privacy standards and guidelines [Q26:3, 4, 5, 9 and 12].
A high court administered by the government with a degree of independence, specialised in electronic privacy violation and with authority to enforce privacy laws and apply penalties [Q26:4, 10, 11 and 12].	By raising users' awareness of privacy by different means, an example is through TV adverts [Q26: 1, 6, and 9].
-	By making the user aware of privacy laws and regulations before using e-government services [Q26:13].
-	Government should initiate funded research in this area [Q26:7].

Table VII.15: Summary of feedback on Q26

VII.6.4 Question 28

Q28: Is there any other features that you think a system for preserving privacy in e-government context should have? If Yes, Please state it below:

The additional features mentioned are in summary:

- The system should inform the user in a simple plain language what, when and by whom his information are accessed, shared, modified or processed at any point [Q28:1, 2, 3, 9, and 12].
- **The user should be able to know before using a service what, when and by whom his information might be accessed or processed [Q28:2,3 and12]**
- Security & Privacy awareness: the system should provide facilities to raise users' awareness of the consequences of a compromise of their privacy [Q28:4 and 12]
- The system should only be run by one government authority that takes complete responsibility for monitoring the quality of the service and the application of the privacy laws [Q28:10 and11]
- Persistent[Q28:5]
- Stability and maintenance [Q28:6]
- A proper way to authenticate people using the system [Q28:5].

- A clear understanding of the differences in privacy requirements in different services [Q28: 7].

VII.6.5 Question 29 (b)

Q29(b): Please explain the reason for your answer in Q29(a) if it was Yes or No? Note: (Q29(a): Do you think implementing such a system to preserve privacy is viable?)

The answers were divided into advantages or success reasons in favour of the system and obstacles that might prevent implementing such a system. A summary of these advantages and obstacles is:

VII.6.5.1 Advantages

Advantages seen by respondents who think the framework is viable are:

- It will increase trust in the government and will encourage citizens to use e-government services [Q29 (b):5,6,9,17,20,22,56,83 and 84]
- It is very important and society needs it [Q29 (b):7,8,18,30,36,38,46, 57, 59,90,94, 95 and 102]
- It will improve communication between the government and /or government's agencies and citizens. Also it will encourage sharing opinions in policy and decision making [Q29 (b):17, 56, 83 and 84].
- It will increase productivity of government employees and citizens as it will save time and effort [Q29 (b):67].
- To prevent fraud and impersonation and related crimes [Q29 (b):96].

VII.6.5.2 Success Reasons

Reasons for the success of the implementation of the proposed framework identified by respondents who think the framework is viable are:

- The required technology is available[Q29 (b):1,42, 48, 78, 88, 91, 98, 109 and113]
- Can be achieved with people with good will especially the political will (from the government) [Q29 (b):1, 2, 3, 16, 29, 61, 39 and 75].
- The required resources are available(e.g. financial and intellectual resources [Q29 (b):16, 31, 34, 41, 45, 62, 65, 71, 77, 79, 82]
- It needs time and hard work[Q29 (b):6, 44, 67]

- The system needs to be reliable and secure[Q29 (b):14]
- All parties need to comply to privacy regulations and laws [Q29 (b):2
- If the system satisfies all the mentioned features [Q29 (b):10
- If there was an independent authority (ies) for issuing, monitoring, executing relevant privacy laws and regulations. [Q29 (b):10,23]
- By learning from international best practices and customising standards and guidelines in local context [Q29 (b):15,100]
- If it provides a way to define clear privacy requirements that include all the different cases that might occur when using e-government services and the requirements of all involved parties [Q29 (b):19, 21, and 80].
- Can be achieved if it has means to prevent corruption [Q29 (b):28, 83].
- Citizens have the right to have their privacy protected by the government [Q29 (b):33, 84, and 85,110,113].
- By raising privacy awareness between all involved parties in e-government services [Q29 (b):47, 50 and 93].
- With good planning and a pre-implementation study [Q29 (b):60, 99 and100].
- If the system has a facility to enforce privacy policies and laws [Q29 (b):63, 93 and 114].
- It will need support from experts and advice from industry in developing such a system [Q29 (b):70 and103].
- With collaboration between all involved parties [Q29 (b):74, 92 and114]
- It should consider a way of deleting users' information from all places if the user opts out of sharing his information [Q29 (b):104].

VII.6.5.3 Obstacles

Obstacles and possible reasons for a failure of the proposed framework identified by respondents who think the system is not viable are:

- People are the weakest link in this system and they can choose to disclose information that they might be able to access within their work. [Q29 (b):3 and12].
- Conflicts in interest of third parties when more information is needed to provide better tailored services which might lead to sharing identifiable user information [Q29 (b):105].

- Unwillingness from government whose bodies are unprepared to reduce control on users' information [Q29 (b):5, 24 and 26]
- It will cost a lot of money [Q29 (b):24 and 26].
- Lack of required knowledge and expertise [Q29 (b):26 and 52]
- Local culture and laws in the current form prevent the system being viable [Q29 (b):43 and 64].
- Weakness in planning [Q29 (b):86].
- There will always be opposition about any suggested privacy level and there will be suspicious about any change in the privacy policy [Q29 (b):106].
- It is difficult to get an agreement between all parties or to find one individual who can take the responsibility for making overall decision on privacy [Q29 (b):107].
- It is difficult to get all parties to "buy" into the system and enforcing it [Q29 (b):109].
- The system can be hacked, since it is on the internet [Q29 (b):87 and112].

VII.6.5.4 General Feedback

- The subject is really important and needs to be communicated to governments [General: 10 and 12].
- E-government is important and preserving privacy is very important to encourage users to trust the services [General: 8, 9 and14].

VII.7 Findings

There were several important findings from the survey analysis. One of the main findings was that there is strong evidence that support the validity of the developed CMRPP and the proposed framework for preserving privacy as the majority of respondents from all countries agreed on the developed RDs of CMRPP. Suggestions made by respondents in the relevant open questions were used to identify possible enhancements to the privacy framework (PRE_EGOV). These possible enhancements were considered in the enhanced PRE_EGOV framework presented in chapter eight. Another main finding is that although privacy was very important to almost all respondents who came from different backgrounds and countries, there was clear evidence of the effect of

social, cultural and political factors on the responses related to how privacy can be preserved when using e-government services and who is responsible for ensuring preservation of privacy of the users of e-government services. This effect was clear in responses from Saudi Arabia and Oman compared to responses from the UK. Saudi Arabia and Oman share similar social, cultural and political environments where as the UK differs greatly in these environments. For example, the effect of political factors was shown in the survey results as the government was most trusted in Saudi and Oman who share similar political systems while less trusted in the UK who have a different political system. This appeared clearly in the responses to Q24 as explained in section VII.3.2.4. This can be due to the nature of the political system as in Saudi and Oman they have been governed by the same political system for a long time where the citizens build stable and long term relationship with the government while in UK, the government might change with each new election. The responses to Q15 which covered the level of control the users should have on information when using e-government services differed. The UK responses favoured “Full control” whereas the Saudi and Oman responses favoured “Limited control”. This is due to cultural and social differences on understanding the rights of the user and the type of control he might have on his own information and again the trust in government that they should decide on what should happen appeared clearly in the Saudi and Omani responses with the opposite in UK responses. A possible explanation for this is the effect of current privacy awareness and relevant privacy laws. As in the UK, there is an established government department for monitoring issues of privacy[11] and there are established laws for data protection such as the Data Protection Act [106]. However, in Saudi and Oman, currently there is no established department for monitoring breaches of privacy and the relevant privacy laws either do not exist or are in their infancy. This conclusion was also supported by the answers of the respondents from all three countries to the relevant open questions. Some of the findings in this survey can be limited by the possible bias identified in the sample of some of the countries (Oman sample) and the sample size representation of some categories of stakeholders (UK sample). These possible limitations were discussed in section VII.3VII.3.2.

[11] Information Commissioner Office, available at: http://ico.org.uk/

VII.8 Suggested Enhancements to the Framework

The following enhancements suggested for the proposed framework have been extracted from the responses to the survey questions:

- A framework should consider users as the key party in deciding what is important and private to them in information about them; however, support from experts is needed to define security requirements.
- Levels of Control can be defined by a legislative authority that represents the users and is unbiased.
- The default should be set to a restricted level of control (High control).
- **Users should be aware of ownership rights and the levels of control and their meanings before using the service.**
- To support the framework, mature privacy laws should be established at a national level capable of protecting users' right to privacy in the country and comply with international privacy standards and guidelines.
- A high court administered by the government with a degree of independence, specialised in electronic privacy violation and having an authority to enforce privacy laws and apply penalties.
- By raising users' awareness of privacy and privacy regulations and laws by different means ,e.g. TV adverts
- **The user should be able to know before and while using a service in a simple plain language what, when and by whom his information might be accessed,** shared, modified or processed at any point
- The system should provide facilities to raise users' awareness of the consequences of a compromise of their privacy.
- The system should only be run by one government authority that takes complete responsibility for monitoring the quality of the service and the enforcement of relevant privacy regulations and laws.
- The system should consider how to delete a user's information from all places if the user opts out of sharing information.
- Should provide a way to understand and identify privacy requirements and consider the differences between services of all the different cases that might occur when using e-government services and the requirements of all involved parties.

While some of these enhancements are out of the scope of the proposed framework and rely on how governments manage their e-government services or on establishing relevant privacy laws and enforcing those laws, related enhancements to the proposed framework will be considered in the extended version of the framework presented in chapter eight.

VII.9 Conclusion

The survey's analysis results supported the defined RDs in CMRPP. In addition, further requirements for the suggested solution have been identified from the responses to the open questions and possible enhancements to the proposed framework for preserving privacy were identified from respondents' feedback.

Chapter Eight

VIII. Privacy REquirements in E-GOVernment Framework (PRE_EGOV)

VIII.1. Introduction

Existing privacy frameworks in e-government were mostly focused on performing guidance on how to assess the impact of privacy when providing e-government services and examples of these frameworks were discussed in section V.2.3. However, the gaps identified in section V.4.2 showed that there is a lack of a privacy framework that considers the ownership rights over users' information and the different aspects involved in the provision of e-government services. Thus, a novel framework for preserving privacy in e-government was proposed and presented briefly in section V.5. The Privacy REquirements in E-GOVernment (PRE_EGOV) framework is a general framework that can be applied to determine privacy and security requirements each time a new e-government service is introduced or to revise these requirements for an existing service. It aims to help e-government services providers achieve a balance between security requirements identified for the provision of the service and the privacy requirements identified for the protection of the privacy of the users of the service. The users of the service here can be data subjects whose personal data is processed by the service such as citizens or not the data subject such as the government employees who process the data to provide the service. The balance between these requirements is achieved by negotiating and agreeing the identified security and privacy requirements in the early stage of the service design with the involved stakeholders. The PRE_EGOV provides a scheme for achieving this balance while giving the user who is a data subject the ability to have control over personal information when he/she uses electronic government services. It also introduces a way to define and assign ownership rights over information about users (data subject users) when providing an e-government service. The subject of the data or information used to provide the service can have different levels of ownership rights over information about

him/her according to the agreement between involved parties. The development of the proposed framework was informed by the CM relevant to achieving authentication developed in section IV.3 and the CMRPP developed in section V.3.1. In addition, the framework considered enhancements identified in the results of the survey used to evaluate CMRPP and the initial proposed framework (section VII.8).

This chapter presents PRE_EGOV framework in details. Section two describes the framework in detail and justifies the activities, section 3 presents a summary of PRE_EGOV phases and activities while section four presents related work in the literature and the final section the conclusions.

VIII.2. PRE_EGOV Framework

The framework phases are described in terms of the main tasks in each phase and the activities in each task. The application of the framework should be integrated into the usual requirements elicitation process when developing e-government services so that the privacy requirements are considered from the very beginning, or used to enhance privacy preservation in existing e-government services.

VIII.2.1 Preliminary Phase:

This is a general and essential phase in the framework. In it, the identified stakeholders should establish an agreement on definitions of data classifications, ownership rights and the levels of control which will be used in the second phase to label pieces of information about the user and to identify the level of control a user can have on each piece of information. In addition, the stakeholders' expectations and needs with regard to privacy are gathered and possible conflicts are identified and resolved if possible. The phase involves iteration between the tasks until an agreement is reached over the definitions and possible conflicts are resolved.

The preliminary phase includes three main tasks:

VIII.2.1.1 Expectations and Needs Identification

The main activities in this task are:

a. Identifying the stakeholders including all parties involved in providing and using the service.

b. Determining the expectations and needs of stakeholders with respect to privacy and resolving possible conflicts that may arise in their expectations and needs while considering possible changes in those requirements.

c. Building consensus between stakeholders on definitions of relevant terms such as ease of use, transparency, flexibility, and the desired level of control over owned information.

In the following a detail discussion of these activities

1. Stakeholders' identification:

A stakeholder in an organisation is defined as "*any group or individual who can affect or is affected by the achievement of the organization's objective"* [124]. Stakeholders in e-government have been used to categorise e-government services, see [11], [71] and [8]. One of the most common categorisation of e-government services is: Government-to-Government (G2G), Government-to-Citizen (G2C) and Government-to-Business (G2B). Other efforts have discussed the benefits and limitations in applying stakeholder's theory [124] in e-government, see [125], [126], [18], [127]. Another approach to identifying stakeholders in e-government is according to their roles. An individual can have one or more roles in e-government and these roles can change due to changes in the circumstances surrounding that individual [18] and [19]. In this framework, stakeholders are identified according to their roles and the relevance of that role to preserving privacy when providing e-government services. The identified roles used in the framework covered most of the roles recognised in the literature in studies such as, [19], [21] and [8]. However, the first four roles are the most frequently recognised roles [19].

Stakeholders' roles are:

1. **Users of the service:** Users can be individuals or groups including citizens, non-citizens, visitors and businesses. This category of

stakeholders also includes users of different age, or gender and users with disabilities.

2. **Government body representatives:** This includes local governors, government officials who are involved in strategic planning, and decision and policy making.
3. **Electronic services providers:** This includes government agency (ies) representatives who provide e-government services. It also includes public administrators and government employees involved in processing and providing e-government service to users. They are considered as users of the back office systems of the services.
4. **Developers of e-government services**: This includes e-government service project managers and developers involved in designing and implementing the services.
5. **Independent Evaluator(s)**: This includes independent government agencies or third parties who monitor and evaluate the performance of e-government services.
6. **Government partners:** This includes third parties who partner with the government to provide e-government services such as a third party who manages e-payments by users on behalf of the government.

The above identified stakeholders list can be updated as new roles emerge with new services.

2. Stakeholders' expectations and needs:

This task involves three main steps:

1. ***Select a representative sample of identified stakeholders:*** To identify the expectations and needs of involved stakeholders, a representative sample of stakeholders covering the identified roles with consideration of the different perspectives that can exist between stakeholders. For example, stakeholders representing the role of a user of e-government services can include perspectives of different groups of users. These include users of different ages, users with disabilities, a guardian who acts on behalf of a user, visitors and business firms' employees, or owners using e-government services relevant to the business.
2. ***Identify the expectations and needs of relevant stakeholders****:* This task identifies privacy requirements by identifying stakeholders' privacy

preferences and needs with regard to an e-government service. The users' expectations and needs are the focus of this task, however other stakeholders' expectations and needs are also considered. There are different stakeholder-driven techniques for gathering these requirements, such as: questionnaires, interviews, story boards and scenarios, group workshops and mock up prototypes [128] and [45]. The elicitation of privacy requirements should be incorporated into the elicitation for the general (functional and non-functional requirements) of stakeholders when a new service is designed or as an additional step in the case of enhancing or updating existing services. The identified requirements are documented and classified into levels of priorities, e.g. high, medium, and low priority where requirements at the same level of priority are in the same level [128]. This classification is based on the degree of importance to stakeholders and the available resources for the system.

3. ***Review stakeholders' requirements and resolve possible conflicts****:* The documented requirements are reviewed by relevant stakeholders to ensure their accuracy and that the prioritisation is approved by stakeholders. This step can iterate with other steps to validate privacy requirements and resolve any conflicts identified between the requirements. Once the privacy requirements are collected and prioritized according to their importance to the stakeholders, possible conflicts are identified. These conflicts might occur within the identified stakeholders' requirements or with other functional requirements of the service [45]. The conflicts can be resolved by negotiating about the alternative options with relevant stakeholders while also considering the impact of environmental factors. These negotiations use several communication means and iterate until general agreement is reached. Table VIII.1 is an example of the form that can be used to document the requirements and identify possible conflicts. For more examples, see Appendix G.b which has the forms used in the evaluation case study described in the next chapter.

Service Description: Renew driving license…….
Stakeholders: User (citizen or resident), Driving agency, Public health partner …

Requirements	Stakeholder	Possible Conflict	Proposed Resolution	Comment
R1: health information needs to be private and not shared between services providers	User	Health information needed to provide a service(R2)	Only allow the sharing of needed health information to provide a service	Resolved by agreements between relevant stakeholders
R2: health information is needed to provide the service.	Service provider	Health information needs to be private(R1)	Only allow the sharing of needed health information to provide a service	Resolved by agreements between relevant stakeholders

Recommendation: Share only needed information in anonymous form….

Table VIII.1: Example of a form for documenting and negotiating privacy requirements

3. Stakeholders' agreement on definitions:

In this task, general terms and definitions relevant to the service or the system in general are communicated to all stakeholders to ensure their understanding and agreement on those terms and definitions and their meaning in the context of the services. Examples of these definitions are the data classifications, the definitions of the ownership rights levels and the levels of control. Also, definitions of terms such as transparent, ease of use and flexibility.

VIII.2.1.2 Data Types Definition

The main activity is defining data types to be used in classifying data and information about users according to an agreed scheme. Although information is processed raw data for a certain purpose [45], in the context of this framework, the term data will refer to data about the user either as raw data or information. Data is usually classified with respect to the impact of disclosure on the subject of the data and on the organisation, and the level of protection needed to prevent the disclosure [129]. A common classification of data in the context of e-government services is restricted, private and public [8], [130], [129], [131]. However, data that is classified as private can have different degrees of sensitivity; therefore, the PRE_EGOV framework has four levels of data classification in the e-government context.

The types of classifications for data types in this framework are:

1. **Restricted Data:** Data is *Restricted* when unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to **the data owner.** The highest level of security measures should be applied to protect *Restricted* data.
2. **Sensitive Data:** Data is *Sensitive* when unauthorized disclosure, alteration or destruction of that data could result in a high level of risk to **the data owner**. A high level of security measures should be applied to protect *Sensitive* data.
3. **Private Data:** Data is *Private* when unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the data owner. A reasonable level of security measures should be applied to protect *Private* data.
4. **Public Data:** Data is *Public* when unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the data owner. While little or no security measures are required to protect the confidentiality of Public data, some measures are required to prevent unauthorized modification or destruction of *Public* data.

To classify data about the user which is processed in an e-government service into one of these data types, a risk assessment should be applied to the data along with identifying the users' expectations with regard to the level of sensitivity of the data. In this framework, the user should be enabled to change the data classification where appropriate and it is recommended that the default data classification is set to the highest sensitive level possible as long as this does not affect the functional requirements of the service or conflict with other stakeholder's requirements.

VIII.2.1.3 Ownership Rights Definition

The main activity is defining ownership rights for each piece of information about a user of a service. Historically, property ownership rights have been a subject of many philosophical theories and legal arguments [132],[133], [134]. The basic concepts of ownership concern the rights to use, control the use and remain in control of whatever is owned [134]. These ownership concepts are applicable to data and information with careful consideration of the fact that data and information might have many owners at the same time [134]. The ownership of data is a subject of conflict in the literature as some argue that the

original data provider is the owner while others argue that the data collector who collects and stores the data is the owner of the data. Many data protection acts and relevant standards were silent about the ownership issue [135].

In this framework, an ownership right to a piece of information is considered to show who owns a piece of information and what access rights the owner can have on that piece of information and for how long. The user perception of ownership of personal information was considered in the definitions along with different perceptions of relevant stakeholders. The concept of controlling who uses the piece of information is defined separately under the levels of control section to provide more flexibility to the framework. The types of ownership that can be assigned to a piece of information about a user are:

1. **Totally Owned:** The subject of the information is the owner who has all the access rights of creating, viewing, editing or deleting that information as long as the information exists.
2. **Partially Owned:** The subject of the information partially owns that information and can have some access rights of viewing and editing that information as long as the information exists. In this type of ownership, the data can be owned by different owners and access rights should be agreed by relevant stakeholders.
3. **Not Owned** The subject of the information does not own the information and the information is owned by the holder of the information (the government or any party authorised by the government), however, the subject of the information has the right to view the information at all times where appropriate.
4. **Official Use Only:** The data about the subject is owned by the government only and the subject of the information cannot view the data through normal access, however, the subject can ask to view the data by an official request to the government representative.

VIII.2.1.4 Levels of Control Definition:

The main activities are defining possible risks on users' owned information, identifying a set of appropriate rules and controls for mitigating possible risks, and categorizing identified rules and controls into levels of control according to an agreed scheme. In this context a Level of control is a set of rules for

controlling the access rights to the user‘s information in order to enforce the protection of the user’s privacy. These rules are determined after identifying possible risks on the user’s information. Risks to the privacy of user’s information commonly identified in the literature [109], [130], [129] are:

- Disclosure of identifiable information either intentionally or accidentally.
- Tracking a user’s behaviour on government sites or other sites.
- Profiling a user using data collected from visited sites.
- Unauthorised sharing of any part of user information between government agencies or third parties.

To mitigate these risks there are a range of general rules and controls that can be applied [109], [104], [113] such as:

- Encrypting users’ information that are confidential and highly identifiable and /or classified as restricted.
- The use of appropriate Privacy Enhancing Technologies (PET) when processing, communicating and transferring any personal identifiable information (PII) to prevent the tracking and profiling of user data or behaviour.
- Ensuring that information about a user is not shared without the user’s consent.
- Anonymising information about the user when sharing it with other parties.
- Enabling the user to know who sees personal information, when it is viewed, and what part is viewed.
- Informing the user of any event of disclosure.
- Collecting only information needed to provide a service.
- Limiting the storage time of users information after the use of the service
- Limit access to a user’s information only to people involved in providing the service.

However, from the user perspective and since this framework is about enabling the user to have control over personal information, the focus will be on what level of control a user can have to allow or prevent access to personal data.

The framework proposes the following levels of control that can be assigned to a piece of information about a user:

1. **Full Control:** The user is given the right to allow or prevent any access to a piece of information.
2. **Partial Control:** The user is given the right to allow or prevent some access rights to a piece of information.
3. **No Control:** The user does not have any right to allow or prevent access to a piece of information.

The access rights in these definitions are to be specified after applying a risk assessment and identifying a set of rules and controls for mitigating identified possible risks on the user's information which will be detailed in the second phase of requirements elicitation.

VIII.2.1.5 Data Types Mapping

The process of assigning an appropriate ownership right and level of control to a piece of information is related to the data type assigned to that piece of information along with the previous risks identified and the impact of that risk on the user. These tasks are illustrated in the Requirements Elicitation phase, however, a general guide for mapping identified data types to the appropriate ownership right and level of control are presented here based on the definitions presented in this phase. For example, a piece of information that has been classified as restricted data which the user considers as very sensitive should be assigned a Totally Owned ownership right, where the user has total ownership and all the access rights to that piece of information. Also, the piece of information should be assigned Full Control level, where the user has full control to allow or prevent access rights to that piece of information. A guide to mapping data types according to the most appropriate ownership right and level of control combination is presented in Table VIII.2.

Ownership right \ Level of Control	Totally Owned	Partially Owned	Not Owned
Full Control	Restricted/ Sensitive/ Private	Sensitive/ Private	N/A
Partial Control	Sensitive/ Private	Private	Private
No Control	N/A	Private	Public/Official Use Only

Table VIII.2: A guide for data types mapping

The following points should be considered when assigning ownership rights and levels of control to data types:

- Information about a user is analysed and classified into data types according to the results of the risk assessment and the identified security and privacy requirements. Each type of information is assigned an appropriate ownership right and level of control based on the identified security and privacy requirements.
- Any piece of information which is classified as restricted should be fully owned and fully controlled by the subject of that information. This type of information is very sensitive to the user and any access right to that piece of information must be granted by the user and the user must have full access rights to that piece of information.
- Any piece of information which is classified as sensitive should have at least a Totally Owned ownership right and/ or a Full Control level of control assigned to it.
- Any piece of information which is classified as private should have at least a Partially Owned ownership right or higher and/or a Partial Control level of control or higher level assigned to it.
- Data about a user that is classified as public can be assigned a Partially Owned ownership right and/or a Partial Control level of control.
- When the data classification is assigned as Partially Owned and / or Partial Controlled, possible conflict in the interests of multiple owners to that data should be considered and the access rights given to each owner should be agreed based on the identified privacy and security requirements.
- Users should be able to view ownership rights and levels of control assigned to data about them at any time.

VIII.2.1.6 Privacy Framework and Authentication Level of Assurance (LoA)

There are three levels of assurance (LoA) recognised by most of the authentication frameworks in e-government. These levels are low, medium and high (see section IV.2). LoA are used to control access to sensitive data and services and a risk assessment should be applied before assigning those levels. In PRE_EGOV, the LoA by OECD [86] are adopted. These levels are

used in controlling access to the settings of data types of user's information and the ownership rights and levels of control assigned to each data type. For example, if a user wants to view the ownership rights and levels of controls assigned to data types of his/her personal information, a low level of assurance will be required, while if the action involves changing the settings of the data type assigned to a piece of information and changing access rights to that information a higher authentication level of assurance (LoA) will be required. The LoA recommended are based on the impact of the action on the disclosure of the user's information. Table VIII.3 summarises recommended LoA for actions done by the user on the privacy settings over personal information.

Action	Recommended LoA	Example
View privacy settings on user's information	Low LoA (Level1)	View the data types settings, ownership rights and levels of control assigned to user's information
Change privacy settings to higher level	Low-Moderate LoA (Level1-Level2)	Change the settings assigned to a piece of information from data type *private* to *sensitive)*.
Change privacy settings to lower level	Moderate-High LoA (Level2-Level3)	Change the settings assigned to a piece of information about the user form data type *private* to *public*.

Table VIII.3: Recommended LoA for actions on privacy settings

VIII.2.1.7 Preliminary Phase deliverables:

The main deliverables of this phase are an agreed set of definitions of the ownership rights of information that are subject to manipulation by e-government service providers, a set of definitions of levels of controls that enable the user to have control of their information and stakeholders requirements and preferences with regard to preserving privacy in the context of providing an e-government service. This phase should be reviewed at different times while applying the framework to check for any changes in expectations and needs and to validate the identified requirements of privacy and design preferences.

VIII.2.2 Requirements Elicitation Phase

This is the second phase in the framework where the privacy and security requirements are identified. The phase consists of four main tasks. Each task involves activities that describe how the task can be performed.

VIII.2.2.1 Data Types Identification

The activities in this task are:

- Analysing the data and information needed by processes when providing the e-government service, then determining data and information about the user that are needed to provide the service.
- Identify users' and relevant stakeholders' preferences with regard to ownership over identified data and information about the user (from the task of the expectations and needs management in the preliminary phase). The ownership rights definitions can be found in section VIII.2.1.3.
- Assign appropriate data types to each piece of information about users that will be processed when providing the service. Examples of data types defined in section VIII.2.1.2.

The data classifications identified in this task revised and updated after identifying privacy and security requirements in the next task.

VIII.2.2.2 Privacy and Security Requirements Elicitation

In this task the privacy and security requirements are determined based on the identified expectations and needs of the users and relevant stakeholders and the identified ownership rights and data types in the previous task in conjunction with performing a risk analysis to determine the privacy and security requirements. The activities in this task are:

- Performing a risk analysis by identifying potential threats to the information and determining possible impacts from these threats. Identifying risks and possible rules and controls for mitigating these risks. In this step, a risk assessment method of the government or authorised partner choice can be used while considering identified ownership rights and data types and user preferences with regard to how to preserve their privacy.
- Consider relevant regulations, policies and laws when identifying privacy and security requirements.
- Identify privacy requirements based on the results of risk assessment.
- Identify security requirements of the provided service by analysing the information needed to provide the service and considering the identified ownership rights and privacy requirements. The selected security requirements elicitation method should satisfy an elicitation of

requirements that can be measured, tested and used as a basis for actions. In this step a goal oriented security requirements method is recommended, such as [136], [137] and [138]. The chosen requirements elicitation approach should consider the identified ownership rights and consider privacy as a soft goal.

VIII.2.2.3 Ownership rights and Levels of Controls Identification:

This involves identifying ownership rights and levels of control that can be assigned to information about the user. Activities involve:

- Identifying ownership rights over data types identified and assigned to pieces of a user's information and assigning predefined (in the preliminary phase) ownership rights to each identified type of information about users.
- Determining the users desired level of control over pieces of owned information.
- Considering the expectations and needs of involved parties.
- Determine and consider identified risks on users' information.
- Consider the identified privacy and security requirements in the previous task.
- Identify appropriate levels of control over users' owned information.

VIII.2.2.4 Ownership Rights and Levels of Controls Assignment:

The main activity is to assign identified ownership rights and levels of control to each type of user owned information while considering the identified privacy and security requirements. The ownership rights and levels of control are assigned to each data type using Table VIII.2 as a guide to which ownership right or level of control can be assigned.

VIII.2.2.5 Requirements Elicitation Phase deliverables:

The main deliverables are the identification and assignment of data types, ownership rights and levels of control to each type of information about the user that is needed by an e-government service. The results of the assignment should be verified against the identified expectations and needs of relevant stakeholders in the preliminary phase. It is important to say that the access rights (e.g. read, write, delete) to the information processed to provide a service

will be determined according to the identified security and privacy requirements and assigned to the information and the data subject who is using the information will have a level of control over these access rights according to the ownership rights and the level of control assigned to him/her over that piece of information. These should not contradict with access rights assigned according to the identified security and privacy requirements.

VIII.2.3 Design Phase

This phase involves presenting the rules and controls in a way that enables the user to apply the assigned levels of control to owned information while using the e-government service.

VIII.2.3.1 Rules and Controls Presentation:

The activities in this task identify the design requirements for presenting the levels of control. The activities are:

- Identify the expectations and needs of relevant stakeholders with regard to how to present the levels of control over user owned information.
- Identify and consider the diversity of user capabilities when presenting the levels of control.
- Consider the stakeholders' desired features and their priorities, when presenting the levels of control such as, ease of use, transparency and flexibility.
- Identify possible features and design requirements relevant to the enforcement of relevant privacy regulations, policies and laws.
- Identify appropriate technologies, especially Privacy Enhancing Technologies (PET) and security mechanisms that can be utilised to satisfy the identified privacy and security requirements.

VIII.2.3.2 Rules and Controls Deployment:

The activities in this task utilize available technology solutions to deploy the assigned ownership rights and levels of control and to enforce relevant rules and controls when presenting the assigned levels of control. The activities are:

- Consider identified design requirements.

- Consider maintaining the deployment of the ownership rights and levels of controls over a piece of user's information throughout the manipulation of that piece of information when using e-government services.
- Utilize appropriate identified technologies to implement the ownership rights and levels of control according to identified privacy and security requirements.
- Develop a prototype of a tool to enable users to set their privacy preferences over information about them.
- Assess the deployment of ownership rights and levels of control according to the expectations and needs of relevant stakeholders using the developed prototype.
- Implement the ownership rights and levels of control and incorporate the implementation as part of the provided service or as a separate tool as appropriate.

An example of the deployment of the ownership rights and levels of control can be presented as shown in Figure VIII.1.

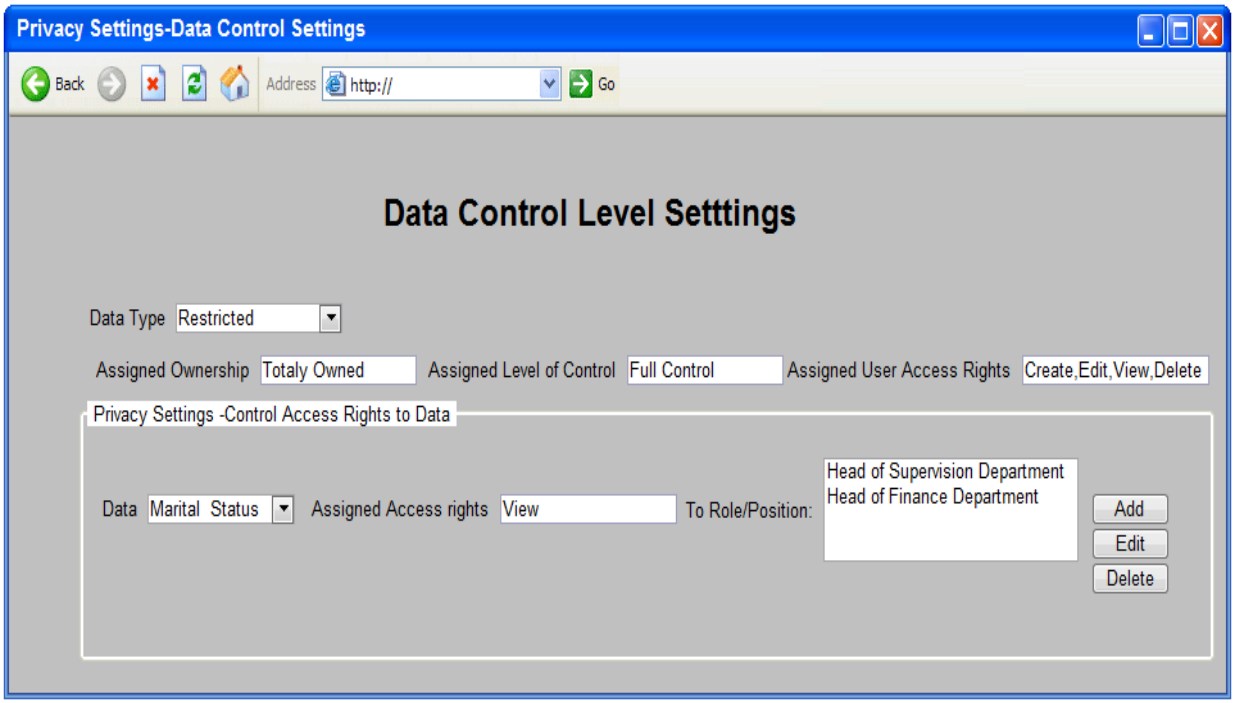


Figure VIII.1: Example of deploying ownership rights and levels of control.

Each piece of information about the user is assigned a data type and each data type is assigned appropriate ownership rights and levels of control according to the identified privacy and security requirements identified and agreed in the Requirements Elicitation Phase. According to the ownership rights and levels of control given over a piece of information, users are enabled to change the settings of the data type of a piece of information as they prefer and to set access rights to that piece of information. There should be a log of all activities performed on any piece of information and the design should consider exceptional emergency cases where employees with senior roles can be given the right to override any privacy settings. The user should be notified about these actions. A complete example of a real world case study is presented in chapter nine.

VIII.2.3.3 Design Elicitation Phase deliverables

One of the main deliverable of this phase is the prototype of a design tool for preserving privacy when using e-government services. The tool is used by the user to set the privacy preferences according to assigned ownership rights and levels of control to each data type. The prototype can be used to assess whether the identified requirements are met and to ensure that the design solution satisfies the expectations and needs of relevant stakeholders. However, the actual implementation of the tool involves the use of appropriate technologies to satisfy the identified security and privacy requirements. Also, it incorporates the implementation of these technologies when developing e-government services.

VIII.2.4 Environmental Factors Influence Management

The influences of environmental factors i.e. political, social and cultural factors is considered by identifying possible impacts of those factors using a set of questions asked during the application of each phase of the framework. Then, deciding how to consider the impact of those factors on the framework activities. The following set of questions are based on a review of several studies discussing the relations and impact of political, cultural and social factors on using electronic services [139], [140], [141], [142] and [143].

VIII.2.4.1 Political Impact Questions

- How the system considers the impact of government stability on the application of the framework?
- How the impact of the government willingness to preserve privacy is considered when applying the framework? What are the possible impacts on framework activities?
- To what extent the government is willing to be open to relevant stakeholders' participation when applying the framework? What are the possible impacts on the framework activities?

VIII.2.4.2 Social Impact Questions

- Does the system consider the impact of differences in users' education level when identifying privacy requirements of the provided e-government service?
- Does the system consider the impact of differences in user's affordability to access the internet? Are privacy requirements considered in any alternatives provided to users with limited or no access to the internet?
- Does the system consider privacy requirements relevant to the use of the service by someone working on behalf of the user (e.g. guardian, carer, lawyer, etc.)?
- Does the system consider providing different access channels to the service? Are privacy requirements considered when using any of those access channels?

VIII.2.4.3 Cultural Impact Questions

- Does the system consider the possible impact of gender when identifying users' privacy expectations and needs? How the impact can be considered when applying the framework?
- Does the system consider the possible impact of society's common beliefs towards data protection and privacy? How the impact can be considered when applying the framework stages?
- Does the system consider the possible impact of the society culture towards new services and change of traditional ways of providing them?

How this impact should be considered when identifying privacy requirements for the service?

- Does the system consider the impact of user's trust in government and e-government services providers when applying the framework?

VIII.2.5 Regulations, Laws and Policies Compliance Management

Relevant privacy policies, regulations and laws have to be identified and considered throughout the framework phases. For example, in the preliminary phase the definition of ownership rights and level of controls should comply with relevant local regulations and laws and international laws that the government is complying with. In addition, in the requirements elicitation and the design phases there should be consideration of any requirements to provide evidence of compliance with relevant privacy regulations or evidence of any violation of these regulations and laws.

VIII.2.6 Privacy Awareness

The framework recognizes the importance of raising privacy awareness and incorporates it within all phases especially in the requirement elicitation and design phases.

In the tools used, appropriate awareness messages are displayed to both the user and the employee, processing the request on behalf of the service provider to illustrate the meaning of selected actions when setting privacy preferences on owned information. In addition, there are awareness messages to explain in simple language the meaning of the current settings and of the assigned ownership rights and levels of control over pieces of user owned information. Training on the use of the tool can be presented in an accessible way to all users, such as a brief online video on the government e-services site.

In addition, activities in this supporting element of the framework include identifying areas needing privacy awareness and the design and implementation of privacy awareness programs and workshops to raise awareness about relevant privacy policies, regulations and laws and to consider best practices in raising privacy awareness between relevant stakeholders. The privacy awareness programs and workshops will provide training for relevant

stakeholders such as government employees and users by explaining privacy rights and relevant regulations and relate it to the provision of e-government services.

VIII.2.7 Other Important Aspects

Other supporting systems are needed for the completeness of the application of the proposed PRE_EGOV framework. These systems are within the government structure and can be mapped to government departments and agencies. These supporting systems are: a system to enforce relevant privacy regulation policies and laws (this could be a legislation body and/ or an independent high court); a human resources system that ensures recruitment and allocation of staff with appropriate skills and capabilities to apply the framework and provide training programs for staff; Knowledge assembly and technology management systems that gather knowledge of best practices, relevant standards, guidelines and the latest technologies to preserve privacy as guided by the framework. Another important supporting system is a monitoring and assessment system that applies local and overall assessment to ensure that the performance of the framework activities satisfies the expectations and needs of the government and its customers.

VIII.3. PRE_EGOV Framework Summary

PRE_EGOV framework provides an easy to follow set of steps which can be used each time a new service is provided or to enhance an existing service to satisfy new privacy requirements. The activities in the phases of the framework are summarised in Figure VIII.2.

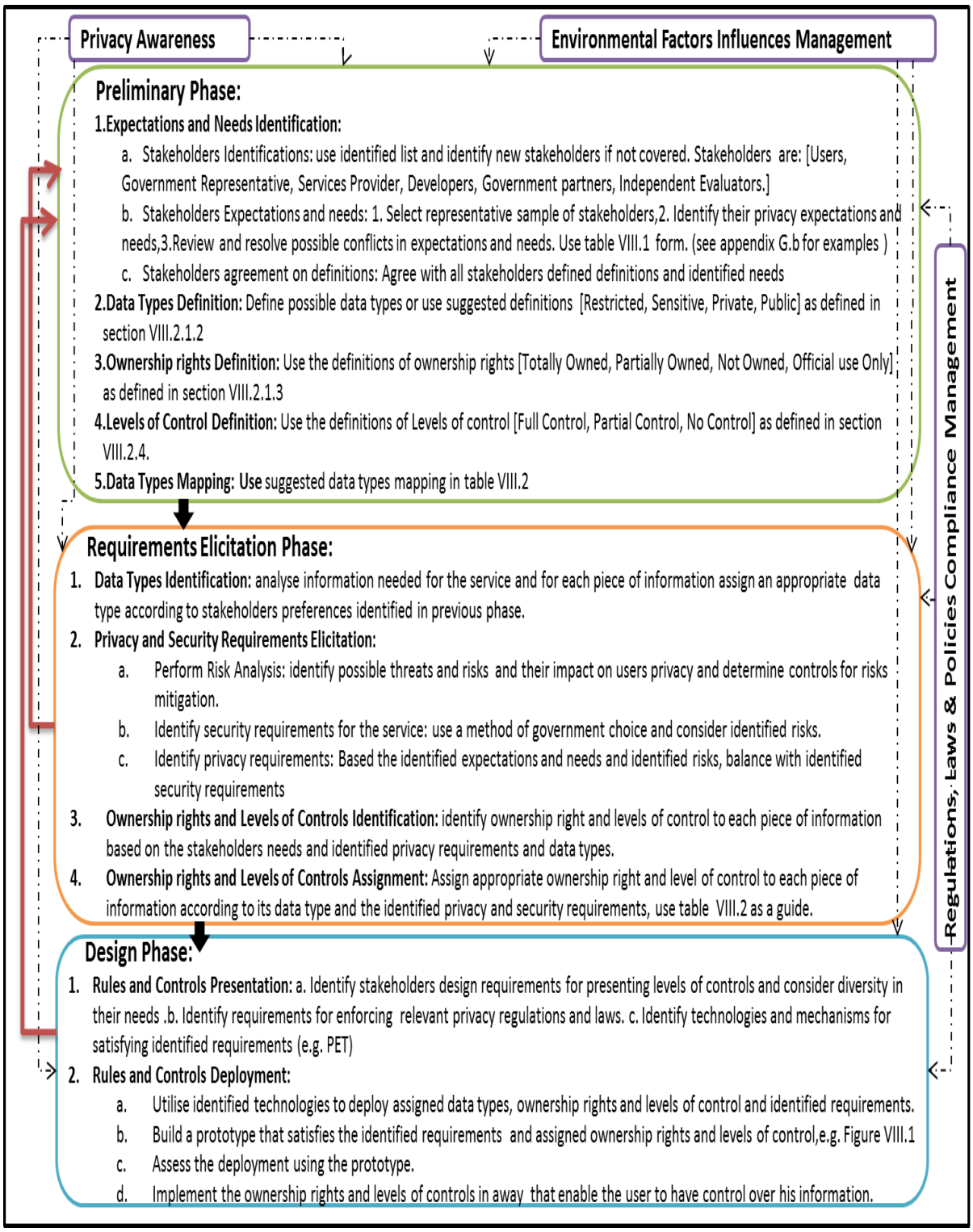


Figure VIII.2: PRE_EGOV framework phases summary

A summary of the activities in the supporting elements of PRE_EGOV framework is provided in Figure VIII.3

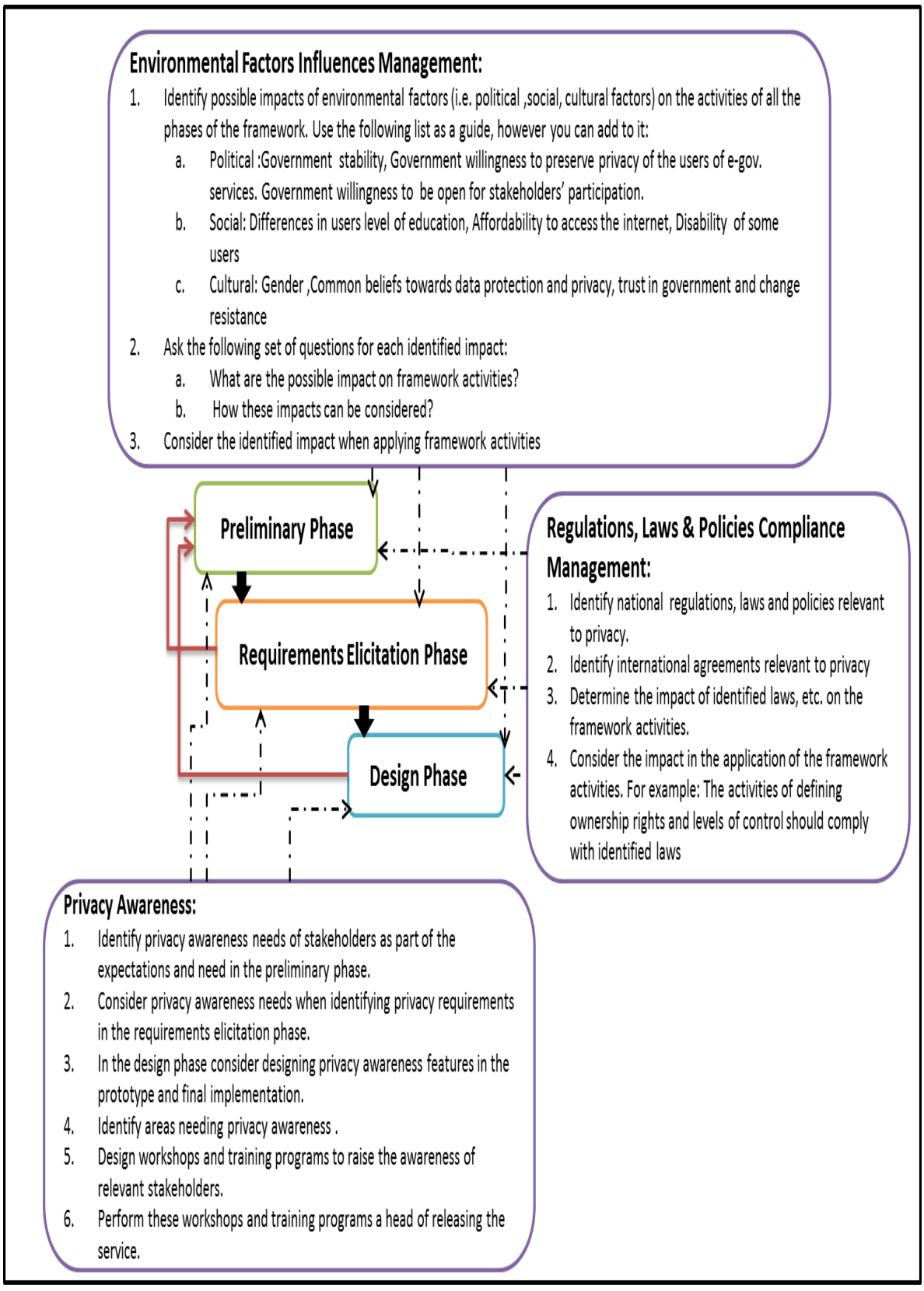


Figure VIII.3 PRE_EGOV supporting elements summary

PRE_EGOV provide a guide for implementing some of the activities, for example, a list of common stakeholders was identified and set of definitions for data types, ownership rights and levels of control. However, when applying the

framework, these definitions and lists can be altered to the need of the government according to its services and the needs of stakeholders.

VIII.4. Related work

Related work to the proposed framework for preserving privacy in e-government can be viewed from different aspects. First, the proposed framework PRE_EGOV complies with the recently published standard of privacy framework [113], although PRE_EGOV framework was developed before this framework was published [5] and the activities in PRE_EGOV cover most of the components of this privacy framework. Privacy frameworks that exist for e-government are most relevant to the proposed PRE_EGOV framework, however, these frameworks vary in the way they approach preserving privacy and the perspectives they represent. Some proposed privacy frameworks in e-government are based on analysing government development stages and identifying privacy implications at each stage such as [11] and [15] while other security frameworks focus on providing a framework to derive security requirements and privacy was considered briefly in these frameworks, such as [136], [13] and [144]. The framework proposed in the early days of e-government development by Wimmer and Bredow [15] provides a general approach for analysing security threats in e-government. Their framework investigates security threats and elicits security requirements using a comprehensive model of three dimensions, namely: 1) the electronic processing dimension which reflects the stage of development where the e-government service occurs; 2) the abstraction layer dimension which includes community, process, interaction, infrastructure and data and information aspects; and 3) the specific e-government domain dimension, where the model focus is on e-administration, e-voting, e-democracy and e-assistance. They suggest investigating security threats and requirements by going through each abstract layer and investigating the threats and possible security solutions from the perspective of this layer. This is done with a focus on the specific domain of e-government where the e-service is classified and the stage of development of the service. They referred to the consideration of social, cultural, political and legal impacts but gave no details on how to consider and identify these impacts when identifying security threats. Also, the community layer identifies relevant involved parties in the provision of the service and investigates security threats

from their viewpoint. However, the focus was more on government representatives and parties involved in providing the service rather than users. The citizen perspective was considered only in the process view, where the main participants in the process of the service provision and their relationships and dependencies are identified. Threats to privacy are not covered by this framework. On the other hand, the framework proposed by Belanger and Hiller [11] has provided a framework for e-government which helps identify the constraints that affect the implementation of an e-government service at each stage of e-government development and according to the categorisation of e-government types of services. They presented a brief example to illustrate how their framework can be used to study privacy implications when implementing an e-government service. The framework identifies global e-government constraints which are laws, regulations and policies, technical capabilities and user feasibility. These constraints were considered in the CMRPP development (section V.3), which informed the development of the PRE_EGOV framework.

From the aspect of requirements engineering, there are several frameworks proposed for requirements engineering, such as the work presented in [136] which is a goal-oriented requirements engineering framework. This framework is based on the *i** framework which is a modelling framework that focuses on the early stages of system design [145]. Their framework is a general requirement engineering framework that aims to support analysing systems affected by social factors and transform the organisation needs and goals into system requirements by adopting concepts of actors, goals and intentional dependencies. Security and privacy issues are considered as soft goals of the involved actors. Another similar work [13] proposed a methodological framework for analysing security and privacy requirements based on the concept of strategic social actors. This framework integrates three steps of security specific analysis into the requirements elicitation process within the *i** method. These are Actor identification, goal/task identification and dependency relationship identification. In this framework they provide a specific example of how to analyse security requirements using various analysis techniques: attacker analysis, dependency vulnerability analysis, counter measure analysis and access control analysis [13], and in this example, privacy is considered a soft goal and mentioned under the access control analysis. Another general

security requirement engineering framework in [144] defines security requirements, as constraints on the functions of the system having development. This framework's main activities include identifying functional requirements, appropriate security goals, security requirements and validation of the system context. There are other security requirement engineering methodologies that have been studied and applied in the context of e-government, such as Secure Tropos [146]. In 2004, a study by Kalloniatis et al [14] compared security requirements frameworks applied in e-government. It concluded that the studied methodologies do not cover all the required components for a requirements framework, and suggested that a combination of different methodologies can lead to a strong security requirements framework [14]. In a recent updated version of this study, the authors investigated the consideration of privacy in these methodologies [147] and concluded that only the secure *i** framework [138] and Secure Tropos [14], [146] have considered privacy goals as soft goals of the actors in their frameworks. Another comparison study by Fabian and et al [148] investigated a wider range of methods that included 18 security requirement methodologies and this study showed that KAOS [128], Secure Tropos [14], [146], Secure i* [138] and Tropos goal-risk FW [149] covered most of the comparison criteria in the study and in particular consideration of stakeholders views. These frameworks cover requirements elicitation in detail; however they do not consider the ownership right and they consider privacy from the perspective of the security goal of confidentiality. Although these frameworks may not relate directly to the proposed framework in this chapter, the activities and steps in these frameworks can be of use for analysing the security requirements of an e-government service.

There is other work in privacy taxonomy, such as the work of Barker et al. in [135], which proposed privacy taxonomy for data at the database level based on four dimensions. These were: 1) purpose of using the data; 2) visibility, refers to who is permitted to access or use the data; 3) granularity of the data; and 4) retention, refers to how long the data is stored. The authors argue that any system aiming to protect privacy should consider these dimensions [135]. The PRE_EGOV privacy framework covers these dimensions implicitly in its definitions of ownership rights and levels of control. However, PRE_EGOV

differs from the work in [135] since the aim of PRE_EGOV is not to provide a way to define and present the concept of privacy, but to provide a way to preserve privacy in an e-government context using a set of activities that need to be executed in order and iteratively at some stages. Also, the work in [135] considers the original provider of the data to be the owner and this owner is not always the subject of the data or the information while the PRE_EGOV framework considers different levels of ownership rights (see VIII.2.1.3) which are assigned to the information processed to provide the service based on the identified security and privacy requirements. Based on identified security and privacy requirements, the subject of the information can have full ownership, limited ownership or no ownership of the information. However, the user of the service can be a data subject of the information such as a citizen using the service or not a data subject who is using the services such as an employee who is processing the data to provide the service.

From a technical aspect, there are several frameworks which propose technical solutions to preserve security and privacy in an e-government context, such as [108], an agent based technical solution and [150], a framework for safe sharing of information between government agencies taking account of the user agreement. However, since the technical aspect is out of the scope of this research, these frameworks do not relate to the PRE_EGOV framework but can be regarded as possible technical solutions to satisfying the identified privacy requirements.

VIII.5. Conclusion

A novel framework for preserving privacy in e-government PRE_EGOV is presented. This framework's development was informed by CMRPP in chapter five and the results of the survey in chapter seven. Its main aim is to enable the user to have control over their information, so the privacy rules must reflect user expectations and needs while satisfying the security requirements of the service and considering the expectations and needs of other involved parties. There are many factors that have an impact on the effectiveness of using such a framework. A key factor in the successful implementation of this framework is the government willpower to protect users' privacy. This can be affected by international privacy agreements which a government is bound by, and the

political agenda and social environment. It also requires formulation and enforcement of privacy laws and regulations and the application of intensive privacy awareness programs to educate stakeholders, such as employees of government agencies providing e-government services and different types of users. The application of this framework can be lengthy especially at the preliminary stage when applied for the first time; however, once relevant definitions are established, knowledge gained can be reused in other services and the expectations and needs of stakeholders can be revised and updated.

Finally, this framework does not aim to provide a technical solution but rather a way to enable the user to have control over their privacy and to balance preserving privacy and satisfying security requirements in the context of e-government.

Chapter Nine

IX. Empirical Research: EduPortal[12] Services

IX.1. Introduction

The application of the PRE_EGOV framework described in chapter eight is part of its validation. To evaluate its usability, first the framework needs to be applied to different case studies from countries with differences in the social, cultural and political environment to demonstrate its applicability and generality. Then after the application of the framework, the usefulness of the framework can be evaluated using a set of semi-structured interviews with relevant stakeholders to determine the usefulness and acceptance of the framework from different perspectives. Therefore, the initial evaluation plan was to apply the PRE_EGOV framework on selected e-government services in three selected countries. These selected countries have established e-government services. In addition, two of these countries have similar political, cultural and social environments while the other one differs greatly in term of these environments. Also the researcher has contacts in these countries which enabled direct communication between the researcher who is applying the framework and relevant stakeholders. However, over a long period of this research several requests have been made to obtain an agreement on applying PRE_EGOV framework on services provided by different government agencies in those countries but these requests were denied and the main concern expressed by these government agencies is that the process will lead them to reveal sensitive information about how information about users is processed when providing their e-government services. This was a serious obstacle which delayed the evaluation phase until finally one government agency agreed to cooperate and the framework was applied on one of the e-services provided by this

[12] The government organisation's name is changed and all contact information and personal identification information are omitted due to the sensitivity of the collected data and the participation restrictions placed by the organisation.

government agency. This could limit the evaluation of the generality of the framework.

This chapter presents details of the application of PRE_EGOV on the selected case study, while chapter ten provides details of the usefulness evaluation based on the framework's application. An overview of the case study is presented in section 2, while details of the application of the framework provided in section 3.

IX.2. EduPortal Services: An Overview

EduPortal Services is an e-government portal which provides all the services that a sponsored student from country B might need in interaction with the government when he/she is studying abroad. The services of EduPortal vary from a simple download of official forms and applications to the submission of financial payment requests and scholarship extensions. The services are used by thousands of students from Country B studying abroad in many countries around the world. All EduPortal services are provided online and some services require the sharing of the students' data between different government agencies. Thus, the EduPortal services were selected for the evaluation of the proposed framework as it provides a suitable range of services.

IX.2.1 EduPortal Services

EduPortal Services is a student portal which provides all the services that a sponsored student from country B might need to perform when he/she is studying abroad. Country B sends a large number of students to various universities around the world to study. Programs of study include various types from short diplomas to PhD degrees and post-doctoral programs. The EduPortal website is the main contact between the students and their sponsors and provides various services. However, most of the services are for students who are sponsored by government B's sponsors, such as Higher Education (HE) ministry, different government agencies, universities supported by the government or commercial companies. To access the services a student is required to log in at the EduPortal website using an assigned id number and a pre-set password (given at registration when the students' file is opened). The

student can change the password through the portal services. The services cover a wide range of student needs - covering general services, educational services, financial services and services related to updating the student record information. Figure IX.1 shows the main categories of services provided by the EduPortal website with example services under each category. The services highlighted in red in Figure IX.1 are the services used in this case study.

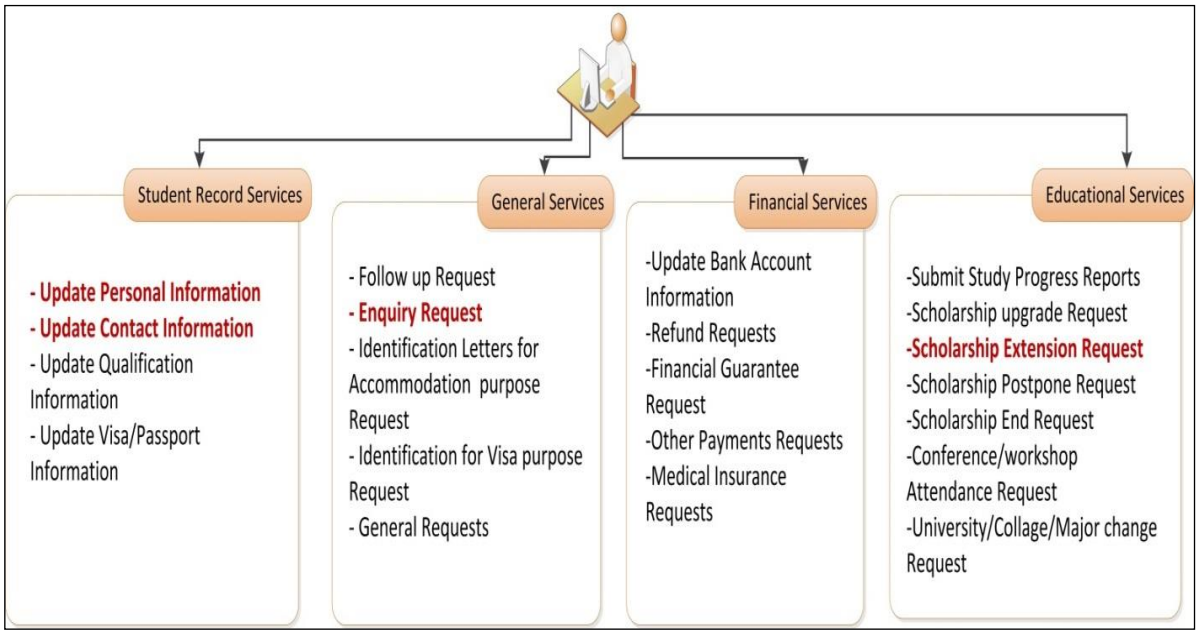


Figure IX.1: EduPortal Services categories

IX.2.2 General work flow

Based on a first round of interviews with relevant stakeholders in the EduPortal Services case study, the general workflow of a service in the current system is shown in Figure IX.2.

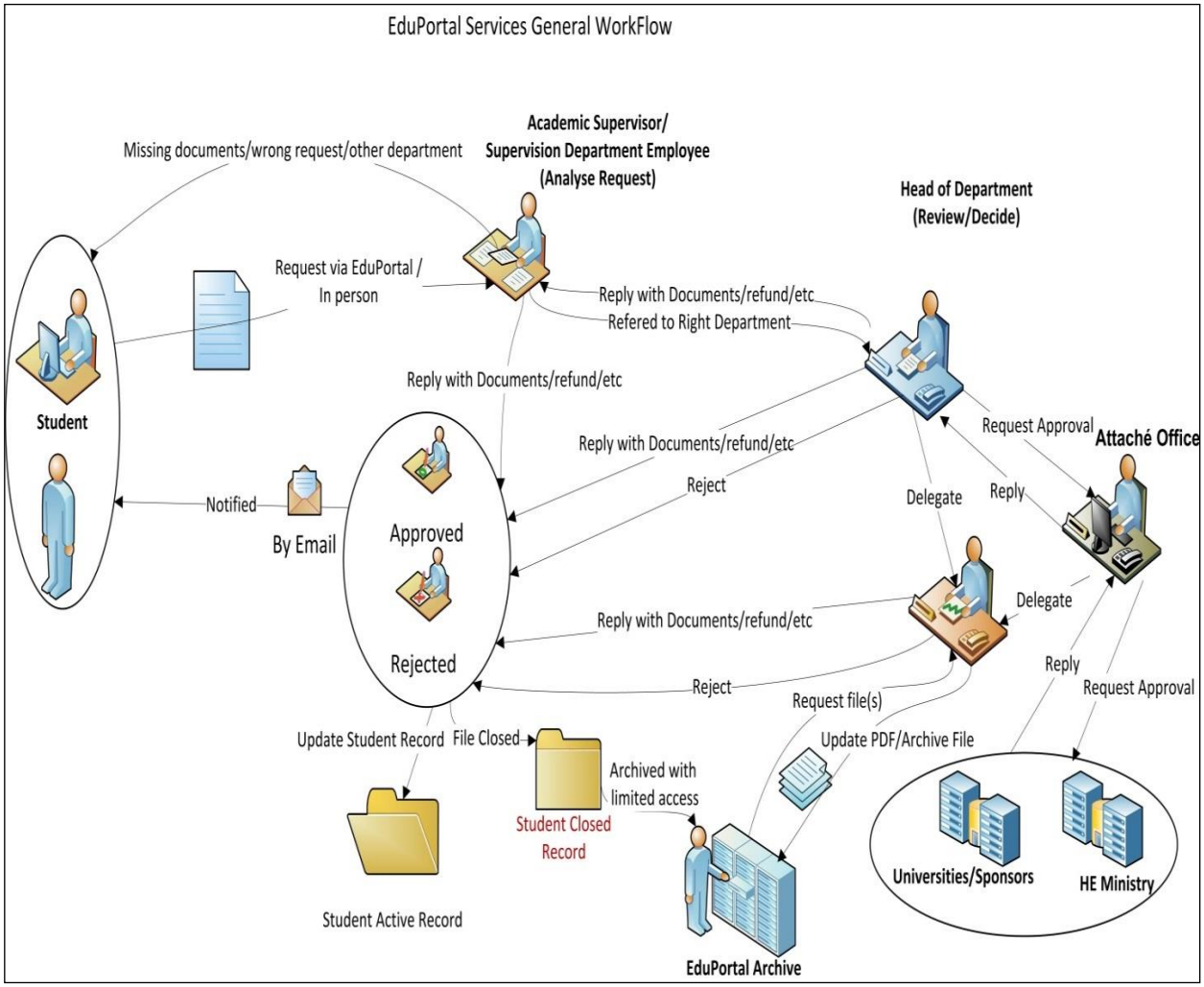


Figure IX.2: A general workflow for a service in EduPortal

A summary of the workflow according to the role of each actor in the system is:

- **Student:**
  - To request any service, the student should first log into the EduPortal website using identity number and password. If authentication is successful, the main page of the student account will appear with all the provided services.
  - The student selects the required service, fills in any required information related to the service and provides (upload) any documents that are required by the service. The student submits a request. However, in some cases the student can come in person to the government offices in the foreign country and ask for a specific service or call by phone (in emergency cases) and the service will be initiated by an employee in the government office at the portal but with a note attached to it that indicates how and by whom the request was initiated.

- **Employee in supervision department (role):**
  - Most requests from students go directly to the relevant supervision department where any employee in the department can work on the request. For example, there is an undergraduate department for students sponsored by the HE ministry studying for a bachelor degree and a postgraduate department for students sponsored by the HE ministry studying for a postgraduate degree (master or PhD). Employees in the undergraduate department can only process and respond to requests made by students from the undergraduate department.
  - When a student makes a request, if the request is not a direct request to the attaché office or to other departments such as (financial requests, travel tickets requests, legal advice requests) then an employee in the students' supervision department will deal with the request. The employee will look at the request, the completeness of the information related to the request and the provision of the required documents if any is required.
  - If there is missing information, the request is returned to the student asking for the missing information. If the request is not appropriate to the service, the request is returned to the student as rejected and the student is advised to submit the correct request for the service.
  - If the information in the request is complete and the request appropriate for the service, the employee, depending on the required action, can provide the service to the student directly in the case of simple requests, such as updating passport and visa information. However, if the request needs higher approval or the required service involves another department, the employee refers the request to the head of the department for review and a decision.
  - For each service requested, there is a section filled by the employee with data related to the requested service and the decision made about the request and providing the service. This section must be filled by each employee and differs according to the employee role, responsibilities and department.
- **Head of Supervision department (role):**

- All student requests which have complex steps or require actions related to other departments are referred to the Head of the student's supervision department.
- If the request does not require actions decided by other departments, the head of the supervision department reviews the request and all the provided documents, makes a decision to support or not support the decision taken by the employee. The supervisor provides comments and any relevant entries in the employee section according to his role and then the outcome of the request is given to the student.
- If the request requires actions or analysis by other departments or by the attaché office, the head of the supervision department provides comments on the request and any relevant entries in the employee section according to his role and then refers the request to the relevant department or the attaché's office as appropriate.
- All the referred requests come back to the head of the supervision department in a return route unless it is a financial request that was initially approved by the head of the department, and sent to the financial department for implementation.

- **Employee of other departments (Financial department, Tickets department, Legal department, Passports department, etc.)**
  - Student requests reach these departments usually through referral from their supervision departments, except for a few cases such as a clear case of a refund or a request for annual tickets where the student request go direct to the corresponding department. When the employee in the corresponding department receive the request, he/she writes comments about the request and the decision taken and returns it to the source of the request.
  - If any documents are issued as a result of the request, these are attached to the student PDF file (an archived file for all documents relevant to the student).
  - If an action is to be taken, for example, paying a refund, issuing a ticket, the employee performs the action and informs the student directly by email and writes it as a comment in the relevant section.
- **Attaché Office (Attaché or Attaché deputy role):**

- Some of the requests need approval by the attaché or need to be referred by the attaché office to the main sponsor for approval. For example, a request for a scholarship extension can be decided by the attaché if the extension period is three months or less. However, if the requested extension is for more than three months then the main sponsor should approve the request. EduPortal system is linked to around 60 sponsors, so in most cases when a request is referred to a sponsor, they log into the system using their own interface and log comments with regard to the request as it is processed. The attaché office can view these comments and the progress in dealing with the request. However, at this point, employees in government offices in a foreign country cannot alter any details in the request until a reply comes back from the sponsor.
- Once a decision is made either by the sponsor or the attaché office, the relevant decision, comments and documents if applicable are logged in the relevant section and the request is returned to the supervision department, then back to the student.

- Note that at the end of processing the request, the student is always informed automatically by email about any actions taken on his record and about any requests for services initiated either directly by the student or by an office employee and about any decision taken regarding these requests when it is rejected or approved.

IX.2.3 Justification of the Selected Services

EduPortal Services provides a large range of e-services that serve various student needs when studying aboard. For the purpose of applying the framework in this case study, the following services were selected:

1. Update Electronic file:
    - Update personal information
    - Update Contact information:
2. Enquiry Request
3. Scholarship Extension Request

These services were selected based on the extent the service uses sensitive user data which is shared with other departments. The Update Electronic file service involves uploading personal information and confidential files which

need protection and use only when needed. The Enquiry Request is general and involves different levels of data sharing between different government departments while the Scholarship Extension Request is rich in details and involves sharing specific data between different government departments and beyond with other government agencies and third parties.

IX.2.4 EduPortal Services - System structure

EduPortal system consists of different applications which a student can interact with using the student interface. These applications are:

- Educational: This deals with most of student requests about study.
- Request Workflow: This deals with listing the requests, allocating them to appropriate departments and managing the interaction between employees and the requests allocated to them according to roles and responsibilities. Using this application, an employee can refer or delegate a request to another employee in the department or another department according to his role's access rights assigned to his role.
- Financial: This deals with all financial requests and orders relevant to the system for students or employees, such as monthly salaries.
- Archive: This is concerned with transferring any paper into digital form and attaching it to the student PDF archived document file. It also updates the student PDF file with any document issued as a result of a request or provided by the student in the request.

IX.2.4.1 Student Record Structure

The student record has two main parts:

1. The Data File: This is stored in a DB which includes all student information and a history of all requests or actions performed on the student record. This record is accessed by all EduPortal portal applications and can be viewed by an employee from any department. However, any updates to the student record are due to data entered using the provided services. This data can be entered by the student, for example, when updating contact information or by an employee in the office as part of a response to a request made by the student.

2. The PDF File: This replaces an old physical paper file and contains any document about the student, since the student started and opened a file in the government office. These documents can be provided by the student, his sponsor, the university providing the study course or by the government office employees. It is segmented into sections, such as financial and educational and a document is added to the relevant section. The file documents are sorted by date of entry to ease access to a required document.

IX.2.4.2 Access rights to student record

Currently the access rights are set as:

1. Access rights to an active student record are role-based. For example, all employees in the department responsible for postgraduate students sponsored by a university can view the records of students supervised by that department, and are not allowed to access records of students of other departments with a few exceptions given to some employees who have senior roles, such as the head of a supervision department who needs to view a student record which is moving to another department (e.g. a student completed a bachelor degree and starting a masters).
2. When an employee is processing a request from a student because of his role, he can view the whole record of the student (Data and PDF parts). However, he cannot change, add or update any parts of the record unless processing a request made by a student and responding to the request initiates the change.
3. Each action performed on a student record due to a request is logged under the request information in the data file section in the student record with information about the employee who performed the action.
4. When a student record is closed (e.g. a student has finished his scholarship and graduated) the record is marked as archived and access rights to this record become more limited.
5. Access rights to view archived files are limited to some senior roles such as the attaché or the deputy attaché.

6. Access to view all student records (active or archived) for reporting or general analysis purposes is limited to a few senior roles (e.g. e-services manager).
7. No student record can be changed altered or updated without a request initiated by the student or an employee in the government office on behalf of the student and the student is always notified about such requests.

IX.3. Applying PRE_EGOV Framework

PRE_EGOV framework has three main stages: Preliminary, Requirements Elicitation Analysis, and Design. The framework also has three main supporting elements. These are the Environmental factors influence management, the Regulations, laws and policies compliance management, and Privacy awareness supporting element. These supporting elements are considered in each phase when applying the framework and relevant questions are asked during each phase in the framework. However, a discussion of these supporting elements will be provided after presenting the main phases of the framework. In the case study, the framework is applied on selected services in EduPortal namely: Update Personal and Contact Information; Enquiry Request; and Scholarship Extension Request.

IX.3.1 Preliminary Interviews

Two rounds of semi-structured interviews with relevant stakeholders were conducted before and during the application of the proposed framework. The aim of the first round of interviews was to understand the current system and the processes of the selected services and identify relevant stakeholders. It also aims to get stakeholders' views on the privacy issues in the current system and to identify their privacy requirements, their expectations and needs when using the selected services. Then a second round of interviews was performed during the application of the framework to confirm the requirements and resolve any conflicts. The selected sample for the interviews included ten users (four male, six female) with different backgrounds and ages, three service provider representatives, two developers and one government representative. Eight of the user's interviews were in person while two were done over the phone and relevant documents were sent to them in advance by email.

IX.3.1.1 First round of interviews

The interviews were used to identify relevant stakeholders, their expectations, needs, and any privacy issues with regard to preserving privacy when using the selected services of EduPortal. Also, the interviews were used to get stakeholders feedback on the proposed definitions of data classifications, ownership rights and levels of control. All participants were asked the same set of open questions and shown the set of definitions proposed in the framework (see section VIII.2.1). The questions and summary of the interviews are Appendix G.a. In the interviews with the service provider representatives, the developers, and the government representative, the same set of questions were asked but from the perspective of their roles. In addition, open questions about how the system works, the workflow of the selected services, the access rights of different actors and the security and privacy policies applied in the system were used in each participant's interview but adjusted to reflect their roles.

IX.3.1.2 Second round of interviews

The second round of interviews validated the identified privacy requirements of the selected services and resolved conflicts between the requirements of stakeholders. This round was conducted with the same sample of stakeholders. It involved validating the identified privacy requirements of the selected services and agreeing on the suggested options to resolve conflicts between stakeholders. These interviews took from 15 minutes to an hour.

IX.3.2 Preliminary Phase

This phase required input from the preliminary interviews with relevant stakeholders (see section IX.3.1) to identify their expectations and needs and establish agreement on the definitions proposed by the framework.

The identified preliminary stage tasks (section VIII.2.1) were applied as follows:

IX.3.2.1 Expectations and Needs Identification:

1. **Stakeholder Identification:**
    a. Users: Students age 18 and over, male and female, studying various degrees, such as English language programs, bachelor degree, diplomas, master degrees, PhD degrees, and post-doctoral degrees. It is

important to clarify that throughout this chapter, we refer to data subject users and when the reference is to other types of users who are using the EduPortal system, and this should be clarified and referred to as non-data subject users.

b. Government body representatives: Higher Education Ministry who provide EduPortal services and E-government strategic planning agency who approve new services or changes in the provided services.
c. E-government services Provider(s): Government Office(s) (mainly embassy(ies)) in foreign countries where students study, Higher Education(HE) Ministry who take part in processing and approving some of the services, Student sponsor representatives who take part in processing and approving some of the services and employees in government offices who are processing users' information (data subject users) to provide EduPortal services.
d. Developers of e-government services: A government owned company who design and implement most of the e-government services, Developers from the HE ministry.

It is important to clarify that other stakeholders, such as the employees in the services providers' stakeholder category, use the system to provide the services (e.g. process students' requests), however, they are considered as non-data subject users and by users we mainly mean data subject users.

2. Stakeholders Expectations and Needs:

In this step, for each service, the expectations and needs with respect to preserving privacy when using the services were gathered by following the steps detailed in section VIII.2.1.1.These are:

1. Select a representative sample of identified stakeholders.
2. Identify the expectations and needs of relevant stakeholders.
3. Review stakeholders' requirements and resolve possible conflicts between the identified requirements.

A sample of ten students using the system was selected as representative of the user category. The aim was to select students with different age, social background and studying different degrees. The selection involved 4 male students and 6 female students who study different courses (undergraduate and post graduate) - some married and others single. The sample for the other

stakeholders categories included, one government body representative, three service providers including a representative of the HE ministry and two employees who work in a government office in a foreign country and deal with student requests made through EduPortal in two different departments, and two developers, one who works for the HE ministry and the other an independent developer working on a similar system. It is believed that the sample is representative of the stakeholder categories as the researcher made every possible effort to select the sample carefully so that it represents student and other stakeholder categories and covers as many varieties in their needs and expectations as possible.

The next step was to identify the expectations and needs of the identified stakeholders. One-to-one semi-structured interviews were used. The identified expectations and needs were documented for each service and prioritised according to their importance to the stakeholders. These expectations and needs were formulated as the privacy requirements presented in section 1IX.3.1IX.3.3.2 while the interviews structure and details can are in Appendix G.a and Appendix G.b.

The main privacy expectations and needs sorted by priority from the perspective of the users who are data subject are:

1. The users of EduPortal services (data subject users) need to have full control over sensitive information about them.
2. The users (data subject users) need to know who is viewing information about them, what information is viewed? , and what is the purpose of viewing that information?
3. Users (data subject users) expect the employee who is processing the requested service to be able to view only information needed and relevant to that service.
4. Sensitive files and documents about the user (data subject users) should be encrypted and accessed only when needed and by limited employees.
5. Users (data subject users) should be notified of any override to the privacy settings set by them over information about them.

6. Employees' identities (who are users of the system but not a data subject of the processed data) should be protected and not viewed by users (data subject users) unless this is needed (by services provider and/or government representative perspectives).
7. There should be an option for overriding privacy settings applied by the user (data subject users) by senior employees in EduPortal system in emergency cases (by services provider and/or government representative perspectives).

3. Review requirements and resolve possible conflicts

For each service, the privacy requirements were reviewed with the stakeholders and identified conflicts and proposed resolutions were negotiated as described in Appendix G.b.

IX.3.2.2 Data Classification

The following data classifications were agreed by all stakeholders: Restricted Data, Sensitive Data, Private Data, and Public Data. Details of the definitions of these classifications are in section VIII.2.1.2

IX.3.2.3 Ownership Rights Definitions

The ownership rights definitions in section VIII.2.1.3 were agreed by all stakeholders with a slight change to the Totally Owned definition, namely "the right to delete the information owned" was omitted from the definition and replaced by a hide option that allow the user to prevent access to the data or viewing it.

IX.3.2.4 Levels of Control Definitions

The definitions of Levels of Control presented in section VIII.2.1.4 were agreed by all stakeholders. With the following changes:

1. **Full Control:** The user is given the right to allow or prevent any access right to a piece of information i.e. allow or prevent view, change or share of the information.
2. **Partial Control:** The user is given the right to allow or prevent the viewing, sharing of a piece of information.
3. **No Control:** The user does not have any right to allow or prevent access rights to a piece of information.

An important requirement is providing an option to override the privacy settings applied by the user. This was introduced to give full control to the service provider in emergency cases.

IX.3.2.5 Data Types Mapping

The data mapping table shown in Table VIII.2 in section VIII.2.1.5, was shown to all interviewees from the different stakeholder categories and agreed. Table IX.1 shows examples from the user data used to explain the relation between ownership rights and levels of control and the data classification.

Data	Privacy Settings	Comments
National ID	{Private, Partially Owned, Partial Control }	The user can view and change the data through a request, while controlling the viewing of the data and changing of the data by others. The system can still use the data for verification of the identity.
Marital status	{ Restricted ,Totally Owned, Full Control}	The user can view, edit and hide the data and have full control on allowing or preventing the viewing, editing of the data by any one.
Passport ID	{ Private ,Partially Owned, No Control }	The user can view and change the data through a request, but has no control on allowing or preventing access rights to the data. However, the user should know who is viewing the data and when the data is viewed and by whom.
Address	{ Sensitive ,Totally Owned, Partial Control}	The user can view, edit and hide the data and have partial control on allowing or preventing the viewing, editing of the data.
Mobile phones	{Totally Owned, Full Control, Sensitive}	The user can view, edit and hide the data and have full control on allowing or preventing the viewing, editing of the data by any one.
Email	{ Private ,Partially Owned, Partial Control}	The user can view, edit the data and have partial control on allowing or preventing the viewing, editing of the data.

Table IX.1: Examples of privacy settings over user's information

IX.3.3 Requirements Elicitation Phase:

In this phase the analyst performs the following tasks based on the identified stakeholders' expectations and needs resulting from the preliminary phase.

IX.3.3.1 Data Classifications Identification

Information about the user that is needed in processing and providing the selected services was analysed and classified to the data types defined in the

preliminary phase according to the identified expectations and needs of the user. The classification is as follows:

- Personal Details:
    - [Name, Gender](Public)
    - [National ID number, place of birth] (Sensitive), Default (Private)
    - [Marital status](Restricted),Default (Sensitive)
    - [Birth date] (Private),Default (Public)
    - [Relatives names] (Private), Default (Public)
    - [Relatives mobile numbers] (Sensitive),Default(Private)
    - [Relatives Addresses](Sensitive),Default (Private)
    - [Bank details] (Sensitive), Default (Private)
    - [Passport ID, Date of issue, Place of Issue] (Private),Default (Public)
    - [Passport Expiry date] (Public)
    - [Visa number, Date of issue, Place of Issue] (Private),Default (Public)
    - [Visa Expiry date] (Public)
    - [Sensitive personal files (e.g. personal pictures, copies of the passport, or any other personal identifiable documents, marriage or divorce certificates)] (Sensitive), Default (Private). Accessed only when the service totally depends on the information in these files)
    - [Official files (e.g. decisions on sponsorship, government letters, etc.)](Private), Default (Private)

- Contact Details:
    - [Mobile numbers] (Restricted), Default (Sensitive)
    - [email](Private),Default (Public)
    - [Addresses](Sensitive),Default (Private)
- Qualifications details [Public]

- Education study details [Public]

The classification of the above information will be revised after identifying the privacy and security requirements in the next step.

IX.3.3.2 Privacy and Security Requirements Elicitation

In this task, first a risk analysis relevant to the privacy of the users' information was performed based on interviews with the stakeholders and the risks identified by the service provider. Table IX.2 summarises identified risks relevant to the services, their potential impact and likelihood, and suggests mitigation safeguards for these risks. The impact levels are low, moderate, and high, and describe the level of the adverse effect on organizational operations, organizational assets, or individuals in the case of the loss of confidentiality, integrity, or availability of the information as defined by NIST [109] and OEDC [104].

Rank	Identified Risk	Potential Impact /Likelihood	Suggested Mitigation Safeguards
1	Disclosure of personal information about the user	High/High	Access rights are limited to user's sensitive personal information
2	Corruption/changes of information about the user	High/High	Changes to users' information are made through processing relevant services.
3	Destruction of information about the user	High/High	No delete option /backup data regularly
4	Unauthorised access to users' information	High/Moderate	Stronger authentication measures/log access
5	Black mailing/threats to users as a result of disclosure/theft of all or part of user information	High/Moderate	Limited access to user information/only when needed
6	Disclosure of information about other people related to the student	High/Moderate	Limited access to relatives' information
7	Unauthorised access to the system	High/Moderate	Strong secure authentication measures /system log
8	Denial Of Service	Moderate/Low	Provide alternative routes for a service,
9	Bias on decisions related to other services as a result of viewing information not needed for the service	Low/Low	Employee should view only needed information for the service

Table IX.2: Identified privacy risks and suggested mitigation

IX.3.3.2.1 Privacy requirements:

Based on the outcome of the interviews and the identified risks on user information, the following privacy requirements were identified for the selected

services. 25 general Privacy Requirements (PR) were identified for all the selected services:

PR1. The system should view only the needed information for the processing of the service.
PR2. The system should allow the user to decide on the information about them which is sensitive.
PR3. The system should allow users to have full control and the ability to limit access to their sensitive information.
PR4. The system should encrypt sensitive files about the user (currently included in the pdf file of the student records).
PR5. The system should provide protection and limit access rights to sections of the student record with sensitive information.
PR6. The system should allow the user to know who accessed his/her personal information, what information was accessed, when it was accessed and for what purpose.
PR7. The system should provide privacy awareness alerts and messages to the user and the employees to explain the impact of their actions on user's privacy when initiating or processing a request where appropriate.
PR8. The system should provide an option to override any privacy settings in emergency cases so that senior roles can access any user information which is needed.
PR9. The system should notify a user when any override occurs to the privacy settings applied by the user.
PR10. The system should consider contact information as sensitive information and limit access to this information.
PR11. The system should notify the user of any changes made to his/her information.
PR12. The system should not allow automatic delegation of processing a user's sensitive information without the user's consent.
PR13. The username used by the user to login to the system should not be a personal identifiable piece of information (e.g. National Identity Number, emails).
PR14. The user should be notified when any disclosure of information about him occurs, (either by accident or by an intended breach of the system or the user account).
PR15. All the system's users should be made aware of relevant privacy policies, regulations and legislations applied or being introduced.
PR16. The system should protect the identities of employees providing a service, by providing an Employee reference number for each employee.
PR17. The system should log the Employee reference number with each process performed on the user's information.
PR18. The identity of the employee with a particular employee reference number should only be known to people with senior roles in the government office.

PR19. The system should ensure that privacy preferences are applied as long as the information exists.
PR20. The system should apply stronger authentication methods to verify the user's identity when the user performs changes to his/her privacy preferences on information.
PR21. The system should limit access rights to backups of user information only to people with a senior role and the user should be notified about this.
PR22. General reports produced by the system should consider a user's privacy preferences.
PR23. The system should provide an option of private enquiry for enquiries that involve providing sensitive information and files.
PR24. Private enquiries should be processed by as few people as possible and only if needed.
PR25. The system should give access to sensitive information or supporting files included in a request, only to employees who are processing a scholarship extension request at a different government agency and only when it is needed for decision making according to their roles.

IX.3.3.2.2 Security requirements:

The Security Requirements (SRs) for the selected services were identified as:

SR1. The system should authenticate the user by username (National Identity number) and a strong password.
SR2. When the user forgets the password, the system should offer the user a way to recover the password (Currently by sending the password to the user's email registered in the system).
SR3. After three fail attempts at login, the user account is locked and can be opened only by answering a pre-set set of challenging questions.
SR4. User information cannot be changed unless it is by one of the system services.
SR5. Sensitive personal information about the user should be protected by high security measures.
SR6. Personal information and contact information should always be up-to-date
SR7. Changes in personal information should be supported by relevant evidence documents to validate the accuracy of the changes before approval. For example, a change in passport information requires providing a copy of the new passport.
SR8. Changes in personal information are only done by request to update personal information.
SR9. Changes in contact information are done by a request to update contact information.
SR10. Contact information should be considered as sensitive information and protected by access rights.

SR11. Any personal official files provided to support the request should be considered sensitive and protected by strong security measures.
SR12. Personal information and files should be accessed only when needed.

IX.3.3.2.3 Additional identified requirements:

Some additional Functional Requirements (FR) which relate to privacy and security were identified:

FR1. The system should give meaningful names for uploaded files by the users.
FR2. When the user is asked to support a requested service with an official document, the system should provide the user with a list of previous uploaded files to allow the user to select the file if it already exists in the system to avoid redundancy by uploading the same file many times.
FR3. The privacy preferences set by the user should not prevent the user from accessing the requested service.
FR4. The user should be notified if the current privacy preferences will affect processing the requested service or delay the response to that request.
FR5. The default privacy preference settings should support protecting the user's privacy.
FR6. The system should allow users to view the workflow of the request and the notes and alerts that concern them, and the expected time of processing of the request at each point as appropriate.
FR7. The system should allow an employee to view relevant alerts about the student related to the requested service.

IX.3.3.3 Ownership Rights and Levels of Control Identifications

In this step, the desired ownership rights and levels of control over information about the user were identified. The users would like to have full ownership rights on sensitive information about them or their relatives and would also like to have full control on such information. However, the service providers and government have some restrictions on giving full control to some of this information. Based on the identified privacy and security requirements in section IX.3.3.2.1 and the desired data classifications agreed by stakeholders in section IX.3.3.1, ownership rights and levels of control over pieces of information were assigned to each data type as described in the next section.

IX.3.3.4 Ownership Rights and Levels of Control Assignment

The assigned ownership rights and levels of controls agreed by relevant stakeholders are presented in Table IX.3 as privacy settings in the form:

Information {Data Classification (DC), Ownership Right (OR), Level of Control (LC)}.

Data	Privacy Settings	Comments
National ID	{Private, Partially Owned, Partial Control}	The user can view and change the data through a request, while controlling the viewing of the data and changing of the data by others. The system can still use the data for verification of the identity.
Marital status	{Restricted, Totally Owned, Full Control}	The user can view, edit and hide the data and have full control on allowing or preventing the viewing, editing of the data by any one.
Passport ID	{Private ,Partially Owned, No Control}	The user can view and change the data through a request, but have no control on allowing or preventing access rights to the data. However, the user should know who is viewing the data and when the data is viewed and by whom.
Address	{Sensitive, Totally Owned, Partial Control}	The user can view, edit and hide the data and have partial control on allowing or preventing the viewing, editing of the data.
Mobile phones	{Totally Owned, Full Control, Sensitive}	The user can view, edit and hide the data and have full control on allowing or preventing the viewing, editing of the data by any one.
Email	{Private, Partially Owned, Partial Control}	The user can view, edit the data and have partial control on allowing or preventing the viewing, editing of the data.

Table IX.3: Ownership rights and levels of control assignments

IX.3.4 Design Phase:

IX.3.4.1 Rules and Controls Presentation

The main requirements with regard to the presentation of the levels of control were identified by considering the identified expectations and needs in the previous phases and by considering the different capabilities of the users. The identified Privacy Design Requirements (PDRs) are:

PDR1. The system should show the privacy settings in the main page.
PDR2. The system should allow one time setting of privacy preferences for all services.
PDR3. The system should provide appropriate privacy alerts when a user changes the level of sensitivity of a piece of information.
PDR4. Privacy alerts and help messages should be provided in a simple language that can be understood by all types of users.
PDR5. Default privacy settings should be explained when the user first uses the system.

PDR6. Employee should have alerts each time he/she logs in to the system about currently applied privacy laws and should acknowledge reading it.

PDR7. A log file should be kept for all transactions made on a user's data while the user record is active.

PDR8. Each log entry should describe the action performed, on what data, when and by whom and who initiates it. For example, if the request was initiated by a user using EduPortal, then the user (identity number) ID and IP address should be entered in the log file. However if the employee is that one processing the request, then the employee reference number should be entered.

PDR9. Access to the student record (PDF file) should be protected by passwords and sections with restricted data should be encrypted.

PDR10. Log files should be protected by high security measures to prevent any tampering with the logged data.

PDR11. A onetime password is required when changing the privacy preferences settings; this password is sent to the registered mobile number of the user.

PDR12. Registering or changing the mobile number of the user should be in person or via the site and answering a security question.

PDR13. A timeout should be set to 5 minutes with no activity on the privacy settings pages.

IX.3.4.1.1 Suggested technologies:

When the requirements are implemented in the system, Privacy Enhancing Technologies (PET) can be used in the implementation to satisfy these requirements. Examples of PETs meeting these are:

- IBM's Secure Perspective software which allows organisations to create and manage enforceable security policies using natural language [26].
- Hewlett Packard's Openview Select Identity which enables organisations to manage users and their privileges [113].
- Privacy meta data use is suggested for tagging information about the user with relevant metadata that defines access rights to the data, any related conditions on the use of the data and whether the user's consent is required before sharing the data with third parties [privacy by design reference].

These are suggested PET technologies; however, any other technology can be used which satisfies the identified privacy requirements.

IX.3.4.2 Rules and Control Deployment

Based on the identified requirements, assigned ownership rights and levels of control identified in the second phase IX.3.3 and in section IX.3.4.1, a prototype which satisfies the identified privacy requirements for the selected services was developed. For the purpose of developing the screens of the prototype, MockupScreens13 tool was selected for its ease of use feature. This is a researcher choice and in the application of this step of the framework any other prototype tool or software development package can be selected which satisfies the requirement of enabling negotiation about the proposed solution with stakeholders. The resulting prototype demonstrates how students using EduPortal can set their privacy preferences on the information about them and how the EduPortal system is affected by these privacy settings. Snapshots of the resulting prototype are presented in

Figure IX.3,

Figure IX.4,

Figure IX.5, Figure IX.6, and Figure IX.7 in the next subsection. The snapshots show screens related to: Privacy preferences settings, Data sensitivity settings, Data control level settings and Employee interface for a selected service (Educational Enquiry Request). Complete scenario screens for the selected services are provided in Appendix G.c. These screens are explained and viewed to relevant stakeholders so that they can provide feedback and possible enhancements which are considered in the final screens presented in Appendix G.c. An actual implementation of the proposed solution within the e-government service is not included as it is out of the scope of the thesis and requires integration with the current system of EduPortal Services. This was not part of the agreement with the government agency that provides EduPortal services when agreed to the evaluation of the framework.

IX.3.4.2.1 Example scenario:

When the student logs in to the system, a Privacy Preference Setting screen appears with three choices (

[13] MockupScreens is an easy to use tool with many features to develop prototype screens for proposed software that allow stakeholders to negotiate the functionalities and design requirements of the proposed software. The tool link can be found at: http://www.mockupscreens.com/

Figure IX.3). When the student selects any of the options, he/she will be asked to enter a onetime password to get access to the selected privacy preferences settings choice (see Appendix G.c). The Privacy Preferences Settings options are: 1) Data Sensitivity Settings; 2) Files Sensitivity Settings; and 3) Data control Levels Settings.

If the student selects the Data Sensitivity Settings option, the student can view and change the sensitivity settings (data type) assigned to a piece of information as appropriate. If the user does not have the required ownership right for a data type, this data type will appear as disabled (see

Figure IX.4). The red question marks provide messages to explain the effect of selecting the corresponding data type. These messages appear when the user clicks on a mark.

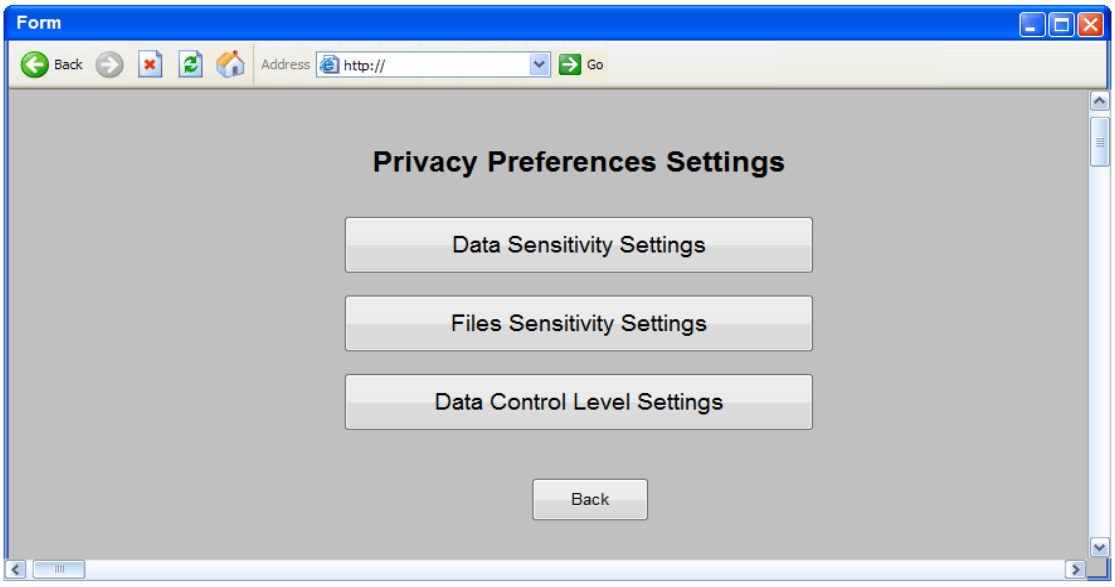


Figure IX.3: Privacy Preferences Settings

Figure IX.4: Data Sensitivity Settings

The option File Sensitivity Setting allows the student to view and change the sensitivity setting (data type) attached to a document that is included in the student record (see

Figure IX.5).

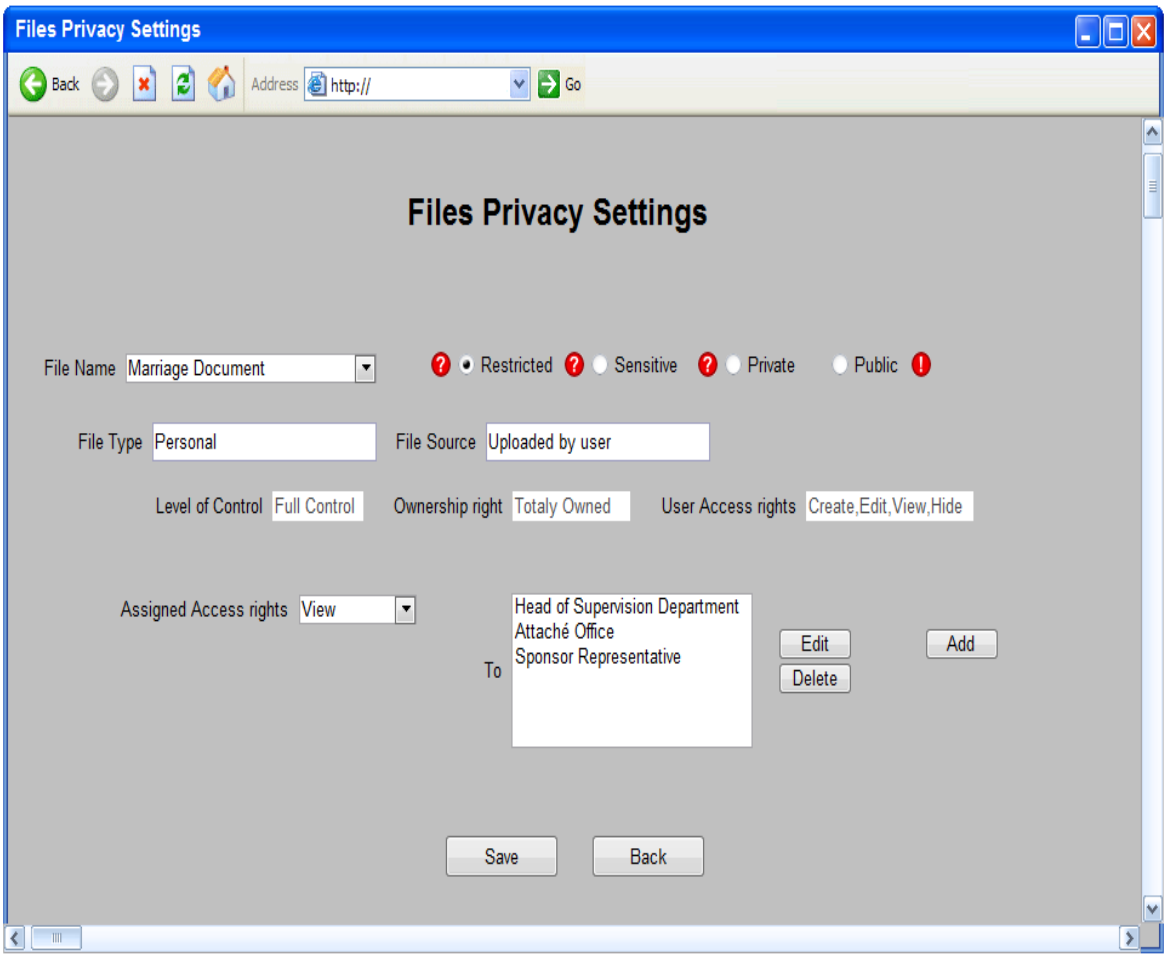


Figure IX.5: File Sensitivity Settings

The option Data Control Level Setting allows the student to change the access rights to each piece of information according to the assigned ownership rights and levels of control of that piece of information. Figure 9.6 shows an example of a user setting the control levels on a piece of information. The user selects a data type, then all pieces of information classified under that data type will appear in the drop down box, in the example, the user selects Restricted data type and then selects from the drop box, Status (marital status). The assigned ownership right and level of control for that piece of information appears. According to the assigned ownership rights and levels of control, the user can control access rights to this information or leave it to the default settings. In the example, the student has Totally Owned ownership right and Full control on this piece of information. Thus, the student has all access rights and can control also access to that information. Figure IX.6, the user gave the view access right to the roles of Head of supervision department, Attaché Office and Sponsor Representative. If the user limits the access rights to this information to none or

very few people, in a way that will affect his/her ability to request a service, appropriate alert message will appear.

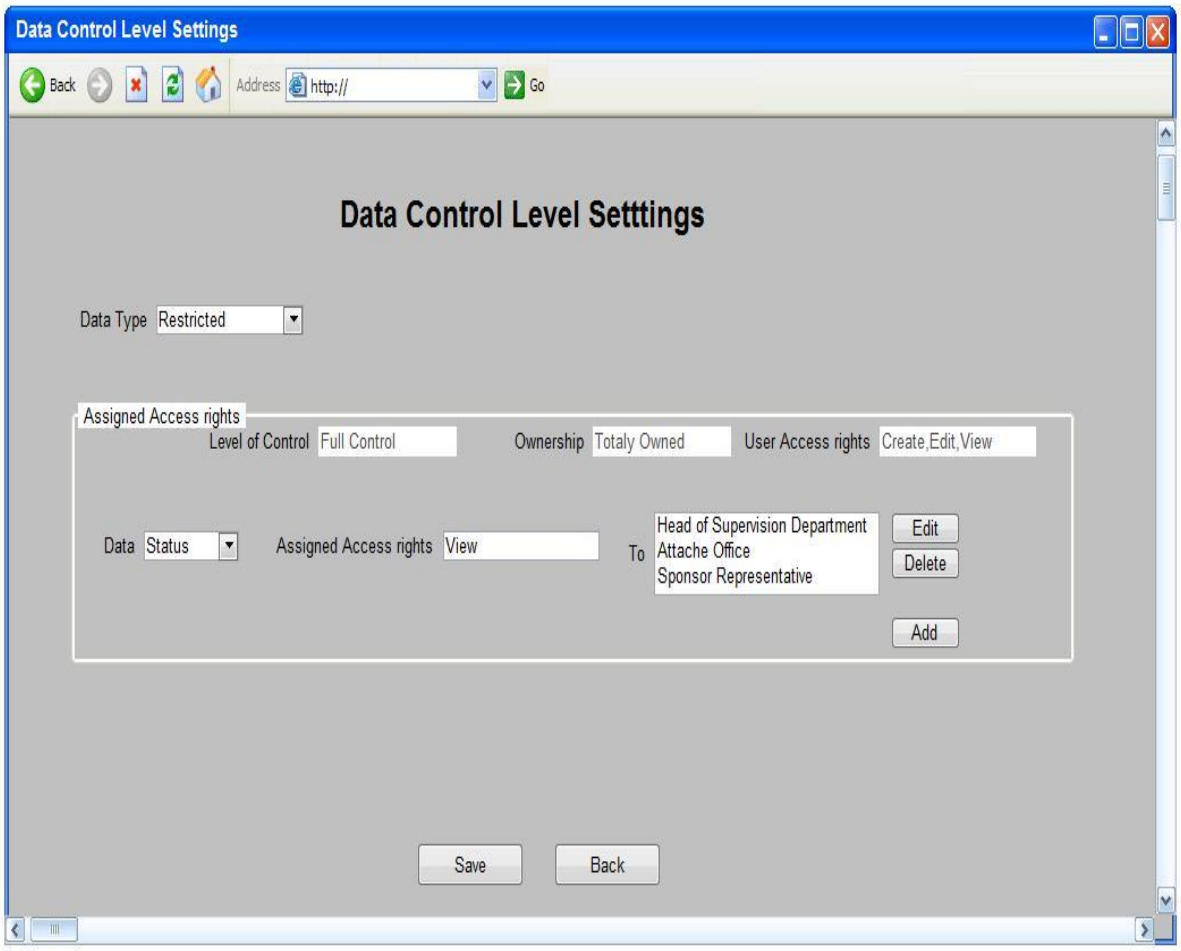


Figure IX.6: Data Control Level Settings for Restricted Data (Marital Status)

The Employee screen (Figure IX.7) shows how the settings applied by the user affected the employee's ability to view some of information. The example in Figure IX.7 is about an employee processing an Enquiry request (Educational). The employee cannot see all the information and only relevant information to the request can be viewed.

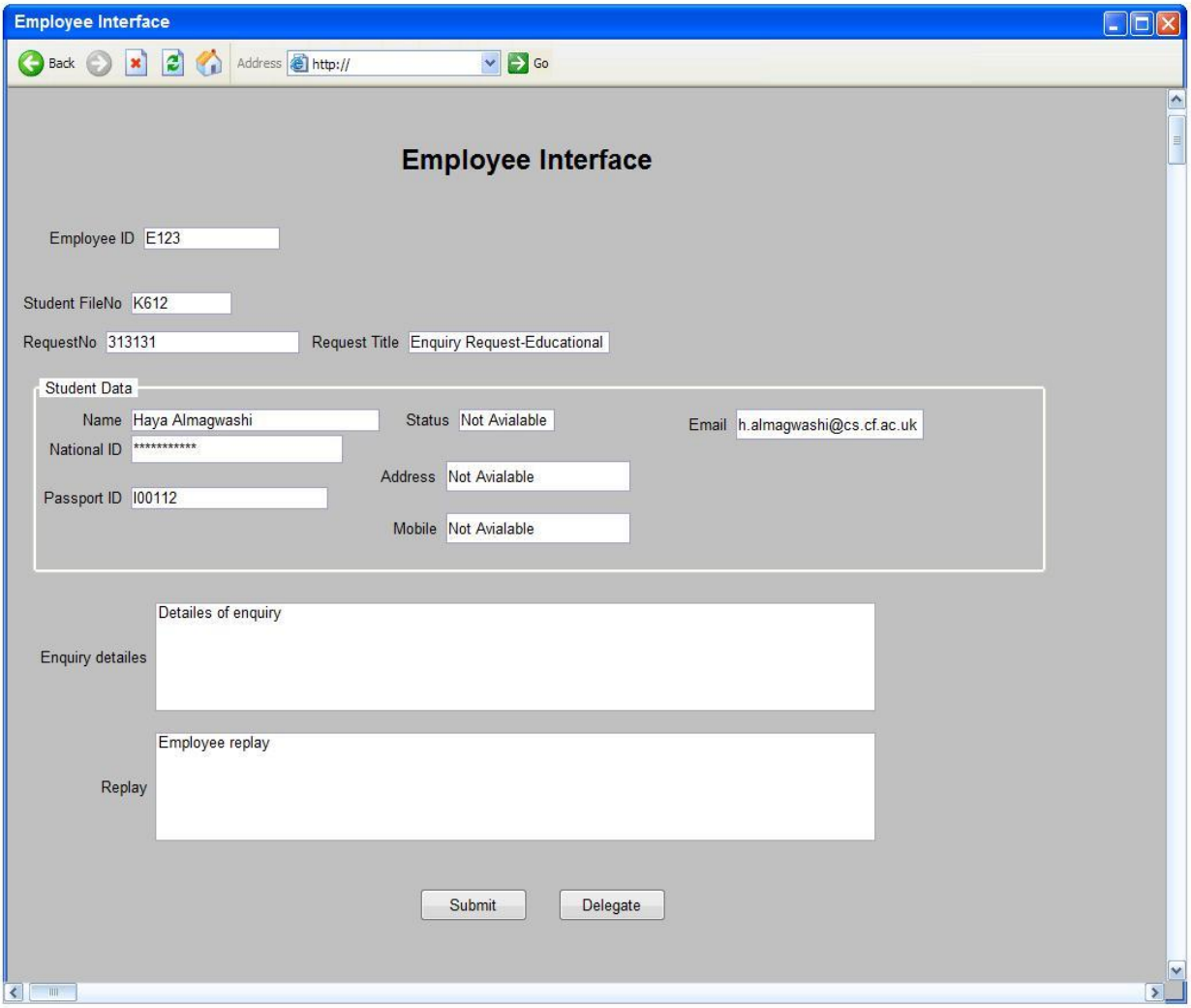


Figure IX.7: Employee Interface for an enquiry request

IX.3.5 Environmental Factors Influence Management

Environmental factors have been identified and their impact on the identification of privacy requirements was considered in the deployment of all the phases of the framework.

The identified factors are:

- The government has signed an international agreement that obliges all agreeing parties to have privacy regulations and laws in place by 2016 and to comply with OECD privacy guidelines [104], [Political, Legal].
- The government are open to different opinions from stakeholders, however, full control on the data used in e-government services should be in the hands of the system owner (the government),[Political].

- Users of the EduPortal system have at least a secondary school level of education, which means they are able to understand how to use the services, [Social].
- All students have access to the internet. Kiosks are provided in foreign government offices. Also, students can request a service in person at a government office, [Social].
- No user is allowed to use the EduPortal services on behalf of another user, [Political].
- Gender difference should be considered when identifying privacy requirements, [Social].
- Increasing a user's trust should be considered, [Cultural, Political].

IX.3.6 Regulations, Laws and Policies Compliance Management

A privacy law was introduced and applied, at the beginning of 2013, which states that any individual or organisation that seeks to collect unauthorised documents or confidential information by any means will face a sentence of up to 20 years in prison and a large money penalty.

IX.3.7 Privacy Awareness

Privacy awareness programs should be provided for both students and employees. The students' privacy awareness program can be given as part of the induction workshop where they learn about using the EduPortal system and for the employees as part of their training programs. In addition, the EduPortal services system will display warning messages for users, when they change their data privacy settings to a lower sensitive level. Alerts about relevant privacy policies also will be displayed to employees as appropriate.

IX.4. Conclusion

In this chapter, the PRE_EGOV framework was applied in a real world case study to demonstrate how the framework phases and elements can be applied. The application of the framework by the researcher was straightforward following the framework activities described in section VIII.3. Applying the PRE_EGOV framework involved full engagement with relevant stakeholders at different phases of the application to identify the privacy requirements, verify and resolve any conflicts in the identified requirements and design the

prototype. The identified privacy requirements were presented to stakeholders and agreed with them. The initial stakeholder's feedback about the framework was positive, however, a detailed evaluation through interviews was conducted following the application of the framework to evaluate the usefulness of the framework from different perspectives of the identified stakeholders. Details of the evaluation interviews and discussion of the main findings is presented in the next chapter. Finally, the application of the framework in the case study described in this chapter presents the first round of action research and lessons learned from this application can be used for further enhancements to the framework. In addition, the framework cannot be generalised unless it is applied in many case studies so refinements can be made according to the feedback gain after each application.

Chapter Ten

X. Evaluation of PRE_EGOV Framework

X.1. Introduction

The evaluation of the proposed framework PRE_EGOV described in chapter 8 was carried out over two phases. In the first phase, the development of the framework was validated using an online survey where the elements of the framework were examined against stakeholders' opinions and feedback and these results are presented in (section VII.7). In the second phase, the usability of the proposed framework was evaluated by applying the framework on a selected case study of actual e-government services, provided by different government agencies to a group of citizens as described in chapter nine. Then, the usefulness and acceptance of the framework was evaluated by conducting a series of semi-structured one-to-one interviews with relevant stakeholders, identified in the case study described in chapter nine, to seek their feedback on the results of applying the framework. This chapter describes details of the second phase of the evaluation and discusses the findings. Section 2 describes the evaluation strategy and some of the obstacles encountered, section 3 presents an overview of the case study used to evaluate the usefulness of the framework while section 4 discusses the findings.

X.2. Evaluation Strategy

The evaluation plan consisted of two phases: the first phase evaluated the validity of the development of the proposed framework and the second phase evaluated its usefulness in the context of e-government.

X.2.1 Evaluating the Framework Development

The first evaluation phase evaluated the validity of the research process in developing the PRE_EGOV framework, to show that the developed framework reflects the perspectives of relevant stakeholders. However, the development of the proposed framework is related to the development of the CMRPP

(section V.5) as the proposed framework is informed by the activities in the CMRP. The validation of the CMRPP was carried out using SSM rules (section 3V.3.2). To evaluate that the framework and the CMRPP reflect the perspectives of relevant stakeholders, an online survey was designed, where the survey questions were devised to determine stakeholders' opinions and agreement with the RDs of CMRPP which informed the development of the framework and the elements of the proposed framework. The survey design is discussed in sectionVI.4. The survey was distributed in three countries to a random sample of participants using emails, social networks and mobile phone text broadcasting apps with the aim of getting as many wide spread responses as possible. The findings of the survey were discussed in section VII.7. The findings supported the research hypothesis and indicated a general agreement among relevant stakeholders on the CMRPP and the proposed framework. In addition, the developed framework satisfied the identified requirements of privacy frameworks in e-government (sectionV.4.3) except for the requirements related to quality and performance assessment, which are out of the scope of this framework. However, the identified expectations and needs of stakeholders can be used to identify measures of performance and quality. In addition, the quality and performance assessment activities are part of the activities run by the government for monitoring and assessing e-government performance.

X.2.2 Evaluating the framework's usefulness

The second phase evaluated the usefulness of the PRE_EGOV framework. The plan was to apply the framework with several e-government services and get feedback on the process of applying the framework and the results of its application from relevant stakeholders during and after applying the framework on the selected services. The selected services should be e-government services provided online. A service can be processed by different government agencies where the user's data are shared to provide the service and where personal information is needed in the provision of the service. The evaluation approach was to conduct several rounds of semi-structured interviews after applying the framework on the selected services to get stakeholders' feedback on the usefulness of the PRE_EGOV framework in preserving privacy in e-government. Some of the evaluation questions were incorporated into the interviews used for understanding the expectations and needs of stakeholders

while applying the framework in the selected case study. The final round of interviews was performed after applying the framework to get feedback from relevant stakeholders' on the usefulness of the proposed framework in preserving users' privacy when using these e-government services.

X.2.3 Obstacles

The main obstacle facing the researcher in the evaluation phase was the lack of willingness of various government organisations that were contacted to participate in the empirical study where the framework would be applied on selected services provided by those agencies. The initial evaluation plan was to apply the framework in three real world case studies from governments with different political, social and cultural environments to demonstrate the utility of the framework and to evaluate the framework's usefulness and generality. However, despite hard efforts by the researcher to get approval from different government agencies, only one government agency agreed to participate in the study. Five government agencies in three countries were approached and asked to participate in the study, however, after long periods of negotiation and communication only one government agency agreed to participate in the study, even then this agreement was limited by restrictions of anonymising the collected data and the feedback. This case study used the EduPortal Services (section IX.2) Details of the application of the PRE_EGOV framework on EduPortal were presented in section IX.3.

X.3. PRE_EGOV Usefulness Evaluation in EduPortal

EduPortal Services is an e-government portal which provides a number of services online for students from Country B, who study aboard and are sponsored by the government or its partner organisations. Several government agencies are involved in the provision of these services to the students and need to share students' information; therefore, selected services provided by EduPortal were used to evaluate the usefulness of the application of PRE_EGOV framework. As part of the evaluation of the usability of the proposed framework, it was applied in selected services of EduPortal (section IX.3). The usefulness of applying the framework in EduPortal case study is evaluated using semi-structured interviews with relevant stakeholders identified in the selected case study.

X.3.1 Evaluation Interviews

The interviews were conducted after applying the PRE_EGOV framework in the selected services of EduPortal. Each interview lasted about 90 minutes and in the first 20 minutes the researcher briefly presented the proposed framework and illustrated the framework steps followed to identify the privacy requirements and assign the ownership rights and levels of control to the user information. Prototype screen shots for different scenarios were used to demonstrate how the application of the framework will enable a user to have control over their privacy while taking account of the security requirements of the provided services. The presentation was followed by asking general open questions. The questions covered what interviewees thought about the proposed framework in general, if the steps of applying the framework were in general clear and whether the application of the framework will increase their trust in using EduPortal services. In addition, interviewees were asked about the identified privacy requirements and assigned ownership rights and levels of control. Two hand-outs of the definitions and the identified privacy requirements, resulting from the application in sectionIX.3, were handed to the interviewees. Hand-out 1 showed the definitions proposed by the framework for the ownership rights and levels of controls and data types illustrated with examples, while the second hand-out had the forms used for identifying privacy requirements and the agreed resolution for identified conflicts (see Appendix G.b). The interviews were followed by providing a set of questions listed in a short questionnaire which each interviewee was asked to answer and complete. The questionnaire can be found in Appendix H.a, while a summary of the responses from the interviews is provided in Appendix H.b.

The sample in the evaluation round of interviews included the same sample of stakeholders who were interviewed during the application of the framework in the EduPortal case study except for two new interviewees from the user category. The sample included: six users (two new users [UserID5], [UserID6] and four users [UserID1], [UserId2], [UserId3], and [UserID4]). Also, the sample included three services provider representatives [SPID1], [SPID2], [SPID3], and two developers, one of them involved in the development of EduPortal services [DevID1] and another independent developer is familiar with the development of e-government services [DevID2]. In addition, a government body representative

[GR] was interviewed. It is believed that the selected sample is representative of the stakeholders, since the user sample was selected carefully to cover different groups of users both male and female, and students with different social circumstances and levels of study, also the number of interviewees from each stakeholder category represents an approximate percentage of their actual proportion in relation to the provision and use of the EduPortal services.

X.3.2 Result Analysis

The aim of the second phase evaluation was to evaluate the usefulness of the PRE_EGOV framework. It involved applying the framework in the EduPortal Services case study then conducting semi-structured interviews with relevant stakeholders to evaluate the usefulness of the proposed framework. The application of PRE_EGOV in the EduPortal case study required three rounds of interviews with a selected sample of relevant stakeholders (section IX.3.1). The aim of these interviews was to engage stakeholders in the steps of applying the framework and identifying privacy requirements. In the evaluation interviews, the aim was to identify privacy issues that users and other relevant stakeholders had with the current system and get their feedback on the proposed framework to see if the proposed framework improved the preservation of privacy and tackled the identified issues in the current system.

X.3.2.1 Responses about the current system (EduPortal Services)

Based on the evaluation interviews, the main features that the users and other stakeholders liked about the current system were: 1) Quick response to requests, 2) Easy to use interface, and 3) Student's data can be changed only via requests initiated by the student. However, there was general agreement that the current system does not preserve the privacy of the users (students) and that any employee processing a request from a student has access to all the student information (Appendix H.b, 2.Q3, Q4). These features were considered when applying the proposed framework and considered in the proposed solution to satisfy the requirements.

X.3.2.2 Responses about the application of PRE_EGOV in EduPortal

The application of the framework required three rounds of interviews and in total around 10 working days this included applying the framework activities, conducting interviews, identifying privacy requirements, verifying the

requirements with relevant stakeholders, and developing prototype screens. However, the arrangement for interviews took longer than expected and periods between responses between rounds of the interviews stretched up to three months with services providers and the government representative. Access to services providers' representatives and the government representative was a real obstacle due to their busy schedules; however, their feedback in the interviews was very valuable. The main findings on the application of the proposed framework are:

- All interviewees agreed on the proposed definitions for ownership rights and levels of control and thought the definitions were clear and comprehensive (Appendix H.b, 2.Q5).
- All interviewees agreed on the identified privacy requirements, and the suggestions for resolving identified conflicts in Appendix G.b, and no additional requirements were identified (Appendix H.b, 2.Q7).

The interviewees were shown a presentation about the steps of applying the framework in selected services of the EduPortal Services and screens of the prototype of the proposed solution resulting from the application of the framework. Next, the interviewees were asked about what they thought about the steps of the application of the framework and the resulting prototype. Their responses were:

- All interviewees from the user category liked the way that they had been consulted throughout the application of the framework and that the resulting requirements expressed their opinions (Appendix H.b.1, 1.Qt4). This was valued also by services provider representatives and the government representative (Appendix H.b.2, Q10.8 and Q10.9), although they emphasised that the system owner (the government ministry of HE) should finalise and approve the privacy requirements to be satisfied by the system (Appendix H.b.1.Qt16, 1.Qt17, and 1.Qt18). An example quote from a service provider representative is: *"Business owners (here the government and its ministry) understand the system more than the student. When it is applied it will remove the conflict between the stakeholders. The framework helps in resolving this conflict and clarifies the picture for all involved parties about the data that are more important*

to the users and should be protected and the privacy issues that a user is concerned about" (Appendix H.b.1.Qt17).

- The users in general thought the steps of applying the framework were clear, however, some users emphasised that providing examples to clarify the data types and the ownership rights and levels of control helped them to decide on what is important and sensitive to them (Appendix H.b.1.Qt9). Services providers and the government representative also said that the steps of the application of the framework were easy to follow while both developers thought the framework is applicable. However, most of the interviewees agreed that the willingness of the government to apply the framework would be a key factor in its successful implementation (Appendix H.b, 2.Q10).

X.3.2.3 Responses about the features of the PRE_EGOV framework

The proposed framework's usefulness, acceptance and effect on increasing users' trust in using the EduPortal services were evaluated in the final interviews. The interviewees were asked if the application of the framework and the implementation of the proposed prototype resulting from the framework will increase their trust in using EduPortal Services. In addition, the proposed framework was evaluated against the criteria of the proposed solutions for preserving privacy in e-government derived from the developed CMRPP and verified by the survey results in section VII.4. The criteria and additional questions about the interviewee agreement on usefulness, viability and acceptance of the proposed framework were included in the short questionnaire which was handed out at the end of the final evaluation interviews.

With regard to the question about whether the application of the proposed framework will increase users' trust in using the EduPortal services, all interviewees agreed that the application of the framework will increase users' trust in using EduPortal services (Appendix H.b.1, Qt19, Qt20, and Qt21). A quote form a services provider representative interview is *"I believe it will increase users' trust in EduPortal services and it will make them make less visits when they have sensitive issues (many students come to the government office when it is a personal matter to avoid uploading files in the service.)" [SPID3]*

A summary of the responses indicating the percentage of total agreement (respondents who chose strongly agree or agree options) is in Table X.1, while the full details of responses are in (Appendix H.b, 2.Q9).

Criteria	Total agreement %				
	All 12)	Users(6)	SP(3)	GR(1)	Dev(2)
Usefulness	100%	100%	100%	100%	100%
Accepted by users	75%	100%	67%	0%	50%
Accepted by Services provider	25%	8%	33%	100%	0%
Is viable	83%	100%	67%	100%	50%
Easy to Use	75%	100%	67%	0%	50%
Transparent	100%	100%	100%	100%	100%
Flexible	58%	83%	33%	100%	50%
Meet identified security requirements	75%	100%	67%	0%	50%
Enforce Local relevant laws, policies ..	50%	33%	67%	100%	50%
Complies with relevant international standards	50%	17%	100%	100%	50%
Considers the impact of social and cultural …	100%	100%	100%	100%	100%
Considers the impact of political factor	42%	17%	67%	100%	50%
Cost effective	25%	17%	67%	0%	0%

Table X.1: Summary of responses of evaluating features PRE_EGOV

The responses show that there is general agreement between stakeholders on the usefulness and transparency of the proposed framework and that the framework considered the identified social and cultural factors. The majority of stakeholders agreed that the proposed framework is viable and easy to use, while a quarter of the stakeholders had no opinion on these two issues. With regard to the flexibility of the proposed framework, more than half of the stakeholders agreed that the proposed framework is flexible. The majority of users and the government representative agreed that the proposed system is flexible and considers dynamic changes in their needs. However, some users, the services provider representatives and one of the developers were cautious in their responses and chose no opinion.

A services provider representative who disagreed about the flexibility of the framework explained his opinion as "*Flexibility depends on the implementation, if the application is designed very well and the policies are applied well, the framework provides these requirements, you propose how it can be satisfied,*

however the way it is applied determines if the flexibility is satisfied, if the requirements defined are met, then the system is flexible[14]" (Appendix H.b, 1.Qt15). With regard to agreement that the proposed framework will be acceptable to users; the responses showed that all users agreed that the proposed framework will be accepted by users of EduPortal.

However, the government representative, and a services provider representative who has an important role in the EduPortal Services, and the developer involved in the development of EduPortal services disagreed. Interestingly, most of the users were cautious on agreeing that the services provider will accept the proposed framework and chose no opinion, while one user disagreed. However, the government representative strongly agreed that the government will accept the proposed framework. This indicates a gap in the understanding of other stakeholders' opinions and mistrust between involved parties.

Users' responses showed a general agreement that the proposed framework has met the identified security requirements. A majority of the services providers have also agreed. With regard to enforcement of local laws, most of the users stated that they do not know if there are any existing laws with regard to privacy and chose no opinion, while the government representative, the developer from the government side and most of the services provider representatives agreed that the proposed framework considered the enforcement of local laws in the identified requirements. A similar response occurred for agreement on whether the framework complies with relevant international standards. All the services provider representatives, the government representative and the developer from the government side agreed that the proposed framework considered relevant international standards and guidelines. However, most of the users chose no opinion as they were not aware of the contents of these standards. The government representative agreed that the political point of view and impact was considered in the proposed framework while most of the users chose no opinion. Finally a majority of the stakeholders gave no opinion on whether the proposed framework is cost effective or not. However, a general impression from the interviews was that there are some worries that it might cost time and money

[14] This is a translation of the actual answer.

especially when applied in the existing services. However, the government representative agreed it could be cost effective in the long term and supported the application of the framework. Some additional feedback was given on the element of privacy awareness. The users liked the consideration of this in the prototype proposed by the framework (Appendix H.b, 1.Qt3, Qt9, Qt11).

In summary, there was positive feedback on the application of the framework and the results of its application. The services provider representative [SPID3] and the government representative [GR] who represented the owner of the EduPortal Services system (the ministry of HE in country B) recommended some of the identified privacy requirements: PR11, PR14, PR15, PR23 and PR24 (See section IX.3.3.2.1) in an update to the services which was due during the application of PRE_EGOV in the EduPortal Services. As a result, some changes in the provided services were made to satisfy these requirements. These are: a new option of private enquiry added to the types of enquiry in the Enquiry Request service with the process of this type of enquiry limited to the role of the head of the supervision department or higher roles; users would receive notification emails when their personal or contact details are changed; and emails about applied privacy policies and laws were sent to users of EduPortal.

X.4. Discussion

This section discusses the evaluation results in more details, the generality of the proposed framework, the quality of the research process and findings, and the research limitations.

X.4.1 Findings

The aim of the second phase of the evaluation plan is to evaluate the usability, acceptance and usefulness of the proposed framework for preserving privacy in an e-government context. Careful observation of the application of the PRE_EGOV framework in the case study (EduPortal) suggests that the proposed framework is useable and can be applied easily in the context of e-government. It also showed that all stakeholders involved in the case study accepted the framework and thought its application will be useful in preserving privacy in e-government. In addition, the PRE_EGOV framework satisfies the criteria identified in V.4.3 for a privacy framework.

X.4.2 Usability Evaluation

The usability of the framework i.e. the ease of use of the framework and the applicability of the framework were confirmed during the application of the framework in the case study. All the interviewees agreed that the framework is useable and can be applied to any e-government service. The interviewees were engaged in the application of the framework and the steps of the framework were explained to them in the initial and final interviews. All interviewees from the different stakeholder categories confirmed that the framework steps are clear and easy to follow. This was also reflected in their responses to the short questionnaire (see Table X.1 in section X.3.2.3). In addition, the viability of the proposed framework at an abstract level was supported by the survey results presented in section VII.3.1.3. Over two thirds of respondents (72%) from three different countries think that the proposed framework for preserving privacy with the features evaluated in the survey is viable. However, the willingness of a government to apply the proposed framework is a key factor in its successful implementation.

X.4.3 Usefulness and Acceptance Evaluation

The results of the survey in section VII.7indicate that applying a framework with the presented features will enable preserving privacy when providing e-government services. In addition, the very positive feedback given by interviewees during the application of the PRE_EGOV in the EduPortal case study supported the usefulness of the proposed framework. The acceptance of the framework was evaluated by direct questions to stakeholders. Although, each stakeholder category confirmed that they accept the proposed framework approach, there were doubts between stakeholders whether the other party will accept the approach. This was observed during the interviews and was clear in the answers to the relevant questions in the short questionnaire (Table X.1, section X.3.2.3).

X.4.4 Quality and Validity of the Research Process and Findings

The research hypothesis states that “balancing preserving privacy when providing e-government services with the identified security requirements of these services (authentication requirements in specific) can be achieved using a privacy framework that provides a method for deriving privacy and security

requirements for a service, while considering the different perspectives of stakeholders and the influences of political, social and cultural factors and that achieving this preservation of privacy (information privacy) will increase the users' trust in using e-government services". The evaluation results show that the PRE_EGOV framework presented in this research has achieved the research objectives and that applying the proposed framework will increase users' trust when using e-government services. The research process followed rigid steps: the application of a structure analysis to the relevant literature; the use of SSM to build relevant CMs for the concepts relevant to preserving privacy in e-government. The results gained from the literature review and gap analysis were used to build a solid basis for the framework which was informed by the CMRPP developed in chapter 5. The developed CMRPP helped to identify criteria for privacy framework in e-government. Both the CMRPP and the proposed framework were validated using a general survey that covered stakeholders in three countries with different political, social and cultural environments. The results of the general survey supported the validity of the CMRPP and the proposed framework and resulted in identification of a set of enhancements to the proposed framework. These enhancements were considered in the detailed description of the PRE_EGOV framework in section VIII.2.

X.4.5 Generality of PRE_EGOV Framework

The successful application of the PRE_EGOV framework in the EduPortal case study in the empirical research presented in chapter nine, increased confidence in the framework's applicability to other case studies. The PRE_EGOV framework development was informed by the CMRPP developed using SSM. The CMRPP was developed based on the defined RDs relevant to preserving privacy in e-government. The main purpose of preserving privacy was defined based on an extensive literature review and consideration of existing privacy definitions in relevant frameworks (V.2.1). These RDs were discussed with experts in the area at relevant conferences and were validated using a general survey that included participants from different countries (section VII.4). For these reasons, we argue that the proposed framework can be generalised and so could be applied to any e-government services in any country, but this would

require long term evaluation and the application of the framework in many case studies in different countries.

X.4.6 Evaluation Limitations

Limitations of the evaluation of PRE_EGOV framework exists in both phases of evaluation. The validity of the CMRPP and the proposed framework was evaluated using the online survey distributed in three countries and the results gave confidence that the CMRPP and the proposed framework reflect the views of relevant e-government stakeholders in those countries. However, based on the results we cannot say that the CMRPP and the framework reflect the views of e-government stakeholders around the world. This would be an area of future work. Future studies should survey stakeholders' views in a wider range of countries with different social, cultural and political environments to gain confidence in the generality of the framework and examine if it reflects the wider range of stakeholders views around the world. Also, it is important to ensure that the samples of the stakeholders in future studies cover various types of stakeholders in reasonable numbers. This will lead to valuable enhancements to the CMRPP and the framework. In the second phase of evaluation, the main limitation is that the PRE_EGOV framework was applied on only one case study. Although the application of the framework on the selected case study was successful and the positive feedback from relevant stakeholders in the case study supported the usefulness and acceptance of the framework, still the framework cannot be generalised based on one result without further investigation. Again, this limitation can be treated by applying the framework in many case studies in different countries and evaluating the application of this framework in short and long term. Also, when evaluating the usefulness and acceptance of the framework, prior to the semi-structured interviews, a brief presentation was provided by the researcher to explain the steps of the framework and how it was applied and the results of its application. Although, the researcher made sure that the presentation is neutral and factual and does not involve any personal opinion, there is a possibility that it might affect the stakeholders' views. In the future, an approach were the stakeholders are involved in the steps of the application of the framework and where they can use the final output of the framework and then give their feedback would be recommended. However, the presentation and semi-structured interviews

approach was followed by the researcher due to the limited time allowed for the evaluation by the stakeholders in the selected case study. Another limitation is that the researcher played the role of the facilitator who applied PRE_EGOV on the selected case study. This may have affected the successful application of the framework as the researcher is aware of all the steps and how they should be applied. However, this limitation can be treated in two ways. First, the PRE_EGOV framework should be used by other analysts in different case studies and feedback on obstacles faced when using the framework can be used to enhance the framework and to provide more details on how to apply different steps in the framework to enhance its generality. Also, details of successful application of the framework on different case studies should be well documented and made public where and when possible. These documented case studies can be used as a general guide on how the framework was applied in real world situations.

X.5. Conclusion

This chapter described the evaluation strategy and phases for the proposed privacy framework PRE_EGOV. Details of the evaluation phases were described. The results of the online survey used in the first phase of evaluation showed that the CMRPP and the elements of the PRE_EGOV framework are valid and reflects the views of involved stakeholders. The findings of the second evaluation phase which was based on the application of the framework in the case study (EduPortal) in chapter nine, showed that PRE_EGOV framework is useable and accepted by stakeholders. The positive feedback on the application of the framework suggests that the framework is useful in preserving privacy in e-government. A general discussion of the findings of the evaluation of the framework was provided. Lastly, the quality and validity of the research process and the generality of the proposed framework was argued.

Chapter Eleven

XI. Conclusions and Future work

XI.1 Introduction

The problem of preserving privacy in e-government services has been investigated. The research developed, justified and validated a novel framework which identifies the requirements for preserving privacy of the users of e-government services. It considers the security requirements of the services and the political, social and cultural impacts in the way users' privacy is preserved. In this chapter, a summary of the key concepts investigated in the thesis is provided and contributions of the research are presented. Research limitations are explored and suggestions for future work provided.

XI.2 Summary of Key Concepts

The research aim was to investigate the problem of preserving privacy in e-government. A system thinking approach to understand and explore the problem and relevant concepts was adopted. SSM and in particular the method of EMA was used in developing four CMs relevant to the concepts of government, e-government, authentication in e-government and preserving privacy in e-government. These CMs were used to understand different aspects relevant to the problem and review relevant literature. Following systems modelling rules which require the modelling of the system before modelling the services of the system, relevant CMs were developed for the concepts of government and e-government. These two CMs were used to understand the problem domain and identify government activities that should be considered when proposing a relevant framework for e-government. Another CM relevant to authentication in e-government was developed. This helped in understanding the process of authentication in e-government and the relation between the authentication process and the privacy issues arising when providing e-government services. The activities of the CM relevant to authentication in e-government were used as criteria for a gap analysis of existing e-government authentication frameworks. One of the major identified gaps was that there is a

lack of consideration of the users' perspectives on their privacy, when applying authentication mechanisms and that there is a lack of involvement of stakeholders in the design of relevant policies and decisions. Another gap that was identified at the time of the study was in providing a privacy framework that gives guidance to government agencies when developing their e-government services. However, privacy impact assessment documents and some e-government privacy frameworks have emerged and been published by some governments since the gap was identified. To understand the concept of preserving privacy in e-government, the CM relevant to Preserving Privacy in e-government (CMRPP) was developed based on extensive review of privacy definitions in the literature. Its activities were used to conduct a structured review of the literature and develop evaluation criteria for a gap analysis of existing e-government privacy frameworks. The main identified gaps were: lack of consideration of ownership management and enabling the user to have control over information about them. Another gap was recognizing and agreeing on levels of control and assigning these controls to users' owned information and presenting and deploying these levels of controls to enable users' control over their owned information and a lack of consideration of the influences of environmental factors such as political, cultural and social factors when identifying the privacy requirements of an e-government service. The requirements for a new approach for preserving privacy in e-government were derived, based on the activities in the developed CMRP. To satisfy these requirements, the Privacy REquirements in E-GOVernment (PRE_EGOV) framework was created as a framework to identify the privacy requirements when providing e-government services. The development of the framework was mainly informed by the activities of CMRPP. The evaluation of this framework showed that it has satisfied the identified requirements for a privacy framework.

The evaluation consisted of two phases. First, an online survey distributed in different countries was used to validate that the concepts provided by the proposed PRE_EGOV framework and the developed RDs in the CMRPP reflect the perspectives of relevant stakeholders in e-government services. Results obtained from the survey supported the validity of the PRE_EGOV framework and the RDs of the CMRPP. To validate the usability, usefulness and acceptance of the proposed framework, an empirical application of PRE_EGOV

in a selected case study of e-government services (EduPortal) was performed. The successful application of the framework in EduPortal increased confidence in the applicability of PRE_EGOV to e-government services. The results of the application of the PRE_EGOV framework in EduPortal were evaluated using semi-structured interviews with relevant stakeholders. Feedback from the interviews provided further evidence of its usability and confirmed the usefulness and acceptability of PRE_EGOV.

XI.3 Reflection on the Research Approach

Developing conceptual models using SSM is not a trivial task and requires considerable practice and expertise. The modelling process can go in iterative cycles to reach a rigorous set of RDs relevant to the problem and this requires time and effort. However, once the analyst's expertise increases in the context of the problem and the modelling process, the development of conceptual models using SSM become quicker. This was the case with the CMs developed in this thesis as the development of earlier CMs, i.e. initial CMs relevant to the concepts of government, e-government, required more time and effort than the development of later CMs, i.e. CMs relevant to the concepts of authentication and preserving privacy in e-government. The use of SSM in developing the CMs presented in this thesis enriches our understanding to the concepts under investigation and helped in capturing the different perspectives of e-government stakeholders about preserving privacy in an e-government service. It also helped in developing a comprehensive set of requirements for authentication and privacy frameworks in the context of e-government. Based on the activities of CMRPP developed using SSM, the PRE_EGOV was developed and the framework captured the essential concepts of systems in SSM by considering preserving privacy as a system whose purpose is to have the capability to enable users (data subject users) to

have control over their personal information and that this system can achieve this purpose with the support of its other parts such as the consideration of the environmental factors and the privacy awareness parts. It also emphasises the essential role of the assessment of the system activities according to the stakeholders' expectations. However, developing CMs in SSM also helped in structuring the problem situation and understanding the purpose of the system and what should be done to achieve that purpose but not how it should be done. The activities in the PRE_EGOV framework guided the analyst as to what should be done to enable the users who are the subject to the information to have control over information about themselves, however, the framework also provided activities to describe how to achieve this purpose. The knowledge gained from analysing existing frameworks and from developing the relevant CMs to the concepts of the problem helped the researcher in the development of the activities in the framework such as how to define the ownership rights and levels of control. However, the framework does not provide recommendations about the technologies for the implementation of the design phase deliverables. It is left to the analysts to decide on the suitable technologies that fit the government resources and this is considered as strength to the framework rather than a limitation as it shows its flexibility.

XI.5 Research Contributions to Knowledge

This research contributes to existing knowledge in e-government research, and security and privacy research in many ways, including:

- A novel approach for preserving privacy in e-government was developed and validated. This approach is represented by the Privacy REquirements in E-GOVernment (**PRE_EGOV**) framework, which provides a way to identify the privacy requirements in e-government and balance these requirements with the identified security requirements of the provided service with emphasis on the consideration of ownership management and enabling users to have control over information about them while considering the impact of social, cultural and political factors and engagement with relevant stakeholders.

- The demonstration of a unique approach for the use SSM methodology in modelling the systems in the domain of government and e-government, authentication and privacy preservation systems as government service systems.

- The development of CMs relevant to the concepts of government and e-government which can be used as reference models when discussing relevant issues to the concepts, and which provide rich understanding of the domain of e-government research

- The demonstration of a systemic approach for analysing the literature using the developed CMs relevant to the concepts of authentication and privacy in an e-government context by developing a CMRPP for the concept of privacy in e-government.

- Development of CMs relevant to authentication in e-government and the CMRPP in government.

- An approach for evaluating CMs developed using SSM by an online survey evaluating the agreement on the statements and elements in the RDs of the CM. This was demonstrated in the validation of CMRPP using an online survey.

- The elicitation of the requirements for privacy frameworks in e-government, with an emphasis on consideration of ownership management and enabling users to have control over information about themselves.

- Development of CMs for the concepts of government and e-government which can be used as reference models when discussing relevant issues to the concepts, and which provide rich understanding of the domain of e-government research.

XI.6 Research Limitations

A number of limitations need to be considered. The first limitation of this work is that the successful application of the framework depends heavily on the willingness of the government to engage relevant stakeholders in the design of e-government services and their willingness to provide the time and money to preserve the privacy of the users. However, with an increasing number of governments participating in international privacy laws and privacy agreements, and increasing pressure from the users of e-government services, this limitation should become less significant in the long term. Another limitation is that privacy awareness is a key aspect in the successful use of the framework. Stakeholders should have a sound privacy awareness to be able to benefit from the framework and to apply the required measures to satisfy the identified privacy requirements. The effect of this limitation can be reduced by well-designed privacy awareness programs to raise the awareness between stakeholders and in particular the users of e-government services. If a user decides to give away his log in information to another person, or does not take enough measures to protect this information, the usefulness of the application of the framework will not be shown. In addition, the application of the framework especially for the first time by e-government services provider might require commitments, time and effort as the preliminary phase of the framework involve negotiating the relevant definitions and agreeing on the ownership rights and levels of control between stakeholders which can take time and effort. However, once these definitions are agreed for the first time. They can be revisited when a new e-government service is introduced. With regard to the research evaluation, it was limited to the application of the framework in one case study due to

constraints of time and resources. This limits the generality of the framework. The application of the framework in a wider range of case studies in different countries will help in enhancing the framework and will increase confidence in the applicability, usefulness and generality of the framework. Another limitation is that the researcher was the facilitator of the framework in the evaluation case study which might have implication on the successful application of the framework. However, this limitation can be treated by other analysts using the framework in different case studies who can give feedback on difficulties that might be faced when using the framework. This feedback can be used to enhance the framework and to provide more details on how to apply different steps in the framework to enhance its applicability and generality. Also, the documentation of successful application of the framework on different case studies is recommended. These documented case studies can be made public where and when possible and used as a general guide on how the framework was applied in real world situations. With regard to the research approach, the validity of the CMRPP and the framework was evaluated using an online survey distributed in three selected countries to capture stakeholders' views about the conceptual model CMRPP and the privacy framework. However, although these countries have different political, social and cultural environments, the views of the stakeholders in these countries do not necessarily reflect the views of e-government stakeholders universally. A suggested treatment of this limitation is conducting a global survey that is distributed to e-government stakeholders in as many countries as possible with various social, political and cultural environments, and the results can then be used for refinements to the conceptual model and the framework. This can be an area of further research.

XI.7 Future Work

Further research can be conducted on different levels:

- Further application of PRE_EGOV in other case studies in different governments with varied political, social and cultural environments will increase confidence in its generality and the lessons learned from these applications will lead to enhancements to the framework.
- The application of the framework was successful in the case of a central government where all legislation, policies and laws are applied to all

government agencies; however, it will be worth exploring how the application of the framework in federated government environments will work and what possible enhancements can be identified for such environments.

- Another interesting area for further research is to integrate the framework with existing security requirements at the requirements and the design levels. The aim of such integration will be to enhance the framework, so that it enables identification of the privacy and security requirements and presents the requirements in a specification form for implementation.

Bibliography

1. Almagwashi, H. Preserving Privacy in E-government: A System Approach. in *IFIP EGOV2012 and IFIP E-Part 2012 conference*. Kristiansand, Norway 2012.
2. Almagwashi, H and Gray, A. E-government Authentication Frameworks: a Gap Analysis. in *the 5th International Conference on e-Government(ICEG2009)*. Boston,US, 2009.
3. Almagwashi, H and McIntosh, S. Understanding the Government to E-government Transition Using a Soft Systems Approach: What is E-government Supposed to do? in *the 9th European Conference on Electronic Government (ECEG)*. London, 2009.
4. Almagwashi, H, Tawileh, A, and Gray, A. Citizens' Perceptions and Attitudes Towards Preserving Privacy and Trust in E-government Services: A Cross-sectional Study. in *the 8th International Conference on Theory and Practice of Electronic Governance – ICEGOV* Guimarães, Portugal: ACM 2014.
5. Almagwashi, H, Gray, A, and Hilton, J. Privacy Requirements Elicitation in E-government: A Systems Approach. in *the Security and Privacy in Collaborative Working workshop, UK e-Science All Hands Meeting 2010 conference* Cardiff,UK, 2010.
6. Fang, Z, E-Government in Digital Era: Concept, Practice, and Development. *International Journal of the Computer, the Internet and Management*, 2002. 10(2): p. 1-22.
7. Heeks, R and Bailur, S, Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice. *Government Information Quarterly*, 2007. 24(2): p. 243-265.
8. Yildiz, M, E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly*, 2007. 24(3): p. 646-665.
9. Carlson, CN. e-Citizenship and its Privacy Protection Issues. in *6th European Conference on e-Government*. Marburg/Lahn 2006.
10. Carter, L and Bélanger, F, The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal*, 2005. 15(1): p. 5-25.
11. Belanger, F and Hiller, JS, A framework for e-government: privacy implications. *Business Process Management Journal*, 2006. 12(1): p. 48-60.
12. Holden, S and Millett, L, Authentication, Privacy, and the Federal E-Government. *The Information Society*, 2005. 21: p. 367-377.
13. Liu, L, Yu, E, and Mylopoulos, J. Security and privacy requirements analysis within a social setting. in *11th IEEE International Requirements Engineering Conference*. 2003.
14. Kalloniatis, C, Kavakli, E, and Gritzalis, S, Security requirements engineering for e-government applications: analysis of current frameworks, in *Electronic Government*. Springer, 2004. p. 66-71.
15. Wimmer, M and Von Bredow, B. A holistic approach for providing security solutions in e-government. in *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*. 2002.
16. Grönlund, Å and Horan, TA, Introducing e-Gov: History, Definitions, and Issues,. *Communications of the Association for Information Systems:* , 2005. 15(39): p. 713-729.
17. United Nations Division for Public Economics and Public Administration, *Benchmarking E-government: A Global Perspective - Assessing the Progress of the UN Member States*. Academic Press, 2002.
18. Scholl, HJ, Involving salient stakeholders Beyond the technocratic view on change. *Action Research*, 2004. 2(3): p. 277-304.

19. Rowley, J, e-Government stakeholders—Who are they and what do they want? *International Journal of Information Management*, 2011. 31(1): p. 53-62.
20. Almarabeh, T and AbuAli, A, A general framework for e-government: definition maturity challenges, opportunities, and success. *European Journal of Scientific Research*, 2010. 39(1): p. 29-42.
21. Heeks, R. Understanding and measuring eGovernment: international benchmarking studies. in *UNDESA workshop,"E-Participation and E-Government: Understanding the Present and Creating the Future", Budapest, Hungary*. 2006.
22. United Nations Division for Public Economics and Public Administration, *E-Government Survey 2012 E-Government for the People*. New York: United Nations, 2012.
23. *e-Government Authentication Framework v1.0,* . Office of e-Envoy,Cabinet Office: UK, 2000. Available from: http://webarchive.nationalarchives.gov.uk/20040722031653/http://e-government.cabinetoffice.gov.uk/assetRoot/04/00/08/36/04000836.pdf.
24. Bolten, JB. *E-Authentication Guidance for Federal Agencies*. 2003. Available from: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.
25. *Australian Government E-security Review*. Office of the Privacy Commissioner: Australia, 2008. Available from: http://www.oaic.gov.au/images/documents/migrated/migrated/sub0808.pdf.
26. *Privacy by Design*. Information Commissioner's Office: UK, 2008.
27. Cullen, R and Reilly, P, Information Privacy and Trust in Government: a citizen-based perspective from New Zealand. *Journal of Information Technology & Politics*, 2008. 4(3): p. 61-80.
28. Cullen, R, Culture, identity and information privacy in the age of digital government. *Online Information Review*, 2009. 33(3): p. 405-421.
29. Cockcroft, S, Information privacy: Culture, legislation and user attitudes. *Australasian Journal of Information Systems*, 2006. 14(1).
30. Hugl, U and Valkanover, H. Privacy from an individuals' point of view in German Speaking Countries:

Assessments and Empirical Results. in *6th WSEAS International Conference on Information Security and Privacy,*. Tenerife, Spain, 2007.
31. Horst, M, Kuttschreuter, Mt, and Gutteling, JM, Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. *Computers in Human Behavior*, 2007. 23(4): p. 1838-1852.
32. McLeod, AJ and Pippin, SE. Security and Privacy Trust in E-Government: Understanding System and Relationship Trust Antecedents. in *Proceedings of the 42nd Hawaii International Conference on System Sciences*. Hawaii: IEEE, 2009.
33. Oxford dictionaries. 2010. Available from: http://www.oxforddictionaries.com/.
34. Navarrete, C. Trust in E-Government Transactional Services: A Study of Citizens' Perceptions in Mexico and the US. in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, 2010.
35. Chang, MK and Cheung, W. Online trust production: Interactions among trust building mechanisms. in *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*. IEEE, 2005.
36. McKnight, DH, Choudhury, V, and Kacmar, C. Trust in e-commerce vendors: a two-stage model. in *Proceedings of the twenty first international conference on Information systems*. Association for Information Systems, 2000.
37. Warkentin, M, et al., Encouraging citizen adoption of e-government by building trust. *Electronic markets*, 2002. 12(3): p. 157-162.

38. Parent, M, Vandebeek, CA, and Gemino, AC, Building Citizen Trust Through E-government. *Government Information Quarterly*, 2005. 22(4): p. 720-736.
39. Welch, EW, Hinnant, CC, and Moon, MJ, Linking Citizen Satisfaction with E-Government and Trust in Government. *Journal of Public Administration Research and Theory*, 2005. 15(3): p. 371-391.
40. Cullen, R. Citizens' Concerns about the Privacy of Personal Information Held by Government: A Comparative Study, Japan and New Zealand. in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. 2008.
41. Scholl, HJ, Discipline or Interdisciplinary Study Domain? Challenges and Promises in Electronic Government Research, in *Digital Government*, H. Chen, et al., Editors., Springer US, 2008. p. 21-41.
42. Hovy, E, An Outline for the Foundations of Digital Government Research, in *Digital Government*, H. Chen, et al., Editors., Springer US, 2008. p. 43-59.
43. Checkland, P, *Systems Thinking, Systems Practice*. West Sussex: Wiley, 1999.
44. Brian Wilson, *Soft Systems Methodology: Conceptual Model Building and its Contribution*. West Sussex: Wiley, 2001.
45. Sommerville, I, *Software Engineering*. 6 ed.: Addison-Wesley, 2001.
46. Senge, PM, The fifth discipline. *Measuring Business Excellence*, 1997. 1(3): p. 46-51.
47. Daellenbach, HG. Hard OR, soft OR, problem structuring methods, critical systems thinking: A primer. in *Conference Twenty Naught One of the Operational Research Society of New Zealand*. 2001.
48. Forrester, JW, System dynamics, systems thinking, and soft OR. *System Dynamics Review*, 1994. 10(2-3): p. 245-256.
49. Lane, DC and Oliva, R, The greater whole: Towards a synthesis of system dynamics and soft systems methodology. *European Journal of Operational Research*, 1998. 107(1): p. 214-235.
50. Mingers, J and Rosenhead, J, Problem structuring methods in action. *European Journal of Operational Research*, 2004. 152(3): p. 530-554.
51. Iivari, J and Hirschheim, R, Analyzing information systems development: A comparison and analysis of eight IS development approaches. *Information systems*, 1996. 21(7): p. 551-575.
52. Quinn, MJ, *Ethics for the information age*. Pearson/Addison-Wesley Boston, 2005.
53. Hiller, JS and Belanger, F, Privacy strategies for electronic government. *E-government*, 2001. 200: p. 162-198.
54. Hilton, J, Burnap, P, and Tawileh, A. *Methods for the identification of Emerging and Future Risks*. Management Working Group,European Network and Information Security Agency (ENISA) 2007.
55. Tawileh, A and Mcintosh, S. Understanding Information Assurance: A Soft Systems Approach. in *In the Proceedings of the 11th International Conference United Kingdom Systems Society* Oxford University, 2010.
56. Wright, C, et al., A Framework for Resilience Thinking. *Procedia Computer Science*, 2012. 8(0): p. 45-52.
57. Rose, J and Haynes, M, A Soft Systems Approach to Evaluation for Complex Interventions in the Public Sector. *Journal of Applied Management Studies*, 1999: p. 199-216.
58. Checkland, P and Scholes, J, *Soft Systems Methodology in Action*. Chichester: Wiley, 1991.
59. Winter, MC, Brown, DH, and Checkland, PB, A role for soft systems methodology in information systems development. *European Journal of Information Systems*, 1995. 4(3): p. 130-142.
60. *e-Government Strategy Framework Policy and Guidelines: Registration & Authentication Framework v3.0*. Office of e-Envoy,Cabinet Office: UK, 2002. Available from:

http://webarchive.nationalarchives.gov.uk/20040722031653/http://e-government.cabinetoffice.gov.uk/assetRoot/04/00/09/60/04000960.pdf.
61. Lee, J and Rao, HR. Citizen centric analysis of anti/counter-terrorism e-government services. in *Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains*. Philadelphia, Pennsylvania, 2007.
62. Davison, RM, Wagner, C, and Ma, LCK, From government to e-government: a transition model. *Information Technology & People*, 2005. 18(3): p. 280-299.
63. Dawes, SS, Pardo, TA, and Cresswell, AM, Designing electronic government information access programs: a holistic approach. *Government Information Quarterly*, 2004. 21(1): p. 3-23.
64. Janssen, M, Kuk, G, and Wagenaar, RW. A survey of e-government business models in the Netherlands. in *Proceedings of the 7th international conference on Electronic commerce*. ACM, 2005.
65. Vassilakis, C, et al., A framework for managing the lifecycle of transactional e-government services. *Telematics and Informatics*, 2003. 20(4): p. 315-329.
66. Whitson, TL and Davis, L, Best practices in electronic government: Comprehensive electronic information dissemination for science and technology. *Government Information Quarterly*, 2001. 18(2): p. 79-91.
67. Reddick, CG, A two-stage model of e-government growth: Theories and empirical evidence for U.S. cities. *Government Information Quarterly*, 2004. 21(1): p. 51-64.
68. Layne, K and Lee, J, Developing fully functional E-government: A four stage model. *Government Information Quarterly*, 2001. 18(2): p. 122-136.
69. Symond, M, Government and the internet: no gain without pain. *The Economist*, 2000. 355: p. 9-14.
70. Coursey, D and Norris, DF, Models of E-Government: Are They Correct? An Empirical Assessment. *Public Administration Review*, 2008. 68(3): p. 523-536.
71. Brown, MM and Brudney, JL. Achieving advanced electronic government services: An examination of obstacles and implications from an international perspective. in *National Public Management Research Conference*. Bloomington, 2001.
72. Evans, D and Yen, DC, E-government: An analysis for implementation: Framework for understanding cultural and social impact. *Government Information Quarterly*, 2005. 22(3): p. 354-373.
73. Makolm, J. A Holistic Reference Framework for e-Government: The Practical Proof of a Scientific Concept. in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences - Volume 04*. 2006.
74. Dawes, SS. Governance in the information age: a research framework for an uncertain future. in *Proceedings of the 2008 international conference on Digital government research*. Digital Government Society of North America, 2008.
75. Centeno, C, Bavel, Rv, and Burgelman, J-C, A Prospective View of e-Government in the European Union. *The Electronic Journal of e-Government*, 2005. 3(2): p. 59-66.
76. OECD. *E-government: Analysis Framework and Methodology*. 2001.
77. Saxena, KBC, Towards excellence in e-governance. *International Journal of Public Sector Management*, 2005. 18(6): p. 498-513.
78. Relyea, HC, E-gov: Introduction and overview. *Government information quarterly*, 2002. 19(1): p. 9-35.
79. Grant, G and Chau, D, Developing a generic framework for e-government. *Advanced Topics in Information Management*, 2006. 5: p. 72-94.
80. Kolsaker, A and Lee-Kelley, L, Citizens' attitudes towards e-government and e-governance: a UK study. *International Journal of Public Sector Management*, 2008. 21(7): p. 723-738.
81. Tolley, A and Mundy, D, Towards workable privacy for UK e-government on the web. *IJEG*, 2009. 2(1): p. 74-88.

82. NIST. *Electronic Authentication Guideline* National Institute for Standards and Technology (NIST), U.S. Department of Commerce: U.S, 2006, [15-07-2014]. Available from: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf,
83. NIST. *Electronic Authentication Guideline*, National Institute for Standards and Technology ,U.S. Department of Commerce: US, 2013. Available from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf,
84. Nenadic, A, et al. Levels of Authentication Assurance: an Investigation. in *Third International Symposium on Information Assurance and Security (IAS)*. 2007.
85. Sánchez, M, et al., Levels of Assurance and Reauthentication in Federated Environments, in *Public Key Infrastructure*, S. Mjølsnes, S. Mauw, and S. Katsikas, Editors., Springer Berlin Heidelberg, 2008. p. 89-103.
86. OECD. *Electronic Authentication and OECD Guidance for Electronic Authentication*, OECD, 2007, [15-07-2014]. Available from: http://www.oecd.org/internet/ieconomy/38921342.pdf,
87. Avison, DE and Taylor, V, Information systems development methodologies: a classification according to problem situation. *Journal of Information technology*, 1997. 12(1): p. 73-81.
88. AGIMO. *National e-Authentication Framework*. Australian Government Information Management Office, Department of Finance and Deregulation: Australia, 2009, [15-07-2014]. Available from: http://www.finance.gov.au/files/2012/04/NeAF-BPG-vol4.pdf.
89. *A Pan-Canadian Strategy for Identity Management and Authentication, Final Report*. Inter-Jurisdictional Identity Management Task Force,Canadian Government: Canada, 2007, [15-07-2014].
90. NRC, *Information Technology Research, Innovation, and E-Government*. National Research Council ,The National Academies Press, 2002.
91. *Guide to Authentication Standards for Online Sevices*, State Services Commission,Crown Copyright ©: New Zealand 2006, [15-07-2014]. Available from: http://ict.govt.nz/assets/Uploads/Documents/egif-guide-to-authentication-standards-june-2006.pdf,
92. *Security,e-Government Strategy Framework Policy and Guidelines v4*. Office of e-Envoy,Cabinet Office: UK, 2002.
93. Kenning, M, Security management standard—iso 17799/bs 7799. *BT Technology Journal*, 2001. 19(3): p. 132-136.
94. *Principles for Electronic Authentication*. Authentication Principles Working Group,Industry Canada: Canada, 2004, [15-07-2014]. Available from: https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/authentication.pdf/$file/authentication.pdf.
95. *Pan-Canadian Assurance Model*. Assurance, Identity and Trust Working Group: Canada, 2010, [15-07-2014]. Available from: http://www.iccs-isac.org/en/km/transformative/docs/Pan-Canadian%20Assurance%20Model.PDF.
96. *Guideline on Defining Authentication Requirements*. Treasury Board of Canada Secretariat: Canada, 2012, [15-07-2014]. Available from: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262&section=text.
97. Framework for the Management of Risk. Treasury Board of Canada Secretariat: Canada, 2010. Available from: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text.
98. Standard on Identity and Credential Assurance. Treasury Board of Canada Secretariat: Canada, 2013. Available from: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776&section=text.
99. *Authentication for e-government Best Practice Framework for Authentication*. State Services Commission: New Zealand, 2004, [15-04-2014]. Available from:

http://www.jipdec.or.jp/archives/PKI-J/shiryou/e-auth_policy/NZ_Framework_E.pdf.
100. McDonagh, M, E-Government in Australia: the Challenge to Privacy of Personal Information. *International Journal of Law and Information Technology*, 2002. 10: p. 327-343.
101. Warren, SD and Brandeis, LD, The Right to Privacy. *Harvard Law Review*, 1890. 4(5): p. 193.
102. Byrne, E, Privacy. *Encyclopedia of applied ethics*, 1998. 3: p. 649–659.
103. Parker, RB, A Definition of privacy. *Rutgers L. Rev.*, 1973. 27: p. 275.
104. OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD 2013. Available from: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm,
105. *Privacy Act of 1974*. Department of Justice,US Government: US, 1974, [15-07-2014]. Available from: http://www.archives.gov/about/laws/privacy-act-1974.html.
106. *Data Protection Act 1998*. UK Government: UK, 1998, [15-07-2014]. Available from: http://www.legislation.gov.uk/ukpga/1998/29/contents.
107. *Proposal for a Regulation of The European Parliament and of the Council*. European Commission Brussels,, 2012, [15-07-2014]. Available from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
108. Hammami, W, et al., Toward a Privacy Enhancing Framework in E-government.
109. McCallister, E, Grance, T, and Scarfone, KA. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),SP 800-122*. NIST,Us Department of Commerce: US, 2010.
110. *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks Guidelines*. Treasury Board of Canada Secretariat: Canada, 2012, [15-07-2014]. Available from: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12451&section=text.
111. *Privacy Impact assessment Guide*. Office of the Australian Information Commissioner, Australian Government: Australia, 2010, [15-07-2015]. Available from: http://www.oaic.gov.au/privacy/privacy-archive/privacy-resources-archive/privacy-impact-assessment-guide.
112. APEC, *Apec privacy framework*. Asia Pacific Economic Cooperation Secretariat, 2005.
113. BSI. *Privacy Framework*, BSI, 2011. Available from: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45123,
114. West, DM, WMRC global e-government survey, October, 2001. *Taubman Center for Public Policy, Brown University*, 2001.
115. Fink, A, *The survey handbook*. Vol. 1. Sage, 2003.
116. Treadwell, D, Surveys :Putting numbers into opinions, in *Introducing communication research: Paths of inquiry*. Sage, 2013. p.
117. Fink, A, *How to Design Surveys, The Survey Kit*, London, Sage.1995.
118. Fink, A, *How to analyze survey data*. Vol. 8. Sage, 1995.
119. Seltman, HJ, *Experimental design and analysis*. UK: Carnegie and Mellon University, 2014.
120. *Saudi Census Report*. Central Department of Statistics and Information, Saudi Government, 2012, [15-07-2015]. Available from: http://www.cdsi.gov.sa/english/.
121. *2011 Census: Key Statistics for England and Wales*. Office for National Statistics,UK Government, 2012, [15-07-2014]. Available from: http://www.ons.gov.uk/ons/rel/census/2011-census/key-statistics-for-local-authorities-in-england-and-wales/stb-2011-census-key-statistics-for-england-and-wales.html.

122. *Census 2010 Final Results* National Center for Statistics and Information, Oman Government: Oman, 2010, [15-07-2014]. Available from: http://www.ncsi.gov.om/NCSI_website/documents/Census_2010.pdf.
123. Longnecker, M and Ott, R, An introduction to statistical methods and data analysis*. ISBN-13*, 2001. 854576151.
124. Freeman, RE, *Strategic management: A stakeholder approach*. Cambridge University Press, 2010.
125. Flak, LS and Rose, J, Stakeholder governance: Adapting stakeholder theory to e-government*. Communications of the Association for Information Systems*, 2005. 16(1): p. 31.
126. Flak, LS and Nordheim, S. Stakeholders, contradictions and salience: An empirical study of a Norwegian G2G effort. in *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*. IEEE, 2006.
127. Tan, C-W, Pan, SL, and Lim, ET, Managing stakeholder interests in e-government implementation: Lessons learned from a Singapore e-government project*. Journal of Global Information Management (JGIM)*, 2005. 13(1): p. 31-53.
128. Lamsweerde, AV, *Engineering requirements for system reliability and security*. Nato Security Through Science Series D-Information and Communication Security, ed. Manfred Broy, Johannes Grünbauer, and Tony Hoare. Vol. 9. IOS Press, 2007. 196-238.
129. NIST. *Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST,U.S. Department of Commerce, 2008. Available from: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf,
130. Office, C. *Government Security Classifications*. UK Government, 2014. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf.
131. Markiewicz, D. *Guidelines for Data Classification*. Carnegie Mellon University, 2011. Available from: http://www.cmu.edu/iso/governance/guidelines/data-classification.html.
132. Carter, AB, *The philosophical foundations of property rights*. Harvester, Wheatsheaf, 1989.
133. Harris, JW, *Property and justice*. Oxford University Press, 1996.
134. Hart, D, Ownership as an Issue in Data and Information Sharing: a philosophically based review*. Australasian Journal of Information Systems*, 2007. 10(1).
135. Barker, K, et al., A data privacy taxonomy, in *Dataspace: The Final Frontier*. Springer, 2009. p. 42-54.
136. Donzelli, P and Bresciani, P. Goal-oriented requirements engineering: a case study in e-government. in *Advanced Information Systems Engineering*. Springer, 2003.
137. Mouratidis, H and Giorgini, P, Secure tropos: a security-oriented extension of the tropos methodology*. International Journal of Software Engineering and Knowledge Engineering*, 2007. 17(02): p. 285-309.
138. Elahi, G and Yu, E, A Goal Oriented Approach for Modeling and Analyzing Security Trade-Offs, in *Conceptual Modeling - ER 2007*, C. Parent, et al., Editors., Springer Berlin Heidelberg, 2007. p. 375-390.
139. Ali, M, Weerakkody, V, and El-Haddadeh, R. The Impact of National Culture on E-Government Implementation: A Comparison Case Study. in *In Proceedings of the Fifteenth Americas Conference on Information Systems*. San Francisco, California, 2009.
140. Akkaya, C, Wolf, P, and Krcmar, H. Factors Influencing Citizen Adoption of E-Government Services: A Cross-Cultural Comparison (Research in Progress). in *the 45th Hawaii International Conference on System Science (HICSS)*. 2012.

141. Prado-Lorenzo, J-M, García-Sánchez, I-M, and Cuadrado-Ballesteros, B, Sustainable cities: do political factors determine the quality of life? *Journal of Cleaner Production*, 2012. 21(1): p. 34-44.
142. Alomari, MK, Sandhu, K, and Woods, P, Measuring social factors in e-government adoption in the Hashemite Kingdom of Jordan*. International Journal of Digit Society (IJDS)*, 2010. 1(2): p. 163-172.
143. Ford, DP, Connelly, CE, and Meister, DB, Information systems research and Hofstede's culture's consequences: an uneasy and incomplete partnership*. IEEE Transactions on Engineering Management*, 2003. 50(1): p. 8-25.
144. Haley, CB, et al., Security requirements engineering: A framework for representation and analysis*. IEEE Transactions on Software Engineering*, 2008. 34(1): p. 133-153.
145. Yu, ES. Towards modelling and reasoning support for early-phase requirements engineering. in *Proceedings of the Third IEEE International Symposium on Requirements Engineering*. IEEE, 1997.
146. Massacci, F, Prest, M, and Zannone, N, Using a security requirements engineering methodology in practice: The compliance with the Italian data protection legislation*. Computer Standards & Interfaces*, 2005. 27(5): p. 445-455.
147. Kalloniatis, C, Kavakli, E, and Gritzalis, S, Designing Privacy Aware Information Systems*. Software Engineering for Secure Systems: Industrial and Research Perspectives*, 2011: p. 212-231.
148. Fabian, B, et al., A comparison of security requirements engineering methods*. Requirements engineering*, 2010. 15(1): p. 7-40.
149. Asnar, Y, et al. From trust to dependability through risk analysis. in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*. IEEE, 2007.
150. Makedon, F, et al., A Safe Information Sharing Framework for E-Government Communication*. IT white paper from Boston University*, 2003.

Appendices

Appendix A : A CM relevant to the concept Government (RDs)

List of Root Definitions (RDs):

RD1- Core Transformation (T1)

-- A system to achieve an agreed "common good" for a nation within internationally defined boundaries by instituting the necessary structures and institutions to deliver approved policies and achieve appropriate targets while constrained by political views, common beliefs, and principles.

RD2- Core Transformation (T2)

A system to ensure the survival and protection of a nation welfare and strategically valuable resources and assets by taking responsibilities of detecting, deterring and defending as appropriate against externally and internally arising threats while considering performing necessary security measures through established structures and institutions and within constraints of relevant international agreements.

RD3- Core Transformation (T3)

-- A system to deliver those services, which are deemed to be most effectively and efficiently performed for the benefit of all the nation's people by determining the balance of advantage between public and private provision of the services, or a mixture of these while considering the needs and expectations of all the nation's people and within constraints of cultural and economic influences.

RD4- Linking System (L1)

-- A system to undertake the communication between the established structures and institutions and their customers by enabling all different eligible customers to participate and engage in democratic dialogues and in policy design and decision making concerning subjects and issues that affect their lives while considering responding to customers' requests and complaints in order to satisfy their needs and expectations and to present a favorable image of the state , at the minimum cost possible and using a diversity of reliable, easy to use and accessible channels while preserving rights of fairness, equality, security and privacy and constrained with political, ethical and social responsibilities.

RD5- Linking System (L2)

-- A system to determine current and potential threats on the nation welfare from internal or external sources by assembling comprehensive and current intelligence about those sources while undertaking the assessment of the options available to prevent these threats within constraints of relevant international agreements.

RD6- Linking System (L3)

-- A system to undertake the relationships between the established structures and institutions by establishing communication channels between these structures and institutions to enable their communication and the exchange of expertise in the development and delivery of services in order to use available resources effectively and efficiently.

RD7- Linking System (L4)

-- A system to undertake the enforcement of policies, regulations, and laws by exercising authority and power to monitor the behavior and response of all involved parties against them and apply the suitable penalties when necessary while educating and raising the public awareness about those policies,

regulations and laws that concern them with consideration of common principles, believes, and people rights of security and privacy.

RD8- Support system (S1)

-- A system to ensure that the human resources available to different established structures and institutions match the requirements of all activities carried out by those establishments in both the long and short term, through the recruitment of personnel with proper capabilities and the acquisition while considering the operation of proper training and education programs for developing current personnel skills in order to balance personnel needs and expectations with established structures' and institutions' requirements.

RD9- Support system (S2)

-- A system to ensure that the physical resources available match the requirements of all established structures' and institutions' activities, by developing the required infrastructures while exploiting latest developments in relevant technology and reflecting related "best practice" as means of enhancing overall performance of established structures and institutions, but recognising appropriate standards ,technical, financial and environmental constraints.

RD10- Support system (S3)

-- A system to match the finances available to the established structures' and institutions' needs by gathering required funds from a variety of available sources and setting a detailed budget plan for allocating the required fund for each established structure and institution within constraints of available funds, strategic plans and political views.

RD11- Support system (S4)

-- A system to develop a current knowledge base to support all activities by assembling relevant intelligence and knowledge about the latest developments in related fields and learning from similar previous experiences while considering making relevant information available as needed and providing the source for reporting as required with respect to data protection and security constraints.

RD12- Planning, Monitoring, and Control system (PMC1)

-- A system owned by a nation, operated by an empowered body of people, to undertake the strategic planning processes for the established structures and institutions by enabling those structures and institutions to derive their strategic plans and targets and to implement these plans in order to carry out their activities in a way that meets the changing needs and expectations of the nation and the dynamic changes in political, social and economic environments with a performance that achieves the defined targets of each established structure and institution, but acting with constraints of finance , available resources, political views and the need to continually improve overall performance.

RD13- Planning, Monitoring, and Control system (PMC2)

-- A system to achieve an agreed "common good" for a "nation" by defining a set of regulations, policies and legislations relevant to the achievement of common good and to the protection and survival of the nation that guide the operation and maintenance of services by the established structures and institutions while constrained by the nation's common beliefs and principles.

RD14- Planning, Monitoring, and Control system (PMC3)

-- A system owned by the nation, operated by an independent body of people, to monitor and control the activities carried out by the established structures and institutions through assessing the performance of the current activities according to defined measures that comply with relevant standards and the needs and expectations of the nation and take required actions when needed under constraints of available resources, and relevant regulations, policies and legislations.

Appendix B : A Gap Analysis of Authentication Frameworks

The symbol ✓ to indicate that the framework had all the activities that satisfied the criteria, ☑ symbol indicates that the framework had most of the activities that partially satisfied the criteria, ☒ symbol indicates that the framework had few activities that satisfy the criteria but with no much details and that the criteria was partially not satisfied, and × symbol indicates the absence of an activity from the framework and that the criteria was not satisfied at all.

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
1.	Decide on how to determine dynamic changes in the needs and expectations of the government and its customers	Change Management (ChMgt)	×	×	×	×	×
2.	Consider Dynamic changes	(ChMgt)	×	×	×	×	×
3.	Take control action to ensure that dynamic changes in the needs and expectations of the government and its customers are considered	(ChMgt)	×	×	×	×	×
4.	Decide on how to undertake the communication between the government and its customers	Communication Management (CommMgt)	☑	☑	☑	✓	☑
5.	Assess the communication between government and its customer	CommMgt	☑	☑	☑	☑	×
6.	Take control action to ensure that the communication between the government and its customers are undertaken in a way that meets their needs and expectations	CommMgt	☑	☒	☑	☑	×
7.	Decide on how to define (set of terms)	Consensus Building (ConsB)	☑	☑	☑	☑	☑
8.	Define genuineness	(ConsB)	✓	✓	✓	✓	✓
9.	Define eligible	(ConsB)	✓	✓	✓	✓	✓
10.	Define accessible	(ConsB)	✓	✓	✓	✓	✓
11.	Define accountable	(ConsB)	✓	✓	✓	✓	✓
12.	Define reliable	(ConsB)	☑	×	☑	☑	×
13.	Assess the definition of set (of terms)	(ConsB)	×	×	×	×	×
14.	Take control action to ensure the(set of terms) are defined	(ConsB)	×	×	×	×	×
15.	Define useful	(ConsB)	☑	☑	☑	☑	☑
16.	Define appropriate	(ConsB)	☑	☑	☑	☑	☑
17.	Define dynamic	(ConsB)	☒	☑	☑		☒

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
18.	Determine technical , financial constraints	Constraints Management(ConstrMgt)	×	×	×	×	×
19.	Determine desired ease of use	(ConstrMgt)	☒	×	☒	×	☒
20.	Determine flexibility	(ConstrMgt)	☒	☒	☒	☒	☒
21.	Assess the impact of the constraints on all activities	(ConstrMgt)	×	×	×	×	×
22.	Decide on how to react	(ConstrMgt)	×	×	×	×	×
23.	Notify impact to controllers	(ConstrMgt)	×	×	×	×	×
24.	Monitor conformance	(ConstrMgt)	☑	☑	☑	☒	☒
25.	Take control action to ensure the conformance of the activities with constraints	(ConstrMgt)	☒	☒	☒	☒	☒
26.	Determine security constraints	(ConstrMgt)	☑	☑	☑	☑	☑
27.	Assess the impact of data protection and security on each activity	(ConstrMgt)	✓	✓	✓	✓	✓
28.	know about standards and guidelines	(ConstrMgt)	✓	✓	✓	✓	✓
29.	Determine how relevant the standards and guidelines	(ConstrMgt)	✓	✓	✓	✓	✓
30.	Assess the compliance of rules and means of establishing a required level of confidence with relevant standards and guidelines	(ConstrMgt)	☑	☑	☑	☑	☒
31.	Take control action to ensure that the activities of establishing the required level of confidence comply with relevant standards	(ConstrMgt)	☑	☑	☑	☑	☒
32.	Determine available finance , resources	(ConstrMgt)	☒	×	×	×	×
33.	Determine current legislations and policies	(ConstrMgt)	✓	☑	✓	✓	✓
34.	Determine available technologies	(ConstrMgt)	☑	☑	☑	☑	☑
35.	Assemble knowledge about the social, cultural, legal and political impacts	(ConstrMgt)	×	×	×	×	×
36.	Assess the impact of current legislations and policies	(ConstrMgt)	☑	☒	☑	☑	×
37.	Assess the impact of relevant standards on each activity	(ConstrMgt)	☑	☒	☑	☑	×
38.	Assess the impact of available finance, resources and technologies	(ConstrMgt)	☒	×	×	×	×
39.	Assess the impact of environmental factors (social, cultural, legal, political)	(ConstrMgt)	×	×	×	×	×
40.	Assemble activity constraints information	(ConstrMgt)	×	×	×	×	×
41.	Monitor conformance	(ConstrMgt)	☑	☒	☒	☑	☒
42.	Take control action to ensure ease of use and customers rights of privacy are maintained	(ConstrMgt)	☒	☒	☒	☒	☒

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
43.	Take control action to ensure that environmental impacts are considered	(ConstrMgt)	×	×	×	×	×
44.	Take control action to ensure the compliance of activities with relevant standards and guidelines as possible	(ConstrMgt)	☒	☒	☒	☒	☒
45.	Identify possible contingency situations	Contingency Planning (ContigP)	☒	☒	×	☒	×
46.	Determine alternatives for the current verification means to establish a required level of confidence in a contingency situation	(ContigP)	×	×	×	×	×
47.	Assess the availability of alternative means on contingency situations	(ContigP)	×	×	×	×	×
48.	Decide on alternative means for contingency situations	(ContigP)	×	×	×	×	×
49.	Monitor the selection of alternative means	(ContigP)	×	×	×	×	×
50.	Take control action to ensure alternative means for establishing a level of confidence are available in contingency situations	(ContigP)	×	×	×	×	×
51.	Define a contingency situation	(ContigP)	☒	☒	×	☒	×
52.	Identify areas where participation of customers is relevant and appropriate	Customers' Participation Management (CosPMgt)	☒	☒	☒	☒	×
53.	Decide on how to enable government's customer participation in decision making and policy design	(CosPMgt)	☒	☒	☒	☒	×
54.	Enable customers' participation	(CosPMgt)	☒	☒	☒	☒	×
55.	Monitor the enabling of customers' participation	(CosPMgt)	☒	☒	☒	☒	×
56.	Ensure that customers' participation is enabled where relevant and appropriate	(CosPMgt)	☒	☒	☒	☒	×
57.	Identify the set of definitions , rules and means of verification to be communicated to government's customer	Environment Shaping Management (EnvShMgt)	☑	☒	☑	☒	☒
58.	Determine measures for awareness	EnvShMgt)	☒	☒	☒	☒	☒
59.	Determine measures for acceptance	EnvShMgt)	☒	☒	☒	☒	☒
60.	Consider diversity in the needs and expectations of customers	EnvShMgt)	☒	☒	☑	☒	☒

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
61.	Decide on how to use communication for raising awareness and acceptance of rules and means of verification.	EnvShMgt)	☒	☒	☑	☒	☒
62.	Decide on how to communicate rules and means of verification to the government's customers	EnvShMgt)	☒	☒	☒	☒	☒
63.	Communicate the rules and means to government's customers	EnvShMgt)	☒	☒	☑	☒	☒
64.	Monitor communicating rules and means of protection to customers	EnvShMgt)	×	×	☒	×	×
65.	Take control action to ensure that communicating rules and means of verification to customers is done	EnvShMgt)	☒	☒	☒	☒	☒
66.	Assess government's customers' awareness and acceptance of the verification rules and means.	EnvShMgt)	☒	☒	☑	☒	☒
67.	Take control action to ensure that communicating rules and means of verification to government's customers have raised awareness and acceptance of these rules and means	EnvShMgt)	☒	×	☑	×	×
68.	Decide on how to identify expectations and needs of both the government and its customers	Expectation and Needs Management (ExpectNMgt)	☑	☒	☑	☑	☒
69.	Identify expectations and needs of both government and government customers	(ExpectNMgt)	☑	☒	☑	☑	☒
70.	Assess the identification of the needs and expectations	(ExpectNMgt)	☒	☒	☒	☒	☒
71.	Take control action to ensure that the expectations and needs are identified	(ExpectNMgt)	☒	☒	☒	☒	☒
72.	Determine government and its customers communication expectations and needs	(ExpectNMgt)	☒	☒	☒	☒	☒
73.	Decide on how to assess the needs and expectations of the government and its customers.	(ExpectNMgt)	☑	☒	☑	☑	☒
74.	Assess the needs and expectations of the government and its customers.	(ExpectNMgt)	☑	☑	☑	☑	☑
75.	Take control action to ensure that the needs and expectations of the government and its customers are assessed.	(ExpectNMgt)	☒	☒	☒	☒	☒
76.	Define empowered staff	Human Resources Management (HRMgt)	☒	☒	☒	☒	☒

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
77.	Identify government authorities with capabilities to run the system activities	(HRMgt)	☑	☒	☑	☑	☑
78.	Determine activities requirements of human resources	(HRMgt)	×	×	×	×	×
79.	Decide on how to assess the achievement of ensuring the availability of required human resources for each activity	(HRMgt)	×	×	×	×	×
80.	Assess the achievement of ensuring the availability of required human resources for each activity	(HRMgt)	×	×	×	×	×
81.	Take control action to ensure that required human resources are available to the satisfaction of governments' needs and expectations	(HRMgt)	×	×	×	×	×
82.	Define roles and responsibilities relevant to system's activities	(HRMgt)	×	×	×	×	×
83.	Identify required skills and capabilities for satisfying those requirements	(HRMgt)	×	×	×	×	×
84.	Identify current recruited personnel with the proper capabilities	(HRMgt)	×	×	×	×	×
85.	Recruit personnel with proper capabilities as appropriate and needed	(HRMgt)	×	×	×	×	×
86.	Allocate personnel with proper capabilities to the activities requirements	(HRMgt)	×	×	×	×	×
87.	Assess the allocation of personnel to the identified requirements	(HRMgt)	×	×	×	×	×
88.	Take control action to ensure that personnel with proper capabilities were allocated to the identified requirements	(HRMgt)	×	×	×	×	×
89.	Identify current personnel skills that needs developments	(HRMgt)	×	×	×	×	×
90.	Determine the training needs for current personnel	(HRMgt)	×	×	×	×	×
91.	Define training and education programs for the identified needs and skills	(HRMgt)	×	×	×	×	×
92.	Determine how to provide the training and education programs	(HRMgt)	×	×	×	×	×
93.	Take necessary actions to provide training and education programs for developing personnel skills	(HRMgt)	×	×	×	×	×
94.	Monitor the provision of training and education programs	(HRMgt)	×	×	×	×	×
95.	Take control action to ensure that the provision of training and education programs is done.	(HRMgt)	×	×	×	×	×
96.	Decide on how to operate means of verification assigned to each level of confidence	Implementation of Rules & Development plans (ImplRDevP)	✓	✓	✓	✓	✓

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
97.	Operate selected means of verification assigned to each level of confidence	ImplRDevP)	✓	✓	✓	✓	✓
98.	Assess the operation of selected verification means	(ImplRDevP)	☑	☑	☑	☑	☑
99.	Take control action to ensure the operation of verification means at each required level of confidence		☑	☑	☑	☑	☑
100.	Decide on how to apply selected technical solutions aligned with relevant rules	(ImplRDevP)	✓	✓	☑	☑	☑
101.	Apply selected technical solutions	ImplRDevP)	✓	✓	✓	✓	✓
102.	Monitor the application of selected technical solutions	(ImplRDevP)	☑	☑	☑	☑	☑
103.	Take control action to ensure technical solutions aligned with relevant defined rules are applied	(ImplRDevP)	☑	☑	☑	☑	☑
104.	Determine activities requirements of relevant knowledge	Knowledge Base and learning Management (KBLMgt)	×	×	×	×	×
105.	Define comprehensive	(KBLMgt)	×	×	×	×	×
106.	Define current	(KBLMgt)	×	×	×	×	×
107.	Decide on how to develop and maintain a current knowledge base	(KBLMgt)	☒	☒	☒	☒	☒
108.	Assess the development and maintenance of current knowledge base	(KBLMgt)	×	×	×	×	×
109.	Take control action to ensure that the knowledge base is developed and maintained is current and meets all activities requirements	(KBLMgt)	×	×	×	×	×
110.	Determine relevant sources for required knowledge and intelligence	(KBLMgt)	☒	☒	☒	☒	☒

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
111.	Identify latest developments in the means of verification and validation of an assertions' genuineness and the eligibility of a claimer.	(KBLMgt)	☒	☒	☒	☒	☒
112.	Identify relevant developments to the establishment of a required level of confidence	(KBLMgt)	☑	☑	☑	☑	☒
113.	Assemble required knowledge and intelligence about latest developments	(KBLMgt)	☒	☒	☒	☒	☒
114.	Define best practice	(KBLMgt)	☒	☒	☒	☒	☒
115.	Identify relevant 'best practices'	(KBLMgt)	☒	☒	☒	☒	☒
116.	Determine lessons learned from the identified relevant 'best practices'	(KBLMgt)	☒	☒	☒	☒	☒
117.	Assess the assembling of knowledge and learning processes	(KBLMgt)	×	×	×	×	×
118.	Take control actions to ensure the assembling of relevant knowledge and learning processes are done	(KBLMgt)	×	×	×	×	×
119.	Decide on how to assess the establishment of the required level of confidence in an assertion genuineness	Overall Performance Control(OPerfC)	☑	☑	☑	✓	☑
120.	Assess the establishment of the required level of confidence in an assertion genuineness	(OPerfC)	✓	✓	✓	✓	✓
121.	Take control action to ensure that the establishment of the required level of confidence in an assertion genuineness is done and meets the needs and expectations of both the government and its customers	(OPerfC)	✓	✓	✓	✓	✓
122.	Determine government performance expectations	(OPerfC)	☑	☑	☑	✓	☑
123.	Determine performance measures	(OPerfC)	✓	✓	✓	✓	✓
124.	Monitor the performance of the establishment of a required level of confidence	(OPerfC)	✓	✓	✓	✓	✓
125.	Take control action to ensure that the performance achieve the government's expectations	(OPerfC)	☑	☑	☑	☑	☑
126.	Decide on how to assess the activities of establishing the required level of confidence in an assertion's genuineness or the eligibility of a claimer	(OPerfC)	☒	☒	☒	☑	☒
127.	Assess the activities of establishing the required level of confidence	(OPerfC)	☑	☑	☑	☑	☑
128.	Take control action to ensure the activities are carried out according to the needs and expectations of both the government and its customers	(OPerfC)	☒	☒	☒	☒	☒
129.	Identify systems activities to be monitored	(OPerfC)	☑	☑	☑	☑	☑
130.	Decide on how to monitor activities	(OPerfC)	☑	☑	☑	☑	☑

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
131.	Monitor system activities	(OPerfC)	☑	☑	☑	✓	☑
132.	Determine needed actions	(OPerfC)	☑	☒	☒	☑	☑
133.	Decide on when and where to take the identified needed actions	(OPerfC)	☑	☒	☒	☑	☑
134.	Take required actions when and where needed	(OPerfC)	☑	☑	☑	☑	☑
135.	Assess the monitoring and action taking processes	(OPerfC)	☒	☒	☒	☒	☒
136.	Take control action to ensure the monitoring and actions taken are done	(OPerfC)	☒	☒	☒	☒	☒
137.	Determine activities requirements of Physical resources	Physical Resources Management (PhRMgt)	☒	☒	☒	☒	☒
138.	Decide on how to assess the achievement of ensuring the availability of required Physical resources for each activity	(PhRMgt)	☒	☒	☒	☒	☒
139.	Assess the achievement of ensuring the availability of required Physical resources for each activity	(PhRMgt)	☒	☒	☒	☒	☒
140.	Take control action to ensure that required Physical resources are available to the satisfaction of activities' requirements	(PhRMgt)	×	×	×	×	×
141.	Determine required infrastructures, hardware and software for each activity	(PhRMgt)	×	×	×	×	×
142.	Decide on how to develop and maintain required infrastructure, hardware and software for each activity	(PhRMgt)	×	×	×	×	×
143.	Develop required infrastructures	(PhRMgt)	×	×	×	×	×
144.	Monitor the development of infrastructure , hardware and software for each activity	(PhRMgt)	×	×	×	×	×
145.	Take control action to ensure that the required infrastructure hardware and software for each activity is developed and maintained	(PhRMgt)	×	×	×	×	×
146.	Determine customers rights of privacy	Privacy Compliance Management (PriComMgt)	✓	✓	✓	✓	✓
147.	Define anonymous	(PriComMgt)	☑	☑	☑	☑	☑
148.	Determine desired level of being anonymous	(PriComMgt)	☒	☒	☑	☑	☒

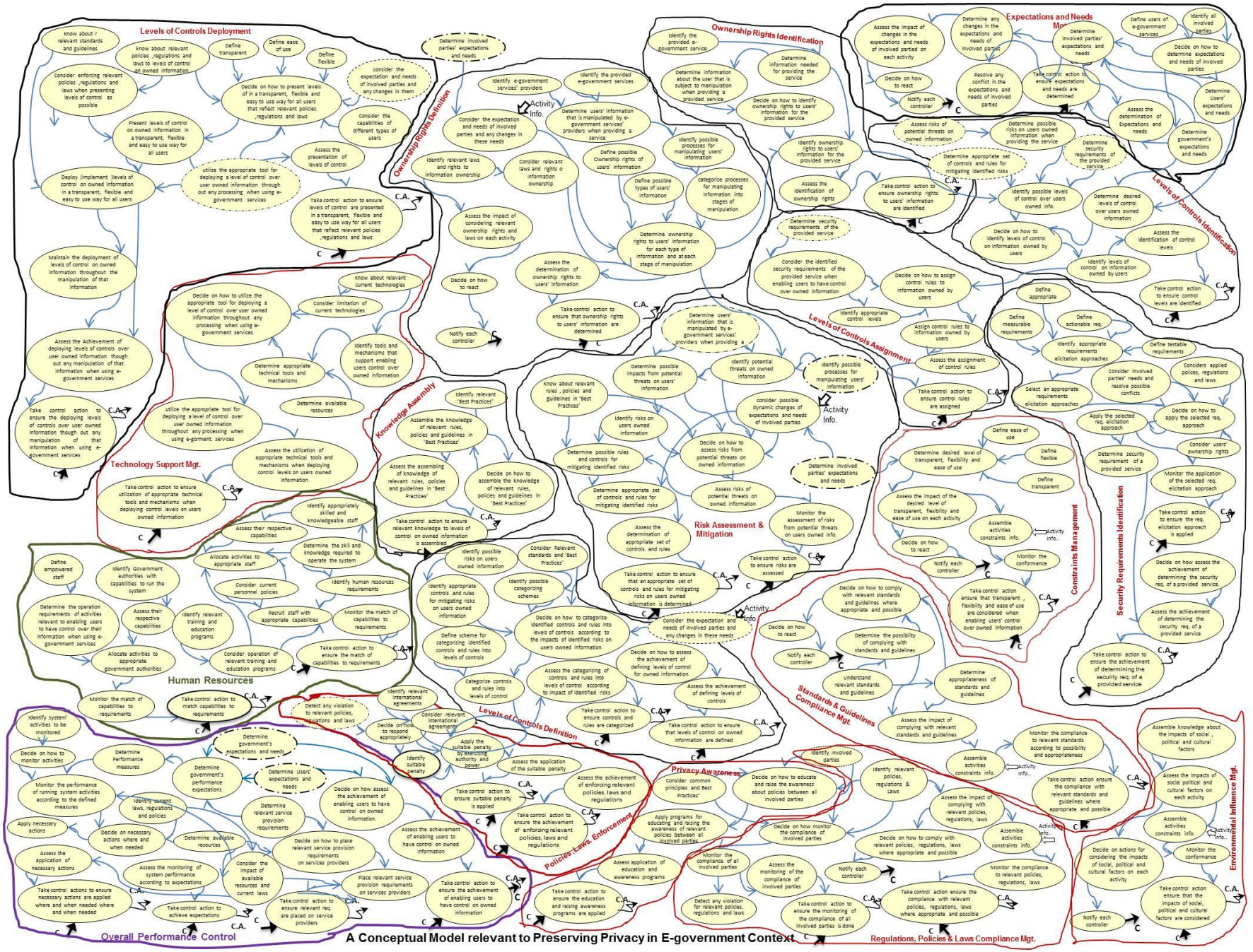
No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
149.	Determine appropriate situations where customers can remain anonymous	(PriComMgt)	☒	☑	☑	☑	☑
150.	Assess the impact of customers' privacy and being anonymous on each activity	(PriComMgt)	☑	☑	☑	☑	☑
151.	Decide on how to comply activities with privacy and the right to stay anonymous in appropriate situations	(PriComMgt)	☑	☒	☑	☑	☑
152.	Take necessary actions to ensure all activities comply with customers' rights of privacy and their rights to stay anonymous as appropriate	(PriComMgt)	☑	☒	☑	☑	☑
153.	Assemble activities constraints information	(PriComMgt)	☒	☒	☒	☒	☒
154.	Monitor the conformance of all activities with customers' rights of privacy and their rights to stay anonymous as appropriate	(PriComMgt)	☒	☒	☒	☒	☒
155.	Take control action to ensure the conformance of all activities with customers' rights of privacy and their rights to stay anonymous as appropriate	(PriComMgt)	☒	☒	☒	☒	☒
156.	Determine reliability, accountability and accessibility, appropriateness measures	Quality Management (QMgt)	☑	☑	☑	✓	☑
157.	Assess the reliability , accessibility ,and accountability appropriateness of the selected verification means	(QMgt)	☑	☑	☑	✓	☑
158.	Take control action to ensure that the selected means of verification are reliable, accountable, accessible and appropriate for establishing a required levels of confidence	(QMgt)	☑	☑	☑	✓	☑
159.	Determine reporting requirements	Reporting	×	×	×	×	×
160.	Decide on how to providing source for reporting	Reporting	×	×	×	×	×
161.	Provide reporting sources as required	Reporting	×	×	×	×	×
162.	Monitor the provision of reports	Reporting	×	×	×	×	×
163.	Take control action to ensure reporting is done as required	Reporting	×	×	×	×	×
164.	Identify actions in the context of e-government that require a level of confidence	(RAMgt)	✓	✓	✓	✓	✓
165.	Identify required levels of confidence for the identified actions in the context of e-government	(RAMgt)	✓	✓	✓	✓	✓

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
166.	Decide on how to determine the security requirements for each level of confidence	(RAMgt)	✓	✓	✓	✓	✓
167.	Determine security requirements for each level of confidence	(RAMgt)	✓	✓	✓	✓	✓
168.	Assess the determination of security requirements for each level of confidence	(RAMgt)	✓	✓	✓	✓	✓
169.	Take control action to ensure security requirements for each level of confidence are determined and reflect the needs and expectations of the government and its customers	(RAMgt)	✓	✓	✓	✓	✓
170.	Assemble knowledge about potential threats	(RAMgt)	✓	✓	✓	✓	✓
171.	Decide on how to assess risks associated with targeted resources and services	(RAMgt)	✓	✓	✓	✓	✓
172.	Assess risks associated from identified threats on targeted resources and services	(RAMgt)	✓	✓	✓	✓	✓
173.	Monitor the assessment of risks	(RAMgt)	✓	✓	✓	✓	✓
174.	Take control action to ensure that risks are assessed	(RAMgt)	✓	✓	✓	✓	✓
175.	Determine means of verification	Rules Formulation & Development Planning (RFDP)	✓	✓	✓	✓	✓
176.	Determine reliability, accountability and accessibility of current means of verification	(RFDP)	✓	✓	✓	✓	✓
177.	Determine appropriateness of means of verification	(RFDP)	✓	✓	✓	✓	✓
178.	Decide on how to select means of verification that are reliable, accountable, accessible and appropriate to establishing levels of confidence	(RFDP)	✓	✓	✓	✓	✓
179.	Select appropriate and useful means of verification	(RFDP)	✓	✓	✓	✓	✓
180.	Assess the selection of verification means	(RFDP)	✓	✓	✓	✓	✓
181.	Take control action to ensure that means of verification are selected as appropriate and useful.	(RFDP)	✓	✓	✓	✓	✓
182.	Identify different potential access channels	(RFDP)	✓	✓	✓	✓	✓
183.	Consider different potential access channels	(RFDP)	✓	✓	✓	✓	✓

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
184.	Determine appropriate verification means for different potential access channels	(RFDP)	✓	✓	✓	✓	✓
185.	Decide on how to assign selected means of verification to levels of confidence	(RFDP)	✓	✓	✓	✓	✓
186.	Assign selected means of verification to levels of confidence	(RFDP)	✓	✓	✓	✓	✓
187.	Assess the assignment of selected verification means to levels of confidence	(RFDP)	✓	✓	✓	✓	✓
188.	Take control action to ensure that means of verification are assigned to levels of confidence as appropriate and useful	(RFDP)	✓	✓	✓	✓	✓
189.	Determine technical solutions	(RFDP)	✓	✓	✓	✓	✓
190.	Determine relevant defined rules	(RFDP)	✓	✓	✓	✓	✓
191.	Decide on appropriate technical solutions and rules	(RFDP)	✓	✓	✓	✓	✓
192.	Decide on how to assess the definition of rules and definitions relevant to establishing a required level of confidence	(RFDP)	✓	✓	✓	✓	✓
193.	Assess the definition of rules and definitions relevant to establishing a required level of confidence	(RFDP)	✓	✓	✓	✓	✓
194.	Take control action to ensure the definition of rules and definitions relevant to establishing a required level of confidence meets the government and its customers' needs and expectations.	(RFDP)	✓	✓	✓	✓	✓
195.	Decide on how to determine relevant set of rules and definitions	(RFDP)	✓	✓	✓	✓	✓
196.	Identify rules and definitions in 'best practice'	(RFDP)	✓	✓	✓	✓	✓
197.	Determine relevant set of rules and definitions	(RFDP)	✓	✓	✓	✓	✓
198.	Take control action to ensure that relevant rules and definitions are determined	(RFDP)	✓	✓	✓	✓	✓
199.	Determine how to define the levels of confidence required and relevant set of rules	(RFDP)	✓	✓	✓	✓	✓
200.	Define required level of confidence and relevant set of rules	(RFDP)	✓	✓	✓	✓	✓
201.	Take control action to ensure that the set of rules and levels of confidence are defined	(RFDP)	✓	✓	✓	✓	✓

No.	Activity in the CM Relevant to Authentication in E-government	Subsystem	UK	US	AU	Ca	NZ
202.	Identify relevant technologies	Technology and 'Best Practice' Management (TechMgt)	☒	☒	☒	☒	☒
203.	Assemble knowledge about latest developments in relevant technologies	(TechMgt)	☑	☑	☑	☑	☒
204.	Select technologies that are available and affordable	(TechMgt)	☑	☑	☑	☑	☒
205.	Determine how to exploit latest developments in relevant technologies	(TechMgt)	☒	☒	☒	☒	☒
206.	Take necessary actions to exploit latest developments in relevant technologies	(TechMgt)	☒	☒	☒	☒	☒
207.	Monitor the exploitation of latest developments in relevant technologies	(TechMgt)	×	×	×	×	×
208.	Take control action to ensure the exploitation of latest developments in relevant technologies is done	(TechMgt)	×	×	×	×	×
209.	Define 'Best Practice'	(TechMgt)	✓	✓	✓	✓	✓
210.	Identify related 'Best Practice'	(TechMgt)	✓	✓	✓	✓	✓
211.	Identify areas where 'Best Practice' can enhance overall performance	(TechMgt)	✓	✓	✓	✓	✓
212.	Determine how to reflect 'Best Practice' as means for enhancement	(TechMgt)	✓	✓	✓	✓	✓
213.	Take necessary actions to reflect 'Best Practice' as means for enhancements	(TechMgt)	☑	☑	☑	☑	☑
214.	Monitor the activities of reflecting 'Best Practice' as means for enhancements	(TechMgt)	☒	☒	☒	☒	☒
215.	Take control action to ensure that 'Best Practices' are reflected throughout all the activities.	(TechMgt)	☒	☒	☒	☒	☒

Appendix C : A Conceptual Model Relevant to Preserving Privacy



A Conceptual Model relevant to Preserving Privacy in E-government Context

Appendix D : Mapping CMRPP Activities to Evaluation Criteria

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
1.	Define users of e-government Determine involved parties	Expectations and needs Mgt.	Does the framework define the users of e-services, determine involved parties?	Consensus Building	Stakeholders should be defined explicitly ,classified according to their needs
2.	Determine involved parties	Expectations and needs Mgt.	Does the framework define the users of e-services, determine involved parties?	Consensus Building	Stakeholders should be defined explicitly ,classified according to their needs
3.	Decide on how to determine expectations of involved parties	Expectations and needs Mgt.	Does the framework provide a way for determining the expectations and needs of the users?	Consensus Building	A structured way for determining the expectations and need of users should be provided
4.	Determine involved parties expectations and needs	Expectations and needs Mgt.	Does the framework provide a way for determining the expectations and needs of all involved parties?	Consensus Building	A structured way for determining the expectations and need of involve parties should be provided
5.	Determine Users' and government expectations and needs (2 activities)	Expectations and needs Mgt.	How the framework determines the involved parties' requirements?	Consensus Building	A structured way for developing stakeholders privacy req.
6.	Assess the determination of expectations and needs	Expectations and needs Mgt.	Does the framework provide away for validating the requirements?	Monitoring & Assessment	A procedure for requirements validation with the stockholders is needed
7.	Take control action to ensure expectations and needs are determined	Expectations and needs Mgt.	Does the framework provide a way for ensuring the requirements have been considered?	Monitoring & Assessment	Requirements validation
8.	Determine any changes in the expectations and needs of involved parties	Expectations and needs Mgt.	Does the framework provide a way for following the changes of requirements?	Consensus Building	A procedure for considering dynamic changes in the requirements
9.	Assess the impact of changes in the expectations and needs of involved parties on each activity	Expectations and needs Mgt.	Can the impact of changes in expectations and needs be assessed or traced to other requirements?	Consensus Building	Requirements validation
10.	Decide on how to react/Notify each controller [2 Activities]	Expectations and needs Mgt.	Does the framework provide a way for considering impacts of changes in the expectations and needs as a feedback to relevant activities	Monitoring & Assessment	A way to consider the impact of dynamic changes in the expectations and needs on relevant activities in the system
11.	Identify a provided service	Ownership rights Identification	Does the framework identify the service provider	Information Ownership Management	Service provider should be identified
12.	Determine information needed for providing the service	Ownership rights Identification	Does the framework determine information needed for providing the service	Information Ownership Management	Determine information needed for providing the service

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
13.	Determine information about the user that is subject to manipulation when providing the service	Ownership rights Identification	Does the framework provide a structure way for determining information about the user which is subject to manipulation?	Information Ownership Management	A structure way for determining user's information which is subject to manipulation when providing the service
14.	Decide on how to identify ownership rights to users' information for a provided service	Ownership rights Identification	Does the framework provide a way for identifying ownership rights to users' information?	Information Ownership Management	A mechanism for identifying ownership rights to users' information
15.	Identify ownership rights to users' information	Ownership rights Identification	Does the framework provide a way for identifying ownership right to users' information?	Information Ownership Management	Identify ownership rights of information about users in a provided service
16.	Assess the identification of ownership rights	Ownership rights Identification	Does the framework provide a way for assessment of the identification process?	Information Ownership Management	Assessment and validation steps of the processes of ownership rights identification
17.	Take control action to ensure ownership rights to users' information are identified	Ownership rights Identification	Does the framework provide a set of action to ensure the achievement of the ownership rights identification process?	Information Ownership Management	A set of actions to ensure the achievement of ownership rights identification Validation/Feedback Requirement (loop)Documentation needed
18.	Identify possible levels of control over users owned information	Levels of Control Identification	Does the framework identify levels of control over users owned information?	Rules and Controls Management	A process for identifying levels of control that can be applied into users' owned information
19.	Determine desired levels of control over users owned information	Levels of Control Identification	Does the framework provide a mechanism for determining desired levels of control over a user owned info?	Rules and Controls Management	Consider different preferences of involved parties with regard to levels of control over users' information
20.	Decide on how to identify levels of control on information owned by users	Levels of Control Identification	Does the framework provide a mechanism for determining levels of control on owned information	Rules and Controls Management	A structured way for identifying levels of control over users' owned information
21.	Identify levels of control on information owned by users	Levels of Control Identification	Does the framework identify levels of control over users owned info?	Rules and Controls Management	Identify levels of control on information owned by users when using a provided service
22.	Assess the identification of control levels	Controls and tools Identification	Does the framework provide assessment and validation steps for the processes	Monitoring and Assessment	Assessment /Validation Requirement
23.	Take control action to ensure control levels are identified	Levels of Control Identification	Does the framework provide validation and documentation steps for the processes	Monitoring and Assessment	Validation/Feedback Requirement (loop)Documentation needed

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
24.	Determine users' information that is manipulated by e-government services' providers when providing a service.	Ownership rights Definition	Does the framework provide a structure way for determining information subject to manipulation when providing e-government services	Information Ownership Management	Provide a structure way for determining information subject to manipulation when providing e-government services
25.	Identify possible processes for manipulating users' information	Ownership rights Definition	Does the framework identify processes for manipulating users' information	Information Ownership Management	Identify possible processes on user's information when providing e-government services.
26.	Define possible types of users' information	Ownership rights Definition	Does the framework classify users' information into types	Information Ownership Management	Classify users' information Into types
27.	Define possible ownership rights of users' information	Ownership rights Definition	Does the framework define ownership rights to users' information	Information Ownership Management	Define possible ownership rights to users' information
28.	Categorize processes for manipulating information into stages of manipulation	Ownership rights Definition	Does the framework categorise processes for manipulating users' information into categories	Information Ownership Management	Categorise processes for manipulating users' information when providing e-government services
29.	Consider the expectation and needs of involved parties and any changes in these needs	Ownership rights Definition	Does the framework provide a way to consider the expectations and need of stakeholders?	Information Ownership Management	Clear way for considering expectations and needs of involved parties.
30.	Determine ownership rights to users' information for each type of information and at each stage of manipulation	Ownership rights Definition	Does the framework provide a mechanism for defining ownership rights to users information at different stages of manipulation	Information Ownership Management	A clear Mechanism for defining ownership rights for each user's information type and at each different t manipulation process
31.	Assess the definition of ownership rights to users' information	Ownership rights Definition	Does the framework provide a way for validating the ownership rights definition	Information Ownership Management	Assessment and validation steps of the processes of ownership rights identification
32.	Take control action to ensure that ownership rights to users' information are defined	Ownership rights Definition	Does the framework provide a set of actions to ensure the achievement of the ownership rights definition process?	Information Ownership Management	A set of actions to ensure the achievement of ownership rights definition Validation/Feedback Requirement (loop)/Documentation needed
33.	Identify relevant laws and rights to information ownership	Ownership rights Definition	Does the framework consider identifying relevant laws & rights to information ownership	Information Ownership Management	Relevant laws & rights to information ownership should be identified
34.	Consider relevant laws & regulations to information ownership	Ownership rights Definition	Does the framework considers relevant ownership regulations and laws	Information Ownership Management	Relevant laws & rights to information ownership should be considered

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
35.	Assess the impact of considering relevant ownership rights and laws on each activity	Ownership rights Definition	Does the framework consider the impact of relevant laws and rights to information ownership	Information Ownership Management	Consider impact of relevant laws & rights
36.	Decide on how to react Notify each controller(2 activities)	Ownership rights Definition	Does the framework provide a way for considering impacts of relevant laws and right to information ownership as a feedback to relevant activities	Information Ownership Management	A way to consider the impact of considering laws and rights relevant to ownership rights on relevant activities in the system
37.	Identify potential threats on owned information	Risk Assessment & Mitigation	Does the framework identify potential threats on owned information	Security Requirements Elicitation	Identifying potential threats on owned information
38.	Determine possible impacts from potential threats on users' information	Risk Assessment & Mitigation	Does the framework determine possible impacts from potential threats	Security Requirements Elicitation	Determine possible impacts from identified potential threats
39.	consider possible dynamic changes of expectations and needs of involved parties	Risk Assessment & Mitigation	Does the framework consider changes in expectations and needs of involved parties?	Security Requirements Elicitation	Consider changes in the expectations and needs of involved parties
40.	Decide on how to assess risks from potential threats on owned information	Risk Assessment & Mitigation	Does the framework provide clear mechanisms on how to assess risks from potential threats	Security Requirements Elicitation	A mechanism to assess risks from potential threats
41.	Assess risks of potential threats on owned information	Risk Assessment & Mitigation	Does the framework consider assessing the risks on owned information	Security Requirements Elicitation	Assess the risks of potential threats on owned information
42.	Monitor the assessment of risks from potential threats on users owned info.	Risk Assessment & Mitigation	Does the framework provide a way for validating the risk assessment process	Security Requirements Elicitation	Assessment and validation steps of the processes of assessing risks
43.	Take control action to ensure risks are assessed	Risk Assessment & Mitigation	Does the framework provide a set of actions to ensure the achievement of assessing the risks from potential threat on owned information?	Security Requirements Elicitation	A set of actions to ensure the achievement of assessing the risks on owned information Validation/Feedback Requirement (loop)/Documentation needed
44.	Identify possible risks on users owned information	Risk Assessment & Mitigation	Does the framework identify risks on users owned information?	Security Requirements Elicitation	Identify possible risks on users owned information
45.	Know about relevant rules , policies and guidelines in 'Best Practices'	Risk Assessment & Mitigation	Does the framework consider knowing about relevant rules, policies and guidelines in 'best practices'?	Security Requirements Elicitation	Recognise relevant rules , policies and guidelines in best practices

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
46.	Determine possible rules and controls for mitigating identified risks	Risk Assessment & Mitigation	Does the framework provide a way for determining possible rules and controls for mitigating identified risks	Security Requirements Elicitation	Have a process for defining possible rules and controls for mitigating risks
47.	Determine appropriate set of controls and rules for mitigating identified risks	Risk Assessment & Mitigation	Does the framework provide away for defining appropriate set of controls for mitigating identified risks	Security Requirements Elicitation	Have a process for defining (appropriate)set of controls for mitigating identified risks
48.	Assess the determination of appropriate set of controls and rules	Risk Assessment & Mitigation	Does the framework provide a way for validating determination of appropriate set of controls	Security Requirements Elicitation	Assessment and validation steps of the processes of determining appropriate set of rules and controls
49.	Take control action to ensure that an appropriate set of controls and rules for mitigating risks on users owned information is determined	Risk Assessment & Mitigation	Does the framework provide a set of actions to ensure the achievement of determination of appropriate set of rules and controls?	Security Requirements Elicitation	A set of actions to ensure the achievement of determining appropriate set of rules and controls/ Validation/Feedback Requirement (loop)/Documentation needed
50.	Consider relevant standards and 'Best Practices'	Levels of Control Definition	Does the framework consider relevant standards and 'Best Practices'?	Rules and Controls Management	Consider relevant standards and 'Best Practices'
51.	Identify possible risks on users owned information	Levels of Control Definition	Does the framework identify possible risks on users owned information?	Rules and Controls Management	Identify possible risks on users owned information
52.	Identify appropriate controls and rules for mitigating risks on users owned information	Levels of Control Definition	Does the framework identify appropriate	Rules and Controls Management	Identify appropriate controls and rules for mitigating risks on users owned information
53.	Define possible categorizing schemes	Levels of Control Definition	Does the framework define categorising scheme for rules and controls	Rules and Controls Management	Define possible categorizing schemes
54.	Decide on how to categorize identified controls and rules into levels of controls according to the impacts of identified risks on users owned information	Levels of Control Definition	Does the framework provide a way for deciding on how to categorise rules and controls into levels of controls	Rules and Controls Management	Guidelines for how to decide on a specific categorisation of rules and controls into levels of controls
55.	Define scheme for categorizing identified controls and rules into levels of controls according to the impacts of identified risks on users owned information	Levels of Control Definition	Does the framework define a scheme for categorising controls and rules into levels of controls	Rules and Controls Management	A scheme for categorising controls and rules into levels of controls.
56.	Categorize controls and rules into levels of control	Levels of Control Definition	Does the framework provide categories for rules and controls (as levels of control)	Rules and Controls Management	Provide categories (levels) for rules and controls

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
57.	Assess the categorizing of controls and rules into levels of control according to impact of identified risks	Levels of Control Definition	Does the framework provide a way for validating the categorizing of controls and rules into levels of control	Rules and Controls Management	Assessment and validation steps of the processes of the categorizing of controls and rules into levels of control
58.	Take control action to ensure controls and rules are categorized	Levels of Control Definition	Does the framework provide a set of actions to ensure the the categorizing of controls and rules into levels of control?	Rules and Controls Management	A set of actions to ensure the achievement of the categorizing of controls and rules into levels of control / Validation/Feedback Requirement (loop)/Documentation needed
59.	Decide on how to assess the achievement of defining levels of control for owned information	Levels of Control Definition	Does the framework have a way to validate the achievement of defining levels of controls	Rules and Controls Management	Defined process for validation
60.	Assess the achievement of defining levels of controls	Levels of Control Definition	Does the framework provide a way for validating the definition of levels of controls	Rules and Controls Management	Assessment and validation steps of the processes of definition of levels of controls
61.	Take control action to ensure that levels of control on owned information are defined	Levels of Control Definition	Does the framework provide a set of actions to ensure the achievement of definition of levels of controls?	Rules and Controls Management	A set of actions to ensure the achievement of definition of levels of controls / Validation/Feedback Requirement (loop)/Documentation needed
62.	Consider the identified security requirements of the provided service when enabling users to have control over owned information	Levels of Control Assignment	Does the framework consider identified security requirements when enabling the users' controls	Rules and Controls Deployment	A way for considering security requirements when enabling users' control over owned information!!
63.	Assign appropriate defined control levels	Levels of Control Assignment	Does the framework show how to assign appropriate control levels	Rules and Controls Deployment	Guidelines for identifying appropriate control levels
64.	Decide on how to assign control levels to information owned by users	Levels of Control Assignment	Does the framework provide a way for deciding on how to assign control levels to information owned by users	Rules and Controls Deployment	A process for assigning control levels to information owned by users.
65.	Assign control levels to information owned by users	Levels of Control Assignment	Does the framework provide a mechanism for assigning control revels to users owned information	Rules and Controls Deployment	A clear mechanism (process) for assigning control levels to users owned information
66.	Assess the assignment of control levels	Levels of Control Assignment	Does the framework assess how the control levels were assigned?	Rules and Controls Deployment	Assessment and validation steps of the processes of assigning control levels

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
67.	Take control action to ensure control levels are assigned	Levels of Control Assignment	Does the framework provide a set of actions to ensure the achievement of assigning the control levels?	Rules and Controls Deployment	A set of actions to ensure the achievement of assigning the control levels/ Validation/Feedback Requirement (loop)/Documentation needed
68.	Define Transparent/ Define ease of use/ Define flexible	Levels of Control Deployment	Does the framework provide a way to agree on definition of desired, ease of use/ simple	Rules and Controls Deployment	Provide agreement on important definitions at early stage!!!
69.	Consider the capabilities (req.) of different types of users	Levels of Control Deployment	Does the framework consider different users requirements/capabilities	Rules and Controls Deployment	Recognise the requirements of different users and their different capabilities
70.	Decide on how to present levels of control in a transparent, flexible and easy to use way that reflect relevant policies, regulations and laws	Levels of Control Deployment	Does the framework provide a way for deciding on how to present levels of controls?	Rules and Controls Deployment	A process for defining design requirements for presenting levels of controls
71.	Present levels of control on owned information in a transparent, flexible and easy to use way to all users	Levels of Control Deployment	Does the framework define presentation (design) requirements?	Rules and Controls Deployment	Design requirements should consider influencing factors, e.g. a transparent, flexible and easy to use way
72.	Assess the presentation of levels of control	Levels of Control Deployment	Does the framework provide a way (measures) for assessing the way the levels of controls were presented	Rules and Controls Deployment	Measures for assessing the presentation of levels of controls
73.	Take control action to ensure levels of control are presented in a transparent, flexible and easy to use way that reflect relevant rules and policies	Levels of Control Deployment	Does the framework provide a set of actions for ensuring the achievement of presenting the levels of controls while considering influencing factors	Rules and Controls Deployment	A set of actions to ensure the achievement of presenting the levels of controls / Validation/Feedback Requirement (loop)/Documentation needed
74.	Know about relevant policies, regulations and laws	Levels of Control Deployment	Does the framework consider knowing about relevant policies, regulations and laws	Rules and Controls Deployment	Know about relevant policies, regulations and laws
75.	Consider enforcing relevant policies, regulations and laws to levels of control on owned information when possible	Levels of Control Deployment	Does the framework consider relevant Laws etc. when defining requirements for presenting and deploying levels of controls	Rules and Controls Deployment	Relevant laws...etc. should be considered when defining levels of control deployment requirements...

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
76.	Deploy (implement) levels of control on owned information in a transparent, flexible and easy way to all users	Levels of Control Deployment	Does the framework provide details on how to deploy (implement) the levels of control on users owned information?	Rules and Controls Deployment	Provide a set of actions/instructions on how to deploy the levels of control on users owned information
77.	Maintain the deployment of levels of control on owned information throughout any manipulation of that information when using e-government services	Levels of Control Deployment	Does the framework provide a way for maintaining the deployment of levels of control on owned information throughout any manipulation to that information?	Rules and Controls Deployment	Maintain the deployment of levels of control on owned information throughout any manipulation of that information when using e-government services
78.	Assess the achievement of deploying levels of controls over user owned information throughout any manipulation of that information when using e-government services	Levels of Control Deployment	Does the framework provide a way (to define some measures) for assessing the deployment of levels of controls throughout any manipulation of users owned information when using e-government services	Rules and Controls Deployment	Define measures for assessing the deployment of levels of controls throughout any manipulation of users owned information when using e-government services
79.	Take control action to ensure the deploying levels of controls on owned information throughout any manipulation of that information when using e-government services	Levels of Control Deployment	Does the framework provide a set of actions for ensuring the achievement of deploying the levels of controls on owned information throughout any manipulation of that information when using e-government services	Rules and Controls Deployment	A set of actions to ensure the achievement of deploying the levels of controls on owned information / Validation/Feedback Requirement (loop)/Documentation needed
80.	Know about relevant current technologies	Technology Support Management	Does the framework consider knowing about current relevant technologies?	Technology Support	Know about relevant current technologies
81.	Consider limitation of current technologies	Technology Support Management	Does the framework consider limitations in current relevant technologies?	Technology Support	Consider limitation of relevant current technologies
82.	Identify tools and mechanisms that support enabling users control over owned information	Technology Support Management	Does the framework provide a way to identify tools and mechanisms …	Technology Support	Identify tools and mechanisms that support enabling users control over owned information
83.	Determine available resources	Technology Support Management	Does the framework consider available resources?	Technology Support	Determine available resources
84.	Determine appropriate technical tools and mechanisms	Technology Support Management	Does the framework provide a way for deciding on appropriate technology	Technology Support	Provide a way for defining the appropriate tools and mechanisms to be used for deploying levels of control on owned information

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
85.	Decide on how to utilize the appropriate tool for deploying a level of control over user owned information throughout any processing when using e-government services	Technology Support Management	Does the framework provide a way for deciding on how to utilize appropriate tools and mechanisms when deploying levels of control over owned information	Technology Support	Provide a way for deciding on how to utilize appropriate tools and mechanisms when deploying levels of control over owned information
86.	utilize the appropriate tools for deploying a level of control over user owned information throughout any processing when using e-government services	Technology Support Management	Does the framework utilize the appropriate tools for deploying a level of control over user owned information throughout any processing when using e-government services	Technology Support	utilize the appropriate tools for deploying a level of control over user owned information throughout any processing when using e-government services
87.	Assess the utilization of appropriate technical tools and mechanisms when deploying control levels on users owned information	Technology Support Management	Does the framework provide a way for validating utilization of appropriate tools and mechanisms	Technology Support	Assessment and validation steps of the processes of utilization of appropriate tools and mechanisms
88.	Take control action to ensure utilization of appropriate technical tools and mechanisms when deploying control levels on users owned information	Technology Support Management	Does the framework provide a set of actions to ensure the achievement of utilization of appropriate tools and mechanisms?	Technology Support	A set of actions to ensure the achievement of utilization of appropriate tools and mechanisms / Validation/Feedback Requirement (loop)/Documentation needed
89.	Identify relevant 'Best Practices'	Knowledge Assembly Management	Does the framework consider identifying relevant 'Best Practices'	Knowledge Assembly	Identify relevant 'Best Practices'
90.	Decide on how to assemble the knowledge of relevant rules, policies and guidelines in 'Best Practices'	Knowledge Assembly Management	Does the framework provide a way for assembling relevant rules, policies and guidelines in 'Best Practices'	Knowledge Assembly	Guidelines for assembling knowledge about relevant rules, policies and guidelines in 'Best Practices'
91.	Assemble the knowledge of relevant rules, policies and guidelines in 'Best Practices'	Knowledge Assembly Management	Does the framework consider assembling the knowledge of relevant rules, policies and guidelines in 'Best Practices'	Knowledge Assembly	consider assembling the knowledge of relevant rules, policies and guidelines in 'Best Practices'
92.	Assess the assembling of knowledge of relevant rules, policies and guidelines in 'Best Practices'	Knowledge Assembly Management	Does the framework provide a way for validating the process of assembling relevant knowledge	Knowledge Assembly	Assessment and validation steps of the processes of validating the process of assembling relevant knowledge

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
93.	Take control action to ensure relevant knowledge to levels of control on owned information is assembled	Knowledge Assembly Management	Does the framework provide a set of actions to ensure the achievement of validating the process of assembling relevant knowledge?	Knowledge Assembly	A set of actions to ensure the achievement of validating the process of assembling relevant knowledge / Validation/Feedback Requirement (loop)/Documentation needed
94.	Define ease of use/Define flexible/Define transparent	Constraints Management	Does the framework consider defining relevant features desired in the system	Environment Awareness	Provide a set of definitions for features of the system (e.g. flexibility)
95.	Determine desired level of transparent, flexibility and ease of use	Constraints Management	Does the framework provide a way (defined scale) to define desired level of transparent ,etc. on each activity	Environment Awareness	Provide a way to define desired level of system features
96.	Assess the impact of the desired level of transparent, flexibility and ease of use on each activity	Constraints Management	Does the framework consider the impact of the desired level of each factor on each activity	Environment Awareness	Consider impact of desired level of influencing factors on each activity
97.	Take control action ensure that transparent , flexibility and ease of use are considered when enabling users' control over owned information	Constraints Management	Does the framework provide measures for ensuring the consideration of (factors..) when enabling user's control over their owned information	Environment Awareness	Should provide measures for ensuring the consideration of environmental factors (e.g. social and cultural factors)
98.	Assemble knowledge about the impacts of social , political and cultural factors	Knowledge Assembly	Does the framework provide a way for gathering knowledge about impacts of environmental factors (social, etc.?)	Environment Awareness	A way to gather information about environmental factors
99.	Assess the impacts of social political and cultural factors on each activity	Knowledge Assembly	Does the framework provide a way for considering the impacts of environmental factors)	Environment Awareness	Considers the impact of social, cultural and political factors on all activities
100.	Monitor the conformance	Knowledge Assembly	Does the framework define measures for assessing the conformance with constraints that affect an activity	Environment Awareness	Define measures for monitoring the conformance with constraints that affect an activity!!!
101.	Decide on actions for considering the impacts of social, political and cultural factors on each activity	Knowledge Assembly	Does the framework provide a way for deciding on actions when considering environmental factors?	Environment Awareness	Guideline on how to act when considering environmental factors.
102.	Take control action ensure that the impacts of social, political and cultural factors are considered	Constraints Mgt.	Does the framework have a way to ensure that environmental factors were considered?	Environment Awareness	Define measures for ensuring the consideration of environmental factors…

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
103.	Determine the possibility of complying with standards and guidelines	Standards and Guidelines Compliance Management	Does the framework considers complying with relevant standards and guidelines	Compliance Management	Should consider compliance with relevant standards and guidelines
104.	Decide on how to comply with relevant standards and guidelines where appropriate and possible	Standards and Guidelines Compliance Management	Does the framework provide a way for deciding on how to comply with standards and guidelines?	Compliance Management	Steps for complying with standards and guidelines?
105.	Assess the impact of complying with relevant standards and guidelines	Standards and Guidelines Compliance Management	Does the framework consider assessing the impact of compliance with relevant standards and guidelines	Compliance Management	Should consider the impact of complying with relevant standards and guidelines
106.	Take control action ensure the compliance with relevant standards and guidelines where appropriate and possible	Standards and Guidelines Compliance Management	Does the framework provide a way for ensuring compliance with relevant standards and guidelines	Compliance Management	Provide a way for ensuring compliance with relevant standards and guidelines
107.	Assess the impact of complying with relevant policies, regulations, laws	Regulations, polices and laws Mgt.	Does the framework provide a way for measuring the impact of complying with laws...?	Compliance Management	Should provide a way for assessing the impact of complying with relevant laws on the framework activities.
108.	Monitor the compliance to relevant policies, regulations, laws	Regulations, polices and laws Mgt.	Does the framework provide a way for monitoring the compliance to relevant laws...?	Compliance Management	Define measures for assessing the compliance with relevant laws…
109.	Decide on how to comply with relevant policies, regulations, laws where appropriate and possible	Regulations, polices and laws Mgt.	Does the framework provide a way for deciding on how to comply with laws…?	Compliance Management	Guidelines for how to comply with relevant laws…
110.	Take control action ensure the compliance with relevant policies, regulations, laws where appropriate and possible	Regulations, polices and laws Mgt.	Does the framework provide a way to ensure the compliance with relevant laws…?	Compliance Management	Define measures for ensuring the compliance with relevant laws,,,
111.	Decide on how to educate and raise the awareness about policies between all involved parties	Privacy Awareness	Does the framework provide a way to decide on how to raise privacy awareness between involved parties	Privacy Awareness	Provide ways to raise privacy awareness between involved parties
112.	Considers common principles and Best practices	Privacy Awareness	Does the framework considers best practices	Privacy Awareness	Identify and consider best practices in raising privacy awareness

No.	Activity	subsystem	Evaluation Criteria	Criteria Category	Possible Requirement
113.	Apply program for raising the awareness of relevant policies between involved parties	Privacy Awareness	Does the framework consider applying privacy awareness...?	Privacy Awareness	Provide privacy awareness programs and training to involved parties
114.	Assess the application of education and awareness programs	Privacy Awareness	Does the framework assess the privacy awareness level	Privacy Awareness	Provide ways to assess the privacy awareness of involved parties
115.	Take control action to ensure the education and raising awareness programs are applied	Privacy Awareness	Does the framework provide actions to ensure raising privacy awareness	Privacy Awareness	Provide ways to ensure privacy awareness between all involved parties is raised
116.	Determine government's performance expectations	Overall Performance Control	Does the framework provide a way for determining government's performance expectations	Overall Performance Management	A process for determining government's' performance expectations
117.	Determine Performance measures	Overall Performance Control	Does the framework determine government's performance expectations	Overall Performance Management	Define performance measures according to government's expectations
118.	Decide on how to assess the achievement of enabling users to have control on owned information	Overall Performance Control	Does the framework provide a way to decide on how to validate the whole processes	Overall Performance Management	Guidelines on how to validate the whole processes?!!
119.	Assess the achievement of enabling users to have control on owned information	Overall Performance Control	Does the framework provide a way (define some measure)for monitoring the achievement of enabling users to have control on owned information	Overall Performance Management	Define measures for overall monitoring of the processes?
120.	Decide on how to react/Notify each controller [12 Activities]	Expectations and needs Mgt./Constraints Management/Standard& Guidelines Compliance Mgt./Regulations, Policies & Laws Compliance Mgt. Environmental Influence	Does the framework provide a way for considering impacts of changes in the expectations / constraints/ environmental factors/regulations &laws/standards & guidelines as a feedback to relevant activities	Overall Performance Management	A way to consider the impact of dynamic changes in the expectations and needs on relevant activities in the system
121.	Take control action to the achievement of enabling users to have control on owned information	Overall Performance Control	Does the framework provide measures for ensuring the enabling of users to have control over owned information	Overall Performance Management	Provide actions for ensuring the achievement of the framework goal according to defined performance measures

Appendix E : Survey Versions

E.1 Survey Pilot Round Version

A Survey on Preserving Privacy in the context of E-government Pilot Round

Purpose:

This survey is part of the evaluation phase for my PhD research in preserving privacy in the context of providing electronic government services. All answers and responds will be kept anonymous and used only for the purpose of this research.

Terminologies: **E-government services**: any service that is provided by the government and can be accessed and used through electronic means such as internet, mobile phones or kiosk points.

Service's Provider: any government agency or a third party who provide an e-government service using any of the above mentioned means under the government approval.

Developer: an individual or a group who participate in the design and technical implementation of an e-government service.

Q1.Please select your age group? (Please circle one answer only)

1. Less than 18 2. Between 18-60 3. Over 60

Q2.Please select your gender? (Please circle one answer only)

1. Male 2. Female

Q3.Have you used e-government services before?

1. Yes 2. No

Q4.If answer is yes, Please tick the category (ies) apply to the electronic government service(s) that you have used(You can select more than one):

- Information Inquiry services.
- Queries, Forms and Complaints submissions services.
- Official Documents Issuing or Renewal services
- Payment Services (e.g. utilities bills, fees, fines).
- Others: Please specify:…… ……

Q5.How often do you use e-government services? (Please circle one answer only)

1. Very often 2. Often 3. Rarely 4. Never

Q6.Please tick the option in the list that describes your relation with electronic government services (You can select more than one):

- Government body representative.
- Electronic Services' Provider.
- User

- Developer of electronic services.

Q7.Please tick the option in the list that describe s your type of use of electronic government services (You can select more than one):

- For personal use as an individual.
- Use on behalf of others (e.g. as a carer, parent). Please specify your role:……..
- Use for business /work related services
- Use for a non-profit organisation

Q8.How important is it to you that your privacy is protected when using e-government services?

1. Very important 2. Important 3. Less important 4. Not important

From Q9 to Q12 Please select to what extent you agree on the following statements for achieving preserving privacy in the context of e-government:

Q9.Privacy can be preserved by not sharing users' information between services' providers at any point.

1. Strongly agree 2. Agree 3. Do not know 4. Disagree 5. Strongly disagree

Q10. Privacy can be preserved by enabling the users to have control over their owned information (i.e. enabling users to decide on who can view and process information about them which they own)

1. Strongly agree 2. Agree 3. Do not know 4. Disagree 5. Strongly disagree

Q11. Privacy can be preserved by monitoring the way information about users is manipulated by services providers.

1. Strongly agree 2. Agree 3. Do not know 4. Disagree 5. Strongly disagree

Q12. Should users have control over their information when using e-government services? All groups

1. Yes 2. No

Q13. To what extent should users have control over their information when using e-government services?

1. Full control 2. Limited control 3. No Control

Q14. To what extent can government agencies share users' information with other agencies and/or third parties (who are providing a service to the user which satisfy the reasons for or part of the reasons for gathering information)?

1. Share all information 2. Share relevant (needed) information to provide the service
3.Share anonymous information 4. Shouldn't Share at all

Q15. In your opinion, who should define the ownership rights of information held about users?

1. Government 2.Users 3.Service providers
4. An agreement derived from the discussion between all the three stakeholders.

Q16. To what extent you agree on the following, allowing users to assign a desired level of control over the whole or part of their information and maintaining the deployment of this level of control

throughout the processing and manipulation of that information when using an e-government service, will enable users to have control over their owned information when using e-government services.

1. Strongly agree 2. Agree 3. Do not know 4. Disagree 5. Strongly disagree

Q17. Defining a user's ownership rights of information about him/her can be achieved by the following statements, please select the most appropriate statement in your opinion.

- Defining Ownership rights of the user's record of information
- Defining types of information collected about the user and defining the ownership right for each type of the information
- Defining ownership rights for each type of information collected about the user and at each stage of manipulation
- None of the above

Q18. If you have other suggestion for the way that defining the user's ownership rights on information about him/her can be achieved please state it below

……

Q19. The levels of control are set of rules for enforcing the protection and sharing of user's information, please select the most appropriate statement for achieving the definition of those levels of control.

- Categorising set of rules into levels of control based on the level of risk identified on users' information.
- Defining levels of control on users' information based on levels of control in relevant standards and guidelines.
- All the above.
- None of the above.
- Do not know.

Q20. Do you have other suggestions for how the levels of controls on users' information can be defined, please state it below

……

Q21. In your opinion, Please circle who should be involved in defining the levels of control on information held about users? (You can circle more than one)

1. Government 2.Users 3.Service providers 4. Developers

Q22. In your opinion, who should monitor and assessed the process of preserving privacy when providing e-government services?

1. A Government body representative
2. An independent third party
3. A representative body of the users.
4. Others. Please state ……

Q23. A system to enable the users to have control over their owned information when using e-government services will need some resources to work? Please tick the resource(s) that you think is (you can choose more than one)?

- Human Resources (Employees, Developers, Software engineers, etc...)
- Technical Support
- Financial Support

- Knowledge and Best Practice Resources
- Law Enforcement Resources
- Others……

Q24. A system for preserving privacy when providing e-government services should have the following features; please rank the features according to their importance to the system. Use rank range of (1 for the highest rank (most important) to 5 (Least important)?

- Easy to use
- Transparent (i.e. user is aware of the way their privacy is preserved and when and by whom their information is shared)
- Flexible (i.e. the systems is flexible enough to respond to dynamic changes in stakeholders' expectations and needs)
- Meet identified security requirements of the provided service.
- Enforce relevant laws, policies and regulations.(laws and regulations put by the government)
- Comply with relevant standards and guidelines.(International standards and guidelines)
- Consider the impacts of social and cultural factors in the system environment.
- Consider the impact of political environmental factor.
- Cost effective.

Q25. Is there any other features that you think a system for preserving privacy in e-government context should have, please state it below and rank it's important to the system :

……

Q26. The enforcement of the compliance of relevant privacy regulations, policies and laws can be achieved by following, please select the appropriate statement (You can select more than one):

- By monitoring the compliance of all involved parties in e-government services provision and empowering relevant authorities to respond to any violation by applying suitable penalties.
- By educating and raising the public awareness about privacy regulations, policies and laws.
- All the above.
- None of the above.
- Do not know.

Q27. Do you have other suggestions for how privacy regulations, policies and laws can be enforced? Please state it below?

……

Q28. To what extent you agree on the following, to ensure that users are enabled to have control over owned information when using e-government services, the government should place relevant provision requirements on service providers.

1. Strongly agree 2. Agree 3. Do not know 4. Disagree 5. Strongly disagree

Q29. Do you think implementing such a system to preserve privacy is viable?

1. Yes 2. No

Q30. Please Explain why?

.....

Open Questions for participants on the Pilot Round:

1. Did you feel that any question was a repetitive to another one? If yes, which one(s)?
2. Was the questionnaire language easy to understand? (If not which part was difficult to understand?
3. Were there any questions that you felt it needed some expertise to be answered? If yes, which one(s)?
4. Were there any parts of the questionnaire that were not clear and you needed more information to be able to answer them? If yes, which one(s)?
5. Please provide any extra comments you would like to add about this questionnaire?
   Thank you so much.

E.2 Final Survey Links and Codes:

Questionnaire- Online English version Link: http://goo.gl/hGaCV

QR Code:

Questionnaire- Online Arabic Version Link: http://goo.gl/lvPHF

QR Code:

Appendix F : Survey Responses Summary

In the following we present a summary for the results of the survey questions, note that questions Q19,Q22,Q26,Q28 and Q29(b) were open(optional) questions and summary of the responses to these questions in a separate section:

1. Close-ended questions:

Q1. What is your nationality country?

Country	Saudi Arabia	United Kingdom	Oman	Other	Total
No. of respondents	**228**	**61**	**36**	**20**	**345**

Appendix_Table F.1: Responses Numbers

Q2 Please selects your age group?

Age group\ Country	Saudi Arabia	United Kingdom	Oman	Other	Total
Less than 18	4%	0%	0%	0%	3%
Between 18 and 60	94%	92%	100%	100%	95%
Over 60	1%	8%	0%	0%	2%

Appendix_Table F.2: Responses by Age Group

Q3: Please select you gender?

	Saudi Arabia	United Kingdom	Oman	Other	Total
Female	50%	26%	58%	45%	46%
Male	50%	74%	42%	55%	54%

Appendix_Table F.3: Responses by Gender

Q4. Have you used e-government services in your country before?

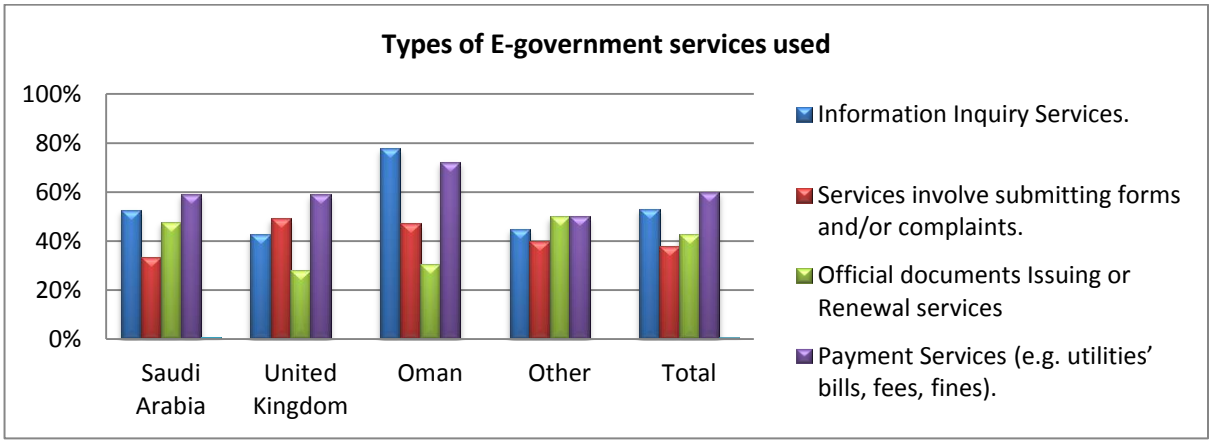
	Saudi Arabia	United Kingdom	Oman	Other	Total
Yes	90%	89%	97%	80%	90%
No	10%	11%	3%	20%	10%

Appendix_Table F.4: Using e-government service

Q5. Please select the category (ies) that apply to the electronic government service(s) that you have used:

	SA	UK	Oman	Other	Total
Information Inquiry Services.	53%	43%	**78%**	45%	53%
Services involve submitting forms/ complaints	33%	49%	47%	40%	38%
Official documents Issuing or Renewal services	48%	28%	31%	**50%**	43%
Payment Services (e.g. utilities' bills, fees, fines)	**59%**	**59%**	72%	**50%**	**60%**
Other	1%	0%	0%	0%	1%

Appendix_Table F.5: Most used services

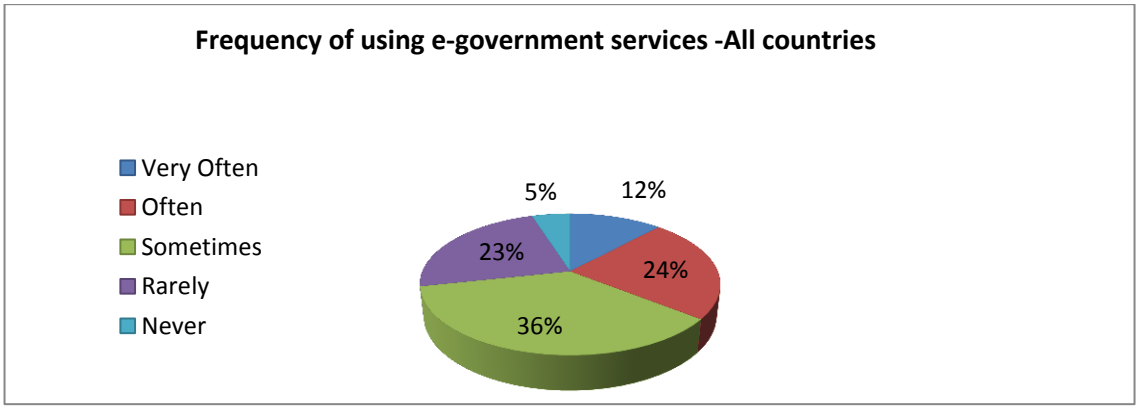


Appendix_Figure F.1: Most used services

Q6: How often do you use e-government services?

	SA	UK	Oman	Other	Total
Very Often	15%	5%	11%	0%	12%
Often	22%	16%	28%	55%	24%
Sometimes	33%	43%	44%	30%	36%
Rarely	23%	31%	17%	15%	23%
Never	6%	5%	0%	0%	5%

Appendix_Table F.6: Frequency of using services

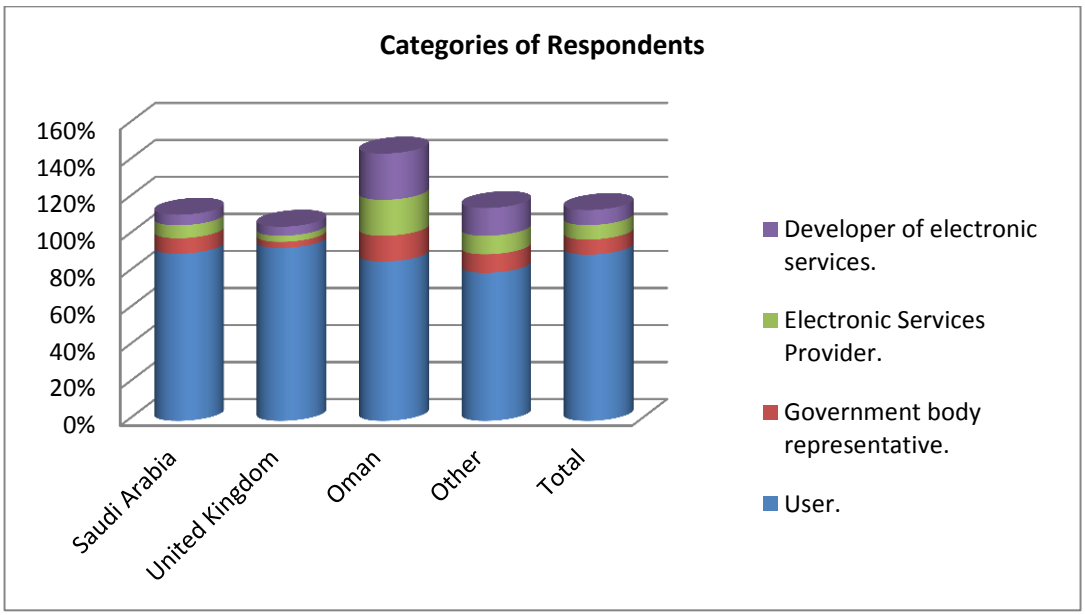


Appendix_Figure F.2: Frequency of using services

Q7. Which of the following describes your relation with electronic government services?

	SA	UK	Oman	Other	Total
User.	90%	93%	86%	80%	90%
Government body representative.	8%	3%	14%	10%	8%
Electronic Services Provider.	7%	3%	19%	10%	8%
Developer of electronic services.	6%	5%	25%	15%	8%
Other	0%	0%	0%	0%	0%

Appendix_Table F.7: Categories of respondents

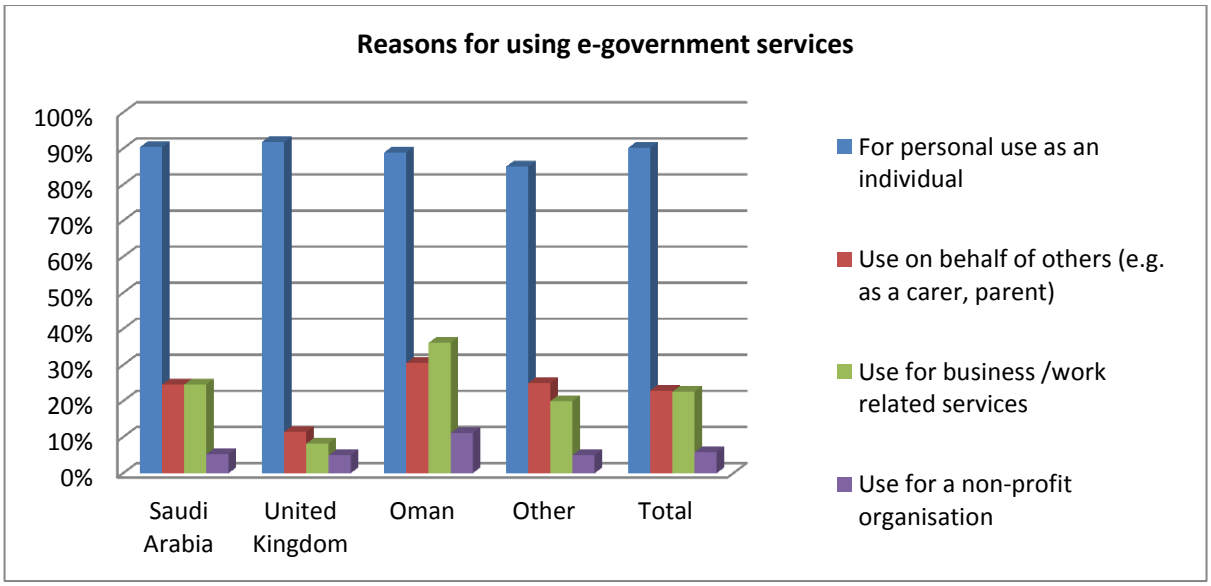


Appendix_Figure F.3: Categories of respondents

Q8: Which of the following describes the reason for your use of e-government services?

	SA	UK	Oman	Other	Total
For personal use as an individual	90%	92%	89%	85%	90%
Use on behalf of others (e.g. as a carer, parent)	25%	11%	31%	25%	23%
Use for business /work related services	25%	8%	36%	20%	23%
Use for a non-profit organisation	5%	5%	11%	5%	6%

Appendix_Table F.8: Reasons for using e-government services

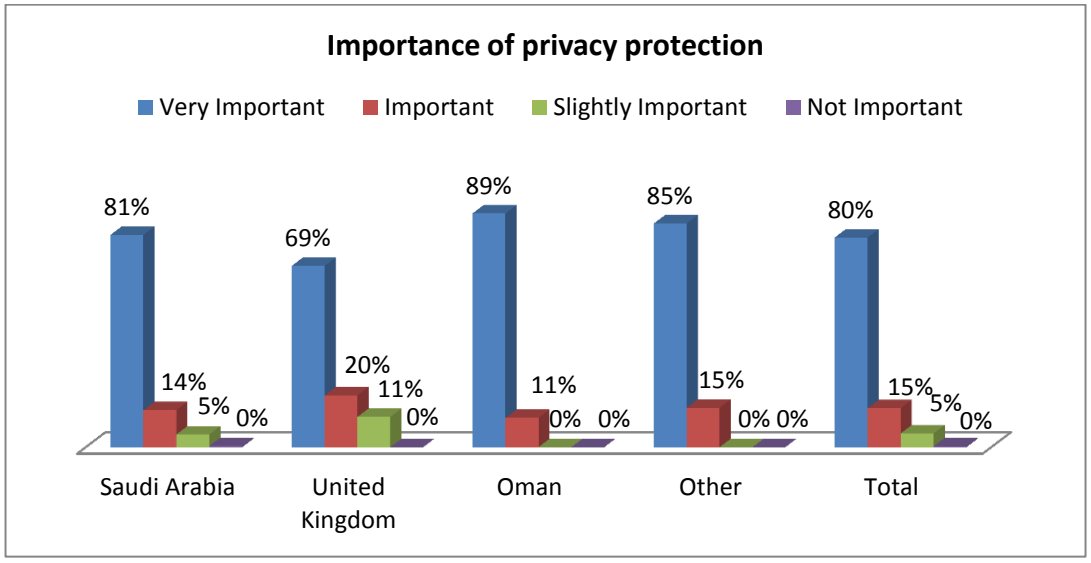


Appendix_Figure F.4: Reasons for using e-government services

Q9. How important is it to protect your privacy when using e-government services?

	SA	UK	Oman	Other	Total
Very Important	81%	69%	89%	85%	80%
Important	14%	20%	11%	15%	15%
Slightly Important	5%	11%	0%	0%	5%
Not Important	0%	0%	0%	0%	0%

Appendix_Table F.9: Importance of privacy protection

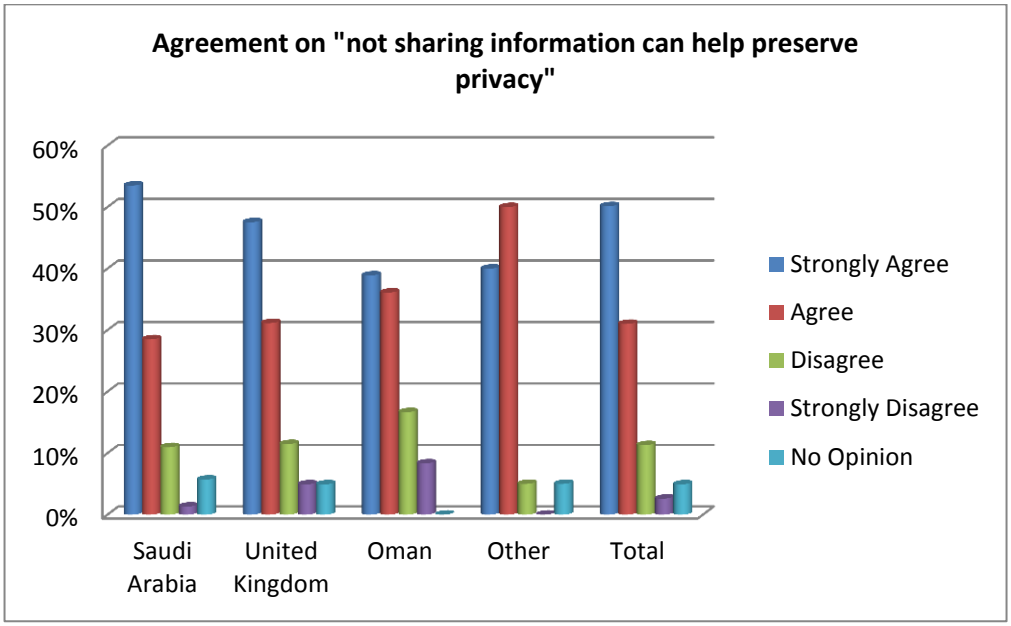


Appendix_Figure F.5: Importance of privacy protection

Q10. Privacy can be preserved by not sharing users' information between services providers at any point. To what extent you agree with the statement?

	SA	UK	Oman	Other	Total
Strongly Agree	54%	48%	39%	40%	**50%**
Agree	29%	31%	36%	50%	**31%**
Disagree	11%	11%	17%	5%	**11%**
Strongly Disagree	1%	5%	8%	0%	**3%**
No Opinion	6%	5%	0%	5%	**5%**

Appendix_Table F.10: Agreement on "not sharing information can help preserve privacy



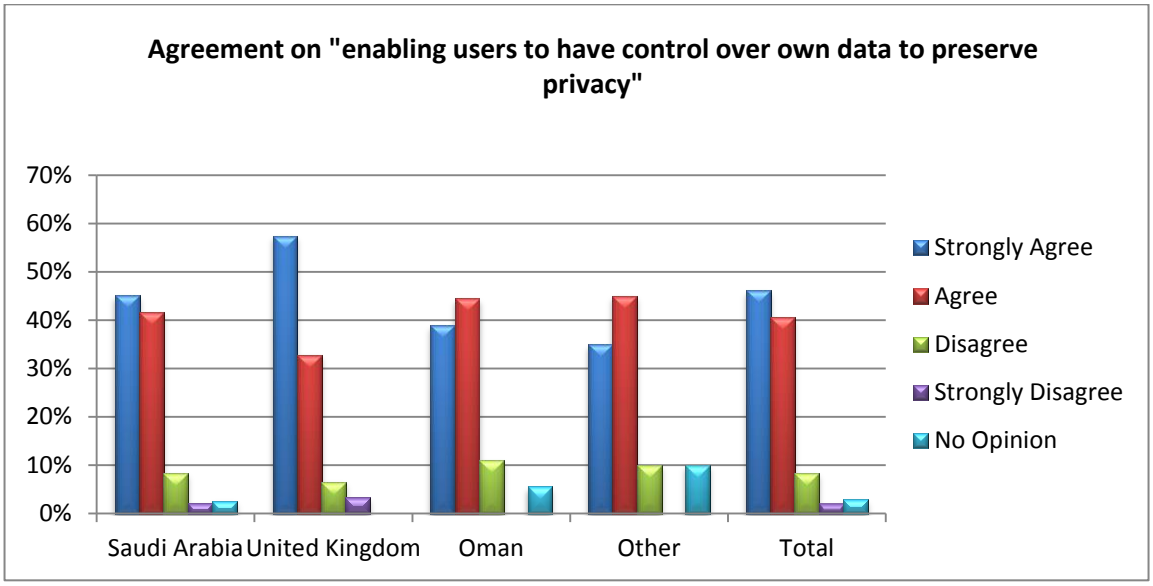
Appendix_Figure F.6: Agreement on "not sharing information can help preserve privacy"

Q11. Privacy can be preserved by enabling users to have control over their information (i.e. enabling users to decide on who can view and process their information).

To what extent you agree with the statement?

	SA	UK	Oman	Other	Total
Strongly Agree	45%	57%	39%	35%	46%
Agree	42%	33%	44%	45%	41%
Disagree	8%	7%	11%	10%	8%
Strongly Disagree	2%	3%	0%	0%	2%
No Opinion	3%	0%	6%	10%	3%

Appendix_Table F.11: Agreement on "enabling users to have control over own data to preserve privacy"



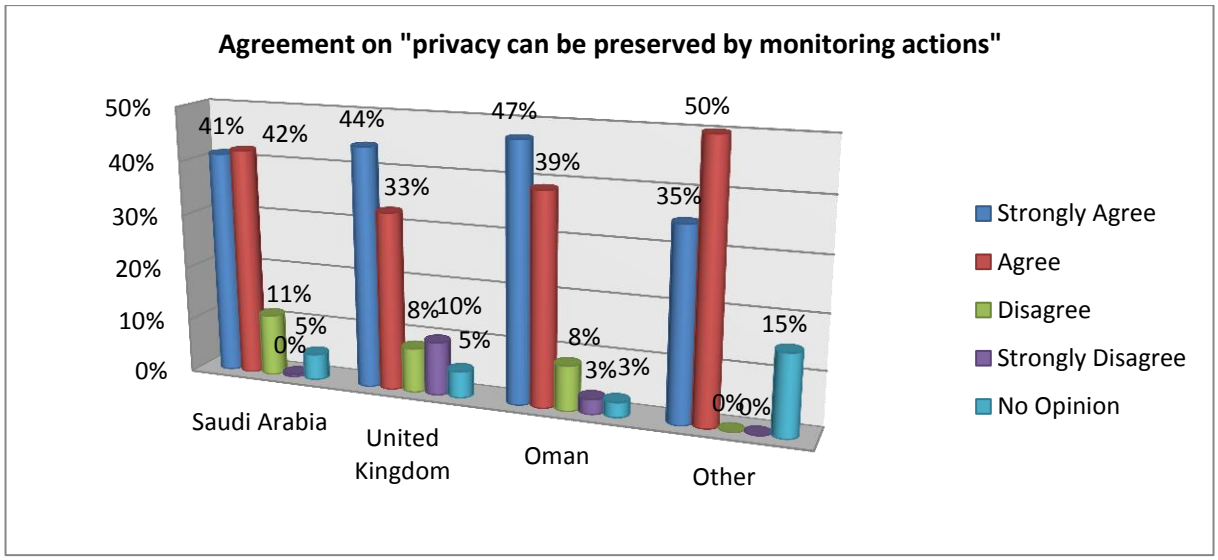
Appendix_Figure F.7: Agreement on "enabling users to have control over own data to preserve privacy"

Q12.Privacy can be preserved by monitoring how services providers manipulate users' information.

To what extent you agree with the statement?

	SA	UK	Oman	Other	Total
Strongly Agree	41%	44%	47%	35%	42%
Agree	42%	33%	39%	50%	41%
Disagree	11%	8%	8%	0%	10%
Strongly Disagree	0%	10%	3%	0%	2%
No Opinion	5%	5%	3%	15%	5%

Appendix_Table F.12: Agreement on "privacy can be preserved by monitoring actions"

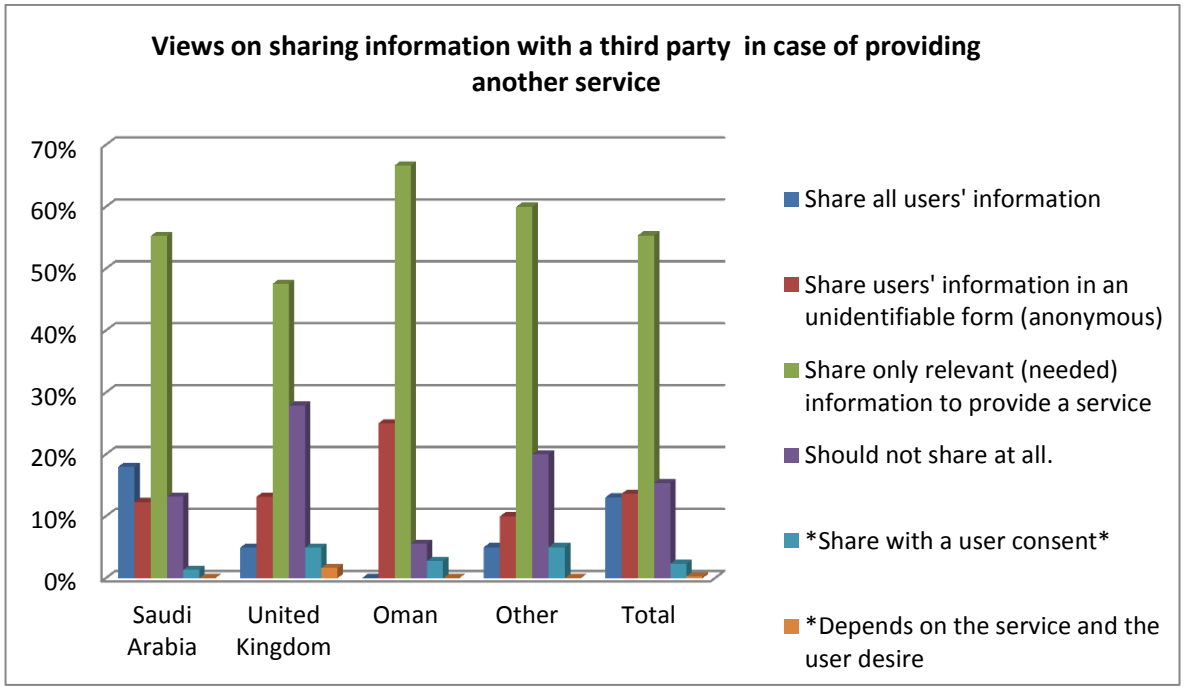


Appendix_Figure F.8: Agreement on "privacy can be preserved by monitoring actions"

Q13.(a) To what extent can government agencies share a user information with other agencies and/or with third parties who are providing a service to the same user?

	SA	UK	Oman	Other	Total
Share all users' information	18%	5%	0%	5%	13%
Share users' information in an unidentifiable form (anonymous)	12%	13%	25%	10%	14%
Share only relevant (needed) information to provide a service	55%	48%	67%	60%	55%
Should not share at all.	13%	28%	6%	20%	15%
Share with a user consent	1%	5%	3%	5%	2%
***Depends on the service and the user desire**	0%	2%	0%	0%	0%

Appendix_Table F.13: Views on sharing information with a third party in case of providing another service

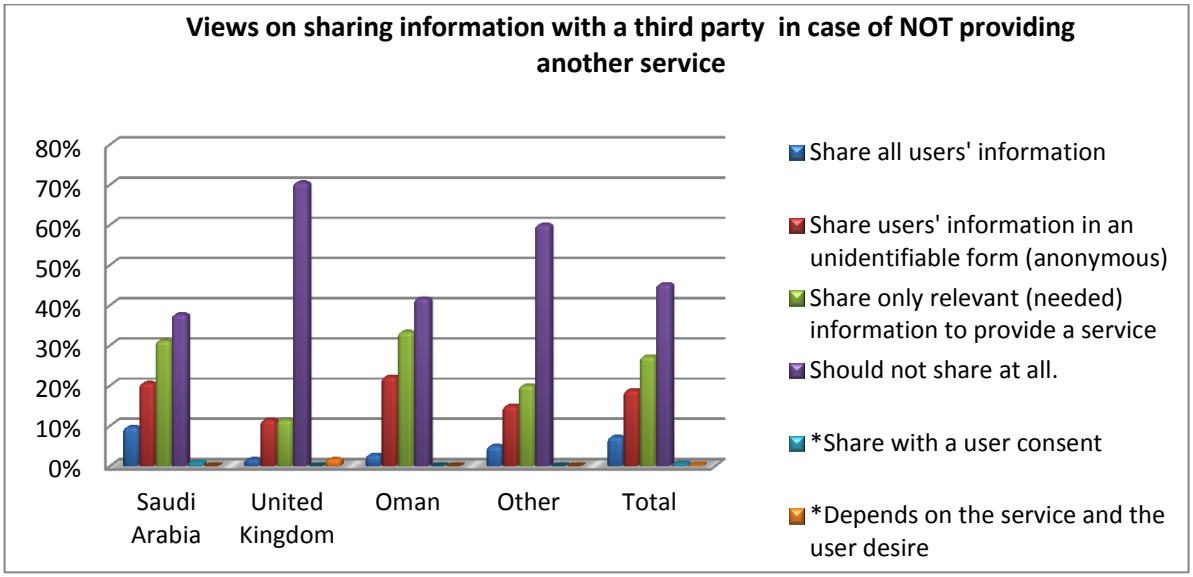


Appendix_Figure F.9: Views on sharing information with a third party in case of providing another service

Q13(b): To what extent can government agencies share a user information with other agencies and/or with third parties who are NOT providing a service to the same user?

Answers	SA	UK	Oman	Other	Total
Share all users' information	10%	2%	3%	5%	7%
Share users' information in an unidentifiable form (anonymous)	21%	11%	22%	15%	19%
Share only relevant (needed) information to provide a service	31%	11%	33%	20%	27%
Should not share at all.	38%	70%	42%	60%	45%
***Share with a user consent**	1%	0%	0%	0%	1%
***Depends on the service and the user desire**	0%	2%	0%	0%	0%

Appendix_Table F.14: Views on sharing information with a third party in case of NOT providing another service

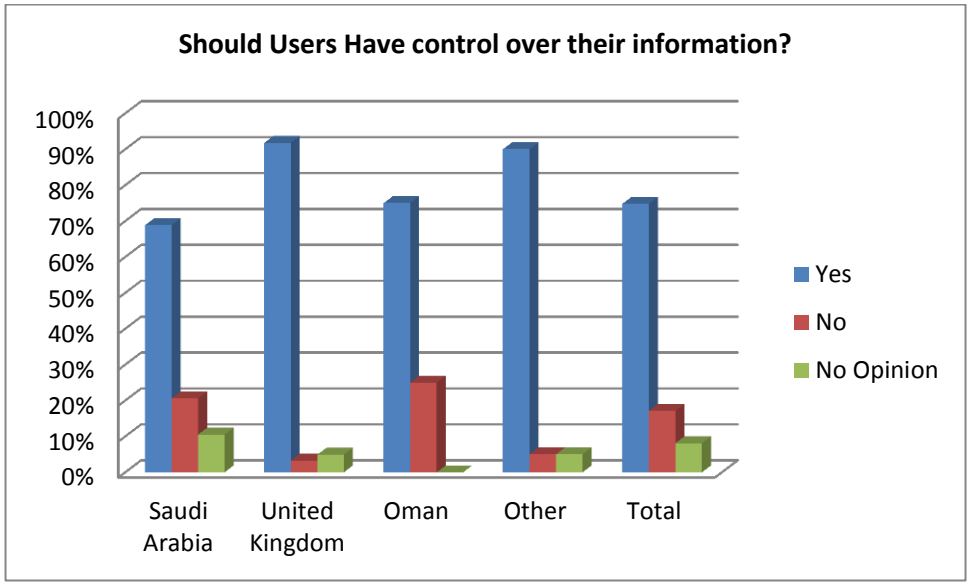


Appendix_Figure F.10: Views on sharing information with a third party in case of NOT providing another service

Q14. Should users have control over their information when using e-government services?

	SA	UK	Oman	Other	Total
Yes	69%	92%	75%	90%	75%
No	21%	3%	25%	5%	17%
No Opinion	10%	5%	0%	5%	8%

Appendix_Table F.15: Should Users Have control over their information?

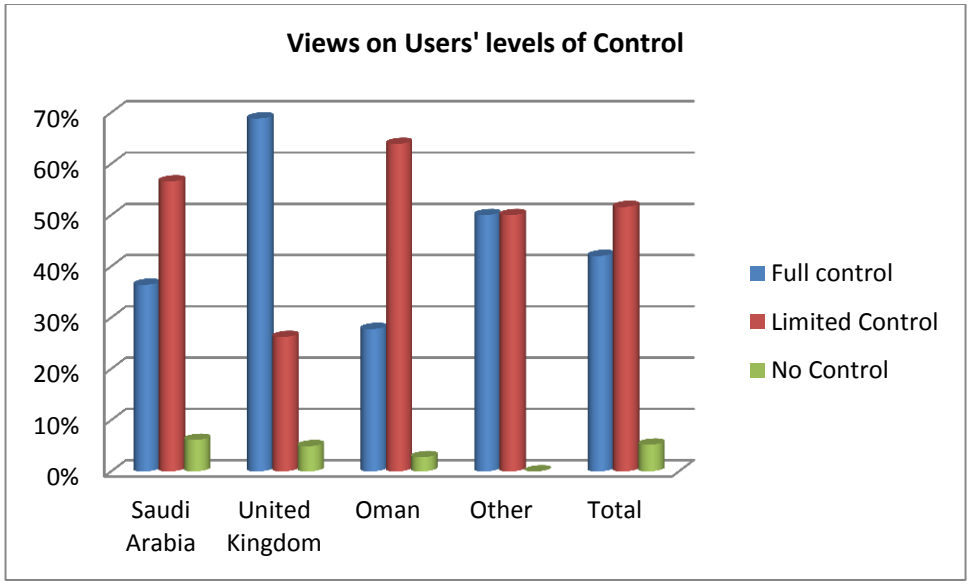


Appendix_Figure F.11: Should Users Have control over their information?

Q15. To what extent should users have control over their information when using e-government services?

	SA	UK	Oman	Other	Total
Full control	36%	69%	28%	50%	42%
Limited Control	57%	26%	64%	50%	52%
No Control	6%	5%	3%	0%	5%

Appendix_Table F.16: Views on Users' levels of Control

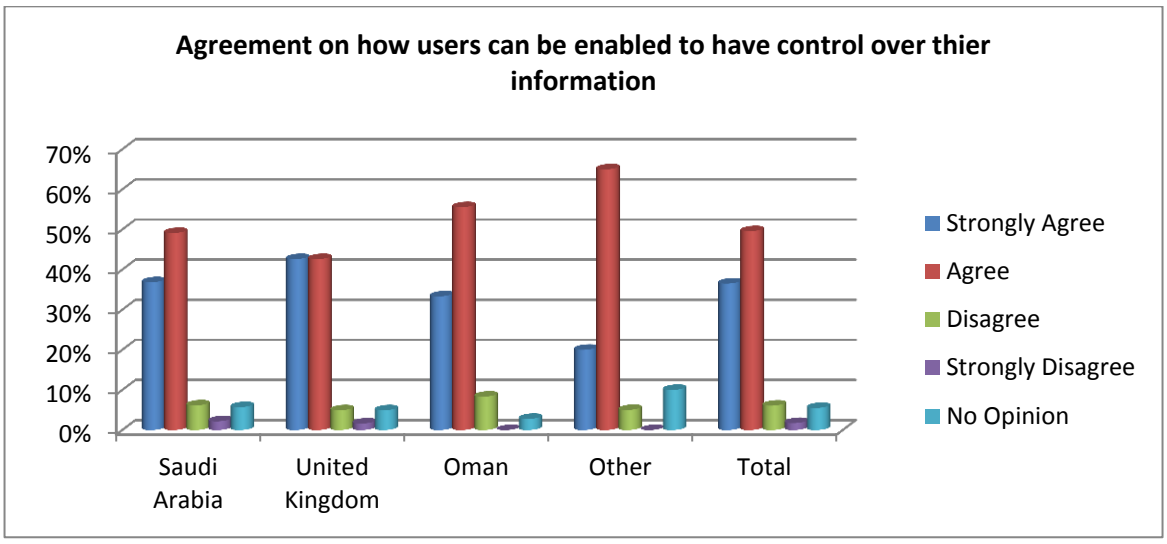


Appendix_Figure F.12: Views on Users' levels of Control

Q16. Users can be enabled to have control over their information by allowing them to apply a desired level of control over the whole or part of their information throughout the processing of that information when using e-government services. To what extent you agree with the statement?

	SA	UK	Oman	Other	Total
Strongly Agree	37%	43%	33%	20%	37%
Agree	49%	43%	56%	65%	50%
Disagree	6%	5%	8%	5%	6%
Strongly Disagree	2%	2%	0%	0%	2%
No Opinion	6%	5%	3%	10%	6%

Appendix_Table F.17: Agreement on how users can be enabled to have control over their information

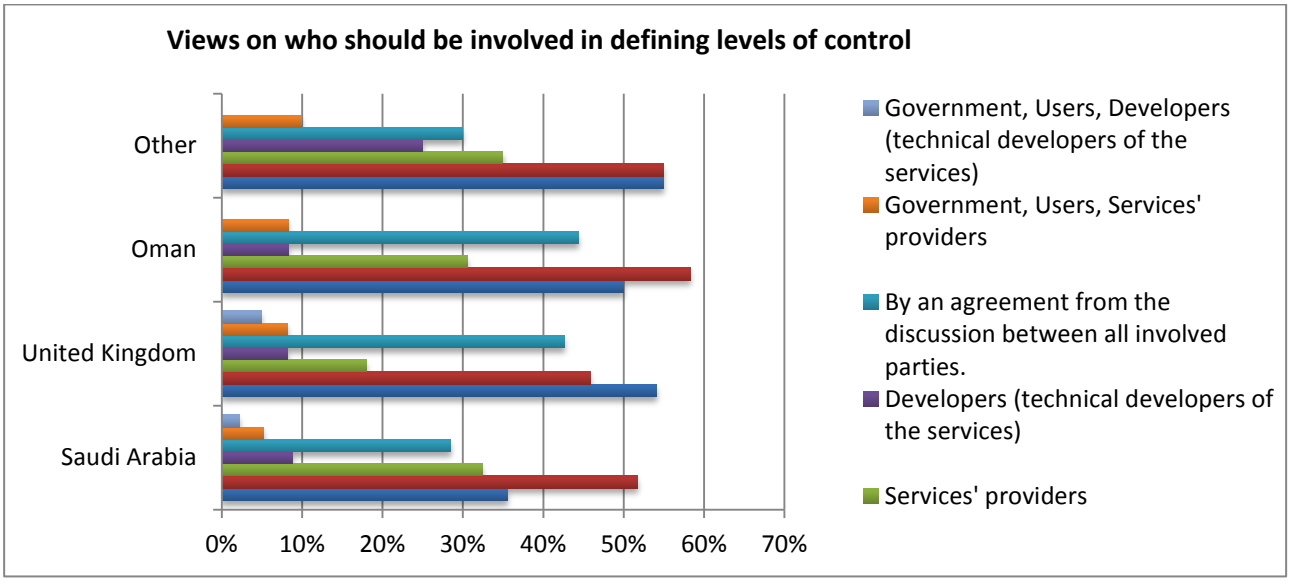


Appendix_Figure F.13: Agreement on how users can be enabled to have control over their information

Q17. Who should be involved in defining the levels of control on information held about users?

Answers	SA	UK	Oman	Other	Total
Users	36%	**54%**	50%	55%	41%
Government	**52%**	46%	**58%**	**55%**	**52%**
Services' providers	32%	18%	31%	35%	30%
Developers (technical developers of the services)	9%	8%	8%	25%	10%
By an agreement from the discussion between all involved parties.	29%	43%	44%	30%	33%
Government, Users, Services' providers	5%	8%	8%	10%	6%
Government, Users, Developers (technical developers of the services)	2%	5%	0%	0%	2%

Appendix_Table F.18: Views on who should be involved in defining levels of control



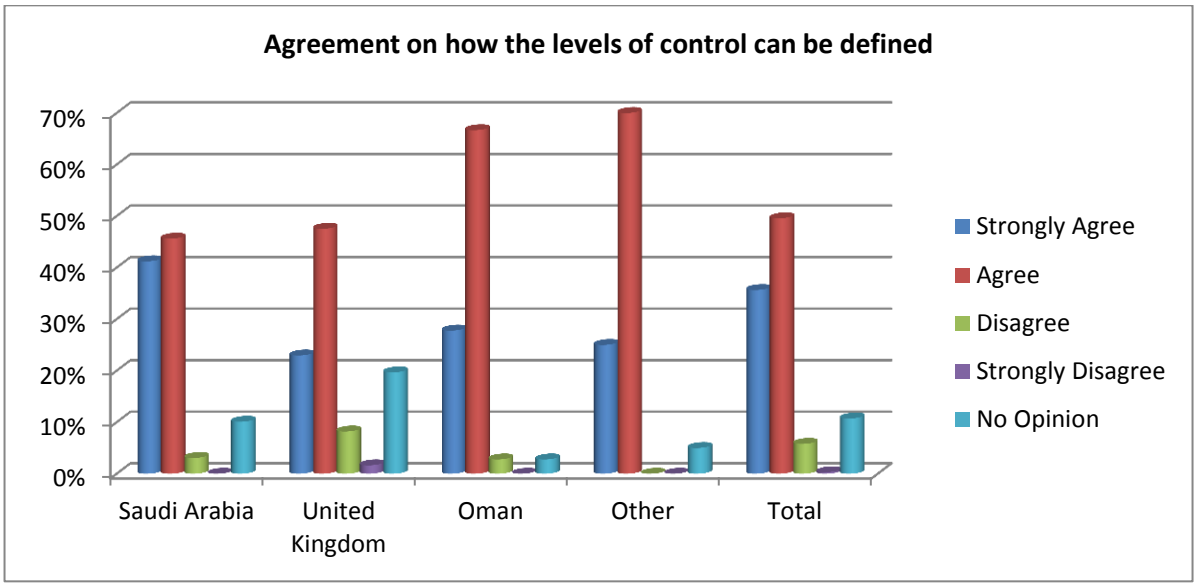
Appendix_Figure F.14: Views on who should be involved in defining levels of control

Q18. The levels of control for enforcing the protection of users' information can be defined by grouping selected sets of security rules into levels of control based on the level of risk identified on users' information while considering relevant standards and guidelines.

To what extent you agree with the statement?

	SA	UK	Oman	Other	Total
Strongly Agree	41%	23%	28%	25%	36%
Agree	46%	48%	67%	70%	50%
Disagree	3%	8%	3%	0%	6%
Strongly Disagree	0%	2%	0%	0%	0%
No Opinion	10%	20%	3%	5%	11%

Appendix_Table F.19: Agreement on how the levels of control can be defined

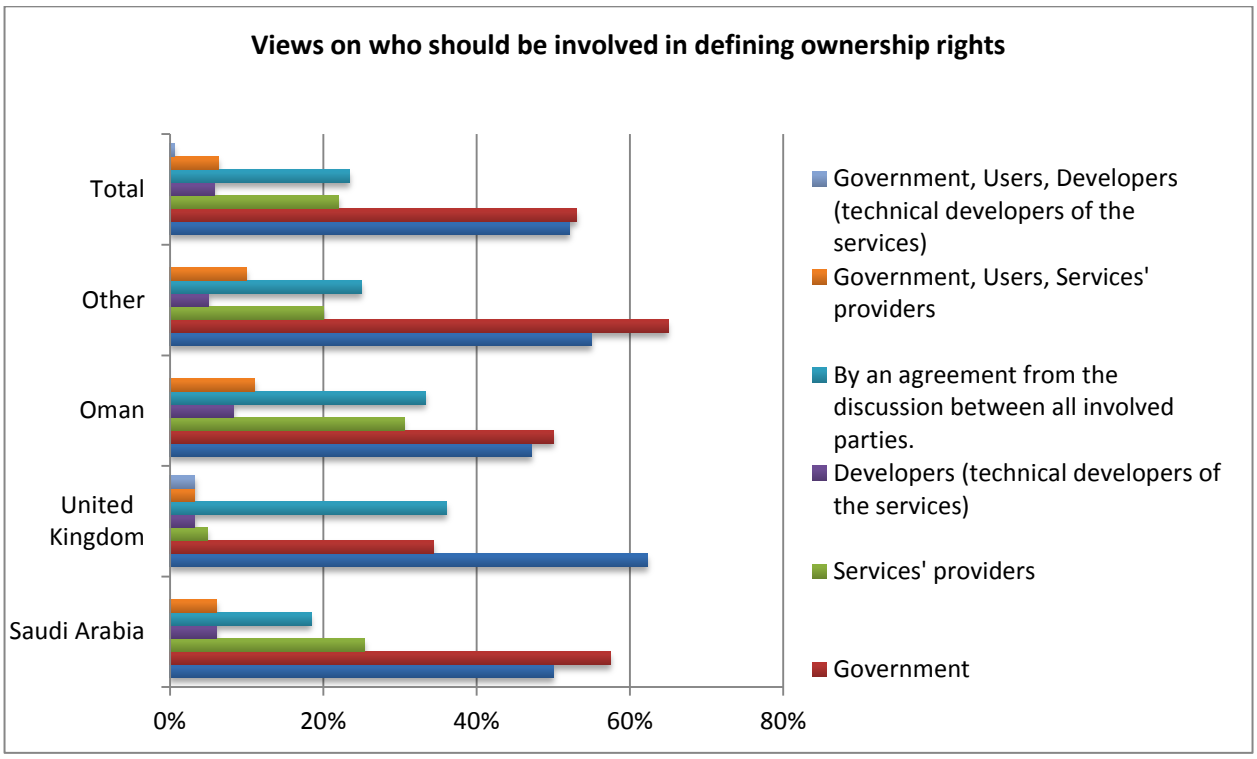


Appendix_Figure F.15: Agreement on how the levels of control can be defined

Q20. An ownership right of a piece of information is a right that shows who owns that piece of information. Who should be involved in defining the ownership rights of information about users of e-government services?

	SA	UK	Oman	Other	Total
Users	50%	62%	47%	55%	52%
Government	57%	34%	50%	65%	53%
Services' providers	25%	5%	31%	20%	22%
Developers (technical developers of the services)	6%	3%	8%	5%	6%
By an agreement from the discussion between all involved parties.	18%	36%	33%	25%	23%
Government, Users, Services' providers	6%	3%	11%	10%	6%
Government, Users, Developers (technical developers of the services)	0%	3%	0%	0%	1%

Appendix_Table F.20: Views on who should be involved in defining ownership rights

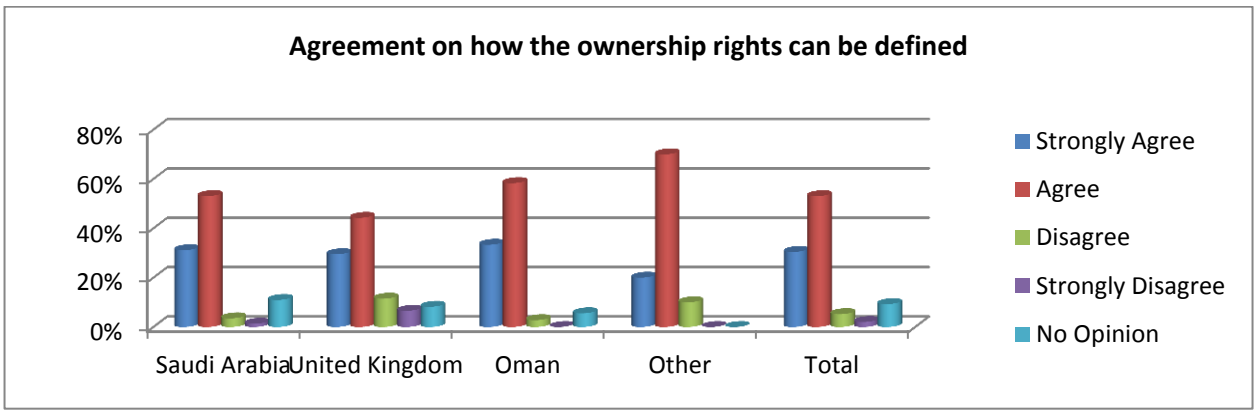


Appendix_Figure F.16: Views on who should be involved in defining ownership rights

Q21. Ownership rights can be defined by identifying who own each piece of information collected about the user and specifying what can the owner do with that piece of information at each stage of processing that information. To what extent you agree with the statement?

	SA	UK	Oman	Other	Total
Strongly Agree	31%	30%	33%	20%	31%
Agree	53%	44%	58%	70%	53%
Disagree	4%	11%	3%	10%	5%
Strongly Disagree	1%	7%	0%	0%	2%
No Opinion	11%	8%	6%	0%	9%

Appendix_Table F.21: Agreement on how the ownership rights can be defined



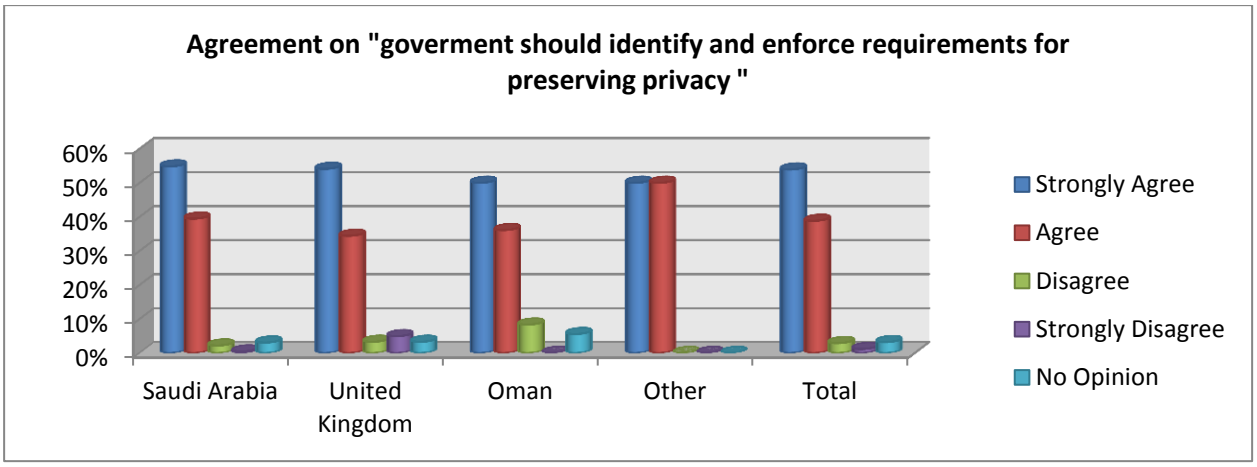
Appendix_Figure F.17: Agreement on how the ownership rights can be defined

Q23. The government should identify and enforce requirements for preserving privacy and require all e-government service providers to satisfy those requirements to ensure that users are enabled to have control over owned information when using e-government services.

To what extent you agree with the statement?

	SA	UK	Oman	Other	Total
Strongly Agree	55%	54%	50%	50%	54%
Agree	39%	34%	36%	50%	39%
Disagree	2%	3%	8%	0%	3%
Strongly Disagree	0%	5%	0%	0%	1%
No Opinion	3%	3%	6%	0%	3%

Appendix_Table F.22: Agreement on "government should identify and enforce requirements for preserving privacy"

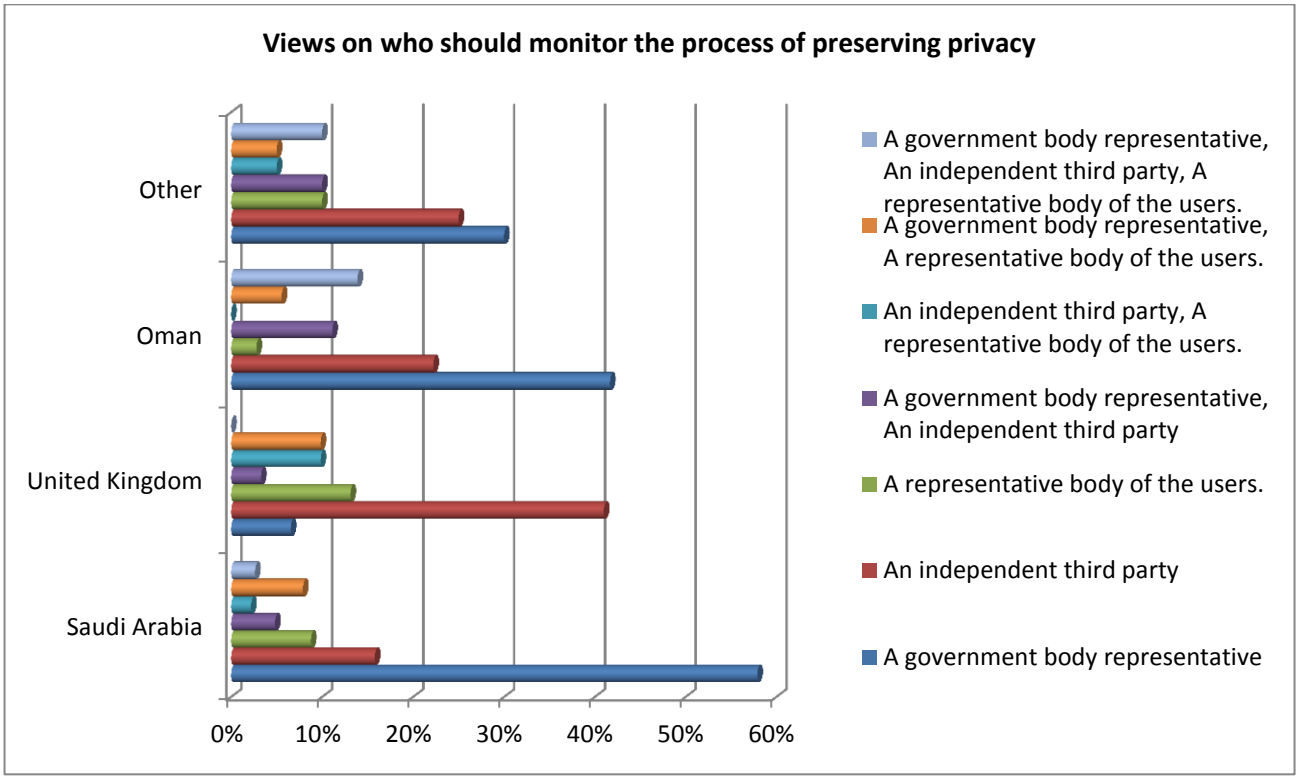


Appendix_Figure F.18: Agreement on "government should identify and enforce requirements for preserving privacy"

Q24. Who should monitor and assess the process of preserving privacy when providing e-government services?

	SA	UK	Oman	Other	Total
A government body representative	58%	7%	42%	30%	46%
An independent third party	16%	41%	22%	25%	21%
A representative body of the users.	9%	13%	3%	10%	9%
A government body representative, An independent third party	5%	3%	11%	10%	6%
An independent third party, A representative body of the users.	2%	10%	0%	5%	3%
A government body representative, A representative body of the users.	8%	10%	6%	5%	8%
A government body representative, An independent third party, A representative body of the users.	3%	0%	14%	10%	4%

Appendix_Table F.23: Views on who should monitor the process of preserving privacy



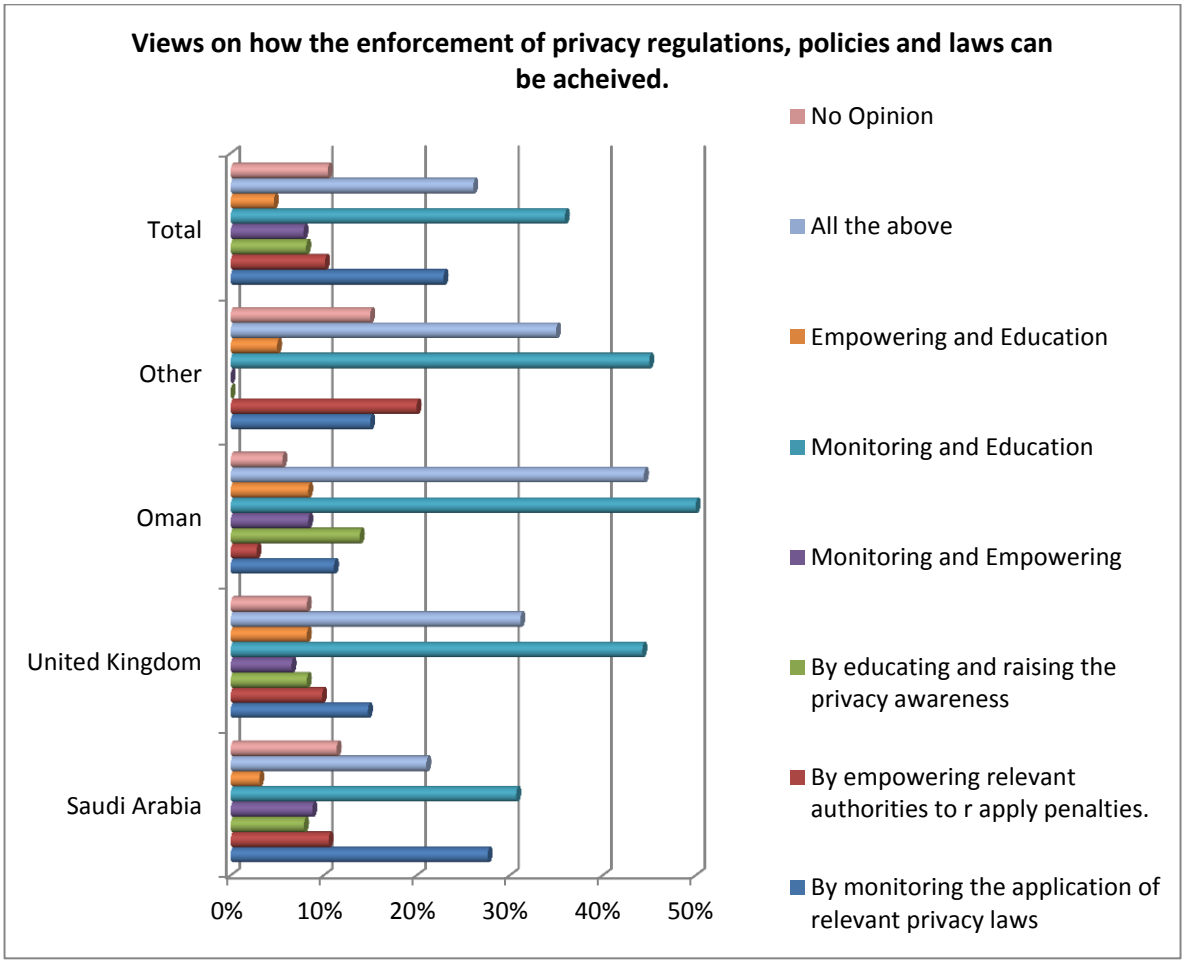
Appendix_Figure F.19: Views on who should monitor the process of preserving privacy

Q25. The enforcement of the applications of relevant privacy regulations, policies and laws can be achieved by the following (Selection of three choices): (You can select more than one):

- By monitoring the application of relevant privacy regulations, policies and laws by all involved parties in e-government services provision.
- By empowering relevant authorities to respond to any violation of relevant privacy laws by applying suitable stated penalties.
- By educating and raising the public awareness about privacy regulations, policies and laws.
- No Opinion

	SA	UK	Oman	Other	Total
By monitoring the application of relevant privacy laws..	**28%**	15%	11%	15%	**22.9%**
By empowering relevant authorities to apply penalties…	11%	**10%**	3%	**20%**	10.1%
By educating and raising the privacy awareness	8%	8%	14%	0%	8.1%
Monitoring and Empowering	9%	**7%**	**8%**	0%	7.8%
Monitoring and Education	**31%**	**44%**	**50%**	**45%**	**35.9%**
Empowering and Education	3%	8%	**8%**	5%	4.6%
All the above	**21%**	**31%**	**44%**	**35%**	**26.1%**
No Opinion	11%	8%	6%	15%	10.4%

Appendix_Table F.24: Views on how the enforcement of privacy regulations, policies and laws can be achieved.

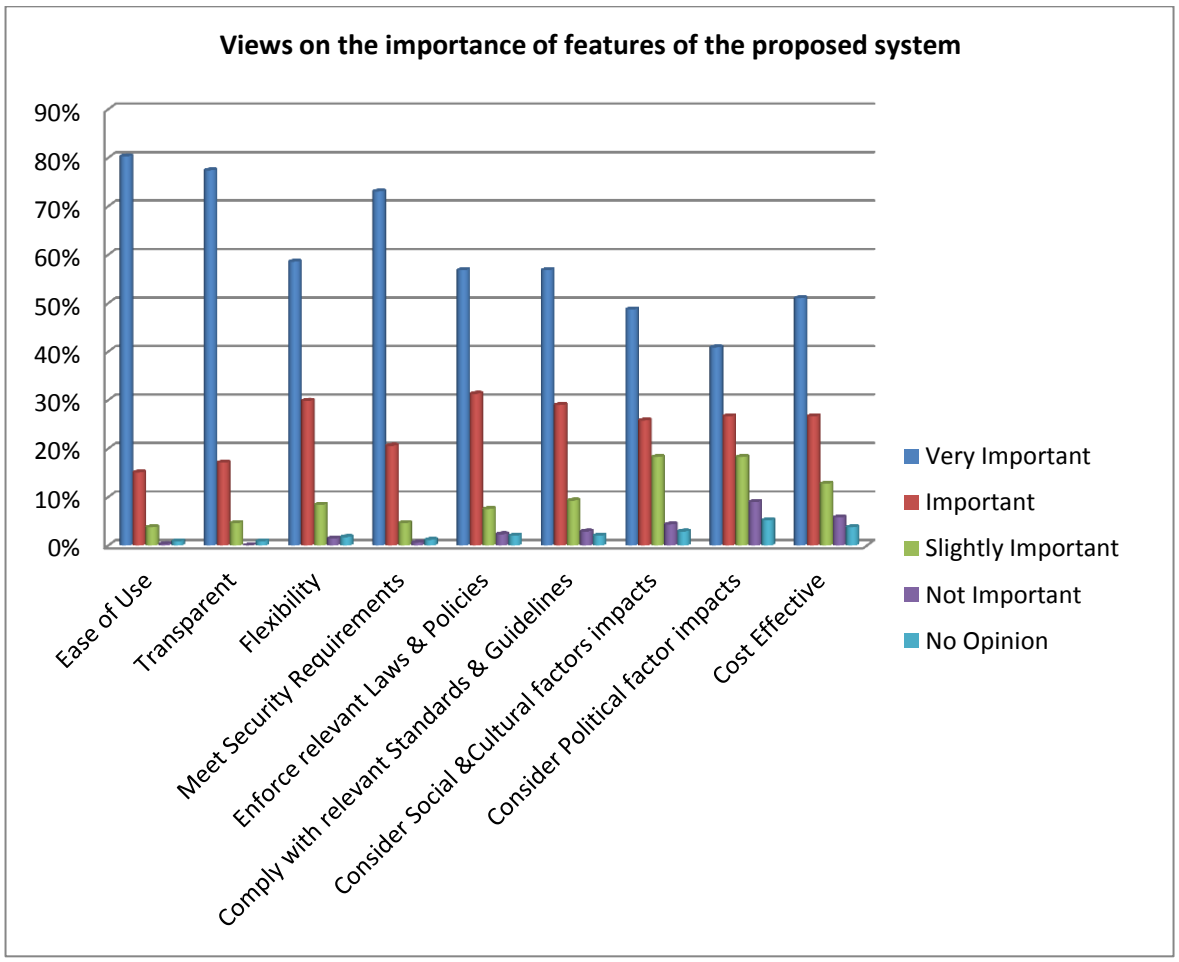


Appendix_Figure F.20: Views on how the enforcement of privacy regulations, policies and laws can be achieved.

Q27. In the future, a system for preserving privacy when providing e-government services should have the following features:

	Very Important	Important	Slightly Important	Not Important	No Opinion
Ease of Use	80%	15%	4%	0%	1%
Transparent	77%	17%	5%	0%	1%
Flexibility	59%	30%	8%	1%	2%
Meet Security Requirements	73%	21%	5%	1%	1%
Enforce relevant Laws & Policies	57%	31%	8%	2%	2%
Comply with relevant Standards & Guidelines	57%	29%	9%	3%	2%
Consider Social &Cultural factors impacts	49%	26%	18%	4%	3%
Consider Political factor impacts	41%	27%	18%	9%	5%
Cost Effective	51%	27%	13%	6%	4%

Appendix_Table F.25: Views on the importance of features of the proposed system

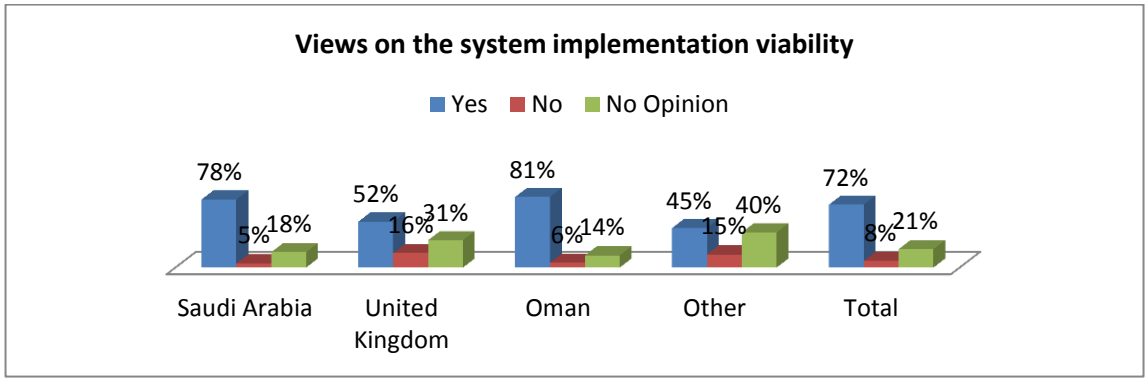


Appendix_Figure F.21: Views on the importance of features of the proposed system

Q29 (a). Do you think implementing such a system to preserve privacy is viable?

	SA	UK	Oman	Other	Total
Yes	78%	52%	81%	45%	72%
No	5%	16%	6%	15%	8%
No Opinion	18%	31%	14%	40%	21%

Appendix_Table F.26: Views on the system implementation viability

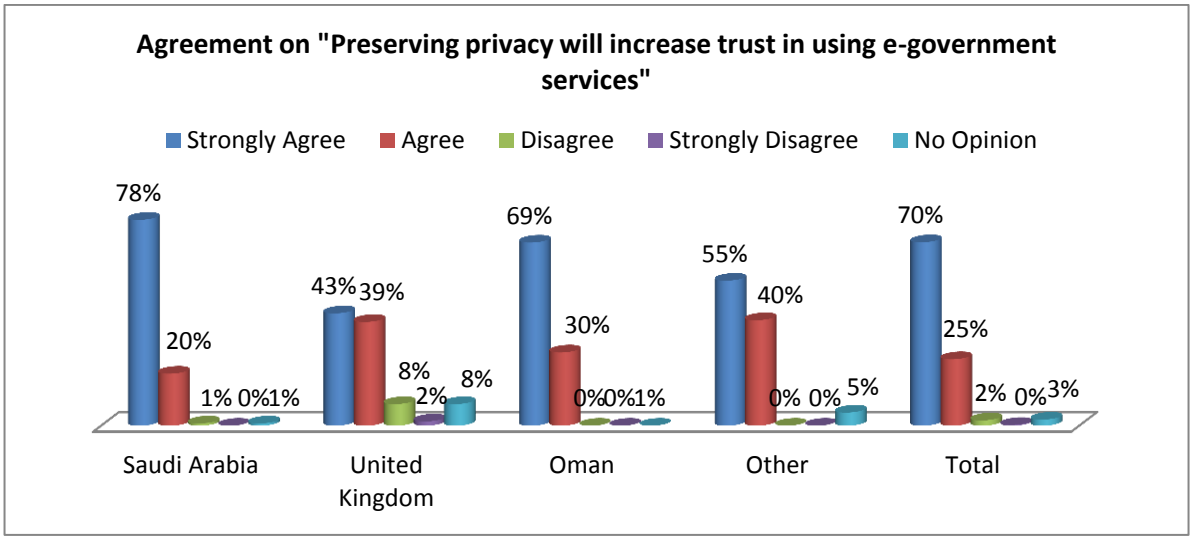


Appendix_Figure F.22: Views on the system implementation viability

Q30. Preserving privacy when providing e-government services will increase my trust in using e-government services?

	SA	UK	Oman	Other	Total
Strongly Agree	78%	43%	69%	55%	70%
Agree	20%	39%	28%	40%	25%
Disagree	1%	8%	0%	0%	2%
Strongly Disagree	0%	2%	0%	0%	0%
No Opinion	1%	8%	0%	5%	2%

Appendix_Table F.27: Agreement on "Preserving privacy will increase trust in using e-government services"



Appendix_Figure F.23: Agreement on "Preserving privacy will increase trust in using e-government services"

2. Open-ended questions:

Questions, Q19,Q22,Q26,Q28 and Q29(b) were open questions presented here a summary of the responses, note that all comments that were complementing(e.g thanks, all the best, etc.) or were confirming that no comments were included(e.g. no comments, only the above,etc.)

Q19: If you have other alternative suggestions for how the levels of control on users' information can be defined, please state it below: (17 comments)

1) It is very important for these control levels to be agreed by the legislative authority, who usually represent people (users) and defend their rights with no bias.
2) would need very high levels of user education to allow them to have "informed consent". The system should protect the user by providing some restrictive default position
3) High Securty
4) Defined by surveying potential users as a part of creating an account for a specific e-services.
5) the level of control should be negotiated between government and users. Service providers and developers should be given rigorous instructions about what control should be given to whom. Definitely no reason for developers to be involved in the discussion - they should only implement privacy requirements specified by system owners. Not quite sure why service providers should have access to private information - I do not think that they should, although there may be some cases where access is required - e.g. payments done via a bank and obviously bank as a service provider will required access to personal data. If you do not give access then they can not do the job. In this and similar situation there could not be a discussion about giving or not giving access to a service provider because there would not be service without that info. So with service providers it is context specific.
6) Subject matter experts to be involved to define these controls and gathering such requirements from the users themselves.
7) I wish that we advance in electronic services as the other neighbour countries to ease the loud on the poor citizen when he go to government agencies to get the services and avoid getting the services fast only if you know somebody inside the government agency.
8) Categorising the government agenciesand dividing the information according to what each governmetn agecny needs to know.
9) It depends on the nature of the provided service and accordingly the amount of information needed is determind
10) It should work as in thebanks where your mobile is a device for verifying your identiy in away to send the passowrd and the mobile is recorded as part of your personal information.
11) The user should have the freedom to determine the level of control he desire on all his information.
12) The government knows better :)
13) The information should be avialable electronically to all government agencies when required
14) I belive in information privacy and the right for indivuslas to keep their personal information safe and they only should categorise how important and secure any part of their information to them.
15) Mentioning this on the gvernment agency site to the users before the users start using the provideed services.
16) I do not agree and I suggest that only the user determine the level of privacy of his information, for example if the user has tow bank accounts one is very critical to him as he might expect large amount in it and does not want any one to know aboutit while another one he doesn't care if the information about this accoutwas known to the world. So the sensitivity and importance of an indivisual's information change with the changes that happen to that indivisual.
17) The person who should have control on e-government electronic servies or any thing relate to the socity should be a very responsible one and someone who respect the privacy of others.

Q22:If you have other alternative suggestions for how ownership rights of information about users of e-government services can be defined, please state it below: (6 Comments)

1) see information on the ICO website
2) Keep this information in safe
3) I strongly believe that information should be own by an individual and he\she should have all rights regarding that info. For example the situation with credit reports seems ridiculous to me: I spend money etc. then someone collects that info and sells it to others and to me as well. I do not own that info - I cannot change it and I cannot even access it for free. I cannot make a claim to change it if I disagree. I think that it even breaks the privacy legislation but it still works that way.
4) Put legal conditions on the service provider that is in favor of the user.
5) Ownership rights has a specific definition and should not be speculation while there is a specific definition.
6) Telling the user about his right before providing the service or using it

Q26: If you have alternative suggestions for how privacy regulations, policies and laws can be enforced, please state it below: (12 comments)

1) show awareness advert on TV about privacy and copyrights
2) 3rd party with power to fire people responsible for violations
3) It is the maturity of the laws in the government .. If the laws are absent then privacy protection is bogus .. There is no body to enforce the claims of privacy ..m
4) "I concerned about what do you mean by (Government). However, as known in any country (or should be) there are three independent authorities; the legislative authority, the execution authority and judicial authority. The law is the criterion"
5) by setting laws that protect user information
6) They shoud ask for right to use
7) Governmental investment in such research
8) through royal decree, national law, and demand from the public.
9) Establish an electronic court speciallised in applying penalities on those who violaite the laws and policies and exploite privacy which people can file complaints to either elctronically or in the traditional way.
10) Establish a High court for electronic cases that is administred by the government
11) Policies and guidelines should be applied by the authorities and should have the nature of governing laws
12) Mention it in the e-government service before providing the service

Q28: Is there any other features that you think a system for preserving privacy in e-government context should have? If Yes, Please state it below: (13 comments)

1) All the above in Q 27(features) must be showing in plain language that enable the user to understand all the terms and conditions
2) User interface system, or a web page to let the user by whos the information is used
3) Priacy should state clearly the extent of exposure of information pertenant to the individuals .. Who is using it, and for what purpose that should be before committing to use the egovernment services .. For sure such information should be clear off hand ahead of time ..
4) aware the users about most dangerous threats that might happen when the privacy compromised
5) "persistent, how will you authenticate and enroll people(users) into the system"
6) Stability and maintenance
7) A clear understanding of purpose. Privacy in passport applications is not the same as privacy in paying fines, sending in company returns or registering the purchase of a house.
8) first of all it should work ;-)
9) To let the user know when and by whom his inofrmation was accessed and what information was accessed and who benift from that.
10) The governer is the one who will gurantee preserving privacy and the quality of application of such a system and the monitoring process.
11) It should be a system run by a specifc government agency not by another agency

12) Security and Privacy of information
13) A feature to enable the user to know who and when his information is viewed or accessed

Q29(b): Please explain the reason for your answer in Q29(a) if it was Yes or No? (114 comments)

Note: (Q29(a): Do you think implementing such a system to preserve privacy is viable?)

1) The technology and knowledge is available. Governments just need the desire to do so.
2) Yes it can be. If Gov, users and ISP comply with regulation.
3) (No), such systems depend on people as well as the system. E.g. I can read private info as part of my job, and then tell my mates about it.
4) Because i think anything desired is viable
5) Will have more trust and valuable
6) but i think it requires too much work and long time to implement it
7) Important in order of privacy as information will be more secure
8) E-government is a necessity... Security is a necessity.. And being transparent about the information and its use should not be an issue.
9) To increase the trust. This, helps citizens to use e-services
10) "As stated previously about the meaning of (Government), but if the system satisfies these criteria: the independent legislative authority agreed and issued the proposed legislations and policies, and also involve in monitoring the execution authority, which provide the services. Also satisfy all other criteria stated above."
11) It should be viable
12) (No), "because system will be administrate by different entities which will put user privacy at risk! Privacy can be preserved by user not by system. Anyone who has an access to this system will have access to the user privacy."
13) It's important to insure that personal information shall only be used where needed and not misused or disclosed by any other means.
14) To make the system reliable and secure.
15) learning from international standards (e.g. data protection act in UK) and customizing to local context is not something impossible to do
16) “But will need political will and money/resources. Is it not just an engineering problem? What are your success metrics?”
17) Such system will encourage citizens to use effectively the e-gov. Services which is the main goal of the e-gov. This will also encourage the process of sharing opinions in decision or policy making.
18) It’s only a decade since such e-services became essential to governments and improvement is needed to protect any intrusion.
19) If you know what you're trying to do with the data you can define privacy in that context, and architect the system to meet that definition. There is no one set fits all definition (imagine refusing to let the police process your data to prosecute you)
20) Increase the security level and public trust
21) As long as you can formulate clear privacy requirements it is technically possible to implement them. The main problem is not with implementation but with eliciting the requirements suitable for every party involved.
22) yes because many user will trust the system
23) If we have policies and regulation that preserve the privacy of people, then a system through IT or business process should be implemented and exist in place that accommodate to privacy policies.
24) (No),Cost and unwillingness from Government
25) (No), Government bodies will not be prepared to reduce the controls they currently hold
26) (No), currently insufficient funding, knowledge or political will, but this is the time it should be done!

27) I don't know, but because there are many similar systems and governments in general are more into usign technology.
28) "Nothing is impossible, even if we are a bit behind in technology, but most important that the system is done without any curroption and then it will be successful
29) Yes it is possible if there is people with fear from god andthose who won't use such system to serve their own needs and personal goals.
30) Because most of the people in the socity with different backgrounds are using internet and able to use electronic means.
31) The world is developing and our country is able to do this financially and intellecutally with God will .

32) When the best using conditions are provided.
33) It is the citizen and the user right to be able to have all the services while preserving his privacy
34) Because all resources are available
35) Yes it is possible, because there is nothing that might prevent such a system from being implemented and it will serve the socity a lot.
36) To make it easy for the user and the employer to reach the information and to save time.
37) Because it is has been applied in some European countries and why not we apply it
38) because it is important and we need it to make it easy for us to use e-government services.
39) Any thing can be done with effort and presistance.
40) Nothing impossible
41) Technologies are advance and human brain can develop it more and made it serve him.
42) We are in a world of information and modern technology and now there are ways to protect information using programs and networks and devices that can be count on to do what is required.

43) (No), We have traditions and laws in our country Saudi
44) Yes , but in long years to come.
45) With the existance of all financial and human resources.
46) So it will be easy for the user to follow up on a service from home or work instead of going to the government agency by himself, etc.
47) The idea exists in reality, all what is needed is some improvement in the system and raise awarness between people.
48) Because of the huge advance in technology in all fields and the eas of use
49) After all, there is nothing impossible
50) Because it is important to implement this system in an effective strong way and to provide flexibility to the users of the system. It is important to provide security and privacy for users to protect all their personal information.
51) It is applied in developed countries and I have l experiences because it is really applied.
52) (No), we do not have enough experience.
53) Around 40% of this is applied already, what is left is add the privacy and security on it and this need a study of the current system and find a way to give the permissions.
54) Because now the system is available in mini version.
55) So there will be privacy consideration when information are secured
56) By improving the communication between the users and the government agencies using effective secure and fast systems that both parties can benefit from it.
57) Yes because the country is walking towards electronic government so this require keeping a continuous progress to simplify services and guarantee the providing of services in the easiest and fastest way.
58) Nothing impossible
59) Maybe the problems that come as a result of stealing data and information will convince the society and the world with the need to impose such system.
60) Easy if been studied well with good planning and implementation

61) Does not require a great effort only sincerity in action
62) If all resources exist and are available
63) When the laws and regulations are established they can be programmed in the portals of e-government... and then the users can be educated on the way to use it
64) (No), As long that there are some limited mentalities I do not think that
65) Because everything is available
66) Nothing is impossible
67) It will result in ensuring the productivity of individuals and ensuring an end to their worries about their privacy by this system and save time for those work on providing these services in an easy way with no interruptions from people who want to enquire about their services and give the individual the opportunity to follow up on their related services from anywhere and put it electronically because the individual is the key element in the productivity and his physical and emotional comfort will makes him feels that his interests kept and cared about and goes with the interest of the organization that he works within.
68) Because as far as I know it is already applied in some countries
69) Because there is nothing impossible now.
70) In case there was a gathering of those with the required expertise we can build a system that can be ideal.
71) This system is an advance one and the kingdom is looking very hard to provide the best electronic system
72) Applying the electronic services is possible and it is the trend of all countries because of the ease of use and the coverage of a wider part of the society that is possible and this system can be applied with an essential consideration of information security.
73) I agree because it has been applied in different areas such as the system of benefits for example "..... system"
74) With collaboration between all parties and agreement on what benefit all involved parties.
75) For sure it is possible because it is applied in a lot of developed countries and what is left is the interest and desire in implementing such a system which is the most important factor.
76) The technical advancement and the international collaboration ensured the ability to do it.
77) There are a lot of genius minds in our country... and they have proved their presence in the west with what they provide in their projects and good ideas...so without doubt we will find who will implement such a system in reasonable costs and high quality because they are the sons of the homeland ..
78) With the advance technologies in computer systems this can be achieved
79) It is possible because we have all the financial resources to implement high tech system that can link all government agencies and the system can determine the right piece of information for each government agency in a way that protects the rest of the information
80) Finding such a sophisticated system is not very difficult, however, we need to understand the meaning of privacy then after that we can use advance technologies in an easy matter.
81) Because this is available in some sites and not in other sites and it should be applied in all sites and on everybody.
82) We have all the required resources but we lack the intellectual resources and awareness
83) Yes, because electronic services became easier to use and made it easy to access most of the current services either from the government or from others and this will help the society especially women in Arab world as it will help the woman to get the services by themselves. From another perspective, it also a fast flexible and useful way to work, however there is people who do not respect the place that they work on and prevent the chance to get a fair government services and the solution is to respect this work from those who have responsibilities towards it.?
84) The least right for an individual in his society is that his personal information are kept secure and well protected so that there will be a trust in electronic services and if this trust was shaken there will be boycotting to the use of electronic services and least trust in the strength of monitoring from the government to the agencies or the services providers.
85) Because the user has the right to know who is viewing and sharing his information and it is a personal right.

86) It is difficult to apply in our Arab world because of the weakness of planning.
87) There is no real privacy in the internet as all applications can be hacked and it differs in the possibility of hacking it as some are easy to hack and others are difficult to be hacked but nothing is impossible in this matter.
88) The implementation of this system is possible in current time due to the advancement of science and to keep up with the world as the world went to the electronic government for easy archival and retrieval of information and to save efforts and money
89) Because there is no difficulty in implementing it.
90) Because I will make things much easier for people
91) The huge advancement in software and the ability to control and adapt programs to the needs
92) Everything can be possible if there was collaboration in the efforts and a suitable environment to achieve it.
93) Because the government is developing in using electronic services and keeps up with the advancements which is an essential requirement in the coming years. However, developing the services that will protect the user and make the citizen knows his rights and raise the awareness may take time and we might face difficulties in applying this so there should be enforcement for strict policies that will change the culture of the Arab nation, but this system is not impossible.
94) Possible especially with the advancements happening in electronic services and it became an essential in current time
95) Because the government departments are so crowded and work is delayed in many occasions
96) Yes, because of widespread fraud and impersonation and the consequent crimes without any sanctions
97) I believe it will be used by all parties and in my opinion the society will accept such a system in much welcome.
98) Because of advancements
99) If we had a real organisation then we will have a realistic application
100) If there was scientific planning for this system and we learn from international lessons and experiences in its strength and weaknesses sides so we can benefit from the strengths side an avid the weakness sides.
101) Data and information is so important now. I personally don't like the idea that I'm used as a number and so as a person due to the amount of data they have on me as an individual, and us as individuals. Therefore keeping my information private is very important to me.
102) Such systems are essential to the use of information, and should have been implemented from the start. The cost of implementing these systems is as nothing compared to their value. While these systems may require more administration than their absence, government agencies have shown time and again that they cannot be responsible for large amounts of user data, and handle it carelessly -- this must stop.
103) It is more than possible to develop such systems if the government body's take some advice from the industry. However, governments are classically poor at developing such systems.
104) There is far too much information being held, not just by government, but also by other organisations, companies, etc. that mean that it is very difficult to see the flow of information between them. If a user says they want this information to not be given to an organisation any more, how long will it take for the information to be removed?
105) Not viable - conflict of interest with 3rd party organizations - more information is better for them to better target services; however more information is potentially making it possible to have user identifiable information shared.
106) Privacy levels are very subjective and there will always be opposition to any suggestion to change privacy rights. People are very uncompromising when discussing their privacy and seem to see any change in policy as a way to introduce a potential loophole.
107) Unlikely to ever get agreement or representation from all parties to come to a conclusion. Unlikely to find any one individual to take responsibility for making overall decisions on privacy policy, and unlikely to ever get the right people together at the right time to make actual decisions instead of just talking
108) Without the agreement of Users; Government would not get engagement with Users; therefore they must provide assurance at all stages that data will be protected and not misused.

109) Technically it's easy to achieve (although clearly expensive). The difficulty would be in getting all the necessary bodies to buy in to the system, and enforcing its use.
110) People have the right to decide what information they wish to disclose, that is what the foundation of democracy is built on.
111) Raising standards to higher levels - rather than meeting minimum requirements as has been the tendency in the past - would serve to avoid many of the incidents of breached security and compromised data that have occurred.
112) Some-one will always find a way to cheat the system or hack into security documents to get the information they want. Technology is too vast to put limitations on most things.
113) It should be easy and a right for each user to have a say on what their personal information is used for. A system to ensure this is easily achievable.
114) Can be done with the collaboration between the efforts of the government and the local communities that deal with the citizens' matters and applying the related laws

General Comments(at the end of the survey): (17* comments)

1) These questions were far too complicated for a general survey.
2) In my opinion Governments may easily do that, if they wanted, by being the main service provider. In another language, by setting the company their selves and open >49% for private sectors for sake of cost effectively. Also, can be done by simply force any interested private sectors; I mean private sector work without government share, to employ a bodies from government to control the privacy. Those people can still be loyal to government if they get paid by them, so it's crucial who pays to those government employees. Thank you
3) For me, my decision to submit my data for any e- government service is decided by how much I need the service and how sensitive is the data requested to get the service... Usually the data to be entered for all government service is my national ID; the rest is already owned and issued by the government... So they (the government) got all my data... Now the other data such as health data and its privacy is a priority... Here I will think twice because my data and the privacy are not in the interest of the government... In short the government is trusted with sensitive data... The problem with other the lack of laws that govern the protection of privacy...
4) Attention should be drawn to companies controlled by the government such as … that violates users' privacy big time. They share users' data with third party (public and private) that bombard us with calls and SMS.
5) Nowadays, in some cases governments require their people to use only e-government services. So, trust is not part of the equation because there is no alternative (i.e. it's not a commercial product). However, preserving privacy is a matter of right that government should preserving while providing any services.
6) Preserving privacy is very important and needs a viable and implemented system.
7) At this time electronic governments are an important requirement for all due to the way it speeds the achievement of government services and other services while saving time and effort. However, the application of the system legally and the success of e-government is based largely on users' trust in the privacy of their personal data, so e-government services' providers must take into account the consideration of preserving absolute privacy for the users' data keeping it confidential in a way that no one can view it except the one who is responsible of providing the services or the employee who providing it.
8) I hope that someone benefits from your questionnaire and your thesis and that it is submitted to government bodies in the country or any country that has an e-government plan, as the electronic government became a very urgent requirement and must be achieved in a safe and confidential way and provided easily.
9) I wish you success and May Allah blesses you/ the subject should be put into government agencies and not only the society because it is really very important.
10) I suggest that if the system was explained in a simple way before the survey start it would make the picture clearer when filling the survey.

Appendix G : EduPortal Case Study

a) Preliminary Phase Stakeholders Interviews Summary

Important Note: Due to the sensitivity of the given information and the conditions imposed by the government agency who agreed to participate in the case study, the exact transcript of all the interviews at all stages was not provided, however, quotes from the interviews were given where appropriate.

First Interviews Structure and Questions:

First the goal of the interview was explained and the framework aim and stages were explained in simple language. Next, the interviewees were shown a drawing of a general workflow of the selected services and different positive and negative (or abnormal) scenarios have been discussed. The Interviewees were shown the definitions proposed by the PRE_EGOV framework for the data classifications, ownership rights and levels of control and how the data types are mapped by the proposed framework. The following general questions were asked for all the categories of the interviewees:

- Q1: What are the most services used in EduPortal Services?
- Q2: Do you have any privacy concerns with the current systems when you use/process any of the provided services? If yes what are they?
- Q3: Do you find the definitions clear? If not which one is not clear?
- Q4: Do you agree with the definitions? [each group of definitions was discussed separately and then the data mapping was explained]
- Q5: What possible risk you might encounter if information about you/about the user were compromised?

The following questions have been asked to Users category:

- QU1: Which information that you worry most about your privacy when processed and to what level?
- QU2: How will you classify information about you used by the system using the following data classification (Restricted, Sensitive, Private and Public)?[The definitions of the data classifications where explained by examples to the interviewees]
- QU3: If you are allowed to have full control on the information about you, what information you believe that you should be the only one who has control on it?

The following are the main questions that have been asked to interviewees from the other stakeholders' categories (Government body representative, services provider representatives and developers) according to their roles as appropriate?

- QS1: Discuss the general workflow of the services in the system and validate the general scenario with the stakeholders including data flow, student record details and system structure.
- QS2: Discuss the workflow of each of the selected services and the information (input and output) from each process?
  - What information about the user that is essential to the provision of the each of those services?
  - Does the current system have any data classification scheme for the student data (e.g. sensitive data)? If yes, what are they?
  - How does the system deal with sensitive data? Is it encrypted?
- QS3: Who are the actors/roles who process each service?
  - What are their privileges/access rights (view, change, delete, etc.) to the student information?
  - How are the actors authenticated to the system?
  - Is there any delegations? How it is performed?
- QS4: If the user was allowed to have control over his/her information? What information you believe that cannot be under full control? Why?
- QS5: What are the current security policies/laws/ guidelines followed?
- QS6: What type of privacy awareness procedures followed?

The following are the expectations and needs identified from the interviews with regard to the selected services and the system in general grouped according to stakeholders' categories.

- **Q1: What are the most services used in EduPortal Services?**
- AQ1: Enquiry Requests, Update Personal Information, Update Contact Information, Financial Requests
- **Q2: Do you have any privacy concerns with the current systems when you use/process any of the provided services? If yes what are they?**
- AQ2: Current system does not preserve the privacy of the user as every employee can see the whole file of the student **[SPID1], [SPID2], [UserID1], [UserID3], and [UserID10].**
- Sensitive data are not currently encrypted in the system but can be protected with access rights **[DevID1], [DevID2].**
- The system is not fully privacy friendly; however, employees are aware about the consequence of revealing information about the students. **[SPID3],[GR]**
- No deep concerns but I would prefer that only one employee process the request and see related information **[UserID2], [UserID4], [UserID8], and [UserID9].**
- Only concern is my sensitive data, I wish not every employee see it, only when they need it **[UserID5], [UserID6], [UserID7].**

- **Q3: Do you find the definitions clear? If not which one is not clear?**
    - AQ3: The provided definitions were clear to all interviewees; however, the difference between sensitive and private data classifications was explained more by examples to two of interviewees from User category.
- **Q4: Do you agree with the definitions? [each group of definitions was discussed separately and then the data mapping was explained]**
    - AQ4: All interviewees greed on the provided definitions, except that [**SPID1], [SPID2], [SPID3], [GR], [DevID1]** had reservation on part of the definition of Totally Owned ownership right were the delete access right was considered dangerous and an appropriate for the system to run probably. An option of hide the information was suggested and considered.

- **Q5: What possible risk you might encounter if information about you/about the user were compromised?**
    - AQ5: Possible risks identified by the stakeholders are:
    - **Users:**
        - Having annoying questions from the employee about social life (as a result of viewing personal information) that has nothing to do with the requested service.
        - Viewing information about the user that are not required by the requested service might affect the decisions taken on some requests which usually shouldn't be affected if the (unrelated information were not known).
        - Knowing some information might affect the decision on other requests.
        - Blackmailing, annoying calls, possible harassments can occur from irresponsible employee or others who somehow had access to personal and sensitive information.
        - Other people like student's relatives can be affected badly if their information was disclosed.
    - **Other stakeholders(Service provider, Government representative, Developer):**
        - Lose of reputation and users trust
        - Lose of money and complications especially when student bank account details are disclosed or changed.
        - Possible legal actions.
        - If case of an unauthorised access to employee account, huge risk on information about the users and requested processed by that employee.

Users Questions:

Note: F=Female, M =Male

- **QU1: Which information that you worry most about your privacy when processed and to what level?**

Answers to this question varied and the following are some of quotes from the interviews:

- "When I use the Enquiry service it is so general and I would prefer to contact someone specific or I would like to know who is exactly dealing with my request and who see all the information" **UserID1[F]**.
- I need to know what the workflow is and who is currently is processing the request. (e.g. as in the system of my university back home) **UserID1 [F]**.

- "I do not want everyone to know the problem and sometimes I need to provide sensitive information or details with regard to that enquiry and I would prefer only one person to deal with it" **UserID3[F]**.
- "I don't want to repeat myself and the story of my request each time I follow up with the enquiry **". UserID2 [M]**.
- "I don't know who see my file and what level of details each employee can see and it annoys me" **UserID5 [F]**.
- "Again, I would prefer one person to deal with it" **UserID5 [F]**.
- "Current system is complicated in the services related to information about updating the student's relatives" **UserID4 [M]**.
- "There is sometimes conflict in the Enquiry request, so when I send a request to finance, it turns out that I should sent it to education and I have to repeat the process all over again" **UserID9[M]**.
- "I need to know who sees uploaded files" **UserID6 [F]**.
- "It will be helpful to know who is processing the information currently". **UserID6 [F]**.
- "No automatic delegation without my permission. And no one should be able to see my information unless I allow it". **UserID1[F]**
- "I would prefer to have control over very sensitive data about me. However, I don't know what will be needed to provide the service to me" **UserID1 [F]**.
- "I am afraid that having a full control over my information might stop me from having a service at the time I need it" **UserID3 [F]**.
- "Do I bother to have control that might stop me from having the service, no" **UserID10 [M]**.
- "I would prefer to have a partial control and giving them the right to override it when necessary", **UserID7 [F]**.
- "I would prefer having the service smoothly rather than having the control but an over headache" **UserID2 [M]**.
- "I would prefer a onetime settings and how it can be done? I don't want to do it every time" **UserID8 [F]**.
- "I would prefer to know who sees my sensitive information and why?" **UserID1 [F]**.
- "I would prefer that only the needed information can be seen by the employee who is processing the service" **UserID6 [MF]**.
- "Anything related to deadline is critical for me that it is not delayed because of privacy settings" **UserID6 [F].**
- "I would prefer them to contact me by different means when it is a critical notification or when they need to override my privacy settings" **UserID1[F]**
- Allow only information needed for a service and only for the person who is processing the service **UserID3[F]**, **UserID3[F]**., **UserID5[F]**., **UserID6[F]**, **UserID7[F]**., **UserID8[F]**..
- Updating Contact details, it is requested many times and accessed by everyone **UserID1[F]**, **UserID2[M]**, **UserID3[F]**., **UserID5[F]**., **UserID6[F]**, **UserID7[F]**., **UserID8[F]**, **UserID9[M]**.
- For Financial services I would rather them to be quick and not to be delayed because of privacy settings that I did**,UserID2[M]**, **UserID3[F]**, **UserID4[F]**, **UserID5[F]**., **UserID6[F]**, **UserID7[F]**., **UserID8[F]**, **UserID9[M], UserID10[M]**.
- I would like to see the workflow and to see the details of the request and track it to know when I need to do a follow up and to know the time limit before any follow up **UserID1[F]**, **UserID2[M], UserID3[F]**, **UserID5[F]**., **UserID6[F]**, **UserID7[F]**., **UserID8[F]**.
- Changing the names of previous loaded files into meaningless names prevents us from understanding if the file is uploaded or not **UserID1[F]**, **UserID2[M]**, **UserID3[F]**
- Adding some files many times although it has been added before but you cannot access the previous ones (all interviewees from Users)
- The current system has a problem in asking the student for doing a new request all over again if the student asked for a service but using the wrong command or request and this is time consuming, I believe they can solve it internally by sending the request to the right people and change it to the correct request instead of the student doing it all over again! (All interviewees from Users).

- **QU2: How will you classify information about you used by the system using the following data classification (Restricted, Sensitive, Private and Public**)?[The definitions of the data classifications where explained by examples to the interviewees]
    - Answers varied between interviewees (Users) in classifying personal data in term of how sensitive it can be, however, there was an agreement on sensitivity of some of the personal data.

- Data Sensitivity (4 levels) (Restricted, Sensitive, Private, Public)
  - Personal details (Name, place of birth)[Public(all users)]
  - Personal details (National ID number) [answers varied between sensitive(2 Users)- private(4 users) and public(4 users)]
  - Personal details (material status) [answers varied between Restricted (4 users),sensitive(2 users), private(2 users) and public(2 users)]
  - Personal details (Birth date)[[answers varied between private(5 users) and public(5 users)]
  - Contact details (Mobile numbers) [answers varied between Restricted (4 users),sensitive(2 users), private(2 users) and public(2 users)]
  - Contact details (emails) [answers varied between private(4 users) and public(6 users)]
  - Contact details (Addresses) [answers varied between Restricted (1 user),sensitive(2 users), private(2 users) and public(5 users)]
  - Relatives names [answers varied between sensitive(4 users), private(2 users) and public(4 users)]
  - Relatives Contacts (mobile numbers) [answers varied between Restricted (2 users),sensitive(2 users), private (2 users) and public(4 users)]
  - Relatives Contacts (Addresses) [answers varied between Restricted (1 user),sensitive(2 users), private(2 users) and public(5 users)]
  - Bank details [answers varied between sensitive(2 users), private(3 users) and public(5 users)]
  - Qualifications details[Public]
  - Education study details [public]
  - Passport details (Pictures) [answers varied between Restricted (4 users),sensitive(2 users),and public(4 users)]
  - Sensitive Official files (e.g. marriage or divorce certificates, A copy of the passport, or any other personal identifiable documents) Only when the service is totally depends on these services)[all users]
  - Other official files (decisions on sponsorship, government letters, etc.) [varied between sensitive (2 users), private (2 users) and public(6 users)]

- **QU3: If you are allowed to have full control on the information about you, what information you believe that you should be the only one who has control on it?**
  - Information I should own and control:
    - Personal information
    - Contact Information
    - Social status and relevant documents.
    - Relatives' information
    - Relatives Contact details
    - Qualification
    - Current study information
    - Any sensitive information that I decide it is sensitive and I want to be the only one to change any information about me by myself.

Other Stakeholders' Questions:

- **QS1: Discuss the general workflow of the services in the system and validate the general scenario with the stakeholders including data flow, student record details and system structure?**
  - The discussions resulted in understanding the current system and validating the general workflow presented in chapter 9, Figure IX.9.

- **QS2: Discuss the workflow of each of the selected services and the information (input and output) from each process?**
  - **What information about the user that is essential to the provision of the each of those services?**
    - The employee needs to see all information related to the request to be able to process the request or take the decision about it. [**SPID1], [SPID2], [SPID3], [GR].**
    - The employee can see (Ethical information) such as alerts about the student to inform his decision. Example, is the student suspended from scholarship? Is he currently in Country B or in the country of study, has the student been refused previous similar or relevant requests? Is there any other request under process which might be related (and or conflicting)? [**SPID1], [SPID2], [SPID3], [GR].**

- **Does the current system have any data classification scheme for the student data (e.g. sensitive data)? If yes, what are they?**
  - No, there is no classification for the data, however, personal information are considered sensitive [**SPID1], [SPID2], [SPID3], [GR].**
- **How the system deals with sensitive data? Is it encrypted?**
  - No, there is not any level of encryption, but the data are protected by limiting access rights to only official employees **[GR], [DevID1].**

- **QS3: Who are the actors/roles who process each service?**
  - **What are their privileges/access rights (view, change, delete, etc.) to the student information?**
    - -Employees from different departments, head of departments, attaché deputy, attaché office and Information Services department.
    - The head of the department have more privileges to see the history of previous requests made by the student and all relevant information to help him have more informed decision but only for students under his department, while attaché deputy, attaché office and Information Services department have full access to all information about students and requests, but changes are made only through requests performed by the system and initiated by the student in person or through EduPortal **[SPID3] , [GR]**

  - **How the actors are authenticated to the system?**
    - User name and passwords...
  - **Is there any delegations? How it is performed?**
    - Delegation are performed between employees to another employee with a higher position and more privileges in case there is sensitive case or request and by passing the request to the higher position to take action, however delegation between employees on the same level can be done by the agreement of a higher level on that and by giving the privileges based on a the employee role to the other employee **[SPID3], [GR].**
- **QS4: If the user was allowed to have control over his/her information? What information you believe that a user cannot have full control on? Why?**
  - User name and passwords, National ID number **[DevID1], [GR].**
  - The student shouldn't be able to tamper or change information that relates to his sponsorship or study directly but he can made any required changes through a request for updating that information while providing evidence that support the accuracy of the new changes **[SPID1], [SPID2], [SPID3], [GR].**
  - Contact details need to be always up to date, and many services need this information, so the student cannot delete this information **[SPID3], [GR].**

- **QS5: What are the current security policies/laws/ guidelines followed?**
  - All information security policies and laws from the government are considered. The employees are aware of the consequences of revealing student information or misusing it **[SPID2], [SPID3], [GR].**
  - All the actions performed on the student files are logged and it shows who performed the action and at what time and using what machine. But not in the case of viewing the file without an action **[DevID1].**

- **QS6: What type of privacy awareness procedures followed?**
  - Users are sent from time to time emails to raise their awareness about looking after their personal information and not sharing their usernames and password with others **[DevID1], [GR].**
  - Employees are given from time to time awareness emails about how to look after their own user names and passwords and about applied security policies **[DevID1], [GR]**.

b) Stakeholders Requirements and Conflict Resolution Forms

1. Selected Service: Update Electronic File: Update Personal Information/Update Contact information

Service Description:

Update Electronic File: This service is available for all students and it involves updating personal information, passport information, visa information, contact information, and qualifications.

- Update Personal Information: This service involves updating any of the following information: Name (any part of it), marital status (single, married, divorced, widowed), National ID card issue date, expiry date, Date of Birth, passport information (number, issue and expiry dates, Place of issue),Visa information (number, issue and expiry dates, Place of issue, type of visa).
- Update Contact information: This service involves updating any of the following: Address, Mobile and telephone numbers, email, relatives' names, relatives contact details, emergency contact details.

Stakeholders: User (student), Employee, Head of departments (Financial, etc.), Attaché Office representatives, HE ministry representatives.

Stakeholders' Privacy Expectations and needs: Privacy Requirements (PR), Functional Requirements (FR), Security Requirements (SR)

No.	Privacy Requirements	Stakeholder	Possible Conflict	Proposed Resolution	Comment
PR1	User need to know who sees his/her data and why(for what service)	User	SR7	A unique employee reference can be provided to the user	Resolved
PR2	Any employee should see only the information needed to process the requested service.	User	FR2	Only needed information for the service should be viewed by an employee	Resolved
PR3	Personal and contact information should be controlled and owned by the user only	User	SR4,FR5	Ownership rights were agreed between stakeholders but with the delete access right.	Partially resolved
PR4	Social status and relevant documents should not be viewed by any one unless a requested service depends totally on viewing these files.	User	FR5	Only needed information for the service should be viewed by an employee	Resolved
PR5	Changes of Personal and Contact information should be only by the user and should be performed securely.	User	FR3	It is performed only by the user, more security measures are suggested	Resolved
PR6 SR1	National Identity number should not be public , a lot can be revealed by knowing only the national ID of a person	User	FR6	An alternative user name and password can be used.	-Not resolved
PR8	Official files should be viewed only when the provided service depends on them	User	-	-	-Agreed

No.	Privacy Requirements	Stakeholder	Possible Conflict	Proposed Resolution	Comment
SR2	Official sensitive documents like personal photos, , identity files, social status related documents ,etc. should be encrypted	User	-	-	-Agreed
PR10	Having control over user information should not prevent the user form having the service.	User	FR5	User's consent should be requested when sensitive information is needed to provide a service.	Resolved
PR11	Having control over information can be optional.	User, SP	-	-	Agreed
PR12 SR3	User should be contacted by many means in case of a critical notification or a need to override privacy settings on user information	User, SP	PR14	In emergency any privacy settings are overridden by senior employees	Resolved
PR13	Relatives information should be considered personal	User	FR4	In emergencies, any privacy settings can be overridden	Resolved
SR4	Personal information is highly sensitive and a higher level of confidence should be achieved in the identity of the user before allowing the changes.	Developer, SP	PR3	No conflict as more security measures will serve preserving the user's privacy when changing personal information	Resolved
SR5	Highly sensitive information should be encrypted and limited access rights should be granted to that information.	Developer, User	-	-	-Agreed
SR6	Actions that involve changes in the information should be logged for auditing. (Date, time, by whom IP address.)	Developer SP, User	-	-	-Agreed
PR14	Contact details are sensitive and they should not appear to the employee unless necessary	User	FR3, PR12 ,SR3	Email can be used to send notifications without being viewed	Partially resolved.
FR1	Supporting file(s) should be provided by students to ensure accuracy of the changes	SP/GR	-	-	-Agreed
FR2	The employee should view supporting files to verify the changes and approve the request	SP/GR	-	-	-Agreed
FR3	A user's Email is used to notify the user about rejection or acceptance of the request.	SP/GR	PR13	Email can be used to send notifications without being viewed	Resolved
FR4	Relatives information and contact details are needed in case of emergency	SP/GR	PR13	In emergencies, any privacy settings can be overridden	Resolved

No.	Privacy Requirements	Stakeholder	Possible Conflict	Proposed Resolution	Comment
SR7	The student should not know the identity of the employee processing his file.	SP/GR	PR1	A unique employee reference can be provided to the user	Resolved
FR5	Most of Personal information are essential and need to be viewed by the employee when providing other services,	SP	PR10	Only needed information for the service should be viewed by an employee	Resolved
FR6	National ID number is essential for many services and used to authenticate the user and should be viewed by all employees	SP/GR	PR6 SR1	An alternative user name and password can be used.	-not resolved

Appendix_Table G.1: Stakeholders' Privacy Expectations - Update Electronic File

Recommendation:

1. At least one time password should be provided along with the Login user ID and password. 2. The user ID should not be personal identifiable information about the user. 3. Only needed information should be viewed by an employee. Contact information should be considered sensitive.

2. **Selected Service: Enquiry Request**

Service Description: This service covers wide range of enquiries and is one of most used services in EduPortal systems. Enquires range covered are: enquiry for the attaché, legal enquiry, educational enquiry, financial enquiry_ Salaries and rewards, Financial enquiries -Refunds, Financial enquiries-Courses' fees, medical insurance enquiries and general enquiries. According to the type of the enquiry the request is processed by the relevant department and the general enquiries are processed by the supervision department responsible about the student.

Stakeholders: User (student), Service provider (Employee, Supervisors, Head of departments (Financial, Legal, Educational, etc.)), Government representative (Attaché Office representative, HE Ministry representative and Information Systems Management department representative).

Stakeholders' Privacy Expectations and needs (Privacy Requirements)

No.	Privacy Requirements	Stakeholder	Possible Conflict	Proposed Resolution	Comment
PR1	Users prefer that least people deal with the enquiry request and preferably one specific person	User	-	-	Agreed
PR2	In cases where the enquiry have sensitive information, the user need to know who is dealing with his/her enquiry request and who is viewing that information	User	SR2	Provide detailed workflow with employee reference (and contact in case of private enquiries only)	Resolved
FR1	There is a need to view the workflow of the request and the stages of processing and who is dealing with it.	Developer	SR2	Provide detailed workflow with employee Reference	Resolved
PR3	If an enquiry was rejected because it was incorrect type ,any relevant information provided with that enquiry should be deleted	User	FR5	If the enquiry is not processed, the student can delete it with relevant files, but if it was processed, it cannot be deleted and it will appear in the history of requests	-Not resolved
PR4	The employee need to see only relevant information needed to process the request	User	FR3	Only needed information relevant to the request should be viewed by the system	Resolved
FR2	In case the user chooses an incorrect enquiry request, the request should be redirected automatically to the right department and changed to the right type!	User	PR1, PR4	The types of requests will be reviewed and changed	Resolved
FR3	The employee need to see all information related to the request to be able to assess the request and take appropriate decision	SP,GR	PR4	Only needed information relevant to the request should be viewed by the system	Resolved
FR4	Alerts about the students are necessary to be viewed by the employee who is processing the request to inform his decision.	SP,GR	-	-	Agreed
FR5	Head of the department have more privileges to see previous requests made by the student, to assess any new requests	Service provider	PR3	Only If the enquiry is not processed, the student can delete it.	-Partially resolved

No.	Privacy Requirements	Stakeholder	Possible Conflict	Proposed Resolution	Comment
R12	Actions that involve viewing highly sensitive information should be logged for auditing.(Date, time, by whom)	User, Developer, SP	-	-	Agreed
PR5	Response to private enquiries should be encrypted or protected by access right so that only the student can see it	User, Developer	-	-	Agreed
PR6	Some enquiries (e.g. medical, general) might have sensitive data that need to be protected and accessed only by the responsible person for processing that enquiry	User, SP	-	-	Agreed
SR1	Highly sensitive information should be encrypted and limited access right should be granted to that information.	Developer	-	-	Agreed
PR7	In case of private enquiry , a user need to know if the enquiry was delegated, to another employee and who is that employee	User	SR2	The employee reference will be provided	Agreed
SR2	The student should not know the identity of the employee processing his file.	SP,GR	PR2, FR1	Provide detailed workflow with employee reference (and contact in case of private enquiries only)	Resolved

Appendix_Table G.2: Stakeholders' Privacy Expectations - Enquiry Request

Recommendation: 1. a new type of enquiry should be added and labelled as private enquiry where any information or documents provided in that enquiry are dealt with by limited people and as needed to response to the enquiry. 2. General enquiries (not private) can cover all types of enquiries and safe the time of users confusing of which enquiry to ask for.

3. Selected Service: Scholarship Extension Request

Service Description: This is used by some students who might need an extension for their scholarship for any reason and is processed across different departments within the government office and the organisation sponsoring the student through EduPortal system. The service involves processing the data and files provided by the students by many employees with different roles inside the government office or at the sponsor organisation.

Stakeholders: User (student), Service provider (Employee, Supervisors, Head of departments), Government representative (Attaché Office representative, HE Ministry), Student sponsors, Information Systems Management department representative, and student sponsor representative.

Stakeholders' Privacy Expectations and needs (Privacy Requirements)

No.	Privacy Requirements	Stakeholder	Possible Conflict	Proposed Resolution	Comment
PR1	User need to know who see the information and files provided and what level of details they can view	User	FR1	Only needed information should be viewed by the employee	Resolved
FR1	The employee need to see all information related to the request to be able to process the request and take the decision about it	SP	PR1	Only needed information should be viewed by the employee	Resolved
FR2	The details of the workflow of the extension request at the sponsor organisation should be viewed by users through EduPortal system	User, SP	-	-	Agreed
FR3	If the user privacy settings might delay the respond for the request, the user should be warned about that and asked to change the settings or give more access rights to specific roles.	User, SP	-	-	Agreed
PR2, SR1	Some extension requests are for private reasons which might have sensitive data and supporting evidence files that need to be protected	User, Developer	-	-	Agreed
PR3	Sensitive data and files in an extension request should be accessed only by the employees who need to view these files	User	FR1	Only needed information should be viewed by the employee	Resolved
FR4	Alerts about the students are necessary to be viewed by the employee who is processing the request to inform his decision.	SP,GR	-	-	Agreed
PR4 SR2	Actions that involve viewing highly sensitive information should be logged for auditing.(Date, time, by whom)	User, SP, Developer	-	-	Agreed
FR5	The details of notes and discussions made on the extension request should not be viewed by the student	SP,GR	FR6,PR5	Student can view the workflow and the notes and alerts that concern his/her request	Resolved
FR6, PR5	The student needs to know the details and notes made on the request and track it to know when to do a follow up ,or if there is something missing	User, SP	FR5	Student can view the workflow and the notes and alerts that concern his/her request and the expected time of processing	Resolved

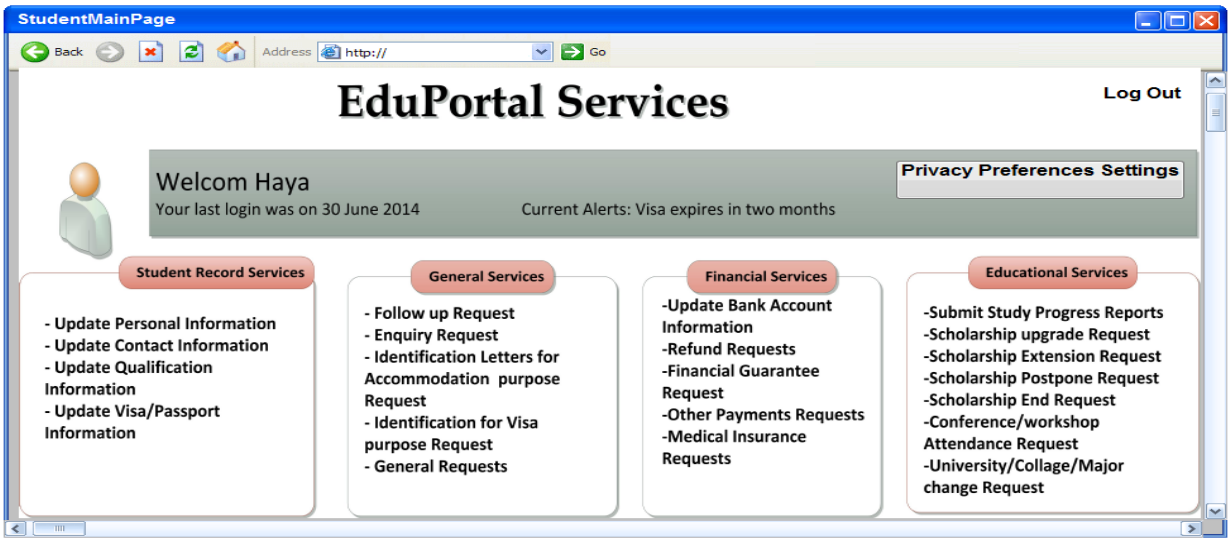
Appendix_Table G.3: Scholarship Extension Request

Recommendation: 1. Sensitive data included in the request should be viewed only by persons who are responsible in taking decision about the request. 2. Student should be able to view the workflow and the notes and alerts that concern his/her request.

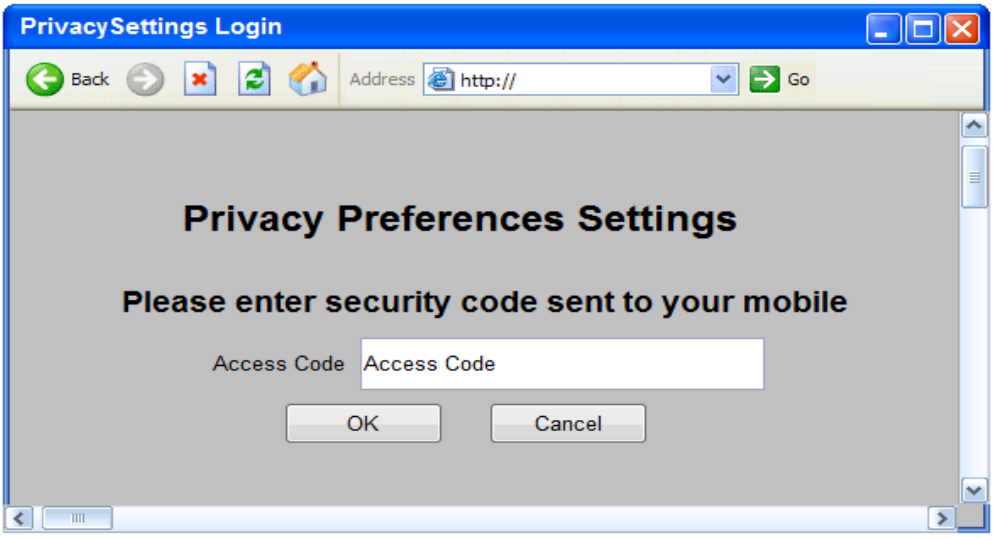
c) EduPortal Prototype Screens

1. Changing Privacy settings

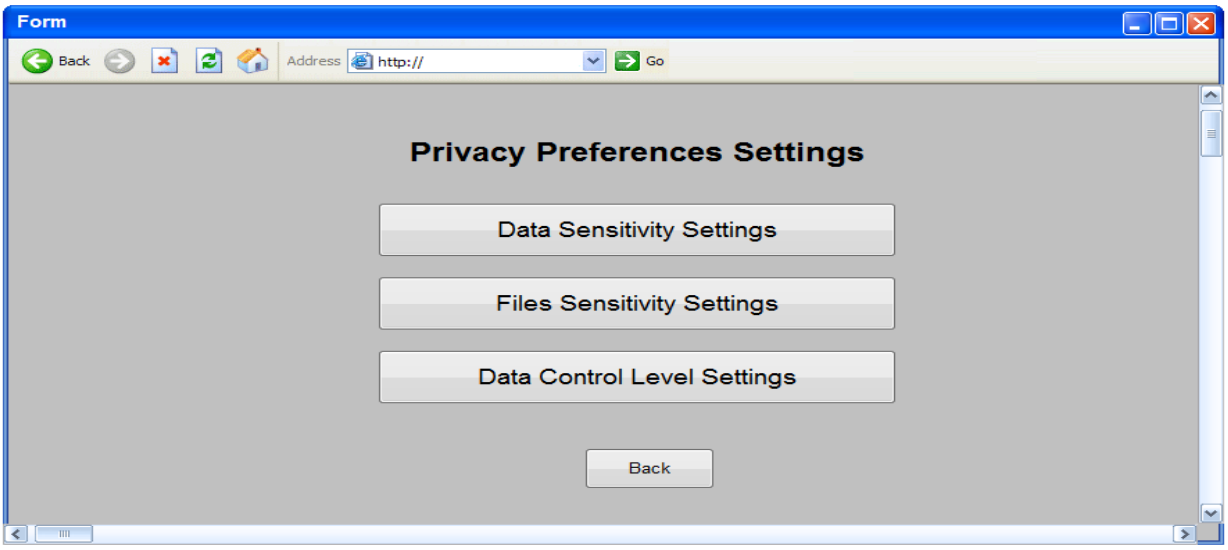
The user will log in to the system using user name and password then select privacy settings from the main screen Appendix_Figure G.1, another authentication screen will appear asking for a onetime password that is sent to the student registered mobile number Appendix_Figure G.2 and when the students enter the correct password, The privacy settings main screen will appear Appendix_Figure G.3.



Appendix_Figure G.1: Changing Privacy Settings

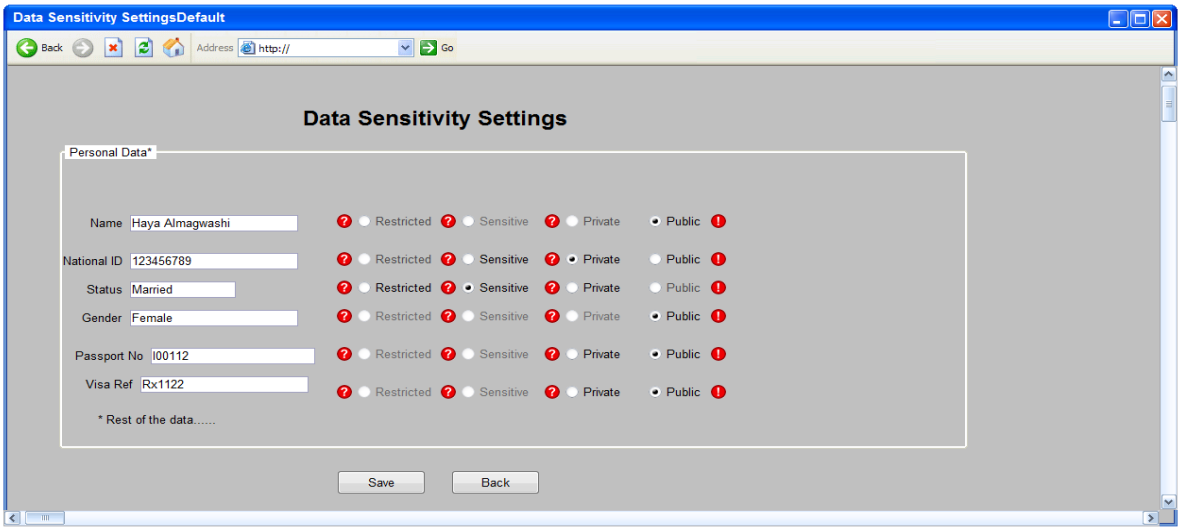


Appendix_Figure G.2: Privacy Settings Login

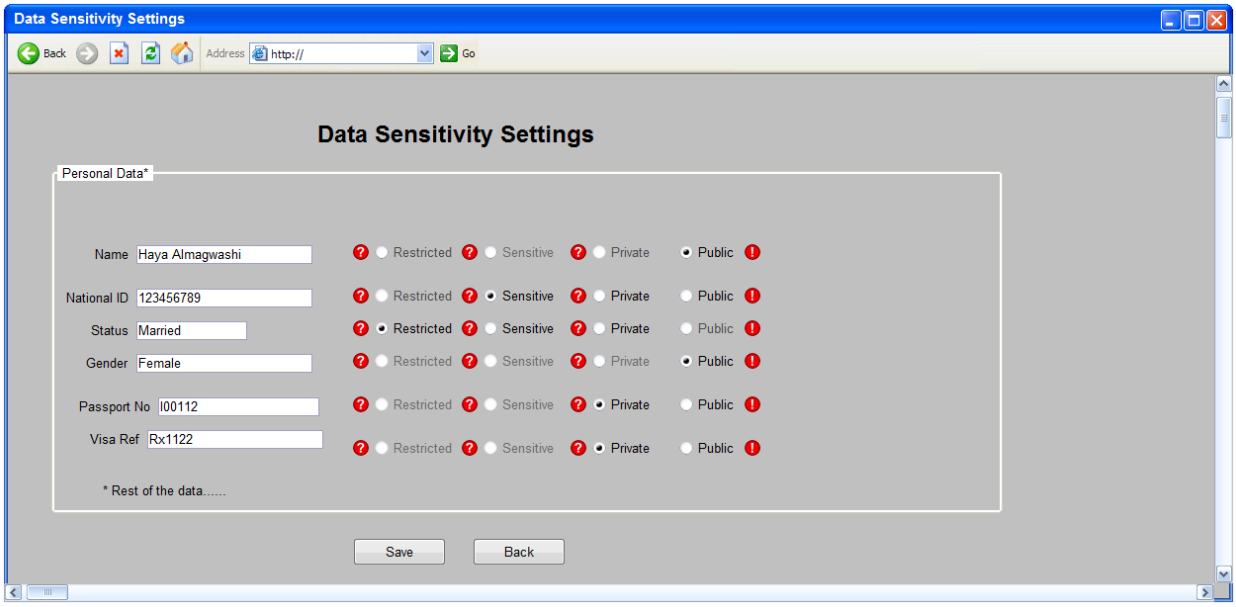


Appendix_Figure G.3: Privacy Settings Main Screen

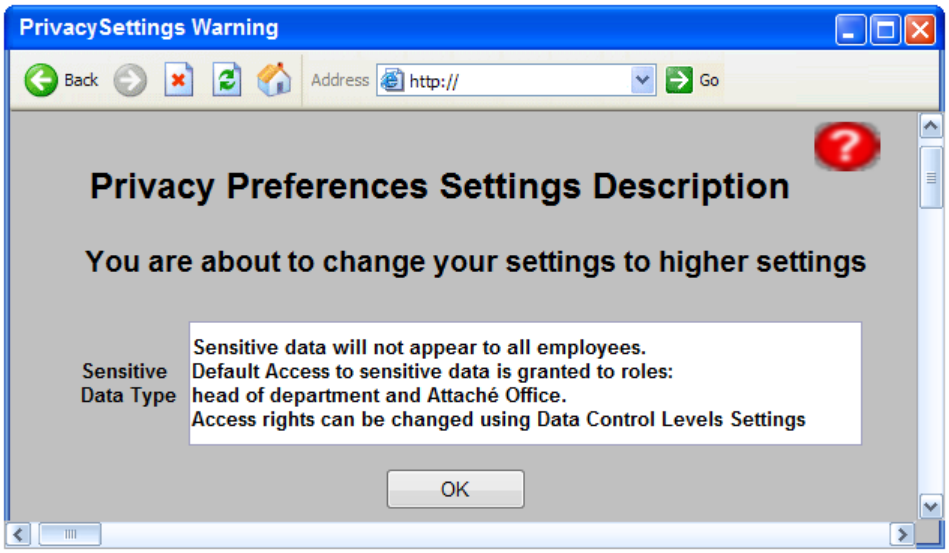
If a student selects Data Sensitivity Settings, the screen for changing the data types of information about the student will appear with the default settings applied by EduPortal system Appendix_Figure G.4 the student can change these settings according to the ownership rights and levels of controls assigned to each piece of information (which a student can view but cannot change). If a data type is not available to for the piece of information, it will appear disabled (grey) as in Appendix_Figure G.5. When any of the red marks is pressed they provide brief explanations to each of the data types and the effect of changing to that data type. In addition, when the student chooses to change to a higher or lower classification of the data type, an alert message will appear Appendix_Figure G.6



Appendix_Figure G.4: Default Data Sensitivity Settings



Appendix_Figure G.5: Data Sensitivity Settings Changed by the user



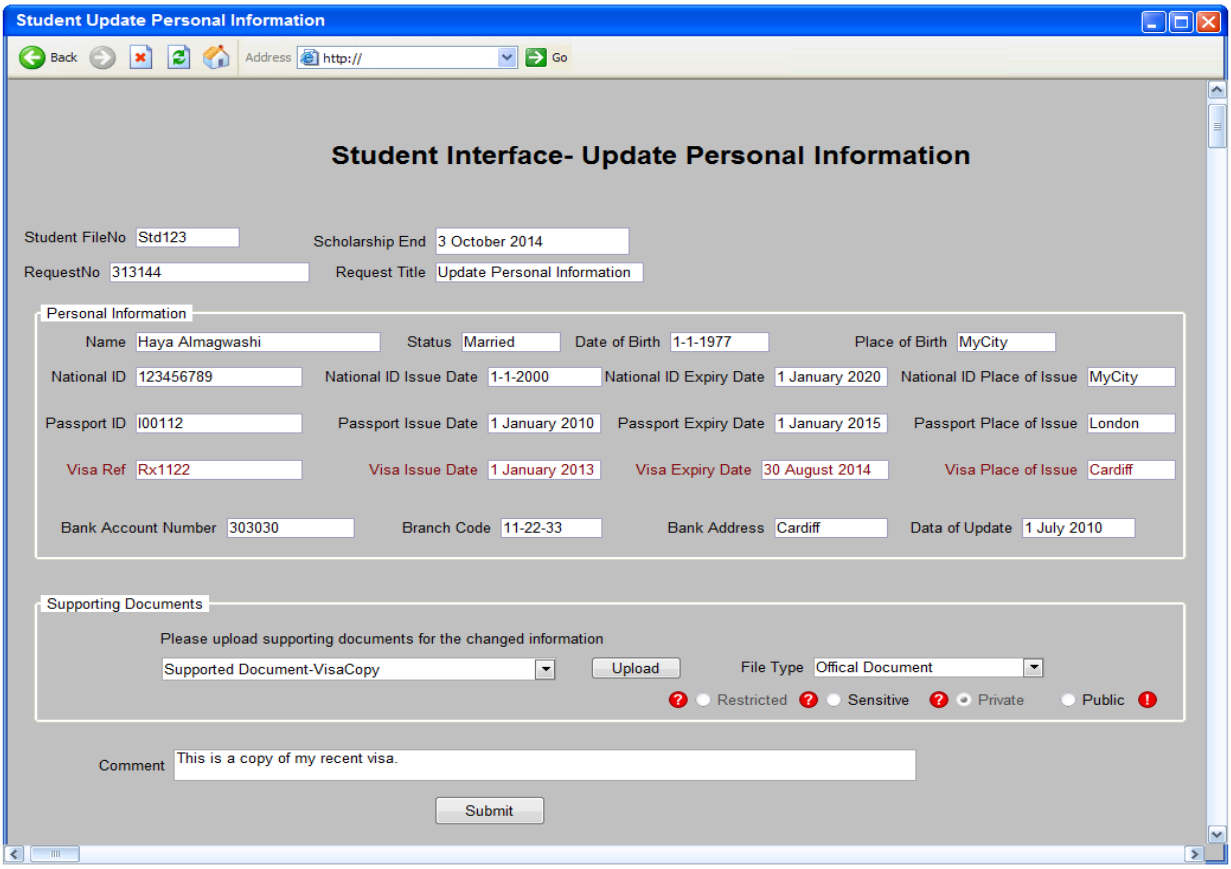
Appendix_Figure G.6: Privacy warning message

When the student saves the settings the privacy setting security screen Figure A9C.2 will appear again.

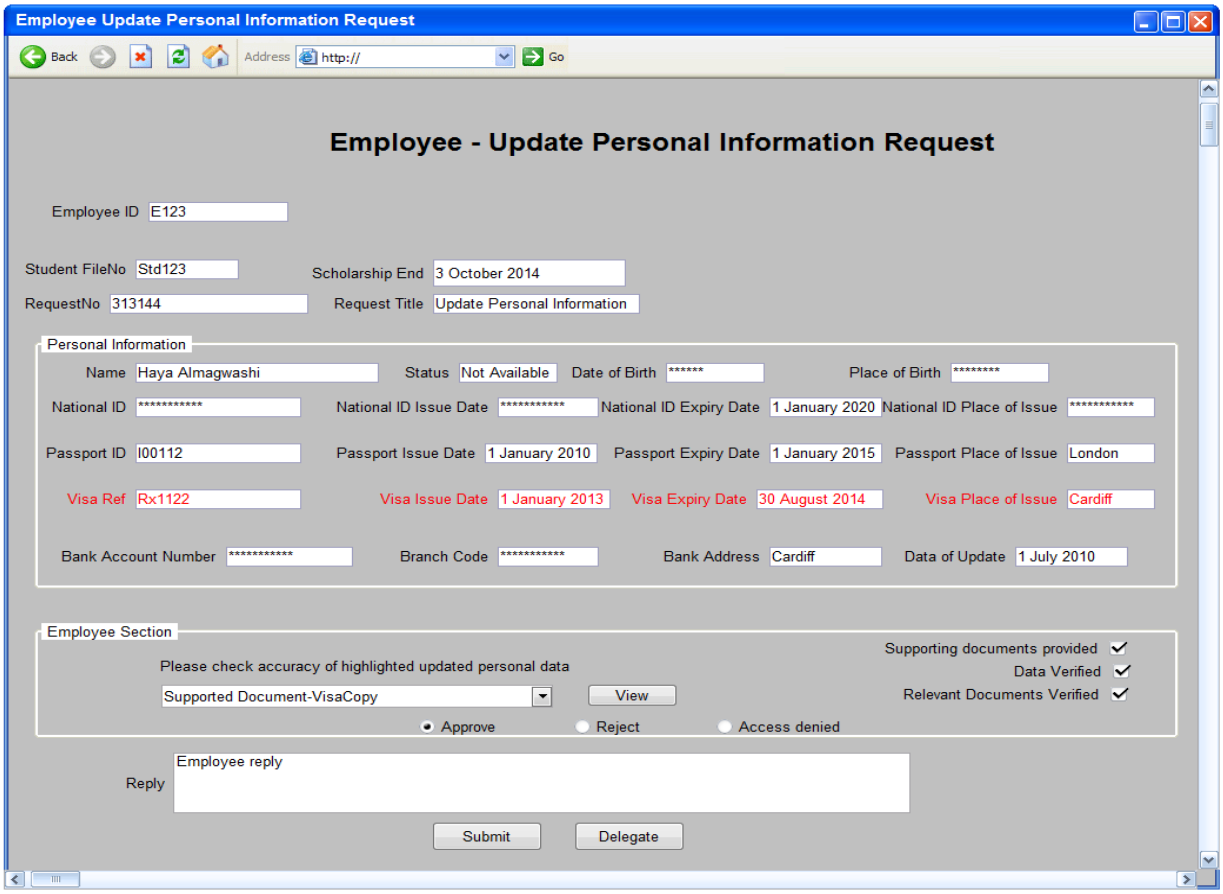
2. Update Personal Information

In this service a similar screen to Appendix_Figure G.7 will appear, the student will update personal information and should provide supporting documents for verifying the changes. When the student upload the supporting document, he/she should select a type for the documents from the list, (Personal, Official, etc.) then should select specify the sensitivity of the document using the provided options. In the employee interface shown in Appendix_Figure G.8, the changed data will appear in red and the employee will verify the changes according to the provided supporting documents. If the documents

classification doesn't allow the employee to view the document, he will response by choosing Access denied and delegating the request to the head of the supervision department after writing comments.



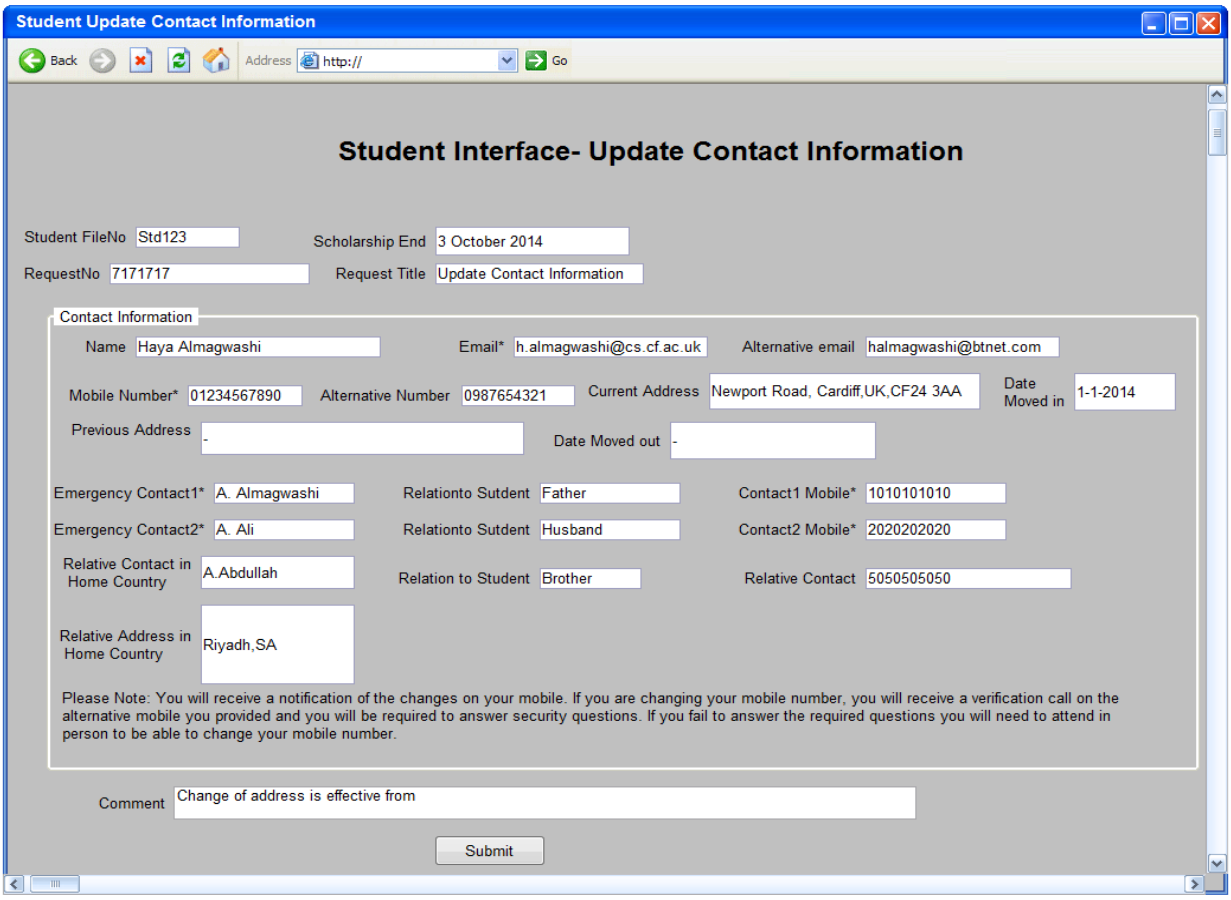
Appendix_Figure G.7: Update Personal Information –Student Screen



Appendix_Figure G.8: Update Personal Information –Employee Screen

3. Update Contact Information

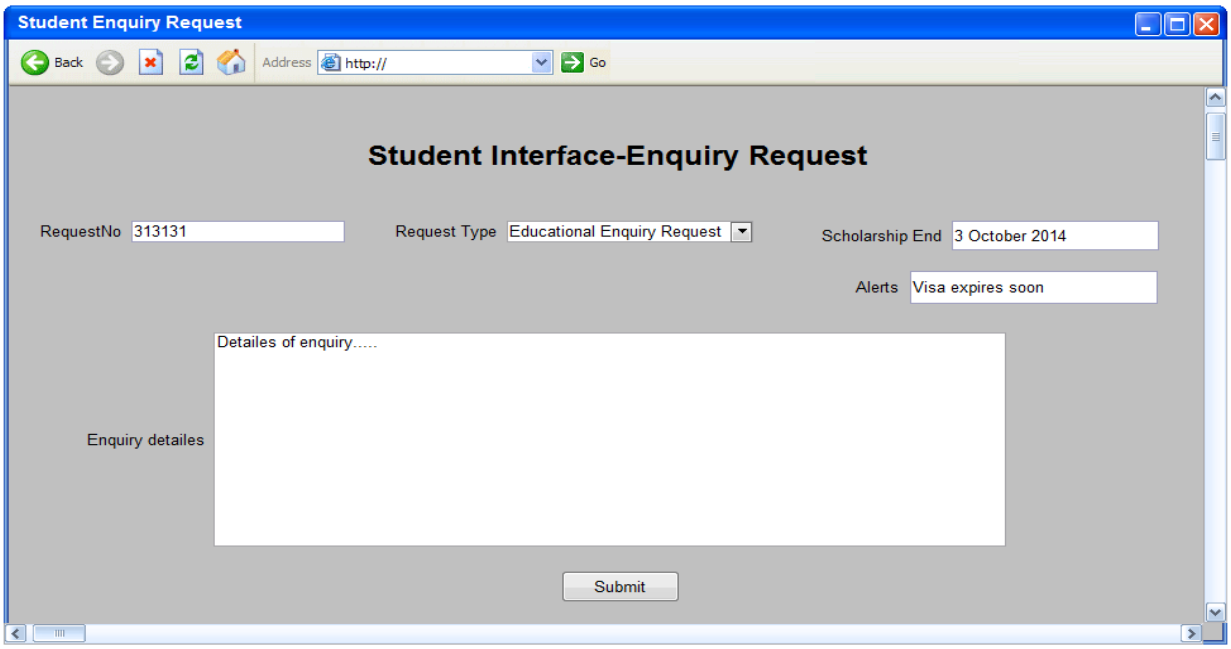
When the student wants to update his/her contact information, no verification is required, however, when the update involves changing the mobile number, the information will be verified over a phone call as described in the message in Appendix_Figure G.9



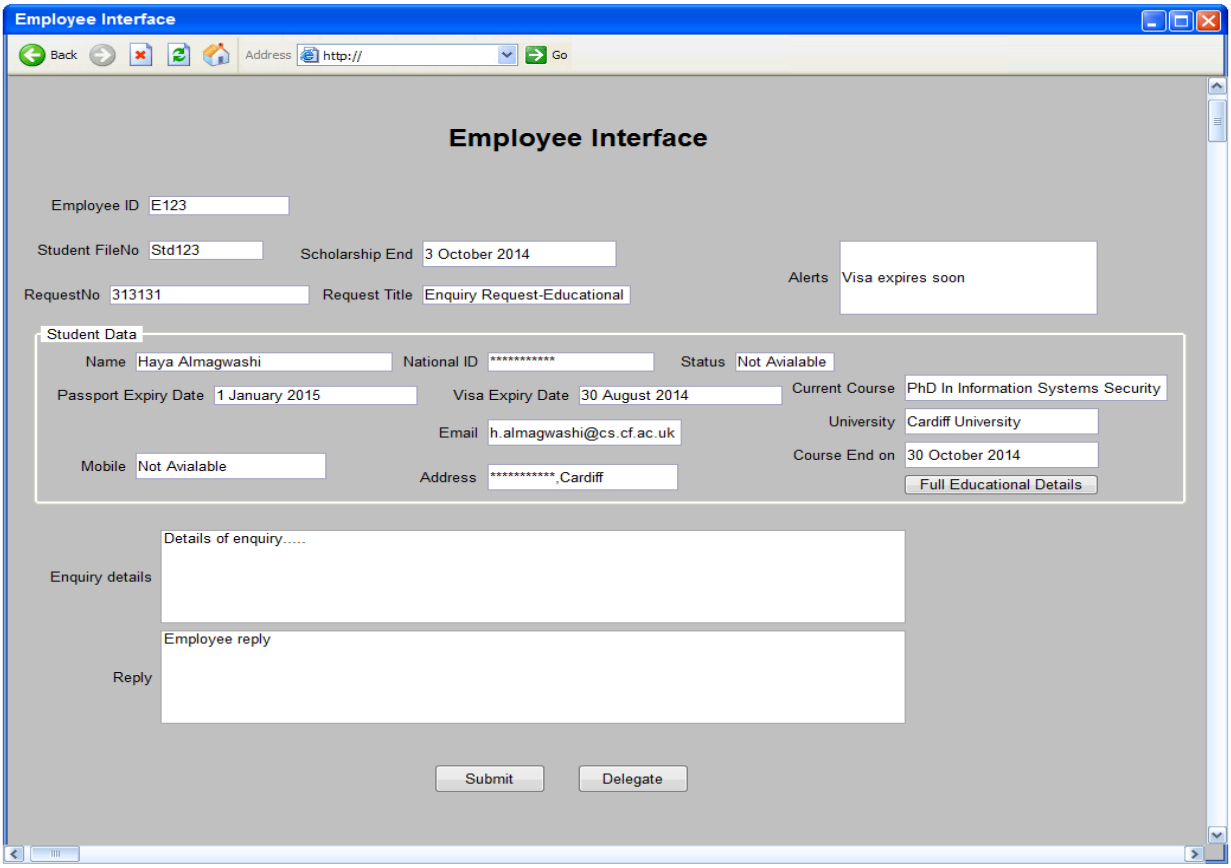
Appendix_Figure G.9: Update Contact Details Screen

4. Enquiry Request

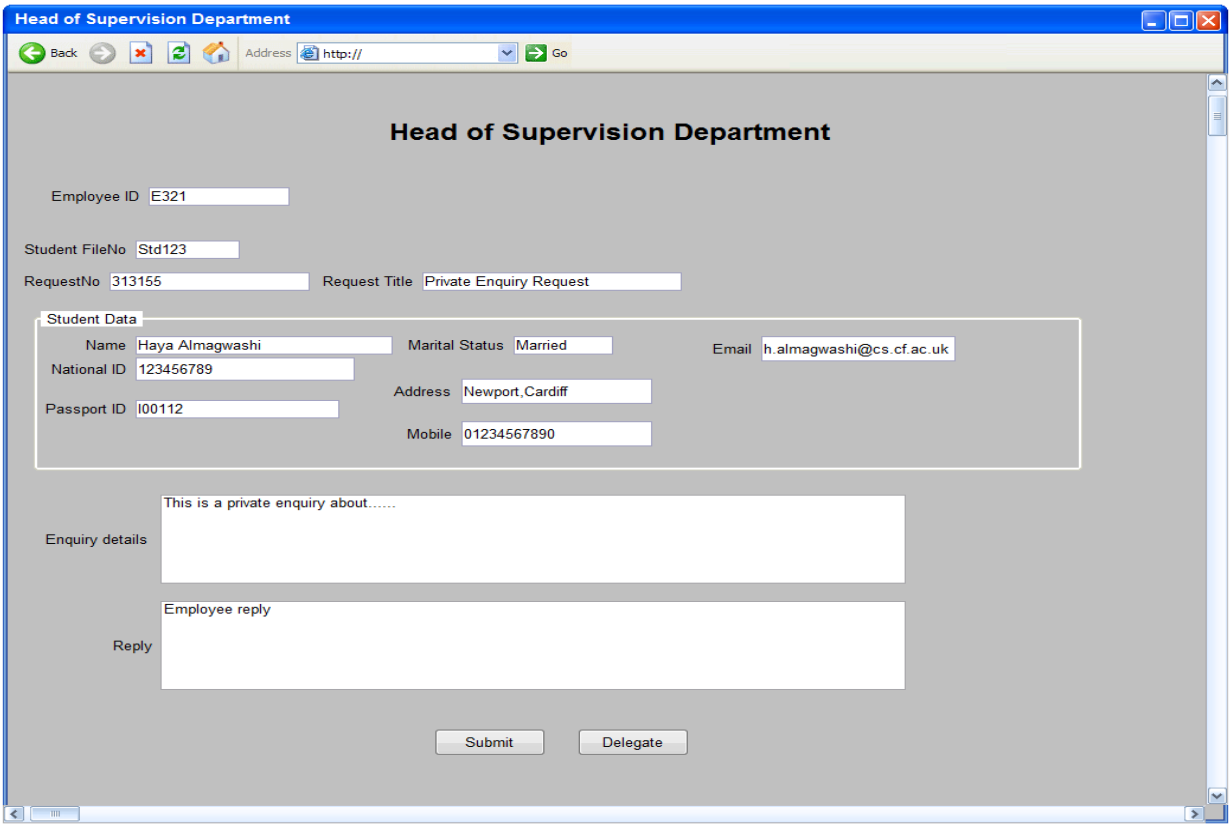
In this service, the student will select a type of an enquiry as in Appendix_Figure G.10, only relevant information to the enquiry type will be available to the employee as in Appendix_Figure G.11. A new type of Enquiry Request service (Private Enquiry) which is viewed only by the head of supervision department was suggested as in Appendix_Figure G.12. In this type, the student mobile number will be available to the Head of department in case there was a need for further direct discussion with the student with regard to the enquiry.



Appendix_Figure G.10: Enquiry Request-Student Screen



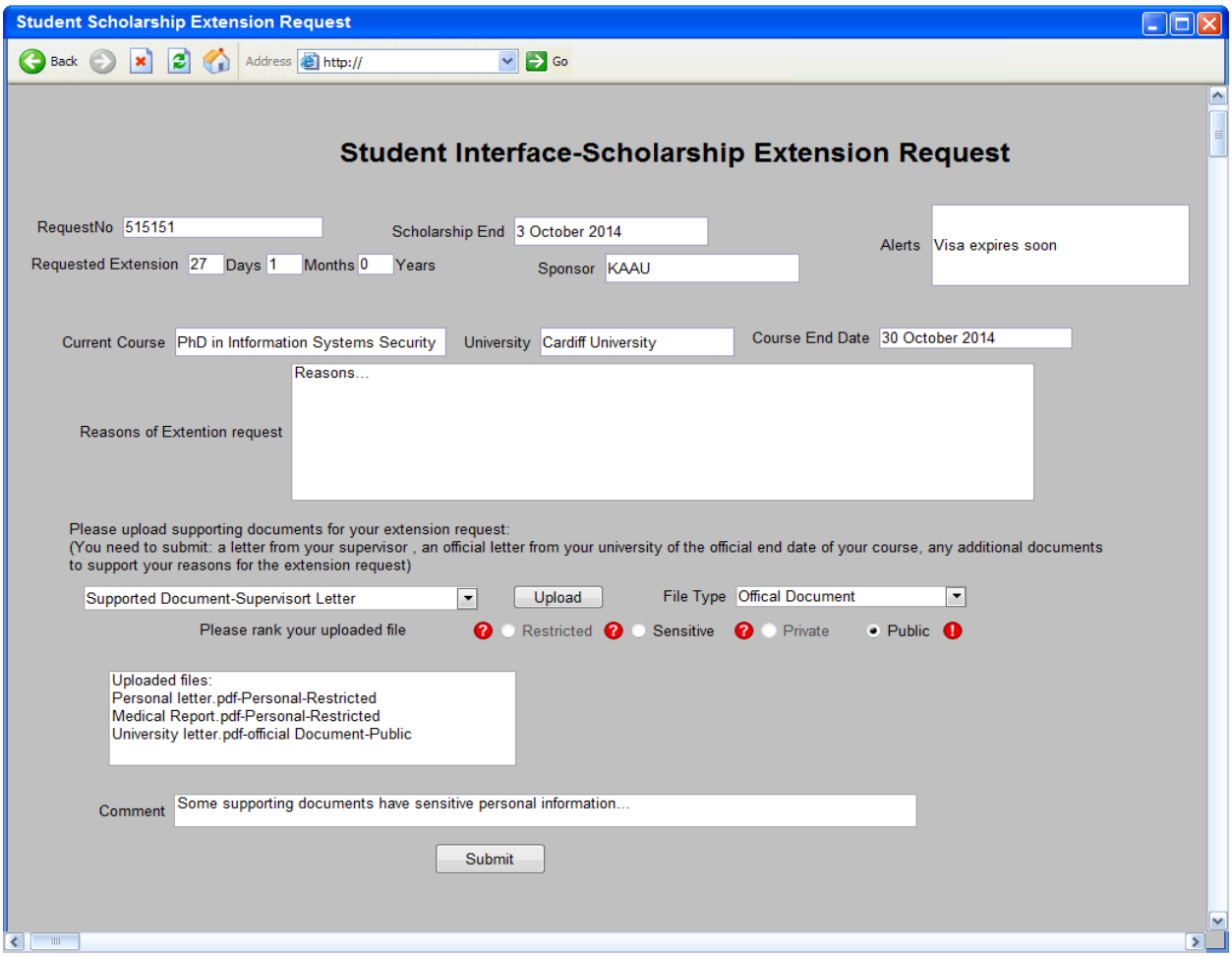
Appendix_Figure G.11: Enquiry Request-Student Screen



Appendix_Figure G.12: Private Enquiry – Head of Supervision Department Screen

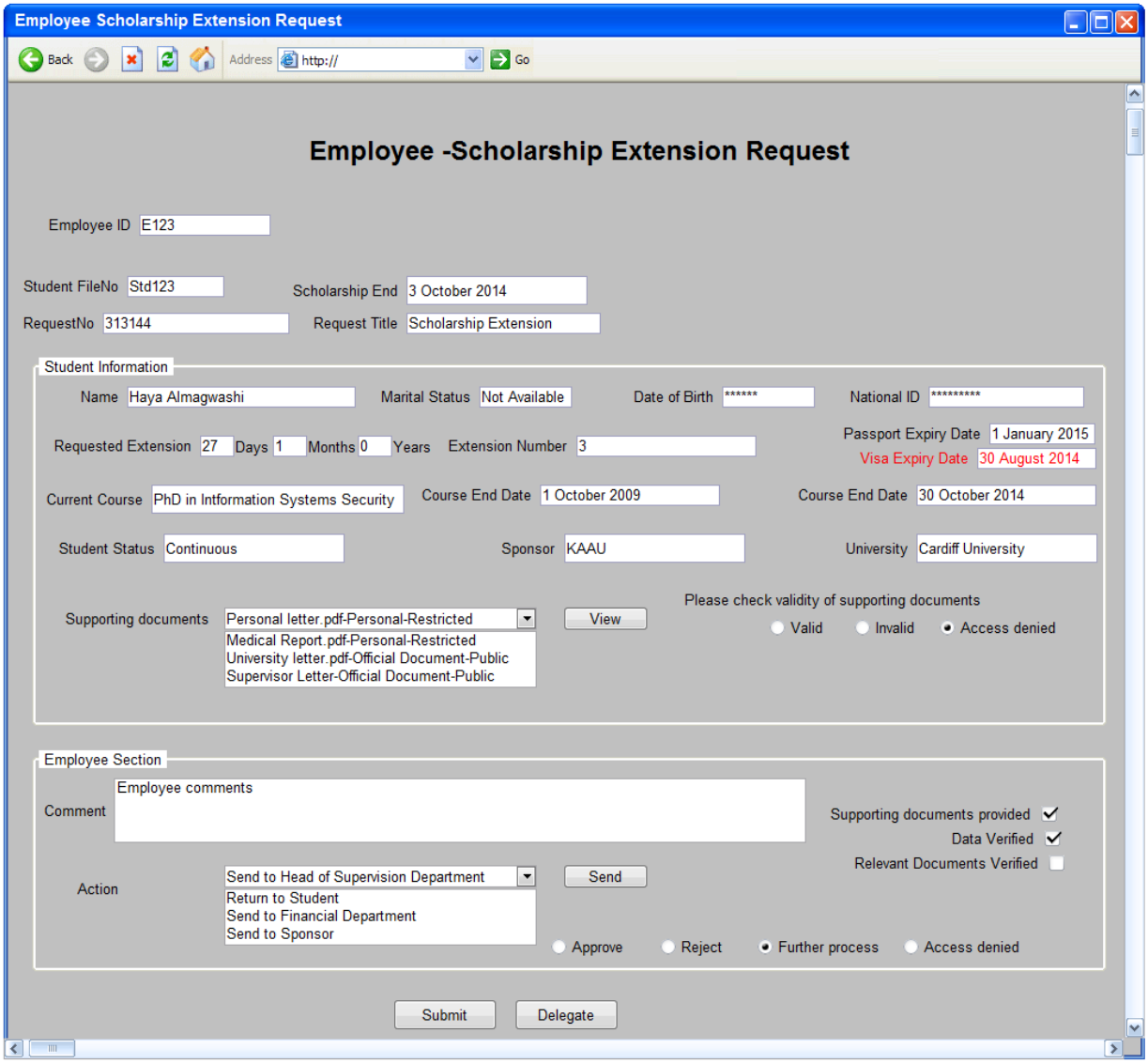
5. Scholarship Extension Request

This service is needed by some students who need to extend their scholarship to cover the time they need to complete their studies. The screen in Appendix_Figure G.13 presents a screen similar to the student screen when requesting the service. The student will enter the required extension time and should provide supporting documents required for the request. Again the student can rank the documents sensitivity as explained earlier in Update Personal Information service.

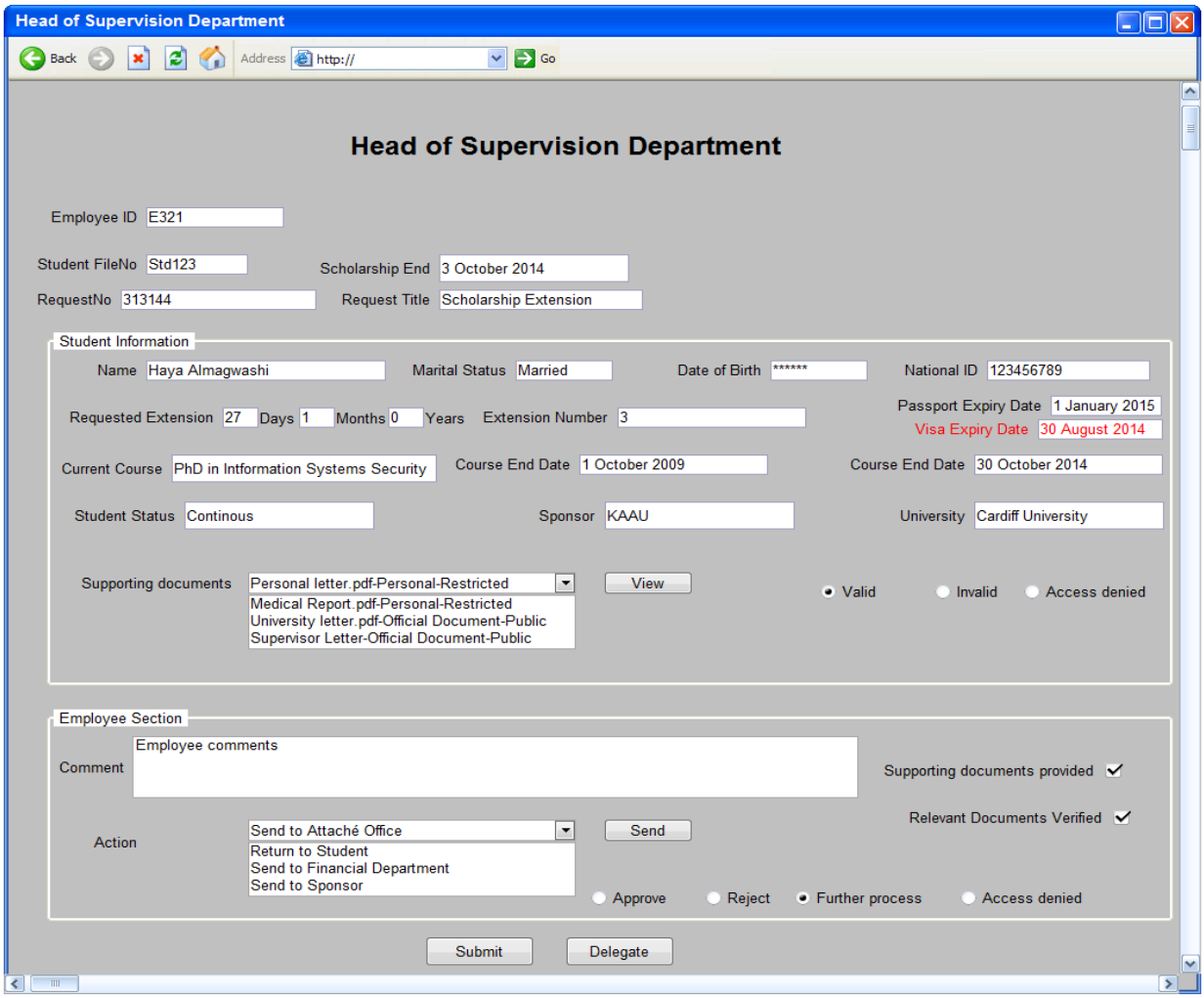


Appendix_Figure G.13: Scholarship Extension Request- Student Screen

The employee will review the request and verify the accuracy of the provided documents. However, if some of the documents were classified as sensitive or restricted or if the employee role was not given access to these documents, the employee will select access denied. In addition, the employee will decide on the next required action before completing the respond as in Appendix_Figure G.14 where the employee sent the request to the head of supervision department. Appendix_Figure G.15 show the screen of the Head of the supervision department where he decides on sending the request to the attaché office for further process.



Appendix_Figure G.14: Scholarship Extension Request- Employee Screen



Appendix_Figure G.15: Scholarship Extension Request- Head of Supervision Department Screen

Appendix H : Evaluation Interviews (EduPortal)

a) Evaluation Interviews Questions

Evaluation of Framework for Preserving Privacy in E-government (PRE_EGOV)

Purpose:-

This brief questionnaire and the semi structured interview are part of the evaluation phase for a PhD research. The questions are about the proposed framework for preserving privacy in the context of providing e-government services illustrated earlier in the presentation. All answers and responds will be kept anonymous and used only for the purpose of this research. Permitted voice recording will be used in this interview as agreed.

Interviewee ID: **Email (Optional):** **Contact (Optional):**

Section A: Background:

Q: 1 Which of the following describes your relation with electronic government services?

- Government body representative.
- Electronic Services' Provider.
- User
- Developer of electronic services.
- Other:……

Q2: Please state your current Role/Study Degree:
……

Q3: What things that you like about the current system from the prospective of preserving student privacy when processing the student requests?

Q4: Do you think that the current system preserves the privacy of the student? How?

Section B: Definitions: (Handout1-Framework definitions):

Q5: What do you think about the definitions?

Q6: Would you like to add/comment about any definition?

Section C: Privacy Requirements Validation: (Handout2-The forms in Appendix 9.b)

Q7: Do you like to add any relevant privacy requirements or mention any conflict that you see with the stated requirements?

Q8: If the user has been given full control over his/her information how you think this will affect your work?

D: Open Questions: (Based on the presentation and provided prototype screens)

Q9: To what extent you agree with that the proposed framework satisfies the following:

a. Useful

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

b. Will be accepted by students

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

c. Will be accepted by services provider

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

d. Is viable (i.e. can be implemented)

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

e. Easy to use

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

f. Transparent (i.e. the users are aware of the way their privacy is preserved and when and by whom their information is shared)

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

g. Flexible (i.e. the system is flexible enough to respond to dynamic changes in the expectations and needs of involved parties)

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

h. Meets the identified security requirements of the provided service.

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

i. Enforces local relevant laws, policies and regulations issued by the government

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

j. Complies with relevant international standards and guidelines.

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

k. Considers the impacts of social and cultural factors in the system environment.

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

l. Considers the impact of political environmental factor.

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

m. Cost effective

1. Strongly agree 2. Agree 3. No Opinion 4. Disagree 5. Strongly disagree

Q10: Do you like to add any comment?

Comments:

……

Thank you for your precious time and help

b) Evaluation Interviews Summary

The interviews were with six users (**[UserID1],[UserID2],[UserID3],[UserID4],[UserID5],[UserID6]),** three service providers([**SPID1],[SPID2],[SPID3]),** one government representative**[GR]** and two developers **([DevID1],[DevID2]).**

Important Note: Again due to the sensitivity of the given information and the conditions imposed by the government agency who agreed to participate in the case study, the exact transcript of all the interviews at all stages was not provided, however, quotes from the interviews were given where appropriate.

1. **Summary of Responses to Open Discussion in the Initial Evaluation interviews during the application of PRE_EGOV and the Final interviews:**
   (Initial Evaluation interviews were in the session to verify the identified privacy requirements and assigned ownership rights and levels of controls).

Qt1. Agreed on removing delete access right from ownership right Totally Owned. Hide is suggested instead. [All interviewees]
Qt2. Interviewees agreed on the requirements, the classification of the data types [All interviewees].
Qt3. The pop up privacy awareness messages that appears according to the user's choices of level of control are clear and informative [All interviewees]
Qt4. I like that our opinion are considered in the provision of the service [all users].
Qt5. The settings of the levels of control should not conflict with the functionality of the system [All interviewees].
Qt6. Sensitive and private types needed more explanations to clarify the difference between them. More examples needed to clarify the difference between the two types [UserID4], [UserID5], [UserID6].
Qt7. I will not want this to affect the respond time for financial requests as time is crucial for such requests [UserID1], [UserID2], [UserID3], [UserID4], [UserID5], and [UserID6].
Qt8. "The service provider might not accept this as it will limit their access rights and it might give overload them with more work" [UserID3].
Qt9. It was useful to explain what is meant by the assigned ownership rights and levels of control to the user by examples so the meaning of those rights is clear [UserID1], [UserID2], [UserID3], [UserID4], [UserID5], and [UserID6].
Qt10. You need to set the default to something that suites every one, and does not slow the functionality and at the same time does not violate the right of privacy of the user [SPID1], [SPID2] [SPID3], [DevID1].
Qt11. The system will not be practical without raising privacy awareness before the use of the system so the user can benefit from the proposed framework [All interviewees].
Qt12. Show how the framework works using scenario [All interviewees].
Qt13. "We have different access privileges, so the level of control that the student can have should limit the provision of the service"[GR]
Qt14. The system owner is the government [GR].
Qt15. "Flexibility depends on other parties, if the application is designed very well and the policies are applied well (the framework provide the requirements , propose how it can be satisfied, however the way it is applied decide on if it is flexibility is satisfied, if the requirements defined are met , then the system is flexible"[SPID3].

Qt16. “The final say should be up to the business owner to finalise the requirements that suites their own policies and according to the cost. End customers will be applying the result”[GR]
Qt17. “Business owners (here the government and its ministry) understand the system more than the student. When it is applied it will remove the conflict between the stakeholders. The framework helps in resolving this conflict and clarifies the picture for all involved parties about the data that are more important to the users and should be protected and the privacy issues that a user is concerned about”[SPID3].
Qt18. “Customer is important, but at the abstract level the business owner has the final say” [SPID2].
Qt19. The application of the proposed framework will increase trust in using the EduPortal Services [All users], [DevID2], [DevID2], [SPID1], and [SPID2].
Qt20. “I believe it will increase users’ trust in EduPortal services and it will make them make less visits when they have sensitive issues (many students come to the government office when it is a personal matter to avoid uploading files in the service.)” [SPID3]
Qt21. “Students have no alternative but using EduPortal services online , however ,I believe it will make them made less enquiries about who is dealing or viewing their data”[GR].

2. Summary of responses to the Final Evaluation Interviews

The first and second questions were about the roles of the interviewees to confirm their category as stakeholders.

For the rest of the questions, the following are the main points highlighted in the interviews:

Q3: What things that you like/or dislike about the current system from the prospective of preserving student privacy when processing the student requests?

Like:

1. The quick response to requests **[All interviewees].**
2. The history of requests with the comments is available to student. **[UserID1], [UserID2], [UserID3], [UserID6]**.
3. All changes to student data are performed only via requests from the system and the student is always aware of the changes and notified by email about any request performed on his record **[All interviewees].**
4. The employee has access to any information that he might need to inform his decision about the request and help his respond quickly **[SPID3], [GR].**
5. Easy to use interface **[All users], [DevID1].**
6. All services totally provided online which safe time **[UserID5].**

Dislike:

1. Employees have access to sensitive information even if not needed **[All users],** [**SPID1], [SPID2], [DevID1], [DevID2].**
2. Students have no control on their personal information **[UserID1], [UserID2], [UserID3], and [UserID4]**.
3. The system does not encrypt any sensitive information **[DevID2].**
4. Every employee can see the whole PDF file and it has sensitive documents **[UserID6].**
5. Student does not know who dealing with his request **[UserID2].**

6. Repeated requests for updating personal information **[UserID5].**

Q4: Do you think that the current system preserves the privacy of the student? How?

1. The current system doesn't preserve privacy in a satisfying way **[GR],** [**SPID1], [SPID2], [SP3], [DevID1], [UserID4], [UserID5], and [User6].**
2. Partially, because security measures applied to prevent other persons from outside the system to log in to the student record, but employee has access to everything in the record **[DevID2], [SPID3], [UserID1], [UserID2], and [UserID3].**

Section B: Definitions: (Handout1-Framework definitions):

Q5: What do you think about the definitions (Ownership rights/Levels of control)?

1. All definitions were clear, comprehensive **[GR], [SPID1], [SPID2], [SP3], [DevID1], [UserID2], [UserID4], [UserID5], [User6].**
2. Clear with provided examples **[UserID1], [UserID3], and [DevID2].**

Q6: Would you like to add/comment about any definition?

3. No comments **[All interviewees]**

Section C: Privacy Requirements Validation: (Handout2-The forms in Appendix 9.b)

Q7: Do you like to add any relevant privacy requirements or mention any conflict that you see with the stated requirements?

1. All interviewees agreed on the provided requirements and the suggestion for resolving conflicts.

Q8: If the user has been given full control over his/her information how you think this will affect your work/service?

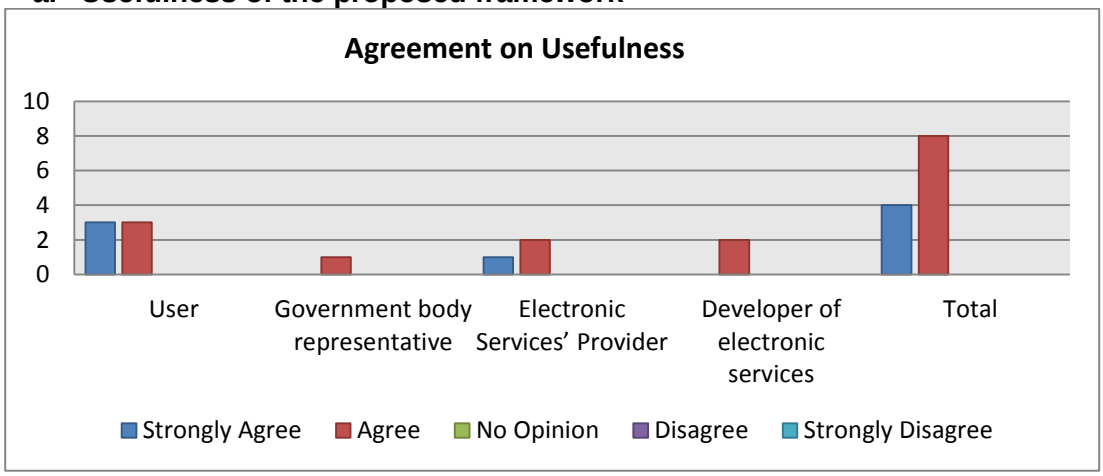
1. "it might make some requests slow as they will be returned to the user to change the privacy settings, the privacy default settings should be something in the middle with less distractions to the process of the service" **[GR]**
2. "Yes I think my access rights will be limited**"[SPID1],** "I am fine with it, it might slow response" **[SPID2],** "it might bring more steps to the process" **[SPID3]**
3. "No effect, we might need to encrypt sensitive data" **[DevID1].**
4. It might slow the process of a request **[DevID2], [UserID1], [UserID2].**
5. It might make the response to request longer, but I still want to be in control of my data [UserID5], [UserID6].
6. No effect [UserID3].

Qt22. "The system might make the respond to my requests take longer time if I made my privacy settings are set to high. But I do not mind as long I know that my private information is secured" [USerID4].

Q9: To what extent you agree with that the proposed framework satisfies the following:

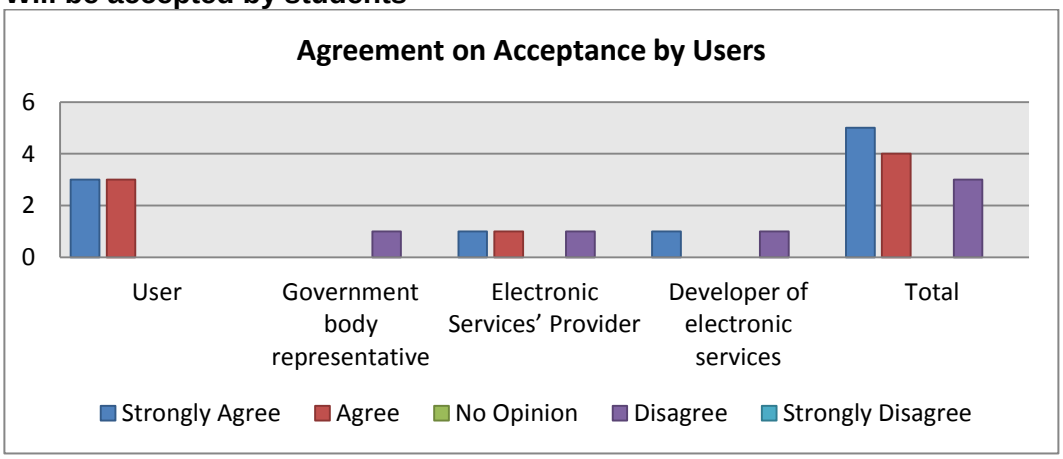
The following figures summaries responses to the elements in Q9:

a. Usefulness of the proposed framework



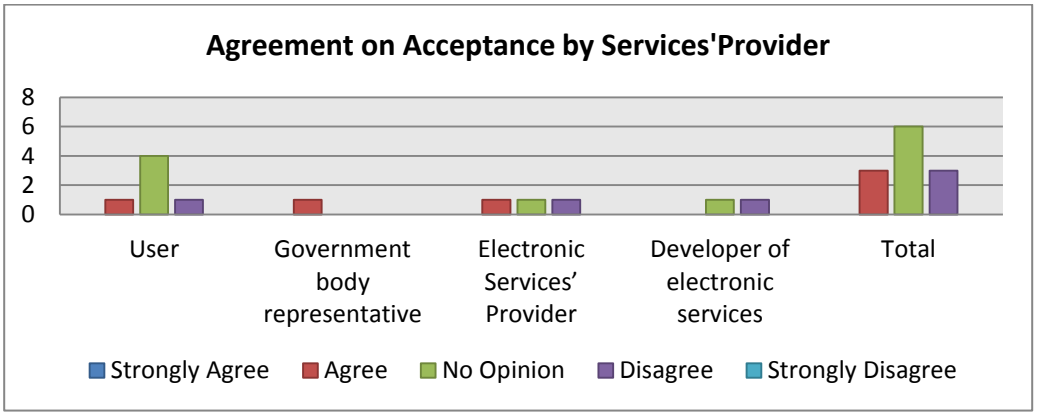
Appendix_Figure H.1: Responses to Usefulness of the proposed framework

b. Will be accepted by students



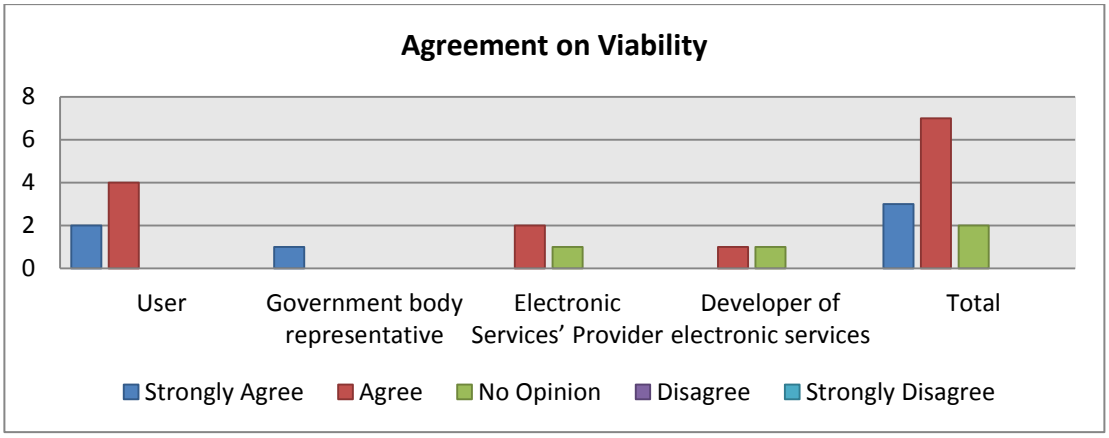
Appendix_Figure H.2: Responses to Users Acceptance of the proposed framework

c. Will be accepted by services provider



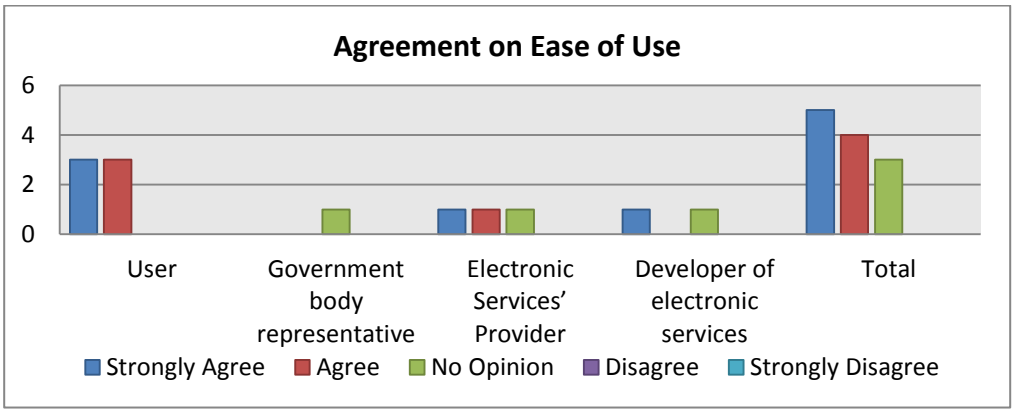
Appendix_Figure H.3: Responses to Services' Provider Acceptance to the proposed framework

d. Is viable (i.e. can be implemented)



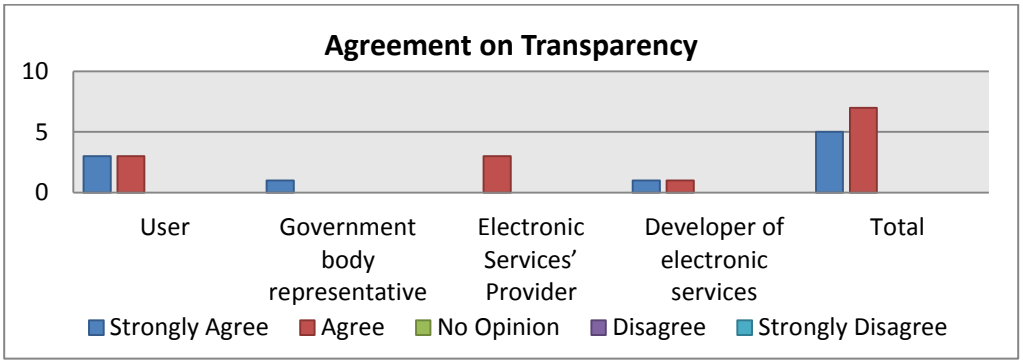
Appendix_Figure H.4: Responses to the Viability of the proposed framework

e. Easy to use



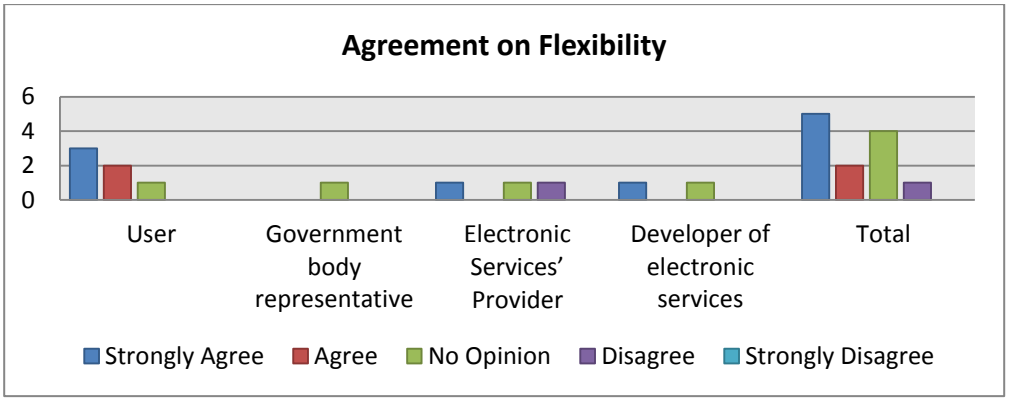
Appendix_Figure -H.5: Responses to the Ease of Use of the proposed framework

f. Transparent (i.e. the users are aware of the way their privacy is preserved and when and by whom their information is shared)



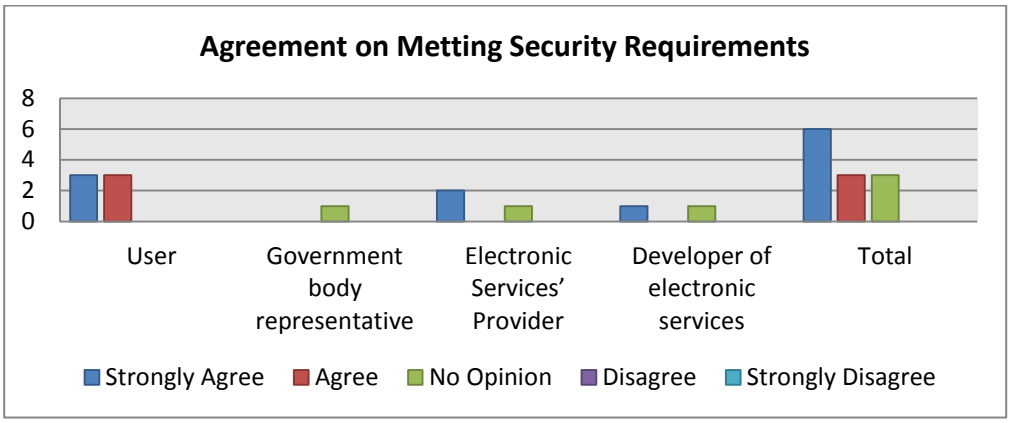
Appendix_Figure H.6: Responses to the Transparency of the proposed framework

g. Flexible (i.e. the system is flexible enough to respond to dynamic changes in the expectations and needs of involved parties)



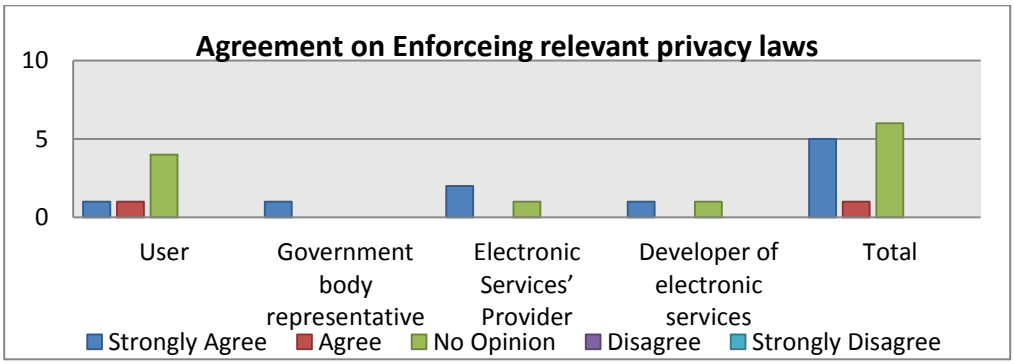
Appendix_Figure H.7: Responses to the Flexibility of the proposed framework

h. Meets the identified security requirements of the provided service.



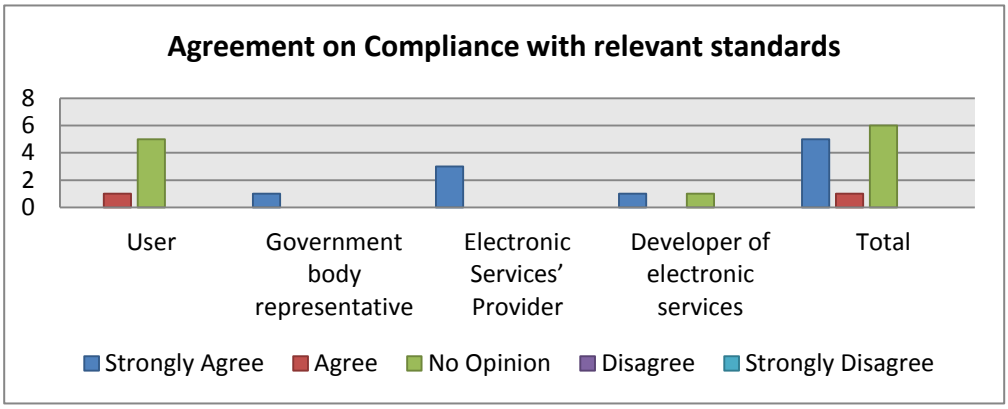
Appendix_Figure H.8: Responses to if the proposed framework meets identified security requirements

i. Enforces local relevant laws, policies and regulations issued by the government



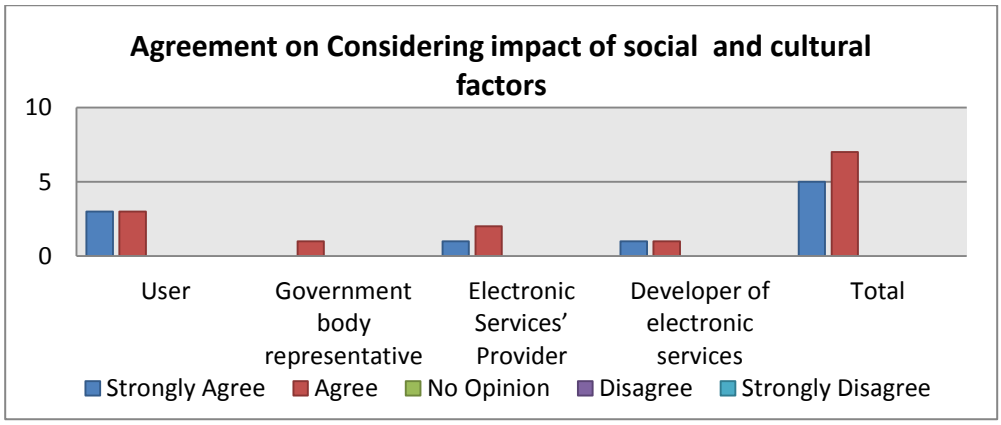
Appendix_Figure H.9: Responses to if the proposed framework enforce relevant laws, policies and regulations

j. Complies with relevant international standards and guidelines.



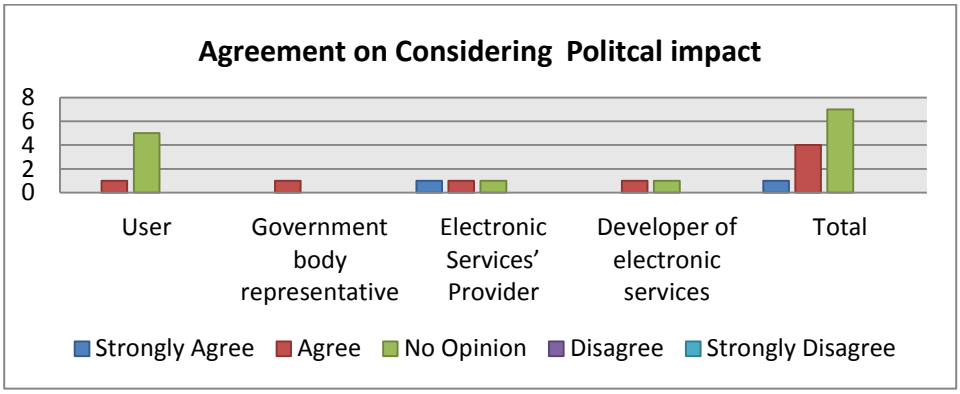
Appendix_Figure H.10: Responses to if the proposed framework complies with relevant standards and guidelines

k. Considers the impacts of social and cultural factors in the system environment.



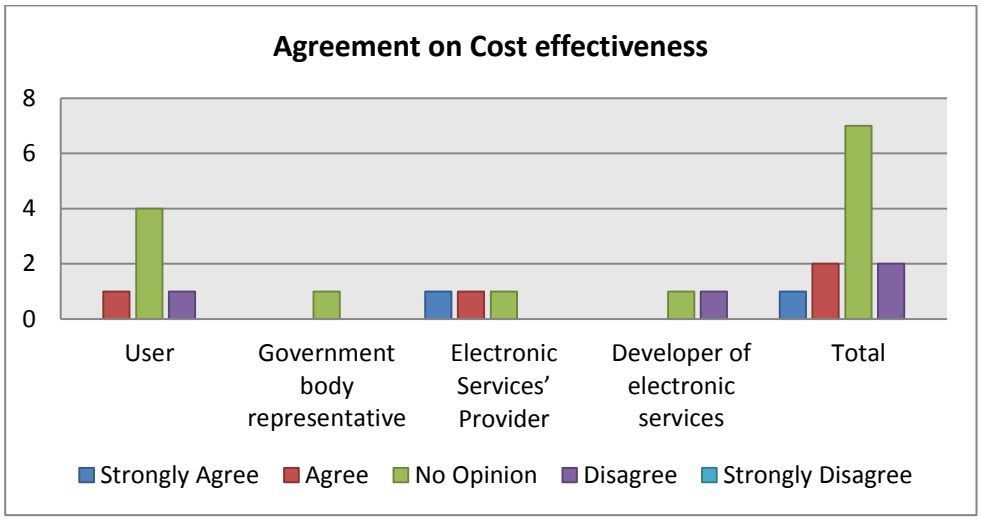
Appendix Figure H.11: Responses to if PRE_EGOV considers the impact of social and cultural

l. Considers the impact of political environmental factor.



Appendix Figure H.12: Responses to if the PRE_EGOV considers the impact of political factor

m. Cost effective



Appendix_Figure H.13: Responses to cost effectiveness of the proposed framework

Q10: Do you like to add any comment?

1. "This is a fantastic study that should be supported. Congratulations and good luck" **[SPID1].**
2. "The system is good from the user point of view, but it might cost the service provider money and time" **[SPID2].**
3. "I think it can be applied but might cost money and time" **[DevID1].**
4. "It needs government will and awareness from users "**[UserID1].**
5. "It needs government will to do it" **[UserID4].**
6. "The system is very useful" **[UserID2].**
7. "I see that the framework is applicable and the government willingness is important for the successful application of this framework" **[DevID2].**
8. "It is a good thing the framework considers the user and the negotiating between stakeholders, example the agreement on the classification of ID File that contains picture (before picture erased for privacy)" **[SPID3].**
9. "It should have the point of view of the user; this is the strength we see in the framework" [**GR].**
10. "I think that applying the framework will increase the acceptance of systems and e-services provided by the government. Although sometimes you are enforced to use e-services by the discounted fees and the limitation of alternatives" **[UserID3].**