Journal of Cybersecurity, 2026, **12**(1), 1–22
https://doi.org/10.1093/cybsec/tyag008
Review Article

JOURNAL OF CYBERSECURITY OXFORD

The anatomy of an access control reader: a cybersecurity perspective

Peter Jones, Lowri Williams*, Eirini Anthi

School of Computer Science & Informatics, Cardiff University, Cardiff, CF24 4AG, United Kingdom
*Corresponding author. School of Computer Science & Informatics, Cardiff University, Cardiff, CF24 4AG, United Kingdom. E-mail: williamsl10@cardiff.ac.uk

Abstract

Access control readers are the first line of defence for organizations to restrict access to their facilities to the people who are supposed to be there. Such readers represent a major investment for organizations and are replaced every 7–10 years. The choice of reader and credential made at the time the system was designed and installed may be vulnerable to an array of attacks, such as credential cloning and data transmission exploits, which would allow a threat actor to pass through an entrance undetected. Once the threat actor has entered the building, the people and/or assets that the organization are responsible for are at risk. Access control readers have a number of interfaces based on different technologies that may be attacked to learn more about the configuration and other features of the device. This information may then be used to craft an attack on a real system. To the best of our knowledge, this is the first paper that outlines the various technologies incorporated into these products and draws upon this data to present the first model of the contemporary access control reader. The model is then further developed by considering the cybersecurity implications of each of the technologies found in an access control reader. Finally, based on known attack vectors, the model may be used as a risk assessment framework for readers and credentials. From this foundation, a series of further research topics are then proposed.

Keywords RFID, access control, smart card, operational technology

Introduction

Locks and keys have been integral to security for ˜4000 years [1]. Since their invention, an ongoing battle has persisted between those designing locks to protect assets and those seeking to defeat them. In the modern era, organizations rely on electronic locks and keys managed by physical access control systems to secure their facilities. These systems represent a significant capital investment, with organizations expecting them to remain effective for 7–10 years before requiring upgrades or replacements [2].

Over the past decade, access control credentials (the ‘keys’) and readers (a component of the ‘lock’) have drawn considerable attention from security researchers and hackers, particularly through platforms like proxmark.org [3] and high-profile publications [4–7]. This body of research has demonstrated numerous credential cloning attacks on widely used access control cards and shown how attackers can bypass readers to inject valid credentials directly into access control systems.

Many access control systems installed in the last decade may not have accounted for evolving cybersecurity threats, nor undergone periodic security assessments. As a result, numerous systems in active use today remain vulnerable. A cloned or spoofed credential allows an attacker to gain unauthorized access, effectively bypassing the access control system as if they were the legitimate cardholder.

Despite the well-documented risks, a standardized penetration testing methodology for access control readers has yet to be established. Current security evaluations are often conducted by individuals with general IT skills, relying on ad hoc techniques derived from sources like proxmark.org [3]. This lack of a formalized framework means that testing is inconsistent and often insufficient. Without a structured penetration testing model, organizations may struggle to assess and mitigate vulnerabilities in their access control systems effectively.

To the best of our knowledge, this is the first paper that presents a comprehensive analysis of a variety of access control readers currently available in the market. This analysis is fundamental in forming the beginnings of an advanced penetration testing framework specifically tailored for these systems. Primarily, this paper highlights the urgent need for a dedicated security evaluation methodology, ensuring that access control technologies are rigorously tested and resilient against emerging threats.

The paper consists of the following contributions:

- A paper-based analysis of commercially available products to identify the technologies used by the readers in enterprise access control systems.
- The construction of a generic model of an access control reader showing the interfaces to the outside world and the flow of data through the device.
- An attacker/penetration tester view of the model, describing the various attack vectors.

Received: 28 July 2025. **Revised:** 7 January 2026. **Accepted:** 18 February 2026

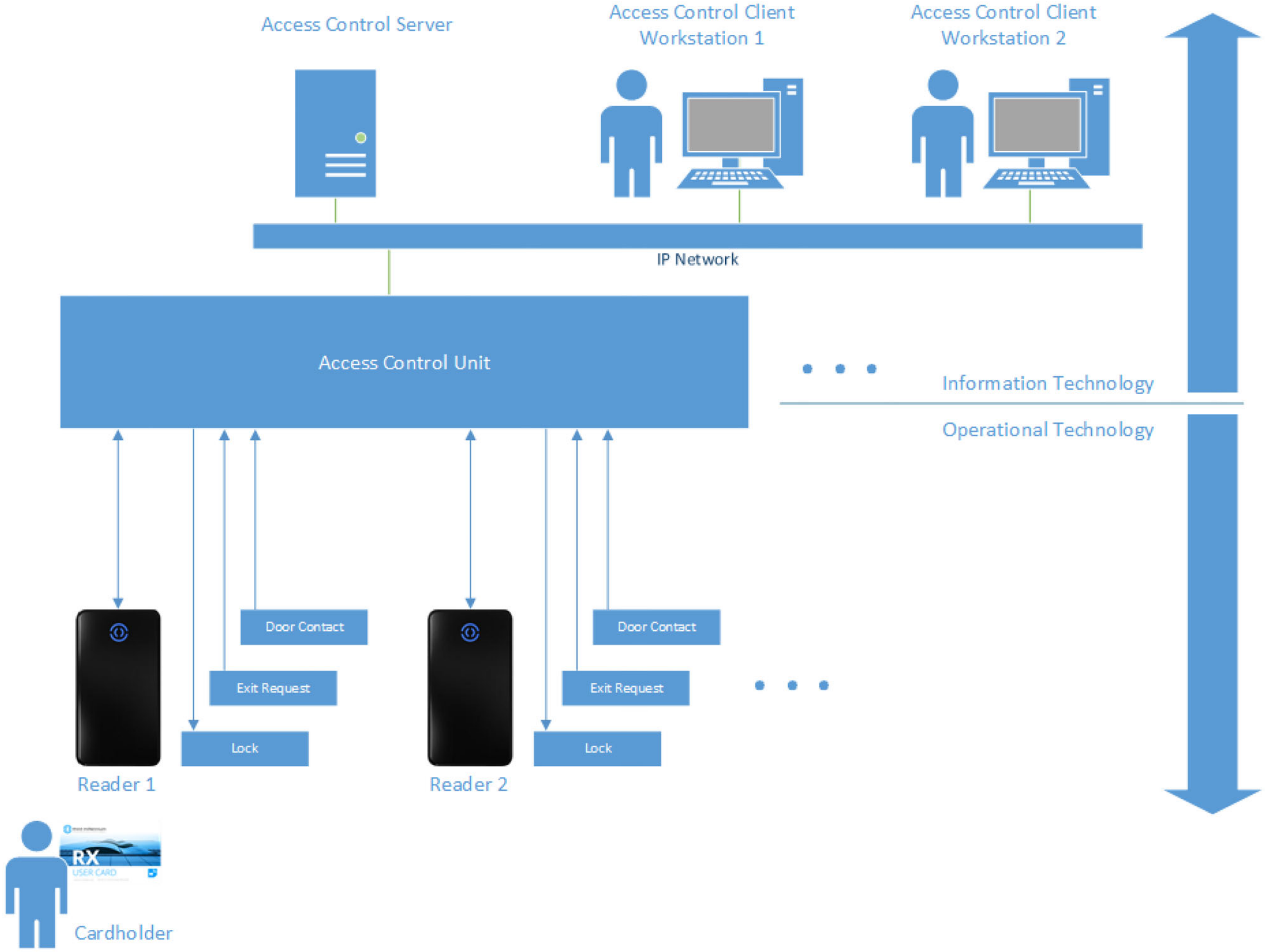


Figure 1. A typical access control system including readers, access control unit, and servers.

The remainder of this paper is structured as follows. The section ‘Background information’ places the access control reader in the context of an enterprise access control system. The section ‘Related work’ reviews existing work related to the cybersecurity of access control readers, with particular emphasis on credential cloning and protocol-level attacks. The section ‘Methodology and scope of review’ introduces the methodology and scope of the study, including the structured review process, inclusion and exclusion criteria, and the rationale for device selection. The section ‘Data sheet review’ presents a structured analysis of manufacturer documentation for the selected readers and summarizes their supported technologies and interfaces. The section ‘Technology and cybersecurity review’ analyses the identified technologies against known cybersecurity issues reported in the literature. The section ‘A functional anatomy of an access control reader’ constructs a generic functional model of an access control reader, compiling relevant technologies and interfaces for subsequent analysis. The section ‘Attacker model’ develops this model from the perspective of an attacker or penetration tester, identifying potential attack surfaces and threat vectors. An illustrative application of the proposed framework is then presented in the section ‘Demonstrative application of the proposed framework’ to demonstrate how it can be applied in a structured manner to reason about security risk using documented configurations. Finally, the section ‘Conclusion’ concludes the paper, and the section ‘Future work’ discusses directions for future research.

Background information

The following sections provide an outline of the structure of a modern access control system. This allows the access control reader to be seen in the context of the overall system. There are a number of enterprise access control systems available on the market today. The OnGuard system from LenelS2 [8] and the C-CURE 9000 system from Software House [9] are examples of two systems used by governments and large enterprises around the world. The abstraction of the architecture described in Fig. 1 is based on direct experience with these systems and may be applied to the majority of access control systems on the market.

Cardholder

The cardholder may be an employee, a contractor, a visitor, or anyone who in some other way is related to the enterprise. As part of their relationship with the host organization, they are issued with a credential that allows them to access certain areas. Access is gained by presenting the credential to an access control reader at the point of entry. The credential can take many forms: a magnetic stripe card, an RFID card or a Bluetooth credential stored on a mobile phone, for example. The enterprise will choose the credential type according to their needs. The enterprise may also enforce multi-factor user verification at the point of entry where a PIN and/or biometric is required to be entered or presented in addition to the credential.

There is also a use case where the term cardholder is a misnomer. There are biometric identification technologies that can identify an individual from a fingerprint, an eye iris scan, or by scanning some other physiological aspect of a human being, and turn this reading into a unique number compatible with the access control system to which they are connected.

The responsibility of the cardholder is to know when, where, and how they may use the credential that has been issued to them.

Reader

The access control reader is an electronic device that reads a unique identifier for the cardholder. There are many types of access control readers: from the single technology reader to a multi-factor biometric device.

Once the credential has been read, the reader may request a second factor (e.g. a biometric reader might require a fingerprint to be read) to verify the identity of the user.

Once this initial read phase has been completed, the unique identifier of the cardholder is transmitted to the Access Control Unit (ACU). The reader may then be asked to display the result of the access control request by the ACU or request a second factor (e.g. a keypad reader may request a PIN to be entered).

The responsibility of the reader is to read a unique identifier from a credential, or the cardholder in the case of biometric identification, relay it to the ACU and display the decisions of the ACU.

Access Control Unit

The ACU provides the local decision-making concerning whether a cardholder may gain access at a particular entry point. The ACU may support a number of readers and, therefore, entry points into and egress points out of the areas and/or buildings defined for the organization.

When a unique identifier, or card number, is transmitted to the ACU by a reader, a decision must be made as to whether the cardholder should be granted access to the entry or egress point:

- Is this card number known to the system?
- Is this card number allowed to access the specified entry or egress point?
- Is this card number allowed access at this time?
- Does the ACU require a second factor for this card number?

These are only some of the many decisions that can be made to determine access or otherwise for the card number read by the access control reader. It should also be noted that there is not necessarily an equivalence between the card number and the cardholder. An access control system deals with card numbers and the ACU makes a decision on the card number delivered by the reader. In this case, the question that is left unanswered is how the system knows that this number has come from a card presented by the cardholder.

In a basic form, the ACU is also responsible for monitoring the egress button used to unlock a door from the inside when there is no reader, the door monitor contact to monitor when the door is opened and closed and for firing the relay that unlocks the door.

In the modern access control system, the ACU sits on the enterprise's IT network. The ACU obtains a local database for local decision-making from the access control server over this network. The database may either be pulled from the server by the ACU or pushed to the ACU by the server.

Access Control Server

The Access Control Server is the 'source of truth' for the entire system, maintaining the state of the system in the master database to be pushed towards the periphery (i.e. the ACU and Readers) and receiving and storing events from these devices. The Access Control Server runs on one or more dedicated server machines that may be on-premise or in the cloud. All of the major systems vendors are now offering cloud-hosted solutions that are more convenient to configure through the use of virtual machines and, increasingly, container-based solutions. Another mainstay of the modern Access Control Server is a Web API to allow integration with external services that can dynamically manage cardholders (e.g. a human resource management system).

Access Control Client

The Access Control Client (client) provides a user interface onto the overall system allowing an administrator to:

- enter cardholders and their permissions into the system,
- configure the ACUs (e.g. IP address, number of doors, readers),
- configure reader operation (e.g. card only, card and PIN),
- monitor events in real-time,
- run reports on past events,
- run reports against the cardholders configured in the system, and
- manage other administrators of the system.

The Access Control Client may be a desktop application (usually running on Windows) or a web browser consuming a web application hosted as a cloud service or implemented directly on the Access Control Server.

Related work

To the best of our knowledge, this work provides the first consolidated, technology-centric analysis of enterprise access control readers from a cybersecurity perspective, focusing on the reader as an integrated system rather than examining individual credential or transmission technologies in isolation. While prior research has investigated vulnerabilities in specific credentials, protocols, or attack techniques, there is no directly comparable study that systematically maps these technologies into a unified reader-level security model.

Accordingly, this analysis draws on a combination of peer-reviewed academic literature, publicly disclosed security research from the penetration testing community, and practitioner expertise from a Chief Technology Officer with over 35 years of experience in access control and physical security. These sources are used to identify known attack vectors and security-relevant behaviours across credential, transmission, and interface technologies. The objective is to consolidate and structure existing knowledge, rather than to introduce new empirical attack demonstrations.

Low frequency cards

Proximity card technology began gaining traction in access control systems from the 1990s onwards. During this period, HID (later known as HID Global) emerged as the dominant player in the market, making their technology a key focus for both security researchers and competing manufacturers.

In 2007, IOActive, a security research firm, planned to present a paper at the Black Hat Convention demonstrating vulnerabilities in HID Global's proximity card technology, particularly its susceptibility to cloning. However, HID Global intervened, requesting IOActive not to publish their findings, leading to the withdrawal of the presentation [10]. HID Global later issued its own statement regarding the situation [11].

This high-profile exchange played out in front of the security research community and underscored HID Global's determination to protect its intellectual property. However, it also sparked broader interest in the security of access control credentials, particularly among researchers and hackers who sought to explore and expose the vulnerabilities of these systems.

Despite the increasing focus on access control security, formal academic research on low-frequency credential technologies remains scarce. Instead, the primary source of practical research into 125kHz low-frequency credentials has come from Proxmark.org [3], an online community dedicated to exploring RFID security. Detailed implementation insights and vulnerabilities for a wide range of low-frequency credentials can be found within this community's research archives.

The fundamental issue with low-frequency credentials in access control systems is their lack of cryptographic protection or any form of secret authentication mechanism. Once the underlying implementation is understood, these credentials can be easily cloned or spoofed, making them inherently insecure. This weakness highlights the pressing need for organizations to transition away from legacy low-frequency systems and adopt modern, cryptographically secure credential technologies to mitigate security risks.

LEGIC Prime

LEGIC Prime (originally known as LEGIC) is an RFID card technology that saw widespread adoption in German-speaking countries, including Germany, Austria, and Switzerland. In their 2011 paper, Plotz and Nohl [12] conducted an in-depth analysis of the technology, combining silicon reverse engineering with protocol analysis, observing the communication between a tag and a reader. Their findings revealed fundamental security weaknesses, leading them to conclude that 'systems must not rely on obscurity but should rather employ cryptography as a base for security functions'.

Similar to earlier low-frequency credentials, LEGIC Prime was ultimately reverse-engineered, allowing researchers to fully understand its implementation. As a result, cloned credentials could be created, effectively undermining the security of systems relying on this technology. This research reinforced the well-documented risk that proprietary security mechanisms without strong cryptographic protections are vulnerable to systematic analysis and exploitation.

MIFARE Classic

According to Garcia and Jacobs [13], by 2008, MIFARE Classic had become the most widely used contactless smartcard technology in the world. Their paper provides a detailed account of how serious security flaws in MIFARE Classic were uncovered and the challenges faced by researchers in disclosing these vulnerabilities. As with other access control technologies, the publication of security weaknesses was met with strong resistance from the manufacturer, NXP, highlighting the ongoing tension between responsible disclosure and corporate interests in protecting proprietary technology.

The paper describes how the MIFARE Classic cipher was reverse-engineered through physical analysis of the integrated circuit, leading to the discovery of multiple cryptographic weaknesses. These vulnerabilities were not merely theoretical—practical exploits were developed that allowed for cloning and bypassing of access control systems. In addition to the technical challenges, the researchers also had to navigate complex discussions with various stakeholders, including NXP and the Dutch government, to ensure their findings were responsibly disclosed without causing widespread security failures.

The MIFARE Classic case serves as a cautionary tale about the dangers of relying on security through obscurity and the critical need for strong cryptographic design in access control systems. The resistance to disclosure from manufacturers did not prevent attackers from eventually discovering and exploiting these vulnerabilities, demonstrating that ignoring security flaws does not make them disappear. This case underscores the importance of regular security audits, where organizations must evaluate their access control technologies to ensure they are not relying on outdated or compromised cryptographic mechanisms. It also highlights the need for a proactive security approach, where manufacturers work collaboratively with researchers to strengthen security before real-world attacks occur.

Ultimately, the MIFARE Classic vulnerabilities illustrate a broader lesson—legacy access control systems without robust cryptographic protections pose a major security risk, and organizations must take preventative action to mitigate these threats before attackers do. Transitioning to modern, cryptographically secure alternatives, such as MIFARE DESFire EV3 or HID Seos, is no longer optional but a necessity for organizations prioritizing security.

HID iClass

HID is the clear market leader for access control readers and their products attract a lot of attention from the security research community. The iClass technology was no exception and a series of papers appeared between 2010 and 2014 that scrutinized the implementation of this technology.

The 2010 'Heart of Darkness' paper [6] reminds us that not all product implementations are perfect. The master key used for standard iClass credentials was a closely guarded secret by HID. Readers supplied by HID had a programming header and it was simple enough to peel away the potting (the protective material, typically a resin, epoxy, or silicone compound around the device) and determine the type of microcontroller used in the reader. It was then possible to extract the flash image of the reader and locate the master key used to read a card. This paper was another example of exposing vulnerabilities and by 2012, HID had responded with an improved version of the technology called iClass SE.

Garcia [5] takes a more academic approach to recovering the iClass master key, critically analysing HID's security decisions. He highlights a fundamental flaw in HID's design choices, stating, 'It is hard to imagine why HID decided, back in 2002, to use single DES for key diversification considering that DES was already broken in practice in 1997'. This observation underscores a lack of security by design in early 2000s access control systems, where outdated cryptographic practices were still being implemented despite known vulnerabilities.

Building on this, Garcia [14,15], while acknowledging the prior contributions of Kim [16] and Meriac [6], expands the research to describe practical key recovery attacks on iClass technology. His findings further reinforce the inherent weaknesses in iClass security, concluding, 'We have shown that the security of several building blocks of iClass is unsatisfactory. Again, obscurity does not provide extra security and there is always a risk that it can be circumvented'. This statement highlights the pitfalls of relying on security through obscurity, demonstrating that without robust cryptographic protections, proprietary security mechanisms can be systematically analyzed and bypassed.

NXP DESFire

At the time of writing (January 2024), the technology of choice for many large organizations and governments [17] is NXP Mifare DESFire. DESFire is currently on its fourth iteration (DESFire EV3).

A successful key recovery attack on first-generation DESFire cards was described by Oswald and Paar [18], leveraging side-channel analysis to extract cryptographic keys. Instead of exploiting weaknesses in the encryption algorithm itself, the attack focused on observing unintended physical leakages, such as power consumption fluctuations during authentication. By carefully measuring these variations while the card processed authentication requests, attackers could identify patterns that revealed portions of the secret key, ultimately leading to a full key recovery. Once obtained, this key could be used to impersonate legitimate cards, clone credentials, or manipulate access control systems.

However, executing such an attack was far from trivial. The process required capturing a large number of power traces, making it computationally expensive and time-consuming. Additionally, precise synchronization with authentication operations was necessary, requiring specialized oscilloscopes and probes to detect subtle power variations. External factors such as electromagnetic noise or fluctuations in the power supply could further distort the collected data, complicating analysis. Moreover, the attack demanded advanced cryptanalysis skills and specialized hardware, limiting its practicality for casual attackers.

Recognizing these vulnerabilities, NXP introduced significant security improvements in DESFire EV1 to mitigate side-channel threats. Countermeasures included randomized power consumption patterns, making power analysis significantly harder, along with enhanced cryptographic protections to reduce the risk of key leakage. These enhancements strengthened resistance against power analysis and other side-channel attacks, ensuring that later generations of DESFire were more secure. While the side-channel key recovery attack on first-generation DESFire was a noteworthy demonstration of potential weaknesses, its complexity limited widespread exploitation. Nonetheless, this research played a critical role in shaping modern smart card security, leading to the development of more resilient access control technologies.

The flawed pseudo-random number generator in first-generation MIFARE Classic credentials led Hurley-Smith [19] to evaluate the true random number generator (TRNG) used in DESFire EV1. His research revealed preliminary results indicating patterns of statistical bias in the TRNG, suggesting that its randomness may not be entirely unpredictable. This is a critical finding, as a compromised TRNG could weaken the cryptographic security of DESFire EV1 credentials, potentially making authentication sequences more predictable and susceptible to attack.

While no follow-up research has been identified, this raises important questions about whether similar biases exist in newer iterations, such as DESFire EV3. Given the widespread adoption of DESFire EV3 for secure access control and payment systems, it would be prudent to re-evaluate its TRNG to ensure it meets modern security standards and does not introduce exploitable weaknesses.

The work by Labafniya [20] makes an intriguing claim, given that the authentication protocol is already documented in NXP's official documentation—though access is restricted under a Non-Disclosure Agreement. However, the context becomes clearer when considering that the research was conducted at the Research Center on Advanced Technologies in Tehran, Iran. This underscores the uneven global diffusion of advanced technologies, where access to proprietary security documentation may not be as readily available in certain regions, potentially driving independent reverse-engineering efforts.

There are also a number of papers that describe hardware and software that can be used to research the capabilities of DESFire. Schmidt [21] describes an open-source implementation of the DESFire specification that can be run on a Chameleon [22], an open-source RFID emulator and security research tool designed for testing and analysing contactless smart cards. Modification of such software could potentially be used to subvert a reader. Casanovas [23] approaches this slightly differently by integrating the emulation into an Android device. By integrating RFID emulation into such devices, researchers gain a portable, upgradable, cost-effective, and widely available security testing tool. This approach lowers barriers to studying and improving the security of access control systems, making it a highly practical innovation in RFID research.

This review of related work shows how research has focused on the various card technologies employed in an access control reader. The dismantling of both MIFARE Classic and iClass provides an insight into the process of how other cryptographically protected RFID smartcards may also be dismantled. Side-channel attacks also provide an avenue for further research that has yet to be explored. These works also highlight which technologies have no security (e.g. Mifare Classic) and do not merit further research, and those on which further research should be performed (e.g. DESFire) to assure or qualify the security of the technology. Where other forms of attack have been proposed and demonstrated, they have not been supported by the appropriate research document.

Methodology and scope of review

Overview of methodology

This paper adopts a structured technical review methodology to analyse contemporary enterprise access control readers and their associated technologies from a cybersecurity perspective. While the work does not constitute a formal systematic literature review, a transparent and reproducible process was followed to select representative devices, identify relevant technologies, and analyse their security implications.

The methodology consists of four stages. First, representative access control readers currently deployed in commercial and governmental environments were identified. Second, reader capabilities, interfaces, and supported technologies were extracted using publicly available manufacturer documentation. Third, credential, transmission, and interface technologies were reviewed against known vulnerabilities reported in peer-reviewed academic literature and relevant standards documentation. Finally, these findings were synthesized into a generic functional model of an access control reader and an attacker-oriented assessment framework.

This approach reflects the realities of access control research, where implementation details are often proprietary and empirical testing is constrained by legal, ethical, and operational considerations. The scope of this study is limited to enterprise-grade physical access control readers deployed in organizational, governmental, and critical infrastructure environments. The focus is on reader-level technologies and interfaces that influence the security posture of access control systems.

Devices were included in the review according to the following criteria:

- The reader is commercially available and actively supported by the manufacturer.
- The reader is intended for enterprise or institutional deployment rather than consumer or residential use.
- The reader supports credential-based authentication, including proximity, smart contactless, mobile, or biometric technologies.
- The reader provides wired communication with an ACU.

The following categories were explicitly excluded from the analysis:

- Consumer smart locks and residential access control products.
- Obsolete or discontinued devices no longer in active commercial deployment.
- Systems for which no publicly available technical or functional documentation exists.

This scoping strategy ensures that the analysis reflects realistic deployment scenarios and security risks encountered in operational access control systems, while maintaining a clear and reproducible boundary for device selection.

Device selection

This section describes how access control readers were selected within the scope and criteria defined in the section ‘Overview of methodology’, with the aim of capturing a representative cross-section of enterprise access control technologies rather than providing exhaustive market coverage.

Access control readers were selected to represent legacy, transitional, and contemporary deployments commonly found in commercial and governmental environments. Selection was guided by market influence, functional diversity, and prevalence in real-world systems. This approach ensures that the resulting analysis reflects realistic deployment scenarios and security risks faced by organizations operating access control systems.

The access control reader market has been dominated by HID Global for the last two decades, having shaped the adoption of proximity and, later, smart contactless technologies through its iCLASS product line. As a result, HID readers were included to represent market-leading deployments. To capture variation beyond the dominant vendor, alternative manufacturers were selected based on their presence in enterprise installations and their support for differing credential technologies, transmission protocols, and user interface features.

According to IPVM [24], a US-based product review and news platform focused on physical security systems, prominent alternatives to HID Global include Allegion/Schlage, Farpointe Data, WaveLynx, 3millID/Blue Diamond, and STid. Readers from these manufacturers were selected to provide diversity in supported credentials, communication methods, and form factors.

Manufacturer datasheets were used solely to identify supported technologies, interfaces, and functional capabilities of the selected readers. These sources were not used to infer security properties; instead, all security-relevant analysis was grounded in peer-reviewed academic literature, standards documentation, and publicly disclosed security research.

Data sheet review

In the following sections, readers have been selected from each of the manufacturers that demonstrate the breadth of capability in each of the product ranges. For each manufacturer, a brief company synopsis is provided followed by a feature list for each of the readers that have been selected. Finally, these feature lists shall then be collated into a feature summary.

HID Global

Although HID Global, introduced in Section ‘Related work’, were not the first to market, it rapidly became the leading supplier of proximity access control readers and has held that position for the last 20 years. HID was acquired by Assa Abbloy in 2000 and merged with Indala and Fargo Electronics in 2006 to form HID Global [25].

Given that HID Global are preeminent in the access control market, products from each of the three main eras of products shall be considered for analysis. These eras are:

- HID Proximity (1991 to 2002)
- HID iCLASS (2002 to 2020)
- HID Signo (2020 to present)

By examining the evolution of the HID Global product line, the major trends over the last 30 years can be observed.

Figure 2. HID Mini Prox Reader.

Figure 3. HID iCLASS SE R10.

HID proximity

The original proximity reader products are still available >30 years later [26]. The HID Mini Prox reader has been selected from this era for review. See Fig. 2.

The reader features the ability to read 125kHz HID Proximity (see the section '125kHz proximity technologies') credentials and output their data using the Wiegand (see the section 'Wiegand') or Clock and Data (see the section 'Clock and Data') protocols using two open-collector transistor drives to the ACU. The reader features a single LED that could be switched to off, red (indicating invalid, expired, or authorization for that entry point) or green (indicating valid, and the door or turnstile is unlocked for entry). By rapidly switching between the red and green states, it was also possible to present an amber state, indicating that the system is processing the credential, the reader is in standby mode, or there is an issue that requires attention.

HID iCLASS

In 2002, HID launched the iCLASS product range which is still available [27]. iCLASS was HID's first attempt at secure communication between the credential and the reader and was based on a technology called Picopass from Inside Contactless [28].

Figure 3 shows the HID iClass SE R10. The reader could read iClass credentials and transmit the data to an ACU using Wiegand or Clock and Data. Later variants of this product could also read 125kHz technologies and communicate securely using the Open Supervised Device Protocol (OSDP) over an RS-485 bus (see the section 'Open Supervised Device Protocol'). The reader also features an LED 'bar' at the top of the reader and a buzzer to indicate access has been granted.

As the market leader, HID Global have a scale that other reader manufacturers cannot match. This allows them to develop niche products to serve large scale projects. The HID iCLASS SE RMK40, shown in Fig. 4, is an example of one such product. This reader features a keypad, where data representing a key press is sent over the data lines. The reader also has the ability to read a magnetic stripe card and both HID Proximity and HID iCLASS credentials. Like the R10, this reader features an LED 'bar' at the top of the reader and a buzzer.

Figure 4. HID iCLASS SE RMK40.

Figure 5. HID iCLASS SE RKLB40.

Figure 5 shows the HID iCLASS SE RKLB40 combined iCLASS, keypad, and biometric reader. A biometric template is read from an iCLASS credential for verification using the fingerprint sensor incorporated in the reader. The standard reader transmits the credential data using the Wiegand or Clock and Data protocols. A plug-in module is also available to allow the reader to support the OSDP protocol. Another key feature of this reader is the text display. Like other readers in the iCLASS family, the reader features an LED 'bar' and a buzzer to interact with the user. As with the RMK40, a keypad is provided to transmit key data to the ACU when a key is pressed.

HID Signo

The current product line from HID Global is their Signo range of access control readers [29]. At the time of release, competing manufacturers were offering readers capable of reading a Bluetooth credential from a mobile phone as well a variety of smart contactless credentials, including DESFire and Mifare Classic. Many are also capable of reading various 125kHz technologies. The release of the Signo range of readers allowed HID to offer a range of multi-technology readers that could work with any HID credential from the previous 30 years. The HID Signo 20K reader is shown in Fig. 6 and also features a keypad, an LED 'bar' and a buzzer.

The HID Signo 25B reader, shown in Fig. 7, is an integrated fingerprint and smart contactless reader for template-on-card applications or against a database of biometric templates held within the reader. Communication to the access control panel is via OSDP. The reader features an LED 'bar' and a buzzer for interaction with the user.

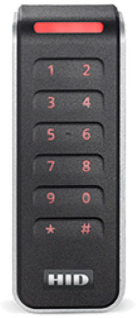


Figure 6. HID Signo 20K Reader.

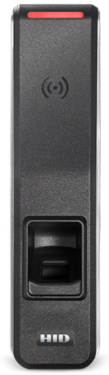


Figure 7. HID Signo Biometric Reader 25B.

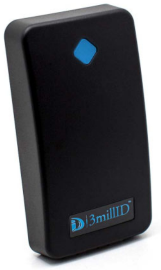


Figure 8. 3millID 3MIL-R11330.

3millID/Blue Diamond

Founded in 2015, 3millID Corporation is based in Colorado. Like many competitors to HID Global, 3millID has focused on high-running products: a mullion reader (see Fig. 8), which is a narrow, vertically oriented access control reader designed to be mounted on a doorframe (mullion) or other slim surfaces where space is limited, a sing-gang reader that is designed to fit into a standard single-gang electrical box, which is a common size for wall-mounted electrical and security devices, and a keypad reader (see Fig. 9).

The readers can read Bluetooth, smart contactless, and 125kHz credentials [30]. Credential data may be transmitted via Wiegand, Clock and Data, or OSDP. The keypad version of the reader sends data to the ACU when a key is pressed and the reader has an LED and buzzer for interaction with the user. The company has also licensed the product range to market-leader, LenelS2, where the readers are sold under the Blue Diamond brand [31].

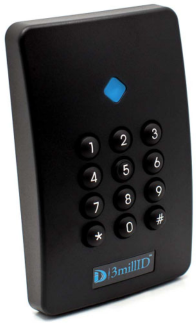


Figure 9. 3millID 3MIL-R11325.

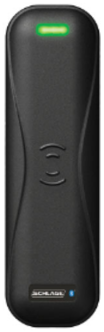


Figure 10. Allegion/Schlage MTB11.

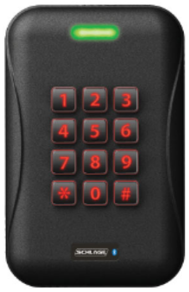


Figure 11. Allegion/Schlage MTKB15.

Allegion

Allegion spun off from Ingersoll-Rand in 2013 [32]. Figures 10 and 11 show two of the five readers in the Allegion reader lineup.

According to the product information [33], the readers support a variety of smart contactless and 125kHz technologies. The standard readers support the Wiegand and Clock and Data protocols for transmission of credential data to the ACU. OSDP is available as a separate variant of these readers.

Farpointe Data

Farpointe Data [34] was founded in California in 2003. They manufacture a range of access control readers. Figure 12 shows one of their original access control readers. The reader only supports 125kHz credentials and transmits the credential data using the Wiegand or Clock and Data protocols. The reader has an LED and a buzzer to interact with the user [35].

Figure 12. Farpointe Data P500.

Figure 13. Farpointe Data CSR-6.4L.

Figure 14. STid ARC16/BT Easyline.

Figure 13 shows one of the latest products from the company, the CSR-6.4L Conekt reader. The reader supports smart contactless and Bluetooth credentials. Data may be sent to an ACU using one of the Wiegand, Clock and Data, or OSDP protocols. The reader features a keypad, transmitting key data over the selected protocol when a key is pressed. The reader also features an LED and buzzer to interact with the user [36].

STid

Based in France, STid was founded in 1996. Two products have been selected for this review, the STid ARC16/BT Easyline [37] and the ARCS-B/BT Easyline [38] access control readers shown in Figs. 14 and 15. Both readers support smart contactless and Bluetooth credentials. Credential data may be transmitted using one Wiegand, Clock and Data, OSDP, or Smart and Secure Communication Protocol (SSCP) (see the section 'Smart and Secure Communication Protocol') protocols. Both readers also have an LED and buzzer for user interaction.

The ARCS-B/BT Easyline reader also has a keypad and key data is transmitted over the selected interface when a key is pressed.

Figure 15. STid ARCS-B/BT Easyline.

Figure 16. WaveLynx ET-10.

Figure 17. WaveLynx ET-25.

WaveLynx

The final manufacturer whose products are under consideration is WaveLynx [39]. Founded in 2012, WaveLynx is also based in Colorado. The selected readers are the ET10 (see Fig. 16) and ET25 (see Fig. 17) [40]. These readers support 125kHz and smart contactless credentials as well as Bluetooth. Credential data may be transmitted using the Wiegand, Clock and Data, and OSDP protocols. Both readers have an LED 'bar' and a buzzer to attract the user's attention.

Additionally, the ET25 reader also has a keypad and key data are transmitted over the selected interface when a key is pressed.

Feature summary

Table 1 provides a comparative overview of various access control readers, highlighting their credential technologies, transmission methods, and user interface features. The credential technologies include Bluetooth, Smart Contactless, and 125kHz proximity cards, with some readers supporting multiple methods. For example, the HID Signo 20K Reader and 3millID 3MIL-R11325 support all three, whereas others, like the HID iCLASS SE RKLB40, only support SC. Some readers also integrate additional authentication

Table 1 Summary of access control reader features.

	Credential Technology				Transmission				UI			
Reader	**BT**	**SC**	**125**	**Other**	**W**	**C**	**O**	**S**	**L**	**B**	**T**	**K**
HID Mini Prox			Y		Y	Y			Y	Y		
HID iCLASS SE R10		Y			Y	Y			Y	Y		
HID iCLASS SE RMK40		Y	Y	Magnetic Stripe					Y	Y		Y
HID iCLASS SE RKLB40		Y		Fingerprint					Y	Y	Y	
HID Signo 20K Reader	Y	Y	Y						Y	Y		Y
HID Signo Biometric Reader 25B	Y	Y		Fingerprint	Y		Y		Y	Y		
3millID 3MIL-R11330	Y	Y	Y		Y	Y	Y		Y	Y		
3millID 3MIL-R11325	Y	Y	Y		Y	Y	Y		Y	Y		Y
Allegion/Schlage MTB11		Y	Y		Y	Y	Y		Y	Y		
Allegion/Schlage MTKB15		Y	Y		Y	Y	Y		Y	Y		Y
Farpointe Data P500			Y		Y	Y			Y	Y		
Farpointe Data CSR-6.4L	Y	Y			Y	Y	Y		Y	Y		Y
STid ARC16/BT Easyline	Y	Y			Y	Y	Y	Y	Y	Y		
STid ARCS-B/BT Easyline	Y	Y			Y	Y	Y	Y	Y	Y		Y
WaveLynx ET-10	Y	Y	Y		Y		Y		Y	Y		
WaveLynx ET-25	Y	Y	Y		Y		Y		Y	Y		Y

Credential Technologies: BT: Bluetooth, SC: Smart Contactless, 125: 125 kHz. Transmission Methods: W: Wiegand, C: Clock and Data, O: OSDP, S: SSCP. User Interface (UI): L: LED, B: Buzzer/Speaker, T: Text Display, K: Keypad.

methods such as fingerprint scanning, as seen in the HID iCLASS SE RKLB40 and HID Signo Biometric Reader 25B. In terms of transmission methods, most readers support Wiegand and Clock and Data, while fewer implement more advanced protocols like OSDP and SSCP, with the STid ARC16/BT Easyline and STid ARCS-B/BT Easyline standing out for their full range of transmission options. User interface features vary across devices, with LED and buzzer feedback being common, but text displays and keypads appear less frequently, suggesting that some readers focus on enhanced user interaction, such as the HID iCLASS SE RMK40 and STid ARCS-B/BT Easyline. Overall, the comparison highlights the diversity of access control readers in terms of compatibility, security features, and user interface, catering to different access control requirements.

Technology and cybersecurity review

In this section, an introduction to each of the technologies that are incorporated into a reader is provided along with known vulnerabilities. This review catalogues the cybersecurity landscape of an access control reader.

Credential technologies

One purpose of an access control reader is to read a payload from a credential. In this section, the three main groups of credentials identified in the section 'Data sheet review' are considered along with the other technologies included in the readers that were reviewed.

125kHz proximity technologies

125kHz card technologies have been used in access control applications since the 1980s. The transponders use a backscatter modulation to send a number repeatedly to a reader whilst the transponder is in the field of the reader. Three different types of modulation are used by various transponders: Amplitude Shift Keying, Frequency Shift Keying, and Phase Shift Keying. Once the data from the transponder has been demodulated, a recurring bit pattern is observed. The bit pattern generally contains framing bits to delineate data, parity bits, or check characters to assure the integrity of the data and the data itself. Once the layout of the data is understood, it is a trivial process to extract the card number. Common 125kHz technologies include transponders from HID, Indala, AWID, Farpointe Data, Kantec, and EM Marin.

In 2007, Seattle-based security research company IOActive demonstrated vulnerabilities in HID's 125kHz proximity card technology, highlighting the potential for unauthorized cloning and access [41]. Over time, more and more details of commercial 125kHz implementation came into the public domain and were published on proxmark.org [3]. A summary of what was known in 2013 can be found on the website. Coupled with experience and access to related materials, an engineering team can quickly construct the equipment to read and create 125kHz proximity cards based on the information provided.

To assess the cybersecurity landscape of 125kHz credentials, it can be viewed through the lenses of confidentiality, integrity, and availability:

- Confidentiality: The credential is encoded into a frame of bits and transmitted repeatedly for demodulation by the access control reader. The data is sent in plain text and can be readily extracted from the data frame. There is, therefore, no confidentiality provided by the transponders in the 125kHz family.
- Integrity: Parity bits and/or check characters are used in the data transmitted from a 125kHz transponder and demodulated by an access control reader. These are only sufficient to identify that the data has been successfully decoded from the data frame.

- Availability: A denial-of-service (DoS) attack can be mounted on a reader configured to read 125kHz credentials by mounting a transponder close to the reader. The reader will continually read this transponder and if another transponder is brought into the reader field, it will not be reported by the reader as it will be unable to demodulate the data.

Given that the widely used 125kHz credentials have no cryptographic protection, are easily cloned and that there is a widespread move to migrate to 'more secure' smart contactless credentials, it is argued that further research into the 125kHz family of technologies would not make a beneficial contribution.

Smart contactless technologies

Smart contactless transponders typically run at 13.56MHz, and like the 125kHz transponder family, use backscatter modulation to communicate with an access control reader. These transponders feature various cryptographic protections and mutual authentication to establish communication between a transponder and an access control reader.

In this section, six common smart contactless transponders supported by the sample set of readers discussed in Section 'Device selection' are considered in chronological order. In each case, a brief history is presented and the current state of security research is considered.

LEGIC Prime: In 1992, LEGIC Identsystems was the first company to present contactless smartcard technology operating at 13.56 MHz using their proprietary protocol between the card and reader. In order to read and write to the cards, a LEGIC Security Module is also required and is driven using a serial protocol.

In 2011, Plötz [12] describes how 'the security of the tags is based on several secret checksums but no secret keys are employed that could lead to inherent security on the cards'. LEGIC Prime transponders can be read, written and spoofed with an emulator. This outcome demonstrates that LEGIC Prime is not a viable avenue of academic research. Indeed, LEGIC introduced an upgraded technology called LEGIC Advant based on ISO standards in 2003.

NXP Mifare Classic: The first Mifare Classic card was introduced by Philips (now NXP) in 1994 and gained widespread use in ticketing applications across the globe as well as being deployed in access control solutions. The technology allows up to 1K byte to be stored on the card and access to this data via a key and an NXP proprietary protocol called Crypto1. Due to the widespread use of this technology, Mifare Classic attracted a lot of attention from security researchers and hackers.

At the 24th Chaos Communication Club, Nohl and Plötz presented how they had reverse-engineered the proprietary Crypto1 cipher [7] in a MIFARE Classic card. This presentation was followed up by a paper in 2008 [42]. Garcia and Jacobs [13] describe the work that ensued, leading to practical attacks on MIFARE Classic transponders. Armed with a Proxmark-3, it is possible to extract the keys from the first generation of Mifare Classic cards.

HID iClass: In the late 1990s, HID started developing its first smart contactless transponder technology: iCLASS. Based on the Picopass transponder chip from Inside Contactless [28], HID launched iCLASS readers and transponders in 2002. The iCLASS product range quickly became the de facto access control product for large enterprises and, consequently, attracted a lot of interest from the security research community.

The dismantling of iCLASS starts with Meriac's 'Heart of Darkness' paper [6] in which a design flaw is used to extract the firmware from an HID iCLASS reader/writer to reconstruct the methods used to read and write iCLASS cards. Further contributions from Garcia et al. [5,14,15] and Kim et al. [16] allowed researchers to read and write HID iCLASS cards.

One of the flaws of the original iCLASS transponders is that they rely on a fixed master key that is used to derive the key for a particular card. Once this key has been obtained, the cards are open. HID established an Elite programme where a different key is programmed into the reader and the cards in the system. Attacks are still possible on Elite keyed readers and cards [14]. Latterly, HID introduced iCLASS SE which programs a Secure Identity Object (SIO) onto an iCLASS card and other types of credentials. The SIO introduced another layer of defence to the readers and cards against possible attacks.

NXP Mifare DESFire: The first Mifare DESFire transponder, the MF3ICD40, was introduced in 2002. This transponder offers a flexible directory and file system and features Triple DES encryption for communication between the reader and transponder and encryption of file data. By 2011, Oswald and Paar [18] had published a paper describing a practical side-channel attack to recover the 3DES key from an MF3ICD40 transponder.

In 2008, NXP introduced the DESFire EV1 range of transponders with 2k, 4k, and 8k byte memories. AES encryption was added as well as Common Criteria certification. Following the work of Oswald and Paar [18], NXP acknowledged [43] the vulnerability and encouraged their users to migrate to DESFire EV1 having determined that these transponders were not susceptible to these types of side-channel attacks. Further features were added to the DESFire line with the introduction of DESFire EV2 in 2016 and DESFire EV3 in 2020. At the time of writing (January 2024), there are no published attacks on these families of transponders.

LEGIC Advant: Based on ISO standards, specifically ISO14443 and ISO15693, the first LEGIC Advant transponders were introduced in 2003. As with LEGIC Prime, a proprietary reader module from LEGIC is required to read and write these transponders. Over time a number of new versions of LEGIC Advant transponders have been introduced leading up to the current range [44].

HID SEOS: HID Global introduced SEOS in 2018 as a replacement for the iCLASS and iCLASS SE transponders. The cards use ISO14443A for communication between the transponder and a reader and a collection of other relevant standards [45]. There is, however, no detailed technical specification with regard to the protocol between the transponder and a reader. This is a closed system. HID Global claim [46] that SEOS 'offers the first and only physical access control card to ever have been certified by an independent security laboratory' through the TÜViT SEAL-5 accreditation [47]. At the time of writing (January 2024), there are no published attacks on the SEOS family of transponders.

In summary, smart contactless credentials are more vulnerable the older they are. However, to mitigate such vulnerabilities, the following techniques are considered:

- Confidentiality: Access to a smart contactless transponder typically requires a shared key between the reader and the transponder and some form of mutual authentication. The type of cryptographic algorithm and key length varies for each of the transponder families that have been identified. Confidentiality is provided by these cryptographic methods.

- Integrity: The integrity of the data transfer between a reader and transponder is supported in ISO14443-3 [48] through the use of parity bits. Transponders that use ISO14443-4 (DESFire, some LEGIC Advant) benefit from the integrity checks provided by the half duplex block protocol. Other protocols built on top of ISO14443-3 provide their block-based integrity checks. It is argued that sufficient integrity checks are provided given the amount of data flowing between the transponder and the reader.
- Availability: Credentials based on ISO 14443 and ISO15693 [49] benefit from a feature called anticollision. Unlike 125kHz transponders, this allows a reader to identify and communicate with multiple transponders in the field of the reader. Availability is therefore better than for 125kHz transponders.

Mobile credential technologies

Mobile credentials are stored securely on a phone and transmitted to a reader using one of two technologies:

- Near Field Communication (NFC): The use of NFC to transmit a credential to a reader is very similar to the method used by a wide variety of smart contactless credentials (i.e. those using ISO14443). The phone needs to be presented within 10cm of the reader. Combined with a technology called Host Card Emulation, a mobile phone essentially mimics a DESFire or similar credential. This approach is the most obvious use case for access control as there is very little change from using a smart contactless card with a reader, something a user would already be familiar with. NFC became the technology on which the Google Pay and Apple Pay solutions have been built. Samsung launched the first Android phone featuring NFC in 2010 [50] and supported in the Gingerbread version of the Android operating system [51].
- Bluetooth Low Energy (BLE): A specification for BLE also marketed as Bluetooth Smart, was first incorporated into Version 4.0 of the Bluetooth core specification in 2010 [52]. In 2011, the iPhone 4S was launched and was the first mobile phone to incorporate the technology [53]. The benefits of BLE are a low power requirement, small physical footprint, low cost, and compatibility with a wide range of mobile phones. These attributes make it ideal for access control readers and the transmission of a mobile credential from a phone.

Unikey, based in Orlando, is widely credited with developing the first mobile credential solution for access control in 2012 when they presented their technology on the US television show Shark Tank [54]. The technology was first brought to market following a licensing deal with Kwikset in 2013 [55]. This solution was aimed at the residential market and stored a mobile credential on an iPhone, which was sent to the lock using Bluetooth.

HID Global launched their Mobile Access solution in 2014 [56] with support for both Bluetooth and NFC credentials. 'Twist and go' gesture technology was used to allow the user to unlock a door and HID Global claimed that the technology 'has been successfully piloted at major universities and businesses in the USA, signals the start of a new era in security solutions'. Despite the optimism around the adoption of mobile credentials in 2014, there have been a number of obstacles to the adoption of mobile credential technology.

The first obstacle has been the reluctance of Apple to open up NFC to its developers. The Apple ecosystem is a closed ecosystem. Steve Jobs was always unapologetic about this approach [57], which 'is to tightly control how everything integrates from the chips to the software to the industrial design'. Whilst Apple was quick to incorporate BLE into their product line in 2011 [53], they waited until 2014 to incorporate NFC hardware into the iPhone 6 to allow for contactless payments using Apple Pay [58]. With subsequent iOS releases, Apple has opened up some NFC functionality but the implementation is far from open. Instead, Apple has focused on the commercial opportunities offered by Apple Pay and Apple Wallet. In 2019, Apple pushed forward with the deployment of access control and other applications based on NFC for students [59]. In early 2022, HID deployed the first enterprise access control reader solution based on Apple Wallet to Silverstein Properties, World Trade Center 7, New York [60,61]. Whilst this progress has been encouraging, Apple continue to tightly control access to its technology.

The 'Bring Your Own Device' scenario, also known as BYOD, refers to a situation where the user's mobile phone is used to carry the credential. Organizations face the challenge of assuring their information security on devices they do not directly control. Users face the risk of a loss of privacy by installing an application on behalf of their employer [62]. This conflict is another obstacle to the deployment of mobile credentials.

The final obstacle is cost. Mobile credentials are generally sold using a Software-as-a-Service model which involves an annual fee for the credential and possibly an annual service cost in addition. Physical credentials are a fixed cost per credential and can last many years if not abused by the user. The total cost of ownership for a physical credential against a mobile credential is generally lower in the current market.

Despite these obstacles, there has been a proliferation of mobile credential solutions as demonstrated by the five manufacturers supporting mobile credentials in the access control readers that have been sampled for this research. Beyond claiming support for mobile credentials in their product literature, none of these manufacturers publish any technical detail on their mobile credential implementations. It has been established, however, that 3millID uses the Supra technology from a sister company to LenelS2 [63] and that Farpointe Data use the LEGIC Connect technology from their sister company LEGIC [64].

The cybersecurity landscape of mobile credentials can be viewed through the lenses of confidentiality, integrity, and availability. For mobile credentials communicated using NFC, the commentary regarding confidentiality, integrity, and availability is the same as for smart contactless credentials (see Section '125kHz proximity technologies'). For mobile credentials communicated using Bluetooth, the commentary is as follows:

- Confidentiality: All manufacturers claim encryption for the information passed between a mobile phone and an access control reader. Through this mechanism, confidentiality is assumed to be assured.
- Integrity: The integrity of the messaging between the mobile phone and the access control reader is assured by the BLE Link Layer.
- Availability: The availability of mobile credentials depends on the communication hierarchy between the mobile phone and the access control reader, specifically whether one acts as the

master and the other as the slave. A slave device can only communicate with one master at a time. If the mobile phone is the master and the access control reader is the slave, then only one mobile credential can be processed at a time. However, if the roles are reversed and the reader acts as the master, it can interact with multiple mobile credentials simultaneously. Javadi et al. [65] explore this further by demonstrating a DoS attack on HID BLE readers, highlighting potential vulnerabilities in mobile credential access control systems.

To summarize, mobile credentials are the latest innovation in access control credential technology. Much of the implementation detail is hidden from view and the various manufacturers and products provide a rich seam of potential research activity.

Other credential technologies

As part of the product review, additional credential technologies were identified, including magnetic stripe card* and biometric authentication methods such as fingerprint recognition. While these technologies are widely used in access control systems, they present unique security considerations and implementation challenges.

Magnetic stripe technology, once a dominant form of access credential, is now considered highly insecure due to its lack of encryption and the ease with which it can be copied or cloned. Using readily available skimming devices, an attacker can extract the credential data from a magnetic stripe card and replicate it onto a blank car*, granting unauthorized access. Given these vulnerabilities, many organizations have migrated away from magnetic stripe access control systems in favour of more secure alternatives, such as smartcards, mobile credentials, and encrypted RFID-based solutions.

Biometric authentication, particularly fingerprint recognition, represents a different category of access control credentials. Unlike magnetic stripe or RFID cards, biometrics rely on physiological characteristics that are unique to an individual. While this offers a high level of security and non-repudiation, biometric access control is a specialized field with distinct challenges, including privacy concerns, template storage security, and potential spoofing attacks (e.g., presentation attacks using synthetic fingerprints).

Given the specialized nature of biometric security and its unique technical and ethical considerations, this study does not explore biometric access control systems in detail. Instead, the focus remains on traditional credential-based access control technologies, where vulnerabilities such as credential cloning, relay attacks, and cryptographic weaknesses play a significant role in security research and threat modelling.

Transmission methods

Wiegand

The Wiegand transmission protocol is the most widely used method of communication between a reader and an ACU. Wehr [66] describes how the Wiegand effect was applied to card technology. The readers for these cards had what became known as a Wiegand output and this became the most common transmission output for access control readers over the last four decades. The Security Industry Association (SIA) published a standard for the protocol in 1991 [67].

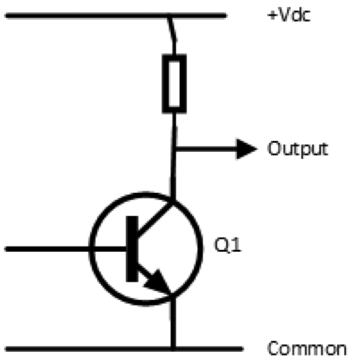


Figure 18. Open collector output used by an access control reader.

In the original Wiegand reader, manufactured by Sensor Engineering, the respective outputs are driven low by two open-collector outputs (shown in Fig. 18) as the wires in the Wiegand strip are passed over the Wiegand-effect sensors in the read head. A resistor is shown in the circuit; it is common practice to include a weak pull-up in the output circuit of an access control reader to mitigate any interfacing issues with some equipment.

Access control readers adopted this method in the 1980s to transmit bit streams read from other card technologies such as, most notably, proximity cards. Unlike a real Wiegand reader, these ‘Wiegand emulation’ readers used a fixed timing for the output as shown in Fig. 19. Individual bits are typically spaced 1 millisecond apart with either the Data 0 (D0) or Data 1 (D1) outputs being driven low for between 50 and 100 microseconds.

Sensor Engineering also created what became a standard bit format for the transmission of card data: the Sensor 26-bit format, more simply known as ‘26-bit’. This is an example of the term ‘Wiegand’ used to describe ‘the standard 26-bit binary card data format’.

This format is described in Fig. 20. Cardholders are identified ‘uniquely’ by a facility code and a card number. Some degree of integrity is provided to the format by the inclusion of two parity bits.

Figure 21 presents an example of a Sensor 26-bit data frame programmed for facility code 99 and card number 1001.

As the industry grew, the Sensor 26-bit format presented two principal problems: the range of facility codes and card numbers is limited, and credential vendors would and still do, accept an order for cards with a specified facility code and card number without any check that the numbers have already been issued. To combat these two issues, custom vendor formats proliferated in an attempt to create security by obscurity.

To assess the cybersecurity landscape of Wiegand, it can be viewed through the lenses of confidentiality, integrity, and availability:

- Confidentiality: Wiegand was never designed for secure data transmission. All data is sent as plain text and can be easily skimmed, as is shown below. The confidentiality of Wiegand is, therefore, non-existent.
- Integrity: As demonstrated in the construction of the Sensor 26-bit format, parity bits are added to the frame to allow the receiver to detect bit transmission errors. This scheme is of minimal benefit as two changed bits within one of the parity fields will result in the reception of the wrong card number at the

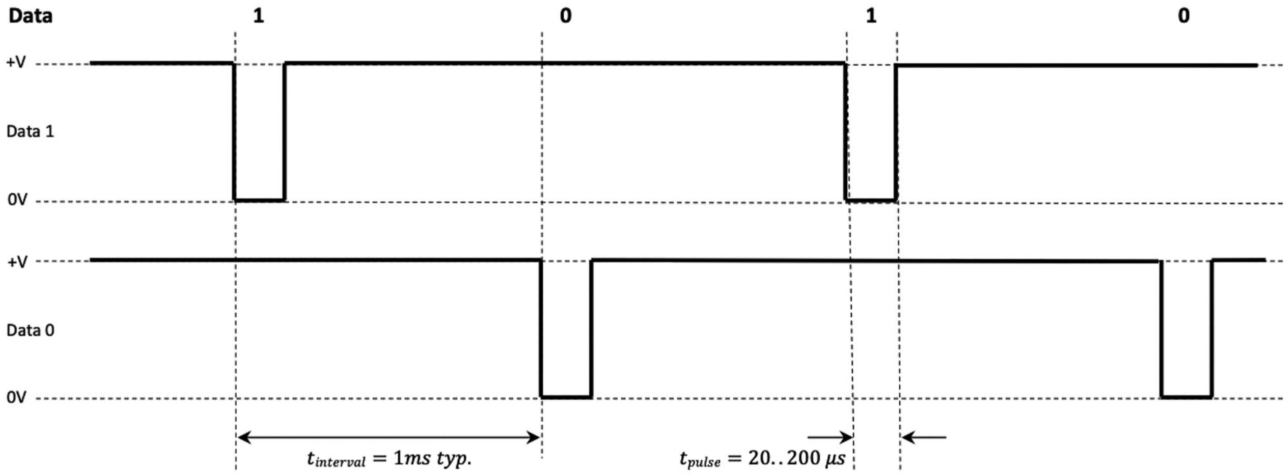
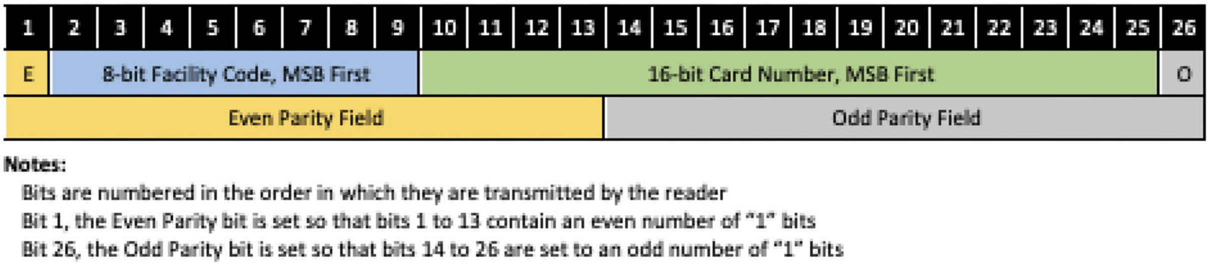


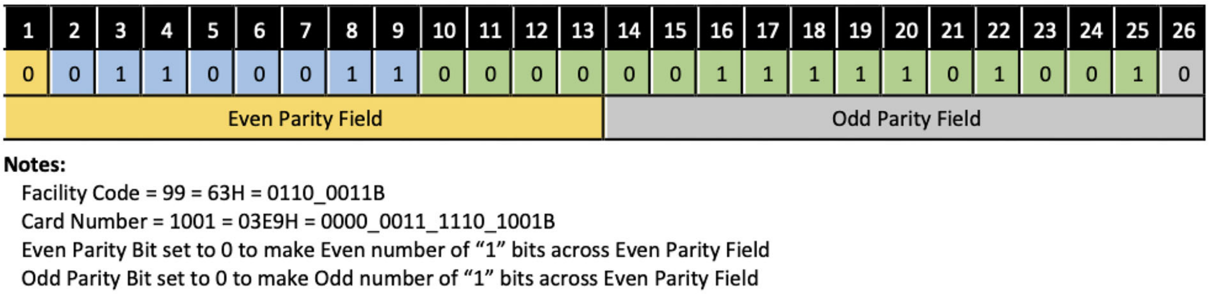
Figure 19. Timing diagram for the Wiegand protocol.



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
E	8-bit Facility Code, MSB First								16-bit Card Number, MSB First																O
Even Parity Field													Odd Parity Field												

Notes:
Bits are numbered in the order in which they are transmitted by the reader
Bit 1, the Even Parity bit is set so that bits 1 to 13 contain an even number of "1" bits
Bit 26, the Odd Parity bit is set so that bits 14 to 26 are set to an odd number of "1" bits

Figure 20. The Sensor 26-Bit Wiegand format.



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	1	0	0	1	0
Even Parity Field													Odd Parity Field												

Notes:
Facility Code = 99 = 63H = 0110_0011B
Card Number = 1001 = 03E9H = 0000_0011_1110_1001B
Even Parity Bit set to 0 to make Even number of "1" bits across Even Parity Field
Odd Parity Bit set to 0 to make Odd number of "1" bits across Even Parity Field

Figure 21. An example of the Sensor 26-Bit Wiegand format.

ACU. It is argued that this does not stand up to the integrity requirements of a modern information system. The integrity of Wiegand-formatted data is, therefore, minimal.

- Availability: To deny service to the Wiegand transmission path, you need to remove the reader from the wall and interfere with the wiring. Shorting the data lines has the benefit of the reader appearing to work while sending gibberish to the ACU. The availability of Wiegand is, therefore, adequate. The assurance of availability can be improved by implementing and monitoring the tamper function if the reader supports it.

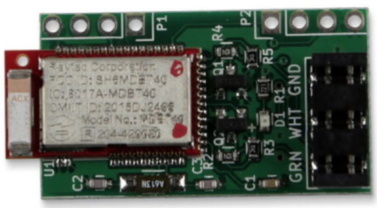


Figure 22. BLE Key, a Wiegand skimming device.

It is presumed that an open collector output was originally chosen for its ability to drive data over a distance of 150 m (the typical cable distance supported by Wiegand output readers) reliably and cheaply. The open collector outputs of a Wiegand reader also allow readers to be wired in parallel so that an ACU can receive data from more than one reader on the same port. This opens the opportunity to skim the data transmitted and replay it to the ACU at a later date.

For $35.00, a device known as a 'BLE Key' [68] (Fig. 22) may be purchased. Installed covertly, this device captures and stores

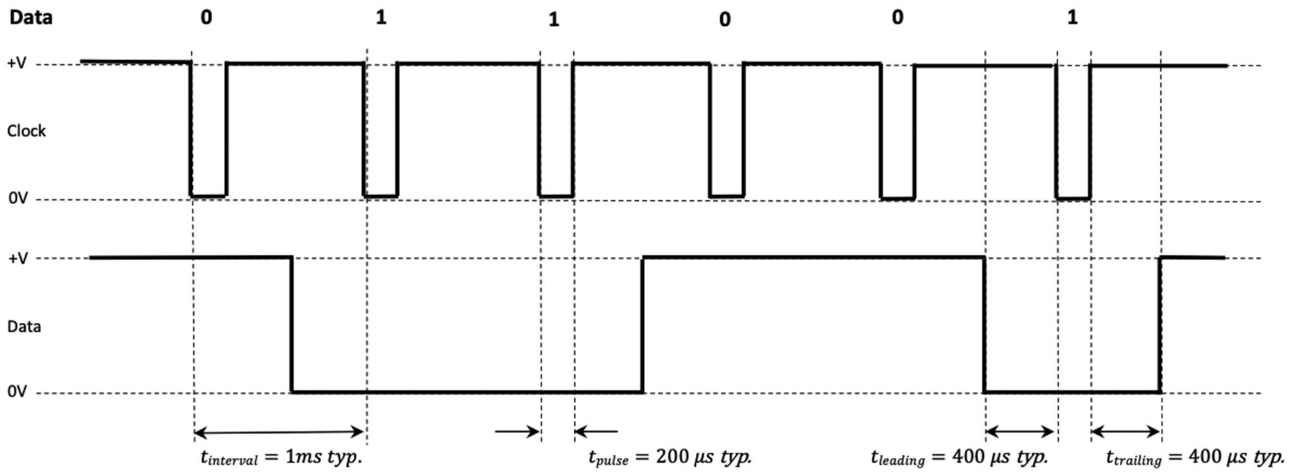

Data
0
1
1
0
0
1
+V
Clock
0V
+V
Data
0V
$t_{interval} = 1ms\ typ.$
$t_{pulse} = 200\ \mu s\ typ.$
$t_{leading} = 400\ \mu s\ typ.$
$t_{trailing} = 400\ \mu s\ typ.$

Figure 23. Timing diagram for the Clock and Data protocol.

Wiegand frames to be replayed to the access control system using a mobile phone via the device's Bluetooth connectivity. This device was presented at the Blackhat USA Conference in 2015 [4] and demonstrates how easy it is to use a replay attack on Wiegand systems.

Clock and Data

Clock and Data is another common transmission method for access control readers and, like Wiegand, utilizes the open collector output shown in Fig. 18. The format of the data transmission is described in Fig. 23. As with Wiegand, data may be easily skimmed and replayed to the ACU.

Open Supervised Device Protocol

The OSDP has its origins at Mercury Security in the early 2000s [69] and its early development was led by Frank Gasztonyi, President of the company. Mercury was one of the success stories of the industry as a developer and manufacturer of ACUs that they sold to access control OEMs who delivered the complete system solution. Rather than mandated by the US government, the protocol was developed by security equipment manufacturers in response to customer demands.

As a result of their success, Mercury was asked to integrate a myriad of devices with their control panels and started to develop a standardized way of approaching the problem to share the load with the peripheral vendors leading to an initial specification in 2007. This version of the specification is commonly referred to as OSDP Version 1 and implements common functions such as LED and buzzer control. It lacked, however, any form of secure channel between the control panel (or ACU) and the peripheral device (a generic term that encompasses access control readers).

By 2009, a means to secure communication between the control panel and peripheral devices had been chosen. This heralded what the industry refers to as OSDP Version 2. This version of the specification was developed over the next 5 years by Mercury and its industry partners, including HID.

From the outset, Mercury recognized that to have lasting success, any specification that they developed with their industry partners would have to be handed to an industry body to steward, foster, and promote the standard to access control vendors. In 2016, the OSDP specification was passed to the SIA [70].

One of the key contributions of SIA was establishing the OSDP Working Group that meets regularly to discuss various aspects of the OSDP standard including the proposal of new features. The objective of SIA was to get the OSDP adopted as an American (ANSI) or international standard (ISO/IEC). The endeavours of SIA and the OSDP Working Group led to this goal being achieved in 2020 with the adoption of OSDP Version 2.2. as IEC 60839-11-5:2020.

The key benefits of OSDP can be compared and contrasted to the features of the Wiegand protocol:

Secure Channel: Secure channel has been the main motivating factor for the adoption of OSDP over Wiegand by manufacturers, integrators and end users alike. Wiegand transmits data as plain text. OSDP has the option of establishing a secure channel between the ACU and the peripheral device. The security of the communication is based on an AES-128 session key and the application of CMAC chaining.

Constant Device Monitoring: Continuous monitoring of devices is possible with OSDP because the peripheral devices are constantly polled for events and status. This is why 'Supervised' is used in the name of the protocol. If the device detects that it is under attack (i.e. in a tamper condition), it can be immediately reported to the ACU.

Support New Device Technologies: The early 2000s saw advances in biometric and smart card technologies and the integration requirements for an access control system. Biometric devices and smart card readers are both supported by appropriate protocol commands.

File Transfer: At one time, if a manufacturer-specific operation on a peripheral device was required, a series of manufacturer-specific commands had to be defined and sent to the peripheral device. While this is a viable approach for the peripheral device manufacturer, it is not practical for every ACU manufacturer to implement support for a plethora of manufacturer-specific commands and use cases. The OSDP file transfer command was devised to avoid this problem. An opaque file that has no meaning to the ACU, is sent to a peripheral device. The peripheral device makes sure it is the intended recipient before processing the file.

OSDP is now widely specified as the best practice for access control systems by security consultants. There has been a major educational push by consultants, equipment manufacturers, and the trade press about the vulnerabilities of Wiegand and the benefits of OSDP. This has led to widespread adoption of at least the secure channel benefit of the protocol by [63] both reader and ACU manufacturers.

However, with widespread adoption, manufacturers have been found to be implementing the protocol in subtly different ways that have led to interoperability problems. To address this concern, SIA has recently introduced the OSDP-Verified programme [71]. Access control equipment manufacturers submit their equipment for compliance and interoperability testing and, subject to passing these tests, the relevant products achieve OSDP Verified certification.

To assess the cybersecurity landscape of OSDP, like Wiegand, it can be viewed through the lenses of confidentiality, integrity, and availability:

- Confidentiality: OSDP provides a Secure Channel operating mode that encrypts the communication between the reader and the ACU. When, and only when, this mode is used is the confidentiality of data provided by the protocol.
- Integrity: OSDP provides a message authentication code (MAC) mechanism to assure the integrity of a message. A MAC can be applied to a plain text message and is mandatory for secure channel messaging.
- Availability: Similarly to Wiegand, service can be denied to an OSDP bus by removing the reader from the wall and interfering with the wiring. Shorting the data lines, in this case, will result in all the readers going offline and alerting the operators of the system. Users will not be able to gain access to the affected doors. Assurance of availability can be further improved by implementing and monitoring the tamper function if the reader supports it.

Smart and Secure Communication Protocol

One of the manufacturers under review, STid, uses a protocol called SSCP [72]. SSCP is promoted by the Smart Physical Access Control (SPAC) Alliance as a new European standard that guarantees interoperability, without compromising security. The protocol specification is available for purchase from the SPAC website. The specification is provided on a confidential basis, which precludes publishing research that breaches this confidentiality. SSCP was originally developed by STid.

Nevertheless, it can be reported that the protocol has a number of similarities to OSDP. The protocol runs on an RS-485 bus, although it can also run on other media. The protocol has a secure communication capability based on mutual authentication and AES128 cryptography. Frame integrity is maintained by the use of a key-hash message authentication code (HMAC). Unlike OSDP, the protocol commands largely map to the functions supported by various NXP transponders, described in the corresponding confidential NXP documents.

Considering SSCP in the context of the confidentiality, integrity, and availability triad:

- Confidentiality: SSCP provides a secure communication channel that encrypts the communication between the reader and the ACU, thus assuring the confidentiality of data sent over the protocol.
- Integrity: SSCP provides a HMAC mechanism to assure the integrity of messages sent over the protocol.
- Availability: Service can be denied to an SSCP bus by removing the reader from the wall and interfering with the wiring. Shorting the data lines, in this case, will result in all the readers going offline and alerting the operators of the system.

User interface technologies

Whilst not having an obvious cybersecurity implication, the user interface is an important feature of an access control reader. An access control reader typically has one or two LEDs, a speaker or buzzer, and often a keypad. As seen in the sample set of readers, a text display may also be present. Most readers also have some form of anti-tamper mechanism.

LED

The complexity of LED configuration has increased over time as new types of LED have been introduced to the market. In the beginning, LEDs were either red or green. Then there were bicolour LEDs that could switch between off, red, green, and even yellow. Next came RGB LEDs that are widely used in the most recent designs that allow almost any colour to be displayed by the reader.

Whilst there is no obvious cybersecurity implication, LEDs are often used to indicate the status of a door by the access control system. Red often typically means access denied. Green often means access granted. Yellow often may mean entering your PIN. Some readers, when losing communication with the ACU, may go into a diagnostic mode to alert users that there is a problem. This can also be useful information to an attacker.

Buzzer/Speaker

Readers usually have a buzzer or speaker to give an audible indication when a card is read. Buzzers emit a single-frequency tone. Speakers are more flexible and can be used to provide additional feedback to the user by playing a tune. Like the LEDs, there may be tones from a reader that may provide information of interest to an attacker.

Text display

Text displays are less common among access control readers and are usually LCD displays with 2 or 4 lines of text. LED/LCD displays are also starting to be used which can display full-colour graphics. As with LEDs and buzzers or speakers, status information could potentially be displayed that may be of interest to an attacker.

Keypad

A keypad is provided when a user is required to enter a PIN corresponding to their credential as a second factor. Access control readers often provide configuration functions through the keypad. This process usually involves ‘logging on’ to the reader by entering a special key sequence including a maintenance PIN. Maintenance PINs might be left in a default state allowing an attacker a means to change the configuration of the reader.

Certain readers may also allow a credential to be entered manually from the keypad in a PIN-only mode. PIN-only entry can be observed from a distance and the keying pattern is replicated to gain entry at a door.

Table 2 Classification of access control reader technologies.

	Input	Output
External	125kHz Smart contactless Mobile credential Other	Wiegand Clock/Data OSDP SSCP
Internal	Keypad	LED Buzzer/Speaker Text display

Tamper

A tamper mechanism provides a method to signal those monitoring an access control system that a reader has been removed from the wall. The tamper function has evolved over the years from a rocker switch hard-wired into the panel, to optical sensors and, most recently, accelerometers driven electronically and signalling to the access control panel using a dedicated output from the reader or by sending an appropriate message across the communication bus.

A functional anatomy of an access control reader

In this section, the various technologies presented previously are classified and constructed into a functional model of an access control reader.

The technologies employed by a reader may be classified as either an Input or an Output. Inputs provide data to be processed by the reader such as credential data or a key press. Outputs provide data to either the user or the access control system such as the buzzer or card data sent to the ACU to which the reader is connected.

The technologies may also be classified as Internal or External to the reader. Internal technologies are intrinsic to the reader such as a keypad or the LEDs. External technologies include credential technologies to be read or a transmission method to send data from the reader to the ACU.

Table 2 summarizes the classification of the technologies according to this scheme.

At the heart of an access control reader is a computer, usually a microcontroller. This is where the code is executed to perform the various input/output functions of the reader. With this device at the centre of the model, the functional anatomy of an access control reader is presented in Fig. 24.

Each technology has been placed into a group corresponding to the classification identified in Table 2. As not all readers support all technologies, each technology is bounded by a dashed line to denote that it is optional. To cater for future reader technologies, an Other box has been added to each of the input and output groups in the model. From this model, it can be seen that the minimum functional access control reader requires one external input and external output technology.

Attacker model

The principal threat to an access control reader is that a threat actor gains entry at an access-controlled door as if they are a legitimate user. They may wish to gain entry for opportunistic reasons or they may wish to gain access to achieve an objective on a carefully crafted kill chain. The level of sophistication required in attacking an access control reader may vary according to which end of the spectrum they are operating. This section examines how an attacker may gather intelligence about and/or compromise an access control reader.

Reconnaissance

Figure 25 presents the anatomy of an access control reader from an attacker's perspective. The original model has been extended to show the external actors to an access control reader: mobile and physical access control credentials, the ACU and the interfaces between these components. Some of the technologies have been colour-coded; those in yellow indicate technologies that have a history of being compromised with ease, and those in green indicate technologies that need to be further investigated.

It is important to highlight that, as of today, there is no officially recognized penetration testing methodology specifically designed for evaluating the security of access control readers. By researching the reader deployment to be attacked, we understand that the attacker can start planning an approach to compromising the system. To further our understanding of the system under attack, the external interfaces and factors are considered as follows:

(1) Can the card be stolen?
By far the easiest way of impersonating a legitimate user is to borrow or steal their card. For the opportunist, stealing the card and gaining entry achieves their objective, provided a secondary factor such as PIN or biometric is not required. Borrowing a card temporarily also allows the sophisticated attacker to evaluate the credential technology for cloning and spoofing.

(2) Can the card be cloned or spoofed?
It is known that the majority of 125kHz transponders and some smart contactless transponders (e.g. Mifare Classic) can be readily cloned. Cloning means that the attacker can replicate a physical credential. With access to a card printer, the attacker can complete the job by replicating the artwork on a real card. Borrowing a valid credential is one way of researching if the credential can be cloned. In some cases, the attacker may have the system information that allows a card to be cloned by knowing the card number and other relevant parameters.
A credential may also be spoofed by a piece of equipment (e.g. a Proxmark 3 [3]) and replayed to an access control reader. The device is used to read the credential. At a later time, the credential may be replayed on demand to gain access at a door.
As far as the reader is concerned, there is no difference between reading a legitimate card, a cloned card or a spoofed card replayed from a device.

(3) Is information leaked on the air interface?
By monitoring the air interface between a physical or mobile credential and a reader, it may be possible to obtain information that might help the attacker. For physical credentials, this is only useful in a desktop exercise where both a valid reader

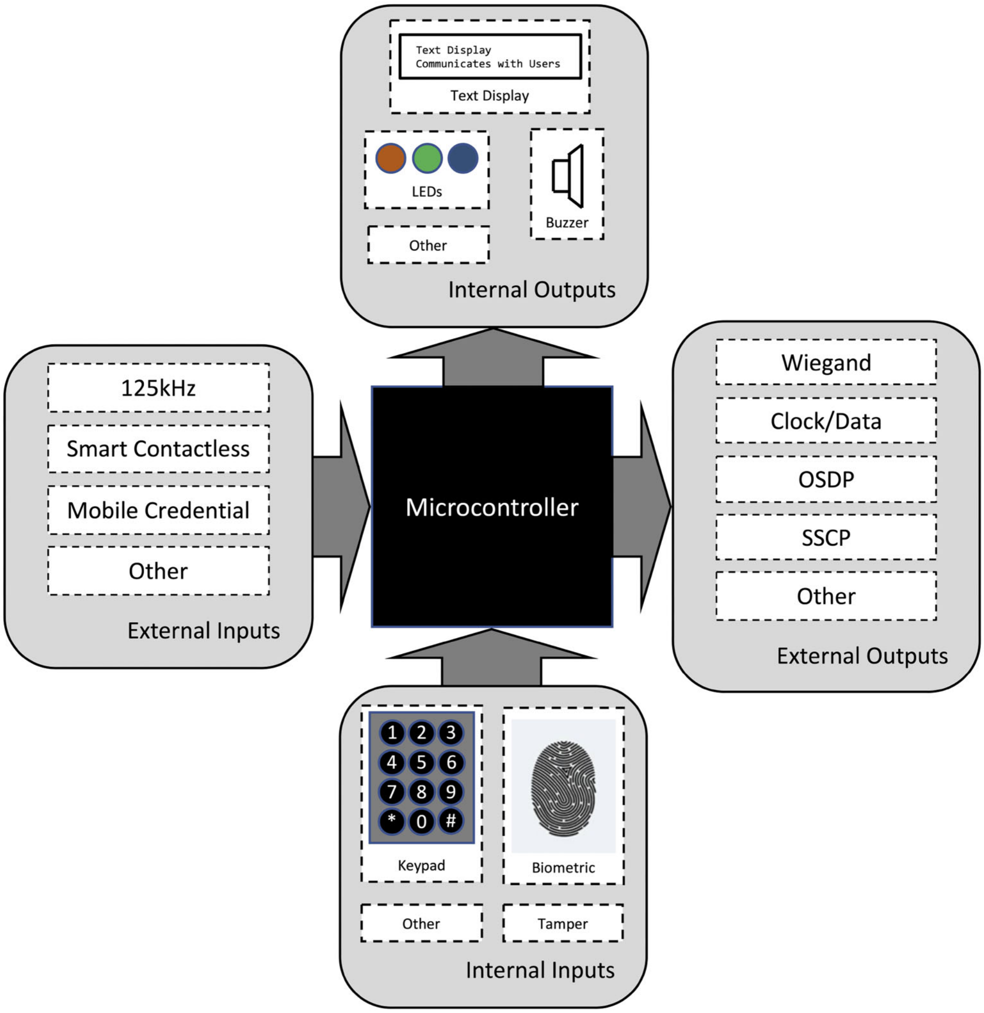


Figure 24. A functional anatomy of an access control reader.

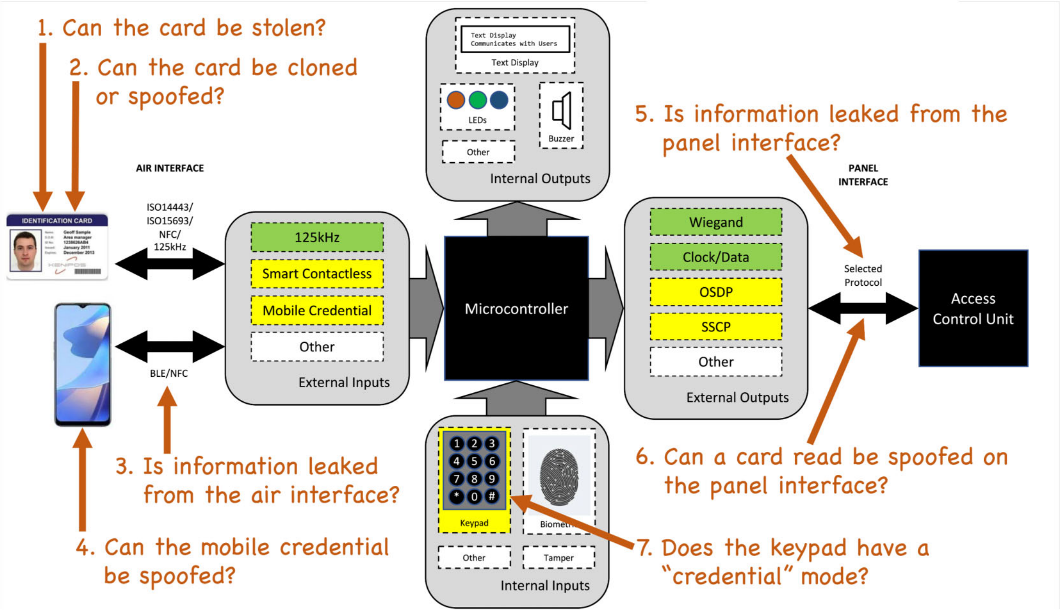


Figure 25. An attacker's view of an access control reader.

and credential are available to the attacker. For a mobile credential using Bluetooth, monitoring communication between mobile phones and a reader may be a legitimate reconnaissance exercise.

(4) Can the mobile credential be spoofed?
This remains an open question in the field of access control security. In this paper, five different mobile credential solutions have been identified, yet none of them have publicly disclosed their technical implementation details. This lack of transparency raises important concerns about security, interoperability, and potential vulnerabilities.
Unlike traditional access control credentials, mobile credentials introduce new attack surfaces, including BLE, NFC, and cloud-based authentication mechanisms. Without access to detailed implementation information, it is difficult to assess their resilience against cloning, relay attacks, man-in-the-middle attacks, or DoS threats.
As organizations continue to adopt mobile-based access control solutions, there is a growing need for comprehensive security research in this space. The absence of standardized testing methodologies for mobile credentials and access control readers leaves a gap in penetration testing and security evaluation frameworks. This makes mobile credential security a new frontier for both attackers and researchers alike, warranting further investigation to ensure secure deployment and risk mitigation strategies.

(5) Is information leaked from the panel interface?
In the case of Wiegand and Clock and Data output from the reader to the ACU, significant data is leaked from the panel interface. Every time a card is presented or a key is pressed, there is activity on the bus. If the green LED input to the reader is also monitored, it is possible to compile a list of valid cards and the corresponding PINs. The BLE Key [68] monitors a Wiegand bus and collects the card data transmitted across the bus. The BLE Key can be installed in the back of an existing reader to capture this data.
RS485 bus protocols like OSDP and SSCP are easily eavesdropped but, when deployed properly, are encrypted transmissions requiring the appropriate keys to extract the data.

(6) Can a card read be spoofed on panel interface?
The BLE Key was designed to do just this on a Wiegand bus. A credential can be replayed from a mobile application from the credentials that have been captured by the BLE Key. The same principle could also be applied to Clock and Data systems. This works because both Clock and Data and Wiegand are monodirectional and allow a device to be piggybacked onto the bus. RS485 buses are bidirectional. If the keys are known and the data stream can be decrypted, a man-in-the-middle device could be installed to insert credential data into the communication path with the ACU.

(7) Does the keypad have a 'credential' mode?
All of the previous questions relate to the potential external vulnerabilities of an access control reader. The attacker should not overlook flaws in the device itself, internal vulnerabilities, that may provide a backdoor to send credentials to the ACU. One such backdoor is keypad-only mode. In this mode, a user enters a PIN and a credential is sent to the ACU. No physical or mobile credential is required. Where a single PIN has been set up on a heavily used door, there may be wear on the keys that correspond to the PIN.

Exploitation

Should any of the aforementioned potential vulnerabilities prove viable or provide the information necessary to clone or spoof a credential and any device-specific back doors are ignored, there are only two ways to attack the system: a credential attack or a panel attack.

In a credential attack, the attacker presents a stolen, cloned, or spoofed credential to the reader and access is granted. This is the easiest way of impersonating a valid user on the system as no additional equipment is required.

Where the system to be attacked is using Wiegand to communicate with the ACUs, a BLE Key needs to be installed at the reader. This can be done on the insecure side of the door although the attacker would need to be aware of any video surveillance or tamper monitoring at the reader to avoid detection. Once installed, the attacker can replay a valid credential via remote control from their phone to the BLE Key.

Assuming that a man-in-the-middle attack is feasible for OSDP and/or SSCP, installing this device would be more challenging for the attacker. This device would need to be installed by breaking the bus and locating it out-of-sight. This could only realistically be done by an installation engineer acting on behalf of the attacker. Once installed, the device could be remotely controlled like the BLE Key.

Using the model as an attacker

The questions posed to the model do not inherently provide an attacker with all the answers needed to compromise an access control system. However, where the model indicates the possibility of credential cloning or a panel attack, an attacker can use this insight to strategically plan their approach. When direct answers are unavailable, the model still serves as a guiding framework, prompting further investigation, reconnaissance, and refinement of attack strategies. In this way, even gaps in knowledge become opportunities for deeper probing, ultimately aiding in the identification of potential vulnerabilities.

Demonstrative application of the proposed framework

To illustrate the use of the proposed framework, this section presents a conceptual application to a representative enterprise access control reader configuration derived from commonly documented system architectures and publicly described deployment practices in the literature. The purpose of this illustration is not to validate the framework through empirical testing, nor to report measurements from a live system, but to demonstrate how the framework can be applied in a structured manner to reason about security risk.

A multi-technology access control reader supporting legacy 125 kHz proximity credentials and smart contactless credentials is considered, using two commonly described configuration scenarios: communication between the reader and ACU via Wiegand, and communication via OSDP with a secure channel enabled. These scenarios are selected based on their prevalence in the literature and industry documentation, and serve solely as illustrative examples.

Applying the framework to the Wiegand-based scenario would highlight exposure at the panel interface, where credential identifiers and keypad inputs are transmitted without cryptographic protection. The framework would identify risks associated with credential replay, unauthorized credential injection, and data harvesting, consistent with previously reported attacks. Importantly, this analysis is based on known properties of the protocol rather than observation of a specific deployed system.

When the same reader configuration is considered under an OSDP secure-channel scenario, the framework would indicate a reduction in confidentiality and integrity risks associated with panel communication, owing to encrypted messaging and message authentication. Availability risks related to physical access to the communication bus would likely remain, reflecting limitations discussed in prior work. This comparison demonstrates how the framework can be used to contrast configuration choices and reason about their security implications.

This illustrative application shows how the proposed framework supports systematic reasoning about attack surfaces and risk concentration using existing knowledge, without requiring access to operational systems or empirical attack execution.

Conclusion

The modern access control reader is a sophisticated convergence of multiple technologies, each introducing potential vulnerabilities that adversaries can exploit to compromise the security of an access control system. While complexity enhances functionality, it also expands the attack surface, making security-by-design a fundamental requirement in reader development. An adversary, however, needs to find only a single weakness to bypass protections and gain unauthorized access, potentially leading to significant financial, reputational, and operational damage to an organization.

This paper presents a comprehensive anatomy of an access control reader, systematically mapping its components to potential vulnerabilities and exploits. By adopting an attacker's perspective, we establish a structured penetration testing framework, enabling a formal cybersecurity evaluation of access control readers. This approach not only enhances the security assessment process but also identifies critical areas for future research in access control technology. Just as physical locks continuously evolve to counter lock-picking techniques, access control credentials must be rigorously scrutinized with each technological advancement. This paper lays the groundwork for future research, driving the development of more resilient and robust enterprise security solutions. The proposed framework is intended as an analytical and structuring tool, with empirical validation in live operational environments left to future work.

Future work

This research identifies two primary attack vectors in access control systems: credential attacks and panel attacks, both warranting further investigation. Future work includes evaluating the feasibility of relay attacks on NXP DESFire credentials (EV1, EV2, EV3) and assessing vulnerabilities in commercial deployments. Furthermore, dismantling and modelling proprietary technologies such as HID SEOS, LEGIC Advant, Apple Wallet, and HID Mobile Access can help uncover undocumented behaviours and potential weaknesses, contributing to a broader understanding of credential-based threats. Despite secure protocols like OSDP and SSCP replacing legacy ones (e.g. Wiegand), research is needed to examine their resilience to eavesdropping and man-in-the-middle attacks over RS-485. Key questions include whether secure modes leak data or allow replay attacks and the implications of these findings for installers, manufacturers, and system integrators. Exploring these areas will inform best practices for securing modern access control systems against evolving threats.

Author contributions

Peter Jones (Writing–original draft), Lowri Williams (Supervision, Writing–original draft, Writing–review & editing), Eirini Anthi (Supervision, Writing–original draft, Writing–review & editing)

Conflicts of interest

No competing interest is declared.

Funding

None declared.

References

1. The Editors of Encyclopaedia Britannica. lock Encyclopedia Britannica, 24 Sep. 2021. https://www.britannica.com/technology/lock-security, Accessed: 1 May 2023.
2. Source Security. What is an acceptable life cycle for a physical security system?. 2017. https://www.sourcesecurity.com/insights/what-is-an-acceptable-life-cycle-for-a-physical-security-system.html, Accessed: 1 May 2023.
3. proxmark.org. *T55x7 and Tags Emulation*. 2013. http://proxmark.org/forum/viewtopic.php?id=1767, Accessed: 27 October 2020. Requires registration.
4. Baseggio Mark, Evenchick Eric. Breaking Access Controls with BLE Key. 2015. https://www.blackhat.com/docs/us-15/materials/us-15-Evenchick-Breaking-Access-Controls-With-BLEKey-wp.pdf, Accessed: 4 November 2022.
5. Garcia FD, de Koning Gans G, Verdult R. Exposing iClass Key Diversification. In: *5th USENIX Workshop on Offensive Technologies (WOOT 11)*. 2011.
6. Meriac M. Heart of darkness-exploring the uncharted backwaters of HID iCLASS^{TM} security. In: *24th Chaos Communication Congress*. 2010.
7. Nohl K, Plötz H. Mifare: Little Security, Despite Obscurity. In: *24th Chaos Communication Congress, December 2007*. San Jose, CA: USENIX Security Symposium, 2007. Available at: https://youtu.be/QJyxUvMGLr0, Accessed: 17 November 2022].
8. LenelS2. OnGuard. 2022. https://www.lenel.com/products/onguard, Accessed on: 13 October 2022.
9. Software House. C-CURE 9000 Security + Event Management. 2020. https://www.swhouse.com/Products/software_CCURE9000.aspx, Accessed on: 13 October 2022.
10. Help Net Security. IOActive withdraws BlackHat presentation; ACLU will present. 2007. https://www.helpnetsecurity.com/

2007/02/28/ioactive-withdraws-blackhat-presentation-aclu-will-present/, Accessed: 28 October 2023.

11. Help Net Security. HID Global statement on IOActive withdrawing their Black Hat presentation. 2007. https://www.helpnetsecurity.com/2007/02/28/hid-global-statement-on-ioactive-withdrawing-their-black-hat-presentation/, Accessed: 16 November 2022.
12. Plötz H, Nohl K. Peeling away layers of an RFID security system. In: *International Conference on Financial Cryptography and Data Security*. Berlin, Heidelberg: Springer, 2011, 205–19.
13. Garcia FD, Jacobs B. The Fall of a Tiny Star. In: *The New Codebreakers*. Berlin, Heidelberg: Springer, 2016, 69–87.
14. Garcia FD, Koning Gans GD, Verdult R *et al.* Dismantling iclass and iclass elite. In: *European Symposium on Research in Computer Security*. Berlin, Heidelberg: Springer, 2012, 697–715.
15. Garcia FD, de Koning Gans G, Verdult R. Wirelessly lockpicking a smart card reader. *Int J Inf Secur* 2014;**13**:403–20.
16. Kim C, Jung EG, Lee DH *et al.* Cryptanalysis of INCrypt32 in HID's iCLASS Systems. *IEICE Trans Fund Elect Commun Comput Sci* 2013;**96**:35–41.
17. GOV.UK. *GovPass to rule them all*. 2021. https://securityprofession.blog.gov.uk/2021/02/01/govpass-to-rule-them-all/, Accessed: 2 January 2024.
18. Oswald D, Paar C. Breaking Mifare DESFire MF3ICD40: Power analysis and templates in the real world. In: *International Workshop on Cryptographic Hardware and Embedded Systems*. Berlin, Heidelberg: Springer, 2011, 207–22.
19. Hurley-Smith D, Hernandez-Castro J. Bias in the mifare desfire ev1 trng. In: *Radio Frequency Identification and IoT Security: 12th International Workshop, RFIDSec 2016. Hong Kong, China, November 30–December 2, 2016, Revised Selected Papers 12*. Springer, 2017, 123–33.
20. Labafniya M, Yusefi H, Khalesi A. Reverse Engineering of Authentication Protocol in DesFire. *ISeCure* 2023;**15**:254.
21. Schmidt MD. A Recent Open Source Embedded Implementation of the DESFire Specification Designed for On-the-Fly Logging with NFC Based Systems. In: *Proceedings of the Future Technologies Conference (FTC) 2021*, Vol. **3**. Springer International Publishing. 2022, 141–58.
22. Kasper T, Ingo VM, David O *et al.* Chameleon: A versatile emulator for contactless smartcards. In: *International Conference on Information Security and Cryptology*. Berlin, Heidelberg: Springer, 2010, 189–206.
23. Casanovas JP, Van Damme G. DESfire Emulation Using Java Card. In: *Trustworthy Embedded Devices*. Leuven, Belgium: Conference Publishing Services IEEE, 2011, 5.
24. IPVM. Top Alternatives to HID and Mercury. 2022. https://ipvm.com/reports/alt-hid-mercury, Accessed: 13 October 2022. Requires a subscription.
25. HID Global. *HID Global*. 2022. https://en.wikipedia.org/wiki/HID_Global, Accessed: 15 October 2022.
26. HID Global. HID Prox Brochure. 2022. https://www.hidglobal.com/sites/default/files/documentlibrary/hid-prox-br-en.pdf, Accessed: 15 October 2022.
27. HID Global. iCLASS SE Reader Family Datasheet. 2022. https://www.hidglobal.com/documents/iclass-se-reader-family-datasheet, Accessed: 15 October 2022.
28. Inside Contactless. Datasheet Picopass 2 KS. 2004. http://www.proxmark.org/files/Documents/13.56%20MHz%20-%20iClass/DS%20Picopass%202KS%20V1-0.pdf, Accessed: 13 October 2022.
29. HID Global. HID Signo Readers Datasheet. 2022. https://www.hidglobal.com/documents/hidr-signotm-readers-datasheet, Accessed: 15 October 2022.
30. 3millID. 3millID Readers. 2022. https://www.3millid.com/readers/, Accessed: 16 October 2022.
31. LenelS2. Blue Diamond. 2022. https://www.lenels2.com/en/us/security-products/blue-diamond/, Accessed: 16 October 2022.
32. Allegion. Allegion. 2022. https://en.wikipedia.org/wiki/Allegion, Accessed: 16 October 2022.
33. Allegion. Allegion Multi-Technology Readers. 2022. https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/DataSheet/Schlage_Multi_Technology_Readers_Data_Sheet_105354.pdf, Accessed: 16 October 2022.
34. Farpointe Data. Farpointe Data. https://www.farpointedata.com/, Accessed: 16 November 2022.
35. Farpointe Data. P-500 Alps Proximity Reader. 2022. https://www.farpointedata.com/downloads/datasheets/P500_TDS.pdf. Accessed: 16 October 2022.
36. Farpointe Data. CSR-6.2L & CSR-6.4L CONEKT Mobile-Ready Contactless Smartcard Reader and Keypad. 2022. https://www.farpointedata.com/downloads/datasheets/CSR62L-64L_Conekt_TDS.pdf, Accessed: 16 October 2022.
37. STid. ARC1S/BT - 13.56MHz DESFire EV2 & EV3 + Bluetooth Mullion Reader. 2022. https://stid-security.com/en/products/arc1s-bt-bluetooth-13-56-mhz-desfire-ev2-mini-mullion-readers, Accessed: 16 October 2022.
38. STid. ARCS-B/BT - 13.56MHz DESFire EV2 & EV3 + Bluetooth Keypad Reader. 2022. https://stid-security.com/en/products/arcs-b-bt-bluetooth-13-56-mhz-desfire-ev2-keypad-readers, Accessed: 16 October 2022.
39. Wavelynx. Wavelynx. https://www.wavelynx.com/about, Accessed: 16 November 2022.
40. WaveLynx. Ethos Readers. 2022. https://wavelynxtech.com/wp-content/uploads/2022/06/WL-EN-Ethos-Readers-DS-3.9-060722-1.pdfs, Accessed: 16 October 2022.
41. The Channel Co. Security Researchers and Vendors Clash At Black Hat, Users Lose. 2007. https://www.crn.com/news/security/197700176/security-researchers-and-vendors-clash-at-black-hat-users-lose, Accessed: 16 November 2022.
42. Nohl K, Evans D.Reverse-Engineering a Cryptographic RFID Tag. 2008. https://www.cs.umd.edu/ jkatz/security/downloads/Mifare1.pdf. Accessed: 17 November 2022.
43. NXP. "Security of MF3ICD40". *Mifare.net*. 2013. Archived from the original on 21 February 2013. https://archive.ph/20130221220435/http://mifare.net/technology/security/mifare-desfire-d40/, Accessed: 24 November 2022.
44. Legic. Multi-purpose RFID ICs. 2022. https://www.legic.com/products/smartcards/legic-smartcard-ics, Accessed: 24 November 2022.
45. HID Global. SEOS™Card Datasheet. 2022. https://www.hidglobal.com/documents/seostm-card-datasheet, Accessed: 24 November 2022.
46. HID Global. Seos®Brochure. 2022. https://www.hidglobal.com/documents/seosr-brochure, Accessed: 24 November 2022.
47. TÜV Nord Group. Trustworthy IT systems and IT products: Trusted Site Security Trusted Product Security. 2018.

https://www.tuvit.de/fileadmin/Content/TUV_IT/pdf/.Dienstleistungsbeschreibungen/englisch/TUViT_TS_TP_Security_V3_0.pdf. Accessed: 24 November 2022.

48. International Standards Organisation. BS ISO/IEC 14443-4:2018: Cards and security devices for personal identification. Contactless proximity objects: Transmission protocol. 2018.

49. International Standards Organisation. ISO/IEC 15693-3:2019 Cards and security devices for personal identification—Contactless vicinity objects—Part 3: Anticollision and transmission protocol. 2019.

50. gsmarena.com. Samsung-made Google Nexus S is now official, 10 days to launch. 2010. https://www.gsmarena.com/samsungmade_google_nexus_s_is_now_official_10_days_to_launch-news-2124.php, Accessed: 3 December 2022.

51. androidcentral.com. Gingerbread feature: Near Field Communication. 2010. https://www.androidcentral.com/gingerbread-feature-near-field-communication, Accessed: 3 December 2022.

52. Murph D. Bluetooth 4.0 specification gets official, devices expected by Q4 2010. engadget.com. 2010. https://www.engadget.com/2010-07-07-bluetooth-4-0-specification-gets-official-devices-expected-by-q.html, Accessed: 3 December 2022.

53. O'Brien D. iPhone 4S claims title of first Bluetooth 4.0 smartphone, ready to stream data from your cat. engadget.com. 2011. https://www.engadget.com/2010-07-07-bluetooth-4-0-specification-gets-official-devices-expected-by-q.html, Accessed: 3 December 2022.

54. YouTube. Unikey Pt 1. 2012. https://youtu.be/coS4jS3uWpA, Accessed: 30 November 2022.

55. Shontell A. AT LAST: A Secure, Key-Free Way To Unlock Your Front Door Has Been Invented. Business Insider. 2013. https://www.businessinsider.com/unikey-is-an-easy-secure-way-to-unlock-doors-without-keys-2013-5?r=US&IR=T, Accessed: 30 November 2022.

56. asmag.com. HID Mobile Access features Twist and Go technology. 2014. https://www.asmag.com/showpost/17781.aspx, Accessed: 30 November 2022.

57. techcrunch.com. Steve Jobs: "Open Systems Don't Always Win. 2010. https://techcrunch.com/2010/10/18/steve-jobs-open-dont-win/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAD2d_hEhR5knl-J8slmR4RIe8XSQP6CxfGnbOzkDofeOISCRy6DiCYHLtqOtrXmYfg YesO4vUMHOQfPXMuy5_xdMMZ1mugog5xaE8Z9HwLDbDIer-F5AFrnB3P1Qb2KFxFocjNl3EPTHG7zNVfwCsxNIQgsjh_flusd2WL mJsFBo., Accessed: 3 December 2022.

58. gototags.com. iPhone NFC Compatibility. 2022. https://learn.gototags.com/nfc/software/iphone/compatibility, Accessed: 3 December 2022.

59. Apple. Apple brings contactless student IDs on iPhone and Apple Watch to more universities. 2019. https://www.apple.com/newsroom/2019/08/apple-brings-contactless-student-ids-on-iphone-and-apple watch-to-more-universities/, Accessed: 3 December 2022.

60. Security Electronics and Networks. HID Employee Badges Added To Apple Wallet At World Trade Center. 2022. https://sen.news/2022/02/04/hid-employee-badges-added-to-apple-wallet-at-world-trade-center/, Accessed: 3 December 2022.

61. HID Global. Silverstein Introduces Employee Badge in Apple Wallet for its World Trade Center Employees and Tenants. 2022. https://newsroom.hidglobal.com/silverstein-introduces-employee-badge-apple-wallet-its-world-trade-center-employees-and-tenants, Accessed: 3 December 2022.

62. Garba A *et al.* Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments. *J Inf Priv Secur* 2015; **11**:38–54. https://doi.org/10.1080/15536548.2015.1010985

63. Waitt T. Safeguarding People & Places in a Mobile World (Multi-Video). *American Security Today*. 2017. https://americansecuritytoday.com/safeguarding-people-places-mobile-world-multi-video/, Accessed: 3 December 2022.

64. Source Security. LEGIC's reader IC and mobile services power Farpointe's Conekt mobile access control solution. 2018. https://www.sourcesecurity.com/news/legic-reader-ic-mobile-services-farpointe-conekt-access-control-co-1040-ga-co-2736-ga-npr.1539152307.html, Accessed: 3 December 2022.

65. Javadi B *et al.* DEF CON 29 - Babak Javadi, Nick Draffen, Eric Bettse, Anze Jensterle - The PACS man Comes For Us All. DEF CON 29. 2021. https://youtu.be/NARJrwX_KFY, Accessed: 4 December 2022.

66. Wehr J.The Wiegand Effect: The 30-year old science project still influences modern security systems. Secure Id News. 2003. https://www.secureidnews.com/news-item/the-wiegand-effect-the-30-year-old-science-project-still-influences-modern-security-systems/, Accessed: 26 October 2022.

67. Security Industry Association. Access Control Standard Protocol for the 26-BIT Wiegand™ Reader Interface. 1996. https://webstore.ansi.org/standards/sia/siaac01199610.

68. Hacker Warehouse. BLEKey. 2022. https://hackerwarehouse.com/product/blekey/, Accessed: 4 November 2022.

69. OSDP Connect. How OSDP Was Developed. 2016. http://www.osdp-connect.com/how-osdp-was-developed.html#, Accessed: 4 November 2022.

70. Security Industry Association. Open Supervised Device Protocol (OSDP). 2020. https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/, Accessed: 1 November 2020.

71. Security Industry Association. SIA OSDP Verified: Comprehensive Testing to Ensure Interoperablility. 2020. https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/sia-osdp-verified/, Accessed: 4 November 2022.

72. SPAC Alliance. Technical Report: Secure and Smart Communication Protocol. 2022. https://en.sp-ac.org/standard-sscp (Confidential), Accessed: 16 November 2022.

Received: 28 July 2025. **Revised:** 7 January 2026. **Accepted:** 18 February 2026