



SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE ACCESS CONTROL COUNCIL AND
IDENTITY COUNCIL WHITE PAPER

Using Mobile Devices for Physical Access Control

Version 1.0

May 2021

Secure Technology Alliance

191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce, and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

Copyright © 2021 Secure Technology Alliance. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Secure Technology Alliance. The Secure Technology Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Secure Technology Alliance disclaims all warranties as to the accuracy, completeness, or adequacy of information in this report. This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.

Table of Contents

1	Introduction	1
1.1	Scope	2
1.2	Intended Audience	2
2	Market Trends for Using Mobile Devices for Physical Access	4
3	Mobile Device Landscape	6
3.1	Smartphones	6
3.2	Tablets	7
3.3	Wearables	8
4	Trust Frameworks	9
4.1	Credential Issuance and Lifecycle Management	10
4.2	Assurance/Confidence Levels	12
4.3	Credentials	14
4.3.1	Credential Types	15
4.3.2	Privilege and Authorization Attributes	16
4.3.3	On-Device Credential Protection	16
5	Use Cases	18
5.1	Buildings	18
5.2	Secure Rooms	19
5.3	Restricted Emergency Areas	20
5.4	Gated Buildings and Parking	21
5.5	Guest Access to Gated Communities	21
5.6	Hotel Rooms	23
5.7	Healthcare Facilities	23
5.8	Cruise Ships	24
5.9	Entertainment Venues	24
5.9.1	Counterfeiting, After-Market Sales, and “Just in Time” Passes	25
5.9.2	Theft, Refund, and Cancellations	25
5.9.3	Throughput, Re-entry, and Tracking	26
5.10	Airport Passengers and Employees	26
5.10.1	Airport Passengers	26
5.10.2	Airport/Airline Employee Access	27

5.11	College/University Campuses	28
5.11.1	Real World Examples.....	28
5.11.2	ROI Benefits.....	29
5.12	Extraordinary Circumstances	29
6	Mobile Devices and Relying Party Interfaces	30
6.1	Mobile Device Interface Modes.....	31
7	Mobile Device Support for Multifactor Authentication	34
7.1	Enhanced Mobile Device Authentication Factors.....	34
7.1.1	Push Notifications.....	34
7.1.2	Leveraging Mobile Device Special Features for Multifactor Authentication	35
8	Conclusion.....	36
9	Publication Acknowledgements	37
Appendix A	Glossary.....	39
Appendix B	References	41

Tables

Table 1. Assurance/Confidence Level Definitions.....	14
Table 2. Use Case Summary by Assurance/Confidence Level.....	18
Table 3. Local Authentication Interface Mode Examples	32
Table 4. Remote Authentication Interface Mode Examples.....	33

Figures

Figure 1. Popular Mobile Devices	6
Figure 2. Smartphone Device Features.....	7
Figure 3. Smart Tablet Device Features	7
Figure 4. Wearable Device Features	8
Figure 5. Fundamental Trust Framework Model	9
Figure 6. Issuer Credential Issuance and Lifecycle Management	11
Figure 7. Mobile Device Contactless Communications Interfaces.....	30
Figure 8. Traditional Relying Party PACS Architecture.....	30
Figure 9. Mobile-Enabled PACS Relying Party Architecture.....	31

1 Introduction

Most of us have had to present identification to enter a building, a room within a building, a garage, a gate, a secured perimeter, or even a highway. Typically, forms of identification used in such physical access scenarios include badges, RFID tags, smart cards, or other tokens. We may have multiple such forms of identification and tokens to manage and maintain, along with all the other paraphernalia that we carry for personal or professional needs. Mobile devices that we already possess can supplant or replace traditional tokens. Along with the everyday features for which we use our mobile devices -- most of these devices are feature-rich with supplemental hardware technologies.

These technologies support authentication over short-range contactless communications interfaces (i.e., Near-Field Communications (NFC) and Bluetooth Low Energy (BLE)) to physical access control system readers, supported by longer-range communications capabilities such as WiFi and cellular to access backend services. These devices are also equipped with cameras, audio recorders, and fingerprint readers which can capture facial photos, voice clips, and fingerprint scans to support multifactor authentication at physical access points.

As the adoption and use of mobile devices (especially smartphones) increase, industries are moving to take advantage of these versatile and handy computing platforms, and their robust security and communications features in current and growing physical access control markets.

This white paper addresses the application of mobile device features and benefits in a wide range of common and unique physical access use cases. Supporting mobile device features are explicitly characterized throughout the white paper. The benefits of employing mobile devices for physical access are as follows:

- Nearly everyone already possesses a mobile device of some kind that could be used as a “mobile token” for physical access.
- A mobile device is typically the one item that a person will always remember to carry when leaving home.
- If a user already possesses a mobile device that can be leveraged to control physical access, an organization need not issue a traditional token or credential to unlock a door or enter a building. This is a direct financial benefit of using mobile devices.
- Powerful free and low-cost mobile application development environments are available for all mobile device platforms. Sophisticated applications can be developed that exploit the feature sets inherent in a wide range of mobile devices.

This white paper was developed by the Secure Technology Alliance Access Control and Identity Councils, which comprise private-sector industry members, and members from public-sector agencies, including the Department of Defense (DoD) Defense Manpower Data Center (DMDc), Department of Homeland Security (DHS), General Services Administration (GSA), and the Transportation Security Administration (TSA). The collective effort illustrates the connection between identity management practices and the use of mobile device technology as enablers.

The members of the Secure Technology Alliance Access Control Council and the Identity Council have identified the potential for using mobile devices for physical access control as a common area of interest within the industry. This white paper draws on member experience and expertise in the areas of mobility, identity management, and physical access control, and is published to identify:

- Established standards and guidance for physical access control

- Mobile device hardware features and mobile applications that exploit these features
- Current implementations and use cases, and the potential for new use cases

1.1 Scope

This white paper covers the use of mobile devices for physical access control in both the public and private sectors, including commercial, federal, state, and local government opportunities.

An all-inclusive discussion of the use of mobile devices for physical access control is unrealistic, as new mobile devices and mobile device features are introduced into the market monthly or even daily. Therefore, this white paper is intended simply to lay a foundation for addressing the use of mobile devices for physical access control that is adaptable to market trends, new technologies, and any future standards, either *de facto* or official.

The white paper sets the stage by:

- Surveying which mobile devices can be leveraged for physical access control
- Describing example use cases that demonstrate the versatility of mobile devices
- Demonstrating how mobile devices can be applied to these use cases within a trusted framework for credential issuance
- Detailing mobile device technical feature sets

The following questions are addressed:

- What are the market trends for using mobile devices for physical access? (Section 2)
- What mobile devices can currently be leveraged for physical access? (Section 3)
- What are some current and potential use cases for using a mobile device to control physical access? (Section 5)
- What are the basic requirements for a relying party to allow a person to enter a controlled physical space? (Section 6)
- What trust frameworks must be set up to support trusted access to controlled physical areas using a mobile device? (Section 4)
- What levels of security and assurance are appropriate for particular use cases, and how are those levels defined and supported? (Section 4)
- What types of credentials can be placed on a mobile device to ensure that the credentials and the possessor of the mobile device can be trusted to access secured locations? (Section 4)
- How can a mobile device and a physical access control reader communicate? (Section 6)
- What mobile device features can be leveraged to support physical access? (Section 6)

1.2 Intended Audience

This white paper is intended for any organization, public or private, that is considering the use of mobile devices for physical access control.

The following audiences will find the information in this white paper of particular interest:

- **Consumer advocates** – Consumer-focused professionals who explore and advocate positions that may benefit individuals and organizations within a consumer ecosystem

- **Organization policy makers** – Individuals, organizations, and committees that define policies, guidance, and standards pertinent to the implementation, deployment, and operation of specific initiatives
- **Organization management** – Management professionals who are responsible for setting the goals and objectives of specific initiatives, and providing oversight of the implementation of those goals and objectives
- **Chief Information Officers/Chief Technology Officers (CIOs/CTOs)** – Organizational officers who establish and oversee the technical policies of an organization
- **Organization security managers (CSOs)** – Officers who establish and oversee the organization's security policies
- **Mobile device manufacturers** – Companies that design, manufacture, and sell mobile devices
- **Mobile application developers** – Software development professionals who create applications for a variety of mobile device platforms
- **Mobile credential issuers** – Organizations that provide credential creation and issuance services based on policy and standards-driven infrastructures and trust frameworks
- **Systems integrators** – Organizations that integrate end-to-end services and technical components into a cohesive service offering to customers
- **Physical access control system (PACS) product manufacturers** – Companies that design, manufacture, and sell physical access control systems
- **PACS system owners and operators** – Individuals and teams responsible for configuring and maintaining physical access control systems

2 Market Trends for Using Mobile Devices for Physical Access

The capabilities, security features, and cost benefits currently offered by mobile devices are driving market trends for the increased use of mobile devices for gaining access to controlled physical spaces. Mobile devices combined with mobile identities and mobile credentials apply equally to physical access trends in the commercial and public sectors.

Another driver for market penetration is the increase in the diversity of mobile devices and the applications that can be easily developed to exploit their features. With this diversity, the definition of “mobile device” is changing. Smartphones come readily to mind, but other mobile devices such as tablets and wearables extend the possibilities for unique physical access implementations. The accessibility and convenience of these various mobile form factors also contribute to increased acceptance of mobile devices in the physical access control space.

In 2017, Gartner predicted that by 2020, 20% of organizations will be using mobile credentials for physical access in place of traditional ID cards, compared with just 5% in 2016.¹ According to IHS Market, the commercial sector, with over a 90% share, will continue to dominate the market for mobile credentials through 2023, especially in the hospitality and office building sectors. Universities and other educational institutions will represent over half the remainder of the market.²

Annual downloads of mobile credentials grew by more than 220% from 2018 to 2019.³ In 2020 and beyond, the trend is set to continue – building on market drivers such as Bluetooth Low Energy (BLE), which dominated the mobile access control platform market (since BLE has been equally supported on both Android and iOS platforms); and Near Field Communications (NFC), which Apple has progressively opened access to NFC chips by iOS application developers on iPhones (but which is still not opened up to the level of accessibility to the NFC chip feature set that the Android platform provides).

Adoption of biometric readers – and a subset of those readers that are ‘frictionless’ – will likely increase. The high cost of frictionless biometrics has discouraged adoption. Now, in the wake of the COVID pandemic, end users will be more willing to use mobile devices that do not require people to touch a common external biometric reader. Rather, users can use the biometrics readers on their personal mobile devices without the fear of being in contact with germs, viruses and bacteria left behind by those who may have previously touched common-use external readers. For similar reasons, adoption rates for mobile credentials will likely increase during the coming years. This technology will be particularly appealing for building owners with frequent tenant users and temporary visitors wishing to gain access.⁴

Higher education continues to adopt mobile devices to host digital IDs and mobile credentials. This trend is driven in large part by an urgent need to upgrade existing access control systems; it also

¹ Gartner, “Gartner Says That 20 Percent of Organizations Will Use Smartphones in Place of Traditional Physical Access Cards By 2020,” Jan. 17, 2017, <https://www.gartner.com/en/newsroom/press-releases/2017-01-17-gartner-says-that-20-percent-of-organizations-will-use-smartphones-in-place-of-traditional-physical-access-cards-by-2020>.

² “Mobile vs physical access credentials - a tough battle,” Security World Market, Oct. 22, 2019, <https://www.securityworldmarket.com/uk/News/Business-News/mobile-vs-physical-access-credentials-a-tough-battle1>.

³ “Physical Security Market Overview Q4 2020,” SIA, November 4, 2020, https://www.securityindustry.org/report/physical-security-market-overview-q4-2020/?utm_source=Informz&utm_medium=Email&utm_campaign=sia%2C%20security%20industry%2C%20security%20industry%20association&zs=8FSVW&zl=DmsJ2.

⁴ ibid

leverages the NFC capabilities of mobile devices for other services.⁵ In the hospitality sector, a growing number of hotels offer premium customers the opportunity to download a room number and digital room key to a mobile device that is registered in the hotel guest system database. This solution benefits both the hotel guest, who does not need to stand in line at the check-in counter to receive a physical token, and the hotel, which may be able to free up front desk staff for other guest service functions⁶.

While higher education, building access, and hospitality constitute a major portion of existing markets and are projected as major growth markets, there are other existing and potential vertical and horizontal markets that are equally compelling for using mobile devices for physical access. Section 5, “Use Cases,” is intended to hint at the scope of how mobile devices have an unlimited secure and convenient applicability in this growing market landscape.

⁵ “Vertical Market Focus: Education--‘Why Use a Card When I Have My Phone?’,” SECURITY INFOWATCH, November 19, 2012, <https://www.securityinfowatch.com/access-identity/access-control/article/10820977/one-card-access-control-moves-closer-to-near-field-communications>.

⁶ “Why mobile key is taking over in hotels,” Hotel Management, December 2018, <https://www.hotelmanagement.net/tech/why-mobile-key-taking-over-hotels>.

3 Mobile Device Landscape

The mobile device technologies that are the focus of this white paper are those that are readily available and accessible in a variety of platforms by consumers — smartphones, tablets, and wearables.



Figure 1. Popular Mobile Devices

Smartphones are the primary device under consideration, since they are feature rich and support a variety of physical access control use cases. Almost everyone possesses a smartphone, and a smartphone is the last thing that a person forgets to carry when venturing outside of the home.

However, there are use cases where a tablet or a wearable device may be equally or more convenient for accessing secured areas. Tablets include many of the features of a portable computer and most of the features of a smartphone. Wearables range from simple RFID “smart rings” to very sophisticated smart watches.

All of these devices are loaded with a rich array of technological features. The following sections address these features and the viability of each mobile device platform for physical access. Prevalent device features are categorized by components, communications, and sensors, along with miscellaneous special elements.

3.1 Smartphones

Smartphones are already being used for physical access control, and their use is projected to increase dramatically over the coming decade. This projected growth is largely due to the following:

- Phones are a convenient form factor.
- All major product operating system (OS) platforms (e.g., Android, iOS, and Windows Mobile) include common contactless communication capabilities (NFC, Bluetooth, WiFi, and cellular).
- Almost everyone has a smartphone (personal or issued by an organization), knows how to use it, and carries it with them most of the time.

Figure 2 provides a sample superset of features available on current smartphones.



Components

- CPU, GPU
- Memory
- Crypto Engine
- SIM
- Keystore/KeyChain
- Clock & Timers
- Display, Touchpad

Communications

- Cellular Service
- WiFi
- Bluetooth (5.0, LE)
- NFC
- USB

Sensors

- Camera (Photo, Video)
- GPS
- Compass
- Accelerometer
- Gyro
- Proximity
- Fingerprint Scanner
- Barometer
- Iris Scanner

Miscellaneous

- Visible Light Source
- IR Light Source
- Barcode/QR Code Scan/Display
- Facial Recognition

Figure 2. Smartphone Device Features

3.2 Tablets

Tablets include many of the features that are prevalent in smartphones. However, tablets are not as convenient to use, and they are too large to be carried in a pocket. Holding them up to an access control reader or scanning a QR code may also be awkward. Further, many tablets do not include NFC capability. Those that have enabled NFC may not permit developers to access a common set of capabilities—that is, different manufacturers allow access to different capabilities. However, these factors do not preclude use of tablets for physical access. Tablet-based physical access control solutions have already been on the market for several years.

Figure 3 provides a sample superset of features available on current tablets.



Components

- CPU, GPU
- Memory
- Crypto Engine
- SIM
- Keystore/KeyChain
- Clock & Timers
- Display, Touchpad

Communications

- Cellular Service
- WiFi
- Bluetooth (5.0, LE)
- NFC
- USB

Sensors

- Camera (Photo, Video)
- GPS
- Compass
- Accelerometer
- Gyro
- Proximity
- Fingerprint Scanner
- Barometer
- Iris Scanner

Miscellaneous

- Visible Light Source
- IR Light Source
- Barcode/QR Code Scan/Display
- Facial Recognition

Figure 3. Smart Tablet Device Features

3.3 Wearables

Wearables (most notably, smart watches) have infiltrated the mobile device physical access control market in the same way as smartphones. Smart watches include a general-purpose operating system and a variety of hardware components that can support a wide range of applications and can leverage NFC, Bluetooth, WiFi, and cellular communications for physical access control much in the same way as smartphones. Other wearables include smart wristbands, smart rings, smart glasses, fitness trackers, smart clothing, and implantables, which could be used for niche or special-purpose physical access control use cases. Wearables provide enhanced convenience; they are readily available for presentation to a reader without having to fumble in a pocket or purse as one might have to do with a smartphone or tablet.

Figure 4 provides a sample superset of features available on current wearables.

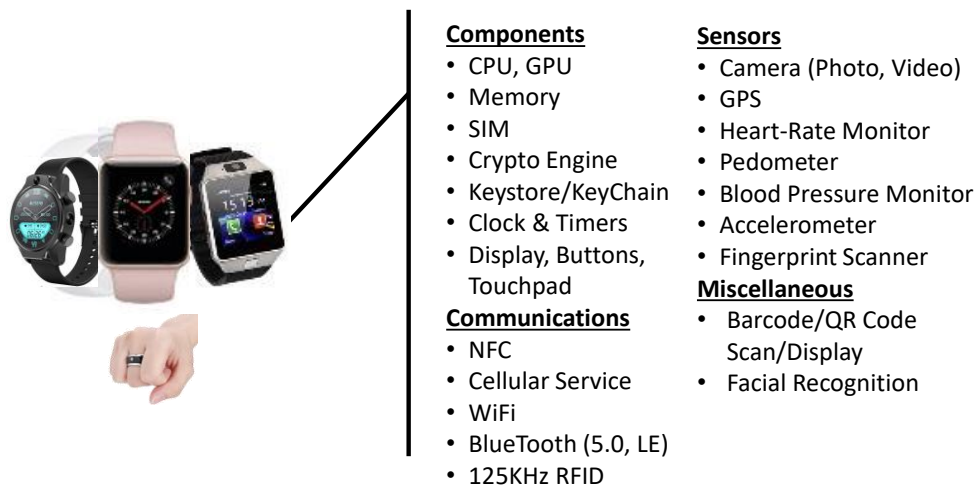


Figure 4. Wearable Device Features

4 Trust Frameworks

In the context of this white paper, a trust framework is defined as a set of policies, processes, and technologies that establishes various degrees of:

- Trust in the individuals who are allowed to access specific controlled physical spaces
- Trust in the mobile device that a user presents to access a controlled physical space
- Trust in the mobile device application that is used to access controlled physical spaces
- Trust that entry points only grant access to trusted users possessing trusted devices
- Trust in the credentials that are issued to the devices to allow all of the above

Trust frameworks are established by organizations to restrict access to physical spaces to eligible individuals. Trust frameworks can be quite simple or very rigorous, depending on both the type and sensitivity of the controlled areas, and the level of assurance or level of confidence required to permit access. The variety of sample use cases provided in Section 4 suggests a wide range of types and complexity of trust frameworks. However, in all such use cases, the associated trust frameworks and their components conform to the fundamental trust framework model depicted in Figure 5.

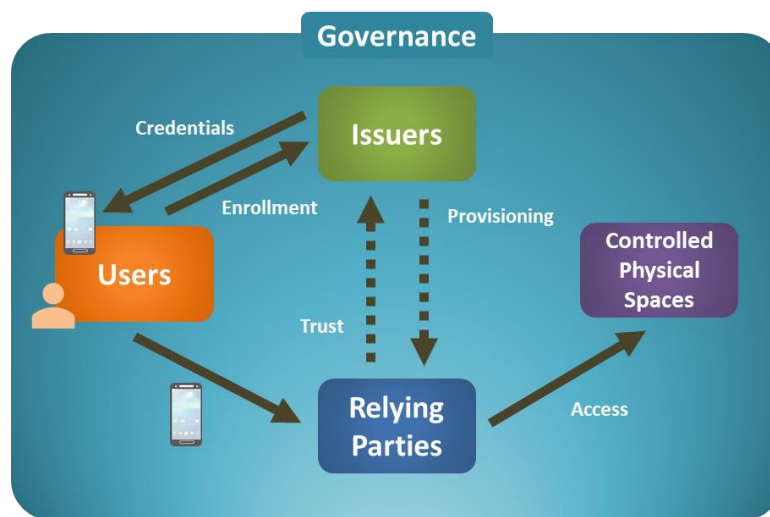


Figure 5. Fundamental Trust Framework Model

The components of the trust framework model are as follows:

- **Governance** – Organizations establish the policies, processes and technologies that govern the trust framework, establish the trust model for all components of the trust framework, and oversee the trust framework operations. The organization defines the credential types and the levels of assurance/confidence of the controlled physical spaces to be accessed by users (see Sections 4.2 and 4.3).
- **Users** – Individuals possess mobile devices which hold credentials to allow them to access the controlled physical spaces under the governance model.
- **Issuers** – Issuers hold the main responsibility for orchestrating the trust framework and implementing the governance policies by:
 - Establishing and managing some form of “identity” for users and their mobile devices through enrollment/registration processes

- Generating credentials for users and their devices
- Delivering the credentials to apps running on user devices
- Provisioning identity and credential information to relying on parties
- Managing the lifecycle of credentials and user identities
- Providing credential validation services to relying parties
- **Relying Parties** – Relying parties are those entities that provide the decision point for allowing users to access physical spaces under their control. Relying parties authenticate and validate user (and device) credentials when they are presented at an access point. A relying party may be a traditional PACS with readers that interface with mobile devices and collect biometric information from the user. A relying party may also be just a person who visually inspects a credential displayed on a mobile device, or who has a handheld reader to interface with the mobile device to access and validate its hosted credential. Relying parties may also have direct access to the issuer components that provide further trust validation of the credential and user (and/or the user's device), such as digital certificate revocation lists (CRLs) and online certificate status protocol (OCSP) responders.
- **Controlled Physical Spaces** – All of the above trust-framework components are in place to protect access to the target controlled physical spaces, which protect assets and resources to which users wish access.

Trust frameworks can be very simple or very rigorous, for example:

- In a simple trust framework, such as one governing an entertainment venue (see use case in Section 5.9), access may require only that individuals prove that they legally purchased a ticket. There may be no requirement for proof of identity, and individuals may remain relatively anonymous, except in certain cases in which an attendant at a venue might require the individual to present an ID (e.g., a driver's license) to compare with the virtual ticket on the mobile device. There is no identity vetting requirement at the time of ticket purchase. All that is required is the ability to pay for the ticket and provide proof of that purchase.
- In a rigorous trust framework, such as for a secure room (see use case in Section 5.2), individuals may have to go through a detailed background investigation to achieve eligibility. This trust framework may require enrolling in-person with fingerprint and facial image capture, registering the device, loading an application on the device, and provisioning a digital certificate to the user and the user's device. The issued digital certificates authenticate the user and device to readers stationed at the entry point of the secure room. There may also be requirements for multifactor authentication, requiring an additional biometric match (e.g., fingerprint, facial recognition, or iris scan).

The use cases described in Section 5 suggest a variety of trust frameworks. However, every trust framework and its components would implement some form of the fundamental trust framework model shown in Figure 5.

4.1 Credential Issuance and Lifecycle Management

As described above, trust frameworks define the governance model for issuing and using credentials. Once the governance model is established, a mechanism for enforcing that all policies, processes and procedures are securely audited must also be implemented. The implementation and operation of the

overall trust framework governance model are fundamental responsibilities of the issuer component of the trust framework.

In reference to Figure 5, Figure 6, below, expands on the functional areas that issuers would implement to issue credentials to trusted users (and/or devices) and manage those credentials throughout their lifecycles. The degree of complexity in the implementation of these issuer functional areas depends on the security requirements for each specific use case.

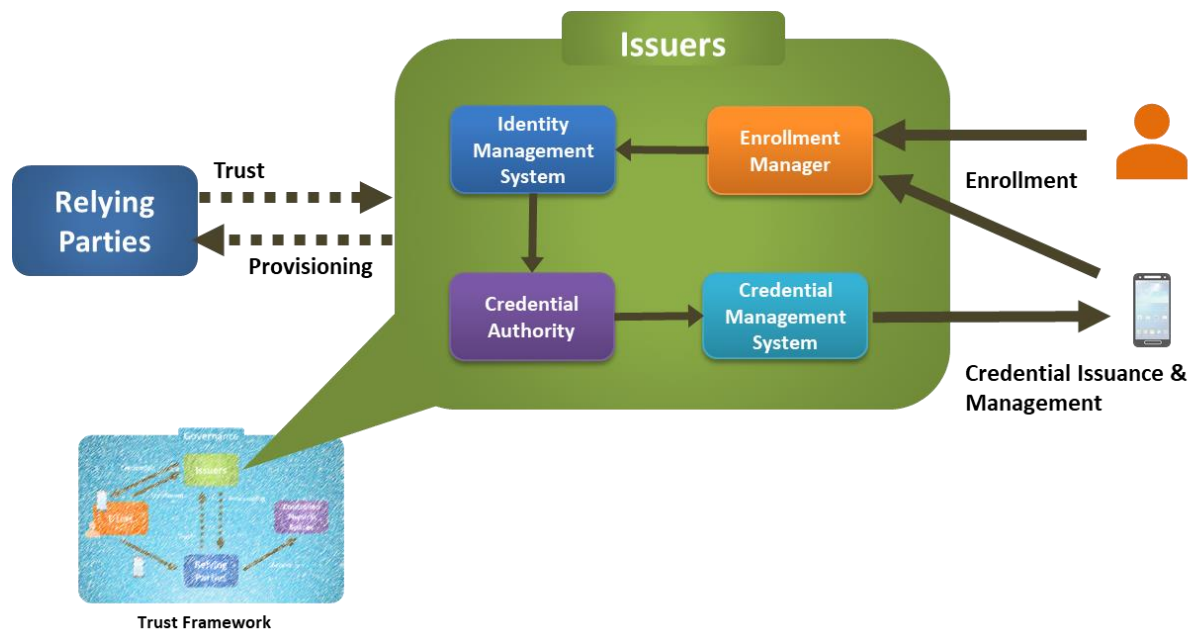


Figure 6. Issuer Credential Issuance and Lifecycle Management

The high-level issuer functional areas for credential issuance and lifecycle management are:

- Enrollment
- Identity management
- Credential authority
- Credential management

Orchestrating the delivery and storage of a mobile credential is similar to the structures that have become commonplace for managing logical access credentials over the past two decades. Traditionally focused on smart cards, issuers ensure the secure delivery of the correct identification credentials to the right person according to an enforced set of policies. Importantly, issuers comprise a single point of administration for all credentials assigned to each person within a given sphere of control.

To start the multi-step credential issuance process, users are introduced into the trust framework through an enrollment process within which they present some form of identification that is validated or proofed to a level of assurance mandated by trust framework policy. In some use cases, user devices may also be enrolled and managed to ensure that credentials are not only issued to the correct user, but also to the correct mobile device that a user may possess.

The form of evidence of identification the user provides binds their identity to their issued credential and to the mobile device on which they want credential to be hosted. This binding is often performed as part of the overall enrollment process and may involve a one-time passcode being sent by email or text to the user, a QR code being scanned by a use-case-specific mobile app, or a 'push' notification to the app on the mobile device.

Once these auxiliary validation methods and the user's identity have been confirmed and validated, a record of the user (and potentially the device) is maintained within the identity management system (IDMS) of the issuer infrastructure.

Following the establishment of the user identity, a credential can be created. Given the wide range of credential types (as addressed in following subsections), the issuer's credential authority creates a credential. A credential could be simply a transaction code which could be provided to the user or user mobile app (e.g., via a QR code), or digital certificate created by a certificate authority (CA). The issuer's credential management system (CMS) subsequently takes over management of the credential and issues/provisions the credential to the mobile device.

It is important to note that at any point, a given user may have numerous credentials on a wide range of devices. Being able to manage those in a unified manner is becoming increasingly important and challenging. Tools that assist users to maintain control and keep track of the number of devices and systems with which they interact are also becoming important as the number of devices each individual user interacts with grows. A comprehensive issuer implementation is vital to maintain the integrity of the trust framework to which the user has subscribed.

Once a credential has been issued, maintenance operations still need to be performed throughout the credential's lifecycle. Credential and lifecycle management is the functionality provided by the issuer's CMS. Maintenance or lifecycle management operations include: cancel and replace, suspend, restore, or transfer credentials in response to real-world events such as losing or upgrading a mobile device. In this respect, mobile devices are much more convenient than smart cards due to their high levels of connectivity. This means that most updates and other activities can be accomplished fully remotely.

However, for more secure systems, a mobile app might be used to generate a cryptographic key pair and send the public key to the issuer. The issuer then associates that public key with the user's device, so that a three-way relationship (person-device-credential) can be maintained. In some cases, the public key may be used by the issuer's credential/certificate authority to create a digital certificate to be returned to the mobile device.

The issuer may also notify a relying party of the credential that has been issued to the user so that it can be provisioned to access points in the relying party's purview; this will facilitate access decisions when the credential is used for physical access attempts. Subsequent events, such as a device being lost, may then result in notifications being sent to any relying party servers to immediately deny access attempts by a user and their mobile device.

4.2 Assurance/Confidence Levels

Several models are used for categorizing the confidentiality, integrity, and availability of relying-party assets, and the potential impact should those assets be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.⁷ These models are also augmented by frameworks

⁷ See NIST FIPS 199. <https://csrc.nist.gov/publications/detail/fips/199/final>.

that establish separate categorizations and levels of assurance for identity and authentication for users that attempt to access those assets.⁸ For convenience, this white paper consolidates those asset and identity categorizations into a general set of assurance/confidence levels. As such, this white paper assurance/confidence level model does not imply any advantage over other assurance models.

Three assurance/confidence levels are defined, “Low,” “Medium,” and “High,” which are based on the following considerations for evaluating the security posture of controlled physical spaces, the assets within the controlled spaces, and the policies for accessing them:

- **CONSIDERATION 1 - Sensitivity of Assets:** *What is the sensitivity of the assets in the restricted area, and to what level do they have to be protected?* The degree of security and risk control required depends on the nature, sensitivity, or importance of the security interests in the controlled space. By categorizing the sensitivity of the assets protected in a controlled area, organizations establish policies for the other two considerations, i.e., identity assurance and authentication.
- **CONSIDERATION 2 - Identity Assurance:** *What are the initial requirements to establish known and trusted digital identities for the “systems” that control access to physical spaces, and to what degree do individual identities have to be “proven” before individuals can be deemed eligible to access those physical spaces?* Depending upon the assets to be protected in controlled spaces, organizations establish policies and processes for establishing trusted digital identities for individuals. For some use cases, an individual's real-life identity might not be required to gain access to a controlled area; e.g., an email account and a credit card⁹ may be the only requirements to establish a trusted digital identity. In other use cases, a stringent identity proofing process may be required that includes an extensive background investigation.
- **CONSIDERATION 3 – Authentication:** *What is the level of assurance/confidence that the individual entering a controlled area is who they say they are, and are eligible and have the privileges to be granted access?* Organizations establish requirements for what degrees and types of authentication are to be performed at the entry points to its controlled areas. Specifically, some level of multifactor authentication¹⁰ is performed by readers or attendants at the entrance to the controlled spaces. In most cases, a credential (“something you have”) is presented and authenticated at the entry point. In other cases, additional authentication factors may be necessary, such as entering a PIN (“something you know”) and/or having a biometric scanned and verified (“something you are”).

Table 1 defines low, medium, and high levels of assurance/confidence (as used in this white paper) in the context of the above considerations.

⁸ NIST SP 800-63 (see reference [SP800-63]), for example. NIST 800-63's defined assurance levels are recognized and adopted outside the federal community and provide guidance across diverse applications such as in driver's license issuance and in the healthcare market.

⁹ Use of a credit card may require providing personally identifiable information (PII) (e.g., name on card and billing address) when making a payment for an entertainment venue, for example, but there is no assurance that the credit card belongs to the person who will actually attend the event – e.g., a mother may be buying a ticket for her daughter.

¹⁰ Multifactor authentication (MFA) – see Section 7.

Table 1. Assurance/Confidence Level Definitions

Assurance/ Confidence Level	Consideration
LOW	<p>Sensitivity of Assets: A breach of the controlled area may cause minor risk to controlled assets.</p> <p>Identity Assurance: There is little or no requirement to link an individual to a specific real-life identity.</p> <p>Authentication: There is some assurance/confidence that an individual controls an approved and authenticatable credential. Single-factor or two-factor authentication maybe employed using a wide range of available authentication methods.</p>
MEDIUM	<p>Sensitivity of Assets: A breach of the controlled area may cause moderate risk to controlled assets.</p> <p>Identity Assurance: There is high assurance that the digital identity/credential is linked to a specific real-life individual. The individual must provide some form of approved identification and other information in order to be issued a credential.</p> <p>Authentication: There is high assurance/confidence that an individual controls an approved and authenticatable credential. Single-factor or two-factor authentication maybe employed using a wide range of available authentication methods.</p>
HIGH	<p>Sensitivity of Assets: A breach of the controlled area may cause severe risk to controlled assets. Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the issuer.</p> <p>Identity Assurance: There is very-high assurance that the digital identity/credential is linked to a specific real-life individual and/or mobile device. The individual may be required to participate in an in-person or remote registration process, along with other appropriate identity proofing requirements, and a background investigation. The individual's mobile device may also be required to be registered during an enrollment process.</p> <p>Authentication: There is very-high assurance/confidence that an individual controls an approved and authenticatable credential. Three-factor authentication is required using a wide range of available authentication methods, along with strong cryptographic authentication of the credential over an encrypted channel. In addition, the individual's mobile device and the application used to authenticate may have their own sets of credentials, and those credentials are authenticated along with the primary user credential.</p>

4.3 Credentials

The credentials issued to mobile devices to establish digital identities are the basis for authentication by relying parties. Credentials vary depending upon the needs of particular use cases. The following subsections discuss potential credential types, additional privilege information, and secure storage of credentials on mobile devices.

4.3.1 Credential Types

A wide range of credential types are suitable for use within different trust frameworks. The type of credential that is chosen depends on the assurance/confidence levels required by specific use cases and on the physical environment associated with each use case. The credentials for controlling physical access that are hosted on a mobile device can be more convenient and secure than the simple identifiers used by legacy tokens such as 125 kHz RFID tags, which can easily be replicated and exploited by bad actors.

Stronger credentials include mobile identifiers or digital certificates that are signed and encrypted. Mobile devices can host additional information that supports user identification and authentication, such as a username, an organization, a facial image, and fingerprints. However, use of these data elements and any other personal identifying information should be kept to a minimum and included only as needed to comply with an organization's security and privacy policies.

The following sections describe some common credential types that can be used when mobile devices are used for physical access. These credential types include:

- Digital certificates
- Identifiers protected with asymmetric cryptographic keys
- Identifiers protected with symmetric cryptographic keys
- Unprotected identifiers

4.3.1.1 Digital Certificates

A digital certificate contains a public key, information identifying a certificate owner (e.g., user principle name [UPN] and distinguished name [DN]), and a verifiable digital signature of the certificate issuer (certificate authority) that is part of the trust framework. Ideally, asymmetric public and private key pairs are generated on mobile devices by apps that manage certificates and use them during the physical access control process. The public key is sent to the issuer as part of a certificate request. The private key is securely stored on the mobile device, never leaves the mobile device, and is used during authentication to verify that the device owns the public key. Typically, digital certificates are provisioned to the relying party's management systems during certificate issuance as part of a trust framework's enrollment or registration process. The relying party only permits physical access by those devices and users that it knows about and trusts.

During authentication, the digital certificate is validated against the issuer by the relying party, and the public and private keys are used to sign and validate a random challenge by the relying party, which proves that the mobile app controls the private key. In addition, these keys can also be used to establish encrypted communication channels between mobile devices and relying-party readers.

Examples of digital certificates in the public and private sectors that have the potential to be leveraged for physical access using mobile devices are derived Personal Identity Verification (PIV) credentials and mobile driver's licenses (mDLs). These types of digital certificates, and other X.509 digital certificate-based credentials, support medium and high assurance/confidence level authentication.

4.3.1.2 Identifiers Protected with Asymmetric Cryptographic Keys

Standalone public and private asymmetric key pairs provide the same capabilities as digital certificate public and private keys. The only difference is that no digital certificate is involved. Ideally, the keys are generated on the mobile device by a mobile app, and only the public key is shared outside of the device. During an enrollment or registration process, the public key is shared with an issuer; the issuer may

assign an identifier to the user or device, and both may be provisioned to a relying party. Alternatively, no separate issuer is involved, and the keys and identifiers are set up and configured by interacting directly with the relying party during a PACS-specific enrollment or registration process.

During authentication, the public and private keys are used to sign and validate a random challenge by the relying party. Trust framework policies determine whether identifiers are encrypted and decrypted during authentication. Examples of such identifiers are FIDO and FIDO2 credentials. Identifiers protected with asymmetric keys support high and medium assurance/confidence levels.

4.3.1.3 Identifiers Protected with Symmetric Cryptographic Keys

Use of symmetric keys requires the mobile app and the issuer to each generate a symmetric key (e.g., AES 256). The keys are shared as mutual shared secrets. These keys can be used to create session keys and establish a secure communication channel between a device and a reader. Within the secured session, user and device digital identities can be shared with a relying party and validated securely.

Symmetric keys must be managed so that only the relying party and the device know them. Security structures must eliminate any possibility that a third party can gain access to them.

Symmetric keys are tightly coupled credentials, along with any user and/or mobile device identifiers. Identifiers protected with symmetric keys support medium assurance/confidence levels.

4.3.1.4 Unprotected Identifiers

Some use cases may not require any protection during an access attempt. Identifiers and any other use-case-specific data can be exchanged between mobile devices and relying parties in the clear. Examples of such credentials are QR codes with an embedded identifier or transaction ID, or a display on the mobile device that can be visually validated by an attendant, e.g., a flash pass. Unprotected identifiers support low assurance/confidence levels.

4.3.2 Privilege and Authorization Attributes

In some cases, privilege/authorization attributes can be associated with a mobile-device-hosted credential, making them accessible to relying parties who first authenticate the user, and then granularly apply the attributes to further determine if the credential owner is privileged or authorized to access specific physical spaces within the relying parties' control. Attributes can include professional qualifications such as "EMT" or "firefighter" for use cases that limit access to only those individuals with specific skills. Credentials such as mDLs contain such attributes; e.g., only a driver with an mDL that contains a class designation that certifies them to drive vehicles with a gross vehicle weight rating greater than 26,000 lbs. may access a motor vehicle depot at a construction site or bring in equipment and supplies to a FEMA-controlled area hit by a natural disaster.

4.3.3 On-Device Credential Protection

On-device credential protection is critical for any identity credential, regardless of whether the credential is stored on a smart card or on a mobile device. Mobile device platforms (e.g., Android and iOS) offer OS-protected keystores/keychains that provide secure storage of sensitive data, such as online account usernames and passwords, and credit card information. Apple Pay and Google Pay are examples of apps that rely on device platform keystores and keychains to protect sensitive data. However, across these platforms, the protection of such sensitive information is not guaranteed to be stored in a hardware module, as is common with smart cards.

In addition to OS-managed keystores/keychains, mobile devices and mobile applications contain cryptographic modules, which can be either software or hardware based. The ideal approach is to leverage mobile device secure elements for those mobile devices that contain them and which are accessible by mobile device applications. A secure element is a tamper-proof chip that is part of the mobile device chipset, where the secure element ensures that cryptographic keys and other data are hardware protected, and only accessible under controlled authentication sessions utilizing strict protocols.

Secure element functionalities vary, depending on the device, but their intent is to provide a hardware-based module that:

- Provides storage of sensitive data, is tamper-resistant, can detect tampering, and can zeroize or destroy stored data when tampering is detected
- Contains a cryptographic engine that can generate symmetric and asymmetric keys
- Provides APIs to perform operations on stored symmetric and asymmetric keys without those keys leaving or being exposed outside of the secure element

NIST FIPS 140-2/3¹¹ specifies requirements for software- and hardware-based cryptographic modules. Modules are certified for meeting the requirements of one of four levels of security. Level 4 offers the most protection that can only be provided by a hardware cryptographic module, which would be contained in a secure element. Cryptographic module manufacturers can submit their products for testing by NIST, and mobile device manufacturers can select FIPS 140-validated cryptographic modules with a security level rating appropriate for their intended market.

¹¹ *Security Requirements for Cryptographic Modules*, NIST Information Technology Laboratory, FIPS 140-3, July 19, 2019, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>.

5 Use Cases

Technologies that can be leveraged for physical access control using contactless interfaces should be familiar. While not physical-access oriented, commercial offerings such as Apple Pay, Samsung Pay, and Google Pay allow users to pay for purchases by holding a mobile device up to a point-of-sale contactless reader. In most potential physical access scenarios, the user experience is similar.

Most of the use cases described in this section are based on contactless technology such as NFC, Bluetooth, WiFi, and cellular communications, but there are a few unique exceptions. Many of these use cases reflect current real-world implementations, while other use cases are provided to highlight the use of mobile devices for untapped scenarios for physical access.

Table 2 lists the use cases included in this section according to the assurance level required by each, and the types of credentials that may be used.

Table 2. Use Case Summary by Assurance/Confidence Level

Use Cases	Credential Types
High Assurance/Confidence Level	
Buildings Secure rooms Restricted areas Gates Hotel rooms Healthcare Cruise ships Entertainment venues College campuses Security escalation	Digital certificates Asymmetric keys Symmetric keys
Medium Assurance/Confidence Level	
Buildings Gates Residential access Hotel rooms	Digital certificates Asymmetric keys Symmetric keys
Low Assurance/Confidence Level	
Buildings Gates Entertainment venues College campuses	Simple identifiers QR codes Visual display

5.1 Buildings

Using smart mobile devices to control access to buildings improves both the user experience and the return on investment (ROI) for organizations that manage PACS. Replacing access cards or tokens with authenticated credentials on a smart mobile device reduces the risk of physical credentials being lost or stolen and of unauthorized access to a building or its secure areas. The cost of issuing physical credentials is also reduced.

Using mobile devices for building access control can streamline the issuance process and eliminate the need to procure and manage physical access cards. An organization's access control manager can assign a unique access credential that incorporates appropriate levels of access, including days, times, and areas of a building, to each authorized individual. Instead of an administrator having to issue a physical credential to a user, the system can send a message to an authorized individual—either an invitation to register the smart mobile device and begin using the mobile access credential system or an update to a previously authorized mobile access credential to change access areas, hours, or other parameters. Employees or guests can use their registered and authorized mobile devices for entry, and administrators can update access control systems either on site or remotely in near real time, which is especially useful in cases requiring temporary secure area access or employee termination.

Building access control administrators have a lot to manage, including equipment purchases, maintenance, and system configuration, without having to manage card or token issuance to every individual requiring access. The potential benefits of replacing the access card or token with an authorized and validated mobile device include:

- **Improved ROI or reduced cost of credential issuance:** With no physical card or token to issue, there is no need to purchase and manage card or token stock inventory.
- **Convenience and availability:** Smart mobile devices are less likely to be forgotten, lost, or misplaced than physical smart cards or tokens, and provide a more convenient and equally secure platform to host physical access credentials.
- **Improved access security:** Once registered and assigned, access authorization is located on an individual's smart mobile device and secured through a unique PIN or biometric access.
- **Improved credential management:** Authorized administrators can manage credentials remotely and in real time, managing a variety of rights, including employee access, authorized visitor and guest access, and temporary secure area access.

Using smart mobile devices to control physical access into buildings can be a strong component of a proactive security approach. With contactless technology, stronger credential issuing processes, and better credential management, the use of smart mobile devices is quickly becoming the new standard for physical access control.

5.2 Secure Rooms

How a secure room is established and certified varies by use.

A secure room in a privately owned facility is typically established to store files or to serve as a sensitive compartmented information facility (SCIF). Secure private rooms also include money rooms and private conference rooms. Secure rooms in federal facilities are established to support the business needs of the occupying agency and include rooms such as judge's chambers, holding areas for law enforcement, contracting offices, secure conference rooms, and SCIFs.

Government SCIFs require both accreditation at the time of construction and periodic recertification. To be certified, SCIFs must meet stringent requirements, and certain standards must be maintained to retain certification. Electronic devices such as notebook computers, tablets, mobile phones, and cameras are prohibited both inside of a SCIF and at the entry point just outside the SCIF. Regulations prohibit the use of mobile devices to control access to a government SCIF.

Companies doing business with the federal government may find it necessary to establish work areas or conference rooms that meet the same requirements as a SCIF. If commercial space is accredited as a SCIF, mobile devices would be prohibited.

Other commercial secure spaces, such as file storage rooms or other storage areas, represent an opportunity for using a mobile device to control access, as long as there is no conflict with the operational policies governing the space. Typically, access to file storage rooms or storage areas is restricted to specific individuals needing to enter the space to perform routine duties.

Security policies and operational regulations are key to considering whether to use a mobile device to control access. If the secure space prohibits the use of portable electronics, mobile devices are probably not a viable solution. Conversely, if there is no limitation on portable electronics, mobile devices may be a potential solution for granting access.

5.3 Restricted Emergency Areas

In the event of a disaster, it is often necessary to establish a secure perimeter around an affected area. Trusted personnel must be given access to the area as efficiently as possible, while unauthorized individuals are excluded. There may also be zones within the affected area that require more severe restrictions. The ability to manage and monitor entry to and exit from each zone is vital to ensure personnel safety and to secure the premises and the assets within an area. Physical access measures apply not only to persons entering a controlled area, but also to their ability to obtain items such as secure equipment containers and specialized tools.

In this environment, mobile devices represent an excellent solution to the numerous challenges presented by an emergency response:

- Speed is of the essence, but security is also crucial.
- Certain first responders should be granted access before they arrive on site, to avoid lines for registration.
- Unknown accredited first responders must be processed quickly to verify their credentials and be given the correct level of access to each zone and asset.
- Previously unknown specialists may need to be granted access.
- Often the location of each person within the perimeter should be tracked.
- Individuals may arrive at the perimeter with a wide range of non-interoperable identity credentials and devices.

To meet these requirements, it is clearly beneficial to be able to assess whether an applicant should receive access permissions and to provision a consistent, interoperable credential rapidly. Historically, this requirement has been handled by issuing temporary smart cards or by registering existing cards with a centralized service and using dedicated handheld devices to validate privileges against a regularly updated list of authorized personnel. However, a combination of derived mobile credential issuance, remote provisioning, and online enrollment capabilities represents a much better technical solution.

A combination of the PACS verification techniques described in this white paper can be used to manage access once a credential has been issued. The process could include both static and roaming authentication infrastructure and could also incorporate geofencing techniques in situations where a physical barrier is impractical.

Restricting access to emergency areas then becomes an issue of verifying identity and provisioning credentials securely. Access credentials can be pushed automatically to devices belonging to registered

emergency response officials before the officials arrive at the site. Other responders can receive a credential on their phone following (for example) verification of a currently trusted card, either on site or remotely.

It is likely that some disasters will cause severe disruption to cellular networks, but this risk can be mitigated by choosing technologies such as WiFi, Bluetooth, and NFC to allow effective offline use of mobile credentials. Initiatives such as the FirstNet LTE can also help limit the effect of overloading public networks in these circumstances.

This approach minimizes on-site authorization delays, saving valuable time during the critical initial stages of an emergency without compromising security.

5.4 Gated Buildings and Parking

Commercial vendors have implemented a variety of ways to use credentials on a mobile phone for access to gated buildings and parking. Current solutions use Bluetooth, WiFi, and NFC protocols for presenting an identity token to an access control reader.

One example uses Bluetooth communications and the secure element (SE)¹² on a phone to access an employee-only gated parking lot by car. At about 25 feet from the access gate, the employee simply waves the phone in the air (some technologies allow for the use of the gyro on the mobile device) to present the credential in the SE to the reader for authentication and authorization. The gate opens before the driver arrives.

NFC technologies and the SE or a token on the phone can be used when the person is closer to the access point. For example, an outside door can be opened by placing the mobile phone against an NFC reader. The credential in the SE or token is authenticated by the system and opens the door.

Finally, WiFi solutions are available that allow users to connect to a network. When moving around inside a building (for example, walking from the accounting department to the marketing department), the SE or token is presented to the WiFi network (possibly invoking geofencing policies), user-authentication and movement-policy rules are applied, and a door is automatically unlocked as the user approaches the door.

Literally dozens of access control solutions on the market today use variants of the scenarios described above to use mobile devices to control employee or visitor access to parking lots, garages, and buildings. Individual use cases must be analyzed to determine suitable technologies and associated costs.

The level of embedded security must be evaluated as well. In the early 2000s, ID badges predominately used proximity technology for building access. This technology turned out to be an inexpensive solution, but hackers quickly realized they could purchase a cheap proximity card duplication device and simply clone a card. In addition, the proximity communications protocol was clear text, so it could be scanned, and the contents cloned onto a new card easily. The use of a mobile device enables all relevant solutions on the market today to employ encryption elements and session protocols during the authentication process.

5.5 Guest Access to Gated Communities

Gated communities face special challenges in granting access to visitors, particularly since access is typically given to a vehicle rather than to the individual passengers in the vehicle. One such use case in

¹² See Section 4.3.3 - On-Device Credential Protection.

North Texas requires a large number of vehicles to access the location at peak times when overflow traffic backs up into nearby intersections.¹³

Critical to this use case is the ability to ensure that resident vehicles can come and go quickly. This requirement is met using public toll tag vehicle window stickers that residents use to pay tolls on state toll roads. The states of Texas and Oklahoma use a common technology and unique numbering system for billing users of the various toll roads in the two states. Gated communities can register these RFID toll tags into an access control system that uses appropriate readers and motorized gate arms for rapid automated access into lanes restricted to residents. This interoperability means communities do not have to worry about vehicle credential management or cost. Such facilities simply enroll the toll tag stickers.

For visitors, however, there is a need to process access requests quickly to avoid backup onto the main streets. If processing is slow, visitor vehicles may have to be diverted to the resident gate, which inconveniences residents and contributes to additional backup.

One solution requires a resident to register a visitor in advance, using technology that sends a pass to the visitor's smartphone. The pass displays a QR code. Guards are equipped with iPads hosting an app that supports a wireless scanner and is connected to the telephone company's wireless infrastructure. When visitor traffic is heavy, guards can walk to the vehicles in line and validate authorization by scanning the QR code, while other guards process vehicles waiting at the guard house for phone confirmation by the resident being visited.

A major benefit of the QR code system is that when the QR code is scanned and access granted, the system sends an SMS message notifying the resident being visited that a visitor is about to arrive. Previously, many residents would not notify the guards in advance about a visitor because they forgot, they did not know when the visitor would arrive, or they simply wanted the guard to call them for approval, thereby getting a heads-up notice of the visitor's arrival. This situation was undesirable; the resident was not always reachable by phone, and the guard had to hold up the line of vehicles while trying to reach the resident.

This use case uses the mobile phone in multiple ways:

- The resident registers a visitor, sending an SMS message containing a QR code to the mobile device.
- The visitor presents the QR code to the guard, who quickly scans and validates it.
- The guard can scan the QR code with a smartphone as a backup to the iPad, if necessary.
- The visitor management system notifies the resident's smartphone that the visitor has arrived.

This solution has multiple benefits:

- Faster visitor throughput without traffic backup
- Courteous and prompt visitor processing
- No requirement to reach a resident for approval
- Notification of residents when the visitor is approaching

¹³ Source: Access Control Council, Rob Zivney, Identification Technology Partners.

The QR code can be designated for multiple use or multiple days, thus saving the cost of issuing multiple paper passes.

5.6 Hotel Rooms

In an effort to improve customer convenience, hotel chains have developed (and continue to develop) infrastructures that enable their customers to use mobile devices to access hotel rooms. Hotel guests can choose to have a room key delivered over-the-air to an NFC- or Bluetooth-enabled mobile device. They must first accept an invitation to download an app from the issuing hotel chain and download the app (the app can also be used to make reservations at hotels of the same brand). The specific device is then registered to the issuing hotel system using a mutual authentication protocol. The issuing hotel system maintains a record of the specific mobile device as part of the hotel's loyalty program. The guest's phone number, email address, and name are also part of the record, as in the loyalty program.

Once the reservation is completed, the reservation details are sent to the phone. Digital room keys are downloaded and validated for the period during which the guest stays at the hotel. On the arrival date, a room number is sent to the mobile device and displayed on the screen. When the guest arrives at the hotel, there is no need to check in at the counter. The guest simply goes to the room, opens the hotel app, and presents the mobile device to the lock on the door.

The hotel must have implemented over-the-air infrastructure and installed NFC- or Bluetooth-enabled locks on room doors. Guests who prefer using traditional cards issued at the registration desk can be accommodated using 13.56 MHz or similar high frequency cards.

5.7 Healthcare Facilities

The use of mobile devices to control physical access to healthcare facilities and deliver safer care is increasing. Healthcare organizations share many of the same physical security use cases as other organizations and industries. As the use of smartphones, tablets and other mobile devices expands, the use of such devices for physical security at healthcare facilities could also expand. Healthcare delivery is managed not only by doctors, nurses, and medical assistants, but also by emergency management personnel and healthcare administrators—all of whom use mobile devices daily in both their professional and personal capacities.

Healthcare facilities are typically thought of as hospitals and doctors' offices. However, modern healthcare facilities include other facilities, such as community care, medical research, and health information technology facilities. Mobile devices can be used to control access to both common care delivery facilities, such as doctor's offices and hospitals, and to these other care facilities as well, increasing security. As is true for other industries, electronic physical access control systems can protect healthcare facilities and keep personnel safe.

The benefits of using mobile devices to control access to healthcare facilities include mitigating facility and parking lot security incidents, and monitoring employee and visitor interactions. Most hospitals require 24-hour public access. (While other industry sectors may require 24-hour access, such access rarely includes the public.) Healthcare facilities also have to control pharmaceutical drugs and protect against infant abductions.

During a viral disease pandemic, medical facilities are on the front line of patient treatment and disease spread. Use of mobile devices can help minimize the number of disease touch points in medical facilities by preventing contact with door handles, push bars, keyboards, and keypads.

In the near future, use of mobile devices may extend beyond the common healthcare facilities to include all healthcare facilities, including tertiary and specialty care facilities. These additional facilities can include dentists, therapists, and hospice care. Use of mobile devices to control access and manage both patient and employee identities electronically can provide stronger physical security, better access control, and improved personal safety.

5.8 Cruise Ships

Cruise ships represent another opportunity to use mobile devices to control access. It often takes 75 minutes for passengers to check in for a cruise, a time period that may involve waiting in multiple lines and holding areas – a very long time for passengers eager to start their vacations. Royal Caribbean Cruises has proposed an answer to getting passengers aboard faster: AI-powered facial recognition.¹⁴

In December 2019, passengers started taking part in a pilot program at a company embarkation point in Ft. Lauderdale, Florida. Before reaching the port, passengers use the company's app to take selfies with their own smartphones. After uploading the selfie and scanning their passport, passengers using the system can go to the port. When they arrive, passengers are directed to assemble under a live view of themselves that is captured by cameras arrayed across the entrance and projected on screens. The screens are arranged to avoid bottlenecks. Behind the scenes, a computer uses an AI-powered database to compare the face of each passenger in port to the selfie provided by the passenger. Once there is a match, a green box is displayed on the screen around that passenger's face. As the passenger boards, a welcoming agent verifies the match, greets the passenger by name, and checks the passenger's passport. Finally, a cruise ship staff member directs the passenger to the assigned cabin.

"We wanted to turn what was a cold transaction into a really welcoming moment," said Jay Schneider, who runs the company's digital operations. The goal is to get passengers "from car to bar in 10 minutes."

Because cruise ships are required to have passenger photos, use of a facial recognition system does not add significantly to the amount of data the company must collect and manage. And the result is a system that whisks passengers aboard and gets the holiday started quickly. "Guests didn't feel like they were on vacation until day 2," Schneider said. "We wanted to give you that day back."

5.9 Entertainment Venues

For entertainment venues of all types, from theme parks to sports stadia to concert venues, convenient, secure access control is important for safety and revenue protection. The infrastructure, security attendants, and logistics required by current paper-based ticketing and access control are becoming increasingly inconvenient and expensive.

Entertainment venues have for years suffered from a number of access control issues (see sections below) that can be addressed by adopting secure mobile credentials to manage visitor and staff access to venues. The benefits of mobile credentials for entertainment venues include being able to:

- Easily detect counterfeit tickets

¹⁴ "AI On Cruise Ships: The Fascinating Ways Royal Caribbean Uses Facial Recognition And Machine Vision" Bernard Marr – Contributor 'Enterprise Tech' - May 10, 2019, <https://www.forbes.com/sites/bernardmarr/2019/05/10/the-fascinating-ways-royal-caribbean-uses-facial-recognition-and-machine-vision/#479b50ae1524>; "Huge leaps in AI have made facial recognition smarter than your brain", Stephen Shankland March 28, 2019, <https://www.cnet.com/news/huge-leaps-in-ai-have-made-facial-recognition-smarter-than-your-brain/>

- Control after-market sales to allow genuine resale but detect ‘ticket touts’
- Enable “just in time” purchases
- Reduce ticket theft by enabling remote ticket cancellation
- Permit easy ticket refunds and cancellations without the risk of fraud due to time delays in notifying the venue of a refunded ticket
- Support re-entry arrangements – the ticket can be swiped in and out of the venue
- Improve entry/exit velocity by automated ticket validation
- Support attendee tracking within the venue

Partial solutions to a number of these problems are already deployed, but most lack the security that is needed to minimize fraud and evasion. For example, static QR codes are widely used for access but are easily forged, intercepted, and copied.

5.9.1 Counterfeiting, After-Market Sales, and “Just in Time” Passes

Two allied problems — counterfeit detection and after-market sales management — are well known to anyone trying to get tickets for a popular event. Printed tickets are easy to copy or replace with a counterfeit that looks legitimate, since there are often multiple ticket styles for the same event. Criminals are able to purchase actual tickets in bulk, using online bots to avoid detection, and then sell them at grossly inflated prices. However, genuine ticketholders also often want to sell tickets for legitimate reasons. A convenient, secure way of doing so would provide advantages to the venue operator, event promoter and the ticketholder.

Binding a cryptographically secured ticket or entry pass to a mobile device and enabling physical access control using NFC or Bluetooth can stop counterfeiting and enable entry passes to be transferred using a trusted broker who is sanctioned by the venue operator or event promoter. Anyone buying a ticket could also validate its authenticity directly.

When an entry pass is immediately available on a mobile device, instant online purchase and secure automated access are simple. This means that one could purchase a new ticket or upgrade an existing one while in line for the event. When a ticketholder cannot attend due to a last-minute problem, their ticket could instantly be resold to someone at the door.

5.9.2 Theft, Refund, and Cancellations

Enabling live challenge-response validation at a physical point of entry simplifies the problem of how to address ticket theft and fraud. The validity of an entry pass can be verified immediately. If the entry point has full connectivity, a direct check against backend systems is straightforward. Where such infrastructure is not possible, an “expiring validation token” could be used. This solution addresses the problem of tickets being cancelled and refunded before the paper tickets are presented at an offline gate. For example, a passholder may be required to validate the pass on line 24 hours before attending. A 48-hour entry token is then downloaded to the passholder’s phone, and the ticket is marked as nonrefundable for the next 72 hours. The passholder can only enter the venue using the short-lived entry token, which itself cannot be revoked.

This solution has the added benefit of requiring fewer staff at entry points, as entry rights can be determined without requiring manual examination of tickets.

5.9.3 Throughput, Re-entry, and Tracking

Fully automated systems facilitate traffic flow at entry and exit points, as has been proven through the use of less secure technologies such as static QR codes. The use of a mobile PACS solution offers the same benefit while improving security and convenience.

Controlling re-entry to venues is frequently challenging, and although putting re-entry tokens onto a phone at the exit point is possible, additional fraud mitigation measures would be needed. For example, two people could enter, then one person leaves with both phones and a third person could enter on the spare re-entry token. However, use of a mobile device to control re-entry will still probably be more secure than the traditional “ink stamp on the back of your hand” approach.

In some situations, it might also be useful to grant additional access privileges to individuals and track those individuals within a facility. For example, a football stadium might permit season ticket holders and VIPs to access a special enclosure and offer instant “VIP for a day” prizes.

Tracking visitors using BLE beacons in conjunction with mobile device door access control may also be valuable in secure areas such as back-stage or facilities maintenance areas.

5.10 Airport Passengers and Employees

Aircraft operators, airport authorities, and the airport security operations are considering the use and acceptance of digital identity credentials for physical access to controlled areas. Digital identity credentials held on a mobile device can facilitate such uses. These controlled areas include access past the airport security checkpoint into the airport “sterile” area, airport control towers, airport security offices, tarmac areas (e.g., vehicle depots), and other internal secured areas. The populations accessing the access-controlled areas include the general aviation passengers, local airport staff airport authority staff, local airport vendors staff, local aircraft operator staff, aircraft operator staff not based at a local airport, law enforcement, and other contractors. For each population, specific risk-based considerations need to be accounted for in regard to the issuance, provisioning, authentication, and management of the identity credentials.

5.10.1 Airport Passengers

Passenger identity transactions are at booking, bag drop, the security checkpoint, and boarding. At booking, passengers manually enter their personal information to reserve their ticket for travel. This information may also be passed to airport security agencies for vetting purposes. Using a mobile digital credential during the reservation process can help improve the customer user experience by simplifying the reservation and assuring proper data is submitted to the airline. Data fidelity during the reservation process will also ensure that the biographic data included on the boarding pass or stored in the security agencies’ flight manifest match the biographic data that will be presented at the security checkpoint. When the data does not match, passengers may be subject to extra screening or may not be permitted past the security checkpoint until the airline reconciles the mismatched biographic data.

At the security checkpoint, identity verification is a critical aspect of the security screening process that ensures that only those who need to be screened are being screened and that those passengers are getting the proper level of screening. The use of digital identity credentials at the checkpoint could lead to improvements in efficiency and overall security effectiveness. Digitizing the identity transactions can lead to opportunities for automation that could lead to higher passenger throughput per screener hour. Furthermore, the digitization of the transactions, if backed by a robust, standards-based, interoperable

digital trust framework, would be an enhancement in security, helping security screeners to have higher assurance that the data presented is authentic and has not been altered.

Other identity touchpoints for passengers are at the bag drop counter, airline lounges, and boarding gate. At the bag drop counter, passengers must present valid IDs to check bags onto a flight. Ticket counter agents check the identification to verify the person checking the bag has a reservation for the flight the bag is being checked on. As previously discussed for identity transactions at the security checkpoint, digitizing the identity transaction could lead to efficiency and security improvements through automation and higher trust in the credential being presented. For boarding and/or access to other passenger amenities, passengers could use their digital credential to directly access these facilities and/or pass various data elements that would allow an airline to stage the data, like a photo, for a tokenless boarding or entry. In all cases, passengers could have a more reliable and seamless experience while airlines would have higher assurance that they are providing services to those who are permitted to have access to various amenities.

The Transportation Security Administration's (TSA) strategy is to leverage electronic IDs (eIDs), including mobile driver's licenses (mDLs), based on ISO 18013-5.¹⁵ This standard leverages images and other personal data elements displayed or transmitted using international standards-based mobile radio technology (NFC, WiFi, Bluetooth, and wireless networks).

5.10.2 Airport/Airline Employee Access

Employee access in the airport currently involves presenting site-specific and/or employer-specific badges based on the area being accessed. Access to these areas is currently a combination of swipe, RFID presentment, or physical ID authentication by a human. Digital credentials could be used to provide strong authenticated access. The current use of an assortment of site-specific and/or employer-specific credentials causes many management and interoperability issues and can create complexities in managing access, as employees may need to carry multiple badges for access. Digital identity credentials, on the other hand, can help simplify access management by creating a derived digital credential to be stored in a mobile wallet or by creating digital attributes/tokens that could be attached to the foundational digital identity along with a foundational digital identity document, like a state-issued mobile driver's license. Authentication and access would be granted and managed based on the interoperable trust framework.

Airports also use mobile devices (in NFC Reader Mode) for "temporary door access" (e.g., during construction, PACS reader out-of-service, atypical operations) using standing security officers to monitor and control access using a mobile device. In this use case, the mobile device app uses NFC configured in the "Reader Mode" and encrypted WiFi communications with the existing PACS database. Users present their existing PACS credential to the mobile NFC device which reads the credential, pulls the associated user record from the PACS database, and electronically validates the credential ID and authorizations via the NFC reader challenge/response with the credential. In addition, the user photo is displayed on the smart mobile device for the security officer to visually confirm the user ID credential. The standing security officer then indicates the user entry/exit via the mobile device that logs the event in the PACS history database.

¹⁵ Source: TSA

5.11 College/University Campuses

Aging PACS at many colleges and universities urgently need to be upgraded, according to a survey of 1,800 higher education security and IT professionals conducted by Genetec and HID Global.¹⁶ The survey shows that 33.76% of readers, 30.6% of controllers, and 24% of software applications are over six years old. Older technologies, such as barcodes, magnetic stripe, and 125kHz low-frequency proximity, still dominate these physical access control systems. More than half of survey respondents still rely on magnetic stripe and almost a quarter still use 125kHz proximity. A total of 64% of the survey respondents said their current access control system malfunctions on occasion.

However, more than a third of the survey respondents (35%) are ready to embrace more modern technology as a way of improving the experience for students, faculty, and administrators. Over half of the respondents (54.2%) would be interested in using their access control credentials to support applications beyond physical access, and 44% stated that better integration with other security systems/components is a key driver for upgrading their access control systems.

Most colleges and universities want their students to use a single card or mobile credential for multiple applications, such as accessing dormitory rooms, checking out books from the library, locking bicycles, and paying for food, parking, and other items.

5.11.1 Real World Examples

Three university pilot projects showcase the benefits of using NFC-enabled smartphones to open doors at universities and in other campus environments: Villanova University, the University of California San Francisco (UCSF), and Arizona State University (ASU).¹⁷ Groups of students and staff can access campus residence halls, facilities, and selected rooms using NFC and credentials embedded into a variety of popular smartphones connected to the major mobile networks.

To open a locked door, participants present their phone to a door reader, just as they currently do with a student ID card. All participants are using their phones for residence hall access, and some are also using them, along with a unique digital key and PIN, to open individual dorm room doors. The technology also supports over-the-air provisioning and management of digital keys, which simplifies administration of the PACS.

These projects highlight the potential for the application of NFC technology to physical access control applications. Villanova, UCSF, and ASU are helping the security industry validate the idea that bringing mobility to access control improves security while enhancing the user experience, making it easier to deploy and manage keys, and making it more convenient to carry them. Any door that is currently opened with a physical key or student ID card can be opened with a smartphone using NFC technology.

Approximately 80% of the student participants reported that using a smartphone to unlock a door was just as convenient as using an ID card. Nearly 90% said they would like to use their smartphones to open all doors on campus. While these pilot projects focused on physical access, nearly all participants also expressed an interest in using their smartphones for other campus applications, including access to the student recreation center and laundry, as well as use for transit fare payment and meal, ticket, and

¹⁶ Genetec press release, “Genetec and HID survey shows higher education institutions ready to move from legacy access control systems and embrace new technology”, Genetec & HID, August 2020, <https://www.globenewswire.com/news-release/2020/08/20/2081430/0/en/Genetec-and-HID-survey-shows-higher-education-institutions-ready-to-move-from-legacy-access-control-systems-and-embrace-new-technology.html>.

¹⁷ See multiple references for the Villanova, ASU and UCSF use cases in Appendix B.

merchandise purchases. "When I first saw this technology used in other applications, I recognized the benefits it could bring to a university campus," said Laura Ploughe, Director of Business Applications and Fiscal Control, University Business Services at Arizona State University. "Today's students are so technologically advanced that it is second nature for them to put everything on their phones and, most of the time, it's already in their hands while walking across campus," explains Kathy Gallagher, Director of the Wild Card Office at Villanova University. "We want to provide our students the utmost in convenience and flexibility through the technology we offer. It's easier for students to use an app on their phone versus digging for their card."¹⁸

The most common comment from students was "I sometimes forget my keys, my ID, my watch, my wallet... but I NEVER forget my phone!!"

5.11.2 ROI Benefits

Villanova University has saved a substantial amount of money by replacing combination and keyed locks with mobile-phone-activated doors, reducing the costs of rekeying dorm rooms each year. The school has also reduced the number of lockouts, because students seldom leave their mobile phones in their rooms. Another saving is the elimination of the need to rekey locks if a master key is lost. The centralized room-key management system makes the annual changeover and other key related actions, such as issuing one-day permissions, both less expensive and easier.

5.12 Extraordinary Circumstances

This white paper project started before the COVID-19 crisis but was completed during the pandemic. While COVID-19 has dramatically decreased the use of physical access points, the pandemic has emphasized the significant safety benefit of using contactless mobile credentials, and the number of organizations implementing such systems is expected to increase accordingly. While many organizations will see fewer individuals entering their buildings on a regular basis, the need to permit authorized access will still be necessary.

Although COVID-19 moved many workers to alternate work locations, such as their homes, essential personnel must still enter buildings—but now the focus is on high-contact areas. Government agencies and private businesses are faced with a new challenge: how to continue to provide secure access but in such a way that contact with access control hardware is minimized. In facilities requiring multifactor authentication, temporary operational changes can substitute use of single factor authentication, in the form of a contactless card read or even a mobile device that acts as a token to identify the person requesting access. Other mitigating controls, such as adding security personnel to entryways and reducing the number of entrances and exits to a facility, could be used temporarily to ensure that there is no degradation in security.

¹⁸ "College Students Favor Smart Phones as Access Control Credential," Locksmith Ledger International, May 2, 2012, <https://www.locksmithledger.com/home/article/10694572/college-students-favor-smartphones-as-access-control-credential>

6 Mobile Devices and Relying Party Interfaces

Mobile device interfaces used for user and device authentication for physical access typically rely on contactless interfaces. In the access modes presented in this section, “contactless” connotes both device-to-reader and device-to-human interaction. In most scenarios, a relying party or PACS presents a hardware reader device at an access point with which a mobile device interacts to allow a user to physically transition into a controlled space. In some access use cases though, there is no physical reader device. Rather, there is a human attendant that may be the only authenticator to allow access by a user.

Figure 7 lists the primary contactless interfaces and the communications services that mobile devices commonly possess to support authentication with physical access relying parties.








Primary Contactless Interfaces	Supporting Interfaces and Services
 Near Field Communication (NFC)  Bluetooth Low Energy (BLE)  Camera  Display	 WiFi  Cellular Services  Push Notifications

Figure 7. Mobile Device Contactless Communications Interfaces

Traditional physical access relying parties are typically based on contact and/or contactless readers at access-control points of entry. Figure 8 shows a configuration for such traditional systems, which are usually based on smart cards, RFID tags and other tokens that contain some form of verifiable credential.

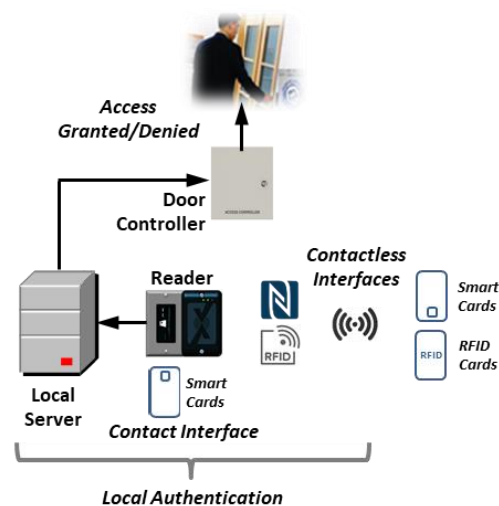


Figure 8. Traditional Relying Party PACS Architecture

In contrast to Figure 8, Figure 9 depicts a notional physical access relying party configuration where mobile devices are used in place of traditional physical access tokens and credentials. In this configuration, mobile devices support both local and remote credential authentication using near-range

(BLE, NFC and QR codes) and long-range (WiFi and cellular access) contactless communications. This configuration model addresses the concept of attended and non-attended scenarios, where there may or may not be a human attendant involved during attempts by users to gain access to controlled physical areas.

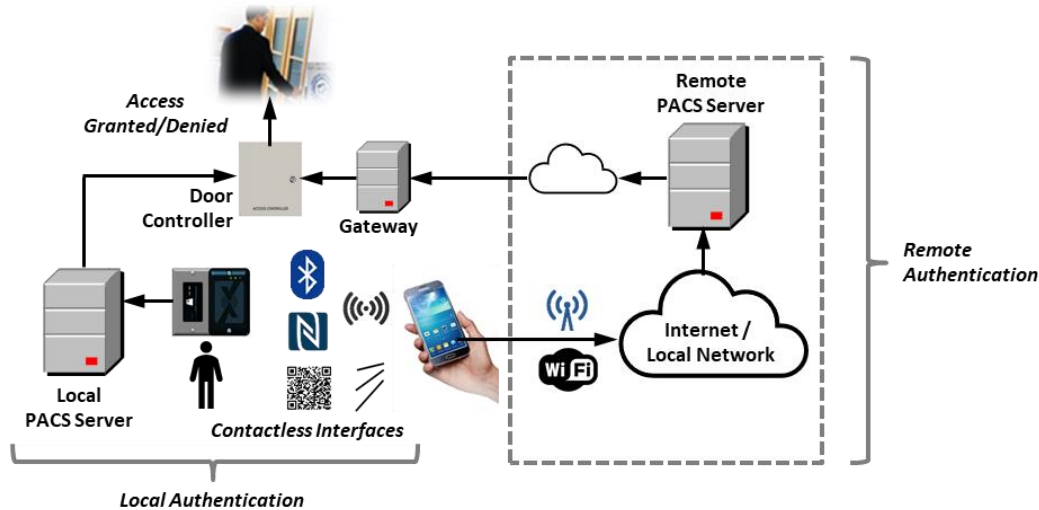


Figure 9. Mobile-Enabled PACS Relying Party Architecture

6.1 Mobile Device Interface Modes

Relying parties have a variety of options for defining and configuring how mobile devices interact with readers, backend systems and attendants that may be involved with mobile device credential authentication. Various contactless interface modes support individual use cases in these configurations. This section provides examples of interface modes that can support local and remote mobile device credential authentication.

Table 3 illustrates the variety of interface modes that mobile devices can use for “local” authentication. These modes use NFC, BLE, QR codes and mobile device screen displays as the primary contactless interfaces to present mobile device credentials to relying parties.

Table 3. Local Authentication Interface Mode Examples








Local Authentication Modes	
Interface Mode	Notional Interface Depiction
<p>Near-Field Communications (NFC): The user presents the mobile device to a reader at an entry point. The mobile device app transmits credentials and identifiers to the reader via NFC short-range contactless communications. The reader/server authenticates the credential through the NFC interface.</p>	
<p>Bluetooth Low Energy (BLE): The user presents the mobile device to a reader at an entry point. The mobile device app establishes a BLE connection with the reader and transmits credentials and identifiers to the reader via BLE mid-range, encrypted, contactless communications. The reader/server authenticates the credential through the BLE interface. Note that since BLE has a range of 100+ meters, entry points would need to be separated by at least that distance so that the mobile device app does not get confused with one or more nearby/adjacent BLE-enabled entry points. Alternatively, the mobile device app must have previous knowledge of the BLE beacon identifier of the entry point that it is intending to access, and/or the mobile device is paired or bonded to the BLE reader prior to access attempts.</p>	
<p>NFC Tag and BLE: In this NFC-BLE hybrid mode, an NFC tag posted at a door or entry point is scanned by an app on the user's mobile device. The NFC tag contains an entry-point identifier, BLE beacon identifier, BLE pairing/bonding information, and other relevant parameters. The mobile device uses the NFC data to establish a BLE encrypted session with the reader. The mobile device app transmits credentials and identifiers to the reader within the BLE session. The reader/server authenticates the credential through the BLE interface. Note that using an NFC tag in conjunction with BLE eliminates the issues with using BLE only, as described above.</p>	
<p>QR Code Display and Camera: The user presents a QR code displayed on their mobile device to a fixed camera or an attendant who has a mobile device app that scans the QR code. The credential (e.g., identifier or transaction code) extracted from the QR code is authenticated by a local or remote backend service, or by an attendant's offline mobile app, which matches the scanned credential against a stored list of valid credentials.</p>	
<p>Flash Pass: The user presents a formatted pass displayed on their mobile device, which is visually verified by an attendant.</p>	

Table 4 illustrates the variety of interface modes that mobile devices can use for “remote” authentication to physical access relying parties. These modes use NFC and QR codes to gather information related to the entry point, which mobile devices can then use to establish remote connections (via supporting WiFi or cellular communications capabilities) to backend physical access services. Backend services authenticate mobile device credentials through the remote interfaces and determine whether users may gain access to managed physical spaces.

Table 4. Remote Authentication Interface Mode Examples

Remote Authentication Modes	
Interface Mode	Notional Interface Depiction
<p>NFC Tag and Network: An NFC tag posted at a door or entry point is scanned by an app on the user’s mobile device. The NFC tag contains an entry-point identifier and other relevant parameters. The mobile app sends (via WiFi or cellular service) the scanned NFC tag data along with a prestored credential to a backend service that authenticates the credential and checks an access control list to verify that the user is authorized to access the entry point.</p>	 <p>The diagram illustrates the NFC Tag and Network mode. On the left, a blue square icon labeled 'TAG' with a white 'N' symbol represents the NFC tag. A hand holds a smartphone, and a blue signal line connects the tag to the phone. From the phone, a blue signal line connects to a cloud icon labeled 'WiFi', which then connects to a server rack icon on the right.</p>
<p>QR Code Tag and Network: A QR code posted at a door or entry point is scanned by an app on the user’s mobile device. The QR code contains an entry-point identifier and other relevant parameters. The mobile app sends (via WiFi or cellular service) the scanned QR code data along with a prestored credential to a backend service that authenticates the credential and checks an access control list to verify that the user is authorized to access the entry point.</p>	 <p>The diagram illustrates the QR Code Tag and Network mode. On the left, a QR code icon is shown. A hand holds a smartphone, and a blue signal line connects the QR code to the phone. From the phone, a blue signal line connects to a cloud icon labeled 'WiFi', which then connects to a server rack icon on the right.</p>

7 Mobile Device Support for Multifactor Authentication

The interface modes discussed in the previous sections can be supplemented with additional factors of authentication. The commonly accepted (traditional) model for multifactor authentication consists of “something you have,” “something you know” and “something you are.”

- **Something you have** – In the context of using mobile devices for physical access, the mobile device and the provisioned credential constitute the “something you have.”
- **Something you know** – PINs, and passwords, for example, can augment authentication assurance during access events. They can be used to unlock the credential hosted on the mobile device, or can be conveyed to a relying party, based on a preconfigured shared secret, where the relying party verifies the shared secret.
- **Something you are** – Biometrics such as fingerprints, facial images, iris scans, and voice samples can be used in a similar fashion to PINs and passwords. That is, they can be used to unlock credentials hosted on the mobile device through built-in mobile-device biometric-capture and comparison features. Alternatively, the mobile device can capture the biometrics and securely send them to the relying party, where “server-side” biometric comparison can be performed during physical access events.

7.1 Enhanced Mobile Device Authentication Factors

Through their diverse feature sets, mobile devices provide functionality that goes beyond the traditional three-factor authentication model. The following sections touch on enhanced authentication factors that mobile devices can provide via their communications connectivity capabilities and the various sensors that these devices possess across the mobile device landscape feature sets.

7.1.1 Push Notifications

Authentication based on push notifications is gaining popularity, because it provides a simple means to authenticate users, especially when used without the need for passwords. Push notifications authenticate a user by confirming that a device registered with the authentication system is in fact in the user’s possession.



Push authentications provide additional benefits to the interface modes described above. Push notifications are generated by backend services, enabling user authentication by sending a notification directly to the user or a mobile app on the user’s device, alerting them that an authentication attempt is taking place. A notification may result in additional authentication steps that need to be acted upon, such as entering a one-time passcode at an entry point reader or leveraging biometrics for multifactor authentication. Notifications can be sent in-band or out-of-band, using any number of communications channels.

When a person registers an account, the account is linked to a mobile device the user owns. To log in to the account, the user submits a username or ID. A notification is sent directly to a secure app on the user’s device (typically a mobile phone), alerting the user that an authentication attempt is taking place. Users can view authentication details and confirm access, typically using a biometric such as a fingerprint. Notifications can be sent in-band or out-of-band, using any number of communications channels.

There are several benefits to push notification authentication:

- Users do not need to memorize and manage passwords.
- Notifications provide a seamless and user-friendly experience. Instead of fumbling with a phone to find and open an authenticator app, users can validate their log in immediately, using the authentication request that comes to them.
- Validating an authentication request is often speedier than entering a complex password.

Push notifications can also be used to inform a user that a credential is about to expire or has expired, or has been revoked.

7.1.2 Leveraging Mobile Device Special Features for Multifactor Authentication

As discussed in Section 3, mobile devices also include an assortment of sensors and miscellaneous capabilities. Some of these sensors and capabilities may be used to provide unique authentication factors in addition to the traditional three-factor authentication model. For example:

- GPS could be used for a “somewhere you are” authentication factor, perhaps to confirm that a user is actually at an authentication reader installed at an entry point.
- Sensors, including gyro, accelerometer, pedometer, and proximity sensors, could be used to support behavioral “something you do” authentication, to establish gesture and movement profiles.
- Heart rate and blood pressure sensors could be exploited to establish a “something else that you are” physiological biometric profile.

While use of these atypical authentication factors is both innovative and futuristic, the factors highlight the extraordinary technologies that can be packed into very small, affordable, and pervasive form factors.

8 Conclusion

Mobile devices, especially smartphones, provide versatile credential hosting platforms that can be employed in a wide range of physical access control use cases. The features provided by these devices support secure credentials that, if implemented correctly, are resistant to cloning, forgery, and alteration. In addition, these devices can protect access to the most secure access control areas with high levels of assurance, due to the implementation of tamper-resistant hardware (e.g., secure elements); the use of strong, multifactor authentication; and the control and management of device configurations, third-party apps that can be installed on the device, and secure forms of communications.

The landscape of mobile device form factors – smartphones, tablets, and wearables – provides unlimited potential and application for physical access. This white paper was developed to provide an educational resource that highlights that potential and promotes the applicability of using mobile devices for physical access across the government, commercial, consumer and academic sectors.

9 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance Access Control Council and Identity Council to discuss how mobile devices can be used for physical access control.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance wishes to thank Council members for their contributions. Participants involved in the development and review of this white paper included: Defense Manpower Data Center (DMDC); DualAuth; General Services Administration (GSA); IDEMIA; ID Technology Partners; Integrated Security Technologies, inc.; IQ Devices; Intercede; JCI Software House; NextgenID; Thales; Transportation Security Administration (TSA); U.S. Department of Homeland Security (DHS); XTec, Inc.

The Secure Technology Alliance thanks **Mark Dale**, XTec, Inc., and **Lars Suneborn**, ID Technology Partners, for leading this project, and the Council members who developed content and participated in the review of the document, including:

- **Hanne Adamsen**, Thales
- **Tim Baldrige**, DMDC
- **Mark Dale**, XTec, Inc.
- **Chris Edwards**, Intercede
- **Christophe Goyet**, IDEMIA
- **Brandon Gutierrez**, TSA
- **Daryl Hendricks**, GSA
- **John Jacob**, IDEMIA
- **Tom Lockwood**, NextgenID
- **Stafford Mahfouz**, JCI Software House
- **Don Malloy**, DualAuth
- **Roger Roehr**, Integrated Security Technologies, Inc
- **Steve Rogers**, IQ Devices
- **Gerry Smith**, ID Technology Partners
- **Lars Suneborn**, ID Technology Partners
- **William Windsor**, DHS
- **Rob Zivney**, ID Technology Partners

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.

About the Secure Technology Alliance Access Control Council

The Secure Technology Alliance Access Control Council focuses on accelerating the widespread acceptance, use, and application of secure technologies in various physical and digital form factors for physical and logical access control as applicable to both persons and non-person entities. The group brings together, in an open forum, thought leaders, manufacturers, and implementers from both the public and private sectors. The Council identifies topical areas which further the use of technologies that are important to the access control community.

About the Secure Technology Alliance Identity Council

The Identity Council provides leadership and coordination and serves as focal point for Alliance's identity and identity related efforts leveraging embedded chip technology and privacy- and security-enhancing software. Directly and in partnership with other Secure Technology Alliance councils, the Identity Council supports a spectrum of physical and logical use cases and applications, form factors, attributes, and authentication and authorization methods. The Council serves to influence standards and best practices, serve as an educational resource, and provide a voice in public policy influencing adoption, implementation, and use.

Key areas of focus for the Identity Council are identity trust frameworks; digital identity; strong authentication; authorization; and biometrics. Additional information on the Identity Council can be found at: <https://www.securetechalliance.org/activities-councils-identity/>.

Appendix A Glossary

Bluetooth/Bluetooth Low Energy (BLE). Wireless technology standard used to exchange data between fixed and mobile devices over short distances. Both Bluetooth and BLE use UHF radio waves in the industrial, scientific, and medical radio bands (from 2.402 GHz to 2.480 GHz).

BLE, which is also called Bluetooth Smart, is a lighter-weight, power-conserving version of Bluetooth. It was introduced to provide an interconnection framework between devices that need to share only small bursts of information, as opposed to classic Bluetooth, which accommodates large amounts of data transfer for applications such as audio and video streaming. BLE operates at distances up to 100 meters in the 2.4 GHz frequency range, with application data throughput rates of 305 kbps, and consumes half of the power required by classic Bluetooth. Another power-conserving factor for BLE is that it allows devices to go into a very low power/sleep mode when there is no need for an interconnection. This power mode enables standalone battery-powered devices that communicate with BLE to live off a single battery for up to 4 years. When BLE devices are interconnected (using a pairing and bonding protocol pattern), they establish an encrypted communications channel similar to SSL/TLS. BLE's longer communications range (up to 100 meters) offers special benefits for communication using NFC, such as hiding PACS readers or placing them on the secure side of a door and making it possible to open a gate without having to roll down the car window and reach out to activate a reader.

Derived Credential. As defined by NIST SP 800-157, an alternative token that can be implemented and deployed directly with mobile devices (such as smartphones and tablets). A derived credential is a client certificate that is issued to a mobile device after end users have proven their identity by using a smart card (Common Access Card [CAC] or Personal Identity Verification [PIV] card) during an enrollment process.

Digital Certificate. An electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (the subject), and the digital signature of an entity that has verified the certificate's contents (the issuer). X.509 is the common standard for the format of digital certificates.

Near Field Communications (NFC). A set of standards that enables proximity-based communication between consumer electronic devices such as mobile phones, tablets, personal computers, or wearable devices. NFC devices can act as electronic identity documents and keycards. They are used in contactless payment systems and allow mobile payment replacing or supplementing systems such as credit cards and electronic ticket smart cards.

NFC-enabled smartphones can store and present access credentials to any reader that supports ISO 14443-compliant contactless access cards. Strategies for real-time and dynamic generation of credentials that can be delivered to the phone, either for storage in the secure element or to a host card emulation (HCE) applet, are possible.

A large number of NFC contactless readers (ISO/IEC 18000-33) has been fielded for physical access control, and that number is growing. This type of PACS technology is a prerequisite for an NFC-driven access credential. Since much of this infrastructure is already in place, the key to further implementation is to provision a compatible credential to the smartphone.

Physical Access Control System (PACS). System for granting access to employees and contractors who work at or visit a site by electronically authenticating their assigned credentials when presented to a credential reader. Credentials can be loaded and stored in a mobile device. Although PACSs are

information technology systems, they must be designed, deployed, and operated in cooperation with physical security teams to be successful.

Appendix B References

STANDARDS

- FIPS 140-2/3, “Security Requirements for Cryptographic Modules,” July 19, 2019, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>
- FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” NIST, February 2004, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>
- FIPS 201-2, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” November 2020, <https://csrc.nist.gov/publications/detail/fips/201/2/final>
- ISO/IEC FDIS 18013-5, “Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application,” ISO, Under development, <https://www.iso.org/obp/ui/#iso:std:iso-iec:18013-5:dis:ed-1:v1:en>
- NIST SP 800-63, “Digital Identity Guidelines,” NIST, June 2017, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>
- NIST SP 800-157, “Guidelines for Derived Personal Identity Verification (PIV) Credentials,” NIST, December 2014, <https://csrc.nist.gov/publications/detail/sp/800-157/final>

CREDENTIALS

- “FIDO Alliance Specifications Overview,” FIDO Alliance, <https://fidoalliance.org/specifications/>
- “Mobile Devices Offer Promise in Identity Solutions,” AFCEA, September 10, 2020, <https://www.afcea.org/content/mobile-devices-offer-promise-identity-solutions>
- “The Mobile Driver’s License (mDL) and Ecosystem,” Secure Technology Alliance Identity Council, March 2020, <https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/>

MOBILE ACCESS CONTROL TRENDS

- “5 access control trends for 2021,” IFSEC Global, December 21, 2020, <https://www.ifsecglobal.com/access-control/5-access-control-trends-for-2021/>
- “Access Control Trends in 2021: The Future of Access Control,” SWIFTLANE, December 14, 2020, <https://www.swiftlane.com/blog/the-future-of-access-control/>
- “Access Control Trends to Watch in 2021,” Total Security Advisor, December 11, 2020, <https://totalsecurityadvisor.blr.com/facility-security/access-control-trends-to-watch-in-2021/>
- “Gartner Says That 20 Percent of Organizations Will Use Smartphones in Place of Traditional Physical Access Cards By 2020,” Gartner, January 17, 2017, <https://www.gartner.com/en/newsroom/press-releases/2017-01-17-gartner-says-that-20->

[percent-of-organizations-will-use-smartphones-in-place-of-traditional-physical-access-cards-by-2020](#)

- “Genetec and HID survey shows higher education institutions ready to move from legacy access control systems and embrace new technology,” Genetec and HID, August 2020, <https://www.globenewswire.com/news-release/2020/08/20/2081430/0/en/Genetec-and-HID-survey-shows-higher-education-institutions-ready-to-move-from-legacy-access-control-systems-and-embrace-new-technology.html>
- “Mobile Access Control Platform Market Forecast to 2027 - COVID-19 Impact and Global Analysis by Technology and Application,” Intrado Global News Wire, September 15, 2020, <https://www.globenewswire.com/news-release/2020/09/15/2094035/0/en/Mobile-Access-Control-Platform-Market-Forecast-to-2027-COVID-19-Impact-and-Global-Analysis-by-Technology-and-Application.html>
- “Mobile vs physical access credentials - a tough battle,” Security World Market, Oct. 22, 2019, <https://www.securityworldmarket.com/uk/News/Business-News/mobile-vs-physical-access-credentials-a-tough-battle1>
- “Physical Security Market Overview Q4 2020,” SIA, November 4, 2020, https://www.securityindustry.org/report/physical-security-market-overview-q4-2020/?utm_source=Informz&utm_medium=Email&utm_campaign=sia%2C%20security%20industry%2C%20security%20industry%20association&_zs=8FSVW&_zl=DmsJ2
- “Vertical Market Focus: Education--‘Why Use a Card When I Have My Phone?’,” SECURITY INFOWATCH, November 19, 2012, <https://www.securityinfowatch.com/access-identity/access-control/article/10820977/one-card-access-control-moves-closer-to-near-field-communications>
- “Why mobile key is taking over in hotels,” Esther Hertzfeld – Hotel Management Technical Editor, December 2018, <https://www.hotelmanagement.net/tech/why-mobile-key-taking-over-hotels>

USE CASES

Cruise Ships

- “AI On Cruise Ships: The Fascinating Ways Royal Caribbean Uses Facial Recognition And Machine Vision,” Bernard Marr, Contributor, Enterprise Tech, May 10, 2019, <https://www.forbes.com/sites/bernardmarr/2019/05/10/the-fascinating-ways-royal-caribbean-uses-facial-recognition-and-machine-vision/?sh=272d2ce81524>
- “Huge leaps in AI have made facial recognition smarter than your brain,” C-NET Stephen Shankland March 28, 2019, <https://www.cnet.com/news/huge-leaps-in-ai-have-made-facial-recognition-smarter-than-your-brain/>

College/University Campuses

Villanova Use Case

- “At Villanova University, NFC Technology Being Tested,” Facility Executive, March 23, 2012, <https://facilityexecutive.com/2012/03/at-villanova-university-nfc-technology-being-tested/>
- “College Students Favor Smart Phones as Access Control Credential,” Locksmith Ledger International, May 2, 2012, <https://www.locksmithledger.com/home/article/10694572/college-students-favor-smartphones-as-access-control-credential>
- “MIFARE® brings Villanova’s Wildcard to life,” MIFARE.NET NXP Semiconductors Austria GmbH, December 15, 2015, <https://www.mifare.net/mifare-brings-villanovas-wildcard-to-life/>
- “Villanova Tests Access Control with Smart Phones,” SECURITY MAGAZINE, March 24, 2012, <https://www.securitymagazine.com/articles/82909-villanova-tests-access-control-with-smart-phones->

Arizona State

- “Arizona State University Mobile Access Pilot,” HID case study, 2001, <https://www.hidglobal.com/press-releases/hid-global-completes-nfc-mobile-access-control-pilot-arizona-state-university>
- “Get Smart About Access Control,” SECURITY MAGAZINE, November 1, 2011, <https://www.securitymagazine.com/articles/82477-get-smart-about-access-control>
- “HID Global Launches First University Pilot of NFC Smartphones Carrying Digital Keys for Access Control,” HID press release, September 14, 2011, <https://www.hidglobal.com/press-releases/hid-global-launches-first-university-pilot-nfc-smartphones-carrying-digital-keys>
- “HID Global pilot uses smartphones for access control at Arizona State University,” FMLINK - Facilities Management Resource, February 24, 2012, <https://www.fmlink.com/articles/hid-global-pilot-uses-smartphones-for-access-control-at-arizona-state-university/>