SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE MOBILE COUNCIL WHITE PAPER

Mobile Identity Authentication

Version 1.0

Date: March 2017

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.

Table of Contents

1 Introduction

In today's increasingly connected world, users of online tools are familiar with the requirement for a user ID and password to access a variety of services. The requirement originates in the early days of computing, when systems needed a digital means to authenticate a user, and has now proliferated into every virtual relationship. Although computer systems and services have evolved and become more widespread, there has been little change to the simple and reliable user ID-password requirement for user authentication, except perhaps for passwords to become more sophisticated.

In addition, consumers are becoming more and more comfortable with online banking, investing, bill payment, and even education as systems that require strong security. Most corporate IT users are familiar with remote work access requirements and the complex encryption provided by virtual private network (VPN) systems. These systems have developed significantly more complex user authentication mechanisms as the risk of data breaches increases. Many of these mechanisms involve the need to change a password regularly, force the inclusion of special characters and numbers in a password, and use a secondary confirmation (e.g., a text message with a one-time passcode) to strengthen the authentication of the person at the other end of a remote connection.

However, the need for higher levels of security is at odds with users' desire for convenience when accessing their digital services. Asking users to develop and maintain ever increasing complex passwords, or regularly engage one-time passcodes, adds friction and potential frustration for the user.

Technology and solution providers in the mobile and digital security industries are quickly evolving techniques for digital authentication which offer a breakthrough in security while improving convenience. Many of these techniques exist in a category called *mobile identity authentication*.

1.1 About Mobile ID Authentication

Consumers expect to be able to use their mobile phones to interact with remote systems and experience the same level of functionality and security as when they use a personal computer, laptop, or tablet. While the size of the mobile phone's screen has expanded, the interface displayed on the screen is still relatively restricted. For example, a recent study[1] has shown that the transaction abandonment rate for eCommerce shoppers using mobile phones outpaces the rate for shoppers using personal computers, laptops, and tablets. Users noted that it was too complex to load user ID and credit card information into the system during checkout while using their mobile phone. This limitation means that systems wishing to grant secured access to mobile users need to find elegant ways to authenticate users quickly, without compromising system security.

Mobile ID authentication is a response to this dilemma. Mobile ID authentication can identify a mobile phone user, reliably and securely, through a greatly simplified user experience, reducing friction for the user without compromising security.

Mobile ID authentication relies on a number of technologies that leverage both hardware and software techniques to reliably identify a user and that user's mobile device for security purposes. Mobile ID authentication supports legally binding authentication and transaction signing for online banking, payment, corporate services, and other secure consumer services (e.g., streaming online content). A user is issued digital credentials that are stored securely on the mobile device (for example, in a

[1] "7 reasons why customers are abandoning your mobile shopping cart," Ventureburn, January 18, 2016, http://ventureburn.com/2016/01/7-reasons-why-customers-are-abandoning-your-mobile-shopping-cart/.

hardware secure element (SE)). The user must then be authenticated locally to the mobile device by entering a passcode or PIN or by using device-level biometrics to be able to use the stored credentials.

Users can prove device ownership and present their secure credentials in several ways:

- In app. The credential is pulled from the secure storage location and transferred to a mobile app for sign in.
- In browser. The credential is pulled from the secure storage location and transferred to a mobile-enabled secured website using a browser.
- Using NFC. The credentials are pulled from the secure storage location and transferred to an NFC reader using card emulation.
- Using an out-of-band sign on. The credentials are used as a primary or secondary factor for strong authentication.

In many cases, what is actually transferred to the receiving party is not the credential but rather a hash of the credential; another approach is to append a cryptogram for additional security.

1.2 About this White Paper

This white paper was developed by the Secure Technology Alliance Mobile Council to provide an overview of mobile ID authentication, to highlight use cases that rely on secure user credentials stored on a mobile device, and to provide some perspectives on how emerging technologies and standards are addressing the growing need for mobile ID authentication. The paper is intended to introduce security-minded professionals across a wide range of industries to the potential benefits and implementation challenges of mobile ID authentication.

The white paper includes an overview of mobile ID authentication technology and market trends. It offers a variety of example use cases, including implementation considerations and challenges and, where appropriate, real-world implementations. It also discusses various authentication techniques and the approaches to securing sensitive user credentials on a mobile device. Uses highlighted include access control, payments, government-to-consumer services, and corporate applications. Mobile devices include smartphones, tablets, and smart watches.

The white paper highlights several technology and solution options which are in use today, and looks at efforts underway to solidify some of the emerging standards (e.g., 3D Secure and the FIDO protocols). The goal of this white paper is to advocate that the mobile industry move forward to more advanced mechanisms for mobile ID authentication and to provide a call to action for consolidation around the use of standards for mobile ID authentication.

This white paper is focused on consumer implementations of mobile ID authentication, including a few government-to-consumer uses (e.g., driver's licenses). Discussion of a mobile credential solution for government-issued Personal Identify Verification credentials (a.k.a. mobile derived PIV) has been intentionally excluded from this paper due to scope limitations. However, the Secure Technology Alliance Mobile Council highly encourages security-minded professionals with broad interest in mobile ID authentication to become familiar with NIST SP 800-157.

2 Overview of the Identity Verification Process

Today, identity verification is requested routinely in a variety of familiar situations—when someone wants to obtain health care, enter a public building or corporate office, or get on an airplane. While system and solution providers must balance ease of use against the required level of security, any identify verification system that provides access to facilities or data typically performs certain activities:

- Identity proofing
- Identity authentication
- Authorization

Identity proofing is the initial validation of an identity of an individual by the party whose data, services or resources are being accessed (also called the "relying party"). Identity proofing is the step that verifies that an applicant for an identity credential is in fact the person the applicant claims to be. Relying parties will have different requirements for the extent to which they need to verify an individual's identity and have different processes for the proofing. For example, the process and the extent of identity proofing used to obtain a driver's license is much different than that used to open an account with an online retailer. Identity proofing can be performed in person or remotely and is the first step for any relying party who wants assurance of an applicant's identity. Once it is completed, the relying party would issue an identity credential to the applicant.

Identity authentication occurs each time a person's identity must be confirmed. Identity authentication compares the identity credentials provided with those previously stored by the relying party. Identity authentication can be accomplished with one or multiple factors; in general, a "strong authentication" process is one that uses multiple factors (e.g., a physical device (card, mobile device) and biometric or PIN).

Authorization grants access to specific data, service or facility. An administrator grants rights and account permissions for access to resources and ties those rights and permissions to a specific identity credential.

Considerations for the identity management process (proofing, authentication and authorization) include the following:

- How does the identity proofing process verify that the identity information presented is accurate and protect the confidentiality and integrity of that information? What rigor is needed to establish that that the applicant is indeed the person they claim to be?
- How will the system protect each individual's information, including while the information is being stored and while it is being used?
- How will the identity credential that an individual carries protect itself from being copied, altered, or hacked, to prevent unauthorized use, misuse, or disclosure of any personal information it carries?

Mobile service providers are challenged by users who want to simplify the process of using their mobile devices to access secured facilities, data and online services.

Mobile devices incorporate a number of technologies that can be leveraged to support the identity verification process. For example, the camera on a mobile phone can capture an image of a driver's license, which then can be used to support identity proofing for the individual to get an identity

credential from another service. Cameras can also be used for facial recognition during identity authentication.

Technologies that support biometrics, such as fingerprint sensors or voice recognition software, are also becoming commonplace on mobile devices. Location awareness can be used as a supplemental data element for both identity proofing and identity authentication. And mobile devices can support a number of technologies that can be used to securely store and use identity credentials.

This white paper reviews how mobile devices and the technologies they support can be used to implement efficient, convenient and secure processes to validate identity. Since identity proofing processes vary widely by relying party, the white paper focuses on the authentication and authorization process.

3 Market Drivers for Mobile Identity Authentication

There is a growing need for service providers across a wide range of industries to offer mobile based solutions for their users. More and more consumers use mobile devices for a variety of activities, from sending and receiving email messages and viewing news stories to checking stock prices, playing games, watching videos, using social media and, in more recent years, moving funds and making payments. Many of these activities are low risk and may not require user authentication. Others, however, such as accessing buildings, accessing and moving funds or financial data, making payments, and accessing or changing medical records, require a higher level of security and authentication.

In this chapter, we review the growing demand by users for services on their mobile device, and we explore how service providers need to implement higher levels of security while minimizing the impact on convenience of use for these services.

3.1 General Trends

GSMA published an October 2015 survey of 1,000 consumers that provided statistics on how consumers answered the following question: "What documents or processes do you expect to store, or carry out, using your mobile phone by 2020?"[2] The responses are shown in Table 1.

Table 1. How Consumers Anticipate Using Mobile Phones in 2020

Response	Consumers (%)	Response	Consumers (%)
Making a payment to an online store without cards	50	Storing loyalty cards and coupons	48
Tickets for travelling on public transport	35	Registering or sharing information with your doctor	35
Actively protecting yourself, your home and your family from hacking and fraud	33	Authorizing access to home Internet and TV	33
Storing your driving license	28	Proving your age when purchasing alcohol or cigarettes at a self-service check out	24
Filing your tax returns	23	Voting in elections	22
Entering your place of work, VPN, printers	19	Entering a country using a passport	17

All of these uses could benefit from a secure, authenticated mobile identity credential, since they involve either personally identifiable information (PII), such as name, age, address, or tax ID, or payment or other sensitive data.

Another study, the TSYS 2016 U.S. Consumer Payment Study,[3] provided 1,000 respondents with a list of 14 mobile services and asked them to indicate their interest in each service on a scale of 1 to 5, with 4

[2] Mobile Connect, *Mobile Connect Consumer Research Report: United States*, http://www.gsma.com/personaldata/wp-content/uploads/2015/10/mc_us_paper3_10_15.pdf.

[3] TSYS, "2016 U.S. Consumer Payments Study," http://tsys.com/Assets/TSYS/downloads/rs_2016-us-consumer-payment-study.pdf

being “slightly interested” and 5 being “very interested.” Table 2 shows the percentage of those respondents who indicated a level of interest in using their mobile devices for managing certain aspects of their payments.

Table 2. Financial Industry Example – TSYS Study on Mobile Services

Service	Percent
Immediately stop a transaction that was not made by you	69
Immediately view transactions made with a debit or credit card	62
Receive instant offers and promotions from the store you are visiting	54
Turn a payment card on or off based on location	53
Turn a payment card on or off based on type of store	50
Turn a payment card on or off based on time of day	50
Keep all of your loyalty/rewards cards on your phone	49

There is clearly interest on the part of consumers in increasing the amount of information they store on their mobile devices or in using their mobile devices to manage payments and credentials for applications.

3.2 Risk Levels for Various Uses of Mobile Identity Authentication

In the past, the most frequent method of authenticating a mobile device and a user was to use a passcode (for the device) and a user name and password or code for user access to individual apps or sites. Recently, the use of multifactor authentication has increased, as has the use of biometric factors (most notably fingerprints), voice, and pictures. For example, Mastercard has rolled out Identity Check Mobile, a new payment technology application that uses biometrics like fingerprints or facial recognition to verify a cardholder’s identity to simplify online shopping. Trials began in October 2015, and now the technology has been made available in several markets including the UK, Austria, Belgium, Czech Republic, Denmark, Finland, Germany, Hungary, Netherlands, Norway, Spain, and Sweden.[4] In March 2016, Amazon filed a patent application for a system that would allow users to authenticate themselves with a selfie or video to complete a transaction.[5] According to the Amazon patent application, the technology would identify the person completing the transaction as "a living human being" by using facial recognition technology.

When discussing authentication, it is helpful to look at common use cases, their associated security objectives, and the impact of a security breach. Using a framework defined by the federal government,[6]

[4] Mastercard press release, http://newsroom.mastercard.com/eu/press-releases/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality/

[5] Leena Rao, “Amazon is Trying to Patent Paying with a Selfie,” *Fortune*, March 14, 2016, http://fortune.com/2016/03/14/amazon-patent-selfie/.

[6] The Federal Information Security Management Act (FISMA) defines security objectives of confidentiality, integrity, and availability for information security. In addition, the Federal Information Protection Standard (FIPS) provides various impact examples resulting from loss of any of the defined security objectives. Additional information on the FISMA objectives can be found in Appendix A.

the Secure Technology Alliance Mobile Council project team developed Table 3 to provide considerations for the levels of authentication that could be implemented across a number of common use cases for mobile ID authentication.

The purpose of Table 3 is to highlight the relative differences that should considered when implementing a mobile ID authentication solution. It should be noted that several elements in Table 3 have a strong dependency on the actual implementation methods, and therefore the table should be considered only as a guide.

Table 3. Common Mobile Device Uses and Their Risks

Use Case	Security Objective	Potential Impact/Risk Level	Considerations for Level of Authentication	Other Considerations
Viewing non-sensitive data (e.g., news sites)	Confidentiality impact	Low	Minimal Single factor	Credentials or method used may be hacked and then "tried" for access to sites that include more sensitive data or capabilities, since many consumers use the same user names and passwords for multiple sites.
Viewing financial data (e.g., banking, investment, payment card sites)	Confidentiality impact	Moderate	Multifactor may be used at enrollment. Some level of device authentication (e.g., registered device) and user log in may be used for subsequent access.	If the site provides access to PII (e.g., by viewing account settings), then a more secure authentication method may be used.
Viewing sensitive financial and non-financial data (e.g., medical records, clinical results)	Confidentiality impact	High	Multifactor may be used at enrollment and for subsequent access.	Access to data needs to be highly secure, due to the time and effort required to rectify the impact should a breach occur.
Conducting financial transactions (making payments, online banking, investing)	Integrity and availability impact	High	Multifactor may be used at enrollment and for subsequent access.	Transaction irreversibility, magnitude, and available risk management techniques affect risk.
Making a purchase	Availability impact	Moderate	Multifactor may be used at enrollment.	Enrollment in payment methods such as mobile wallets may leverage multifactor authentication. Subsequent transactions at the POS can leverage current payment customer verification methods, such as a PIN.
Accessing buildings and areas where sensitive data is available	Confidentiality impact	High	Multifactor may be used at enrollment and for subsequent access.	

The examples provided in Table 3 are not comprehensive. Authentication policy must be determined by the specific use case, since the impact of failing to achieve a security objective may not be monolithic. For example, an organization managing public information on its web server may determine that there is no potential impact from loss of confidentiality, moderate potential impact from loss of integrity, and

moderate potential impact from loss of availability. In this case, multifactor authentication may not be considered as important.

As another example, consider a power plant with a supervisory control and data acquisition (SCADA) system that controls the distribution of electric power to a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant may determine that for the sensor data, there is no potential impact from loss of confidentiality, high potential impact from a loss of integrity, and high potential impact from a loss of availability. In this case, multifactor authentication may be considered critical.

4 Evolution of Mobile Identity Authentication Mechanisms

When mobile devices connect to a broadband or WiFi network, authentication plays a critical role in preventing attacks, abuses, and misuses. Mechanisms to properly authenticate users on mobile devices have evolved, and the pace of innovation is increasing, as users demand access to more platforms via their mobile devices. This section describes some of the more common authentication mechanisms that have been used in the past with their limitations, and some mechanisms that are emerging to assure a user's identity can be verified and confirmed in a fast, convenient and secure manner.

4.1 User ID and Password

The traditional means of authenticating users to an online service is a user ID and password. Over time, however, online accounts have proliferated to the point that the average U.S. consumer now has more than 130 passwords.[7]

Two strategies have helped consumers manage their passwords, both of which have drawbacks in terms of security:

- Use the same password for everything, which is not a good idea for obvious reasons.
- Use a password manager. Security then depends on the security of the password manager, which in theory represents yet another point of vulnerability.

Passwords can be static or dynamic. Simple passwords are guessed easily, resulting in the application of length, complexity, and timeout parameters. But such requirements can make it difficult to enter the password using a mobile device. A better approach is to combine passwords with policies that cater to mobile needs, such as letting users receive notifications without entering a password and providing a mobile password recovery process.

Even with the introduction of creative ways to manage passwords, the proliferation of new approaches to security and authentication that are enabled by the power of mobile devices and associated sensors promises to ultimately eliminate passwords.

4.2 Multifactor Authentication

Because user ID and password techniques are losing favor, the security methods used today by many digital service providers to assure mobile ID authentication usually involve a technique called multifactor authentication. Multifactor authentication requires the presence of two or more of the following authentication factors:

- Something you have, such as a card, a token, or a mobile device
- Something you know, such as a password, a passcode, or a pattern
- Something you are, meaning a physical characteristic such as a fingerprint or the retina pattern revealed by a scan
- Where you are, revealed through geofencing or location awareness

A commonly used multifactor authentication mechanism consists of a small hardware device or token which is assigned to a user, and which generates an authentication code at fixed intervals. The token

[7] Tom Le Bras, "Online Overload – It's Worse Than You Thought," *DashLane Blog*, July 21, 2015, https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought.

can be plugged into a USB port to provide the authentication code directly to the host system. Or, the token displays the code to the user, who must enter this code along with their user ID and password in order to get access to a host system. A mobile phone can also serve as a "soft token" where the dynamic authentication code can be delivered securely to a mobile device, and then used during login on a laptop or desktop computer.

Mobile devices can also be useful in augmenting the security of the user ID-password combination for online providers. For example, numerous financial services companies now use a text message code or one-time passcode (OTP) for out-of-band authentication, providing an additional layer of security when a customer accesses online banking services from an unfamiliar device or IP address.

Because entering text on a device can be cumbersome, it is often more effective to authenticate a user to a device using non-text passwords, such as by requiring the user to tap symbols within a randomly generated matrix or a sequence of points on an image. Enabling device access this way can also grant access and unlock services on the device.

Digital certificates can be used to bind an identity to a public-private key pair and are considerably stronger than passwords, as long as the owner's private key is protected. Combining a mobile device lock with certificate-based network authentication is a proven method of associating a user with a device.

Biometric factors, such as fingerprints, voiceprints, iris scans, and "scribbles" or handwritten signatures, can also be used to identify a user. Mobile devices are increasingly being released with biometric capabilities, making the use of biometrics very convenient. The preferred method involves matching the biometrics on the device and unlocking local cryptographic keys. This method is gaining far more widespread support than the higher risk method of matching biometrics with the remote relying party.

Location awareness and geofencing are becoming more common as ways to deliver services such as targeted marketing, coupons, and offers to mobile devices when the user is in proximity to or entering a store. Location awareness and proximity can also be used to authenticate a user. Such proximity-based authentication factors can be combined with other authentication factors to unlock specific services on a mobile device (such as payments or access to connections) while keeping others locked.

It should be noted that some of the mechanisms listed above have a dependency on either the hardware or the operating system (or both) of the mobile phone. Other mechanisms were developed as standalone or proprietary solutions to address a particular business need. These factors can limit the scalability of certain multifactor authentication mechanisms and are driving the industry towards more standards-based solutions.

4.3 Standards-Based Approaches for Mobile Authentication

Any mobile authentication scheme that is to be widely deployed must be based on accepted standards. Standards development for mobile ID authentication is still in the early stages, and the industry needs to continue to develop robust, proven mechanisms.

This section describes a few examples of standards that have been or are being developed. Developers and implementers alike should consider these and other industry standards for use in their mobile ID authentication schemes.

4.3.1 FIDO Authentication[8]

The Fast Identity Online, or FIDO, Alliance is a group of software, hardware, and service providers formed to address the lack of interoperability among strong authentication devices and the problems associated with creating and remembering multiple usernames and passwords. The goal of the Alliance is to develop specifications, standards, and methodologies that define an open, scalable, and interoperable set of mechanisms that can allow users of online services to be authenticated without relying on passwords. Passwords are to be replaced with so-called FIDO authenticators, which can be used with fixed or mobile devices.

The FIDO authentication protocols are designed to enable robust authentication while providing a superior user experience and protecting user privacy. They incorporate the following principles:

- Strong authentication
- A user experience that combines ease of use with proof of intent. Proof of a user's physical presence activates the protocol.
- Privacy protection

The FIDO protocols rely on strong cryptographic techniques to authenticate a device to online services. Secrets are stored only on that device and are never exposed to the cloud.

The FIDO specifications also include several requirements that focus on user friendliness without jeopardizing user privacy. Unique site-specific credentials authenticate a user to individual websites, thus preventing users from being tracked across online services. The architecture is designed to retain each user's passwords, biometric factors, or private keys securely in that user's device.

The FIDO specifications include two options for user authentication using FIDO authenticators: passwordless and second factor. (Figure 1) The passwordless option replaces the password with a local authentication factor. The second factor option augments a password with a device (such as a dongle) that complies with FIDO specifications, enabling password simplification. Both options improve security while providing satisfactory usability.

4.3.1.1 PASSWORDLESS OPTION

The FIDO Alliance Universal Authentication Framework (UAF) is designed to provide a method of authenticating that the rightful user of a UAF enabled authenticator (e.g., mobile phone with fingerprint sensor) is present at the time the relying party requests an authentication event. To achieve this requires three actions.

First, the user registers their fingerprint with their FIDO UAF-enabled authenticator (e.g., mobile phone). This process is local to the mobile phone and no information is exchanged with any server or with the cloud. The fingerprint is stored locally, verified locally and secured within the user's personal device.

Second, the user signs into a website of a FIDO-enabled relying party. The relying party determines that the device the consumer is using is FIDO certified and asks the user if they would like to use their authenticator instead of their password the next time they sign in. The authenticator creates a unique public-private key pair. It stores the unique secret securely within itself and offers the public key to the relying party to be associated with the user's account. The next time the user signs into the relying party's website, the relying party challenges the authenticator to prove that the user is present. The

[8] https://fidoalliance.org/specifications/overview/

user is prompted to present their fingerprint for local authentication. If the authenticator is successful, it will sign the challenge with the unique secret key associated with that relying party.

Third, the relying party uses the unique public key associated with that user to authenticate the challenge.

For each relying party, the authenticator creates a unique public-private key pair, assuring the user that the various relying parties with which they have associated their authenticator cannot create associations between other parties with which the user has a relationship. Security, convenience and privacy are the key objectives of the FIDO Alliance.

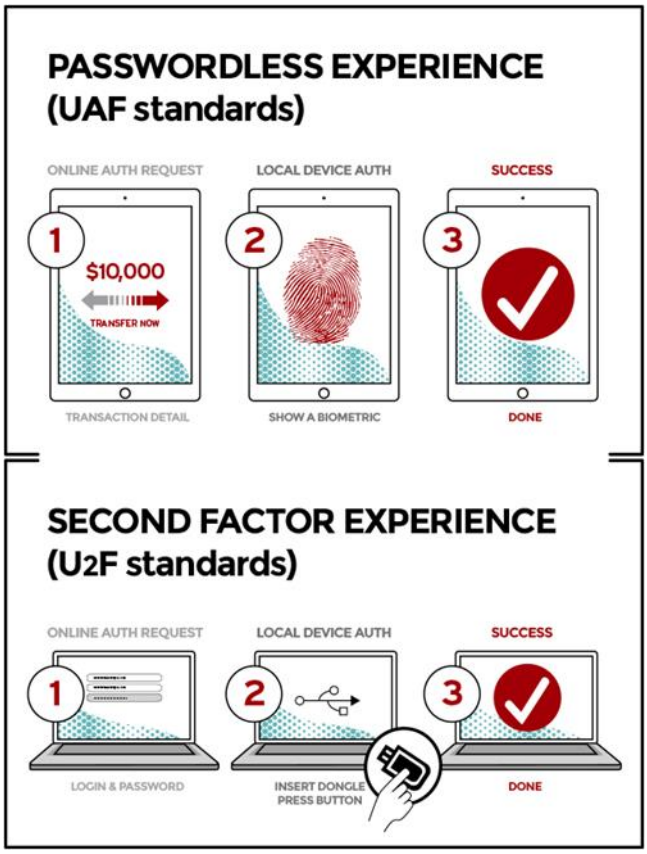

Figure 1. FIDO Authentication Alternatives to Passwords

4.3.1.2 SECOND FACTOR OPTION

FIDO Universal Second Factor (U2F) is an open authentication standard that enables users to access any number of online services securely with one mobile device. The second factor option relies on the U2F protocol. Online services can augment the security of their existing password infrastructure by adding the requirement for a strong second factor—a U2F device—to user login. The user logs in with a username and password as before. The service can prompt the user to present the second factor device at any time.

This requirement for the strong second factor allows a service to simplify its password requirements (to, for example, a 4–digit PIN) without compromising security. U2F therefore strengthens password authentication by adding the requirement for a simple-to-use token, the presence of which constitutes a second authentication factor.

4.3.2 W3C Web Crypto API[9]

The W3C Web Crypto API offers authentication mechanisms over common API interfaces to the underlying cryptographic key storage. This approach is applicable to a variety of use cases, such as multifactor authentication managed within a mobile application; protected exchange of documents by wrapping with public keys and unwrapping using private keys; cloud storage; document signing; data integrity protection; and secure messaging.

Web Crypto API defines low level interfaces for interaction with cryptographic key materials, which are exposed through an interface that provides common access functions and is managed or exposed by user agents. This API creates an agnostic layer to the applications that is compatible with multiple underlying key storage implementations from different cryptographic vendor solutions. Web Crypto API offers a common set of interfaces to rich web applications that can be used to access a variety of cryptographic operations, including key and hash generation and verification.

4.3.3 3D Secure Protocol[10]

The EMVCo 3D-Secure protocol enables bank card issuers to authenticate consumers directly for online transactions. This protocol is intended to prevent online transaction fraud and protect merchants from exposure to chargebacks. The protocol provides an additional layer of security and has different implementations depending on the specific payment network implementation.

The three domains are the acquirer domain (the merchant), the issuer domain (the card issuer), and the interoperability domain (the infrastructure, which includes software providers).

4.3.4 Client TLS Certificates

The use of client certificates to provide two-way authentication between clients and servers is defined in the Internet Engineering Task Force (IETF) RFC 5246.[11] Within the handshake that establishes a secure session, the server may demand a certificate and proof of ownership from the client. Due to historical constraints on certificate delivery and extended trust relationships, this mechanism has until now largely been confined to enterprise networks, where it is frequently used for VPN or website authentication with smart cards or desktop certificates.

However, these constraints can now be avoided, due to the prevalence of smartphones and the availability of cloud services capable of easily deploying dedicated, affordable certification servers. Certificates can now be used as a highly secure and very convenient alternative to password authentication, especially when they are deployed in conjunction with biometric user authentication to the handset. Implementation of this mechanism requires a certification server.

[9] https://www.w3.org/TR/WebCryptoAPI/.
[10] https://www.emvco.com/specifications.aspx?id=299.
[11] https://tools.ietf.org/html/rfc5246.

5 Best Practices for Authenticated Identity Credential Protection on Mobile Devices

When secured identity credentials are stored in a mobile phone, one key question is how to protect them. Although many experts may consider the mobile phone operating system (OS) to be more secure than a personal computer, it is still vulnerable. Best practices would require using proven, recommended security mechanisms that go beyond the security features native to a mobile phone's operating system.

This section discusses the several security approaches currently used to secure credentials in mobile devices and highlights the advantages and disadvantages of each approach.

5.1 Hardware Secure Element

One option for securely storing a mobile ID credential on a smartphone is to use a hardware secure element (SE). Credentials that are stored in an SE are protected using the same techniques that protect credentials on a physical chip card. These include both physical and software-based techniques.

The SE provides a root of trust that has specific production requirements ensuring protection of private keys. The SE also goes through a certification process that verifies the efficacy of its secure storage, access control, and cryptographic processors.

A hardware SE may be permanently soldered (embedded) in the smartphone or connected through a UICC or MicroSD. Whichever form factor is used, an SE in the smartphone is indirectly connected to the Internet. The potential for attacks is thus much higher than for attacks on a physical card, which can only be accessed if it is inserted into a contact reader or happens to be close to a contactless reader, and then only if the reader has been compromised. Therefore, it is necessary to limit access to the credential on the SE to authorized applications only.

GlobalPlatform® has standardized an SE access control mechanism. Support for this mechanism (or an equally secure alternative) should be a prerequisite for allowing any application running in the mobile operating system to access the secure mobile IDs stored on a smartphone.

5.1.1 Advantages

This approach has the following advantages:

- It is tamper-resistant, meaning that it recognizes and responds to both software and hardware attacks.
- It can run cryptographic algorithms with hardware acceleration.
- It can run multiple applications isolated through firewalls.
- It can provide lifecycle management of card applications through secure channels.
- Card-based applications can be migrated to the mobile SE easily.
- Access from a Trusted Execution Environment (TEE) and mobile applications is well defined.
- Compliance and certification programs are in place to ensure interoperability and conformance to specifications.

5.1.2 Disadvantages

This approach has the following disadvantages:

- Memory in the SE is limited.
- Lifecycle management requires trusted, secured systems.
- Access to the storage space and lifecycle management requires business relationships.

5.2 Trusted Execution Environment (TEE)

Another option is to store credentials in a TEE. A TEE is an execution environment that runs alongside the smartphone operating system (the rich OS). A TEE provides security services and isolates access to its hardware and software security resources from the rich OS and associated applications. In this way, a TEE can protect the mobile ID credential from threats that are potentially present in the rich OS.

A TEE implementation can leverage techniques such as encryption, tokenization, and code obfuscation to further strengthen the protections provided by the core TEE architecture.

5.2.1 Advantages

This approach has the following advantages:

- It uses mobile device memory secured by a dedicated cryptographic processor.
- It is accepted by the Android OS and several standards groups (e.g., oneM2M, FIDO).
- Keys can be stored in the SE or other hardware-based secured system (e.g., UICC).
- There are defined specifications for a trusted user interface and secured storage.
- GlobalPlatform® has a certification program that certifies TEE security mechanisms.

5.2.2 Disadvantages

This approach has the following disadvantages:

- The trusted application execution environment is a restricted environment, and access usually requires business relationships.
- Lifecycle management requires trusted, secured systems.

5.3 Host Card Emulation

The latest versions of the Android operating system support host card emulation (HCE). HCE is covered in this section because it allows secure credentials to be stored in several different ways, for example, via a cloud service, or in conventional memory on the mobile device. However, the reader should be cautioned that HCE is NOT a security mechanism. HCE implementations simply allow NFC commands to be routed to an application running in the smartphone OS rather than being routed directly to an SE. Use of HCE does not define where credentials and sensitive data are stored nor how they are processed. Nor does HCE provide or specify any security techniques, so security must be implemented on top of an HCE implementation.

It is recommended that any HCE-based mobile ID application leverage additional techniques such as encryption, tokenization, code obfuscation, or white box cryptography. Risks can also be reduced using system-level countermeasures. Back office systems should be designed to detect fraud by tracking transaction details, such as the phone's location, and looking for irregularities. HCE applications can also be implemented using an SE or TEE to enhance security. These approaches, along with similar traditional approaches, can reduce the risk of securing credentials in an HCE implementation.

5.3.1 Advantages

This approach has the following advantages:

- No special access control is required. The credential is stored in the mobile device's main memory.
- HCE is supported by Android OS, with similar approaches available for Windows Phone and Blackberry.
- Updates and modifications to a credential or any supporting application can be deployed rapidly and remotely.

5.3.2 Disadvantages

This approach has the following disadvantages:

- Security is not provided as part of HCE.
- An application is installed with keys that are exposed to the rich OS.
- Credentials are less secure when they are stored in a phone's main memory.
- Applications need to have their own security mechanisms, which may be more vulnerable to attack.

5.4 Summary and Recommendations

The best choice for secure storage of mobile identity credentials on a smartphone can depend on the specific requirements of the use case and the degree to which system-level countermeasures can be effective.

Storage in a hardware SE assures that the credentials are stored securely on a mobile handset in a consistent manner across various handset hardware and operating systems. However, several parties are typically involved in managing access to the SE. Using a TEE can reduce the complexity involved in accessing a secure storage location and managing applications. Using HCE involves assessing security and developing on-device security measures, which must be balanced against factors such as cost, time to market, and scale of interoperability.

Depending on the risk profile of a typical mobile identity credential, as outlined in Section 3.2, the recommended approach to storing mobile identity credentials on smartphones is to leverage the stronger security found in using SE and TEE implementations. HCE implementations should at a minimum use tokenization and store encryption keys in either the SE or TEE.

6 Use Cases for Mobile Identity Authentication[12]

This section describes a variety of situations in which mobile ID authentication would be useful. Each description includes value propositions as well as the challenges involved. The use cases are:

- Mobile device access
- Physical access control
- Government-issued citizen IDs, including mobile driver's licenses, mobile vehicle registration, and mobile recreational licenses
- Proximity payments
- Remote payments
- Financial services access

6.1 Mobile Device Access

Definition	Participants	Challenges
User credentials are stored securely on the mobile device and used to grant authorization to use that mobile device	Mobile device makers Mobile phone OS providers Security software providers Certificate authorities	Compatibility across hardware and security domain variations Requirement for easy to use, easy to learn methods for distributed enrollment Approaches to minimize false acceptance rates and false rejection rates

In this use case, credentials for authorized users are securely stored on a specific mobile device and a user must present matching credentials each time they wish to access or use privileges on that specific mobile device. Access can be controlled locally on the device, via a log-on to a connected server, or via a hybrid scheme such as the one outlined by the FIDO Alliance (see Section 4.3.1). Access can be managed for the entire mobile device, or can be layered, requiring the user to first be granted access to the mobile device (e.g., PIN to unlock the phone) and then be granted access to a specific mobile app (e.g., biometric authentication to use a mobile banking app).

6.1.1 Value Proposition

Mobile devices contain or provide access to an ever-increasing amount of sensitive information. This can be personal information or information owned by an enterprise that allows users to access its data through their mobile devices. Mobile device users and parties responsible for the controlled access to this sensitive information can leverage the authentication mechanisms of mobile devices to assure only authorized persons are granted access.

6.1.2 Implementation

The traditional mechanism for mobile device access is the keyboard/screen entry of a passcode (PIN, password, and more recently touch patterns) which has been stored in the device by its owner. Typically, these passcodes are stored in a secured portion of memory (e.g., SIM, key vault, other trusted area) to reduce the likelihood of the data being hacked.

[12] Company, product and service references are included with the examples to document the use cases. This white paper does not endorse any specific company, product or service.

Biometrics can act as an alternative to pattern or PIN screen unlocks, and can greatly simplify the log-in process on a mobile device. Cameras and microphones are two of many standard components on mobile devices that can be leveraged for biometrics (e.g., for facial or voice recognition). Likewise, the majority of newer smartphones include a biometric sensor capable of reading fingerprints.

6.1.3 Challenges

Traditional passcodes suffer from a linear relationship between complexity and security. Passcodes must be made longer to increase the device's protection against someone simply guessing the passcode. For a mobile device with a modest sized screen, this makes a highly secure log-in rather inconvenient. Biometrics offer the advantage of a simplified log-in but can suffer from both hardware and user limitations. For example:

- A percentage of humans have fingerprints that are not readable by fingerprint sensors, and
- Ambient light and noise can reduce the reliability of facial and voice recognition systems.

6.1.4 Examples

Apple Touch ID.[13] Beginning with the iPhone 5S in September 2013, Apple introduced a biometric sensor as standard equipment on their phones. It was first used to lock/unlock the phone and authenticate purchases on iTunes and the App Store. Beginning in September 2014, with the launch of iPhone 6, this sensor (Touch ID) was also used by the Apple Pay native service to authenticate a user whenever a payment transaction is attempted with Apple Pay.

Google Face Unlock.[14] Introduced in 2011 as part of Android 4.0 (a.k.a. Ice Cream Sandwich), this native security service could be used to lock and unlock your Android phone. The service used a front-facing camera to capture an image of authorized users. Once the facial image was registered, the camera could be unlocked whenever a matching image was seen. Initial implementations could be fooled by a photograph of the registered user, but recent updates have improved that limitation. This feature became Trusted Face with Android 6.0 (Lollipop) and provided significant usability improvements.

Google Trusted Voice.[15] Available in early 2015, this voice recognition tool allows an Android smartphone to be unlocked with a voice command. After setting up the service, whenever a user says "Ok Google" from a secure lock screen, Google can be asked to do things for the user, or visit sites, without manually unlocking the device.

Iris Scanning. The Samsung Galaxy Note 7[16] contains a feature that allows users to unlock the device simply by staring the screen. Cameras on the phone's front face capture the patterns of the iris in the eyes of the person staring at the phone and compare this to the pattern stored in the device. This offers the simplicity of use of facial recognition, but with dramatically higher levels of security because of the unique patterns that exist in each person's eyes.

---

[13] https://en.wikipedia.org/wiki/Touch_ID

[14] http://www.dailymail.co.uk/sciencetech/article-2522605/Unlock-phone-FACE-Hidden-software-lets-Android-owners-use-head-PIN-people-similar-looks-able-hack-it.html

[15] https://support.google.com/nexus/answer/6093922?hl=en and http://lifehacker.com/google-starts-rolling-out-trusted-voice-smart-lock-opti-1697437287

[16] http://www.samsung.com/global/galaxy/galaxy-note7/security/

6.2 Physical Access Control

Definition	Participants	Challenges
Smartphones can store access credentials and present them to access control readers.	OEM handset makers Trusted service managers Tokenization service providers Security system integrators Local distributors/servicers Door access hardware providers Physical access control system manufacturers Commercial, industrial, residential, and government users	Static data protection Solution provider access to the SE Approach to efficiently leverage tokenization services Door hardware upgrade Door reader support for the appropriate technology (NFC or Bluetooth) or protocols Availability of NFC support in different manufacturers' phones Potentially inappropriate antenna design and placement in phone

In this use case, access credentials are provisioned to mobile devices and used to replace commercial badges, corporate badges, institutional badges, and keys to doors in universities and homes.

6.2.1 Value Proposition

Mobile ID authentication is a major trend. The advantages of instantly issuing ID credentials on smartphones are compelling. A guest does not have to wait for a visitor badge to open doors or pay for a coffee. Operators can save costs and increase convenience by streamlining their ID issuing processes. End users benefit from a mobile ID credential, because it is very convenient to always have all access credentials at hand. And mobile access credentials can already work with many existing reader infrastructures.

Implementing mobile ID credentials for physical access control offers the following value propositions:

- Convenience – no need to wait for a visitor badge
- Streamlined ID credential issuing process
- Over-the-air (OTA) provisioning and just-in-time credentials
- Inventory and management cost controls
- Secure ID credential storage

6.2.2 Implementation

Current cloud services allow access-product vendors to port their smart card applications to smartphones, simply and securely. These services are easy to integrate into current access management back-end systems, such as a physical access control system (PACS), hotel property management system, campus residence door control system, or student identity and privilege management system. Such systems typically include simple APIs for integration with other software.

Smartphones that support NFC can store access credentials (mobile access IDs) and present them to readers that support ISO/IEC 14443-compliant contactless access cards. The credentials can be generated in real time or dynamically and delivered to the phone, either for storage in the SE or for use via a host card emulation (HCE) app.

Alternatively, Bluetooth technology can be used to present access credentials which are stored on a mobile device. Bluetooth-capable door locks or access mechanisms can be integrated into physical

access control systems and be enabled only when authorized credentials are found in a device within Bluetooth range. Best practices would include the use of a mobile app which activates the Bluetooth link only when prompted by the user.

Some implementations may benefit from the use of a token-based solution, wherein the actual credential assigned to the individual is stored at a secure token service provider, and only a surrogate (token) is sent to the mobile device. This solution provides protection against counterfeiting because the tokens can be time or transaction count limited, and if detected, cannot be directly associated to the underlying original credential.

6.2.3 Challenges

Implementation of mobile ID authentication for physical access control has many of the same challenges as traditional card-based physical access, plus a few new challenges. The challenges of mobile physical access include:

- Door access systems or PACs are typically designed to recognize and authenticate static card data, which is passed to a local server to approve or deny access. Static data on a smartphone needs to be protected to prevent compromise.
- If the data is stored in the SE, the solutions provider would need to be able to access the SE. The challenges of using the SE could be avoided if the implementation relies on HCE and tokenization. However, door hardware would have to be upgraded to facilitate synchronization with the tokenization scheme used.
- While the software in more recent versions of door access readers is configurable, many currently installed readers are configured to support only specific contactless protocols that may not be supported by all phones.
- If the implementation leverages NFC, antenna placement and design on some phones could be less than optimal, making for a poor consumer experience. If the implementation leverages Bluetooth, it can pose other challenges for PACS use, including read range and limited support by door lock providers.

Mobile ID authentication for physical access control also requires:

- Real-time over-the-air management of credentials, especially for hospitality applications, or if tokenization is used to combat the risks associated with static data.
- Compatibility across a wide variety of security and communications technologies used on mobile devices and mobile operating systems.

Token-based solutions will also require a reliable token service provider who can maintain the integrity of the tokens while distributed in the mobile devices, as well as in all databases used to authorize access.

6.2.4 Examples

Three pilot projects illustrate the benefits of using mobile ID authentication together with NFC-compliant smartphones to open doors on a campus. In projects at **Villanova University, the University of San Francisco, and Arizona State University (ASU)**, groups of students and staff access campus

residence halls, facilities, and selected rooms using a variety of popular NFC smartphones.[17] Participants use their phones to access residence halls, and some are also using them with a unique digital key and PIN to open individual dorm room doors. Their phone is used to store and present a security credential that has been issued by campus security. To open locked doors, participants present the phone to a door reader, just as they would a student ID card.

OpenKey is a hospitality technology startup that helps hotels offer mobile room keys to guests. Their mobile app leverages Bluetooth technology for access control, and also sends guests room-ready notifications. Their technology has been pilot tested by major hotel chains, and has been integrated at several boutique hotels throughout the U.S. Once the user downloads the OpenKey app, they are issued a mobile ID credential OpenKey. This credential is used by the participating hotel to recognize the consumer, and the hotel system binds the mobile ID to a room for the period of their stay. When the user wants to enter their room, they "tap" a button in the app which unlocks the door when they are near it.[18]

6.3 Government-Issued Mobile Citizen IDs

Government-issued citizen IDs (government-to-citizen IDs) are credentials such as a driver's license or vehicle registration. For a successful implementation, the process by which mobile credentials are provided should consider implementing the following principles:

1. Be voluntary
   Participation in the program must be voluntary; the citizen should be able to control who can share the information and the device.
2. Be interoperable
   The implementation should work with major smartphone handset manufacturers and operating systems.

   The implementation should be viable across jurisdictions, states, provinces, and continents.
3. Be secure
   The implementation should be based on a strong, standards-based cryptography platform.

---

[17] Information for these use cases can be found in:
- "The Buzz on NFC," College Planning and Management, Feb. 1, 2015, https://webcpm.com/Articles/2015/02/01/Near-Field-Communication.aspx?Page=1.
- "Using NFC to replace campus one-cards with smartphones," University Business, March 2013, http://www.universitybusiness.com/article/using-nfc-replace-campus-one-cards-smartphones.
- "Villanova pilot NFC video available on YouTube, CR80News, March 30, 2012, http://www.cr80news.com/news-item/villanova-pilot-nfc-video-available-on-youtube/.
- "Villanova University Conducts Most Comprehensive NFC Access Control Trial to Date," Ingersoll Rand press release, March 21, 2012, https://investor.shareholder.com/ir/releasedetail.cfm?releaseid=658725.
- "Arizona State University tests NFC," NFC World, Sept. 14, 2011, http://www.nfcworld.com/2011/09/14/39936/arizona-state-university-tests-nfc/.
- "School Security: NFC Proves Itself on Campus," SecurityInfoWatch, July 17, 2013.
- "NFC on Campus: Using Smart Phones as Campus Credentials," Ingersoll Rand presentations, ISC West, April 10, 2013 and NAACU, April 15, 2013, http://www.iscwest.com/RNA/RNA_ISCWest_v2/docs/2013/conference-materials/NG02_NFConCampusUsingSmartPhonesasCampusCredentials.pdf?v=635007721450876632 and http://www.naccu.org/images/2013/1-NFC_on_Campus_IngersollRand.pdf.
- Arizona State University Mobile Access Pilot, HID Global case study, https://www.hidglobal.com/sites/hidglobal.com/files/resource_files/hid-asu-mobile-access-cs-en.pdf.

[18] http://www.openkey.co/news

Citizen's data should only be able to be viewed by the intended authenticating smartphone.

4. Be private
   No one else can access personal data or track identity.
   Data must be verifiable without the citizen relinquishing the smartphone.

5. Be remote capable
   A citizen's mobile ID must be securely available, even in remote areas without Internet or telecommunications networks. This requirement also applies to provisioning, updating, or revoking credentials.

6.3.1 Mobile Driver's License

Definition	Participants	Challenges
A driver's license can be provisioned to and carried on a smartphone.	Citizens Law enforcement Issuing authority Solution providers Third-party businesses and suppliers Politicians	Availability of credential offline Security of credential Complex set of industry, political and government stakeholders Education for citizens, political and government stakeholders, and law enforcement

In this use case, a driver's license is provisioned to and carried on a smartphone. The citizen can then present the driver's license as a digital credential in situations that would typically use a physical driver's license to prove identity or authorization to drive. Additionally, new use cases, where the credential could be utilized digitally, could realize increased efficiencies and value that are not possible with physical driver licenses.

6.3.1.1 VALUE PROPOSITION

Mobile driver's licenses offer the following value propositions:

- More convenience, functionality, and security than current identification methods
- Better control over personal information
- Improved law enforcement-citizen interactions
- More efficient issuing process for agencies
- Revenue opportunities for businesses and government bodies
- Standardized security across states
- Fewer false IDs due to higher security

Examples of future mobile driver's license features, functions and benefits may include:

- Real-time information for law enforcement, even if the smartphone is not functioning
- Offline verification
- Greater citizen control over what is shared
- Ability to update an address, age, organ donor status, change in driving status, endorsement, or restriction instantly
- Improved convenience for citizens: remote issuance frees citizens from waiting in long lines
- Enhanced authentication, decreasing the incidence of fraud and identity theft

- Increased capabilities that the Department of Transportation can take advantage of, such as the ability to push out public service information, register and title a car, or check records
- Visible and covert security features that are linked and layered in the digital image seen on the mobile device screen
- Use at airports by security officers to screen travelers to increase throughput
- PIN and fingerprint-based security plus facial recognition that could be used to increase ease of use to quickly access mobile driver's license

6.3.1.2 IMPLEMENTATION

No states have yet implemented a mobile driver's licenses, although the State of Iowa has recently published a request for proposals (RFP) to do so.

6.3.1.3 CHALLENGES

The following are challenges to implementing mobile driver's licenses:

- Availability. Credentials must be provisioned directly onto a mobile phone rather than just be available through the cloud, making them always available for offline verification.
- Security. Implementation must address all security concerns so that a mobile driver's license is not only seen as viable but far more secure than existing solutions.
- Complex set of stakeholders. Industry, political and government stakeholders must collaborate on implementation; no one company or stakeholder can singlehandedly make mobile driver's licenses a reality.
- Citizen attitudes/fear. Citizens must be educated that a mobile driver's license is not only more convenient but more secure than their current physical driver's license.
- Education. Politicians and state and federal authorities must be educated that a mobile ID credential protects individual rights and liberties while protecting the nation as a whole. Law enforcement must be educated that mobile driver's licenses will enhance their jobs, allowing them to do their job more effectively and safely and have better interactions with citizens. A mobile driver's license may ultimately allow police have access to real-time insurance, accident and crime information.

6.3.1.4 EXAMPLES

A number of states have enacted legislation that enables them to study or pilot mobile driver's licenses. Each implementation will allow the industry to learn in real time and apply that learning to subsequent projects, accelerating the shift to mobile credentials.

In 2015, the **Iowa Department of Transportation** conducted a 90-day pilot study of mobile driver's licenses with MorphoTrust.[19] A mobile driver's license was tested within a large group of state employees (numbering in the hundreds) who are assessing and validating the solution in situations where physical licenses are typically presented. The pilot is also testing the feasibility of updating records on the phone in real time.

[19] "Iowa Digital Driver's License Pilot Begins," Government Technology, Sept. 4, 2015, http://www.govtech.com/state/Iowa-Digital-Drivers-License-Pilot-Begins.html

The **New South Wales, Australia, state government** announced intent for a mobile driver's license.[20] The government also intends to issue digital recreational fishing licenses, responsible service of alcohol licenses, and responsible conduct of gambling licenses.

6.3.2 Mobile Vehicle Registration

Definition	Participants	Challenges
A vehicle registration credential can be provisioned to and carried on a smartphone.	Citizens Law enforcement Vehicle registration Government agencies Politicians	Availability of credential both online and offline Security of credential and of the authentication process Complex set of industry, political and government stakeholders Education for citizens, and political and government stakeholders

In this use case, a vehicle registration credential is provisioned to and carried on a smartphone. The citizen can then present the digital credential in situations that would typically use a physical credential to prove vehicle ownership or for new use cases where the credential could be presented digitally.

6.3.2.1 VALUE PROPOSITION

Mobile vehicle registration offers the following value propositions:

- Increases the effectiveness of law enforcement and transportation authorities and improves their performance
- Provides law enforcement with real-time access to vehicle registration/owner/insurance information and accident/crime data
- Improves vehicle registration fee and tax collection
- Improves convenience for citizens; supports the timely issuance of a registration
- Reduces waiting time and improves overall citizen experience; citizens must be present only to enroll

6.3.2.2 IMPLEMENTATION

There is no current implementation for a mobile vehicle registration solution – although a pilot has recently begun in Nigeria (see Section 6.3.2.4).

6.3.2.3 CHALLENGES

The following are challenges to implementing mobile vehicle registration:

- Security. Stakeholders have concerns with regard to all levels of security, including the security of information on mobile ID credentials and readers as well as authentication of the electronic information.
- Attitudes/fear. Citizens and law enforcement must be educated that mobile vehicle registration is not only more convenient but more secure.

[20] "Digital licences are coming to NSW next year, state government announces," The Sydney Morning Herald, Nov. 25, 2015, http://www.smh.com.au/technology/technology-news/digital-licences-are-coming-to-nsw-next-year-state-government-announces-20151124-gl6nob.html

- Availability. Solutions must be designed such that vehicle registration credentials are provisioned directly to a smart phone and available for law enforcement to securely verify both online and offline. Offline verification also enables interoperability among different governing jurisdictions.
- Complex set of stakeholders with differing agendas. Motor vehicle agencies and law enforcement must hold a shared vision. Political leadership and vision are required.

6.3.2.4 EXAMPLES

The **Nigerian Police Force** has embraced mobile vehicle registration to improve the security and effectiveness of the government's vehicle registration program. In this program, vehicle registration credentials will be delivered to the smartphones of Nigerian citizens.[21]

Nigeria has a population of 170 million people (nearly one-quarter of Africa), with an estimated 50 to 60 million vehicles on the road. Driver data and vehicle data are held in different databases and are not always readily available to the police out in the field. To remedy the situation, the Nigerian Police adopted a mobile Biometric Central Motor Registry (BCMR) to provide real-time access to biometrically verifiable information as well as ongoing access to accident and crime data.

In the first phase of the project, citizens register their vehicles into a biometrically enabled central database and receive an RFID credential with encrypted data based on HID Global's Seos® technology. An officer approaching a registered vehicle can use the card's advanced visual security to verify the driver's appearance matches the biometric information and further access all credential, insurance, and accident information in real time using a handheld reader.

The second phase of the project will migrate to full-scale mobile vehicle registration. HID Global, in conjunction with local partner Media Concepts, will facilitate the delivery of vehicle registration credentials to the smartphones of Nigerian citizens, using HID Global's Seos-based goID™ mobile infrastructure. Compatibility between the card and the mobile credential means that a single reader can be used for verification. As the project matures, smartphones could ultimately be deployed as readers.

Two additional advantages of this use case are that (1) the registration is issued immediately (once the paperwork is processed), and (2) a citizen will only have to be present to enroll.

6.3.3 Mobile Recreational Licenses

Definition	Participants	Challenges
A license for hunting, fishing, gun ranges, or other sports and outdoor activities can be provisioned to and carried on a smartphone.	Citizens State game enforcement wardens Issuing authority Solution providers Politicians	Availability of credential both online and offline Security of credential Citizen privacy Security of cloud-based services

In this use case, recreational licenses are provisioned to and carried on a smartphone. The citizen can then present the digital credential in situations that would typically use a physical credential or for new use cases where the credential could be presented digitally.

[21] "HID Global Launches First Mobile ID Program in Nigeria with Partner Media Concepts," HID Global press release, May 12, 2016, https://www.hidglobal.com/press-releases/hid-global-launches-first-mobile-id-program-in-nigeria-partner-media-concepts.

6.3.3.1 VALUE PROPOSITION

Mobile recreational licenses offer the following value propositions:

- More convenient, up-to-date, and secure than current paper licenses
- Easier to locate for the user
- More efficient issuance process
- Easier communications with citizens. Issuers can more easily broadcast information to users about service, weather, alerts, renewals, or policy updates and can connect users to additional resources (such as maps)
- Additional revenue opportunities for issuing agencies

6.3.3.2 IMPLEMENTATION

Mobile recreational sports licenses can either be issued as a standalone ID credential or be incorporated as an additional data field in a mobile driver's license and carried on a smartphone. Many states currently offer access to mobile permits for upland game, turkey, fishing and associated stamps. Relying on visual authentication alone of the mobile device, however, leaves room for potential counterfeiting. Therefore, increased security will be realized by association with a provisioned mobile ID credential.

6.3.3.3 CHALLENGES

The following are challenges to implementing mobile recreational licenses:

- Security of credential. All security concerns must be addressed so that any mobile document or license is seen as both viable and adding to the overall security of an individual's digital presence.
- Privacy. All personal privacy concerns must be addressed (based upon the amount of information that is/will be accessible via a mobile ID credential on a smartphone).
- Security of new cloud-based services. State licensing departments' concerns about perceived vulnerabilities to databases and issuing/business processes must be addressed.
- Availability. Credentials must be provisioned directly onto a mobile phone rather than just being available through the cloud, making credentials always available for offline verification.

6.3.3.4 EXAMPLES

The **New South Wales, Australia, state government** is gearing up to deliver digital recreational fishing licenses in 2016.[22] These licenses eliminate the need to stand in line and allow individuals in rural areas to avoid a long commute to service centers or licensing bureaus. This effort is part of a larger digital license program that will roll out nearly 770 types of licenses and identification cards over the next several years. The first licenses to go mobile will be recreational fishing licenses, responsible service of alcohol licenses, and responsible conduct of gambling licenses.

[22] The Sydney Morning Herald, op. cit.

6.4 Mobile Contactless Payments

Definition	Participants	Challenges
A transfer of funds in return for goods or services in which a mobile device is involved in initiating and confirming payment	Issuers Merchants Acquirers Payment networks POS and terminal hardware and software providers Mobile wallet (app) providers	Complex security methodology Complex ecosystem

Mobile contactless payments are initiated by a mobile device at the merchant POS device. To make the payment using a mobile device, the consumer taps the mobile device close to (no more than 4 cm from) the POS device. The payment application is invoked, and the consumer is authenticated before the credit or debit card details are sent to the POS device using NFC. The POS device contacts the issuer bank before approving the payment transaction.

As in a regular credit and debit card transaction, the issuer defines the required authentication. A PIN or passcode required to unlock the mobile device represents an additional authentication factor.

If a mobile device used for contactless payments is lost, the issuer bank can send a request to deactivate the payment application or block the consumer's credit or debit card.

6.4.1 Value Proposition

Contactless payments using a mobile device offer the following value propositions:

- Convenience. Users can carry several payment credentials on a single device.
- Familiarity. The transaction is similar to a credit or debit card transaction.
- Speed. An NFC tap-and-pay transaction is faster than a contact EMV transaction where the card is inserted into a reader. On-device consumer validation (such as a fingerprint) can eliminate the requirement to enter a PIN.

6.4.2 Implementation

Consumer credit or debit account information can be stored in an SE or accessed using HCE (see Section 5).

In smartphones, an SE can be an enhanced SIM card or a chip embedded directly in the phone's hardware. The issuer's payment application and consumer's payment account information are stored securely in the SE, and the payment application actually emulates a contactless card during the payment transaction. HCE stores the consumer payment account information in a cloud database; the information is tokenized, and the token is stored on the phone.

The payment application authentication methods chosen should be based on industry best practices, such as PCI DSS, dynamic cryptograms, and multifactor authentication.

6.4.3 Challenges

The following are challenges to implementing mobile contactless payments:

- Complex security methodology. HCE is more flexible than secure elements, but needs a more complex cloud system and stronger cryptograms. Secure elements require complex solutions to accomplish provisioning.
- Complex ecosystem. Many entities are involved in payment processing and need to update system capabilities to support mobile payments.

6.4.4 Examples

Android Pay[23] is a mobile payments platform developed by Google to perform tap-to-pay purchases with mobile devices that run the Android OS. Android Pay uses NFC to transmit card information to the retailer's POS device. The consumer uses a passcode, pattern, or a fingerprint to activate Android Pay. Android Pay uses tokenization and HCE to store card information securely.

Samsung Pay[24] uses NFC to process payments at tap-to-pay or contactless terminals. Samsung Pay authenticates the consumer payment transaction using a fingerprint or a PIN. Samsung Pay uses tokenization to protect payment information; the account or credit card numbers are not stored on the device. Each time a purchase is made, Samsung Pay transmits a 16-digit token that represents the credit or debit card number along with a one-time code or cryptogram that is generated by the phone's encryption key.

Apple Pay[25] uses NFC and a tokenization mechanism to process contactless payment transactions at the POS using iPhone devices. Apple Pay first requires the consumer to enroll using biometrics (finger print/Touch ID) as the identifying mechanism. Consumers then register their credit or debit cards in the Apple Wallet as a one-time registration and payment tokens are assigned by the payment networks. The payment tokens are stored securely in the secure element on the iPhone device. During a contactless payment transaction using Apple Pay, the consumer is authenticated using fingerprint/Touch ID (biometric authentication) and, once authenticated, payment token information is transferred from iPhone device to POS using NFC (emulating a contactless card transaction).

6.5 Remote Payments

Definition	Participants	Challenges
A transfer of funds or payment using a mobile device when the payer and payee are not physically close to each other	Issuers Merchants Acquirers Payment networks Mobile app providers, web browsers	Stronger authentication method requirement Complex ecosystem

Remote payments are performed using a Web browser on a mobile device or smartphone application installed on a mobile device. The mobile device is used to authenticate the consumer's personal information remotely during the payment transaction. Remote payments can also be made using SMS text messages or carrier billing. Remote payments can be used to perform eCommerce and mCommerce payment transactions.

[23] https://www.android.com/pay/
[24] http://www.samsung.com/us/samsung-pay/
[25] http://www.apple.com/applepay/

6.5.1 Value Proposition

Remote payments using a mobile device offer the following value propositions:

- Convenience. Users can complete payment transactions using standard security methods.
- Familiarity. The transaction is similar to a credit or debit card transaction.

6.5.2 Implementation

Remote payments completed using a mobile app (in-app) and eCommerce payments using a mobile Web browser can leverage a payment credential stored on the device or complete transactions using a "card on file" in the remote system using authentication information stored in a secure area of the mobile device.

In typical remote payment transactions, the mobile device acts as a trusted device; the user must activate the payment from the device. During payment authorization, the payment application or Web application validates the user credentials. Users are authenticated by a password, PIN, or biometric factor, as determined by the mobile application or website that accepts the payment. Additionally, issuers can mandate two-factor authentication, requiring something the user has (e.g., the mobile device) and something the user knows (e.g., a PIN).

For payment transactions initiated from an app, user authentication can be handled using fingerprint recognition or another biometric factor. A PIN or passcode required to unlock the mobile device represents an additional authentication factor. Similarly, in financial payment transactions using websites, the user can enter the payment credentials over a secure Wireless Application Protocol (WAP) interface. Before completing the payment transaction, the user can be authenticated by entering a PIN or password that has been sent to the mobile device.

6.5.3 Challenges

The following are challenges to implementing remote payments:

- Stronger authentication method requirement. As with other Web browser-based approaches, stronger authentication methods than username and password are needed.
- Complex ecosystem. Mobile applications and Web browser applications need to update system capabilities to support mobile payments.

6.5.4 Examples

Paypal allows payments and money transfers to be made over the Internet using a mobile device on which the Paypal application is installed. The application requires that the user enter a PIN or use a fingerprint before authorizing the financial transaction.

6.6 Biometrics for Financial Services Access

Definition	Participants	Challenges
Use the capabilities of a mobile device to augment security schemes that authenticate users of online or mobile services offered by a financial institution	Financial services provider End user Mobile app provider Mobile security services provider	Proliferation of approaches and lack of industry-wide standards Lack of standard metrics to compare relative security/reliability of biometric techniques Willingness of consumers to adopt new security approaches Privacy concerns

In this use case, the mobile device's ability to capture biometrics is used to authenticate the user prior to accessing online financial services.

6.6.1 Value Proposition

Using a mobile device to authenticate users of online or mobile financial services offers the following value propositions:

- Convenience. Users can access services from their mobile devices rather than a desktop or laptop.
- Simplification. Users can access secured services using their mobile devices without the need to enter complex passwords on a small screen.
- Security. Providers can leverage multiple data points to validate that a user is authorized to access services.

6.6.2 Implementation

Authentication can be active, requiring the customer to scan a fingerprint rather than enter a password or PIN, or passive, such as by recognizing the location of the user's device.

Authentication can be based on biometric factors (such as fingerprints, finger and palm vein technology, facial recognition, eyeprints, or heartbeats), behavioral factors (recognizing a person's cognitive and physiological traits, such as how the person swipes, types, or uses a phone; left/right handedness; pressure; and hand tremor), voice recognition (creating and recognizing a unique voice print), device fingerprinting and geolocation.

6.6.3 Challenges

- Proliferation of different approaches and lack of industry-wide standards can limit adoption by issuers. Many issuers will wait until standards emerge and are widely adopted before implementing solutions on their platforms.
- Lack of standard metrics to compare relative security/reliability of biometric techniques means there are security risks if new attack methods evolve.
- Lack of willingness of consumers to adopt new security solutions could delay adoption rates and delay general market education and acceptance.

- Privacy concerns regarding how much information on a biometric image is stored and where it is stored could limit consumer's willingness to use the technology.

6.6.4 Examples

Financial institutions are relying on a variety of biometric factors to authenticate users accessing their services on a mobile device. Examples include the following:

- Spurred on by the Apple iPhone TouchID, many banks are replacing passwords in their apps with fingerprints.
- In Poland, more than 1,700 ATMs are equipped with finger vein technology, and palm vein technology is being used in Japanese ATMs.[26]
- Both Mastercard and USAA are using facial recognition to authenticate customers.[27]
- Mountain America Credit Union is experimenting with Eyeprint ID in its mobile banking app.[28]
- UK bank Halifax, owned by Lloyds Banking Group, is trying out technology that uses a customer's heartbeat to authenticate access to its digital financial services.

Behavioral authentication is being used in a number of implementations, including the following:

- A number of banks in North America, Europe, and Latin America are using Biocatch, which proactively collects and analyzes more than 400 cognitive parameters to generate a unique user profile.[29]
- Nationwide Building Society won an award for its use of BehavioSec, which analyzes the user's physical usage patterns on a smartphone or tablet to establish uniquely identifiable behavioral profiles.[30]

And finally, many banks are using voice recognition to improve the customer experience with both mobile and call centers. Organizations using voice recognition include the following:

- Canadian bank Tangerine combines voice recognition with speech recognition, using Nuance for voice banking users to interact with the mobile banking app through a conversational interface.
- USAA, ING, US Bank, and the Polish banks Meritum Bank and Bank SMART all use voice recognition.
- Wells Fargo is using SpeechPro's biometric technology, which combines voice, facial, and anti-proofing "liveness" tests to authenticate customers.[31]
- Varam Capital, a provider of micro-finance inclusion solutions in India, is using SayPay to authenticate payment transactions with voice.[32]

---

[26] Warwick Ashford, "HSBC launches biometric security for mobile banking in the UK," *Computer Weekly*, Feb. 19, 2016, http://www.computerweekly.com/news/4500273410/HSBC-launches-biometric-security-for-mobile-banking-in-the-UK.

[27] EyeVerify, "What's the real story with biometrics and mobile banking?" Jan. 29, 2016, http://www.eyeverify.com/blog/whats-the-real-story-with-biometrics-and-mobile-banking.

[28] Ibid.

[29] Early Warning press release, Apr. 14, 2015, https://www.earlywarning.com/news/press-releases/2015/early-warning-biocatch-align-to-help-fight-fraud-improve-mobile-online-experience.html.

[30] Justin Lee, "Unisys and BehavioSec behavioral biometric prototype for Nationwide wins award," *Biometric Update.com*, May 26, 2016, http://www.biometricupdate.com/201605/unisys-and-behaviosec-behavioral-biometric-prototype-for-nationwide-wins-award.

[31] Kate, "Biometrics in Banking: Who Is Killing the Passwords in 2016?" *Let's Talk Payments*, Feb. 24, 2016, https://letstalkpayments.com/biometrics-in-banking-who-is-killing-the-passwords-in-2016/.

7 Conclusions

Mobile identity authentication is a rapidly evolving series of techniques to simplify the user experience across a wide range of connected services. The ubiquitous nature of smartphones makes them a handy platform for authentication. The use cases described in this paper are evidence of the strong interest in mobile identity authentication by both users and service providers. Applications in payments, government identity, and access control are likely just the beginning of a long list of services to be securely simplified via mobile identity authentication. For each application, security, privacy and flexibility are considerations that need the proper trade-offs. In addition, offline authentication considerations are critical in many applications, putting the burden on the implementation to be highly secure, yet usable on a mobile smart device.

A significant value proposition for mobile ID authentication comes from a powerful combination of the convenience provided to users together with the enhanced data available from smart devices. Consumers no longer need to struggle with long passwords nor carry around extra devices (e.g., passcode generators). They can simply press their fingers to a sensor, or stare into a locked phone screen (for an iris scan) to gain secured access to a variety of services from their smart devices. Likewise, service providers benefit from both the competitive advantage of offering a more convenient service, and the added security provided when they leverage the on-device security (e.g., embedded secure element) and the enhanced data from smart device, such as biometrics and location.

The mobile and computing industries recognize the potential, but also recognize the security and costs risks if each application chooses a unique method for mobile ID authentication. There are both established and emerging standards for securing cryptographic keys and biometric templates on devices, as well as processing the authentication between a mobile smart device and the relying party service provider. Several of these techniques are described in this paper. The Secure Technology Alliance encourages all technology providers to adopt established standards where possible, and assist in developing new standards where appropriate.

[32] "Varam Capital Embraces SayPay Authentication," FindBiometrics, Jan. 7, 2016, http://findbiometrics.com/varam-capital-embraces-saypay-authentication-301074/

8 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance Mobile Council to provide an educational resource on mobile identity authentication techniques and use cases.

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 of this white paper included: Capgemini; CH2M; CPI Card Group; Discover Financial Services; Entrust Datacard; First Data; FIS; Giesecke & Devrient; GlobalPlatform; HID Global; ID Technology Partners; Intercede; IQ Devices; JPMorgan Chase; Oberthur Technologies; Paygility Advisors; SHAZAM; TSYS; Vantiv; Verifone; Wells Fargo.

The Secure Technology Alliance thanks **Tony Sabetti**, JPMorgan Chase, for leading the project and the following Council members who wrote content and participated in the project team for this document:

- **Deborah Baxley**, PayGility Advisors
- **Hank Chavers**, GlobalPlatform
- **Chris Edwards**, Intercede
- **Sarah Hartman**, TSYS
- **Cathy Medich**, Secure Technology Alliance
- **Jean-Louis Meyer**, Entrust Datacard
- **Manish Nathwani**, SHAZAM
- **Joseph Pearson**, HID Global
- **Lokesh Rachuri**, Capgemini
- **Steve Rogers**, IQ Devices
- **Tony Sabetti**, JPMorgan Chase
- **Brian Stein**, CH2M
- **Mike Strock**, Secure Technology Alliance
- **Lars Suneborn**, Secure Technology Alliance
- **Sree Swaminathan**, First Data
- **Sanjay Varghese**, Discover Financial Services
- **Rob Zivney**, ID Technology Partners

The Secure Technology Alliance also thanks Council members who participated in the review of the white paper including:

- **Philip Andreae**, Oberthur Technologies
- **Amanda Guillen,** Discover Financial Services
- **Imran Hajimusa,** Verifone
- **Peter Ho,** Wells Fargo
- **Damon Kachur**, Giesecke & Devrient
- **Umesh Kulkarni,** FIS
- **Christine Lopez,** Vantiv

Trademark Notice

About the Secure Technology Alliance Mobile Council

The Secure Technology Alliance Mobile Council focuses on building industry awareness around the business and security impacts of utilizing different technologies for distributing, storing and using secure credentials on personal mobile and tethered wearable devices. The Council believes raising awareness will facilitate broader discussion on creating standards. The Council creates resources to help implementations and accelerate the adoption of payments, loyalty, marketing, peer-to-peer, identity, and access control applications using mobile and tethered wearable devices. The Council focuses on activities that will help to educate the industry on implementation and security considerations and will act as a bridge between technology development/specification and the applications that can deliver business benefits to industry stakeholders. Additional Council information can be found at http://www.smartcardalliance.org/activities-councils-mobile-council/.

9 Appendix A: FISMA Security Objectives

The Federal Information Security Management Act (FISMA) defines three security objectives for information security: confidentiality, integrity, and availability. In addition, the Federal Information Protection Standard (FIPS) provides various examples of the impact resulting from loss of any of the defined security objectives (Table 4). Each of the use cases in Section 3.2, Table 3 has been evaluated for objective and impact according to these standards.

Table 4. FIPS Impact Definitions for Security Objectives

Security Objective	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

10 Appendix B: Glossary

Secure Element (SE). Secure component that comprises autonomous, tamper-resistant hardware within which secure applications and their confidential cryptographic data (e.g., key management) are stored and executed. There are three different form factors for an SE: Universal Integrated Circuit Card (UICC), embedded SE, and smart microSD. Both the UICC and smart microSD are removable. Each form factor links to a different business implementation and satisfies a different market need.

Trusted Execution Environment (TEE). A secure area of the main processor in a smart phone (or any connected device) that ensures that sensitive data is stored, processed, and protected in an isolated, trusted environment. The TEE's ability to offer isolated safe execution to authorized security software, known as trusted applications, enables it to provide end-to-end security by enforcing protection, confidentiality, integrity, and data access rights. The TEE offers a level of protection against software attacks, generated in the rich OS environment. It assists in the control of access rights and houses sensitive data.