GLOBALPLATFORM®

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

# Mobile ID:

## Realization of Mobile Identity Solutions by GlobalPlatform Technologies

*White Paper*

*November 2015*


secretariat@globalplatform.org | www.globalplatform.org | 

## Table of Contents

**About GlobalPlatform**

GlobalPlatform defines and develops specifications to facilitate the secure deployment and management of multiple embedded applications on secure chip technology. Its standardized infrastructure empowers service providers to develop services once and deploy across different markets, devices and channels. GlobalPlatform's security and privacy parameters enable dynamic combinations of secure and non-secure services from multiple providers on the same device, providing a foundation for market convergence and innovative new cross-sector partnerships.

GlobalPlatform is *the* international industry standard for trusted end-to-end secure deployment and management solutions. The technology's widespread global adoption across finance, mobile/telecom, government, healthcare, retail and transit sectors delivers cost and time-to-market efficiencies to all. GlobalPlatform supports the long-term interoperability and scalability of application deployment and management through its secure chip technology open compliance program.

As a non-profit, member-driven association, GlobalPlatform has cross-market representation from all continents.  130+ members contribute to technical committees and market-led task forces. For more information on GlobalPlatform membership visit www.globalplatform.org.

**Publication Acknowledgements**

GlobalPlatform wishes to offer special thanks to the members of the Mobile Task Force and their respective organizations for their involvement in developing this white paper.

Contributors include the following:

*Members:*

Padmakumar Subramani – Alcatel-Lucent

Kennie Kwong – AT&T

Beatrice Peirani – Gemalto

Alexander Summerer – Giesecke & Devrient

Philip Hoyer – HID Global

Jean-Philippe Galvan – Samsung

*GlobalPlatform Team Members:*

Kevin Gillick – GlobalPlatform – Executive Director

Gil Bernabeu – GlobalPlatform – Technical Director

Hank Chavers – GlobalPlatform – Technical Program Manager

Lee'Ann Kaufman – iseepr – Managing Director

Adam Powers – Alliances Management – Operations Secretariat

Kathleen Carter – Alliances Management – Technical Writer

Meagan Schuver – Alliances Management – Technical Writer

## Intended Audience

This white paper provides product managers and business analysts with a brief overview of market opportunities for Mobile ID in various market sectors, and informs system integrators and engineers how GlobalPlatform technologies can be used to implement Mobile ID solutions.

## Executive Summary

Mobile devices are more than just a way of communicating. Mobile devices are used for email, social media, gaming, banking, photos. Mobile devices are used for both business and personal use, and today mobile phones are used more widely than personal computers. Mobile ID can replace plastic cards, badges, and ID cards and allow users to complete identification, authentication, payments, and even digital signatures. Previous methods of physical personal identification can be stored or accessed in the mobile device, eliminating the need to carry a wallet, or wait for replacement cards to come in the mail.

As the ubiquity of mobile devices changes how people engage in day-to-day activities, it also increases security concerns about the information stored or accessed by these devices. To be trusted, Mobile ID schemes call for the enforcement of privacy and security requirements.

GlobalPlatform is responsible for driving global standardization of Secure Elements (SEs) and Trusted Execution Environments (TEEs) and its specifications can be used to leverage Mobile ID solutions and to meet the security requirements for Mobile ID deployments for a wide variety of markets, such as government-to-citizen, government-to-government, enterprise, eHealth, financial, and commercial.

The GlobalPlatform infrastructure robustly safeguards the security, integrity, and privacy of services deployed on a platform alongside services from other providers. Only a service provider can access and control their own services; there is no security risk from, or to, other services sharing the platform, making it the ideal technology for Mobile ID applications.

For Mobile ID service providers there are many decisions to be made when creating a new Mobile ID deployment. The most important being how to acquire credentials, what type of authentication is needed, and which combination of execution environments will best fulfil the needs of the application in regards to viability, security, deployment, and usability.

This white paper primarily discusses how credentials can be managed and implemented in an SE or in a TEE using GlobalPlatform Specifications. The paper examines the management of these credentials by remote credential management systems which use the GlobalPlatform Messaging Specifications for Trusted Service Management. Futhermore, it outlines on different implementation levels how standard Mobile ID applications and authentication protocols like FIDO (online authentication), GSMA Mobile Connect (telecommunication sectors), VPN RADIUS (enterprise sectors), TLS (web authentication), PIV (U.S. government specifications), and eIDAS (EU regulation with respective ISO/IEC, ETSI and CEN standards) can be implemented on a TEE/TUI or SE, in order to securely store credentials, protect applications, or secure the user interface. Finally, this paper discusses Mobile ID architecture and implementation scenarios for combinations of the Rich Execution Environment (REE), the SE, or the TEE as platforms for the Mobile ID applications. This paper is focused on an architectural and administrative view and refers to other documents for topics like privacy considerations, security mechanisms, and technical specifications.

## SECTION 1: Introduction

Mobile ID, also referred to as Mobile Identity, is a rapidly growing market that enables mobile devices to be used as proxies or replacements for traditional identity cards and badges. The Mobile ID movement is primarily focused on using a smartphone as an enterprise badge, a government ID, or a driver's license; however, the concept can be applied to any combination of identification card and mobile device. Mobile ID can be issued independently and be used as a wholesale substitute for a physical ID card, or it can be derived from already issued physical ID cards and used as a convenient digital alternative. Mobile ID provides a number of benefits: it enables mobile-based identification use cases, it is more convenient for users, and it is cost effective for deploying agencies when leveraging the digital transformation. According to the Security Identity Alliance, it is anticipated that digital transformation saves governments worldwide up to $50 billion annually by 2020[1].

The deployment of Mobile ID has a number of considerations, including ID management and user enrollment; the issuance and life-cycle-management of credentials; the usage and storage of credentials; and ultimately the uses of Mobile ID for authentication, authorization, encryption, and signatures in a number of different scenarios. Some of the interoperability, security, and scalability challenges associated with the deployment and management of Mobile ID are being solved by a number of standards and technologies.

GlobalPlatform plays an important role in standardizing secure components, including Trusted Execution Environments (TEEs) and Secure Elements (SEs).

- The TEE is a secure area of the main processor in a smartphone (or any connected device) that ensures sensitive data is stored, processed, and protected in an isolated, trusted environment. The TEE's ability to offer isolated safe execution of authorized security software, known as 'Trusted Applications', enables it to provide end-to-end security with secure endpoints on devices and secure connections to remote endpoints. This is achieved by enforcing protection, confidentiality, integrity, authenticity, originality, 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 applications, which need to be isolated from the Rich OS.

  For a brief overview of the TEE, refer to Appendix A; or, for a more in-depth review, refer to the TEE White Paper [TEE WP].

- The SE is a secure component which comprises autonomous, tamper-resistant hardware within which secure applications and their confidential cryptographic data (e.g. key management data) are stored and executed. The three most popular form factors of SE are the 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. With GlobalPlatform specifications regardless of which form factor is used all SE implementations can be managed the same way.

---

[1] 'Research: eGovernment services would yield up to $50 bn annual savings for Governments globally by 2020', November 2013, available at https://www.secureidentityalliance.org/index.php/resources.

The TEE and SE enable Mobile ID applications to be implemented in a secure way and are essential to fulfill specific privacy and security requirements by providing platforms which deny disclosure of confidential credentials and allow the execution of applications in secure environments. GlobalPlatform technologies can also be used in combination with a Rich Execution Environment (REE), controlled by a Rich OS. Depending on the application, the single use or combination of these three elements can address the varying requirements of Mobile ID schemes.

The goal of this white paper is to introduce various Mobile ID implementation scenarios and offer solutions using the REE, and the REE in combination with GlobalPlatform's standardized SE or TEE.

To assist with mapping out these scenarios, this paper provides background on Mobile ID and explores how Mobile ID solutions can be securely implemented based on GlobalPlatform technologies and specifications for cards, devices, and systems.

The following sections investigate the Mobile ID landscape, including its market potential, key use cases, and enabling technologies. The document then explores the steps of deployment and application and their use cases, followed by Mobile ID architecture, and security. Finally, four implementation scenarios for combinations of the execution environments using the REE and GlobalPlatform's SE and TEE are presented.

## SECTION 2: Market Segments Impacted by Mobile ID

As an increasingly important part of the field of identity management, Mobile ID holds the promise of providing the traditional identity management functionality of authentication, authorization, and policy enforcement, through consideration of privacy aspects, while offering convenience and innovative applications associated with the booming smartphone market. Many countries have already deployed a countrywide Mobile ID for government applications. Some examples of deployments are Estonia[2], Moldova[3], Finland[4] and Austria[5].

The security, reliability, and flexibility of government issued Mobile IDs has inspired a number of commercial applications, involving the healthcare, finance, retail, and enterprise sectors, to name a few. The following section gives a brief overview of the vast market segments where Mobile ID will have a significant impact.

### 2.1. Government-to-Citizen

The most obvious and prevalent use of Mobile ID takes the form of government issued identification for citizens, ranging from identification cards to drivers' licenses to passports.

Mobile ID not only provides government agencies with a more secure way of identifying citizens, but it streamlines the infrastructure and lowers deployment costs, enabling a broad range of eServices[6]. Considering that most citizens already have mobile devices which can be used to host Mobile IDs, the deployment of Mobile ID can drive the dematerialization of any public services involving citizen authentication and identification.

A broad variety of eServices have already been deployed by governments using digital identity programs:

- **Digital Voting**: Governments can offer online voting backed by anonymous or pseudonymous identification, authentication and / or authorization.
- **Tax Collection**: Governments can track citizen income, withholdings, benefits, deductions, declarations, and other information from multiple government databases, as well as enabling digital signing during tax preparation[6].
- **Social Welfare Program Access**: Governments can enable secure access to benefits and track current and potential benefits to citizens across multiple agencies. This offers the possibility to declare or update unemployment status, and to request social minimum payment.
- **Travel Authorization and Security**: Governments can request secure identification of airline, train, and other passengers for threat assessment. There may also be visa application possibilities.

---

[2] https://e-estonia.com/component/mobile-id/

[3] http://www.moldova.org/the-service-mobile-signature-launched-in-moldova-232925-eng/

[4] http://www.mobiilivarmenne.fi/en/

[5] https://www.buergerkarte.at/en/

[6] 'e-Tax', *e-Estonia*, https://e-estonia.com/component/e-tax/.

- **Census and Population Registrar**: Governments may hold a centralized database of citizens containing their basic information, such as name, date of birth, address, language, education, and profession[7]. Citizens may be able to renew identity documents, declare birth/death/marriage, and request certificates.
- **Police Services**: Police may have access to multiple databases during a traffic stop, including motor vehicle records, criminal records, insurance records, weapons registries, and more[8].

Estonia, for example, deployed a smart card-based digital identity system in 2002 that offers citizens a personal identification credential combined with a credential for both transportation and electronic voting[9]. In 2007, Estonia launched a Mobile ID system[10] that enabled augmenting or replacing smart cards with the SIM cards in mobile phones[11].

### *2.1.1. eIDAS Framework in Europe*

The eIDAS Framework in Europe is an example of Government-to-Citizen use cases in action. The European Union is currently introducing a regulation for Electronic Identification and Trust Services (eIDAS). Initially published in the summer of 2014[12], it will replace *Directive 1999/EC/93 on a community framework for electronic signatures* and introduce several trusted services, in addition to electronic signatures – all legally recognized by all member states. The services include electronic authentication, electronic seal (electronic signature for legal entity), electronic time-stamp, electronic documents, electronic delivery services, and website authentication. Electronic identification will remain a national prerogative, but whenever an electronic identification is used, all other member states should recognize it.

The eIDAS Token Specification [BSI] [eIDAS Token] proposes an Interoperability Framework for electronic identification, compliant with the mobile environment. The specification provides a modular and homogeneous SE API to protect the authenticity, integrity, confidentiality, and privacy of the data stored on tokens in different form factors for electronic identification, authentication, and signatures. The German identity card is already compliant to the eIDAS token specification. It is intended to also be deployable as mobile ID on an SE.

Several electronic use cases have already been targeted, such as student enrollment in a university abroad, tax declaration submission to another member state, public call for tender for companies abroad or signing contracts with partners abroad. The applications

---

7 'Population Register', *e-Estonia*, https://e-estonia.com/component/population-register.

8 'e-Police', *e-Estonia*, https://e-estonia.com/component/e-police/.

9 'Electronic ID Card', *e-Estonia*, https://e-estonia.com/component/electronic-id-card/.

10 'Avaleht > Mobiil-ID > ID.ee', http://www.id.ee/index.php?id=36810.

11 'Mobile-ID', *e-Estonia*, https://e-estonia.com/component/mobile-id/.

12 'Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC',

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

of this legal framework are primarily government-to-citizen, but could potentially be used in other application fields such as healthcare, finance, and government-to-government.

### 2.2. Government-to-Government

In addition to facilitating government-to-citizen interactions, Mobile ID can be a benefit to government-to-government interactions. Such interactions include, for example, inter-agency authentication as an employee or contractor and determining policy-based access to third-party agency resources.

In general, digital identity programs can facilitate inter-agency information sharing about citizens by establishing a decentralized unique identifier system for citizens that allows agencies to link data across their corresponding databases[13]. Mobile ID can further this benefit by making the use of digital identity more pervasive and by further integrating more data into an already broad ecosystem of information sharing.

As an example, National Institute of Standards and Technology (NIST) released the Personal Identification Verification (PIV) derived credential standard [SP 800 157], which allows employees of U.S. federal agencies to derive a Mobile ID from their PIV card badges to access federal services online from a mobile device[14].

### 2.3. Enterprise

While government issued digital identification can be a benefit to enterprises, such as when establishing a right to work, enterprises can also benefit from using Mobile ID as a replacement of, or augmentation to, their existing enterprise-issued badging and authorization systems. This includes granting employees and contractors access to both physical facilities and online systems using a centralized, secure identification system. Enterprise-issued identification systems can also be backed by government-issued identification. Government identification can be used, for example, as a more standard and secure form of second-factor authentication.

The Smart Card Alliance defines a Commercial Identity Verification (CIV) ID card specification for the enterprise market which is based on the PIV standard FIPS 201 [FIPS 201]. With CIV, enterprises can also take advantage of the PIV derived credential technology that enables Mobile ID deployments[15].

### 2.4. eHealth

While healthcare applications can be very similar to enterprise applications—maintaining badging and authentication for healthcare providers, for example—the sensitivity and importance of healthcare means that digital identity can provide additional benefits. These benefits parallel many of those associated with existing health cards, including:

---

[13] 'X-Road', *e-Estonia*, https://e-estonia.com/component/x-road/.

[14] 'Guidelines for Derived Personal Identity Verification (PIV) Credentials, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf.

[15] The Commercial Identity Verification (CIV) Credential–Leveraging FIPS 201 and the PIV Specifications, http://www.smartcardalliance.org/publications-the-commercial-identity-verification-civ-credential-leveraging-fips-201-and-the-piv-specifications/.

- **Patient Record Tracking**: Ensures that diagnoses, allergies, and patient histories are associated with the right patient.
- **Patient Information Sharing**: Enables multiple healthcare providers and specialists to securely find and share information about a patient[16].
- **Patient Declaration:** Offers official notification and tracking of sick leave.
- **Prescription Tracking**: Enables patients to securely and easily fill out prescriptions.
- **Insurance**: Associates services with patient insurance plans.

### 2.5. Financial

The financial sector can use digital identification provided both by the government and through their own privately-issued identification (such as bank cards). Not only can financial institutions increase security and reduce fraud expenses through digital identity, but Mobile ID can provide a convenient form of digital signature enabling new secure financial and banking applications.

As an example PostFinance in Switzerland is offering their bank customers Mobile ID services[17]. In Turkey, bank customers at several banks can use a Mobile ID for online banking[18] [19].

### 2.6. Commercial

Identification is currently used in diverse ways in commercial applications, ranging from age verification for restricted transactions (e.g. alcohol, tobacco, firearms), to verifying legal eligibility for services (e.g. driver's license verification for rental car services), and identification for reservations (e.g. airline and hotel). While Mobile ID may serve as a more convenient way of enabling these services, innovation through mobile applications can enable new ways of performing these services. An example of a Mobile ID deployment in e-commerce is the FIDO implementation of PayPal which allows consumers to authorize payment transactions at online-shops using FIDO authentication on supported devices[20].

Across all market segments, the motivation to deploy a Mobile ID solution is to serve as a convenient alternative or innovative replacement to other costly and untechnical identification methods. Once Mobile ID has been identified as a solution for the market

---

[16] 'Electronic Health Record', *e-Estonia*, https://e-estonia.com/component/electronic-health-record/.

[17] 'Mobile ID' PostFinance, https://www.postfinance.ch/en/priv/prod/bcase/pk14/127.html.

[18] http://www.teb.com.tr/security/turkcell-mobile-signature/

[19] http://www.garanti.com.tr/en/personal_banking/delivery_channels/internet_banking/security/mobile_signature/turkcell_mobile_signature.page

[20] http://www.prnewswire.com/news-releases/samsung-and-paypal-select-nok-nok-labs-to-power-the-first-fido-ready-authentication-ecosystem-256153881.html

segment, the next variable for service providers to consider how to access the credentials necessary for a Mobile ID application.

## SECTION 3: Mobile ID Derivation and Deployment

Regardless of market segment or use case, all Mobile ID applications need to access the identification credentials. A Mobile ID is implemented as an application in a mobile device; the application can be used to perform local or remote identification, authentication, and authorization. A Mobile ID application typically stores personal information, passwords, and cryptographic keys. The Mobile ID can be created either by generating the identification credentials in the mobile device directly, or by generating the identification credentials in a backend system and downloading the identification credentials remotely to the mobile device.

A Mobile ID could also be derived from an existing physical ID card. In this case, the Mobile ID serves as a second identification credential beside the identification credentials of the physical ID card. This allows identification credentials in a mobile device to be used directly without the need to use the physical ID card on the mobile device.

The following sections discuss the derivation and deployment of Mobile ID for the use cases previously described in Section 2.

### 3.1. Generated Credentials

A Mobile ID can either be created by generating the ID credentials in the mobile device locally or by downloading the credentials from a remote management system.

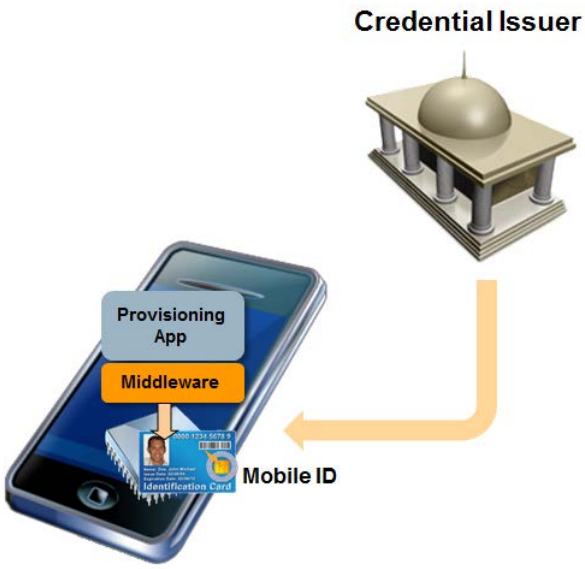


**Figure 1: Generated Mobile ID Credentials**

The end result is the same: The mobile device can be used as a form of identification for a number of different use cases. The creation of Mobile ID credentials typically implies a user validation by the credential issuer before the Mobile ID credentials are generated and issued. This ensures that the Mobile ID credentials are assigned to the right user and cannot be misused by unauthorized entities. The sophistication of the proof and vetting process usually depends on the required quality level of the Mobile ID credentials. For example, weak Mobile ID credentials which can be used for less risky operations might be assigned to a user once the user confirms an email or SMS. Strong Mobile ID credentials for sensitive transactions typically require in-person user validations.

For additional details on the technical provisioning of Mobile IDs, refer to Appendix B.

### 3.2. Derived Credentials

A new Mobile ID use case which has not been broadly available in the past is the creation of Derived Mobile ID credentials. A Derived Mobile ID credential can be used the same way as the Generated ID credential, but may have some limitations on how, when, or where it can be used.

Traditional identifications have typically used a unique identifier: a driver's license number, passport number, badge ID, etc. New digital identity techniques, rather than relying on a single unique identifier, establish a chain of trust using a Public Key Infrastructure (PKI). This means that a user can have IDs that are essentially certificates signed by the originating institution, rather than an opaque string of digits. The use of certificates instead of unique identifiers enables users to create new IDs and sign them through an authentication method so that the chain of trust extends to the new IDs. For example, this means that the healthcare system has the ability to create a new health card with a different identifier / certificate but that is functionally linked back to the same user's account.

Issuing derivatives of the same ID is extremely useful:

- Issuing Mobile ID credentials is simplified since the issuer can rely on the ID card credentials for the user validation which already exist on the ID card. More detailed proof and vetting processes, which typically require in-person validation, can be replaced by automated processes which validate the user by performing an ID card authentication online.
- Management of Mobile ID credentials is simplified because it is unnecessary to define a dedicated credential life cycle. Instead the life cycle of the main credentials, which is already managed by the ID card issuer, may be used.
- The damage caused by security breaches may be limited since a Derived ID credential may have limited permissions and expiration dates. For example, a Derivative Social Security ID may expire after a week or a month, limiting a user's exposure to fraud or identity theft.
- Several IDs may be derived and used individually for different purposes on different mobile devices. A single Derivative ID may be revoked at any time without impacting others.
- A Derivative ID can be used to replace a physical ID card, at least temporarily. For example if an ID card is lost, stolen, or forgotten at home, the Derived ID can

be used instead of the physical ID card in identification, authentication, and authorization processes.

- Derivative IDs allow users to temporarily and securely share their Mobile ID for verification purposes without giving up possession of their mobile device. It does this by enabling several Mobile IDs to be derived on different mobile devices. It even allows users to derive a Mobile ID from a different Mobile ID stored on another mobile device.

One already deployed derived credential scheme is the specification for PIV derived credentials [SP 800 157], which allows these credentials to be stored on mobile devices, with the exception of the main PIV credentials on the PIV card. Potentially this concept of Derived IDs could be applied to any kind of ID card such as bank cards, national IDs, driver's licenses, health cards, or company badges. Thus, identity management institutions across different market segments can take advantage of the Derived ID concept.

The concept of Derived Credentials can be split into two categories, remote provisioning and local provisioning:

- Remote provisioning: The user performs an ID card authentication towards a Derived Credential Issuer system in the backend. Once the authentication is successfully performed, the user downloads the Derived Credential from the Derived Credential Issuer system to the mobile device (e.g. TEE, SE). [SP 800 157], for example, relies on a remote provisioning scheme for Derived ID Credentials for PIV cards. The GlobalPlatform messaging specifications [GP Msg], End-to-End Framework [GP E2E], and the TEE Management Framework [GP TEE Mgmt] allow the implementation of this scheme based on a TEE or SE by providing an end-to-end security solution in a system.
- Local provisioning: The user taps the ID card on the mobile device. A provisioning app on the mobile device accesses the ID card via NFC and triggers a derivation of credentials from the ID card. The Derived Credentials are securely transferred from the ID card to the mobile device (e.g. TEE, SE) by using secure channel protocols. The Privacy-based Chip Authentication (PCA) protocol defined in EN 419 212:2014 [EN 419 212], for example, relies on a local provisioning scheme for Derived ID Credentials for signature cards. The GlobalPlatform Privacy Framework [GP Privacy] could be potentially used to offer protocols for Derived Credentials local provisioning schemes such as the PCA protocol as an SE service.

The above schemes are examples and might have certain variations. The choice of Derived Credential scheme depends on the credential issuer.

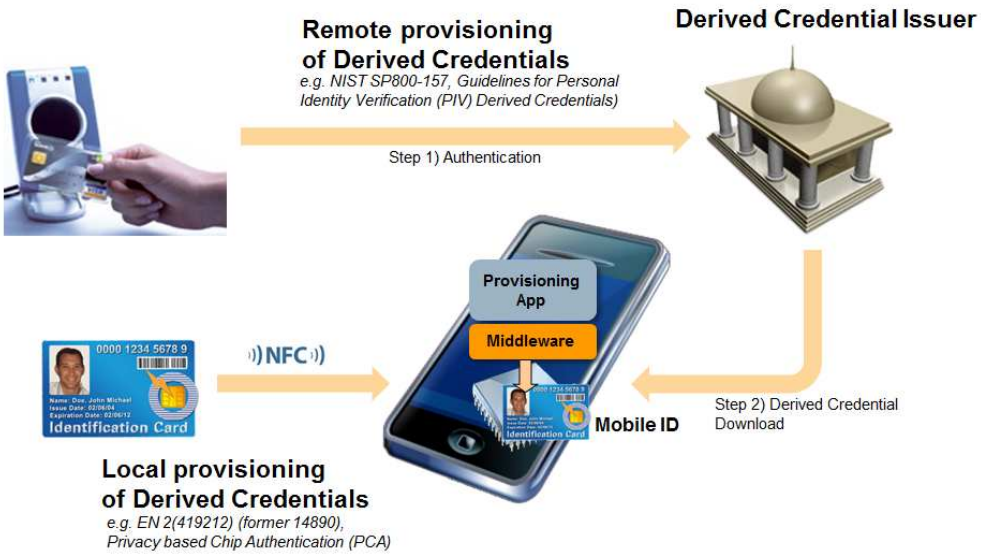


**Figure 2: Remote and Local Provisioning of Derived Credentials**

In both schemes GlobalPlatform specifications provides the building blocks for the derivation method of credentials. The benefits of using the SE and TEE is that they are standardized and platform agnostic. A service provider, once familiar with the GlobalPlatform APIs and security architecture, can design a solution once and deploy it across multiple channels and device types in any given market. The behavior of the Mobile ID will be the same regardless of the device or number of devices the credentials are derived on.

A decision between generated and derived credentials must first be made by the service provider in order to deploy the Mobile ID solution. After deployment, the application stage begins by determining the appropriate levels and types of authentication for the Mobile ID implementation.

## SECTION 4: Mobile ID Application Use Cases

Once the requirements of credentials have been examined, a Mobile ID implementation can be deployed and be used to enable any number of use cases. These include authentication for remote login; securing existing services through second factor authentication; and enabling innovation through secure downloadable applications.

This section explores the importance of authentication capabilities to enable Mobile ID applications.

### 4.1. Authentication

Mobile ID applications are mainly used for authentication purposes. The ID on the mobile device can be used to perform verification locally or remotely with a mobile device for different applications in the field. Authentication use cases can be split into three different categories:

1) Authentication to another local application

   In order to get access to a local application service (e.g. a service API for payment transactions or media streams) provided by another mobile application or by the mobile operating system itself, the mobile application which is intended to use this service typically requires authorization (application single-sign-on). This authorization is usually granted by a successful authentication towards the application or system component which is offering this service. Another example would be a Bring Your Own Device (BYOD) container service allowing applications to use their own device for secure services, while a separate mobile application can authenticate the user for using this BYOD container [TEE WP].

2) Authentication to another mobile device or terminal

   The Mobile ID on the device can be used to authenticate to another separate device, e.g. for getting access to buildings. In this case the terminal interacts with the Mobile ID using proximity technologies such as Bluetooth or NFC. In the NFC example the mobile device has to be tapped to a terminal (proximity: mobile device acts like a contactless ID card, based on card emulation). Another possible example would be a local identification by using another mobile device, e.g. a police officer checks the driver's license (for example, Iowa Department of Transport plans to pilot a Mobile ID as driver's license[21]) by interacting with the mobile device of the citizen. Since mobile devices can be easily connected to another client device (e.g. a desktop computer) the Mobile ID on the mobile device can even be used by another client device e.g. for remote authentication by using a Bluetooth, USB, WIFI or NFC connection.

3) Authentication to a remote server or cloud service

   The Mobile ID could be used to authenticate the user towards a remote server or cloud service. One example is using the Mobile ID like a usual PKI smart card which leverages a wide range of typical PKI applications on the mobile, including VPN and TLS. Another example is an online verification based on a FIDO key pair or a one-time-password. In the latter case, the one-time-generator reflects

[21] 'Iowa's going to have smartphone driver's licenses', http://www.washingtonpost.com/blogs/govbeat/wp/2014/12/09/iowas-going-to-have-smartphone-drivers-licenses/.

the Mobile ID application. FIDO and GSMA Mobile Connect are examples of specific authentication schemes which can be implemented based on an SE in a mobile device. A Mobile ID can also be used to authenticate the user to an identity provider. After successful authentication by an identity provider, federation protocols like OpenID Connect or SAML allow the login to remote servers or cloud services. Since Mobile ID credentials typically include a set of cryptographic keys they can be applied to a variety of use cases which include all kinds of signature and encryption use cases, like data encryption, including mail and storage cloud data.

The choice of the platform (REE, TEE, SE) for the Mobile ID usually depends on the use case and requirements, especially security requirements (as covered in Sections 5 and 6 below). Depending on the chosen platform, the mobile device has to support the corresponding APIs, such as GlobalPlatform Client API [GPD TEE Client], GlobalPlatform TEE SE API [GPD TEE SE API], or SIMalliance Open Mobile API [Open Mobile API], which allow applications to use the Mobile ID. Middleware as a service API may help to integrate the Mobile ID capabilities into the different client applications on the mobile device or desktop computer.

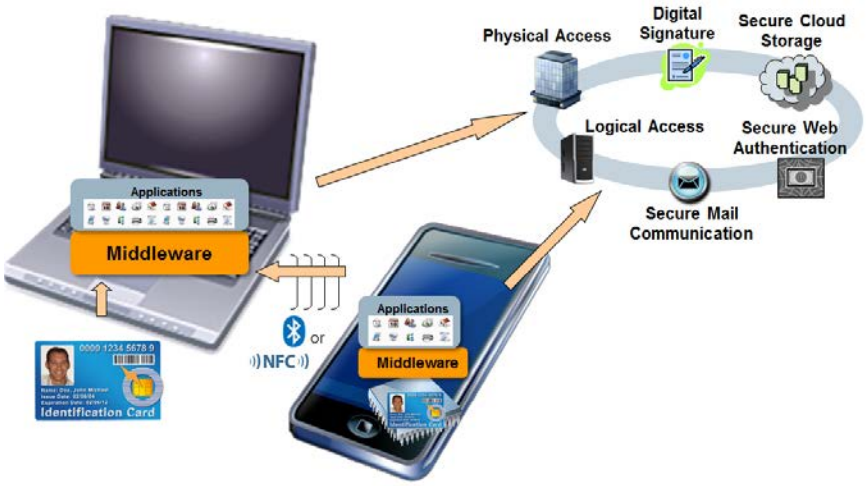


**Figure 3: Authentication Mobile ID Use Cases**

### 4.2. Multi Factor Authentication

Often to obtain a higher level of assurance during the authentication process, multi factor authentication is used. This means that the primary authentication factor (e.g. the username and password; something that the user knows) is complemented by additional factors such as something that the user has (proof of possession of a key) or something that the user is (e.g. via biometrics).

Mobile devices are an ideal carrier for something that the user has (e.g. a user proves during the authentication process to be in possession of the phone that carries, for example, a cryptographic key that has been provisioned during enrollment). Additionally with the increasing proliferation of built in biometric sensors, cryptographic keys can be further protected by being released for use (e.g. to sign the cryptographic proof) only after local authentication has taken place using the biometric sensor.

If the original transaction that needs to be protected is performed on an additional terminal, the backend system can obtain an out-of-band proof of the Mobile ID. In this case, the user would attempt, for example, to perform a sensitive transaction such as transferring money or sending a tax return. Before proceeding with the transaction, the backend system would then contact the Mobile ID on the user's mobile phone that was registered. The backend system can then interact with the Mobile ID via the cellular network and obtain the required proof that the user was present and in possession of its Mobile ID. These out-of-band Mobile ID mechanisms are extremely difficult to attack. GSMA Mobile Connect is an example of such a scheme, which is using out-of-band OTA messages in conjunction with the Mobile ID application as defined in CSPA8 (SIM authentication applet) on the UICC.

New and alternative out-of-band scenarios are becoming a reality due to the increasing embedding of proximity network technologies such as Bluetooth Low Energy (Bluetooth Smart). In this case the transaction terminal (e.g. laptop, tablet) can interact locally via the Bluetooth Smart network with the Mobile ID on the smartphone.

The FIDO Alliance has standardized this scenario in the FIDO U2F 1.1 specifications [FIDO U2F].

In multi factor scenarios, the keys to prove the second or multiple factors can be held within the GlobalPlatform secure components that allow keys to be stored in secure boundaries. For example, they could be stored within an applet in the SE, such as the UICC, the embedded SE or even a smart microSD. In other solutions they could be stored within the boundaries of the TEE. Additionally the TEE secure PIN entry can be used to authorize the use of the second factor key.

Finally both the TEE and the SE can harbor the keys that would protect communication with the backend or the local transaction terminal (allowing mutual authentication of the Bluetooth channel for example).

### 4.3. Mobile ID and Mobile Applications

The success and widespread adoption of today's mobile devices, such as smartphones and tablets, can be partially credited to the widespread availability and innovation of downloadable applications. Mobile ID provides a new era of security to applications that will enable users to trust their applications with increased responsibility, and enable new functionality. Today's applications require one-off solutions for authentication and assurances of security, but Mobile ID will enable broad deployment, ease of access, familiarity, and rapid innovation for new applications. This will usher in a new wave of document signing, financial services, secure communications, ticketing services, and beyond.

Without these authentication methods Mobile ID applications would not provide value to market segments. By developing specifications to enable secure, standardized, and isolated execution environments for authentication, GlobalPlatform specifications enable the Mobile ID application requirements.

Section 5 looks closer at how the SE and TEE play an important role in Mobile ID architecture and can be combined with other technologies like the Rich OS or Contactless Frontend (CLF) to design a complete Mobile ID solution.

## SECTION 5: Mobile ID Architecture

The deployment and application steps help service providers determine the necessary requirements for their Mobile ID application. After these steps have been completed service providers can start designing the architecture needed to run their Mobile ID with credentials, and authentications in mind, and prepare to review the security considerations and implementation scenarios.

This section explains the Mobile ID components in the mobile device architecture. A TEE enabled mobile device consists of two execution environments, a TEE and a Rich Execution Environment (REE). In both environments, applications can be installed and executed. Applications installed in the TEE (Trusted Applications) run in an isolated environment and can use trusted services provided by the TEE OS, such as the Trusted User Interface. The operating system of both environments offer SE APIs which allow an APDU communication towards the different kind of SEs (SIM/UICC, smart microSD, embedded SE), which are available in the mobile device.

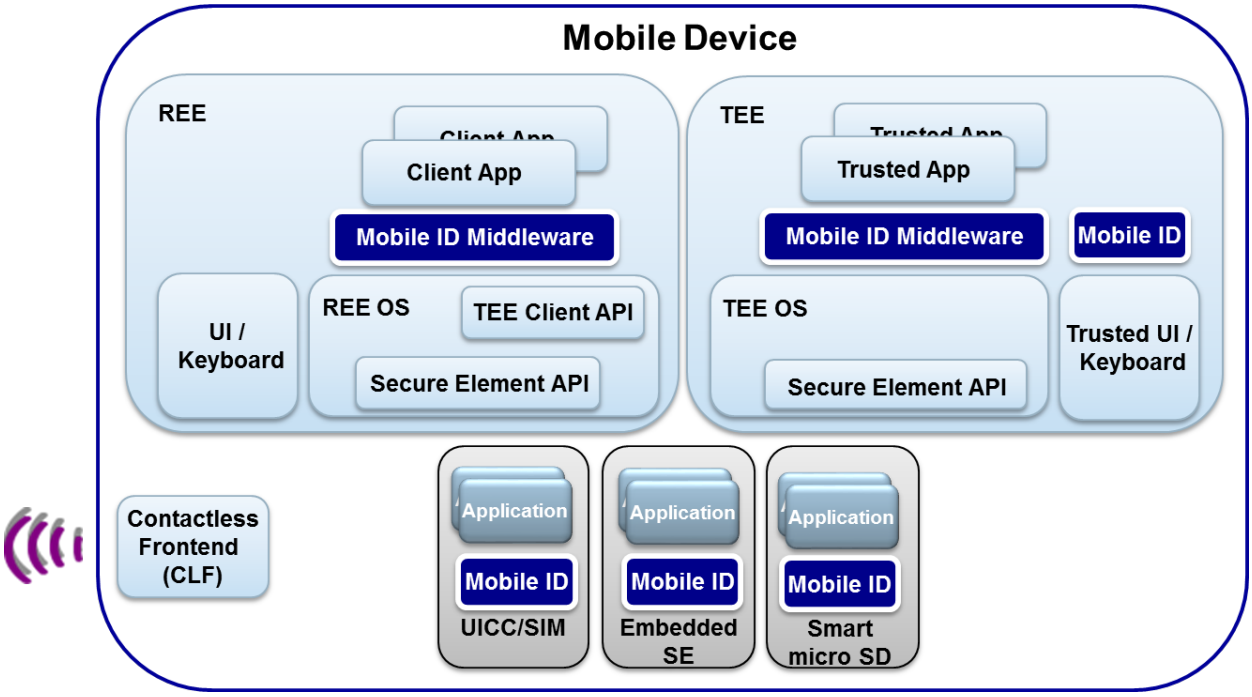


**Figure 4: Mobile ID Architecture**

### Mobile ID Middleware

Middleware abstracts the interface of a Mobile ID application installed in an SE. An application in the TEE or REE may use this middleware to perform operations (e.g. signatures, encryption) based on the Mobile ID credentials hosted by the Mobile ID application. The middleware translates high level API functions to APDUs and performs the transfer of the APDU commands. It interprets the content of response APDUs and provides appropriate feedback to calling applications. Middleware can also be used to abstract the interface of Mobile ID application residing in the TEE.

### 5.1. Mobile ID

The Mobile ID consists of a set of credentials (typically cryptographic key) hosted by a Mobile ID application which is installed on an SE or in the TEE.

### 5.2. Secure Element API

The SE API is a service provided by the operating system, either REE or TEE. It can be used by mobile applications in the REE or TEE to access different kind of SEs (SIM/UICC, Secure Micro SD, embedded SE).

### 5.3. Contactless Frontend (CLF)

The contactless frontend provides the NFC interface to external interface (e.g. terminals, other mobile devices) and can be used by external devices to access the Mobile ID credentials on the SE for local validations like physical access control.

### 5.4. User Interface (UI) / Keyboard

From displaying content on the mobile device display to fetching the user input (e.g. from the keyboard or touch screen), the REE provides a framework which can be used by mobile applications to interact with users.

### 5.5. Trusted UI / Keyboard

The TEE may provide a trusted user interface which can be used to perform secure PIN/password entries or to display secure data on the screen. Trusted Applications may access the trusted user interface functionalities by using the TUI APIs of the TEE.

### 5.6. Client Applications

Client Applications (CAs) are mobile applications installed in the REE. CAs can make use of the Mobile ID credentials residing in the SE or TEE by using a Mobile ID middleware. CAs are typically triggered by user actions, by network servers or by NFC trigger events. A client app may request PIN/passwords from the user for Mobile ID operations (e.g. to unlock keys for authentication, signature operations or encryption) by using the user interface framework of the REE.

### 5.7. Trusted Applications

Trusted Applications are applications installed in the TEE. Trusted Applications can make use of the Mobile ID credentials residing in the SE by using a Mobile ID middleware. TAs are typically triggered by user actions, by network servers, or by NFC trigger events. A TA may request PIN/passwords from the user for Mobile ID operations (e.g. to unlock keys for authentication, signature operations, or encryption) by using the trusted user interface API of the TEE.

A Mobile ID application contains very sensitive and private personal user data. With a Trusted Application and the TEE architecture, service providers do not need to consider the Client Applications that may be residing on the device or that could be installed in the future. Consumers use their mobile devices for everything, one device may host multiple services or applications from various service providers. GlobalPlatform's infrastructure robustly safeguards the security and integrity of services deployed on a platform

alongside services from other providers. If using GlobalPlatform technology, service providers of Mobile ID applications can have the peace of mind that they, and only they, can control their services. In addition, their service poses no threat to, nor is at risk to, any service sharing the platform.

For an overview of Mobile ID Characteristics see Appendix C.

## SECTION 6: Security

Regardless of market sector or use case, and regardless of the technical implementation chosen for a Mobile ID, security is an overarching concern for all Mobile ID deployments. Various Mobile ID implementations require different security levels, based on market needs which range from low security for non-sensitive operations (e.g. customer loyalty programs) to high security for very sensitive operations (e.g. large financial transactions). The security levels of Mobile ID implementations can be determined by a security assurance method and completed by a security evaluation and certification program (such as Common Criteria). Varying levels of security are provided by different platforms with varying security mechanisms. The lowest level of security for non-sensitive operations is typically provided by a REE, while higher levels of security are typically provided by a TEE or SE.

### 6.1. Security Levels

The security level of a Mobile ID implementation in a mobile device depends on three functionalities: storage, user I/O, and processing. All of these functionalities contain potential vulnerabilities and it is the responsibility of the platform to provide protection for these functionalities. The following section discusses the different security levels, which can be achieved by using an REE, TEE, or SE as platform for a certain functionality in a mobile device.

1) Credential Storage (Possible platforms: REE, TEE, SE)

   Mobile ID credentials include highly sensitive assets such as cryptographic keys which need to be protected in order to assure a certain trust level. Credential storage can be implemented at a basic level in the REE; however, there is a potential risk that the credentials might be replaced or compromised once the REE is rooted. Using the TEE for credential storage eliminates the risks of potential software attacks which occur in the REE (e.g. OS rooting, jailbreaking, malware). In order to assure protection against hardware attacks, the SE can serve as a tamper-proof credential storage environment; however the storage capacity of SEs is limited.

2) Data Entry and Display (Possible platforms: TEE, REE)

   The usage of Mobile ID credentials for signatures, encryption, or authentication requires a user verification, which is typically based on PIN/password entry or by biometric operations (e.g. fingerprint verification). After successful verification of the Mobile ID key, credentials are unlocked and can be used to perform a cryptographic operation (e.g. a digital signature for authentication). The PIN/password entry requires the implementation of a mobile application with user interface. Another Mobile ID use case where a user interface is required is the display of Data to Be Signed (DTBS), which will be signed for transactions. The entry of PIN/password, as well as the display of DTBS, is a highly sensitive operation and the security of the user interface relies on the operating system of the underlying platform. The REE can be used to implement the user interfaces, however, there is a risk that the PIN/password can potentially be intercepted or the display content can be counterfeited by malware, especially once the Rich OS is rooted or malware pretends to be the genuine application. Using a TEE allows the execution of these highly sensitive user interface operations in a secure environment which is resistant against software attacks even if the REE is

compromised. Moreover the Trusted User Interface (TUI) can guarantee users that they interact only with genuine applications for sensitive transactions.

3) Processing of Services (Possible platforms: TEE, REE, SE)

   Mobile ID use cases such as authentication, signature creation, or encryption operations can be processed either in the REE, TEE, or SE. The REE is characterized by high processing speed capability. In contrast the SE provides slower performance and data speeds (making it well adapted to short message processing), yet is physically isolated therefore offers exceptionally strong security for operations. For interactions with backend systems, such as authentication servers, the SE has to rely on external clients (e.g. in the REE) and cannot operate on its own. The TEE, by contrast, offers an ideal solution for high-security applications that have high processing speed and it provides a certain level of security. It balances security (trust and isolation) with performance, and it is able to perform all transactions on its own. The TEE does not provide the strong physical isolation of SEs; however, a TEE can be coupled with an SE when the use case and security requirements demand it.

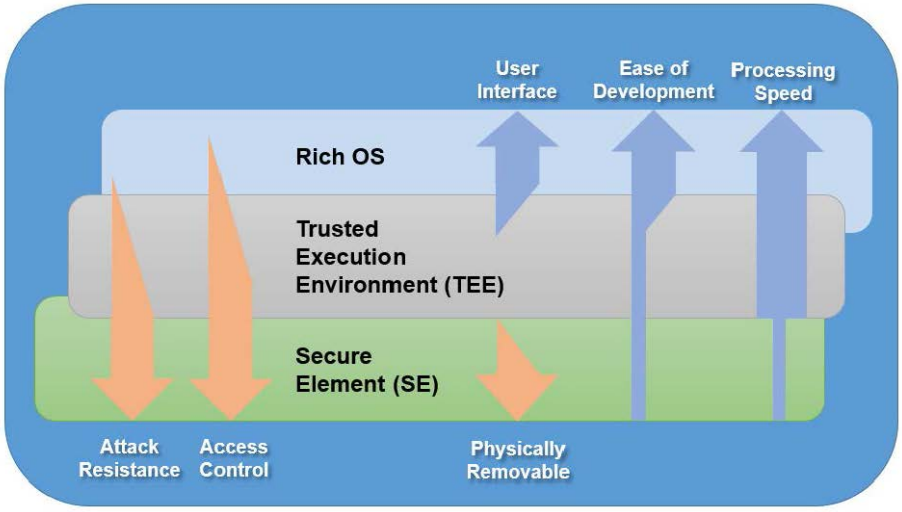


**Figure 5: Processing of Services in the REE, TEE, and SE**

## 6.2. Assurance Level

In order to determine the security level requirements as described above, the required assurance level for the specific application or service needs to be examined. ISO/IEC standard [29115] provides a framework for managing entity authentication assurance in a given context. [29115] establishes four Levels of Assurance (LoA), and the criteria and guidelines for achieving each level. The framework involves all the possible actors: Users, Credential Service Provider (CSP), Registration Authority (RA), Relaying Party (RP), Verifiers, and Trusted Third Party (TTP)). The different phases present in the process are enrollment, credentials management, and entity authentication.

Level 1 is the lowest level of assurance; Level 4 is the highest level of assurance. The following table gives a view on the description of levels of assurance, how to control identity, which method is used between local or remote (remote identity proofing over a

network means not being able to physically see the entity, whereas local identity proofing requires physically seeing the entity), and an example use case for each level.

**Table 1: Description of Assurance Levels and Corresponding Requirements**

| Level | Description | Controls for identity proofing | Method of processing | Authentication method | Use case |
|---|---|---|---|---|---|
| 1 – Low | Little or no confidence in the claimed or asserted identity | Self-claimed or self-asserted | Local or remote | Self-registered username/password, MAC address<br>(no need for cryptographic methods) | Register for on-line access to public documents (e.g. downloading GlobalPlatform whitepaper) |
| 2 – Medium | Some confidence in the claimed or asserted identity | Proof of identity through use of identity information from an authoritative source | Local or remote | Single-factor authentication | Online modification of personal information (identity, banking information…)<br>e-reputation |
| 3 – High | High confidence in the claimed or asserted identity | Same as for LoA2 + identity information verification | Local or remote | Multi-factor authentication<br>(no requirement on generation and storage of credentials) | Online access to account for financial transactions |
| 4 – Very High | Very high confidence in the claimed or asserted identity | Proof of identity through use of identity information from multiple authoritative sources + identity information verification + entity witnessed in-person | Local only | Multi-factor authentication with in-person identity proofing<br>(tamper-resistant storage of keys, PKI) | Corporate access, VPN… |

Depending on the technology, authentication methods, storage of credentials, and applications, the assurance level may be very different.

The following figure (extracted from Eurosmart's position paper on server signing[22]) shows the mapping between assurance level, on the model proposed by ISO, and mobile device authentication method.

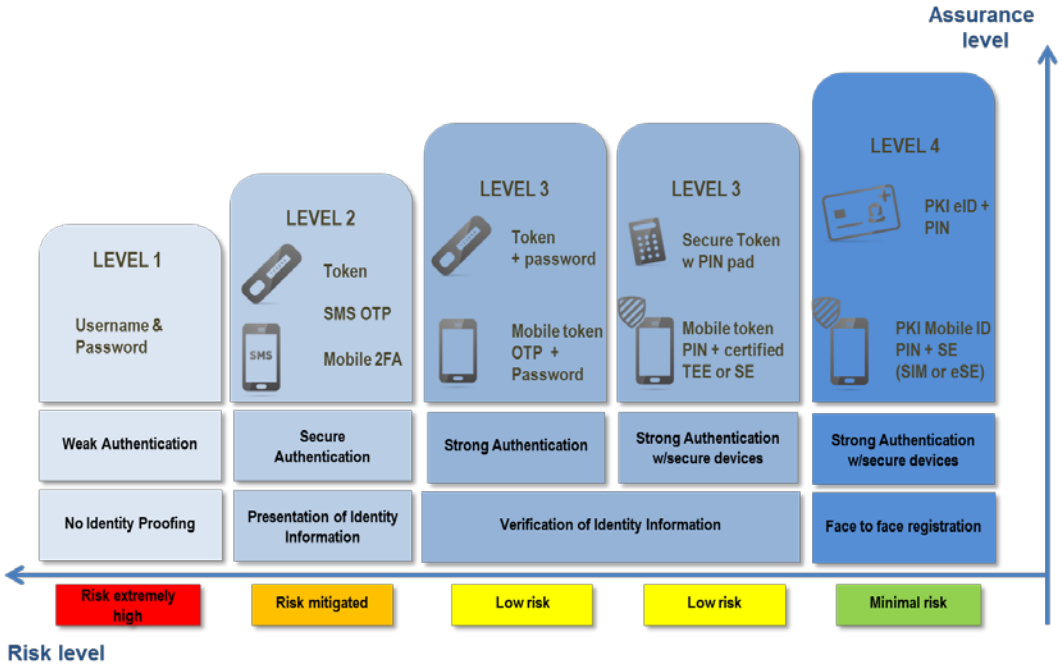


**Figure 6: Mapping between (ISO) Assurance Levels and Authentication Methods**

Figure 6 shows the importance of the TEE and SE in guaranteeing a good level of assurance (starting from Level 3). Note that the TEE and SE are essential for implementing levels 3 and 4.

### 6.3. Certification Requirements for Secure Elements and Devices

Typically, platforms for ID applications have to fulfill security requirements that are assured by certification schemes. The mobile device is gaining more and more security thanks to the SE and TEE, which are certified against Common Criteria or FIPS.

Secure Elements have been required to complete security certification, to address sensitive use cases such as government, telecommunication, or banking. The certification is based either on Common Criteria methodology [CC] or FIPS methodology [FIPS].

In addition, GlobalPlatform has issued a TEE protection profile with EAL2+ security assurance level [GPD TEE PP], based on CC methodology and listed by Common Criteria in the category Trusted Computing [CC TC].

---

[22] 'Eurosmart position paper – Server Signing within the eIDAS Regulation', http://www.eurosmart.com/images/doc/Publications/Eurosmart%20Position%20Paper%20-%20Server%20Signing%20within%20the%20eIDAS%20Regulation.pdf.

## SECTION 7: Implementation Scenarios for Mobile ID Solutions

Mobile ID solutions can be implemented on different platforms. The choice of platform depends on different factors: required security level; development, integration and maintenance costs; and the availability of the technologies in the mobile devices on which the Mobile ID solutions will be deployed. This chapter outlines the different implementation scenarios for mobile solutions based on the platforms REE, SE, TEE and the corresponding GlobalPlatform technologies, which, in addition to the previous analysis of requirements, can help Mobile ID services decide which solution scenario best fits the requirement of their market sector.

### 7.1. Solution Scenario: REE

Mobile ID credentials are stored in the memory of the REE. A mobile application that is using the Mobile ID credentials might store them directly within the application package or might use Mobile ID credentials stored by the Rich OS or by another mobile application. If the Mobile ID credentials are not stored within the application package itself, the mobile application needs an exposed cryptographic API which allows usage of the externally stored Mobile ID credentials. The cryptographic operation itself is performed within the REE and the cryptographic algorithms are typically implemented by the Rich OS. The user interfaces for the user verification are implemented by the mobile application.


**Figure 7: REE Mobile ID Scenario**

**Table 2: REE Mobile ID Benefits**

| | |
|---|---|
| **Viability** | This solution can be deployed on any mobile device. NFC-based Mobile ID use cases, such as physical access control, can only be implemented on devices supporting HCE [HCE]. |
| **Security** | Mobile ID credentials are stored and used in the REE. Storage and operation might be secured using methods such as white box cryptography; however the security relies on the security provided by the operating environment.<br><br>The user verification, such as PIN entries, is implemented in the REE which relies on the security mechanisms provided by the underlying rich execution operating system.<br><br>For NFC based use cases, SCP '11' [GP SCP11] can be used to secure the routing between the NFC interface and the Mobile ID application. |
| **Deployment Considerations** | This solution does not require service contracts for deploying applications on a TEE or an SE. |
| **Usability** | The Mobile ID can only be used if the phone is powered and in some cases it might require further user interactions (such as unlock the screen) especially after the reboot. |
| **Security Considerations** | If the mobile device is purely based on the REE it is generally vulnerable to replication attacks. If the device is rooted, the risk is very high that the Mobile ID application will be compromised. The security level of this solution scenario relies entirely on the security of the OS and the security level of the different operating systems maybe very different. |

### 7.2. Solution Scenario: REE + SE

Mobile ID credentials are stored in an SE and cryptographic operations are also performed within this SE. The mobile application can trigger cryptographic operations with these Mobile ID credentials within the SE using the command interface of the Mobile ID application of the SE. The commands can be sent using the SIMalliance Open Mobile API [Open Mobile API]. Complementary Middleware of the Mobile ID application can simplify the usage of the Mobile ID application by providing a high level cryptographic API for performing the operations on the SE. The user interfaces for verification are implemented by the mobile application in the REE.

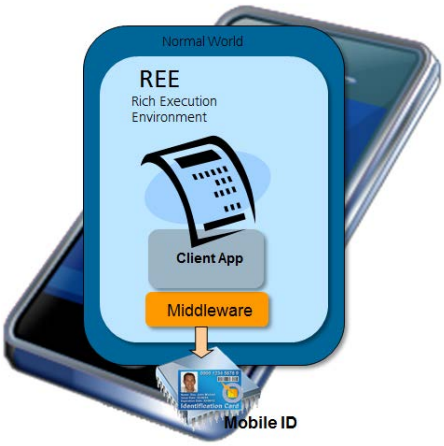


**Figure 8: REE + SE Mobile ID Scenario**

**Table 3: REE + SE Mobile ID Benefits**

| | |
|---|---|
| **Viability** | In cases where mobile applications need access to the Mobile ID credentials in the SE, this solution can only be deployed on mobile devices which support an SE which can be accessed by APIs on APDU level.<br><br>In specific Mobile ID use cases, like physical access control, where an external terminal validates the Mobile ID, the SEs need to be accessible via NFC.<br><br>NFC based Mobile ID use cases, like physical access control, can only be implemented on devices supporting HCE [HCE]. |
| **Security** | Mobile ID credentials are stored and used in a tamper resistant environment that prevents a large number of attacks, including physical attacks. The credentials on the SE can be securely managed via End-to-End secured channels. The SE allows the implementation of Mobile ID applications with non-repudiation. This solution allows the different Mobile ID applications on the SE by using the GlobalPlatform Security Domain technology.<br><br>The user verification, such as PIN entries, is implemented in the REE, which relies on the security level provided by the rich execution operating system.<br><br>For NFC based use cases, SCP '11' [GP SCP11] can be used to secure the routing between the NFC interface and the Mobile ID application. |
| **Usability** | The SE could allow access to the Mobile ID even if the mobile device is powered-off or locked, i.e. via the NFC interface when a terminal is validating the Mobile ID. In case of a removable SE, e.g. UICC or µSD, the Mobile ID can be easily transferred to another mobile device. |

| | |
|---|---|
| **Deployment Considerations** | This solution requires the deployment of applications in the SE, which necessitates an installation contract with the SE issuer or a deployment on an own SE. |
| **Security Considerations** | This solution provides tamper resistant protection for Mobile ID credentials and can perfectly protect an identity against external environments and other actors issuing credentials and applications on the same SE, thanks to GlobalPlatform's Security Domain model. However, the user verification happens in an external environment which is not under control of the SE. Most of the SEs are certifiable environments under stringent security schemes which are sometimes required for applications on ID cards. |

### 7.3. Solution Scenario: REE + TEE

The Mobile ID credentials are stored in a TEE and cryptographic operations are performed within this TEE. The mobile application can trigger cryptographic operations with these Mobile ID credentials within the TEE by using the commands of the Mobile ID application residing in the TEE. The commands can be sent by using the TEE Client API [GPD TEE Client]. Complementary Middleware to the Mobile ID application can simplify the usage of the Mobile ID application by providing a high level cryptographic API for performing the operations on the TEE.

The Mobile ID in the TEE could be offered as a global service towards all client applications in the REE. This would allow developers to use TEE security services for their mobile application without the need to write a TEE Trusted Application for each mobile application. This global service could be implemented by a single Trusted Application as a shared service (a so called pure TEE model) or it could also be part of the TEE OS (a so called backed-TEE model).

If the TEE does not support a Trusted User Interface, the mobile application handles the user interactions and asks the user for the password or PIN code which will be finally transferred to the TEE and verified by the Mobile ID Trusted Application residing in the TEE.

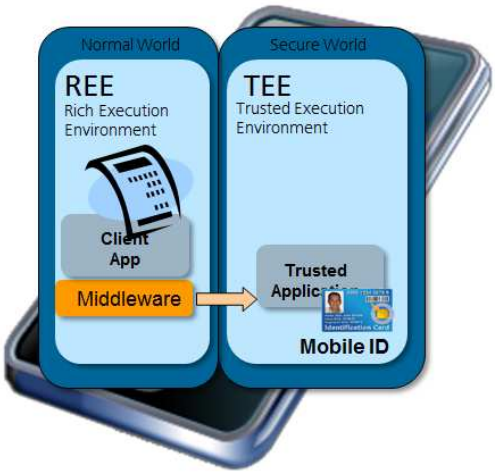


**Figure 9: REE + TEE Mobile ID Scenario, Step 1**

If the TEE supports a Trusted User Interface as a feature, the user interfaces for the user verification can be implemented by the Mobile ID application in the TEE in a secure way by using the TEE Trusted User Interface API [GPD Trusted UI]. Through its Trusted User Interface feature, the TEE makes it possible to securely collect a user's password or PIN code that can be verified by the Mobile ID Trusted Application. This trusted user authentication can be used to verify the Mobile ID owner.


**Figure 10: REE + TEE Mobile ID Scenario, Step 2**

**Table 4: REE + TEE Mobile ID Benefits**

| | |
|---|---|
| **Viability** | A solution based on a TUI can only be deployed on mobile devices which support a TEE with TUI. |
| **Security** | The storage and usage of Mobile ID credentials are performed in the TEE, preventing a large number of software attacks. If the TEE supports a TUI, the user verification can be protected from software attacks as well. |
| **Usability** | The Mobile ID can only be used if the phone is powered and in some cases it might require further user interactions (such as unlocking the screen), especially after the reboot. |
| **Deployment Considerations** | This solution requires the deployment of applications in the TEE which requires an installation contract with the TEE owner or TEE trusted service manager. |
| **Security Considerations** | Since the TEE is a certifiable environment, this solution allows the implementation of Mobile ID applications where all critical components, from user interface, processing environment and storage, can be certified. |

### 7.4. Solution Scenario: REE + TEE + SE

The Mobile ID credentials are stored in an SE and cryptographic operations are performed within this SE. The Trusted Application in the TEE is triggered by a client application in the REE and performs the user verification by using the TEE Trusted User Interface API [GPD Trusted UI]. Once the user is successfully verified, the Trusted Application triggers the cryptographic operations in the SE using the commands of the Mobile ID application. The commands can be sent by using the TEE SE API [GPD TEE SE API]. Complementary middleware to the Mobile ID application in the SE can simplify the usage of the Mobile ID application for the Trusted Application by providing a high level cryptographic API for performing the operations on the SE. The user interfaces for the user verification are implemented by the Mobile ID Trusted Application in the TEE, by using the TEE Trusted User Interface API [GPD Trusted UI]. Through its Trusted User Interface feature, the TEE makes it possible to securely collect a user's password or PIN code that can be verified by the Mobile ID application in the SE. This trusted user authentication can be used to verify the Mobile ID owner.

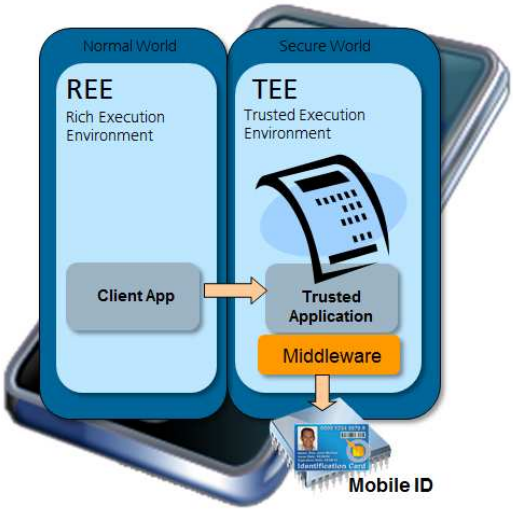


**Figure 11: REE + TEE + SE Mobile ID Scenario**

**Table 5: REE + TEE + SE Mobile ID Benefits**

| | |
|---|---|
| **Viability** | This solution can only be deployed on mobile devices which support a TEE with TUI and an SE which can be accessed by APIs on APDU level. |
| **Security** | Mobile ID credentials are stored and used in a tamper resistant environment which prevents a large number of attacks, even physical attacks.<br>The user verification is performed in the TEE, preventing a large number of software attacks.<br>The communication between the TEE and SE can be secured using the SCP '11' [GP SCP11], which assures a secure channel even if the communication environment between TEE and SE is untrusted. |
| **Usability** | The SE could allow access to the Mobile ID even if the mobile device is powered-off or locked, i.e. via the NFC interface when a terminal validates the Mobile ID. In case of a removable SE, e.g. UICC or smart microSD, the Mobile ID can be easily transferred to another mobile device. |
| **Deployment Considerations** | This solution requires the deployment of applications in the TEE and SE, which implies service contracts for the installation in two environments. Moreover the deployed applications in the TEE and SE need to be managed and synchronized. Overall this solution implies the highest installation and maintenance costs of all solution scenarios. |

| | |
|---|---|
| **Security Considerations** | This solution provides the highest level of security and is especially useful for Mobile ID applications in critical environments or for use cases with highly sensitive operations and security requirements. Since the TEE and SE are certifiable environments, this solution allows the implementation of Mobile ID applications where all critical components, from user interface, processing environment and storage can be certified. The SE, which hosts the Mobile ID credentials and performs the cryptographic operations, even allows certification under stringent security schemes. |

Implementation solutions are not one-size-fits-all; one solution does not meet the needs of all market segments, types of credentials and authentications, or security levels. When designing a Mobile ID solution service providers must consider all variables presented in this paper to design the appropriate architecture for the Mobile ID implementation.

## SECTION 8: Conclusion

Mobile ID is increasingly important for a wide range of applications, including government-to-citizen, government-to-government, and public sector applications in finance, healthcare, and others. Mobile ID has a diverse number of use cases around the deployment and use of various IDs, and each ID implementation has varying levels of potential technical implementations and security requirements. This involves the SEs, TSMs, Card Specifications and GlobalPlatform's TEE.

The choice of whether a Mobile ID solution should exist solely in the REE or should include some combination of SE or TEE is subject to usability, deployment, and security considerations. GlobalPlatform's TEE provides security beyond the capabilities of the REE, through a combination of Trusted User Interface and Trusted Applications. Security can be further enhanced against physical attacks through the use of an SE.

Further, GlobalPlatform's technologies provide many benefits for the development of services due to the freely available and standardized infrastructure. This includes the management of Trusted Applications and APIs, and safeguards for the security, integrity, and privacy of services deployed on a platform alongside services from other providers. Additionally, any device that has been certified as 'compliant' to GlobalPlatform specifications carries the assurance that the service will behave in the correct way, regardless of the device it is deployed on. This portability of service addresses compatibility and scalability issues frequently encountered in multi-device, multi-app, and multi-platform deployment scenarios. GlobalPlatform is an established and standardized technology, with many guidelines to assist with the deployment of services. This allows service providers to learn GlobalPlatform technology and APIs without having to research the specificities of all the possible target products' APIs and associated security architecture. The established infrastructure shortens time-to-market for service providers.

While the number of applications, use cases, and deployments of Mobile ID is large today, the size and scope of these deployments is rapidly increasing. GlobalPlatform provides frameworks, configurations, profiles, protocols, interfaces and standards, which assure interoperability, consistency and enables implementation of end-to-end solutions in a secure and certified way. Ongoing large-scale deployments, innovation, and promises of security require the support of standards-based technologies such as the TEE, which will continue to play an important role in the growth of the Mobile ID market.

All feedback is welcome, comments or questions may be submitted to secretariat@globalplatform.org.

## APPENDIX A: Trusted Execution Environment (TEE)

The Trusted Execution Environment (TEE) is a secure area of the main processor in a smartphone (or any connected device) that ensures sensitive data is stored, processed, and protected in an isolated, trusted environment. The TEE stands in contrast to the Rich Execution Environment (REE), which is the general operating system where consumer applications execute. The purpose of the TEE is to provide a dedicated and trusted execution environment, isolated from the REE, which allows the execution of applications on a mobile device in a secure way. This provides the foundation for a multitude of applications, such as secure payments and authentication, and could potentially serve for the foundation of Mobile ID as well.

The TEE is built on the GlobalPlatform Specifications. To date, GlobalPlatform has published the Internal Core API [GPD Core API], Secure Element API [GPD TEE SE API], Trusted User Interface API [GPD Trusted UI], and Sockets API [GP TEE Sockets] specifications for the TEE which can be used by TEE applications to perform standardized cryptographic and storage operations, secure element communications, secure interactions with the user, and secure communication with servers.
[GPD TEE Client] allows REE applications to communicate with applications in the TEE. Specifications currently under development include the TEE Management Framework, for secure administration of TEE applications, and Fingerprint Biometrics API for secure user identification by TEE applications.

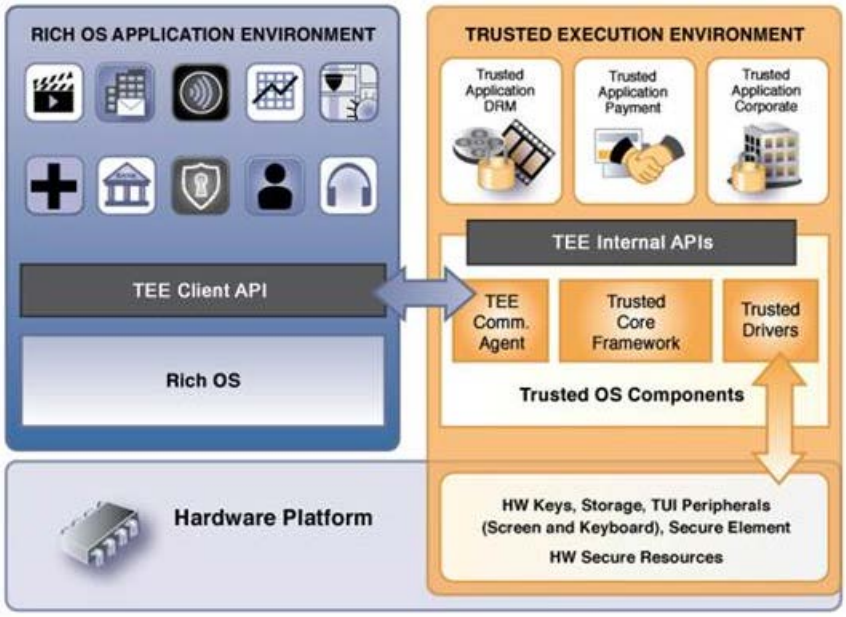


**Figure 12: Architecture of the TEE**

While Mobile ID implementations could certainly recreate each of these capabilities through proprietary implementations, the existing TEE APIs provide faster time to market and are based on the TEE Protection Profile established by GlobalPlatform. GlobalPlatform is creating its own certification process, which complements the Common Criteria option in order to extend the geographic coverage for TEE certification. Starting in late 2015 or early 2016, candidates to certification will thus be able to choose an evaluation facility qualified by GlobalPlatform.

For more details on TEE certification visit the GlobalPlatform Certification website, http://www.globalplatform.org/teecertification.asp

## APPENDIX B: Technical Provisioning of Credentials

Provisioning of Mobile IDs is discussed briefly in section 3. This appendix provides additional technical detail.

The Mobile ID might reside in the SE or TEE. Depending on the technology chosen, different scenarios are possible to issue and manage the Mobile ID credentials on the different mobile devices in the SE or TEE. GlobalPlatform specifications provide frameworks, configurations, profiles, protocols, and interfaces which allow administration and life cycle management for a TEE and an SE to be performed in a secure and interoperable way. These specifications allow a multi-tenant security domain model, on an SE and a TEE. Infrastructure scenarios with TSM, OTA, CMS, and CAs can build on these specifications in order to perform remote provisioning and management of the Mobile ID application and the corresponding Mobile ID credentials, on different mobile devices.

### B.1. Provisioning Credentials on UICC

The service provider manages the identities with its Credential Management System (CMS). It uses an SP-TSM and connects to an MNO TSM in order to manage the ID Trusted Application and the ID credentials.

The credentials are managed via OTA (using SCP ‘80’ or SCP ‘81’ as defined respectively in [GP Card] and in GlobalPlatform Remote Application Management over HTTP [GP Amd B]), which allows an end-to-end secure communication to the UICC based on protected and encrypted binary SMS (ETSI [102 225], [102 226]). The OTA communication is directly performed through the modem of the mobile device and hence the messages cannot be intercepted or inhibited by mobile applications by the user once the device is connected to the mobile network. Mobile ID credentials may also be transferred via TLS secured TCP/IP channels with a remote agent on the mobile device according to GlobalPlatform SE Remote Application Management [GP SE RAM]) if the Mobile ID credentials are too large for an OTA transfer.

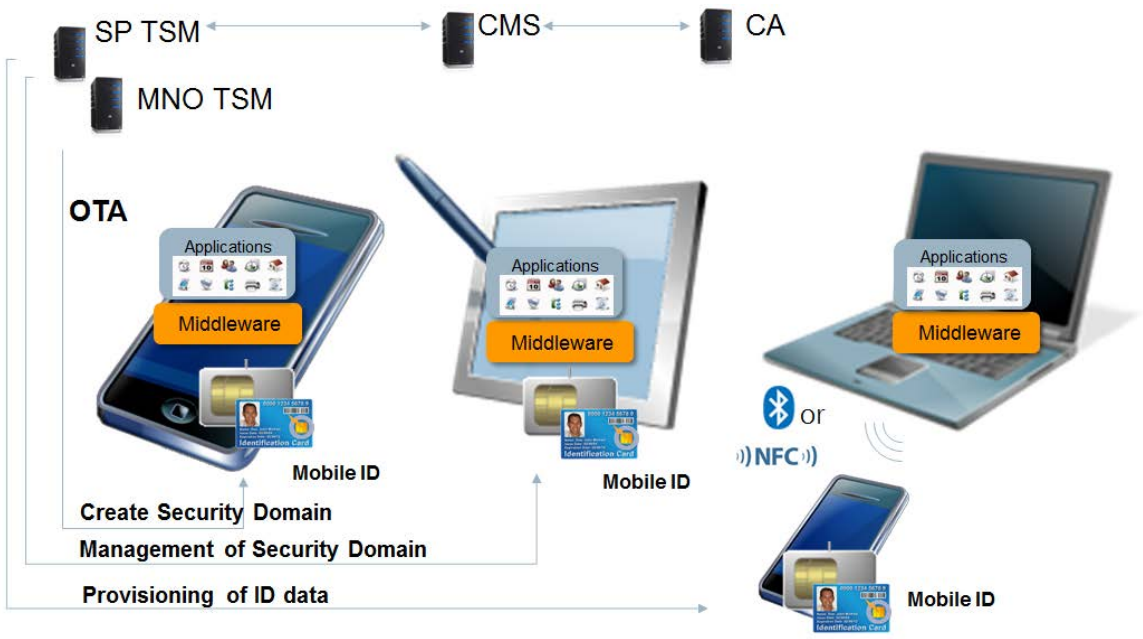


**Figure 13: Credentials on a UICC**

### B.2. Provisioning Credentials on an eSE or smart micoSD

The service provider manages the identities with its Credential Management System (CMS). It uses an SP TSM and connects to the SE Owner-TSM in order to manage the ID Applet and the ID credentials. The credentials are managed via TCP/IP with a remote agent on the mobile device according to the GlobalPlatform SE Remote Application Management [GP SE RAM] specification.

.

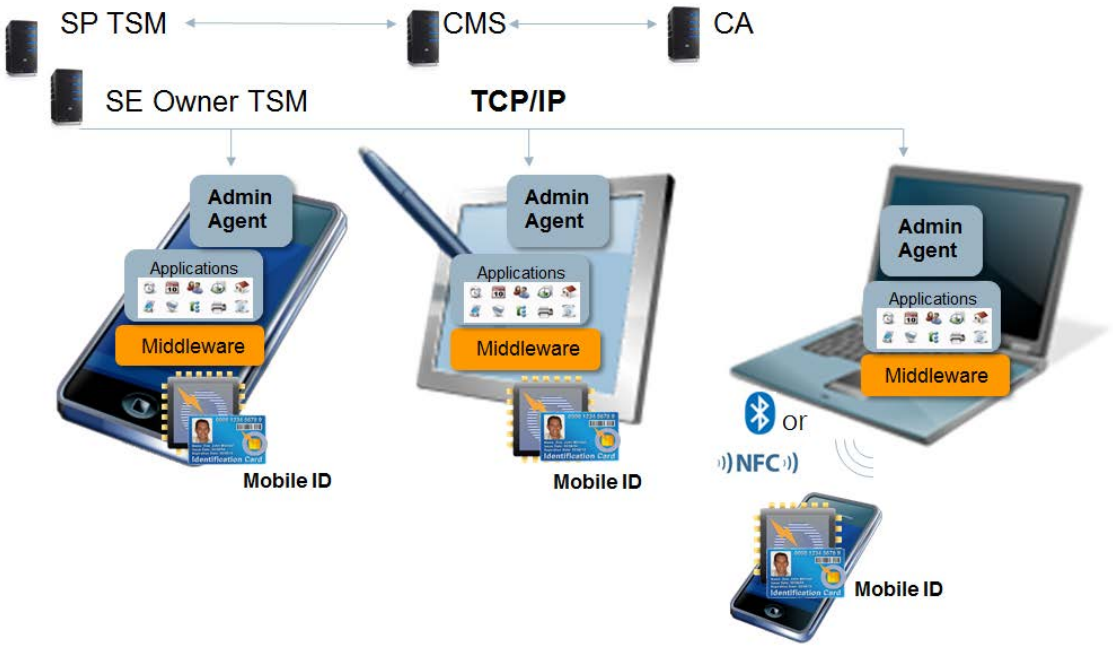


**Figure 14: Credentials on an eSE or smart microSD**

### B.3. Completing Provisioning

The MNO TSM (for UICC) or SE Owner (for an eSE or smart microSD) creates a Security Domain, which is assigned to the service provider. After the Security Domain creation the service provider downloads the Mobile ID application in its Security Domain and loads the corresponding Mobile ID credentials into the Mobile ID application. GlobalPlatform provides the Security Domain model on the card [GP Card], the corresponding messaging standard [GP Msg], and an End-to-End Framework specification [GP E2E] with guidance for implementers and integrators.

## APPENDIX C: Mobile ID Characteristics

This Appendix outlines the characteristics of Mobile ID credentials and applications. It provides additional information for those interested in the Mobile ID architecture.

### C.1. Mobile ID Credentials

Mobile ID credentials may exist in different forms issued by an authority (e.g. enterprise, government, bank) and stored on a mobile device (e.g. smartphone, tablet, laptop). The Mobile ID credentials can be of different forms like QR codes, RFIDs, photographs, cryptographic keys. All the Mobile ID credentials issued on one Mobile ID are typically correlated to one Mobile ID credential issuance entity.

### C.2. Mobile ID Application

A Mobile ID application hosts the Mobile ID credentials which is installed on a platform (i.e. on the SE or TEE depending on the security policies associated with the use case). The purpose of the Mobile ID application is to manage the use of the Mobile ID on this platform.

### C.3. Mobile Application Capabilities

The Mobile ID application capabilities depend on the Mobile ID scheme. For example, if the Mobile ID is defined by a set of cryptographic key credentials, the Mobile ID application has to allow the storage of keys and the execution of cryptographic operations based on these keys. If the Mobile ID is defined by a one-time-password the Mobile ID application acts as an OTP generator which allows the generation of OTPs. If the Mobile ID includes user information in the form of attributes (e.g. name, age, birthday), fingerprint templates or photos, the Mobile ID application has to provide storage records protected by access control functionalities such as privacy protocols or PIN protection.

### C.4. Mobile Application Installation

Mobile ID applications are installed either before or after the issuance of an SE, or a Mobile Device including a TEE or embedded SE:

- **Pre-issuance:** The Mobile ID application is already installed on the SE/TEE. In some cases the application needs to be activated locally or remotely for using the Mobile ID service and in some case the application is already activated and can be immediately used after issuance.
- **Post-Issuance:** The Mobile ID application is provisioned in the field. In this case the Mobile ID application has to be loaded and installed either locally via provisioning tools or remotely via a TSM before the Mobile ID service can be used.

## APPENDIX D: Abbreviations

| Abbreviation | Meaning |
|---|---|
| APDU | Application Protocol Data Unit |
| API | Application Programming Interface |
| CA | Certification Authority |
| CC | Common Criteria |
| CIV | Commercial Identity Verification |
| CMS | Credential Management System |
| CSP | Credential Service Provider |
| EAL | Evaluation Assurance Level |
| eIDAS | Electronic Identification and Trust Services |
| eSE | Embedded Secure Element |
| ETSI | European Telecommunications Standards Institute |
| FIDO | Fast IDentity Online |
| FIPS | Federal Information Processing Standard |
| GSM | Global System for Mobile |
| HCE | Host-based Card Emulation |
| I/O | Input/Output |
| IDM | Identity Management System |
| Ipsec | Internet Protocol Security |
| LoA | Level of Assurance |
| MNO | Mobile Network Operator |
| NFC | Near Field Communication |
| NIST | National Institute of Standards and Technology |
| OS | Operating System |
| OTA | Over-the-Air |
| OTP | One-Time-Password |
| PCA | Privacy-based Chip Authentication |
| PIV | Personal Identification Verification |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| RAM | Remote Application Management |

| Abbreviation | Meaning |
|---|---|
| REE | Rich Execution Environment |
| RP | Relying Party |
| SE | Secure Element |
| SMS | Short Message Service |
| SP | Service Provider |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TEE | Trusted Execution Environment |
| TLS | Transport Layer Security |
| TSM | Trusted Service Manager |
| TTP | Trusted Third Party |
| TUI | Trusted User Interface |
| UI | User Interface |
| UICC | Universal Integrated Circuit Card |
| VPN | Virtual Private Network |

## APPENDIX E: Terminology and Definition

| Term | Document |
|---|---|
| eServices | The provisions of services via the internet |
| Mobile device | A handheld device: (i.e. a small form factor receiving device suitable for carrying in hand, purse or pocket. The antenna is built-in, either internal or deployable. Normal operation is either at pedestrian speeds walking or at vehicular speeds in a moving vehicle. This is typically the mobile phone or smartphone) or portable device (i.e. A receiving device that uses a built-in or set-top antenna, transportable to different locations. This is typically the tablet.) |
| Mobile ID | An ID document hosted in a Mobile Device. This ID document is realized by a Mobile ID application which stores Mobile ID credentials and which allows the usage of these credentials within this application for identification and authentication use cases. The Mobile ID application can be installed and executed in different platforms, REE, TEE or SE. |
| Rich Execution Environment (REE) | An environment that is provided and governed by a Rich OS, potentially in conjunction with other supporting operating systems and hypervisors; it is outside of the TEE. This environment and applications running on it are considered un-trusted.<br>Contrast *Trusted Execution Environment*. |
| Rich OS | An operating system for mobile devices (e.g. Android, Window 8, iOS) that allows the loading of third party applications. The Rich OS runs on top of the Rich Execution Environment. |
| Secure Channel Protocol | A cryptographic protocol referring to a way of transferring data that is resistant to overhearing and tampering. |
| Secure Element (SE) | A secure component which 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 of 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. |

| Term | Document |
|---|---|
| Secure Element Access API | An API used by device applications to exchange data with their counterpart applications running in the Secure Element. |
| Secure Element application | A software application installed and running on the Secure Element. |
| Smart microSD | A small, portable, non-volatile memory card format developed by the SD Card Association (SDA). |
| Trusted Execution Environment (TEE) | The TEE is a secure area of the main processor in a smart phone (or any connected device) that ensures sensitive data is stored, processed and protected in an isolated, trusted environment. The TEE's ability to offer isolated safe execution of authorized security software, known as 'trusted applications', enables it to provide end-to-end security by enforcing protection, confidentiality, integrity and data access rights.<br>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 applications, which need to be isolated from the Rich OS.<br>Contrast *Rich Execution Environment*. |
| Trusted OS | An operating system running in the TEE. It has been designed primarily to enable the TEE using security based design techniques. It provides the GP TEE Internal API to Trusted Applications and a proprietary method to enable the GP TEE Client API software interface from other EE.<br>Contrast Rich OS. |
| Universal Integrated Circuit Card (UICC) | A Secure Element used in the mobile communications industry, as defined in ETSI TS 102 221 [102 221]. |

## APPENDIX F: References

| Reference | Document | Ref |
|---|---|---|
| Common Criteria Methodology | Common Criteria for Information Technology Security Evaluation, Parts 1-3: CCMB-2012-09-001, CCMB-2012-09-002, CCMB-2012-09-003 | [CC] |
| Common Criteria Protection Profiles | Common Criteria Protection Profiles<br>https://www.commoncriteriaportal.org/pps/<br>(The GlobalPlatform TEE Protection Profile is listed in the category Trusted Computing.) | [CC TC] |
| FIPS Methodology | Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules<br>http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm | [FIPS] |
| eIDAS | eIDAS – Trusted Services and eID<br>http://ec.europa.eu/digital-agenda/en/trust-services-and-eid | [eIDAS] |
| eIDAS Token Specification | BSI TR-03110 eIDAS Token Specification<br>https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110-eIDAS_Token_Specification.html | [BSI] |
| eIDAS Token Technical Report | Technical Report: Signature creation and administration for eIDAS token<br>http://www.ssi.gouv.fr/agence/publication/publication-des-specifications-techniques-en-matiere-didentification-electronique-eidas/ | [eIDAS Token] |
| EN 419 212:2014 | EN 419212-1:2014; Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services. (under revision)<br>Available at: http://www.beuth.de/de/norm/din-en-419212-1/226320105 | [EN 419 212] |
| ETSI TS 102 221 | Smart cards; UICC – Terminal interface; Physical and logical characteristics, Release 6, 2004 | [102 221] |
| ETSI TS 102 225 | Smart Cards; Secured packet structure for UICC based applications | [102 225] |
| ETSI TS 102 226 | Smart Cards; Remote APDU structure for UICC based applications | [102 226] |

| Reference | Document | Ref |
|---|---|---|
| ETSI TS 102 622 | Smart Cards; UICC – Contactless Front end (CLF) Interface; Host Controller Interface (HCI), Release 7, 2009 | [102 622] |
| FIDO Universal Second Factor (U2F) | FIDO Universal Second Factor (U2F) 1.0 NFC and BLE (under development) | [FIDO U2F] |
| GPC_SPE_034 | GlobalPlatform Card Specification v 2.2.1, January 2011 | [GP Card] |
| GPC_SPE_007 | GlobalPlatform Card, Confidential Card Content Management, Card Specification v2.2 – Amendment A | [GP Amd A] |
| GPC_SPE_011 | GlobalPlatform Card, Remote Application Management over HTTP, Card Specification v2.2 – Amendment B | [GP Amd B] |
| GPC_SPE_025 | GlobalPlatform Card, Contactless Services, Card Specification v2.2 – Amendment C | [GP Amd C] |
| GPC_SPE_093 | GlobalPlatform Card, Secure Channel Protocol '11', Card Specification v2.2 – Amendment F | [GP SCP11] |
| GPC_GUI_049 | GlobalPlatform Card Secure Element Configuration v1.0, October 2012 | [GP SE Config] |
| GPC_GUI_010 | GlobalPlatform Card Specification v.2.2.1<br>UICC Configuration v1.0.1, January 2011 | [GP UICC Conf] |
| GPC_SPE_100 | GlobalPlatform Card Technology Card Specification<br>GlobalPlaform Privacy Framework v1.0 (under development) | [GP Privacy] |
| GPD_SPE_120 | GlobalPlatform Device Technology<br>TEE Management Framework (under development) | [GP TEE Mgmt] |
| GPD_SCP_21 | GlobalPlatform Device Committee<br>TEE Protection Profile, v1.0 | [GPD TEE PP] |
| GPD_SPE_007 | GlobalPlatform Device Technology<br>TEE Client API Specification | [GPD TEE Client] |
| GPD_SPE_009 | GlobalPlatform Device Technology<br>TEE System Architecture | [GPD Sys Arch] |

| Reference | Document | Ref |
|---|---|---|
| GPD_SPE_010 | GlobalPlatform Device Technology<br>TEE Internal Core API Specification | [GPD Core API] |
| GPD_SPE_020 | GlobalPlatform Device Technology<br>Trusted User Interface API | [GPD Trusted UI] |
| GPD_SPE_024 | GlobalPlatform Device Technology<br>TEE Secure Element API | [GPD TEE SE API] |
| GPD_SPE_100 | GlobalPlatform Device Technology<br>TEE Sockets API Specification | [GP TEE Sockets] |
| GPD_SPE_008 | GlobalPlatform Device Technology<br>Secure Element Remote Application Management | [GP SE RAM] |
| GPS_SPE_002 | GlobalPlatform Systems, Messaging Specification for Management of Mobile-NFC Services | [GP Msg] |
| GPS_GUI_006 | GlobalPlatform Systems<br>End-to-End Simplified Service Management Framework, v1.1 | [GP E2E] |
| GSMA Mobile Connect | GSMA Mobile Connect<br>http://www.gsma.com/personaldata/mobile-connect | [GSMA Mobile] |
| Host Card Emulation | Host-based Card Emulation<br>https://developer.android.com/guide/topics/connectivity/nfc/hce.html | [HCE] |
| ISO/IEC 29115 | Information technology – Security techniques – Entity authentication assurance framework | [29115] |
| NIST FIPS201-2 | Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013.<br>Available at:<br>http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf | [FIPS 201] |
| NIST SP800-157 | Guidelines for Derived Personal Identity Verification (PIV) Credentials, December 2014.<br>Available at:<br>http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf | [SP 800 157] |

| Reference | Document | Ref |
|---|---|---|
| Open Mobile API | SIMalliance Open Mobile API<br>Available under http://www.simalliance.org | [Open Mobile API] |
| TEE Whitepaper | The Trusted Execution Environment:<br>Delivering Enhanced Security at a Lower Cost to the Mobile Market | [TEE WP] |
| TLS | RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2<br>Available at https://www.ietf.org/rfc/rfc5246.txt | [TLS] |

## APPENDIX G: Table of Figures

## APPENDIX H: Table of Tables