GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Practical Considerations: Technical Overview

Realizing FIDO Authentication Solutions with GlobalPlatform Technologies

White Paper Companion

High Level Technical Guide

January 2018

Table of Contents

OVERVIEW

The aim of this document is to provide a high-level technical overview of the necessary considerations when implementing FIDO-based authentication standards based on GlobalPlatform technologies. This paper is intended to educate technical analysts and is a companion to the business considerations white paper.

Please refer to the *Practical Business Considerations White Paper for Realizing FIDO Authentication Solutions with GlobalPlatform Technologies* *https://www.globalplatform.org/mediawhitepapers.asp* for business considerations and use case scenarios.

SECTION 1: TECHNOLOGY ARCHITECTURE

1.1. FIDO Protocols, Credentials, and Application Characteristics

FIDO has standardized two protocols, Universal Authentication Framework (UAF) and Universal Second Factor (U2F). The FIDO protocols use standard public key cryptography techniques to provide stronger authentication and are designed to protect user privacy.

The main tasks users perform using FIDO technology are initial registration with a given online service and subsequent authentication with that service. For this to work, the user needs a FIDO Authenticator that provides the verification mechanism. There are many FIDO Authenticator options, including standalone hardware devices like a U2F token or a fingerprint sensor and its firmware that are integrated into a device.

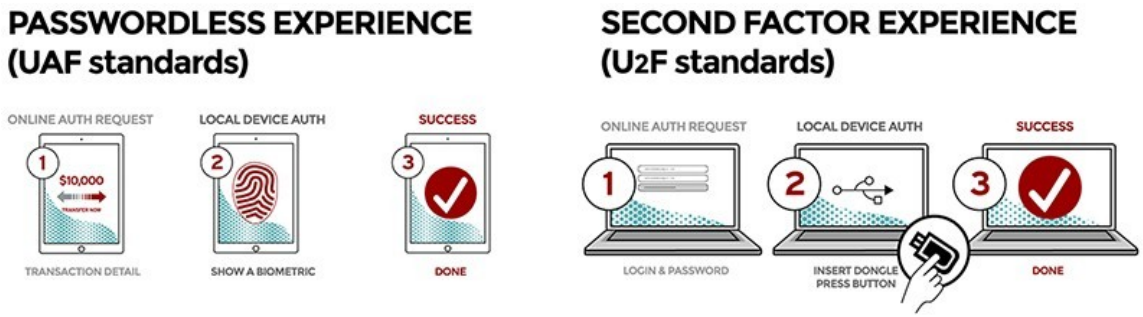


Figure 1: FIDO Standards[1]

1.1.1. UAF Passwordless User Experience

The FIDO Universal Authentication Framework (UAF) provides a passwordless experience. The user registers their device to the online service by selecting a local authentication mechanism, such as swiping a finger, looking at the camera, speaking into a microphone, entering a PIN, etc. The UAF protocol allows the service to select which mechanisms are presented to the user. Once registered, the user simply repeats the local authentication whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms, such as fingerprint and PIN.

1.1.2. U2F Second Factor User Experience

The Universal Second Factor (U2F) Protocol supports the second factor FIDO experience. Second factor allows online services to augment the security factor of their existing password infrastructure by adding a second factor device at any time. The strong second factor allows the service to simplify its passwords (e.g. 4-digit PIN) without compromising security. During registration and authentication, the user presents the second factor by simply pressing a button on a USB device or tapping over near field communication (NFC). The user can use their FIDO U2F device across all online services that support the protocol, leveraging built-in support in web browsers.

[1] https://fidoalliance.org/

1.1.3. FIDO Credentials

FIDO credentials consist basically of the attestation public/private key-pair of the authenticator which can be used to check authenticity: the authentication device itself and the authentication of the public/private key-pair. The public/private key-pair is generated on the authenticator during user registration on a service provider's website, and is later used to authenticate the user to this website.

1.1.4. FIDO Authenticator Application

A FIDO Authenticator application hosts the FIDO Authenticator credentials (public/private keys) which are installed on the authenticator platform (i.e. on the Trusted Execution Environment (TEE) or Secure Element (SE), depending on the security policies associated with the use case). The purpose of the FIDO authenticator application is to manage, store and operate the FIDO credentials on this platform.

1.1.5. FIDO Authenticator Capabilities

The FIDO Authenticator capabilities depend on the used FIDO scheme, U2F and UAF, and on the security requirements. It stores the FIDO credentials and implements the cryptographic algorithms needed to compute the signatures for a FIDO-based authentication, and might also contain features such as user interfaces and buttons that can perform user verification. If the FIDO Authenticator platform is a SE or a TEE, the FIDO Authenticator functionality is typically realized in a FIDO Authenticator application.

1.2. GlobalPlatform Specifications

GlobalPlatform has three main specification areas: Trusted Execution Environments (TEE), Secure Elements (SE), and mobile messaging. This paper focuses on how FIDO-based authentication credentials can be implemented and managed with a TEE or SE using GlobalPlatform Specifications.

FIDO Authenticator Application Installation on a TEE or SE

FIDO Authenticator applications can be installed before or after the issuance of a SE / mobile device with a TEE or embedded SE:

- **Pre-issuance:** The FIDO Authenticator application is already installed on the SE/TEE before issuance. In some cases the application needs to be activated locally or remotely to use the FIDO Authenticator in a service, and in some cases the application is already activated and can be used immediately after issuance.
- **Post-issuance:** The FIDO Authenticator application is provisioned in the field. In this case the FIDO Authenticator application has to be loaded and installed either locally or remotely via provisioning tools (e.g. a TSM) before it can be used.

1.2.1. Trusted Execution Environment Architecture Technical Overview

The GlobalPlatform TEE is a secure area of the main processor in a smart phone (or any connected device). It ensures that 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 protected execution of authenticated code, confidentiality, authenticity, privacy, system integrity, and data access rights. Comparative to other mobile device security environments, the TEE offers high processing speeds and a large amount of accessible memory.

GlobalPlatform's work in this space makes it easier to secure sensitive information or premium content, which is important for the future of the technology. Built on GlobalPlatform Specifications, the TEE helps protect, ease, and accelerate the deployment of value added mobile services, ensuring security while retaining a rich user experience.

The TEE is ideally suited to securing FIDO-based authentication. Adoption of the TEE is especially helpful in addressing public concern around privacy and offers a level of protection against attacks targeting 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 example, the TEE is the ideal environment for content providers offering a video for a limited period, as premium content (e.g. HD video) must be secured so that it cannot be shared for free.

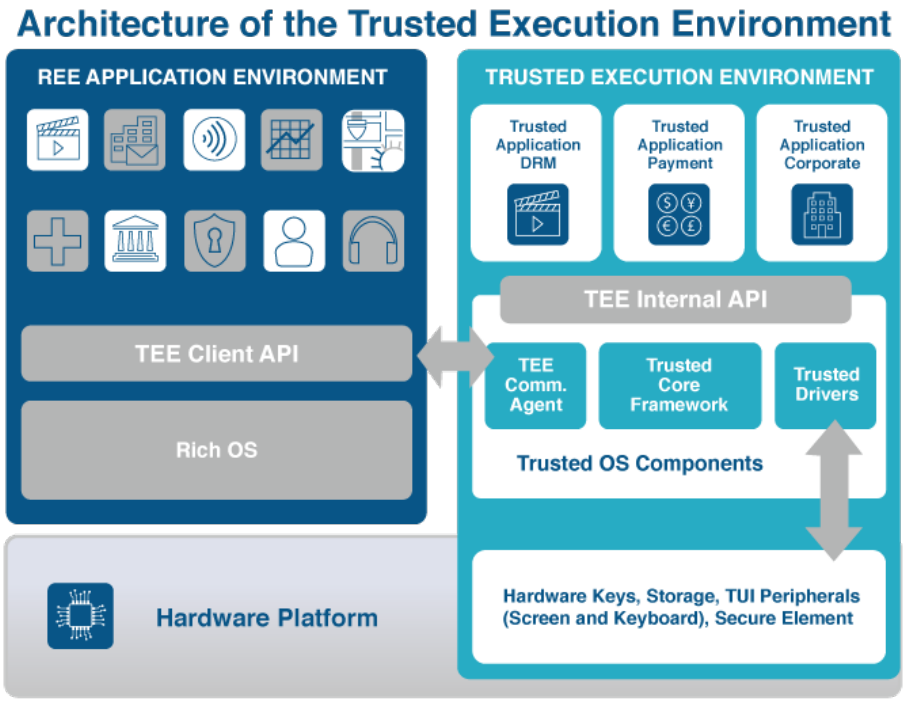


Figure 2: Architecture of the TEE

The TEE exists because of the rising number of mobile services that require a greater user authentication.

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 execution environment, isolated from the REE, which allows the secure execution of applications on a mobile device. This provides the

foundation for a multitude of applications, such as secure payments and authentication, and could potentially serve for the foundation of a FIDO Authenticator as well.

Using the TEE as the hosting platform of FIDO Authenticators has a lot of advantages. For example, the TEE's Trusted User Interface enables trustworthy user verification to be performed in an environment that is physically isolated from the REE. This basically enables the implementation a U2F FIDO Authenticator which is built into the mobile device without the need to use an external device like a token. Moreover, the TEE and its applications can be managed remotely with end-to-end security via a trusted service manager. This allows for a variety of use cases which are not typically implementable on usual FIDO Authenticators.

TEE specifications can be downloaded free of charge from the GlobalPlatform Device Specifications webpage. Also, be sure to read the GlobalPlatform 'Made Simple' guide and the TEE White Paper [TEE WP].

1.2.2. Secure Element

A Secure Element (SE) is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. It ensures that sensitive data is stored, processed and protected in an isolated, secure chip.

GlobalPlatform SE is platform agnostic. There are three different SE form factors: Universal Integrated Circuit Card (UICC), embedded SE, and microSD. Both the UICC and microSD are removable.

Each form factor links to a different business implementation and satisfies a different market need. With GlobalPlatform specifications all SE implementations can be managed the same way, regardless of which form factor is used.

Visit the GlobalPlatform Specification webpages to download the SE Configurations.

SECTION 2: ADVANTAGES OF USING GLOBALPLATFORM TECHNOLOGIES FOR FIDO DEPLOYMENT

GlobalPlatform allows a variety of FIDO deployment scenarios based on the TEE and SE standards on client-devices in the field, including mobile devices, tokens, wearables, and smart cards.

FIDO-based authentication provides a number of powerful benefits to each of its stakeholders – consumers, online service providers, and enterprises. For consumers, FIDO provides strong security and a superior user experience, all while protecting their privacy. It eliminates the need to remember many passwords while providing a higher level of security. FIDO enables the use of many mobile applications that were previously hampered by lack of sufficient security, regardless of market sector, use case or technical implementation.

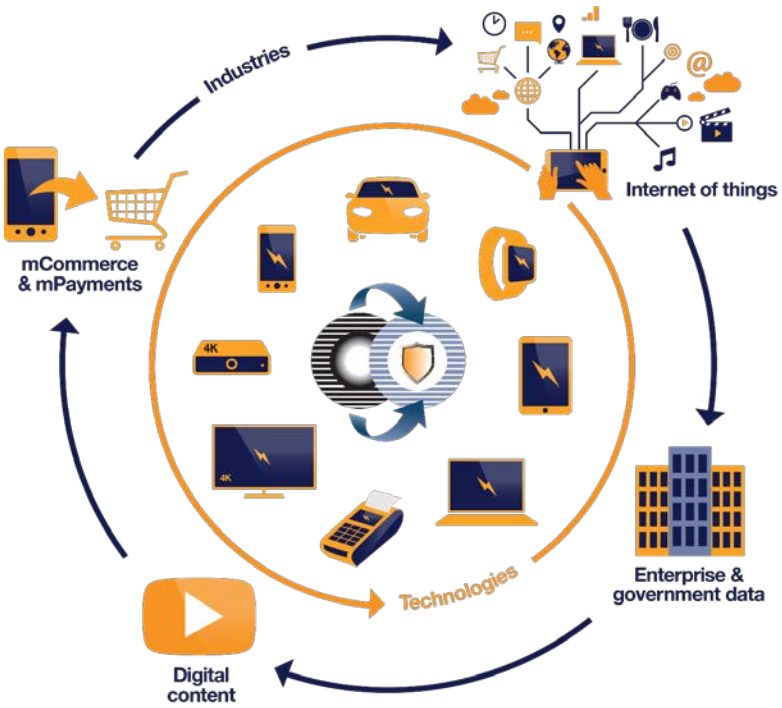


Figure 3: GlobalPlatform Ecosystem

The GlobalPlatform TEE and SE standards enable FIDO Authenticators 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 REE, controlled by a Rich OS. Depending on the FIDO Authenticator type, the single use, or combination of these three elements, can address the varying requirements of FIDO authentication schemes.

Various FIDO 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 FIDO implementations can be determined by a security assurance method, and completed by a security evaluation and certification program. 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 the GlobalPlatform technologies TEE or SE.

2.1. Devices and Standardization

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, a FIDO implementation calls for the enforcement of privacy and security requirements.

GlobalPlatform is responsible for driving global standardization of SEs and TEEs. Its specifications can be leveraged by FIDO solutions and meet the security requirements of FIDO deployments in 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 FIDO Authenticators.

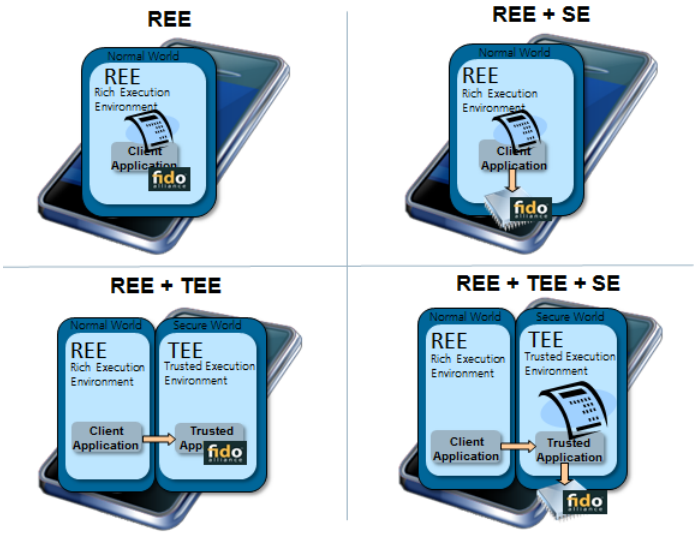
For service providers there are many decisions to be made when integrating FIDO-based authentication with an application service. The most important are: how to enable the user to authenticate themselves; what security level is required; and which combination of execution environments will best fulfill the needs of the service provider application in regard to device requirements, security, deployment, and usability.

SECTION 3: IMPLEMENTATION SOLUTIONS

This section outlines the different implementation scenarios for mobile solutions based on the platforms REE, SE, and TEE, which can help FIDO Authenticator implementers to decide which implementation scenario fits the requirements of their market sector best.

FIDO Authenticators 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 security technologies in the devices (e.g. mobile devices, token devices, wearable devices).

When designing a FIDO Authenticator or solution, service providers and vendors must consider all variables presented in this paper to design the appropriate architecture for the implementation.



3.1. Implementation Solution Scenario: REE

FIDO credentials are stored in the memory of the REE. An REE application that is using the FIDO credentials might store them directly within the application package, or might use FIDO credentials stored by the Rich OS, or by another mobile application. If the FIDO credentials are not stored within the application package itself, the mobile application needs an exposed cryptographic API which allows use of the externally stored FIDO 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 REE application.

Figure 4: REE Implementation Scenario

Table 1: REE FIDO Benefits

Device Requirements	This application can be deployed directly on any device of the same REE platform.
Security	FIDO credentials are stored and used in the REE. Storage and operation might be secured using methods such as white box cryptography, but protection relies on the security provided by the underlying operating system. The user verification data entry occurs on a capture device (e.g. PIN entries on a touch screen managed by the REE) which relies on the security mechanisms provided by the underlying operating system.
Deployment Considerations	This application issuer does not require service contracts for deploying its applications on a TEE or an SE.
Usability	The FIDO credentials stored in a REE mostly apply to mobile devices, and require the mobile application to be started before it can be used as FIDO Authenticator.
Security Considerations	If the FIDO implementation is purely based on the REE it is generally vulnerable to replication attacks. If the device is rooted, the risk that the FIDO credentials will be compromised is very high. The security level of this solution scenario relies entirely on the security of the REE OS, as security levels of different operating systems and different versions of the same operating systems vary.

3.2. Implementation Solution Scenario: REE + SE

FIDO credentials are stored and cryptographic operations performed in a SE. The REE application triggers the SE cryptographic operations (e.g. performing the signature for authentication) with these FIDO credentials. The command interface of the FIDO Authenticator residing on the SE may be the SIMalliance Open Mobile API [Open Mobile API] on mobile devices or PC/SC [PCSC] on laptop/workstation computers. The user interfaces for verification are implemented by the application in the REE.

The FIDO Authenticator application in the SE could be offered as a global service towards all client applications in the REE. This would allow developers to use SE security services for their mobile application without the need to write a SE application for each REE application. This global service could be implemented by a single SE application as a shared service, or be part of the SE OS.

Figure 5: REE + SE Implementation Scenario

Table 2: REE + SE FIDO Benefits

Device Requirements	In cases where REE applications need access to the FIDO credentials in the SE, this solution can only be deployed on devices which support or embed a SE. In specific FIDO use cases where an external terminal uses the FIDO credentials, the SE would need to be accessible via NFC, Bluetooth Low Energy (BLE), USB or any other means.
Security	FIDO 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 FIDO Authenticators with non-repudiation. This solution allows the installation of a FIDO application among other applications on the SE in an isolated way by using the GlobalPlatform Security Domain model. The user verification data entry, such as PIN entry, occurs on a capture device (i.e. on a smartphone) not on the SE itself. Therefore, user verification data entry has the same level of security as the capture device, rather than the higher level of security of the SE. For NFC and BLE based use cases, SCP '11' [GP SCP11] can be used to secure the wireless/contactless communication between the capture device and the SE.
Usability	In case one, if the device has an embedded SE then the FIDO credentials are stored in the eSE. In the second example, with a SE such a contactless smart card, an external terminal (e.g. the end-user's mobile device) can directly use the FIDO credentials stored on the SE via the contactless interface.
Deployment Considerations	This solution requires the deployment of a FIDO application in the SE, which necessitates an installation contract with the SE issuer or a deployment on one's own SE.
Security Considerations	This solution provides tamper resistant protection for FIDO credentials and can perfectly protect these credentials 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 data entry happens in a separate component, the capture device, which is not under control of the SE. Most of the SEs are certifiable environments under stringent security schemes, which may be required for strong authentication.

3.3. Implementation Solution Scenario: REE + TEE

The FIDO credentials are stored in a TEE and cryptographic operations are performed within this TEE. The REE application triggers the TEE cryptographic operations with these FIDO credentials. The command interface of the FIDO Authenticator residing in the TEE may be the TEE Client API [GPD TEE Client].

The FIDO Authenticator application 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 REE application. This global service could be implemented by a single Trusted Application as a shared service or could be part of the TEE OS.

If the TEE does not support a Trusted User Interface (TUI), the mobile application in the REE handles the user interactions and data entries, asking the user for the password or PIN code, for example, which will finally be transferred to the TEE and verified by the FIDO Trusted Application residing in the TEE.

Figure 6: REE + TEE FIDO Scenario, Step 1

If the TEE supports a Trusted User Interface as a feature, the user interfaces for the verification data entry can be implemented directly by the FIDO Authenticator within the TEE by using the TEE Trusted User Interface API [GPD Trusted UI]. The TEE makes it possible to securely collect the user's input (e.g. password or PIN code), which can be verified by the FIDO Authenticator Trusted Application. Additionally, the FIDO Authenticator Trusted Application can inform the user about the relying party requesting authentication and use the Trusted UI for the implementation of FIDO Transaction Confirmation (i.e. "what-you-see-is-what-you-sign").

Through its Trusted User Interface feature, the TEE can even implement a FIDO U2F authenticator in the same device as the user applications. This is possible as the user presence verification is physically isolated from the user applications in the REE and therefore acts like a dedicated second factor authenticator (e.g. USB/NFC token). Moreover, the TEE also enables fingerprint-based user verification if the TEE supports the TEE Biometrics Fingerprint API [GPD TEE Bio API]. In this case, all fingerprint templates are stored in the TEE and the matching process is operated entirely within the TEE.

Figure 7: REE + TEE FIDO Scenario, Step 2

Table 3: REE + TEE FIDO Benefits

Device Requirements	A solution based on a TUI can only be deployed on devices which support a TEE with TUI.
Security	The storage and usage of FIDO credentials is performed in the TEE, preventing a large number of software attacks. If the TEE supports a TUI, the user verification data entry can also be protected from software attacks and leverages the TEE as a U2F authenticator serving as a second factor token integrated in the device. This protection can even be extended to the fingerprint-based user verification as long as the TEE supports the Biometrics Fingerprint API.
Usability	The FIDO credentials in a TEE mostly apply to mobile devices and require the mobile application to start before it can be used as FIDO authenticator from another device (e.g. connected via BLE connection).
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 FIDO Authenticators where all critical components, from user interface to processing environment and storage, can be certified.

3.4. Implementation Solution Scenario: REE + TEE + SE

The FIDO credentials are stored in a SE and cryptographic operations are performed within this SE. The FIDO Authenticator is a Trusted Application in the TEE that is triggered to perform the user verification by a client application in the REE. Once the user is successfully verified, the Trusted Application triggers the SE cryptographic operations. The command interface between the TEE and SE may be the TEE SE API [GPD TEE SE API]. The user verification data entry may be 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 input (e.g. password or PIN code) that can be verified by the FIDO application in the SE. Moreover, the TEE also allows

fingerprint-based user verification if the TEE supports the TEE Biometrics Fingerprint API [GPD TEE Bio API]. In this case all fingerprint templates are stored either in the TEE or SE and the matching process is completely operated within the TEE/SE. Additionally the FIDO Authenticator Trusted Application can inform the user about the relying party requesting authentication and use Trusted UI for the implementation of FIDO Transaction Confirmation (i.e. “what-you-see-is-what-you-sign”).

Figure 8: REE + TEE + SE FIDO Scenario

Table 4: REE + TEE + SE FIDO Benefits

Device Requirements	This solution can only be deployed on mobile devices which support a TEE with TUI, and support or embed an SE. The SE might be an internal SE such as a UICC, eUICC, eSE or smart microSD. The SE might also be an external SE like an ID-1 card, NFC or USB token which is tapped on or plugged into the device.
Security	FIDO credentials are stored and used in a tamper resistant environment which prevents a large number of attacks, including physical attacks. The user verification is performed in the TEE, preventing a large number of software attacks. 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 usage of the TEE for the Trusted User Interface mostly applies to mobile devices and requires the FIDO application to start before it can be used as a FIDO Authenticator from another device (e.g. connected via BLE). In the case of a removable SE, e.g. UICC or smart microSD, the FIDO credentials can be easily transferred to another mobile device. Since external SEs like an ID-1 card, NFC or USB token can be used on a variety on devices (also laptop computers, workstations or terminals) it cannot be always assured that the interacting device has the capability of a TEE for the user verification.
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 higher installation and maintenance costs than other solution scenarios.
Security Considerations	This solution provides the highest level of security and is especially useful for FIDO 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 FIDO applications where all critical components, including the user interface, processing environment and storage, can be certified. The SE, which hosts the FIDO credentials and performs the cryptographic operations, even allows certification under stringent security schemes.

SECTION 4: TECHNICAL ON-BOARDING AND PROVISIONING FOR FIDO ON TEE AND SE

The onboarding and provisioning of FIDO Authenticators and credentials are discussed briefly in section 3. This section provides additional technical detail.

The FIDO Authenticator might be implemented based on the TEE or SE platform. Depending on the technology chosen, different scenarios are possible to on-board the FIDO Authenticator and to provision corresponding FIDO credentials (e.g. authenticator attestation keys). GlobalPlatform Specifications provide frameworks, configurations, profiles, protocols and interfaces which allow the administration and life cycle management for TEEs and an SEs to be performed in a secure and interoperable way. These specifications allow a multi-tenant Security Domain model, on a TEE and a SE Infrastructure scenarios with TSM and OTA can build on these specifications in order to perform remote on-boarding and provisioning as well as management of the FIDO Authenticator application on different mobile devices.

4.1. On-boarding and Provisioning of FIDO on a UICC

The service provider uses an SP-TSM and connects to an MNO-TSM in order to download the FIDO Authenticator application and corresponding attestation keys to the UICC.

The on-boarding and provisioning operations are realized 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, hence the messages cannot be intercepted or inhibited by mobile applications once the device is connected to the mobile network. The FIDO Authenticator application and credentials may also be transferred via TLS secured Transmission Control Protocol (TCP) / Internet Protocol (IP) channels with a remote agent on the mobile device according to GlobalPlatform SE Remote Application Management [GP SE RAM]) if the application or credentials are too large for an OTA transfer.

Figure 9: On-boarding and Provisioning FIDO on a UICC

4.2. *On-boarding and Provisioning of FIDO on an eSE or smart microSD*

The service provider uses an SP-TSM and loads the FIDO Authenticator application and FIDO credentials (attestation keys) on the Security Domain of the eSE or smart microSD previously created by the SE Owner TSM. The communication to the end-device is realized via TCP/IP with a remote agent on the devices, according to the GlobalPlatform SE Remote Application Management [GP SE RAM] Specification.

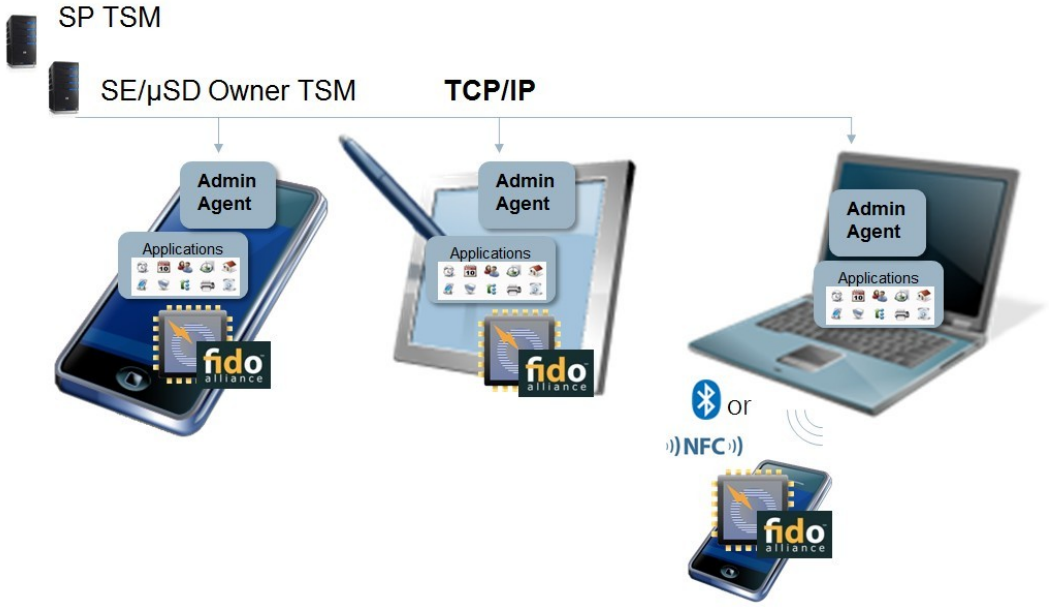


Figure 10: On-boarding and Provisioning FIDO on an eSE or smart microSD

4.3. *Completing On-boarding and Provisioning of FIDO*

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 creation of the Security Domain, the service provider downloads the FIDO Authenticator application in its Security Domain and loads the corresponding FIDO credentials (attestation keys) into the FIDO Authenticator 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.

4.4. *On-boarding and Provisioning of FIDO on a TEE*

Like in the eSE/smart micro SD case, the service provider uses an SP-TSM, which enables downloading of the FIDO Authenticator application with its corresponding FIDO credentials (attestation keys) to its own Security Domain, which was previously created by the TEE owner. The communication to the end-device can be realized via TCP/IP with a remote agent on the devices. The TEE management protocols are defined in the GlobalPlatform Trusted Management Framework [GP TEE TMF].

4.5. *On-boarding and Provisioning of FIDO on SE/TEE via App Store*

GlobalPlatform also allows service providers to on-board FIDO Authenticator applications on TEEs and SEs via the app store and without involving an Issuer-TSM. The scheme for SEs is described in the GlobalPlatform Decentralized Secure Element Management (DSEM) and is based on public-key cryptography and access management based on certificates. Likewise, the TEE scheme is defined as an offline-management implementation option in the GlobalPlatform Trusted Management Framework [GP TEE TMF].

4.6. *Post-loading the FIDO application*

GlobalPlatform allows secure downloading of a FIDO application to a secure component in the field via TSM and remote management after the initial download.

GlobalPlatform also allows downloading of a FIDO Authenticator application via master device (user device, e.g. mobile phone, laptop) to an authenticator (e.g. a token or smart card) and management afterwards from the user device based on a BLE connection. The BLE functionalities provided by GlobalPlatform cover discovery and communication:

Discovery: Allows a master device to search for authenticators and to understand that there is a GlobalPlatform Secure Component (SC) available.

Communication: “BLE Tunneling Agent”. Manages the transfer of the GlobalPlatform commands from a master device to the TEE or SE.

SECTION 5: SECURITY, COMPLIANCE, AND CERTIFICATION

Typically, authentication devices such as tokens or smart cards must fulfill security requirements that are defined by certification schemes. Nowadays mobile device security has also improved thanks to the integration of SE and TEE technology, which are certified against Common Criteria [CC] or FIPS [FIPS] like smart cards and tokens.

The GlobalPlatform TEE Certification Scheme evaluates the security level of a given TEE implementation. To drive this initiative, GlobalPlatform has also launched a TEE Security Evaluation Secretariat to manage the scheme. Under the scheme, providers of TEE products will be able to submit their products to the new GlobalPlatform Secretariat for independent evaluation of their conformance to the organization's TEE Protection Profile.

5.1. Implementation Security Levels

The security level of a FIDO implementation on the client device depends on three functionalities: storage, user I/O, and processing. All 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 platforms for a certain functionality in a FIDO client, specifically the FIDO Authenticator which the FIDO client application relies on to execute a FIDO authentication with the FIDO server.

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

   FIDO credentials (i.e. Authenticator private keys) include highly sensitive assets such as cryptographic keys which need to be protected to assure a certain trust level. Credential storage can be implemented at a basic level in the REE, however there is a risk that the credentials might be compromised if the REE is hacked. Using the TEE for credential storage eliminates the risk of software attacks which can occur in the REE (e.g. OS rooting, jail breaking, malware). In order to assure protection against hardware attacks, the SE can serve as a tamper-proof credential storage environment, although the storage capacity of SEs is limited.

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

   The usage of FIDO credentials for authentication requires user verification, which is typically based on PIN/password entry or biometric operations (e.g. fingerprint verification). After successful verification of the user, credentials are unlocked and can be used to perform a cryptographic operation (i.e. a digital signature for authentication). The PIN/password entry requires the implementation of an application with a user interface. Another FIDO use case where a user interface is required is the display of Data to Be Signed (DTBS), which will be signed for transactions (FIDO Transaction Confirmation). 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 underlying platform of the capture device. The REE can be used to implement the user interfaces (e.g. touch screen), however, there is a risk that the PIN/password could be intercepted or the display content could be counterfeited by malware, especially if the Rich OS is hacked 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 that is resistant against software attacks even if the REE is compromised ("what-you-see-is-what-you-sign"). 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)

   The FIDO use cases registration and authentication 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 offering 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 provides a certain level of security. It balances security (trust and isolation) with performance, and can 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.

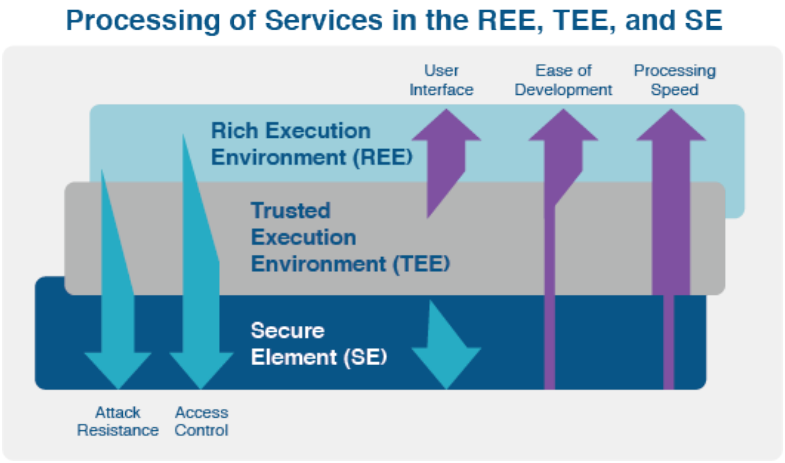


Figure 11: Processing of Services in the REE, TEE, and SE

GlobalPlatform has invested in compliance since 2002 to evaluate the alignment of smart cards and SEs to GlobalPlatform Specifications. The GlobalPlatform Compliance Program provides a foundation for interoperability, stability, and confidence in the secure chip industry by evaluating the functional behavior of products against GlobalPlatform requirements. This lowers the cost of progress for industry players such as application developers, hardware manufacturers, and software developers by removing barriers caused by interoperability issues.

SEs are required to complete security certification, to address sensitive use cases such as government, telecommunication, or banking. The certification is based either on Common Criteria (CC) 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 in its Trusted Computing [CC TC] category.

The GlobalPlatform Compliance Program evaluates the functional behavior of a product against the requirements outlined in GlobalPlatform Configurations and associated Specifications to achieve market interoperability.

With FIDO, you have one universal specification to build to, while the rich ecosystem of FIDO Certified products and services enables turnkey deployment.

It is essential that secure chip services perform as intended ***every single time without fail,*** across not only a variety of device types but across many makes and models of the same device type from different manufacturers AND across different service delivery channels AND independently and securely from any other service or app used by the end consumer.

When using the GlobalPlatform infrastructure, service providers can be sure that their service will behave in the correct way, regardless of the device it is deployed on. Any device/product that has been certified as 'compliant' to GlobalPlatform Specifications by a range of independent third-party test laboratories carries this assurance.

Deploying FIDO-based solutions can help protect customer privacy and meet global regulations.

While proprietary implementations could certainly recreate each of these capabilities, the existing TEE APIs provide faster time to market and are based on the TEE Protection Profile established by GlobalPlatform.

GlobalPlatform is committed to ensuring the long-term interoperability of embedded applications on secure chip technology. It has developed an open and thoroughly evaluated compliance ecosystem for the SE and TEE components and systems, with qualified products, test tool suppliers and laboratories.

Service providers want users of their service to have a consistent and predictable experience every single time.

Devices certified as compliant to GlobalPlatform Specifications give secure chip service providers the peace of mind that their service will always behave as intended when running on that device, regardless of variable deployment choices (e.g. device type, make and model, service delivery channels).

GlobalPlatform's infrastructure also ensures that secure chip services hosted on a device alongside other services or apps, remain independent and secure.

TEE Security Certification Scheme helps protect, ease and accelerate the deployment of value added mobile services, ensuring security while retaining a rich user experience.

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

For more details about the FIDO Alliance and its standardization efforts, please visit http://fidoalliance.org.

APPENDIX A: ACRONYMS AND ABBREVIATIONS

Abbreviation	Meaning
APDU	Application Protocol Data Unit
API	Application Programming Interface
CA	Certification Authority
CC	Common Criteria
EAL	Evaluation Assurance Level
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
MNO	Mobile Network Operator
NFC	Near Field Communication
OS	Operating System
OTA	Over the Air
PKI	Public Key Infrastructure
RAM	Remote Application Management
REE	Rich Execution Environment
RP	Relying Party
SCP	Secure Channel Protocol
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
TUI	Trusted User Interface
UI	User Interface
UICC	Universal Integrated Circuit Card

APPENDIX B: TERMINOLOGY AND DEFINITIONS

Term	Definition
µSD	MicroSD
APDU	Application Protocol Data Unit
API	Application Program Interface
BLE	Bluetooth Low Energy
DSEM	Decentralized Secure Element Management
DTBS	Data to be Signed
ETSI	European Telecommunications Standards Institute
FIDO	Fast IDentity Online
HTTP	Hypertext Transfer Protocol
HW	Hardware
I/O	Input/Output
MNO	Mobile Network Operator
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.)
NFC	Near Field Communication
OTA	Over the Air
PIN	Personal Identification Number
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. 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.
SC	Secure Component
Secure Channel Protocol (SCP)	A cryptographic protocol referring to a way of transferring data that is resistant to overhearing and tampering.

Term	Definition
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.
Secure Element 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).
SMS	Short Message Service
SP	Service Provider
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
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. 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. 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 execution environments. Contrast: *Rich OS*
TSM	Trusted Service Manager
TUI	Trusted User Interface
U2F	Universal Second Factor
UAF	Universal Authentication Framework

Term	Definition
Universal Integrated Circuit Card (UICC)	A Secure Element used in the mobile communications industry, as defined in ETSI TS 102 221 [102 221].
USB	Universal Serial Bus

APPENDIX C: 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 https://www.commoncriteriaportal.org/pps/ (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 http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm	[FIPS]
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]
ETSI TS 102 622	Smart Cards; UICC – Contactless Front end (CLF) Interface; Host Controller Interface (HCI), Release 7, 2009	[102 622]
FIDO Privacy Principles	FIDO Privacy Principles, Whitepaper, Feb 2014	[FIDO Privacy]
FIDO Universal Authentication Framework (UAF)	FIDO Universal Authentication Framework (UAF) 1.0	[FIDO UAF]
FIDO Universal Second Factor (U2F)	FIDO Universal Second Factor (U2F) 1.0 NFC and BLE	[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]

Reference	Document	Ref
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 UICC Configuration v1.0.1, January 2011	[GP UICC Conf]
GPC_SPE_100	GlobalPlatform Card Specification GlobalPlatform Privacy Framework v1.0 (under development)	[GP Privacy]
GPD_SPE_120	GlobalPlatform Device Technology TEE Management Framework (under development)	[GP TEE Mgmt]
GPD_SCP_21	GlobalPlatform Device Committee TEE Protection Profile, v1.0	[GPD TEE PP]
GPD_SPE_007	GlobalPlatform Device Technology TEE Client API Specification	[GPD TEE Client]
GPD_SPE_009	GlobalPlatform Device Technology TEE System Architecture	[GPD Sys Arch]
GPD_SPE_010	GlobalPlatform Device Technology TEE Internal Core API Specification	[GPD Core API]
GPD_SPE_020	GlobalPlatform Device Technology Trusted User Interface API	[GPD Trusted UI]
GPD_SPE_024	GlobalPlatform Device Technology TEE Secure Element API	[GPD TEE SE API]
GPD_SPE_042	GlobalPlatform Device Technology TEE Trusted User Interface API for Biometrics	[GPD TEE Bio API]
GPD_SPE_100	GlobalPlatform Device Technology TEE Sockets API Specification	[GP TEE Sockets]
GPD_SPE_120	GlobalPlatform Device Technology TEE Management Framework	[GP TEE TMF]
GPD_SPE_008	GlobalPlatform Device Technology Secure Element Remote Application Management	[GP SE RAM]
GPS_SPE_002	GlobalPlatform Systems, Messaging Specification for Management of Mobile-NFC Services	[GP Msg]

Reference	Document	Ref
GPS_GUI_006	GlobalPlatform Systems End-to-End Simplified Service Management Framework, v1.1	[GP E2E]
Host Card Emulation	Host-based Card Emulation https://developer.android.com/guide/topics/connectivity/nfc/hce.html	[HCE]
Open Mobile API	SIMalliance Open Mobile API Available under http://www.simalliance.org	[Open Mobile API]
PCSC	PC/SC Workgroup Specifications 2.01.10	[PCSC]
TEE Whitepaper	The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market	[TEE WP]

APPENDIX D: TABLE OF FIGURES

APPENDIX E: TABLE OF TABLES