GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Practical Business Considerations

Realizing FIDO Authentication Solutions with GlobalPlatform Technologies

White Paper

January 2018

Table of Contents

INTRODUCTION

In the past decade, many global industries seeking to meet the needs of their customers via new routes to market have capitalized on the digitalization of services: payments, telecoms, transportation, automotive, smart cities, smart home, utilities, healthcare, premium content, government and enterprise ID, to name just a few. As consumer and industrial demand continues to drive growth in digital services, an increasing number and choice of devices are accessing digital services, such as smartphones, tablets, set top boxes, wearables, connected cars, other Internet-of-Things (IoT) devices and smart cards.

Growth in the number of mobile devices alone is multiplying five times faster than the population globally[1]. In 2014 the number of mobile devices was reported to be over 7.2 billion[2], officially surpassing the number of human beings on the planet.

But the ubiquity of connected devices is changing how people engage in day-to-day activities and increases security concerns about the information stored on, or accessed by these devices. This growth also challenges product and service providers to deliver a secure, frictionless user experience across different markets, devices, and channels.

GlobalPlatform exists to solve the very real security challenge that this dynamic landscape creates: it empowers service providers and device manufacturers to ensure that all devices are secure enough to protect against threats and attacks, and so enable the delivery of secure digital services to end users.

In parallel, FIDO Alliance is working to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords. To be trusted, though, the implementation of FIDO-based authentication calls for the enforcement of privacy and security requirements.

GlobalPlatform-certified secure components enable the protection and secure management of digital services and, as such, are perfectly suited to securing FIDO Authenticators for robust online authentication.

For this reason, GlobalPlatform and FIDO Alliance are collaborating. This means that device makers that want to integrate a stable solution can rely on GlobalPlatform technology. By choosing to develop and deploy secure services using GlobalPlatform's open and standardized infrastructure, service providers can develop their service once, deploy everywhere, and support all use cases; both today and in the future. This solution also creates significantly more choice, convenience and privacy for consumers.

This document provides an overview of GlobalPlatform's work to standardize and certify secure components and demonstrate the value that they bring to secure FIDO-based authentication for a range of different use cases. It also offers guidance on where to find in-depth implementation guidance. This paper is primarily a tool to help product managers and business analysts to understand the value of GlobalPlatform technologies in the context of FIDO-based authentication. More technical details are available in the companion document: *Practical Considerations: Technical Overview* white paper available at *https://www.globalplatform.org/mediawhitepapers.asp*.

As always, we welcome all feedback on this business perspective and any of the documents published through GlobalPlatform.

Kevin Gillick
Executive Director
GlobalPlatform

BACKGROUND

An Introduction to GlobalPlatform

GlobalPlatform is a non-profit industry association driven by over 100 member companies. Members share a common goal to develop GlobalPlatform's specifications, which are today highly regarded as the international standard for enabling digital services and devices to be trusted and securely managed throughout their lifecycle.

GlobalPlatform protects digital services by standardizing and certifying a security hardware/firmware combination, known as a secure component, which acts as an on-device trust anchor. This facilitates collaboration between service providers and device manufacturers, empowering them to ensure adequate security within all devices to protect against threats.

GlobalPlatform specifications also standardize the secure management of digital services and devices once deployed in the field. Altogether, GlobalPlatform enables convenient and secure digital service delivery to end users, while supporting privacy, regardless of market sector or device type. Devices secured by GlobalPlatform include connected cars, set top boxes, smart cards, smartphones, tablets, wearables, and other Internet-of-Things (IoT) devices.

The technology's widespread global adoption delivers cost and time-to-market efficiencies to all. Market sectors adopting GlobalPlatform technology include automotive, healthcare, government and enterprise ID, payments, premium content, smart cities, smart home, telecoms, transportation, and utilities.

GlobalPlatform's legacy of successful technical specification development is thanks to two decades of energetic and effective industry collaboration. Members influence the organization's output through participation in technical committees, working groups and strategic task forces. GlobalPlatform technology is developed in collaboration with numerous standards bodies and regional organizations across the world, to ensure continual relevance and timeliness. For more information visit www.globalplatform.org.

A Collaborative Ecosystem

GlobalPlatform works with its members and a number of industry bodies to ensure its specifications address the requirements across vertical markets and geographies. These collaborations promote open ecosystems, in which all stakeholders can efficiently deliver innovative digital services while providing greater security, privacy, simplicity and user convenience.

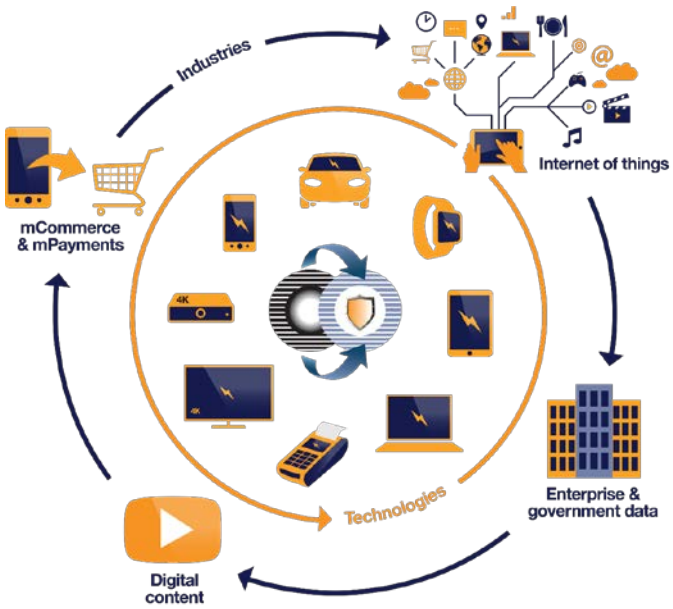


Figure 1: GlobalPlatform Ecosystem

Managing risk is in the interests of all stakeholders. GlobalPlatform technology enables secure digital services to be brought to market by protecting digital assets (e.g. a fingerprint or cryptographic keys) and their associated security services (e.g. authentication). GlobalPlatform's membership does this by standardizing two secure component technologies: Secure Element (SE) and Trusted Execution Environment (TEE). These address various functional and security requirements of the market, giving OEMs the interoperable hardware-based platforms they need while offering service providers the required levels of on-device security.

The impact of GlobalPlatform's collaborative work can be seen in the global deployment of secure components in line with its specifications:

- **SE –** GlobalPlatform conservatively estimates that 41% of all Secure Elements (SE) deployed globally between 2010 and 2016 were based on GlobalPlatform Specifications – a total of 22.018 billion.[3]
- **TEE -** Currently, more than a billion processors that can support TEE are shipped worldwide per quarter.[4]

Introducing the FIDO Alliance

The FIDO (Fast IDentity Online) Alliance is a non-profit organization nominally formed in July 2012 to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords. It is changing the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services.

The cross-industry consortium provides a rich set of specifications and certifications for an emerging and interoperable ecosystem of hardware, mobile, and biometrics-based devices. This ecosystem enables web service providers to deploy strong authentication solutions that reduce password dependencies and provide a superior, simpler, and trusted user experience.

This new standard for security devices and browser plugins allows any website or cloud application to interface with a broad variety of existing and future FIDO Certified devices that users can leverage for enhanced online security. For more information visit www.fidoalliance.org.

GLOBALPLATFORM – SECURE COMPONENTS & CERTIFICATION

GlobalPlatform works with the ecosystem to ensure its secure component specifications answer the rapidly evolving needs of a wide range of device manufacturers, vertical markets and geographies. This section assesses the value of these secure components, and the association's functional and security certification programs, for the protection of FIDO Authenticators.

GlobalPlatform-Certified Secure Components

GlobalPlatform-certified secure components can be used by OEMs to implement FIDO-based authentication and to safeguard the security, integrity and privacy of digital services from multiple providers deployed alongside each other on the same platform. 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 to secure FIDO Authenticators for robust online authentication.

The following outlines the attributes of GlobalPlatform-certified secure components.

Trusted Execution Environments

The GlobalPlatform TEE is a secure area in the main processor of 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 security environments on the device, the TEE also offers high processing speeds and a large amount of accessible memory. Additionally, the GlobalPlatform TEE Specifications support the concept of Trusted User Interface (TrustedUI), allowing users to interact with the secure portion of their device in a trusted way (e.g. secure PIN entry and "what-you-see-is-what-you-sign").

For more information on TEE, refer to the following resources:

- Companion Technical document to this white paper
    - Practical Considerations: Technical Overview - Realizing FIDO authentication solutions with GlobalPlatform Technologies
- TEE 'Made Simple' guide
- TEE specifications can be downloaded free of charge from the GlobalPlatform Device Specifications webpages.

Secure Elements

SEs are secure components which comprise 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 microSD. Both the UICC and microSD are removable. Each form factor links to a different business implementation and satisfies a different market need.

For more information on SE, refer to the following resources:

- SE 'Made Simple' guide
- SE specifications can be downloaded free of charge from the GlobalPlatform Card Specifications webpages.

GlobalPlatform Functional and Security Certification

GlobalPlatform TEE and SE technologies enable digital services and devices to be protected and securely managed, while privacy is supported. These address various functional and security requirements of the market, while offering service providers the required levels of on-device security.

Through its security and functional certification programs, GlobalPlatform enables device manufacturers to proactively market their products as meeting the needs of digital service providers. The programs objectively illustrate that a device manufacturer's GlobalPlatform-based secure component and digital service management capabilities are interoperable and meet required security levels, aiding service providers in their selection of products.

Functional certification (for SE and TEE products) evaluates the functional behavior of a product against the requirements outlined by GlobalPlatform Configurations and associated specifications to achieve market interoperability. Independent testing provides confirmation that the digital service will perform as intended in the field.

Security certification (for TEE products) confirms conformance of TEE products to the Common Criteria recognized GlobalPlatform Protection Profile, through independent security evaluation. It ensures that secure components meet the required levels of security defined for a particular service, enabling service providers to comply with industry requirements and manage risk effectively.

Certified GlobalPlatform technology gives service providers and device manufacturers the means to interact seamlessly when deploying secure digital services, regardless of market or device type. The resulting collaboration makes the mass marketing of secure digital services possible, while bringing time and cost efficiencies to stakeholders within the ecosystem.

- **Device manufacturers** can embed a standardized and certified security hardware/firmware combination, known as a secure component. This meets the needs of service providers for an accessible, on-device physical 'trust anchor' to protect digital services from fraud and attack.
- **Service providers** are free to focus on enhancing their digital offerings by using a secure component to solve security challenges. Additionally, service providers are empowered to develop their digital service just once and deploy it universally across any device with a secure component, with the assurance that security levels will be maintained across all.
- **Digital service users** benefit from greater simplicity, convenience, security and privacy through a limitless expansion of the digital services market.

FIDO ALLIANCE DEPLOYMENT WITH GLOBALPLATFORM TECHNOLOGIES

The below explains the authentication frameworks defined by FIDO and how GlobalPlatform supports the deployment and protection of FIDO Authenticators in consumer devices and hardware tokens.

FIDO Protocols

FIDO technology allows consumers to perform an initial registration with an online service and subsequently authenticate themselves to access and use the service. For this to work, the user needs a FIDO Authenticator to act as the verification mechanism.

To enable secure online authentication and protect user privacy FIDO defines two standardized protocols that use standard public key cryptography techniques: Universal Authentication Framework (UAF) and Universal Second Factor (U2F). These protocols support many FIDO Authenticator options, two of which are as follows:

1. Using a fingerprint sensor and its firmware that are integrated into a device;
2. Using a standalone hardware device such as a U2F token.

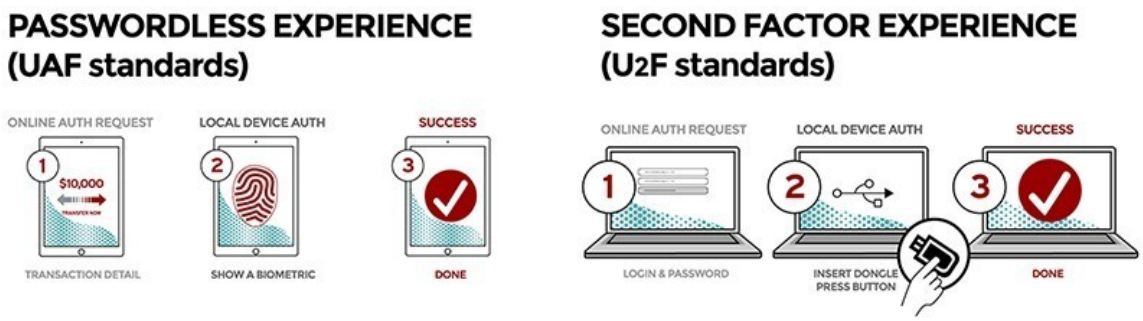


Figure 2: FIDO Standards[5]

FIDO Universal Authentication Passwordless User Experience

The passwordless experience allows users to register a device with an online service by selecting a local authentication mechanism, such as swiping a finger, looking at the camera, speaking into a microphone and entering a PIN. The UAF protocol used to achieve this allows the service to select which mechanisms are presented to a user. Once registered, users simply repeat the local authentication whenever they need to authenticate to the service. Users no longer need to enter a password when authenticating from that device and the UAF protocol allows experiences that combine multiple authentication mechanisms such as fingerprint and PIN.

FIDO Universal Second Factor User Experience

The second factor experience allows online services to augment the security of their existing password infrastructure by adding a strong second factor to the user login process. The 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 second factor device across all online services, that support the protocol, via built-in support in web browsers.

GlobalPlatform and FIDO Alliance

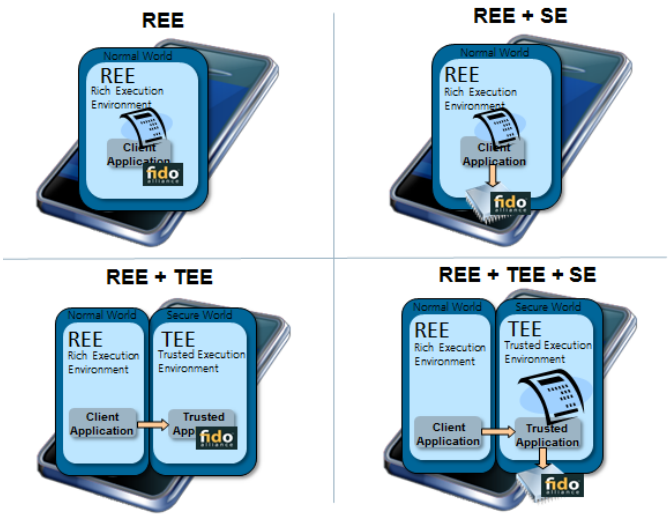
GlobalPlatform-certified TEE and SE secure components enable a variety of FIDO deployment scenarios on client-devices – like smart phones, tokens, wearables, and smart cards – and across a range of vertical markets.

The FIDO Alliance's mission to simplify and secure online authentication is supported by GlobalPlatform. To be trusted, a FIDO implementation calls for the enforcement of privacy and security requirements. This can be achieved using GlobalPlatform's proven and standardized Secure Components, as SEs and TEEs isolate applications and restrict access to authorized parties.

The two bodies are therefore working closely to align various FIDO authentication implementation scenarios with the GlobalPlatform Specifications. This will enable secure online authentication solutions by combining the functionality of the Rich Execution Environment (REE) with GlobalPlatform's standardized TEE or SE. FIDO solutions leverage this infrastructure to achieve the required security levels for a wide variety of markets, such as government-to-citizen, government-to-government, enterprise, eHealth, financial, and commercial.

Implementation Solutions by Platform

Different device manufacturers, service providers and use cases have different requirements, and FIDO Authenticators can be deployed and protected in three different ways using GlobalPlatform-certified infrastructure. This could be by combining the device's REE with a GlobalPlatform SE or TEE, or by leveraging the combined attributes of a TEE and a SE. When designing a FIDO Authenticator or FIDO solution, it is important to consider all variables presented in this paper to design the appropriate architecture.



The choice, or combination, of secure components depends on different factors like the required security level, the cost of development, integration and maintenance, and the availability of the various secure components in the devices being used (e.g. mobile devices, token devices, wearables, smart cards etc.).

It is important to remember that a single implementation solution, from the above options, will not always meet the needs of all market segments, credential types and authentications - or required security levels. GlobalPlatform enables service provides to develop their apps once and deploy everywhere across a range of implementation solutions, safe in the knowledge that FIDO Authenticators will be protected.

GlobalPlatform & FIDO – The Benefits

This collaboration brings a number of benefits to streamline and expedite implementations. From an industry perspective, the FIDO UAF and U2F Protocols can be implemented and managed more securely by using GlobalPlatform technologies. This brings benefits for the wider ecosystem, for example:

- **Tailored security -** Security levels and requirements can be tailored depending on the service provider's market requirements. For example, non-sensitive operations like customer loyalty programs can have different requirements to very sensitive operations like accessing financial transaction data. The collaboration with FIDO and the wider industry enables greater simplicity when combining security measures. For example, SE or TEE can be used on their own in a device, or then can be combined to meet the needs of a particular deployment.
- **Remote management -** FIDO Authenticator Applications (including activation, deactivation, revocation, synchronization, and deletion) can be remotely managed in the field by using the GlobalPlatform Messaging Specifications for trusted service management.
- **Utilize end-user devices -** Implementation of a FIDO U2F authenticator within a GlobalPlatform-certified TEE – which are already integrated in a range of connected devices – means that a separate authentication token is not required. U2F authenticators that do not use TEE are traditionally extra tokens or devices separate from the user's connected device.
- **Public/private key creation -** The device (not the remote server) creates a public/private key pair for each combination of user/device/relying party during registration, before sharing the public key with the relying party. Because the crypto engine of secure components is tested to ensure state of the art implementations, service providers can be sure that the credential generated by the authenticator cannot be reverse-engineered.
- **Existing tokens -** GlobalPlatform also enables FIDO authenticator reuse in already existing SEs and smart cards. For example, bank-issued credit cards, government or enterprise-issued ID cards, and operator-issued SIM cards.
- **Multiple authentication options -** Working with many different types of authenticator factors such as a fingerprint sensor, iris scanner, or via trusted PIN entry brings a range of time and cost savings.

For the business community, the ability to securely implement FIDO authentication, and remotely manage credentials, using GlobalPlatform technologies delivers greater confidence across the ecosystem due to enhanced security and cost-efficiencies, while enhancing functionality.

USE CASES

By combining FIDO-based authentication with consumer devices or tokens that are already in circulation, service providers can enable secure and convenient authentication for a wide range of different use cases. Below is a deeper dive into some of these areas.

Banking and Financial Services

Mobile finance incorporates a vast range of financial services including mobile wallets, peer-to-peer payments and contactless payments, in addition to the use of mobile devices as point-of-sale (POS) terminals. The advancement of technology is now seeing sensitive transactions like online banking and payments, and contactless payments, being performed on a range of connected devices.

The nature of these devices and types of transactions involves a higher potential for fraud, making strong authentication indispensable. As mobile and electronic finance continues to evolve, and new stakeholders engage in the market, there is a need for stronger, more standardized security to ensure that consumers can carry out any financial transaction in a safe and trusted environment.

Regulators, payment service providers, and banks around the globe must quickly adapt. Countries are already enacting regulatory frameworks for mobile and internet payments to bring greater consumer protection while ensuring competition in each unique market space. Examples are the European Banking Authority's (EBA) Final Guidelines on the Security of Internet Payments[6] and European Central Bank's (ECB) recommendations for the security of mobile payments[7], outlining the minimum internet and mobile finance security standards that online payment service providers should implement. 2018's EU Payment Services Directive 2 (PSD 2)[8] is also setting out to ensure consistent internet payments services across the EU Member States, including requirements for the secure download and transfer of security credentials as well as for strong authentication.

The FIDO Alliance has been heavily engaged in this evolution with some of the first implementations in the marketplace today[9]. Since the FIDO scheme covers both transaction signing and online authentication, it can be easily adopted by financial and banking service providers for customer login and transaction confirmation.

With its multi-application architecture, GlobalPlatform helps banks to use existing EMV smart cards as FIDO authenticators, reducing costs and eliminating the need to issue special FIDO authenticator tokens. The tamper resistant security of the SE embedded in an EMV smart card is ideal for this task since it controls interactions between trusted sources (a bank), the trusted application (a payment application) stored on the SE, and third parties (an entity the customer is making a payment to). The secure domain protects user credentials and processes the payment transaction in a trusted environment, ensuring safety of user data.

Internet of Things (IoT)

The Internet-of-Things (IoT) crosses many segments and use cases including healthcare, smart homes, industrial, automotive, and wearables.

Some key IoT trends include:

- Automobile connectivity to access online-services;
- Connected manufacturing plant equipment transferring data to a backend-system;
- Company devices connected to the internet for employees to perform job specific duties;
- Smart home connectivity to enable use cases like energy efficiency and kitchen devices placing orders at online grocery stores.

Authentication in these scenarios is essential to assure only approved devices and privileged users can access online services. Many devices require strong security due to the high risk of potential fraud. Many of these already integrate a GlobalPlatform-certified secure component as GlobalPlatform satisfies the demand for strong security and allows a seamless integration of FIDO-based authentication.

Retail

Technology is changing the way consumers interact with retailers. Customers now adopt an omnichannel approach, 'going digital' at all stages of the buying process. By enabling physical and digital retail experiences, merchants can ensure customers can perform a transaction seamlessly at any time. Retailers are also implementing technologies to create exciting customer experiences across channels by offering interaction through connected devices like wearables with beacons and inventory tracking systems[10].

These trends present challenges for retailers. Consumers typically maintain multiple accounts across a range of retailer websites, largely using username and passwords to authenticate. Remembering multiple, complex passwords is inconvenient meaning credentials often get reused. This has a huge impact on security as they can potentially be used across multiple sites should they be stolen. This represents tremendous risk and potential costs for retailers and their customers.

Retailers therefore need to implement technologies that improve security and prevent data breaches. FIDO can easily help to mitigate these risks and improve the user journey. For example, millions of devices are now equipped with a fingerprint sensor that can be easily integrated with a FIDO Authenticator to support a secure online login procedure. GlobalPlatform's TEE technology safely stores the fingerprint templates in the end-user device, limiting misuse of the user's account without the paired device[11].

Government

More and more government services now being offered online, simplifying bureaucratic procedures, improving accessibility and reducing cost. Since many public services require identity validation, many agencies demand strong, two-factor authentication to prove a user's identity. Existing implementations rely on special hardware authentication tokens, but these can be costly and complicated to scale for governments and inconvenient for end users.

FIDO UAF authentication enabled by devices integrating GlobalPlatform-certified secure components reduces cost and time to market, while increasing convenience and security for users. Additionally, more and more governments issue smart card-based national ID cards, driver's licenses, passports, or agency employee badges. With GlobalPlatform's multi-application architecture, governments can easily enable the issued cards to be used for FIDO-based authentication.

Both of these scenarios enable strong authentication without the need to issue separate, dedicated hardware tokens. Recent implementations in the United Kingdom underscore the benefits of this approach to the citizenry, government agencies, and service providers. Citizens can easily and securely access digital public services using a roster of identity providers, validated using FIDO U2F tokens before services can be accessed[12].

Mobile

Mobile devices can now manage nearly every function of or digital lives and are more widely than personal computers. To offer a measure of this market's potential, the global mobile wallet market reached $113.5 billion in 2015 and is predicted to hit $635.0 billion by 2020. That's a compound annual growth rate (CAGR) of 41.1%[13].

With multiple applications now being stored and their processes executed in end-user devices, the presence of a SE or TEE is essential to the deployment of value added services (VAS). Authentication, identification, signatures, and PIN management are all central to the deployment of VAS and all require a protected environment to operate securely. Taking a payment application as an example, it is important that the user's credentials do not become visible.

Considering the limited user interface dialogs of mobile devices, the permanent online connection and the high risk of loss or theft, strong security and more convenient login procedures are increasingly important. The combination of FIDO and GlobalPlatform perfectly satisfies this need. FIDO is standardizing the authentication scheme by considering different convenient user verification methods and GlobalPlatform defines the underlying platform technologies including APIs, protocols, and frameworks, which allow implementation of FIDO-based authentication in a secure way.

Enterprise

The security of IT systems - especially identity and access management – is crucial. With security breaches on the rise, many enterprises require two-factor authentication using tokens or smart cards (e.g. company badge) to access enterprise servers. Traditionally, however, these systems rely on certificate-based public key infrastructure (PKI) systems which are often too complex and costly for small and medium size companies.

Additionally, mobile devices are increasingly common in enterprise environments and companies are struggling to securely integrate them into their infrastructure. The usage of authentication tokens or cards with mobile devices (for example, reading a company badge with a smartphone) is also cumbersome and loading a derived credential in the smartphone may be more efficient.

Combining FIDO and GlobalPlatform technologies can achieve this. FIDO-based authentication does not rely on a PKI infrastructure and therefore represents a realistic alternative for enterprises of all sizes. The FIDO UAF strong authentication framework can also combine authentication with biometric user verification. GlobalPlatform-certified TEEs are already available on many mobile devices, allowing the implementation of FIDO UAF without the need to deploy additional hardware.

Taking Google as an example, it is combining existing GlobalPlatform-certified tokens with FIDO U2F authentication for its employees. To ensure unauthorized users cannot log into an account, login must be performed with a physical FIDO U2F authenticator in parallel with a username and password.[14]

CONCLUSION

Device manufacturers and service providers have many decisions to make when integrating FIDO-based authentication to enable strong and convenient authentication for users. Importantly, they need to define what type and level of security is needed to decide which combination of REE and secure components will best fulfill their needs.

This paper has demonstrated the value of GlobalPlatform-certified secure components for the secure deployment of FIDO-based authentication. It is the combination of these technologies that enables users to quickly, conveniently and, importantly, securely authenticate themselves to access their digital services.

Using this infrastructure, service providers can develop their service once, deploy everywhere, and support all use cases. By utilizing existing devices and tokens, service providers can also save money and time, while enabling a more convenient and secure service.

The collaboration between GlobalPlatform and FIDO Alliance gives device manufacturers a stable solution. Implementation of a GlobalPlatform-compliant secure component smooths the path for FIDO-based authentication, and enables them to promote their equipment meets the needs of the marketplace.

For consumers, FIDO provides strong security with a superior user experience, all while protecting their privacy. It eliminates the need to remember many passwords while providing a higher level of security. All of this makes it possible for new services, that were previously hampered by lack of sufficient security, to be confidently brought to mobile devices.

GlobalPlatform's collaboration with FIDO continues, working to offer even more value to service providers and the wider industry. If you would like to contribute to this work effort, or have any questions or feedback, please contact the GlobalPlatform Secretariat: secretariat@globalplatform.org.

CONTRIBUTORS & ACKNOWLEDGEMENTS

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

About the GlobalPlatform Identity Task Force

The GlobalPlatform Identity Task Force (ITF) was established in 2015 to identify and address the identity use cases that can be supported by GlobalPlatform technologies, including and specifically encompassing privacy.

The scope of activities encompasses:

- Government Identity – to continue GlobalPlatform's role in addressing the long-term needs of governments engaged in large-scale ID and e-ID deployments for both government-to-employee and government-to-citizen applications. This role, formerly undertaken by the Government Task Force (GTF), has been integrated into the ITF. More details about the GTF are highlighted below.
- Enterprise Identity – to determine GlobalPlatform's role in addressing the long-term needs of enterprises in e-ID deployments for their employees, both when the identity is issued directly by the enterprise or it is hosted on an employee device, as in bring your own device (BYOD).
- Consumer Identity – to determine GlobalPlatform's role in addressing the long-term needs of consumer identity to consumer services, with respect to consumer centric e-ID models or bring your own credential (BYOC) models.

Contributors include the following:

GlobalPlatform Members

Alexander Summerer – Giesecke & Devrient

GlobalPlatform Team

Lori Allen – Alliances Management

Meagan Karlsson – Alliances Management

Rob Peryer – iseepr

For more on GlobalPlatform, please visit www.globalplatform.org or contact us at secretariat@globalplatform.org.

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

REFERENCES

1 United States Census Bureau world population international database: http://www.census.gov/popclock/

2 There are officially more mobile devices than people in the world: http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

3 GlobalPlatform Technology Deployed on 22 Billion Secure Elements: https://www.globalplatform.org/mediapressview.asp?id=1315

4 Currently, more than a billion processors that can support TEE are shipped worldwide per quarter: https://www.globalplatform.org/mediapressview.asp?id=1320

5 FIDO Standards: https://fidoalliance.org/approach-vision/

6 EBA: FINAL GUIDELINES ON THE SECURITY OF INTERNET PAYMENTS: https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29_Rev1

7 ECB: RECOMMENDATIONS FOR THE SECURITY OF MOBILE PAYMENTS (DRAFT): http://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf

8 EBA seeks input on strong customer authentication and secure communication under PSD2: https://www.eba.europa.eu/-/eba-seeks-input-on-strong-customer-authentication-and-secure-communication-under-psd2

9 Mobile World Congress: Forget Your Passwords – Samsung Galaxy S5: https://www.paypal.com/stories/uk/mobile-world-congress-forget-your-passwords-samsung-galaxy-s5-

10 How Beacons Can Reshape Retail Marketing: www.thinkwithgoogle.com: https://www.thinkwithgoogle.com/articles/retail-marketing-beacon-technology.html

11 Cyber crooks hack into Amazon accounts to place pricey orders and steal the goods: http://www.mirror.co.uk/news/uk-news/cyber-crooks-hack-amazon-accounts-8528512

12 UK Becomes the First Government to Offer Secure Online Identities Based on FIDO U2F Standards: http://www.benzinga.com/pressreleases/16/03/m7748597/uk-becomes-the-first-government-to-offer-secure-online-identities-based#ixzz43jhgyL1d

13 Mobile Wallet and Payment Technologies: Global Markets: http://www.researchandmarkets.com/reports/3774272/mobile-wallet-and-payment-technologies-global#rela7

14 Google evaluates FIDO authentication: http://sdtimes.com/google-evaluates-fido-authentication/.