WHITE PAPER
Smart Card Alliance

A SMART CARD ALLIANCE IDENTITY COUNCIL

WHITE PAPER

Smart Card Technology and the FIDO Protocols

Publication Date: April 2016
Publication Number: IDC-16001

Smart Card Alliance

191 Clarksville Rd.
Princeton Junction, NJ 08550

www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information, please visit http://www.smartcardalliance.org.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report. This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.

Table of Contents

1 Introduction

The Fast IDentity Online (FIDO) Alliance has attracted more than 250 members with a vision for simple, secure online user authentication. Leaders from multiple industry segments are working together to create an interoperable environment in which users can access online services through web sites and mobile device apps with a high degree of security but without compromising usability. To this end, the FIDO Alliance has established foundation principles on which to base specifications for authentication protocols. Allowance is made for interoperable products from multiple vendors that implement different technologies.

This white paper was developed by the Smart Card Alliance to describe the role of smart card technology in enhancing the security of FIDO implementations. The white paper includes the following content:

- An overview of the FIDO principles and protocols
- A description of the security benefits of using smart card technology in FIDO protocol implementations
- Examples of use cases currently implementing the FIDO protocols with smart card technology

It is important to note that the white paper focuses on the identity authentication process. While the identity life cycle also includes identity management and proofing processes, these are not covered.

While smart cards are typically used for strongly proofed identity, smart card technology can also be used with the FIDO protocols and enable the highest level of token assurance and trust. The FIDO protocols can be implemented using smart card technology and provide anonymity. It is up to the relying party to define the level of trust and token assurance required.

2 Secure Online Authentication Overview

The de facto standard for online authentication is the use of user names and passwords, implemented through the web form capability that is supported by all web servers and browsers. However, password-only authentication is susceptible to a wide range of attacks. To mitigate some of these attacks, users must use a different password for every web site, which can rapidly become a burden. Historically, in order to improve security, stricter rules must be imposed, adding friction or inconvenience for the user. It is an unfortunate fact that for both enterprise (employee) and public (consumer) authentication convenience has been the goal, while security has been an afterthought.

A number of different technologies are available to improve security:

- SSL/TLS client certificates
- Multi-factor authentication (e.g., one-time passwords (OTPs), public key infrastructure (PKI), smart cards)
- Out-of-band authentication
- Trusted Platform Module (TPM)
- Embedded security (e.g., Trusted Execution Environment (TEE), trusted enclave, embedded secure element)

Individual vendors have created solutions to improve the user experience and enhance security. But without standards, those solutions only work with certain devices and specific web sites.

FIDO addresses these issues with a simple enrollment protocol and a highly secure authentication protocol. The FIDO specifications promote principles of good design to improve the user experience. The devices used to implement a FIDO solution are manufactured by different vendors; therefore, the user experience and security level achieved vary by device.

The Smart Card Alliance promotes the benefits of smart card technology for a variety of market segments. Smart card technology is used globally for secure payments in the retail and transit markets and for healthcare, employee, and citizen identity applications. Use of smart cards for online authentication has been most successful in segments with strong standardization, such as the U.S. government (e.g., the Personal Identity Verification (PIV) card and Common Access Card (CAC)). Implementing the FIDO protocols with smart card technology can strengthen the security of the identity authentication process and bring the benefits of smart card technology to a wider audience.

3 FIDO Overview

The mission of the FIDO Alliance is to change the online authentication process, making it both more secure and more user friendly. Specific goals are:

- Develop technical specifications that define an open, scalable, interoperable set of mechanisms to reduce the reliance of the online authentication process on passwords
- Operate industry programs to help ensure worldwide adoption of these specifications
- Obtain formal standardization for these specifications

3.1 Principles

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

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

The protocols rely on strong cryptographic techniques to authenticate a user device to online services. Secrets are stored only on that device and are never exposed to the cloud. This design principle is the cornerstone of the FIDO protocols, Universal Second Factor (U2F) and Universal Authentication Framework (UAF) (described in Sections 3.3.3 and 3.3.4). Both protocols improve security while providing satisfactory usability. U2F strengthens password authentication by adding a requirement for a simple-to-use token, the presence of which constitutes a second authentication factor. UAF can eliminate the password requirement by using biometrics or another authentication factor to authenticate the user to the local device. That same authenticator can be used across multiple online services.

The FIDO specifications also include several requirements that put user friendliness in focus, without jeopardizing user privacy. Unique site-specific credentials authenticate each user to each individual web site, thus preventing tracking a user across online services. The architecture is designed in a way that user's passwords, biometrics or private keys are securely kept in the user's device. Figure 1 illustrates the FIDO protocol principles.

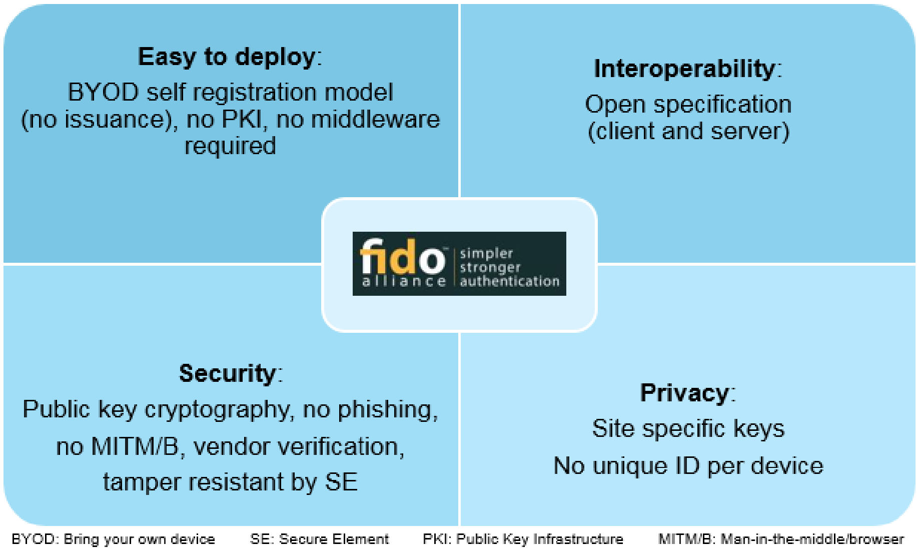
Easy to deploy:
BYOD self registration model
(no issuance), no PKI, no middleware required
Interoperability:
Open specification
(client and server)
fido alliance
simpler
stronger
authentication
Security:
Public key cryptography, no phishing,
no MITM/B, vendor verification,
tamper resistant by SE
Privacy:
Site specific keys
No unique ID per device
BYOD: Bring your own device
SE: Secure Element
PKI: Public Key Infrastructure
MITM/B: Man-in-the-middle/browser

Figure 1. FIDO Protocol Principles

3.2 Cryptography

The FIDO protocols are based on the techniques of standard public key cryptography but do not require a public key infrastructure (PKI). No certificate authorities or complex policies are required.

The protocols (described in Section 3.3) rely on a FIDO *authenticator,* which is a hardware or software appliance possessed by the user of the online service. When a user registers the FIDO authenticator with a new web site (see section 3.3.1), the authenticator generates a unique key pair for that specific web site. The public key is stored on the web site; the private key, or data sufficient to derive the private key, is stored on the FIDO authenticator. Each key pair is unique and specific to the URL of that particular web site.

Every FIDO authenticator needs to secure key pair generation, allow secure storage of the private keys, provide a random number generator, and support a cryptographic engine that can use those keys to create a unique digital signature that the web site can authenticate, using the public key previously associated with that FIDO authenticator.

3.3 Specifications

The FIDO Alliance has created specifications for two protocols: the U2F protocol and the UAF protocol (see Figure 2). Both use the standard public key cryptography techniques described in Section 3.2 and are based on the common FIDO design principles described in Section 3.1.

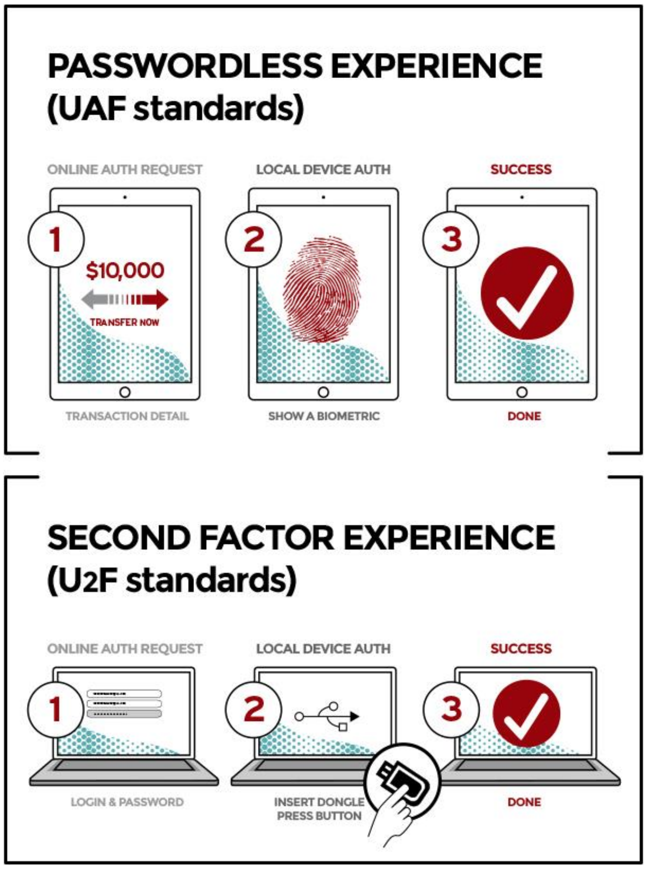

Figure 2. UAF and U2F Experience

The FIDO Alliance published the two version 1.0 specifications in December 2014. The UAF and U2F Technology Working Groups remain active; their mission is to "develop the FIDO Technology Specifications necessary to create and ensure the viability and widespread interoperability of the authentication security ecosystem between devices, clients and servers."

U2F and UAF were developed in parallel and are specified separately in the final 1.0 specifications. The two protocols are expected to be developed further and harmonized in the future. With FIDO 1.0 specifications published, FIDO has authorized the formation of a new technology working group. The mission of the new FIDO 2.0 Specification Technology Working Group is to consider future requirements, and to ensure widespread interoperability within the authentication ecosystem among devices, clients, and servers.[1]

The protocols rely on a FIDO authenticator and have two main phases: registration and authentication.

[1] FIDO 2.0 Technology Working Group as referenced online at https://fidoalliance.org/working-groups/

3.3.1 Registration

Registration is the initial set-up, which occurs once for each online service the user wants to use. During registration, the user's FIDO authenticator creates a new key pair. It retains the private key and submits the public key for registering by the online service. Prior to registration, the user is verified by the online service according to that site's requirements, such as a user ID and password. Identity and verification are determined by and are the responsibility of the relying party and are not part of the FIDO protocol. The FIDO authenticator registration process follows these steps (see Figure 3)[2]:

1. The user is prompted to choose a FIDO authenticator from the list of authenticators that match the online service's acceptance policy.
2. The user unlocks the FIDO authenticator using a fingerprint reader, a button on a second-factor device, securely-entered PIN or other method.
3. The user's device creates a new public-private key pair that is unique for the local device, the online service, and the user's account.
4. The public key is sent to the online service and associated with the user's account. The private key and any information about the local authentication method (such as biometric measurements or templates) never leave the local device.

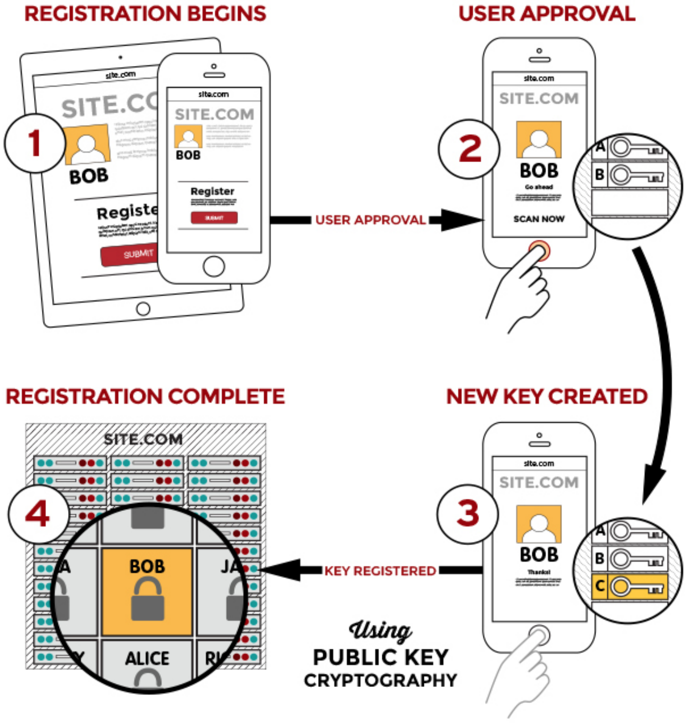

Figure 3. FIDO Registration Process

[2] The registration steps are from: "Specifications Overview," FIDO Alliance web site, https://fidoalliance.org/specifications/overview/.

3.3.2 Authentication

Authentication is performed by the user's FIDO authenticator and proves possession of the private key to the online service. To perform authentication, the online service prompts the device to sign a challenge. The authentication process follows these steps (see Figure 4)[3]:

1. The online service challenges the user to log in with a previously registered FIDO device that matches the service's acceptance policy.
2. The user unlocks the FIDO authenticator using the same method used at registration (Step 2 in the registration process).
3. The device uses the user's account identifier provided by the online service (Step 4 in the registration process) to select the correct key and signs the challenge received from the service.
4. The client device sends the signed challenge back to the service, which verifies it with the stored public key and logs the user in.

This authentication process takes place any time the online service wants to authenticate the user.

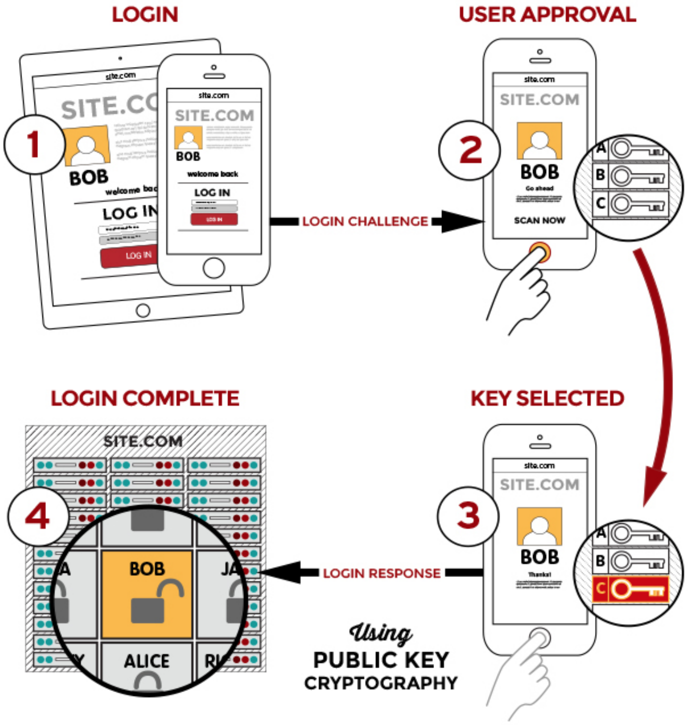

Figure 4. FIDO Authentication Process

[3] The authentication steps are from: "Specifications Overview," FIDO Alliance web site, https://fidoalliance.org/specifications/overview/.

3.3.3 U2F Protocol

The U2F protocol allows online services to augment the security of their existing password infrastructure by requiring a physical token, called an authenticator. The authenticator provides a strong second user authentication factor to augment user login. In a U2F deployment, the user logs in to an online service as usual, with an established credential. When prompted, the user presents a U2F token and "unlocks" it. At the moment three interface types are specified in FIDO U2F. Universal Serial Bus (USB) was the first, followed by Near Field Communication (NFC) and Bluetooth (Classic and Smart aka Low Energy (BLE)). Unlocking is a test of user physical presence and requires a token-specific gesture, such as pushing a button on a USB device, tapping a U2F device to an NFC-enabled device such as a mobile phone or tablet, or pressing a button on a BLE-enabled token or fob. The user can use the same FIDO U2F device[4] on all online services that support the protocol.

3.3.4 UAF Protocol

The UAF protocol authenticates a user locally, before the local device used to access the online service authenticates itself to the server. No user password is required.

The FIDO authenticator authenticates the user using a PIN, biometric factor (e.g., face, voice, iris, fingerprint recognition), or similar data before proving presence to the online services. The PIN or biometric data should be securely stored, thereby preventing these credentials from leaving the device. FIDO specifications define a common interface for whatever local authentication method the user exercises.

3.3.5 FIDO Protocol Implementation and Security

The FIDO protocols described are based on strong cryptography and provide a high security level. However, this is of limited benefit if the actual implementations of these protocols do not provide the corresponding assurance. The following properties should be ensured:

- The cryptographic keys should be securely generated, stored and used. Any recovery or modification by an attacker would potentially allow impersonation of the user.
- The random number generator should be secure, meaning that its outputs are cryptographically strong and unpredictable. The random number generator is used in key generation and signatures and the strength of this security mechanism relies on its quality.
- All data used for the local user authentication (e.g., PIN, biometric data) should be securely stored. Any disclosure or modification would allow impersonation of the user or constitute a privacy breach.

The importance of these properties is underlined by the FIDO Alliance in the document, "FIDO Security Reference,"[5] which provides an analysis of the security goals and the threats to the FIDO authenticator. As will be discussed in the following sections, smart card technology is the most capable of providing the highest level of security for FIDO implementations.

[4] A U2F device could be a USB device, a card, or other physical object.

[5] https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-security-ref-v1.0-ps-20141208.html

3.4 Levels of Authentication

The U.S. Office of Management and Budget (OMB) guidance, “E-Authentication Guidance for Federal Agencies,” [OMB M-04-04][6] establishes and describes four levels of identity assurance for electronic transactions requiring authentication. These levels, Levels 1 thru 4, are described in terms of consequences of authentication errors and misuse of credentials. Level 1 is the lowest assurance level and Level 4 is the highest.

It is important to note that current government systems do not separate functions related to identity proofing during the registration process from the credential issuance process. The defined guidance for all levels of assurance is described in terms of identity proofing and registration of applicants, tokens for authentication, and their inherent strength relative to a prescribed level, token and credential management, protocols, and assertion mechanisms. FIDO neither prescribes nor relies on all of these terms.

In the simplest of terms, FIDO delivers strong token assurance but does not address the notion of identity assurance at all. It becomes incumbent upon the relying party to determine if an identity association with the FIDO token makes sense and is reasonable to establish. FIDO in itself provides a strong token assurance model, enabling relying parties to trust that the token being utilized in a transaction is the same token that was used in a separate and previous transaction.

Traditionally, a smart card token (i.e., a Level 4 token as defined by OMB) requires a stringent identity proofing process (among other considerations) in order to be issued to an individual. This is an expensive and infrastructure-intense undertaking. FIDO, by separating identity assurance from token assurance, can offer token assurance to help protect transactions in ways previously not available to the general public; implementing FIDO protocols with smart card technology provides the highest level of token assurance.

3.5 Smart Card Technology in FIDO

The smart card chip or embedded secure element contains a secure microprocessor, working RAM, nonvolatile memory, and (typically) a crypto-coprocessor. The memory and processors are protected physically, using a variety of software and hardware security technologies. The processor includes either a single external input/output (I/O) interface or, in the case of a dual-interface contact-contactless chip, two separate interfaces, that are controlled by the processor. Vendors creating FIDO authenticators can either include a second processor to manage I/O and control user input and output on the device or provide a single-chip solution that combines both functionalities. When the FIDO authenticator is implemented within an embedded secure element (eSE), it takes advantage of the smart card security features as well providing a secure environment to host other security-critical applications like payment or transport.

Implementing FIDO using smart card technology and hardware-based security brings the following security benefits:

- Generates keys using true random number generators

[6] https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

- Protects keys
- Generates cryptographic signatures
- Provides tamper-resistant hardware security
- Prevents cloning and counterfeiting
- Enables multiple form factors (e.g., card, USB devices, mobile device secure element, microSD, wearables)
- Leverages device manufacturers' security certifications
- Provides the highest level of security available to protect FIDO-related credentials and biometrics

Running the software that implements the FIDO protocols on the processor in a smart card chip or embedded secure element physically isolates the software from the device hosting the browser, allowing the software to execute securely. Both code and data are encrypted. In addition, they are protected by the layers of hardware in the chip and module packaging. An attacker must first obtain the device and then implement a difficult, time-consuming, and expensive attack to have any chance of accessing the device holder's private keys. Even if an attacker succeeds with one device, the same sequence will not be successful on a different device so the attack is not scalable.

3.5.1 Smart Card Cryptographic Operations

Every FIDO authenticator needs to be able to generate key pairs securely and store private keys, and must include a cryptographic engine that includes a random number generator and that can operate on the stored keys. FIDO authenticators generate public key pairs for each web site with which they communicate. Key generation places a high load on computing resources, especially in the case of general purpose CPUs. Smart card technology is purpose-built to perform key pair generation quickly, with low power consumption. Because smart card technology uses a secure element, key pair generation is performed securely and is efficiently protected, even from advanced attacks. Smart card technology protects private keys in hardware with interaction restricted to a limited set of commands and responses.

3.5.2 Security Evaluations

Security is a core element of any authentication application, and it must achieve the level required to address anticipated risks and threats. Smart card technology is a critical element in secure system design, providing trusted security.

The smart card industry uses established standardized security evaluation and certification programs. These programs use a small number of trusted third party labs to identify threats and verify that they can be prevented up to a defined level. Product evaluation and certification allow issuers to be confident that a product meets the expected security requirements.

Several methods are available to certify and evaluate smart cards. Two standardized approaches are Federal Information Processing Standard 140 (FIPS 140) and the Common Criteria for Information

Technology Security Evaluation (CC).[7] FIPS 140 specifies the requirements for cryptographic modules used by departments and agencies of the U.S. Federal Government. It defines four levels of security that require increasing security features. CC is an internationally approved security evaluation framework (ISO/IEC 15408) currently recognized by 25 countries. CC specifies an evaluation assurance level (EAL) that indicates how thoroughly security was reviewed and tested. Levels range from EAL1 (functionally tested) to EAL7 (formally verified design and tested). CC testing allows customers in any of the approving countries to purchase products with confidence in their security to the assigned level.

The smart card industry produces hundreds of certified products each year. Using secure smart card technology for FIDO implementations provides additional security benefits as a result of these processes.

3.5.3 User Experience

Smart card technology enables small, light, lower power devices with very fast response times to enable a positive user experience. This provides an ability to do strong authentication over a wide range of use cases without the well-known problems associated with username and password. By making strong cryptography widely available, smart card technology in the FIDO use case creates a better online world for all of its users. It also enables a wide range of manufacturers to implement these solutions and promotes competition and user choice as a result. It can also be combined easily with many existing commercially available devices and other authentication technologies to further enhance user choice and online security.

3.5.4 Use Cases

Companies participating in the FIDO Alliance come from various industries and bring the variety of FIDO implementations necessary to enable standard adoption by the general public.

For password-less experience using UAF, a software-based client and server are required. UAF authenticators may take different forms. Implementations may range from a secure application running inside tamper-resistant hardware to software-only solutions on consumer devices

For the second factor experience using U2F, the user presents the second factor – which has various interpretations and implementations, both on the server and on the authenticator sides.

The FIDO Alliance launched a certification program in 2015 that measures compliance to the FIDO specifications and ensures interoperability among products and services that support FIDO specifications. Products that pass the tests can use the “FIDO Certified™” logo. As of January 2016, 108 products completed the program and are “FIDO Certified.”[8] The FIDO Certified program replaced the “FIDO Ready™” program, which tested compliance to draft specifications.

This section describes examples of use cases that implement the FIDO U2F or UAF protocols and incorporate smart card technology. Other use cases can be found from among other participants in the FIDO effort.

[7] For more information on Common Criteria, see https://www.commoncriteriaportal.org/.

[8] The FIDO Certified product list is available at https://fidoalliance.org/certification/fido-certified/. The FIDO Certified program replaced the “FIDO Ready” program.

3.5.4.1 Yubico/Google

The Yubico U2F-only Security Key and multi-technology Yubikey NEO both support the FIDO U2F protocol and incorporate smart card technology. "Each Security Key has an individualized secure chip which performs cryptographic functions triggered by a simple touch of the key. The FIDO U2F Security Key provides a unique public and private key pair for each application it protects. The secure smart card chip is of the same class as those used in SIM cards, electronic passports, military electronic IDs and chip-and-PIN credit cards. Like those devices, the chip is specially "hardened" so it's extremely difficult to steal the secrets hidden inside. The secrets contained in the Security Key belong to the end-user exclusively and are never transferred, copied or stored by a service provider or any other application provider."[9]

The YubiKey NEO device[10] from Yubico supports multiple authentication protocols including the FIDO Alliance U2F protocol, one-time password, and smart card functionality (e.g., OpenPGP, the Federal government's Personal Identity Verification (PIV) credential). The device supports both contact (USB) and contactless (NFC and MIFARE) interfaces. The device is commercially available and can be used for U2F login with online services that support U2F (e.g., Gmail, GitHub and Dropbox). The device uses Common Criteria-certified smart card technology-based hardware secure elements[11] to protect encryption keys.

In October 2014, Google Chrome became the first web browser to support the FIDO U2F protocol. Google also announced that they were supporting the Yubico U2F-compliant Security Key as a second factor device to strengthen the Google 2-Step Verification process for Google accounts.[12]

3.5.4.2 NXP Example

NXP supports the FIDO ecosystem with both U2F and UAF reference designs based on NXP's proven security architecture. NXP has participated in the FIDO interoperability testing program and several products carry the FIDO Certified™ logo.

NXP has several reference designs supporting the FIDO Alliance U2F authentication protocol. The A7 USB/NFC reference design is a USB/NFC token that enables the fast design of a U2F authenticator and is based on the proven A7 secure element integrated circuit (IC) with contact and contactless (ISO/IEC 14443) interface. Both interfaces (USB and NFC) have been certified according to the FIDO Certified™ program. This smart card microcontroller provides the cryptographic engines, secure true random number generator and tamper-resistant storage to allow strong authentication with any FIDO U2F server. It can be used as a USB key or as a contactless fob or wearable with any NFC-enabled mobile device. There are several A7-based USB and NFC key designs in mass production and used in the FIDO ecosystem.

[9] "FIDO U2F Security Key," Yubico web site, https://www.yubico.com/products/yubikey-hardware/fido-u2f-security-key/

[10] "Yubico NEO," Yubico web site, https://www.yubico.com/products/yubikey-hardware/yubikey-neo/

[11] "Smartcard Features on the Yubikey NEO," LWN.net, Nov. 5, 2014, http://lwn.net/Articles/618888/

[12] "Google Launches Security Key, World's First Deployment of Fast Identity Online Universal Second Factor (FIDO U2F) Authentication," FIDO Alliance press release, Oct. 21, 2014, https://fidoalliance.org/google-launches-security-key-worlds-first-deployment-of-fast-identity-online-universal-second-factor-fido-u2f-authentication/

The BLE reference design is based on the same A7 secure element in combination with NXP's Ultra Low Power BLE System-on-Chip Solution, allowing the creation of authenticators that can communicate with any BLE-enabled device.

The embedded secure element PN65O reference design supports the FIDO Alliance UAF authentication protocol. This type of secure element is widely used on mobile platforms and provides a similar set of security features as well as full NFC capability. This allows the integration of hardware-based FIDO UAF applications on any computing platform.[13]

3.5.4.3 Infineon Example

With the SLE78 family of products, Infineon supports all hardware-based authenticators for FIDO regardless of the interface. This can be a U2F token with USB, NFC, Bluetooth, audio jack interface or a combination of these; or UAF, with its embedded secure element and TPM (Trusted Platform Module). Infineon is currently featuring several FIDO reference designs.

Until today, U2F FIDO Certified™ specifications were defined only for USB solutions, and Infineon was one of the first to achieve FIDO certification for its USB token prototype. The token is based on a single-chip USB security controller from Infineon's SLE78 family, which is used in both contact and contactless security applications such as identity documents, passports, healthcare cards, and driver's licenses. In addition to a secure USB microcontroller, the SLE78 chip provides NFC capabilities, with additional input and output lines, allowing for combined solutions – a token that can interact both with a PC (through a USB port) and a hand-held device (through NFC, BLE, or an audio jack). The USB token alone and in combination with NFC is already being sold by Infineon's partners and deployed by end users for the available FIDO services.

BLE and NFC are interfaces targeting authentication solutions for handheld devices. Infineon offers two reference designs, one for each interface, that are also based on the SLE78 family.

The microSD solution is a hybrid solution, which can support both UAF (as a secure element in a handheld device) and U2F (as a microSD removable device, which could be transferred to a different terminal). Together with partners, Infineon has received the FIDO Ready label, and has made the products available on the market.

The UAF implementation with its TPM (SLB9660 chip) received the FIDO Ready™ label last year and is already deployed in various laptops and PCs[14].

3.5.4.4 Morpho (Safran)[15]

The Morpho secure element (SE) based FIDO authenticator is a UAF roaming authenticator that leverages the use of a smart card for the storage of the user's private keys. For each relying party, the cryptographic key pair is generated inside the secure element (i.e., using on-board key generation) and only the public key is sent to the FIDO server. Access to the user's private key for authentication requires matching the user's face against a template stored in the smart card. The user's secret/private key remains under the user's exclusive control and can be neither copied nor transferred.

[13] Information provided by NXP Semiconductors: http://www.nxp.com/applications/cyber-security/cloud-security.html.

[14] For more information, please refer to http://www.infineon.com/cms/en/product/promopages/about-fido/.

[15] Information provided by Morpho.

The Morpho authenticator works with different secure elements such as an eID card, an embedded secure element (eSE), or a SIM. In addition to the security it provides, the SE-based roaming authenticator is particularly interesting because it can be used across different devices when the SE is in a removable or external form factor. The user can utilize the same FIDO authenticator with all their contact and contactless or NFC devices.

The combination of the biometric match on card (MOC) and the generation and storage of the FIDO private keys in the smart card preserves the user's privacy and makes it extremely difficult for an attacker to steal the user's secret.

For users that interact with multiple relying parties, the Morpho authenticator implements the FIDO key handle mechanism. In this case, a master key stored in the secure element is used to protect the user's private keys.

3.5.4.5 Gemalto[16]

Gemalto completed certification for a FIDO UAF authenticator on a secure element in December 2015. The secure element implementation provides secure storage for cryptographic keys and biometrics. This implementation integrates the UAF protocol into the secure mobile infrastructure.

3.5.4.6 Oberthur Technologies[17]

Oberthur Technologies FIDO UAF implementation is based on secure elements. Leveraging both secure storage and secure cryptographic capabilities, the FIDO UAF authenticator provides end user state-of-the-art security with the convenience of using a single device to connect to all of their cloud-based services.

In addition to biometrics, Oberthur Technologies brings all the necessary features to enable FIDO UAF on multiple form factors, while keeping the security level of the solution as high as possible.

[16] Information provided by Gemalto.
[17] Information provided by Oberthur Technologies.

4 Conclusions

The FIDO Alliance has tackled a crucial problem in the online world: to promote the use of strong multi-factor authentication as an alternative to usernames and passwords. The collaborative cross-industry effort has succeeded in publishing important specifications for a standardized solution that is now being implemented by multiple stakeholders. This work is foundational for achieving a trusted online environment for both end users and online service providers.

The use of smart card technology in FIDO protocol implementations is integral to achieving the FIDO Alliance goals for broad use of the protocol to provide simple, secure online user authentication. Smart card technology provides tamper-resistant hardware security to store and protect keys and generate cryptographic signatures or hashes. Smart card technology is widely available in a variety of form factors from multiple vendors, providing a cost-effective, easy-to-use device for FIDO U2F implementations and enabling hardware-based security for FIDO UAF implementations using mobile devices. Smart card technology is in use globally, providing security for identity, access and payment applications, and is a foundational technology for providing an easy-to-use and secure user device. While smart card technology is typically used for strongly proofed identity, it can also be used to support anonymity with the FIDO protocol.

Broad implementation and use of the FIDO protocol have the potential to solve one of today's most troubling problems – authenticating users to online services using a cryptographically sound protocol. It also has the potential to drive increased adoption of smart card technology for authentication, providing an easy-to-use, browser-friendly implementation that leverages the security of smart card technology built into the end user's device. Multiple vendors are now offering FIDO-compliant devices that use smart card technology, enabling relying parties to have a high degree of trust in the FIDO token.

The combination of smart card technology and FIDO protocol implementation is a critical piece of the puzzle to make the online world more trusted. The Smart Card Alliance is a strong supporter of the FIDO effort. Many members are active in both the FIDO Alliance and the Smart Card Alliance and increasingly support many of the same users. This white paper describes how smart card technology is integral to the FIDO effort and how the advancement of the FIDO protocols and smart card technology together will bring a wide range of benefits.

5 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Identity Council to describe the role of smart card technology in implementations of the FIDO protocols.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank Council members for their contributions. Participants involved in the development of this white paper included: CertiPath; CH2M; Deloitte and Touche LLP; Gemalto; Identiv; IDmachines; Infineon Technologies; Initiative for Open Authentication (OATH); Morpho (Safran); NXP Semiconductors; Oberthur Technologies; SAIC; SureID, Inc.; XTec, Inc.

The Smart Card Alliance thanks Council members who participated in the project team to write and review the document, including:

- **Abrar Ahmed**, SureID, Inc.
- **Philip Andreae**, Oberthur Technologies
- **Don Campbell**, Sure ID Inc.
- **Peter Cattaneo**, Identiv
- **Fabien Cordier**, Oberthur Technologies
- **Sal D'Agostino**, IDmachines
- **Virginie Galindo**, FIDO Alliance
- **Emmanuelle Dottax**, Oberthur Technologies
- **Steve Howard**, CertiPath
- **Bryan Ichikawa**, Smart Card Alliance
- **Don Malloy**, OATH
- **Cathy Medich**, Smart Card Alliance
- **Gary Moore**, XTec, Inc.
- **Michael Poitner**, NXP Semiconductors
- **Jenya Rivkin**, Infineon Technologies
- **Chadrick Sine**, SAIC
- **Brian Stein**, CH2M
- **Mike Strock**, Smart Card Alliance
- **Nicholas Vondrak**, Morpho (Safran)

The Smart Alliance thanks the FIDO Alliance for their review of the white paper and for their permission to use the graphics in Figures 1-6.

Trademark Notice

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

About the Smart Card Alliance Identity Council

The Identity Council is focused on promoting best policies and practices concerning person and machine identity, including strong authentication and the appropriate authorization across different use cases. Through its activities the Council encourages the use of digital identities that provide strong authentication across assurance environments through smart credentials – e.g., smart ID cards, mobile devices, enhanced driver's licenses, and other tokens. The Council furthermore encourages the use of smart credentials, secure network protocols and cryptographic standards in support of digital identities and strong authentication on the Internet.

The Council addresses the challenges of securing identity and develops guidance for organizations so that they can realize the benefits that secure identity delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to address the challenges of securing identity information for proper use.