x.509 FIDO UAF Authentication

Queralt Inc

This white paper describes how the combination of FIDO (Fast Identity Online) Universal Authentication Framework (UAF) specification and Public Key Infrastructure (PKI) makes it possible to enable strong authentication and ID verification while providing a private and frictionless mobile user experience.

Information in this white paper is based on research funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T) under contract number D15PC00001. Any opinions contained herein are those of the performer and do not necessarily reflect those of DHS S&T.

x.509 FIDO Authenticator

Integrating Trusted Identification Verification into the FIDO Authentication Process

Abstract

This white paper describes how the combination of FIDO (Fast Identity Online) Universal Authentication Framework (UAF) specification and Public Key Infrastructure (PKI) makes it possible to enable strong authentication and ID verification while providing a private and frictionless mobile user experience.

The development of the FIDO x.509 Authenticator was partially funded by the United States Department of Homeland Security's Science and Technology Directorate under contract #D15PC00001 titled "The Mobile Authentication Interoperability for Digital Certificates (MAIDC)". The project was focused on a Government use case scenario that extends the use of PIV (Personal Identity Verification) and PIV-I credentials into mobile devices. The objective was to deliver a capability conforming to both the PKI and FIDO specifications to ensure that a derived credential on a mobile device can be utilized in either government or private enterprises.

The objective was achieved by developing a middleware application that links the strong proof of identity provided by the PKI process and derived credentials with a convenient user authentication mechanism that is open, interoperable, scalable and commercially acceptable according to the FIDO UAF protocol.

Background

Identity

Personal Identity Verification (PIV)

A personal identity verification (PIV) card is a United States federal smart card that contains the necessary data for the cardholder to be granted access to Federal facilities and information systems and assures appropriate levels of security for all applicable federal applications. The PIV card was developed to satisfy the requirements of HSPD (Homeland Security Policy Directive) 12, which requires a common identification standard for all Federal employees and contractors and is based on the PKI standard.

Derived PIV Credentials (DPC)

In December of 2014, the National Institute for Standards and Technology (NIST) released Special Publication 800-157, Guidelines for Derived Personal Identity Verification (DPC)

Credentials.[1] NIST was responding to and anticipating the need for using PIV credentials in conjunction with mobile devices, such as smartphones and tablets. NIST SP 800-157 "provides an alternative to the PIV Card in cases in which it would be impractical to use the PIV Card. Instead of the PIV Card, SP 800-157 provides an alternative token, which can be implemented and deployed directly with mobile devices (such as smart phones and tablets). The PIV credential associated with this alternative token is called a Derived PIV Credential (DPC)."[2]

A Derived PIV Credential can be defined as an X.509 Derived PIV Authentication certificate, where the PIV Authentication certificate on the Applicant's PIV Card serves as the original credential.

Public Key Infrastructure (PKI)

The hierarchical infrastructure for managing and authenticating these identities is known as PKI[3], a public key infrastructure, comprised of a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

PKI, while secure, has presented a number of challenges and shortcomings in implementation and deployment, hindering adoption of PIV based authentication and the number of applications that are PKI-enabled.

Developments Made in Authentication

FIDO (Fast Identity Online . . . www.FIDOalliance.org)

As mobile devices and services became ubiquitous, a new level of complexity was added to the identity and authentication sector. In response, the FIDO Alliance developed open and scalable standards that enable simpler and more secure user authentication experiences across many websites and mobile services. FIDO enables better security for online services, reduced cost for the deploying enterprise, and a simpler and safer consumer experience.

FIDO & the Government

The white paper entitled "FIDO Alliance White Paper: Leveraging FIDO Standards to Extend the PKI Security Model in United States Government Agencies" published by the FIDO Alliance describes the

[1] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf
[2] Ibid., p. iv.
[3] https://en.wikipedia.org/wiki/Public_key_infrastructure

many benefits of FIDO adoption: "There are compelling reasons for agencies to look to FIDO solutions aside from its security characteristics: its standards-based approach, adoption by key industry players, ease of use, and privacy-respecting architecture and design. FIDO's lightweight approach to asymmetric public-key cryptography offers agencies a way to extend the security benefits of public-key cryptography to a wider array of applications, domains and devices – especially where traditional PKI has proven difficult or impossible. To be clear, FIDO is not a replacement for PKI but rather complements it, enabling greater number of users and applications to be protected using asymmetric encryption. This is especially important in situations where the alternative has been username and password."[4]

The white paper further suggests that a vetted identity could be associated in the FIDO process with (1) the issuance of a FIDO Derived PIV Credential, i.e. "a FIDO public/private key pair, linked to the same identity record the PIV card is linked to" or (2) the employment of "Web Access Management (WAM) tools for single sign-on (SSO) or PK-enablement of non-PK applications, allowing FIDO authenticators to be used alongside PKI in these tools…"[5]

As a result of changes made by the National Institute of Standards and Technology DIGITAL IDENTITY GUIDELINES (NIST SP 800-63-3), including the change to separate identity from authentication assurance, the FIDO protocol can now complement PKI in expanding the U.S. Government's authentication ecosystem as it meets government guidelines for asymmetric, public-key (PK) cryptography for authentication. This will lead to strong mobile authentication to FIDO enabled applications and resources that were previously too difficult and or expensive to PKI enable.

FIDO Limitations

One of the limitations of FIDO is the inability to directly integrate with PKI. As a result, government required standard identification credentials (PIV or Derived PIV) are not used in the FIDO authentication process. Furthermore, to date, there has been no published guidance relative to issuance and management of the FIDO Derived Credential. This will hinder the use of FIDO mobile authentication to services requiring a high level of identity assurance.

The Challenge

The nearly ubiquitous distribution of smartphones in daily life presents both an opportunity and a challenge. Users across all federal agencies want to use their mobile devices to perform their daily functions. However, technology managers have been wisely moving to require the use of

[4] https://fidoalliance.org/wp-content/uploads/White-Paper-Leveraging-FIDO-Standards-to-Extend-the-PKI-Security-Model-in-US-Govt-Agencies.pdf
[5] Ibid, pg 5

PIV credentials for accessing sensitive government data, and, heretofore, using PIV credentials with mobile devices has been technically difficult.

The Opportunity

Authentication via FIDO standards provides an opportunity to strengthen authentication for non-PKI enabled services. Integrating Derived PIV verification into the FIDO authentication process will not only enable mobile access to sensitive data but also the ability to leverage existing identification credentials for access to a wider range of applications.

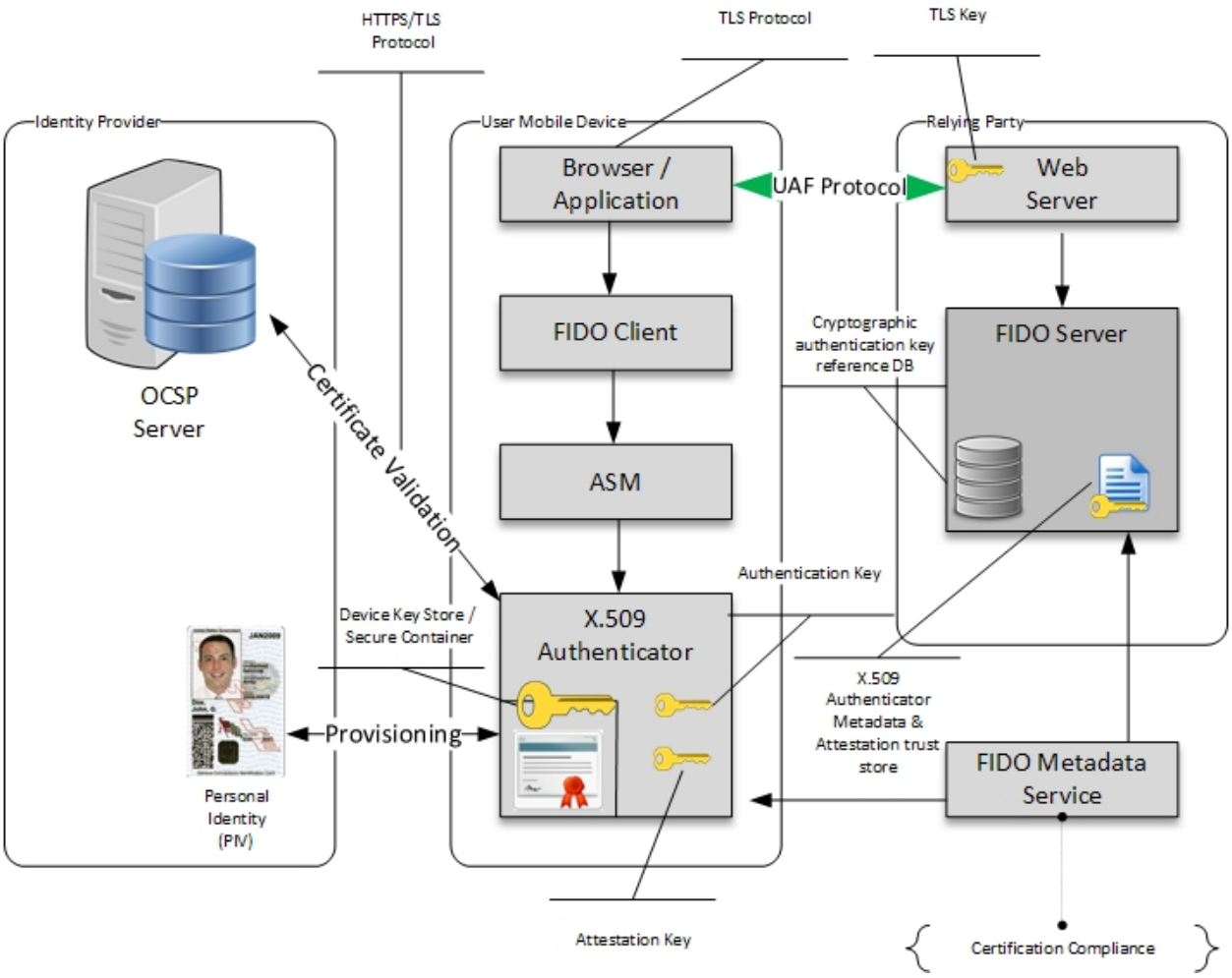
Introduction

The X.509 FIDO Authenticator (Authenticator) is a unique solution for interfacing government Derived PIV Credentials to application services, adding great utility to the leading mobile authentication standard, FIDO. *It comes onto the market as certificate-based attributes and personal credentials are being utilized in the development of mobile identities.*

The solution is essentially middleware joining certificate credentials seamlessly to FIDO Alliance enabled application services. The Authenticator occupies a unique niche in the identity management supply chain, interfacing the business layers of identity to the technology layers of authentication and device level cryptography.

The Authenticator is FIDO UAF 1.0 Certified for the Android operating system. It supports US Government Standards FIPS 140-2 and NIST SP 800-157 and meets authentication level AAL3 as defined by NIST SP 800-63-3.

Figure 1 – Basic Architecture of the x.509 FIDO Authenticator



As depicted above, the Authenticator consists of a User, a Mobile Device, a Derived Credential, an Identity Provider / Certificate Authority (CA) and a FIDO enabled Relying Party (RL).

The Mobile Device contains a Derived Credential, a Relying Party App, a FIDO Client and the Authenticator.

The Identity Provider / Certificate Authority (CA) provisions the Derived Credential in a secure manner on the Mobile Device. It also verifies and validates the certificate prior to (a) binding the certificate to the Authenticator, (b) registering the user with the Relying Party Service and (c) authenticating the user to the Relying Party Service. Verification and validation is performed via the OCSP (Online Certified Status Protocol) check using TLS (Transport Layer Security) 1.2.

The Authenticator is loaded and stored in a secure location of the Mobile Device. As a Certified FIDO UAF authenticator, it will automatically be recognized and initiated while registering or authenticating to a FIDO enabled Relying Party Service.

The Relying Party Service (a) provides the Relying Party App downloaded on the user Mobile Device and (b) utilizes a FIDO server for authentication purposes.

User Experience

The user interacts with the Authenticator in three separate processes: Initial Registration, Relying Party Registration and Relying Party Authentication.

Credential Provisioning / Initial Registration

With both the Derived Credential and Authenticator loaded on the Mobile Device, the user binds the three components together via the Initial Registration process. Once opened, the Authenticator will find and recognize the Derived Credential and automatically verify its validity with the CA. If valid, the Authenticator will prompt the user to create an 8-digit PIN that will bind that credential to the Authenticator. *Thereafter the Authenticator / Derived Credential can only be used by securely entering the PIN, and only if the credential is verified via multiple methods, including signature, time or OCSP check with the proper certificate authority.*

Registration with FIDO-Enabled Relying Party Service

Registration occurs once for each online service the User wants to use.

When a User first opens a FIDO-enabled Relying Party App after completing the Initial Registration process, the Relying Party Service recognizes that the Mobile Device contains a certified FIDO authenticator and asks if the User would like to register using FIDO. If the User responds positively, the User unlocks the Authenticator by entering the PIN created in the Initial Registration process triggering verification of the Derived Credential validity with the CA. If valid, the Authenticator binds the Smart Device and Derived Credential to the Relying Party Service by (a) linking a key field within the Derived Credential to the User account identifier for the Relying Party and (b) creating a private key/ public key pair that is unique to the Mobile Device, Relying Party Service and the User's account. The public key is

then sent to the Relying Party Service and is associated to the User's account, while the private key and authentication method and PIN never leave the Smart Device.

As a result the User's Mobile Device is registered with the Relying Party's Service enabling a passwordless experience for future authentication without the need to ever share private information or secrets with the Relying Party Service.

Authenticating with a FIDO-enabled Relying Party Service

The User opens the Relying Party's Application, which automatically prompts the User to unlock the Authenticator by securely entering the PIN established during the Initial Registration process

Once the Derived Credential has been validated, the Authenticator unlocks the FIDO UAF process that utilizes the public/private key pair and User account identifier to authenticate seamlessly with the Relying Party Service. Specifically, the Mobile Device utilizes the User's account identifier provided by the Relying Party Service to select the correct private key and sign the challenge that is sent from the Relying Party Service. It then generates the signed challenge, which is returned to the Relying Party Service which verifies it with the stored public key and provides the User access to the Relying Party Service.

Benefits

By integrating trusted identification verification into the FIDO authentication process, the Authenticator roots trust in the CA through Derived Credentials. This adds great utility to the FIDO platform in that it, in effect, PK-enables FIDO authentication in a very simple, private, secure and lightweight manner. For U.S. Government applications, this provides the means to utilize FIDO and all of its benefits without the need to create a new FIDO Derived Credential or employ other PK-enablement services.

As a result the x.509 FIDO Authenticator will facilitate rapid development and integration of mobile authentication into government and private sector systems by providing agencies and commercial relying party applications the ability to achieve the security benefits of strong identity assurance and public key cryptography without the traditional cost to PKI enabling its applications.

A summary of the more significant features and benefits provided by bridging the PKI and FIDO worlds are summarized in the table below:

Benefits	Provided By	Features
Security	PKI FIDO	Verified Proof of Identity Based on public key cryptology with no link-ability between services or accounts eliminating the risk of stolen identities.
Privacy	FIDO	Privacy – no personal information shared with relying party.
Interoperability	PKI PKI FIDO	Leverage investment in Trusted Identities Enable the use of x.509 certificates in hardware for proof of identity PK-enable applications where PIV/PKI integration is not feasible such as mobile, cloud services and legacy systems
Reduced Costs	FIDO FIDO FIDO	No Password Management Support already built into many devices and services Lightweight authentication protocol resulting in a reduction in complexity and costs to enable applications
Simplification	FIDO PKI / FIDO	Frictionless User Experience Single Credential for multiple uses

Potential Uses

Below are examples of identified use cases where the Authenticator can add value by effectively and efficiently delivering the combination of strong identity and authentication from a mobile device:

Government & Industry	Employee, customer and contractor access to secure enterprise applications and services
Education	Leveraging existing student credentials to an institution's logical applications
Finance & Banking	Stepped-up authentication relative to corporate accounts
First Responders	Lightweight federated solution
Blockchain Transactions	Providing a strong proof of identity for on boarding into subscription based blockchain networks. Delivering transaction privacy and an audit trail for regulatory purposes
EU National ID	Leveraging vetted ID's for access to both government and commercial resources
Health Care	Digital licenses utilized for e-prescriptions
IoT	Utilizing the device identity for a secure machine to machine authentication.

Implementation Effort

Success and scalability will be based on the ability to integrate into current identity management processes and environments. The following table describes effort required to implement the Authenticator:

Entity	*Activity*	*Effort*
Identity Provider / Certificate Authority	Issue and bind digital certificate to mobile devices	Medium
FIDO - Relying Party – Service	Download metadata Use authenticator	Low
Native Application - Non-FIDO Relying Party	Deploy FIDO Server API Integration Download metadata Use authenticator	Medium
Web Application – Non-FIDO Relying Party	Deploy FIDO Server Download metadata Provide FIDO Client Use authenticator	Medium
End User	Download FIDO authenticator onto device Provision certificate from source Create 8 Character PIN number Use authenticator	Low
Application Developer	Embed authenticator into application utilizing FIDO API	Medium

For compliance documentation see appendix A

Conclusion

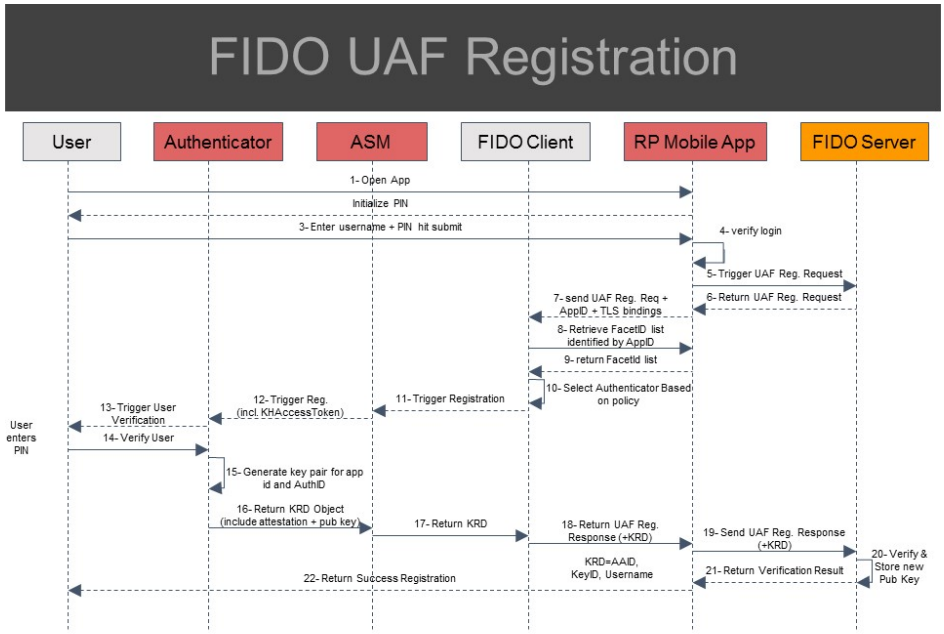
In this white paper and appendices, we have introduced how PKI, through derived credentials stored on a mobile device, can be integrated into the FIDO UAF registration and authentication processes, enabling verification of trusted identities with FIDO authentication. The solution effectively bridges the secure world of PKI identity and the simpler strong authentication world of FIDO, delivering the benefits of both.

This combined approach not only makes the password a thing of the past, but also creates an environment in which all parties have a high level of trust, allowing innovation to expand the use of digital identities in online, IoT and Blockchain applications.

Appendix A – Meeting NIST 800-63-3 standards for highest authorization assurance

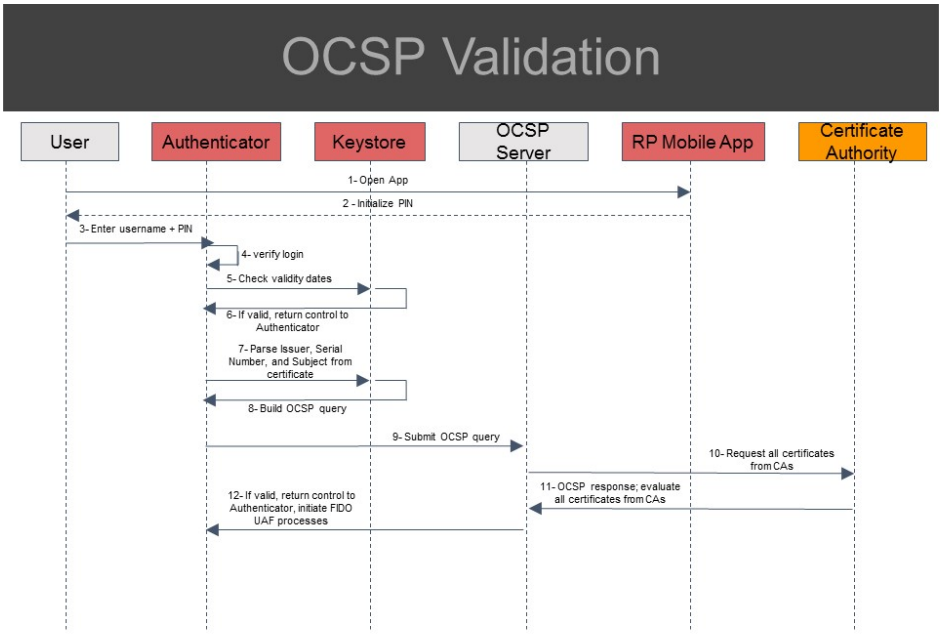
Requirement	AAL3 Compliance Options	x.509 FIDO Authenticator Compliance
Permitted authenticator types	• MF Crypto Device; • SF Crypto Device plus Memorized Secret; • SF OTP Device plus MF Crypto Device or Software; • SF OTP Device plus SF Crypto Software plus Memorized Secret	Compliant: • SF Crypto- All keys are stored inside the mobile device key store. • Memorized Secret – 8-digit PIN with up to 6 login attempts • Authentication binding – meets 800-63A – binding with a memorized secret at registration
FIPS 140 validation	• Level 2 overall (MF authenticators) • Level 1 overall (verifiers and SF Crypto Devices) • Level 3 physical security (all authenticators)	Compliant: • Level 1 – SF crypto devices
Re-authentication	• 12 hours or 15 minutes inactivity; SHALL use both authentication factors	Compliant • Policy controlled –the authenticator can be invoked or forced to re-authenticate based on time limitations in the policy
Security controls	• SP 800-53 High Baseline (or equivalent)	Compliant • FIDO meets SP 800-53
MitM resistance	• Required	Compliant • Works within the secure container of the device
Verifier-impersonation resistance	• Required	Compliant • FIDO meets requirement
Verifier-compromise resistance	• Required	Compliant • Memorized secret is properly hashed
Replay resistance	• Required	Compliant • FIDO is replay resistant.
Authentication intent	• Required	Compliant • Memorized secret is required for every authentication event
Records Retention Policy	• Required	Compliable • Authenticator can support CSP reporting requirements
Privacy Controls	• Required	Compliant • No private information shared between the certificate & the relying party

Appendix B – x.509 FIDO Authenticator - UAF Registration Process



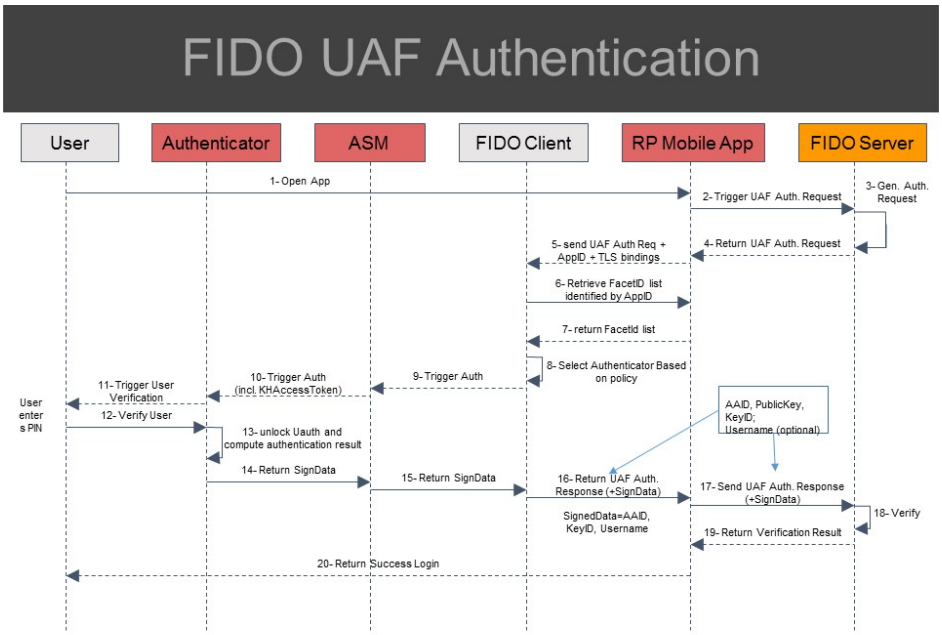
Steps	Description
1	A user opens a relying party mobile app.
2-3	The mobile app requests the user for a PIN and for the user name and PIN to be submitted.
4-6	The mobile app then verifies the login and triggers a UAF Registration request to a FIDO server, which returns the UAF registration request to the relying party mobile app
7-8	The mobile app then sends the UAF registration request along with the application identification and Transit Layer Security (TLS) bindings to the FIDO client, which sends a facet identification list identified by the application identification to the relying party mobile app
9-10	The relying party mobile app returns the facet identification list to the FIDO client, which selects an authenticator based on a policy
11	This in turn, triggers registration from the FIDO client to the Authenticator Specific Module
12	The Authenticator Specific Module triggers registration including a KH Access Token with Authenticator
13 -14	Authenticator triggers user verification with user, such that user enters a PIN and sends a certificate verification and validation to PKI Process
15-17	PKI Process verifies the user, which is sent back to Authenticator for generation of a key pair for the application identification and authentication identification.
18-19	The Authenticator returns a KRD Object including attestation and public key to the Authenticator Specific Module, which in turn, returns the KRD to FIDO client.
20-21	The FIDO client returns the UAF registration response including KRD to the relying party mobile app, which in turn, sends the UAF registration response including KRD to the FIDO server.
23-24	The FIDO server then returns the verification result to the relying party mobile app, which in turn, indicates a successful registration to the user

Appendix C – x.509 FIDO Authenticator – OCSP Validation Process



x.509 Authenticator - OCSP Validation Process	
Steps	Description
1	A user opens a relying party mobile app
2-3	The mobile app requests the user to enter a PIN. The user enters their user name and PIN, which is received by the Authenticator
4-5	The Authenticator then verifies the login and checks the validity of dates with Keystore.
6	If the Keystore confirms validity, then control is returned to the Authenticator
7-8	The Authenticator then parses the issuer, serial number and subject from the certificate from which the Keystore builds the OCSP query
9	The Authenticator will then submit the OCSP query to the OCSP Server.
10	The OCSP Server then requests all certificates from the Certificate Authority.
11	The Certificate Authority then sends the certificates for evaluation by the OCSP Server.
12	Finally, if the OCSP Server determines that the certificates are valid, and then control is returned to the Authenticator for initiation of the FIDO UAF processes.

Appendix D – x.509 FIDO Authenticator – UAF Authentication Process



Steps	Description
1	A User opens a Relying Party Mobile app
2	The Mobile App triggers a UAF authentication request, which is sent to FIDO Server.
3-4	A general authorization request is generated and the UAF authentication request is returned to the relying party mobile app.
5	The Relying Party Mobile app then sends the UAF authentication request along with the application identification and the TLS bindings to the FIDO Client.
6	The FIDO Client seeks to retrieve the Facet identification list identified by the application identification, which request is sent to the Relying Party Mobile app.
7	The Relying Party Mobile app then returns the Facet identification list to the FIDO Client.
8-9	The FIDO Client then selects an authenticator based on policy, which triggers an authentication to the Authenticator Specific Module.
10	The Authenticator Specific Module then triggers an authentication including a Key Handle (KH) access token with the Authenticator
11-12	This triggers user verification, such that when the User identifies themselves, a certificate verification and validation request is sent to PKI Process.
13-14	The PKI Process would then send user verification back to the Authenticator.
15-17	The Authenticator then unlocks the user authentication and computes the authentication result and sends signed data to the Authenticator Specific Module, which in turn, sends the signed data to the FIDO Client.
18	The FIDO Client sends a UAF authentication response including the signed data to the Relying Party Mobile App
19-20	The Relying Party Mobile App sends the UAF authentication response to the FIDO Server, which verifies the UAF authentication response.
21-22	The verification result is then sent to the Relying Party Mobile App, which in turn, provides the login information to the User.

Appendix E – FIDO Certificate

Certification

In recognition of Queralt Inc's achievement of FIDO® UAF Certification

Company: Queralt Inc
Product: X.509 Authenticator
Specification: Universal Authentication Framework (UAF)
Specification Version: 1.0 (2014-12-09)
Implementation Class: Authenticator
AAID: 0037#0001
Operating System: Android
Policy Version: 1.3.2
Interoperability Date: September 14, 2017
Conformance Self-Validation Date: September 7, 2017
Derivative: No
Source Certificate(s): N/A

fido CERTIFIED UAF

Certificate No.
UAF100020170926001

Issued
September 26, 2017