Mobile Authentication Interoperability for Digital Certificates (MAIDC)

Project Initiation Document

1. Summary

Principal Investigator(s):	**Michael Queralt (Queralt Inc.)**	
Period of Performance:	Feb 2016 – July 2016	
Project Champion:	Anil John (HSARPA, DHS S&T Directorate)	
R&D Project Type:	[ ] Basic Research [ ] Applied Research	[X] Advanced Development [ ] Product Development
Project & Funding Status:	[X] Approved	[ ] Under Review

1.2 Summary Description

This project will conduct the advanced development, engineering and certification processes needed to ensure that a X.509 Digital Certificate stored in a secure container on a mobile device will be recognized and can be used as a valid FIDO UAF Token.

Furthermore, to ensure compliance with the USG PIV Derived Credential (PDC) specification, the project will ensure that the X.509 certificate complies with the PDC data model and is stored in the mobile device in a manner that complies with the PDC storage security requirements as defined by NIST.

2. Proposal

2.1 Working Hypothesis

It is possible for a X.509 Digital Certificate compliant with the PDC specifications to also be recognized as a valid FIDO UAF Token and as such, with no further development work on the part of the Credential Issuer, be used with any existing FIDO compliant relying parties for authentication.

2.2 Background

The USG is seeking to leverage the existing investments made in the very high assurance HSPD-12 Personal Identity Verification Program when it comes to mobile devices. PIV Derived Credentials are X.509 Certificates that are “derived” from an existing PIV Credential and provisioned using a secure process for use onto a mobile device while preserving those existing investments.

Mobile Authentication Interoperability for Digital Certificates (MAIDC)

Project Initiation Document

Given the PDC direction, agencies are putting into place secure PDC provisioning "rails" to deploy the credential from their credential issuance infrastructures to a mobile device. And given priorities, risk appetites, and existing technical capabilities, these provisioning and key management rails are often unique to an agency.

Furthermore, agencies are making different choices in where they will store and how they will utilize the credential once it is deployed onto the device. These storage choices range from storing the PDC in a native key store, a MDM container key store, or a secure element. Similarly, usage of the credential range from using the PDC to integrate with native apps on the device to using it with container based apps or a combination of the above.

This project understands the above Agency related moving parts that are operationally focused, and as such is focused on leveraging them rather than replicating them. This project instead is focused on leveraging the one point of consistency across the multiple moving pieces – An agency specific mechanism will exist to provision a PDC onto the mobile device.

Using the existence of the PDC on the mobile device as a starting point, this project is focused on answering the question of how best to leverage that PDC for use, with no further investments by the Agency, across the widest variety of use cases especially when it comes to non-federal government interoperability use cases.

Which is where FIDO Alliance specifications comes into the picture. The FIDO Alliance is a new consortium of identity management vendors, product companies and service providers working on improving online authentication by developing open, interoperable industry specifications that leverage device-based user verification for better usability and proven public key cryptography for stronger security.

FIDO standards support a range of interoperable authentication factors and modalities, including biometrics. There is already a growing amount of products ready for FIDO deployment, and an ever expanding Relying Party ecosystem, including leading mobile device manufacturers, financial institutions and technology companies, such as Google, Paypal, Samsung, Lenovo and LG.

The Mobile Authentication Interoperability for Digital Certificates (MAIDC) project will deliver a capability that is conformant to both the PDC and FIDO specifications to ensure that a PDC can be utilized in either government or commercial environments under the FIDO (Fast Identity On-Line) protocol. The objective is to bridge the PDC worlds of strong authentication on mobile devices to enterprise server authentication methods via the FIDO protocols.

2.3 Timing

This project is built on the foundation established by both the USG PIV Derived Credential Specification and the FIDO Alliance Universal Authentication Factor (UAF) Specification.

Currently PIV credentials are carried on smartcards that contain secure private keys. The Derived Credentials variation on PIV replicates the digital certificates in approved mobile devices, meeting government standards as required by NIST.SP.800-63.

The logic of FIDO is that once an individual has activated their personal secure device, they should be able to use that device to then authenticate to any digital service. The FIDO Protocol UAF codifies a number of attributes and signals that help a service provider know what sort of device is being used, how exactly the user has unlocked their device, and so on; this data feeds a rich variety of risk management decisions that may be made at the server, all based on the PDC that has been stored in the mobile device.

A FIDO UAF Certified PIV Derived Credential token is the bridge between USG credentials to enterprise server side resources without the server needing to implement a unique or government-specific credential validation capability. With FIDO protocols being increasingly accepted by commercial servers, the proposed token, will enable high assurance interoperability of first responders, for example; to emergency response management partners, energy utilities, healthcare facilities, and financial entities, safeguarding the privacy of the individual and extending the value of the credential to be used in a diverse range of authentication activities.

2.4 Scope and Project Phases

In-Scope

- Ensuring that the X.509 Certificate is fully conformant to the USG PDC Specifications
- Ensuring that the X.509 Certificate meets the NIST PDC requirements for secure storage on the mobile device, ideally in a Trusted Execution Environment.
- Ensuring that the X.509 Certificate can be used as a FIDO UAF token using the FIDO defined UAF Protocol
- Defining and ensuring that the data elements that are generated during an authentication event, and conveyed via the FIDO protocols, contain the relevant information that allow a relying party to make an informed decision on the credential usage.
- Ensuring that the developed capability is successfully certified via FIDO certification processes to ensure that the PDC is recognized as a valid FIDO UAF Token

Out-of-Scope

- Provisioning or key management “rails” needed to deploy the PDC onto the mobile device

- Implementation of functionality needed to utilize the deployed PDC with native or custom apps on the mobile device

Viability (Phase 1):

- Examine the currently available technologies (including PIV cards, PKI, and FIDO) to assess market needs and potential customers (government and private sector)
- Identify candidate phase 2 partners
- Research detailed mobile-to-enterprise authentication requirements in target sectors, and analyze FIDO utilization among targeted industrial segments
- Review security considerations and validate them with appropriate authoritative bodies, and refine the approach to be used in later phases.

Execution (Phase 2):

- Acquire necessary hardware and software, map technical and security requirements to software design objectives
- Build the software components (PDC unlocking mechanism, FIDO Authenticator, FIDO ASM, certificate validation code)
- Create a sample relying party application, test using scripts
- Complete the FIDO Alliance certification formalities in preparation for an interoperability demo
- Prove out the integration of mobile credentials to enterprise backend systems, and demonstrate verified code to transition partners, in readiness for phase 3.

Transition (Phase 3):

- Engage with earlier selected partners in government and/or elsewhere to understand the provisioning and deployment "rails" they have built
- Partner with one or more transition partners to integrate their provisioning API into the MAIDC solution
- Demonstrate, with transition partner support, an end-to-end interoperability demo that utilizes the partner's existing provisioning mechanism as well as the use of the PDC on the mobile device with a FIDO compliant relying party.

2.5 Objectives and Output

Objectives:

- **Conformance to NIST specifications for PDC (Data Model and Storage)**
  - Access to the PIV Derived Credential will be controlled by 6-digit PIN authentication
  - There will be a mechanism to block use of the Derived PIV Authentication private key after a number of consecutive failed activation attempts as stipulated by the department or agency

- Will meet NIST.SP.800-157 and related specifications for storing and any handling of the by the Derived PIV Credential FIDO Authenticator.

- **FIDO UAF Certification**
  - Map PIV Derived Credential onto FIDO's Universal Authentication Framework (UAF) protocol assertions
  - The FIDO PDC Authenticator will conform to the FIDO UAF authenticator, Authenticator Specific Module (ASM) specifications
  - Profile of PDC information sent to FIDO server & made available to Relying Party

- **Security and Privacy**
  - Certificate Path Discovery and Validation: Certificate revocation checking will be done, including other certificate validation methods like: digital signature validation and expiration checks.
  - Definition and conveyance of PDC specific data elements in the authentication process
  - The new token will be engineered to ensure it meets the requirements of Electronic Authentication Guideline NIST.SP.800-63

Outputs:

- **Phase 1**
  - Analysis of market need and commercialization approaches
  - Systems integrator and OEM partnership strategies
  - Technical analysis and associated white paper on the use of Trusted Existing Environments to meet NIST PDC storage requirements
- **Phase 2**
  - Proof of concept mobile application
    - Registration of credential to back end FIDO services.
    - Translation module – PIV Derived Credential to FIDO AUF attributes.
    - Proof of concept for the use of PIV Derived Credential for FIDO enabled transactions.
  - FIDO Certification of Authenticator Specific Module
- **Phase** 3
  - Integration of capability with one or more transition partner provisioning API
  - FIDO ASM ready for commercialization
  - A White Paper summarizing the project for third party audiences

3. Benefits and Risks

3.1 Benefits

- Increase PIV certificate value and use
  - Extending the use of the certificate into commercial activities - safeguarding privacy and certificate information.
- Enhance security and privacy
  - Reduce the need to use passwords
  - Provides authentication without losing the strength of the certificate, by decoupling personal information from the authentication event
  - Decreases the ability of a social engineer attack via the help desk – by reducing the number of password reset request – as passwords are not utilized
- Lower operations cost
  - Extending current investments made on the PIV certification process into mobile devices
  - Reduce security operational cost – by reducing the use of password it will reduce the number of password-reset calls into the helpdesk.
- Rapid development and integration of mobile authentication into government and private sector systems

3.2 Risks and Mitigation

Risk	Mitigation
NIST PIV Derived Credential Specifications are not finalized	Utilize the latest versions of NIST 800-157, 800-63, and 800-53 to guide the security requirements to guide this project and closely coordinate with authoritative bodies to ensure conformance. Obtain access to latest drafts for testing; maintain close relations with NIST; track progress; make best effort to produce a reference implementation.
FIDO Certification is Delayed	Use FIDO Test Suites to determine compliance; Release product if necessary with qualifications while ensuring future compliance.

Lack of Adoption by Relying Parties	Ensure that transition partners are engaged with from the beginning and are kept in the loop on project progress. To the extent feasible, obtain letters of intent from qualified partners to lay the groundwork for transition activities.

Are you a Government Program Manager responsible for ensuring the security and trustworthiness of the programs and services you manage?

Are you interested in learning more about this project, being kept up to date on its progress, and how it could help you mitigate risk and deliver value?

If so, contact:

Anil John
Program Manager, Identity and Privacy R&D
DHS Science & Technology Directorate
anil.john@hq.dhs.gov