Request for Demonstration:

Issuance and Lifecycle Management of a Derived FIDO2 Credential (DFC)

ATARC Identity Management Working Group

July 2022

ATARC

Advanced Technology Academic Research Center

Table of Contents

Table of Contents ii

1 Executive Summary 1

2 Summary of Issuance and Lifecycle Management for the DFC 2

3 Derived FIDO2 Credential (DFC) Issuance Workflow 3

4 DFC Authentication 5

5 Demonstration Format 6

6 Capabilities Demonstration 7

6.1 DFC Issuance 7

6.2 DFC Lifecycle Management 7

6.3 DFC Authentication 7

7 Authoritative References 8

7.1 Guidance 8

7.2 Directive & Memoranda 8

Disclaimer: *This document was prepared by the members of the ATARC Identity Management Working Group in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with.*

1 Executive Summary

The Advanced Technology Academic Research Center (ATARC) is requesting demonstrations to show the feasibility of the issuance and lifecycle management of a Derived FIDO2 Credential (DFC) based upon previous guidance for the issuance of X.509 based Derived PIV Credentials.

By leveraging this workflow, vendors will demonstrate how to assert organizational attestation of the FIDO2 hardware token, strong identity binding tying a user's existing PIV or CAC smartcard to the issuance of the DFC, and leveraging attribute based access control (ABAC) to provide attestation of the assurance level of the DFC during authentication. These controls are established practices that minimize the risk of impersonation, and allow for managing which resources an End User can interact with while leveraging a DFC. Currently, no such guidance exists for the issuance and management of FIDO2 credentials, and enterprise use of these credentials has been limited for this reason.

2 Summary of Issuance and Lifecycle Management for the DFC

With the release of FIPS 201-3, non-X.509 based authenticators are in scope for satisfying a Derived PIV Credential. These credentials are for use when the use of a PIV is not practical, and are to contain a lifecycle independent of the end user's PIV smartcard and PIV X.509 certificates with exception to when the user is no longer PIV eligible, at which time the DPC must be revoked.

While FIPS 201-3 only requires the form factor of the DPC to adhere to NIST SP 800-63b, OMB-M-22-09 restricts Multi-Factor Authentication (MFA) to phishing-resistant authenticators. One common example of a phishing-resistant authenticator is a FIDO2 WebAuth token. The memorandum goes on to specify "To the greatest extent possible, agencies should centrally implement support for non-PIV authenticators in their enterprise identity management systems, so that these authenticators are centrally managed and connected to enterprise identities. (OMB M-22-09, p.8)"

To facilitate this central management and connectivity to enterprise identities, ATARC is exploring the feasibility of aligning the issuance and lifecycle management of a FIDO2 WebAuthn authenticator to those of a Derived PIV Credential. This would, in effect, create a Derived FIDO2 Credential or DFC. This management would align with NIST SP 800-157 and NIST SP 800-79-2, which provide guidance for the issuance of a traditional, X.509 based, Derived PIV Credential.

This workflow would begin with supervisorial approval for the issuance of the DFC, which would then allow the user to register an organizationally issued DFC token. The user would register this token by first proving possession of a valid PIV authentication certificate associated with a valid PIV smartcard. This binds the identity proofing of the DFC to that of the presented PIV smartcard, resulting in the derived nature of the DFC. Following this authentication, the user will register their FIDO2 WebAuthn authenticator, and a directory attribute will be assigned, which can be used for attestation of the trust of the DFC during authentication and/or authorization events, similar to the presence of the id-fpki-common-derived-pivAuth or id-fpki-common-derived-pivAuth-hardware object identifier (OID) found within a Derived PIV Credential.

Following registration, the DFC validity period would be independent of the certificate and card lifetimes of the user's PIV smartcard presented during issuance. This allows the DFC to be available for use should the user's PIV smartcard become lost or damaged and to support authentication into devices where the PIV smartcard form factor is not supported. The exception to this shall be in the case where the user is no longer eligible to be a valid PIV cardholder. In this case of the removal of the user's PIV eligibility, all associated DFC must be rendered incapable of authentication.

3 Derived FIDO2 Credential (DFC) Issuance Workflow

Step 1: Supervisor Approval Received for End User to receive a DFC MFA

- Consistent with NIST SP 800-157

Step 2: End User receives the DFC Physical Token. The DFC should have an organizational certificate installed during manufacturing or loaded by the organization upon receipt of the unassigned FIDO2 tokens.

- No current Policy for this, but mirrors smart card supply chain controls, and provides organizational attestation to the physical FIDO2 token

Step 3: End User logs into the DFC Credential Management System (CMS) with their PIV Authentication Certificate binding the issuance of the DFC to the established identity proofing of the PIV smart card.

- PIV Authentication certificate revocation list (CRL) validation and PIV Authentication Object Identifier (OID) check to be performed during authentication
- 7 days later, CRL validation to be repeated on the PIV Authentication certificate presented by the End User during issuance of the DFC
    - If found to be revoked, action may need to be taken to revoke the issued DFC
- Consistent with NIST SP 800-157 and NIST SP 800-79-2

Step 4: Registration and Issuance of DFC by the CMS

- Registration and Issuance of the DFC conforms to the FIDO2 standard and exists between the CMS and the DFC. This binding can be leveraged to replace individual application registration to the DFC, and can be centrally leveraged by the agency's Federation Policy Engine
    - This conforms to OMB M-22-09 for central identity policy management and enforcement

Step 5: Registration of the DFC by the CMS binds the FIDO2 token to the End User identity within a directory

- Several attributes should be generated during the directory binding to include DFC lifetime.
- The DFC CMS shall generate an attribute indicating the level of assurance of the credential. This shall take the place of the id-fpki-common-derived-pivAuth and id-fpki-common-derived-pivAuth-hardware OIDs found within Derived PIV Credentials
    - Consistent with NIST SP 800-157 and NIST SP 800-79-2

- For this demonstration, vendors will be given the option to decide the format and contents of this DFC attribute

Step 6: The End User's PIV Card Revocation status shall be checked from the issuing PIV smart card CMS by the DFC CMS

- Should be performed every 18 hours
  - Consistent with NIST SP 800-79-2

Step 7: While the lifetime of the DFC should be independent of the certificate and smart card lifetimes of the End User's associated PIV, when the End User is no longer PIV eligible, all DFCs belonging to that End User shall no longer be authorized for authentication. While the FIDO2 standard does not currently provide an analog to X.509 certificate revocation, the DFC CMS shall ensure that End User's FIDO2 tokens cannot be used for successful authentication.

- This further necessitates the need for the FIDO2 binding to exist only between the DFC and the DFC CMS rather than with each individual end application
- Consistent with FIPS 201-3, NIST SP 800-157, and NIST SP 800-79-2

4 DFC Authentication

As outlined within Step 5 of the DFC issuance workflow listed above, the DFC CMS generated an attribute indicating the level of assurance of the credential. This attribute allows for the attestation of the trust of the DFC during authentication, and allows for subsequent authorization decisions.

To assert this attestation, the authentication system should follow the requirements outlined within section 7 of FIPS 201-3. This requires the DFC authentication to be enforced through federation, and shall follow the guidelines listed within NIST SP 800-63c. The federated session shall include the DFC level of assurance attribute within the assertion or federation scope. This attribute should be used for authorization decisions either directly by an application, or, more preferably, by a policy enforcement point.

By authenticating the DFC through a federation, the end user is not required to register the DFC with each application or relying party. This allows for greater scalability, reduces the burden of use on the end user, and enables more efficient administration of the DFC.

5 Demonstration Format

Length of Demo:	30 min
Calendar:	ATARC will send a Zoom link for each vendor. Presentations will begin no earlier than July 26th, 2022
Visual Format:	Vendors will be given the option to present a live demonstration, slide material, and/or videos
Vendor Collaboration:	Vendor collaboration is encouraged, and demonstrations featuring multiple vendors will be permitted. If presenting a multi-vendor solution, consideration will be given for a time extension for the demonstration, if necessary

6 Capabilities Demonstration

Vendors will demonstrate one, all, or a combination of the following. Vendors will identify in the beginning of the demonstration which capabilities they will cover. Capabilities not covered within this section, and not relevant to the topics covered within this document should not be demonstrated.

6.1 DFC Issuance

Vendors will demonstrate as closely as their product permits the issuance and registration of a FIDO2 token to an End User following the DFC Issuance Workflow outlined above. Only commercial off the shelf solutions should be presented. A valid PIV, test PIV, or an alternative X.509 certificate (soft certificate is acceptable) shall be used during issuance. For the purposes of this demo, identity proofing of the X.509 certificate shall be assumed to have previously occurred at an Identity Assurance Level 3 (IAL 3, NIST SP-800-63a).

6.2 DFC Lifecycle Management

Vendors should demonstrate the ability to manage a validity period for the issued DFC, and shall demonstrate the ability to retire or revoke a DFC from authentication in case of a lost or damaged DFC token. Additionally, vendors will demonstrate the ability to revoke all issued DFCs to a user when the End User is no longer PIV eligible.

6.3 DFC Authentication

Vendors will demonstrate the ability to (a) assert the DFC attribute identified in Step 5 of the DFC Issuance Workflow to an application or policy enforcement point during authentication, and (b) perform an authorization decision to grant or restrict access based upon the attestation of the DFC attribute. Vendors are encouraged to follow the guidance within the DFC authentication section of this document.

7 Authoritative References

7.1 Guidance

Title	Description
FIPS 201-3	This is the standard for federal agencies to implement HSPD-12.
NIST SP 800-63-3	This is a special publication on the digital identity guidelines for identity verification, authenticator assurance, and federation considerations for federal agencies. The document contains three additional publications labeled a, b, and c.
NIST SP 800-157	This is a special publication on how federal agencies can derived the trust from an established PIV smart card to issue a new X.509 certificate(s).
NIST SP 800-79-2	This is a special publication providing technical guidance on the issuance of PIV and Derived PIV X.509 certificates.

7.2 Directive & Memoranda

Title	Description
OMB M-22-09	This memorandum lays out the strategy for federal agencies to improve on enterprise identity and access controls.