Whitepaper: A Shared Services Model to Promote Rapid Adoption of FIDO2 Within the Federal Government

by Sarbari Gupta, PhD

Since early 2023, Electrosoft, in support of the General Services Administration (GSA) Office of Governmentwide Policy (OGP), has been seeking ways to accelerate Fast IDentity Online 2 (FIDO2) adoption within the federal enterprise. Microsoft defines FIDO2 as "an open standard for user authentication that aims to strengthen the way people sign in to online services to increase overall trust. FIDO2 strengthens security and protects individuals and organizations from cybercrimes by using phishing-resistant cryptographic credentials to validate user identities." An industry consortium, known as the FIDO Alliance, issued this standard for passwordless authentication in 2018.

The Electrosoft–GSA effort has been an iterative process involving extensive stakeholder engagement with other federal agencies as well as industry representatives. The ultimate goal is to develop a shared services model that simplifies FIDO2 adoption for federal agencies. Feedback received to date has led to improvements to the architecture as well as enhanced operational readiness. Ongoing discussions seek to identify agencies willing to and/or capable of taking responsibility for model governance and technical operations.

Given the current cyber threat environment, a straightforward means for multifactor, phishing-resistant authentication is needed. The vulnerabilities associated with traditional passwords are well known and well documented. The advantages of a FIDO2/Derived FIDO2 Credential (DFC) shared services model are many, as this whitepaper will detail. Federal agencies are therefore encouraged to explore becoming part of the FIDO2 shared services model for phishing-resistant authentication.

HISTORICAL PERSPECTIVE

For years, federal enterprise users (employees and contractors) had to authenticate their identity using either a Personal Identity Verification (PIV) card or a Common Access Card (CAC), depending on affiliation with either a civilian (PIV) or Department of Defense (CAC) agency. Essentially, both forms represent a smart card that includes Public Key Infrastructure (PKI) credentials verified via digital certificates. Trust in these forms of authentication arises from Federal PKI (FPKI) trust and governance principles.

In 2014, the National Institute of Standards and Technology (NIST) issued a special publication (SP) designated NIST SP 800-157. This document introduced the concept of a Derived PIV Credential (DPC) for mobile platforms. NIST defines a DPC as, "A credential issued based on proof of possession and control of a PIV card. Derived PIV credentials are typically used in

situations that do not easily accommodate a PIV card, such as in conjunction with mobile devices."

Later, in 2020, Office of Management and Budget (OMB) Memorandum M-19-17 allowed the use of "additional solutions (e.g., different authenticators) that meet the intent of Homeland Security Presidential Directive 12 (HSPD-12) and advance the technical approach to managing identities." These "additional solutions" comprise non-PKI authenticators.

In 2023, NIST formally expanded the concept of non-PKI derived credentials beyond mobile devices. In NIST SP 800-157 rev. 1, NIST wrote that derived PIV credentials would "include non-PKI-based phishing-resistant multi-factor credentials." Notably, FIDO2 solutions fit the basic description of non-PKI Derived Credentials but must satisfy additional requirement to be approved for federal use.

DFC REQUIREMENTS

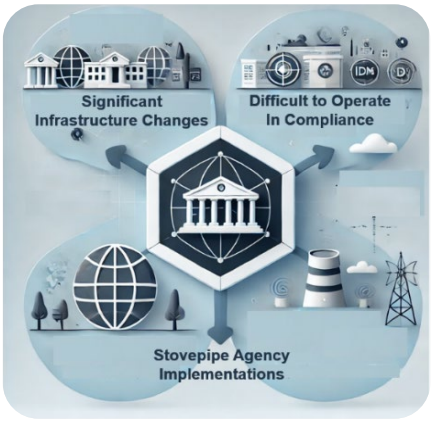
FIDO2 incorporates many important features that federal authenticators should possess. For example, they should be phishing resistant and multifactorial, easy to use and intuitive, readily available, allow synchronization, enable credential recovery, and allow cross-platform use.

However, DFCs must comply with specific requirements delineated in NIST SP 800-157 rev. 1. First, they must be issued by the same agency that issued the user a PIV card. Second, users must prove they can successfully authenticate using their PIV card. Third, the DFC must be associated with the user's PIV identity account. Fourth, the DFC is to be used in a federation model employing Identity Providers and Relying Parties. Finally, the DFC's lifecycle must be managed as part of the PIV identity account, which means the DFC is terminated when the PIV identity account is terminated

Because DFCs are associated with a PIV card, the strong identity proofing processes of card acquisition convey to DFCs as do lifecycle management capabilities stemming from the related PIV account. These additions makes them suitable for federal use.

FIDO2 ADOPTION CHALLENGES

Two types of challenges exist relative to FIDO2 adoption by federal enterprise users. They are technical and business in nature.



Technical Challenges

There are at least three technical challenges with DFC implementation: compliance difficulties associated with federal policy; interoperability issues; and the need for significant infrastructure changes.

As discussed previously, DFCs must comply with five separate requirements prescribed in NIST SP 800-157 rev. 1. To meet

all five, Application Programming Interfaces or APIs will need to be developed in order for FIDO2 Identity Providers (IdPs) to connect with an agency Identity Management System (IDMS).

The federal government is replete with stovepipe agency implementations. To overcome interoperability issues, multiple proprietary APIs will likely be needed to connect with the different IDMS employed by various agencies. This possibility could lead to a proliferation of APIs.

Like stovepipe issues, agency infrastructure also affects ease of implementation. Current infrastructure in many agencies will necessitate significant changes, increasing the complexity of DFC adoption.

Business Challenges

Here, too, there are several potential roadblocks to federal DFC adoption. Governance, insofar as the government's ability to vet FIDO2 products/services for potential use as DFCs within agencies, is a primary concern. Then, too, the government's ability to oversee DFC operations in terms of compliance comes into play. Right now, there is no federal unit designated to execute the governance role.

Cost is a concern as well, both on the front and back ends. Some agency implementations will be quite costly due to complexities associated with infrastructure. In turn, this issue creates two more troublesome ones. First, ongoing operations and maintenance costs to maintain compliant DFC use can be steep. Then, too, the efforts undertaken to overcome infrastructure challenges may result in vendor lock-in due to reliance on proprietary APIs to connect to IDMS. These agencies may be subject to unreasonable price escalations and not have the option to switch providers.

A PROPOSED SHARED SERVICES SOLUTION

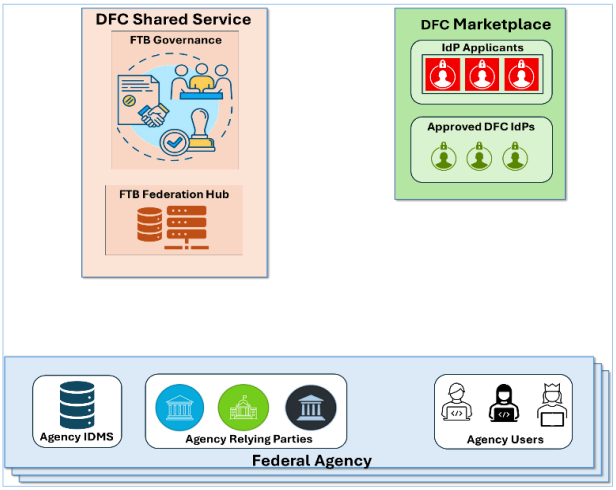
The FIDO2/DFC Shared Services Model, as articulated herein, addresses the technical and business challenges delineated above. The major model components comprise three stakeholder entities: the DFC Shared Service, the DFC Marketplace, and various federal agencies that wish to engage with the DFC Shared Service.

DFC Shared Service

This component comprises the Federal Trust Broker (FTB) governance function and the FTB Federation Hub (FedHub).

The FTB governance function provides three primary services:

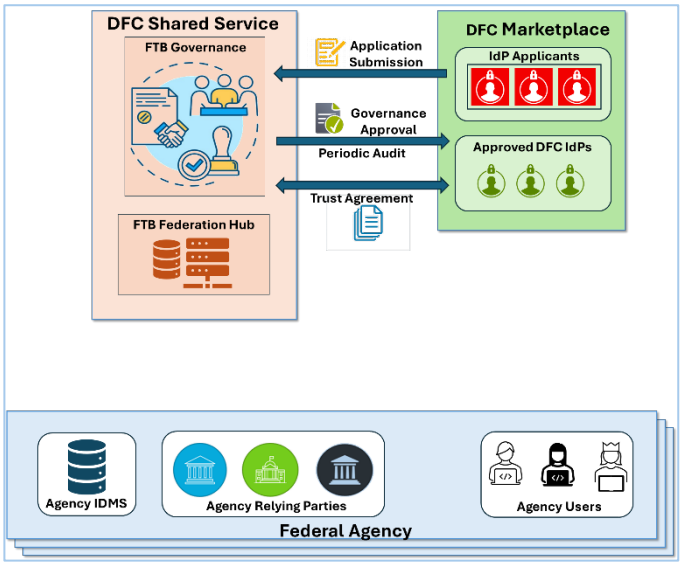
1. *Vetting and approval of DFC providers.* This effort establishes an approved DFC IdP marketplace consisting of FIDO2 providers that meet the functional and policy requirements established for DFCs via NIST SP 800-157 rev. 1.
2. *Oversight.* Periodic audits of approved DFC IdPs as a means of ensuring ongoing compliance.
3. *Federation Trust Agreement creation and management.* Such pairwise agreements involve the approved DFC IdPs and Relying Parties (RPs), that is, the agency online applications that provision services to agency enterprise users.



The FedHub establishes transitive trust between agency RPs and DFC IdPs. It interprets federation assertions sent by DFC IdPs and creates enhanced federation assertions to be consumed by agency RPs.

DFC Marketplace

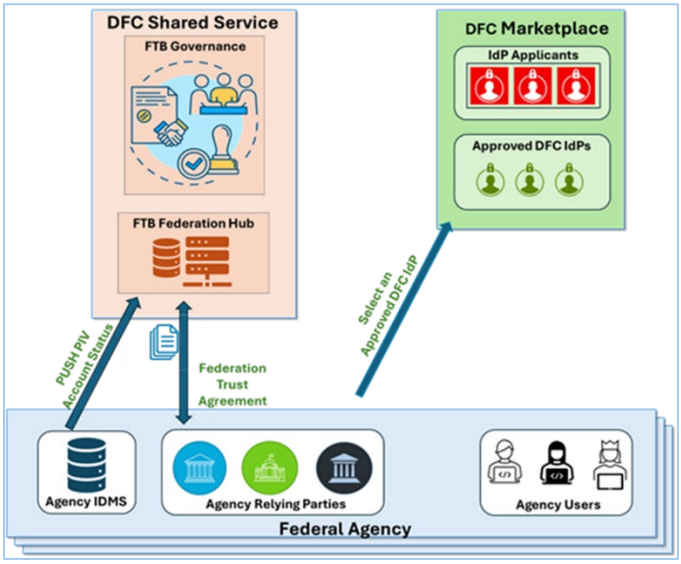
As previously established, FIDO2 IdP enrollment is predicated on successful completion of the FTB vetting and review process shown. This process ensures two elements: (1) compliance with NIST requirements and (2) inter-operability with the DFC Shared Service solution.



Approved DFC IdPs must then enter into a trust agreement with the FTB and have the capability to both access a Common API and execute the following NIST requirements: (a) ascertain the PIV/CAC account status for specific PIV/CAC accounts and (b) register new DFCs with the appropriate user's PIV account. Approved DFC IdPs will be required to send federation assertions to the FTB each time a DFC is used to authenticate a user.

Federal Agency Customers

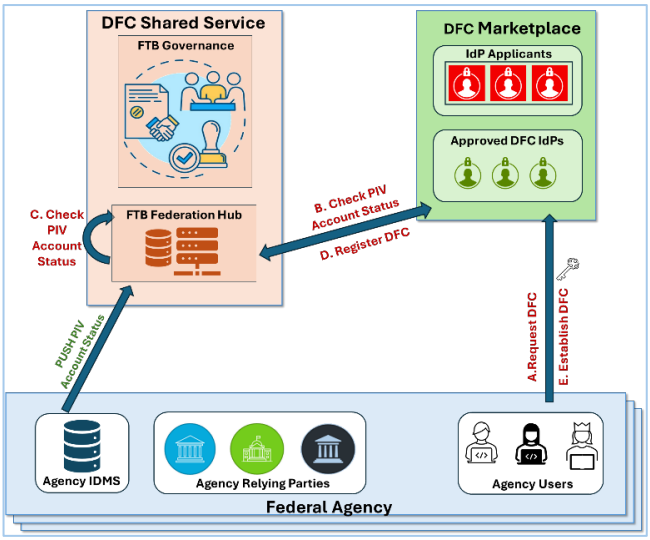
Agencies that engage with the DFC Shared Service will be requested to: (a) select one of the preapproved DFC identity providers, (b) set up a federation trust agreement with the FTB FedHub, and (c) sign an agreement to send to the FTB FedHub a daily feed of PIV account status (active/terminated) information for all PIV accounts within the agency's IDMS.



Selecting a specific DFC IdP by an agency implies that all enterprise users of that agency will be required to use that DFC IdP for issuance and authentication of DFCs. When the agency sets up a regular push of the PIV account status data, the DFC FedHub saves the data to a local database to maintain an up-to-date status of the PIV account status for all enterprise users of that agency. This provision allows the FTB FedHub to respond to DFC issuance requests for that agency as well as translate federation assertions for agency users who authenticate using their DFCs.

SOLUTION MECHANICS

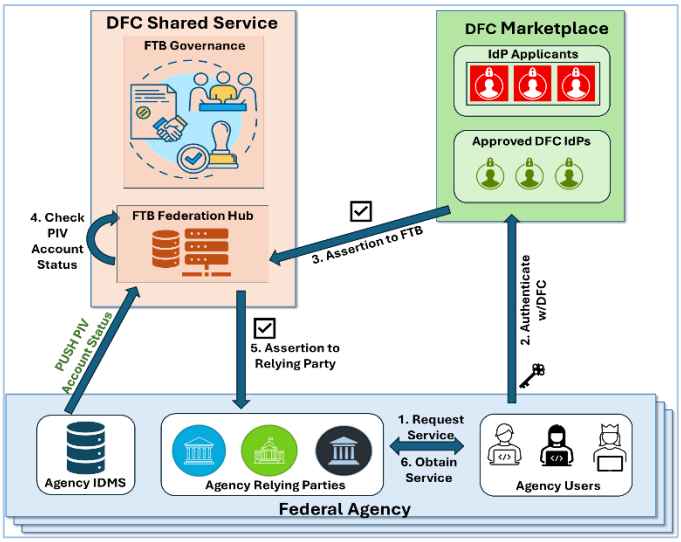
Under the envisioned model, efforts to establish and maintain the DFC marketplace are inaugurated. Here, FIDO2 IdPs would apply for approval to the FTB. The FTB would vet each applicant for: (a) compliance with NIST SP 800-157 rev. 1 and (b) its capacity to support a common API. Next, the FTB would establish Pairwise Trust Agreements between the FedHub and each approved DFC IdP. Finally, maintenance would take the form of periodic audits of approved DFC IdPs.



Agencies seeking to participate in the Shared Services Model would select from among the approved IdPs. Next, agency enterprise users would establish a Federation Trust Agreement with DFC FedHub. Then, provisions to provide a daily push of PIV/CAC account status to the FTB would be put in place.

In turn, users within the agency would request a new DFC and receive a link to the selected DFC IdP. Users would authenticate (typically via a remote online connection) to the selected DFC IdP using their PIV card. The DFC IdP would then check the status of users' PIV/CAC account using the common API and, if active, the DFC IdP would issue a new DFC authenticator. The DFC IdP would then register each user's new DFC public key with the FedHub as shown above.

Next, users would authenticate using their DFC to gain access to the agency's online services. This process begins by requesting access to an RP service. The RP redirects users to the FedHub for authentication. In turn, the FedHub redirects users to the agency's chosen DFC IdP. Users then must authenticate to the DFC IdP using their DFC. Successful DFC authentication results in an assertion being sent to FedHub.



Upon receipt by the FedHub, the process of verifying the user's PIV/CAC account status as active begins. If active, FedHub creates a new assertion and sends it to the RP, which authorizes the user to access the service as shown here.

The end result is a process that establishes trust in conformance with the NIST prescription for a "non-PKI-based phishing-resistant multifactor credential."

SOLUTION ADVANTAGES

The DFC Shared Services Model both overcomes the enumerated technical and business challenges and offers other benefits as well. Specifically, these advantages are:

- *Security*: Uses phishing-resistant, passwordless authentication.
- *Scalability*: Can easily onboard agencies and FIDO2 identity providers.
- *Cost Efficiency*: Reduces IT costs by sharing infrastructure across agencies.
- *Interoperability*: Allows cross-platform use on both traditional and mobile devices.
- *Compliance*: Aligns with FIPS 201-3 and NIST SP 800-157 rev. 1.

SUMMARY

FIDO2 is a strong, scalable, and secure authentication standard. Development of the shared services model simplifies FIDO2 adoption for federal agencies, enabling them to benefit from enhanced security, compliance, flexibility, and cost savings.

Model development and refinement has been an iterative process since early 2023. Beyond the expertise applied by GSA and Electrosoft, there's been significant stakeholder engagement encompassing industry and federal entities. The current model is responsive to compliance, security, scalability, interoperability, and cost-efficiency concerns. And, as circumstances dictate, future enhancements will be made.

Right now, there are two pressing needs. First, identify agencies willing to embrace the governance and operational roles associated with model implementation. Second, secure model buy-in by federal agencies seeking to implement a multifactorial, phishing-resistant authentication methodology.

ELECTROSOFT AS AN INDUSTRY LEADER IN AUTHENTICATION TECHNOLOGY

Beyond the specific efforts detailed herein, Electrosoft has been a leader in the online authentication realm for nearly two decades. While a detailed accounting of Electrosoft's expertise exceeds the confines of this whitepaper, some highpoints follow:

- Promoting robust cryptographic key management practices for use within cloud computing environments.
- Co-authoring NIST SP 800-63-1, *Electronic Authentication Guideline* (and subsequent revisions through SP 800-63-4) and NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*.
- Presenting novel authentication methodologies using mobile platforms: "Strong Authentication for Physical Access Using Mobile Devices," "Me and My Mobile Device: A New Approach for Strong Multidimensional Authentication," and "Digital Authentication – Mobile Platforms to the Rescue."
- Publishing multiple blogs including "Authenticator Management," "Double Down on Multi-Factor Authorization," "PIV Cards Going Away? Not Quite. New OMB Memo Reaffirms and Expands Their Role," and "Passing on Passwords."
- Presenting "No More Excuses: Feds Need to Lead with Strong Authentication," Case Study: "Strengthening Security Posture Through PIV Card Issuance, Authentication, and Single Sign-On," Case Study: "Enterprise PIV-Authentication Sans Active Directory," "Leveraging Passkeys for a Federated Federal Government Environment," and "A Shared Services Model to Promote Rapid Adoption of FIDO2 Within Federal Government."
- Delivering Kantara assessments to credential service providers, supporting GSA's Federal Public Key Infrastructure Management Authority, and defining a vision and

architecture for an HSPD-12–compliant Personal Identity Verification Authentication Engineering and Design Solution.

- Serving as a panel member at ATARC–Electrosoft webinar "Beyond Traditional Boundaries: Modernizing PIV/CAC Authentication."

CONTACT US

To learn more information about Electrosoft and our capabilities, contact us at info@electrosoft-inc.com.

ABOUT ELECTROSOFT

Electrosoft delivers comprehensive technology-based solutions and services that propel mission success for federal government customers. Specializing in cybersecurity, Electrosoft supports civilian and defense organizations in advancing cybersecurity postures, achieving digital transformation, and adopting agile approaches to improve operational efficiency and security. Electrosoft is headquartered in Reston, Virginia. www.electrosoft-inc.com.