authenticate 2024
THE FIDO CONFERENCE

A Shared Services Model to Promote Rapid Adoption of FIDO2 Within Federal Government!

Dr. Sarbari Gupta, CISSP, CISA
Founder & CEO, Electrosoft

Signature Sponsors:

cisco | Microsoft | yubico | Google

authenticatecon.com

Agenda

- Current Landscape for Federal Identity
- Challenges with FIDO2 Adoption for Federal Enterprise Users
- Proposed FIDO2 Shared Services Solution
  - Approach
  - Operations
- Wrap-Up

Current Landscape for Federal Identity

Digital Authentication of Federal Enterprise Users

Source: fedidcard.gov

- **Federal Enterprise Users (Employees and Contractors) are mandated to authenticate using PIV Cards (or DoD CACs)**
  - **Smart Card that includes PKI Credentials (FIPS 201)**
  - **Trust based on Federal PKI (FPKI) Trust & Governance**
- **NIST SP 800-157 (2014) introduced concept of Derived PIV Credentials for mobile platforms**
  - **Additional PKI Credentials issued under FPKI Trust**
- **OMB M-19-17 (2020) opened the door for:**
  - **"additional solutions (e.g., different authenticators) that meet the intent of HSPD-12"**
  - **Non-PKI Authenticators**
- **NIST SP 800-157r1 (2023) introduced non-PKI Derived Credentials**
  - **FIDO2 is a very good fit - but additional requirements apply!**

Derived FIDO2 Credentials (DFC)

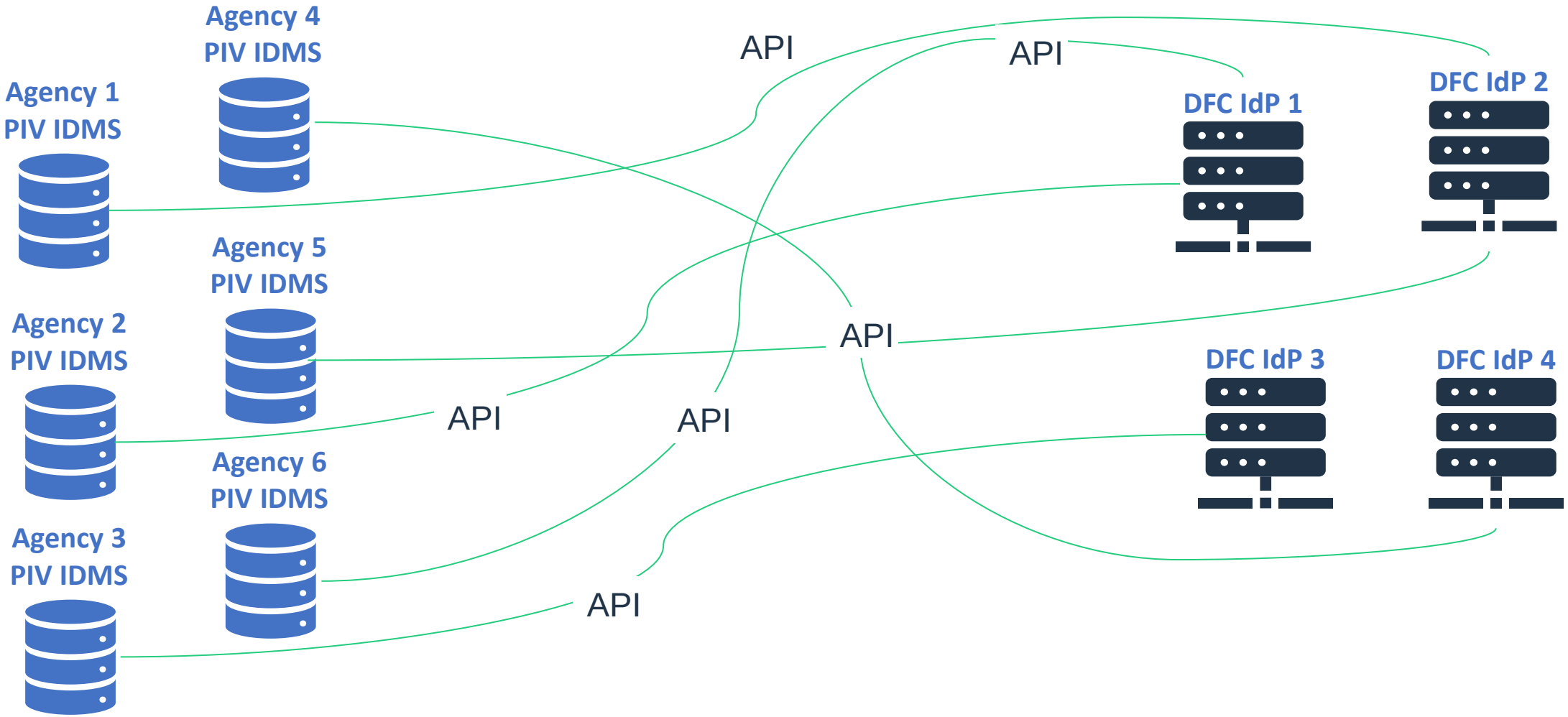
- **What are Derived FIDO2 Credentials?**
  - FIDO2 Authenticators for Federal Enterprise Users
  - Issued to PIV/CAC holders as Derived PIV Credentials
  - Embodies the combined strengths of PIV and FIDO2
- **DFC Requirements from NIST SP 800-157r1 (2023)**
  - Issued by Agency that issued the PIV Card to the User
  - Requires User to authenticate with their PIV Card
  - Needs to be “bound” to the PIV Identity Account for the User
  - Used in a federation model with Relying Parties (RPs)
  - Lifecycle managed as part of the PIV Identity Account
    - Terminated when the PIV Identity Account is terminated
- ***New APIs needed for FIDO2 Identity Providers (IdPs) to connect to Agency Identity Management System (IDMS)!***

Challenges with FIDO2 Adoption for Federal Enterprise Users

Technical Challenges

- **Difficult to Operate in Compliance with Federal Policy**
  - NIST SP 800-157 r1 requirements need to be met
  - New APIs needed to interact with Agency Identity Management System (IDMS)
- **Stovepipe Agency Implementations**
  - Proprietary APIs to IDMS
  - Can lead to proliferation of APIs
- **Significant Infrastructure Changes**
  - Agency-specific DFC Implementations Complex

Proliferation of Proprietary APIs to Agency IDMS



IDMS – Identity Management System
DFC IdP – Derived FIDO2 Credential Identity Provider

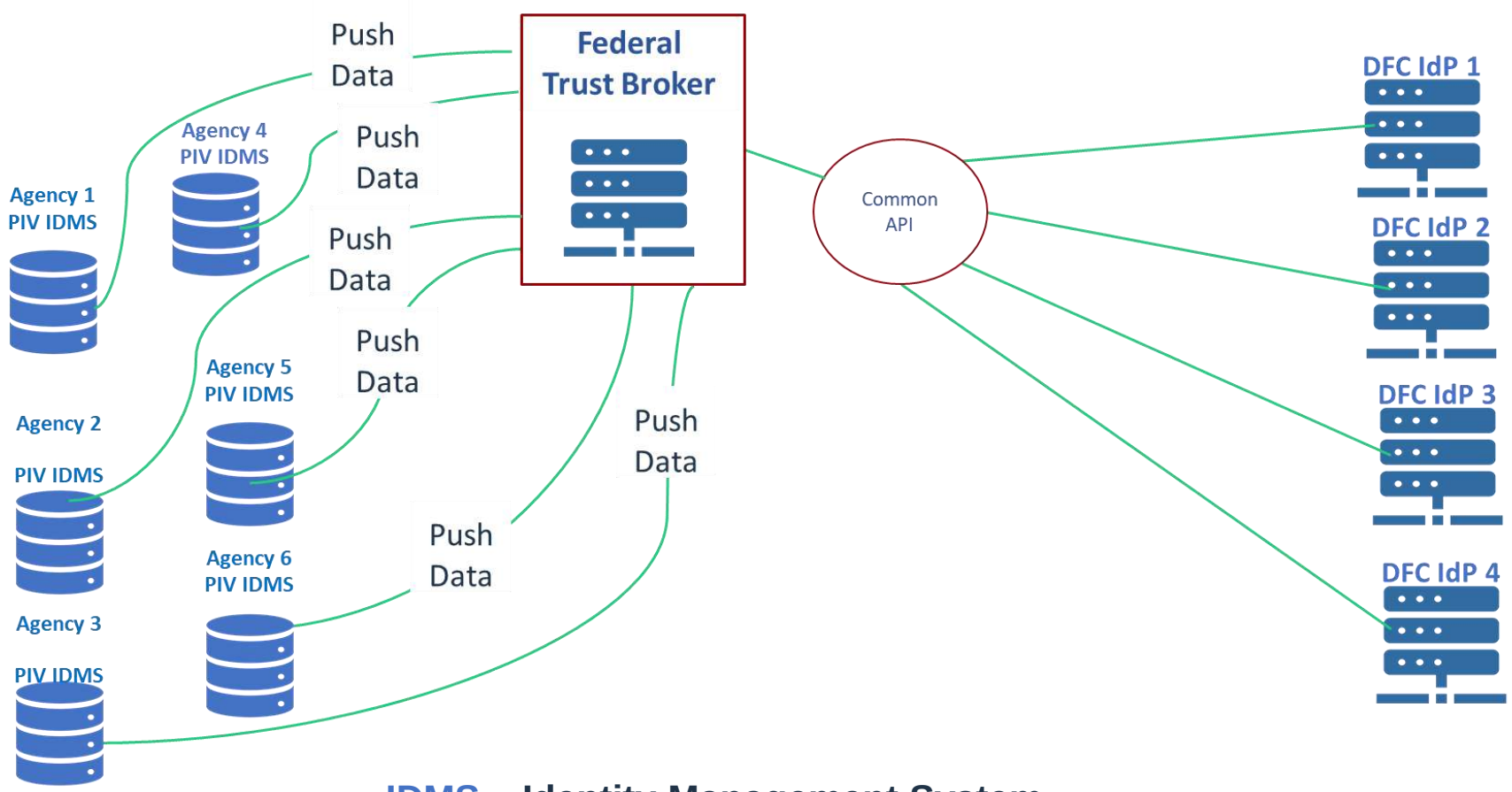
Business Challenges

- **Lack of Governance**
  - Vetting of FIDO2 Products/Services for Federal Use as DFCs
  - Oversight of Compliant DFC Operations
- **High Cost**
  - Agency-specific DFC Implementations Costly
  - Compliant DFC O&M Costly
- **Possible Vendor Lock-In**
  - Potential Lock-in with FIDO2 Vendor/Service or Integrator due to proprietary API to IDMS

Proposed FIDO2 Shared Services Solution – Approach

FIDO2/DFC Shared Services – Concept

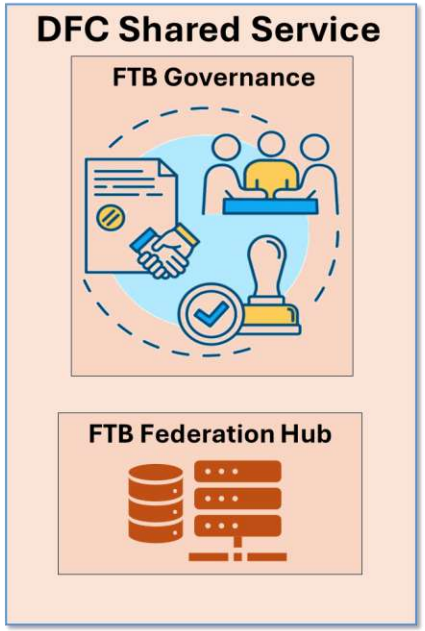
- **Centralized Federal Trust Broker (FTB)**
  - Sits between DFC Identity Providers and Agency IDMS
  - Provides DFC lifecycle management
- **Common API**
  - Standardized interface for all DFC identity providers
- **DFC IdPs**
  - FIDO2 Providers compliant with DFC requirements
  - Pre-approved through vetting by FTB

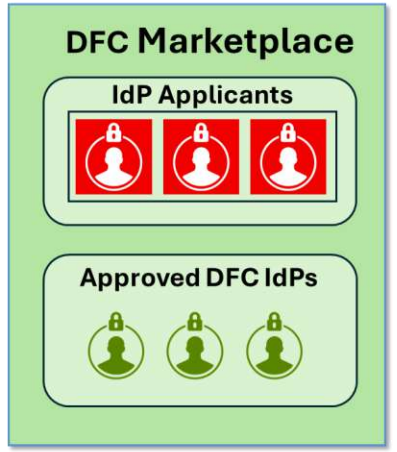


IDMS – Identity Management System
FTB –Federal Trust Broker
DFC IdP – Derived FIDO2 Credential Identity Provider

FIDO2/DFC Shared Services – Components

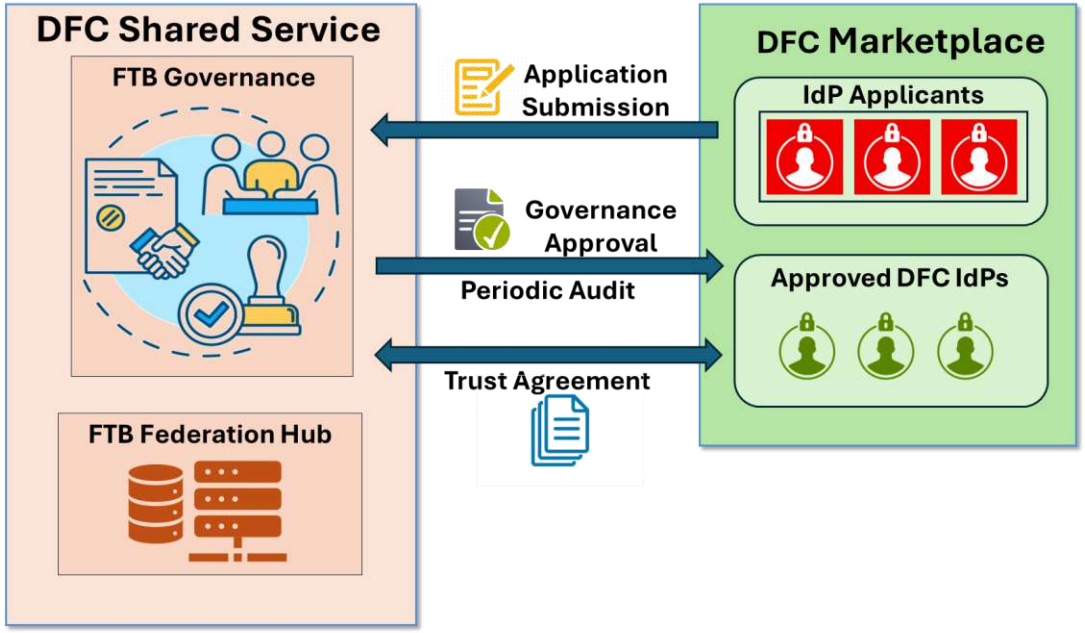
- **DFC Shared Service**
  - Federal Trust Broker (FTB) Governance
  - FTB Federation Hub (FedHub)
- **DFC Marketplace**
  - FIDO2 Identity Providers capable of issuing DFCs
    - Applicants
    - Approved DFC IdPs
- **Federal Agency Customers**
  - Interested in DFC Shared Services





Proposed FIDO2 Shared Services Solution – Operations

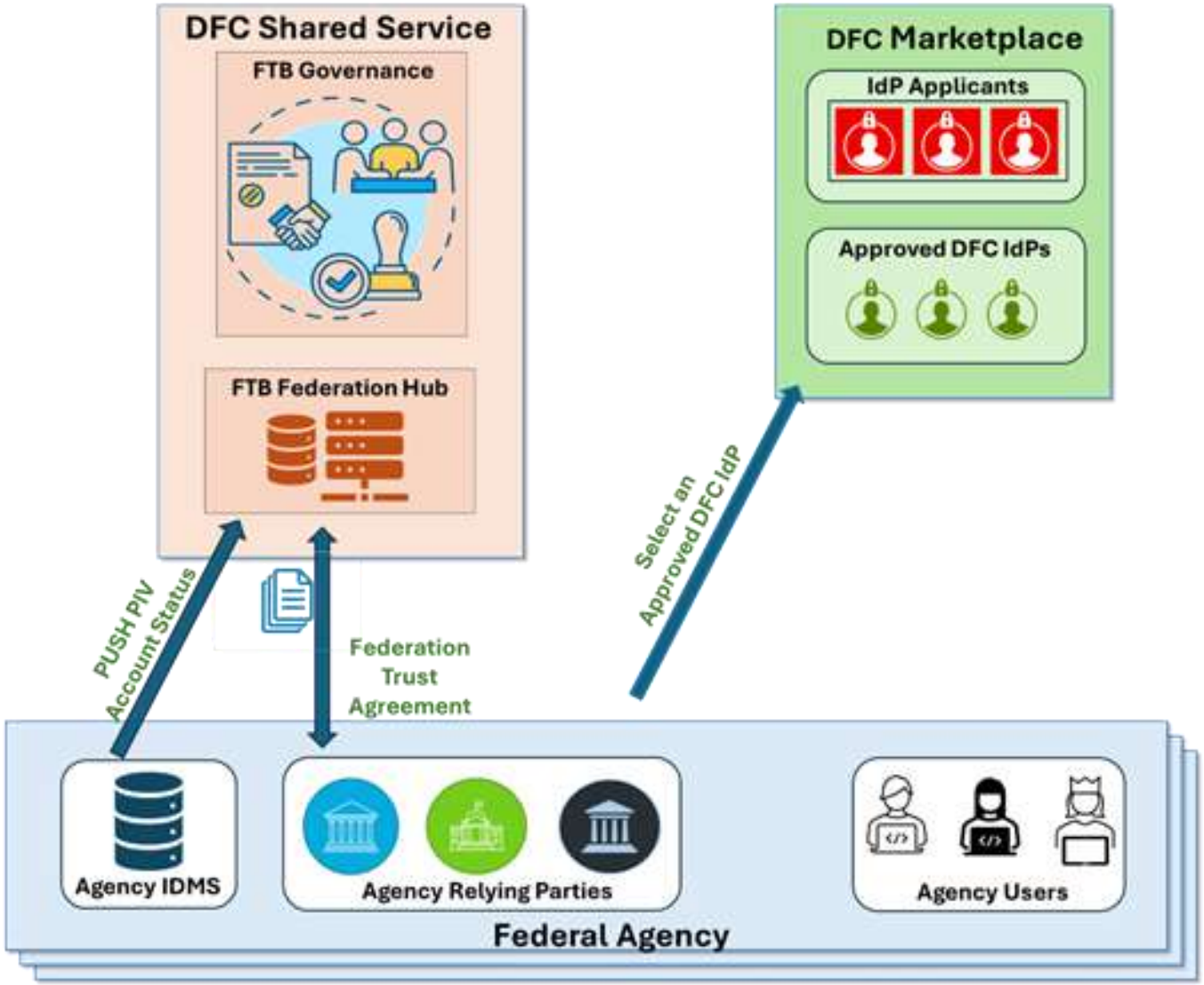
Establishing/Maintaining the DFC Marketplace



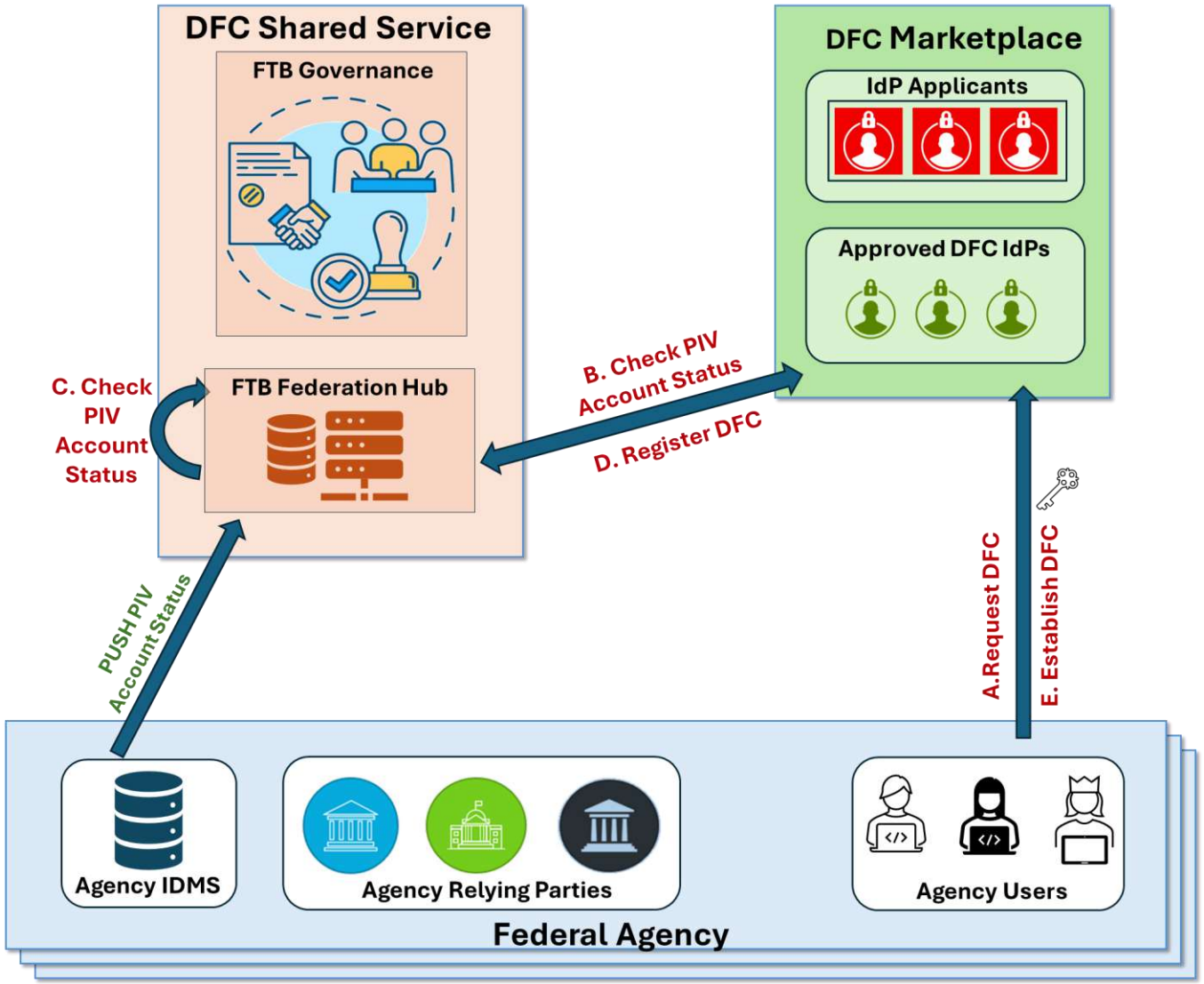
- FIDO2 IdP Applies for Approval
- FTB Governance Vets and Approves IdP for:
  - Compliance with NIST reqts
  - Support for Common API
- Pairwise Trust Agreements established between:
  - FTB FedHub
  - Approved DFC IdP
- Periodic Audits of Approved DFC IdPs

Federal Agency Engagement with DFC Shared Services

- Select an Approved IdP
- Set up Federation Trust Agreement with DFC Federation Hub
- Set up Daily Push of PIV Account Status to FTB



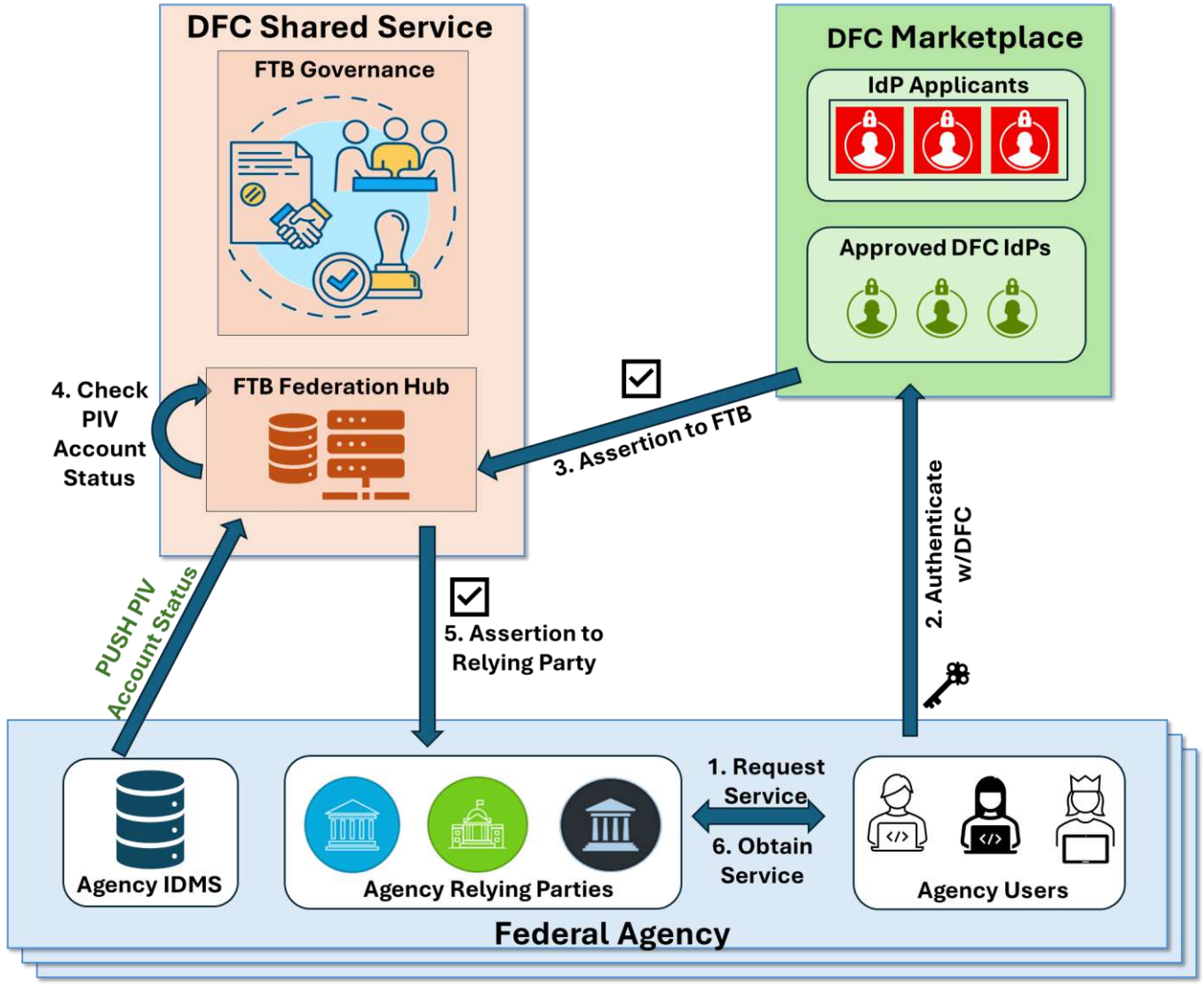
DFC Issuance to Agency User



- Agency User gets link to selected DFC IdP
- User Requests new DFC
  - Authenticates using PIV/CAC
- DFC IDP checks status of User's PIV Account
  - Using Common API
- DFC IdP issues new DFC
- DFC IdP registers new DFC against User's Account
  - Using Common API

DFC Authentication by User to obtain RP Services

- User Requests RP Service
  - Redirected to DFC IdP
- User Authenticates with DFC
- DFC IdP sends Assertion to FTB FedHub
- FTB FedHub checks Users PIV status
  - Using Common API
- FTB FedHub sends assertion to RP
- RP offers service to User



Wrap-Up

Advantages of the FIDO2/DFC Shared Services Model

- **Security**: Phishing-resistant, passwordless authentication
- **Scalability**: Easily onboard agencies and FIDO2 identity providers
- **Cost Efficiency**: Reduces IT costs by sharing infrastructure across agencies
- **Interoperability**: Cross-platform use on both traditional and mobile devices
- **Compliance**: Alignment with FIPS 201-3 and SP 800-157r1

Positive Feedback and Iterative Development

- **Work in Progress since early 2023**
  - In support of the General Services Administration (GSA) Office of Governmentwide Policy (OGP)
  - Seeking ways to accelerate FIDO2 adoption within Federal Enterprise
- **Extensive Stakeholder Engagement**
  - Multiple Government and industry consultations over the past year
- **Iterative Refinement**
  - Feedback led to improved architecture and operational readiness
- **Ongoing discussions on Responsible Parties**
  - Agencies that can/will take on governance and technical operations

Summary

- **Key Takeaways:**
  - FIDO2 is a strong, scalable, and secure authentication standard
  - The shared services model simplifies FIDO2 adoption for Federal Agencies
  - Agencies benefit from enhanced security, compliance, flexibility, and cost savings
- **Call to Action:**
  - Federal agencies are encouraged to explore the FIDO2 shared services model for phishing-resistant authentication

authenticate 2024

THE FIDO CONFERENCE

Thank you

Signature Sponsors:

cisco | Microsoft | yubico | Google

authenticatecon.com