authenticate 2023

THE FIDO CONFERENCE

Leveraging Passkeys for a Federated Federal Government Environment

Dr. Sarbari Gupta, CISSP, CISA

CEO, Electrosoft

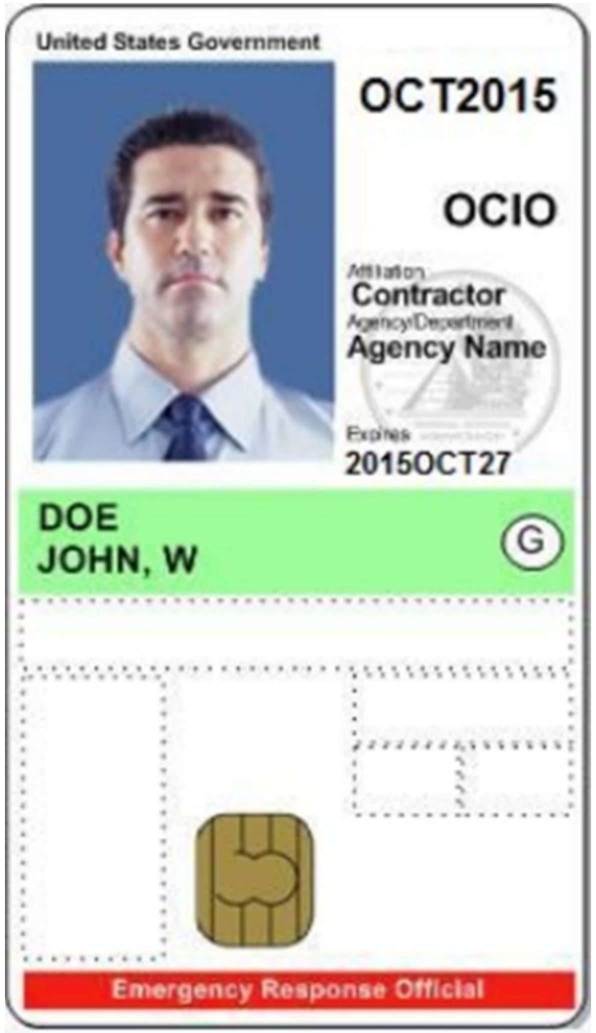
Agenda

- **Fundamentals**
  - PIV and Derived PIV
  - FIDO2/Passkey
- **Federated Solution Models**
  - **Model #1: Agency as DPP Issuer**
  - **Model #2: Outsource DPP IdP to Vendor**
  - **Model #3: Federal Trust Broker (FTB)**
- **Summary**

Fundamentals – PIV, Derived PIV and FIDO2/Passkey

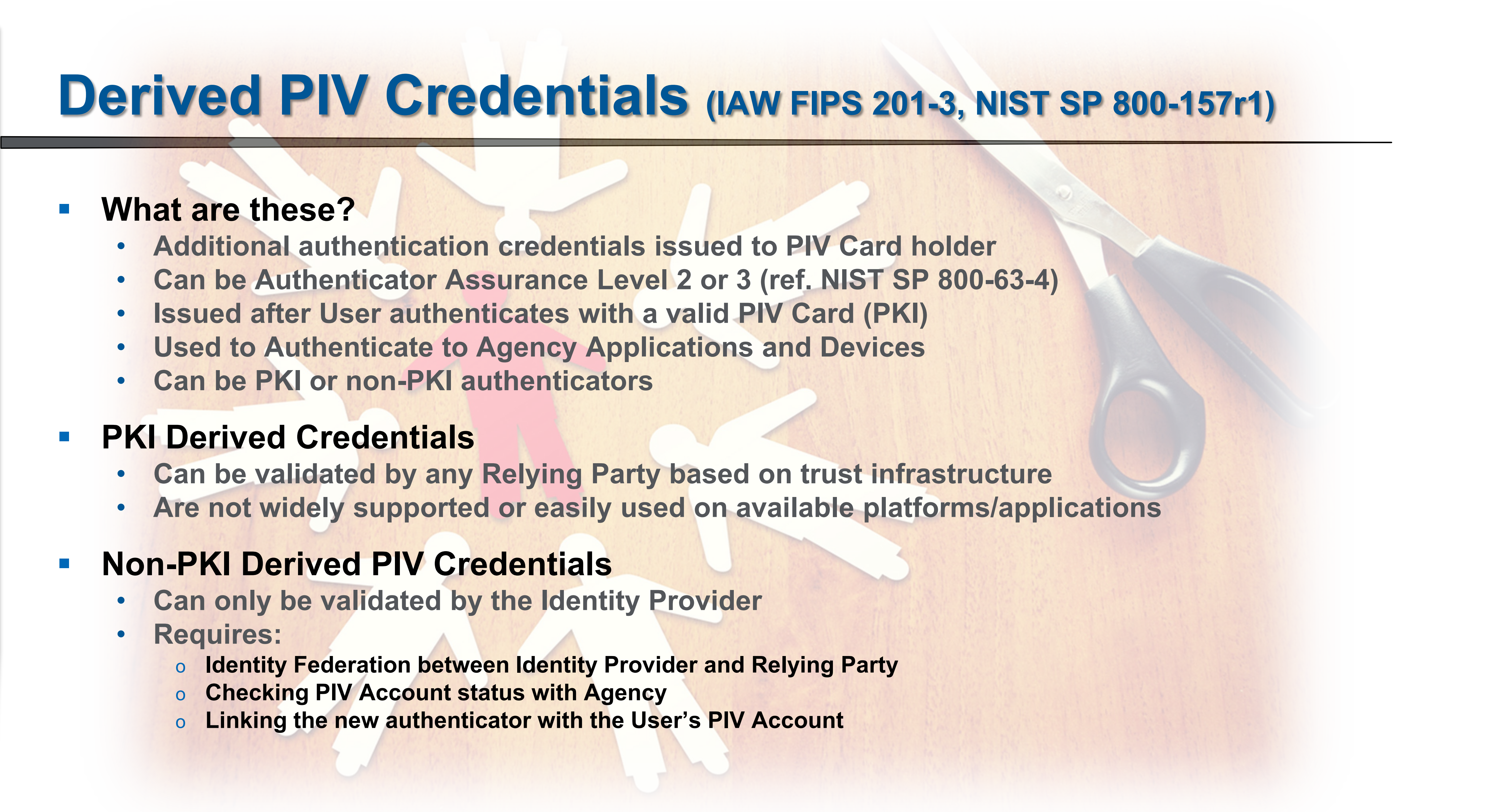
Personal Verification Card (PIV) Card

- **US Federal Government Smart Card Identity**
  - Based on FIPS 201 Standard
- **Includes:**
  - 4 PKI credentials
  - Biometrics (fingerprints, facial image)
  - Activation with PIN or biometric
- **Strengths:**
  - Rigorous Identity Proofing and Vetting
  - Strong Lifecycle Management of PIV Credentials
  - Strong Form Factor
  - Phishing Resistant
- **Drawbacks (for Online Authentication):**
  - Requires card readers
  - PKI credentials not user-friendly



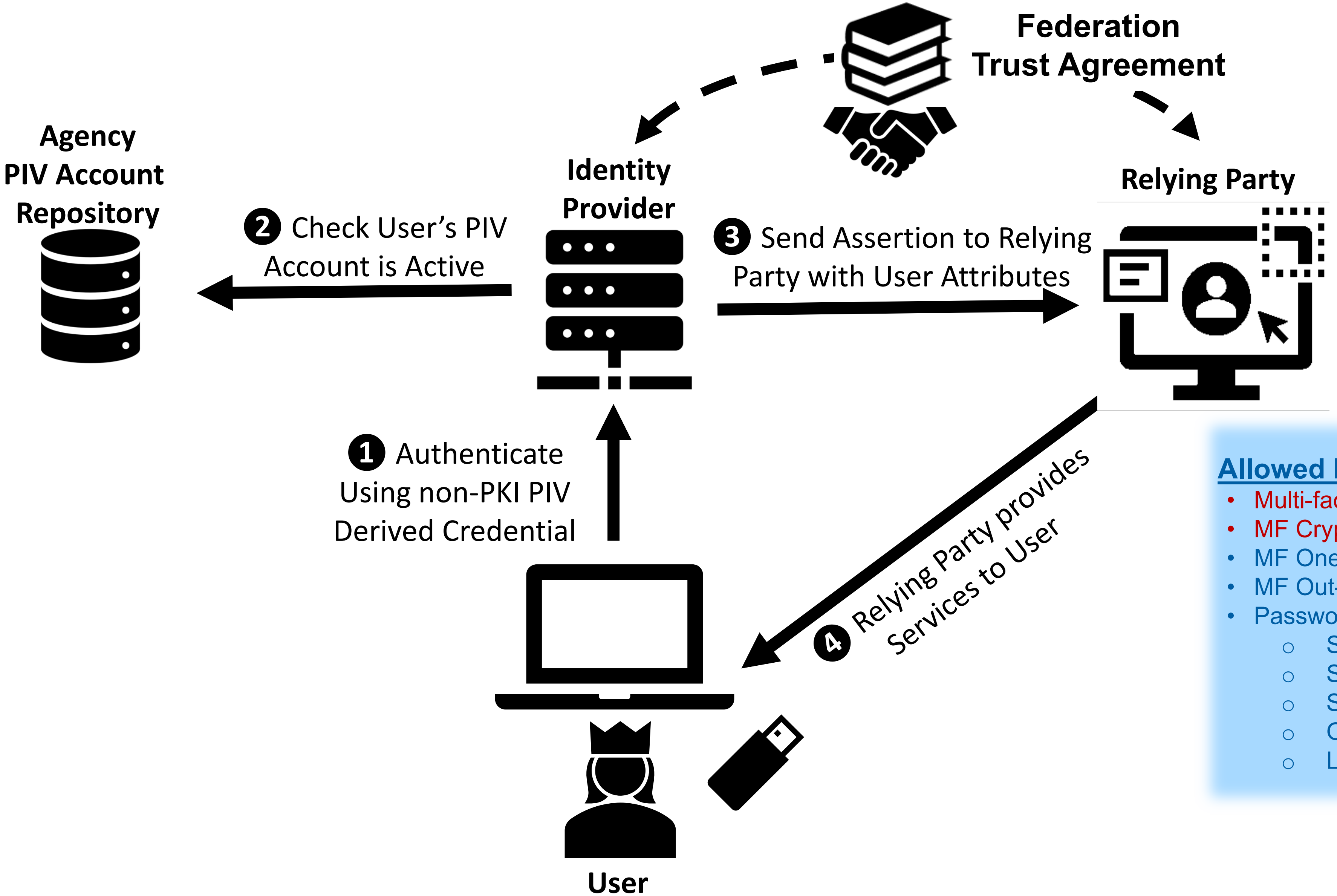
Source: fedidcard.gov

Derived PIV Credentials (IAW FIPS 201-3, NIST SP 800-157r1)



- **What are these?**
  - Additional authentication credentials issued to PIV Card holder
  - Can be Authenticator Assurance Level 2 or 3 (ref. NIST SP 800-63-4)
  - Issued after User authenticates with a valid PIV Card (PKI)
  - Used to Authenticate to Agency Applications and Devices
  - Can be PKI or non-PKI authenticators
- **PKI Derived Credentials**
  - Can be validated by any Relying Party based on trust infrastructure
  - Are not widely supported or easily used on available platforms/applications
- **Non-PKI Derived PIV Credentials**
  - Can only be validated by the Identity Provider
  - Requires:
    - Identity Federation between Identity Provider and Relying Party
    - Checking PIV Account status with Agency
    - Linking the new authenticator with the User’s PIV Account

Identity Federation for Non-PKI Derived PIV Credentials



Federation Trust Agreement

Agency PIV Account Repository

Identity Provider

Relying Party

User

❶ Authenticate Using non-PKI PIV Derived Credential

❷ Check User's PIV Account is Active

❸ Send Assertion to Relying Party with User Attributes

❹ Relying Party provides Services to User

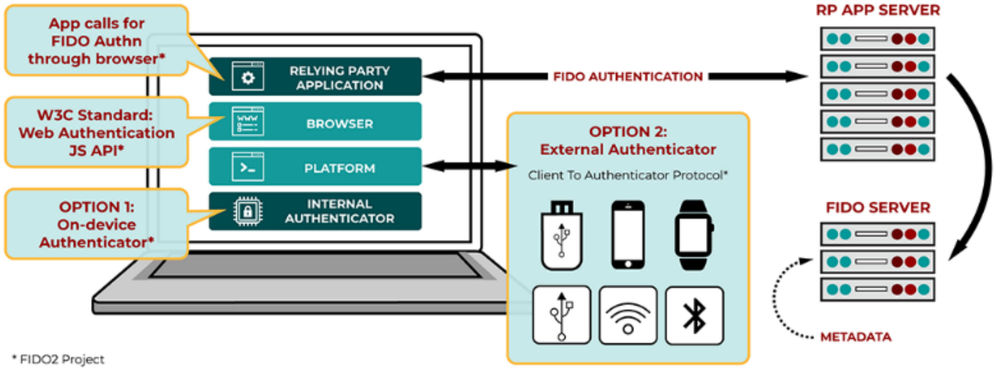
Allowed Non-PKI Derived PIV Credentials

- Multi-factor (MF) Cryptographic Device
- MF Cryptographic Software
- MF One-Time-Password (OTP) Device
- MF Out-Of-Band (OOB) Authenticator
- Password Plus:
  - Single Factor (SF) Cryptographic Device
  - SF Cryptographic Software
  - SF OTP Device
  - OOB Device
  - Look-Up Secret

FIDO2/Passkey

- **What is it?**
  - Non-PKI Authenticators based on FIDO2 Standards (WebAuthn and CTAP2)
  - Pairwise Asymmetric Crypto Key Pair between User and Service Provider
  - Multifactor Authenticator unlocked with local biometric or PIN

- **Strengths**
  - Phishing resistant, Multi-factor Authenticator
  - Intuitive, user-friendly interfaces
  - Available on leading browsers and platforms
  - Supports authenticator synchronization
  - Supports cross-platform use


App calls for FIDO Authn through browser*
W3C Standard: Web Authentication JS API*
OPTION 1: On-device Authenticator*
RELYING PARTY APPLICATION
BROWSER
PLATFORM
INTERNAL AUTHENTICATOR
FIDO AUTHENTICATION
OPTION 2: External Authenticator
Client To Authenticator Protocol*
RP APP SERVER
FIDO SERVER
METADATA
* FIDO2 Project

Courtesy fidoalliance.org

- **Drawbacks**
  - Does not address identity proofing/vetting prior to issuance
  - Does not address authenticator lifecycle management

Derived PIV Passkeys (DPP)

- **What are DPPs:**
  - Passkeys issued as Derived PIV Credentials
    - May be Device-Bound Passkeys or Synched Passkeys (based on use case)
  - Embodies the combined strengths of PIV and Passkeys

- **DPP Requirements (from NIST SP 800-157r1)**
  - 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

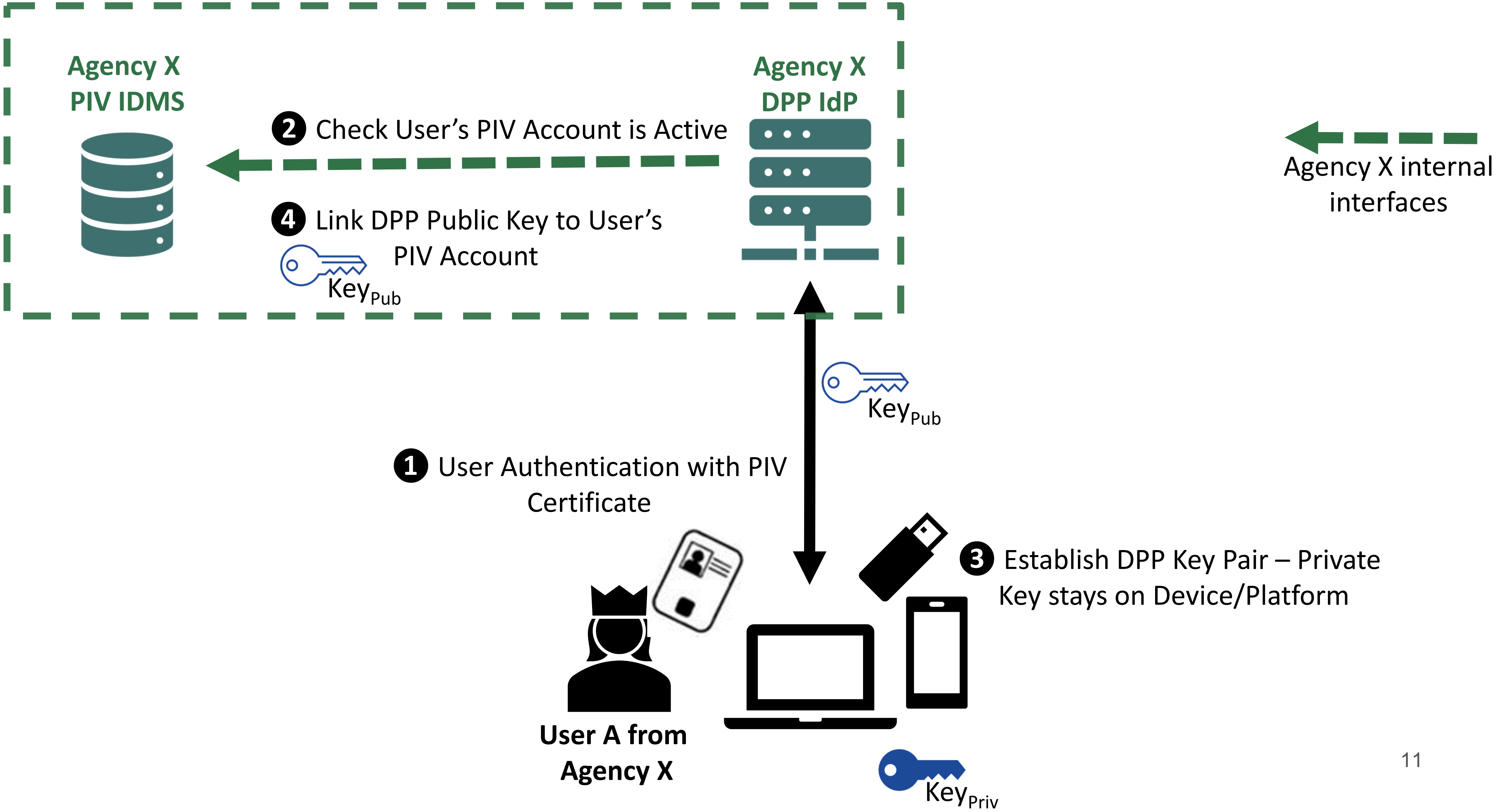
Federated Solution Models

authenticate

Model #1: Agency as DPP Issuer

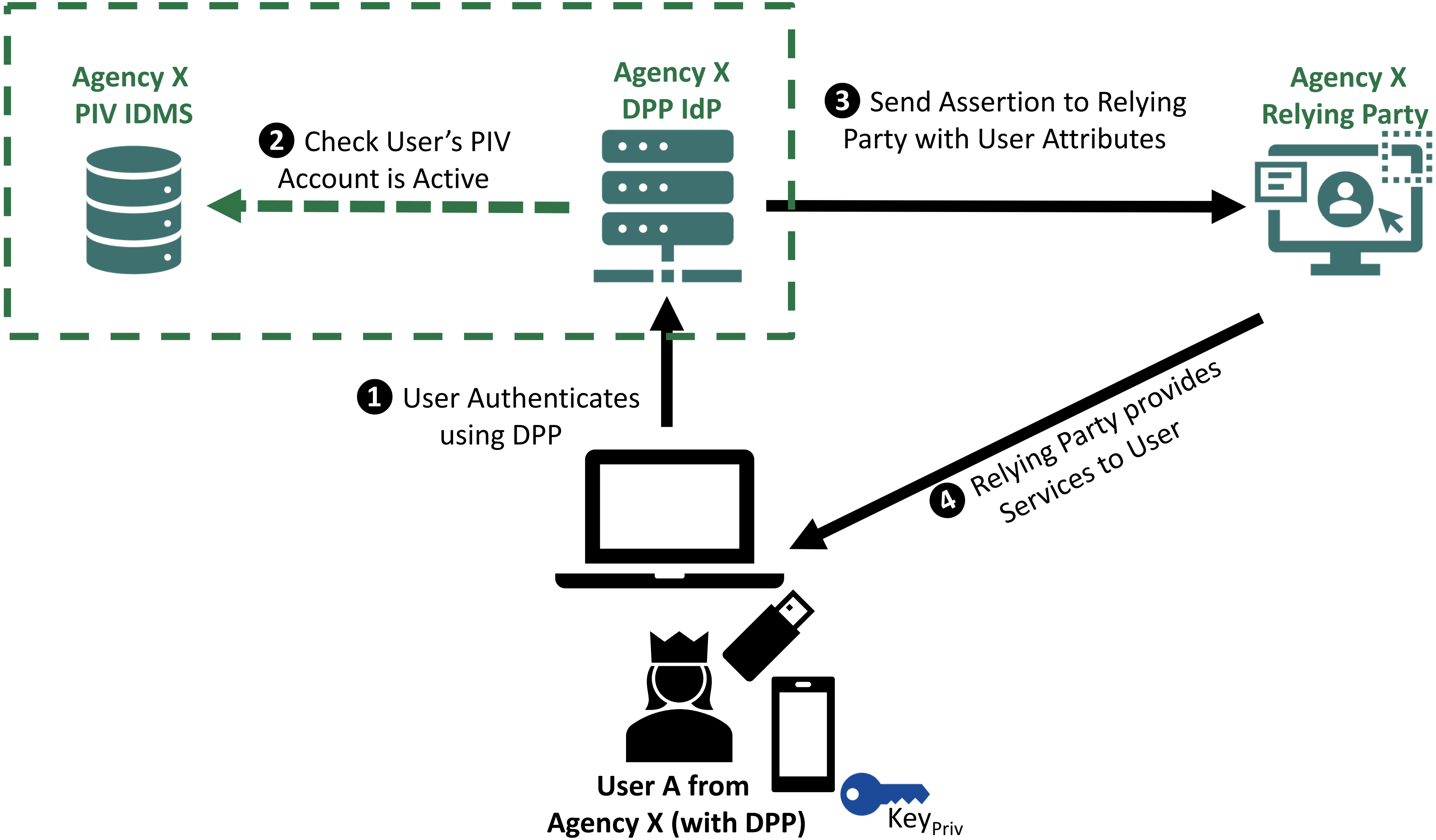
- Agency issues DPP to User following:
  - Successful PIV Card Authentication
  - PIV Account active status check
- DPP used in Identity Federation environment
  - Agency Identity Provider (IdP) – Issues and Verifies DPPs
  - Agency Relying Parties (RPs) – Accepts assertions from IdP
- New DPP issued to User linked to User’s PIV Account
- DPP lifecycle managed as part of User’s PIV Account

Model #1: DPP Issuance



Agency X
PIV IDMS
Agency X
DPP IdP
❷ Check User's PIV Account is Active
❹ Link DPP Public Key to User's PIV Account
Key$_{Pub}$
Agency X internal interfaces
Key$_{Pub}$
❶ User Authentication with PIV Certificate
❸ Establish DPP Key Pair – Private Key stays on Device/Platform
User A from Agency X
Key$_{Priv}$

Model #1: DPP Authentication & Assertion


Agency X
PIV IDMS
❷ Check User's PIV Account is Active
Agency X
DPP IdP
❸ Send Assertion to Relying Party with User Attributes
Agency X
Relying Party
❶ User Authenticates using DPP
❹ Relying Party provides Services to User
User A from Agency X (with DPP)
Key_{Priv}

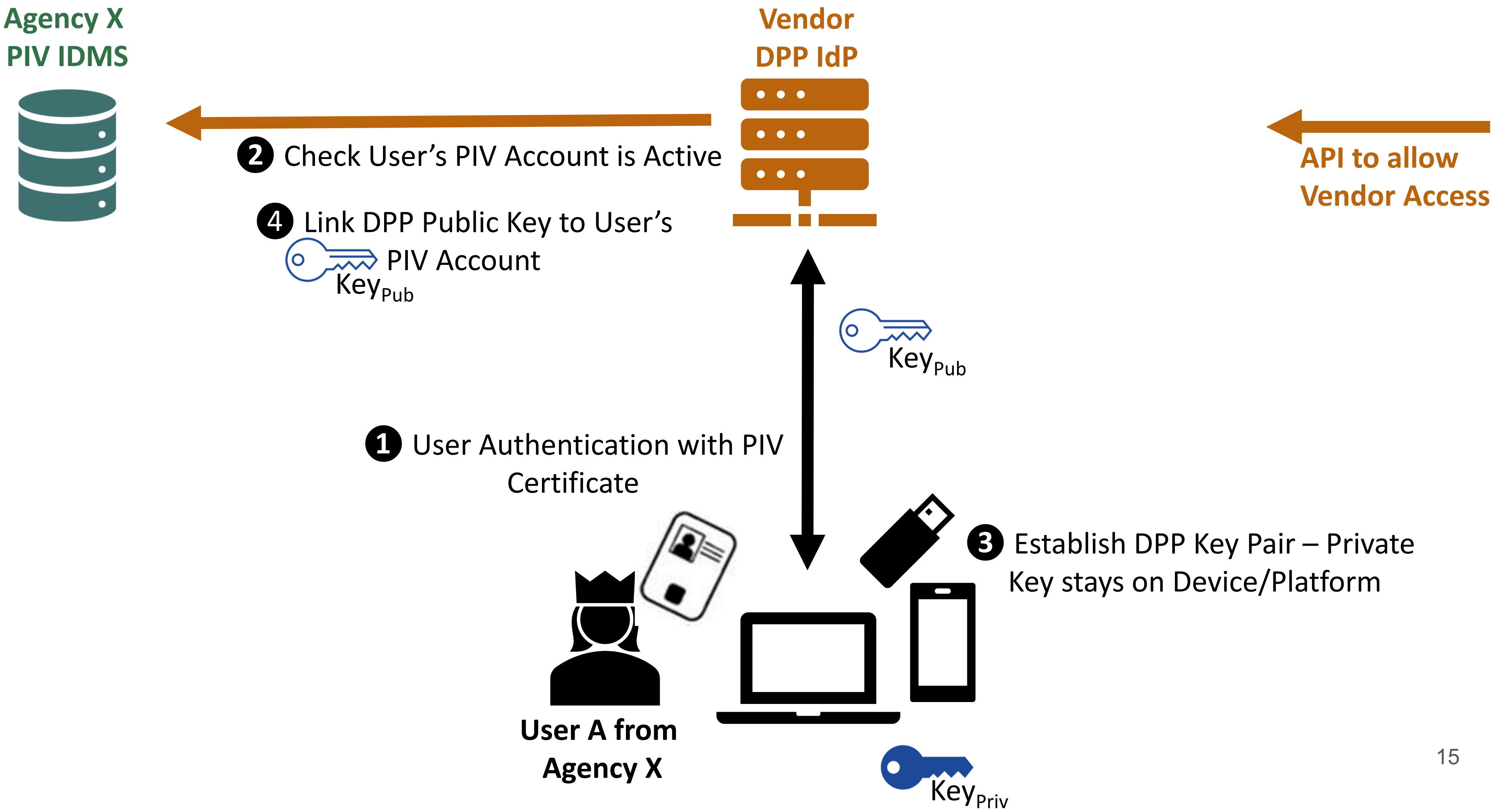
Model #1: Benefits/Drawbacks

- **Benefits**
  - Federation Trust Agreements simple
    - Between Agency IdP and Agency RPs
  - IdP has access to Agency PIV IDMS through internal interfaces
- **Drawbacks**
  - Introduces complexity to Agency Identity Solutions
  - Agency has O&M responsibility of DPP IdP

Model #2: Outsource DPP IdP to Vendor

- **Agency engages Vendor to provide DPP IdP function**
- **Formal Trust Agreements need to be set up**
  - Between Outsourced DPP IdP and Agency RPs
- **Vendor issues DPP to Agency Users**
  - Following authentication with PIV Card and PIV Account Check
- **DPP used in identity federation environment**
  - Outsourced Identity Provider (IdP) – Issues and Verifies DPPs
  - Agency Relying Parties (RPs) – Accepts assertions from IdP
- **Vendor needs API access to Agency PIV IDMS:**
  - Check PIV Account status for User
  - Link DPP to User's PIV Account

Model #2: DPP Issuance



Agency X PIV IDMS

Vendor DPP IdP

API to allow Vendor Access

❷ Check User's PIV Account is Active

❹ Link DPP Public Key to User's PIV Account

Key$_{Pub}$

Key$_{Pub}$

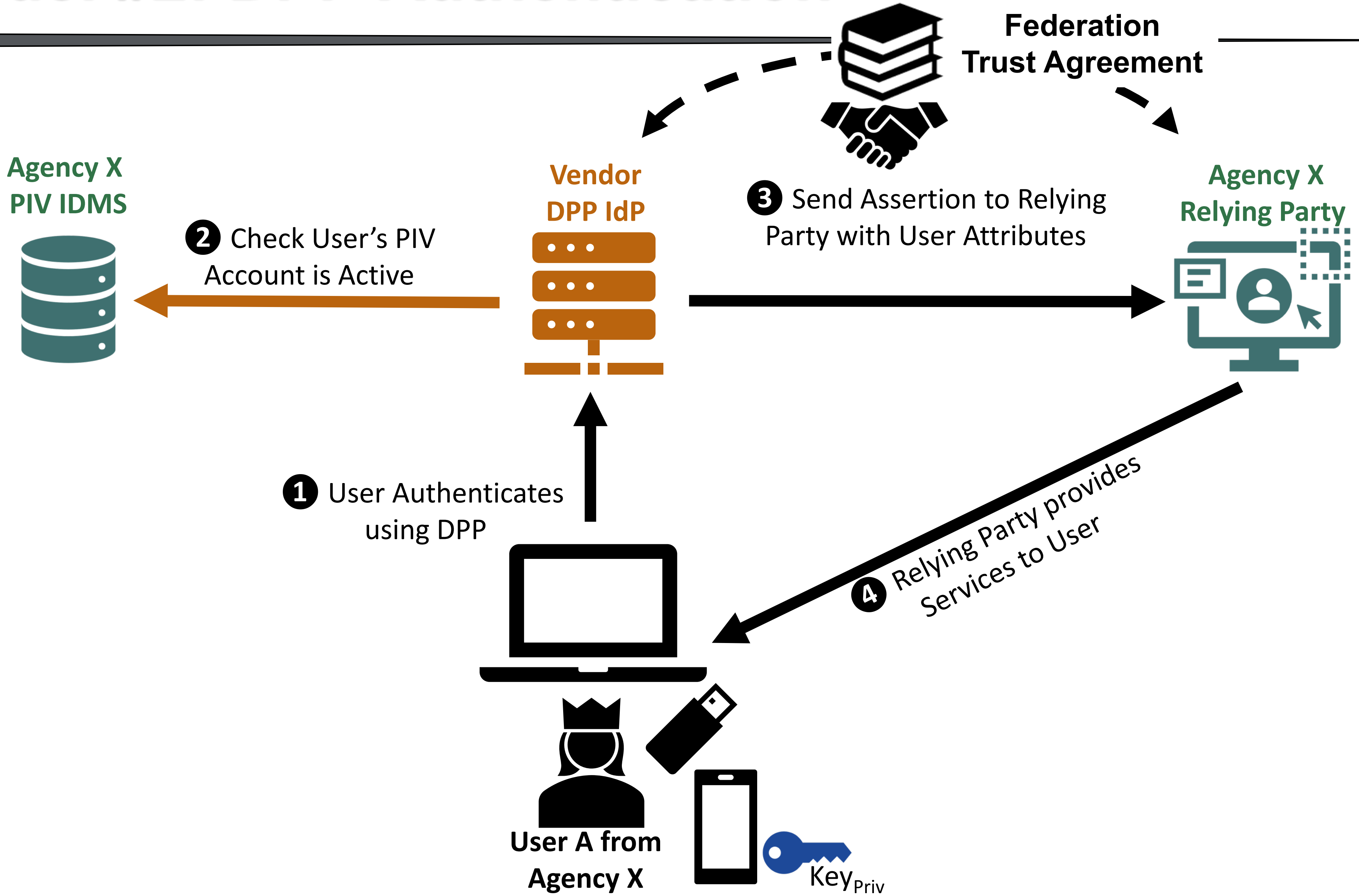
❶ User Authentication with PIV Certificate

❸ Establish DPP Key Pair – Private Key stays on Device/Platform

User A from Agency X

Key$_{Priv}$

Model #2: DPP Authentication



Federation Trust Agreement

Agency X PIV IDMS

Vendor DPP IdP

Agency X Relying Party

❷ Check User's PIV Account is Active

❸ Send Assertion to Relying Party with User Attributes

❶ User Authenticates using DPP

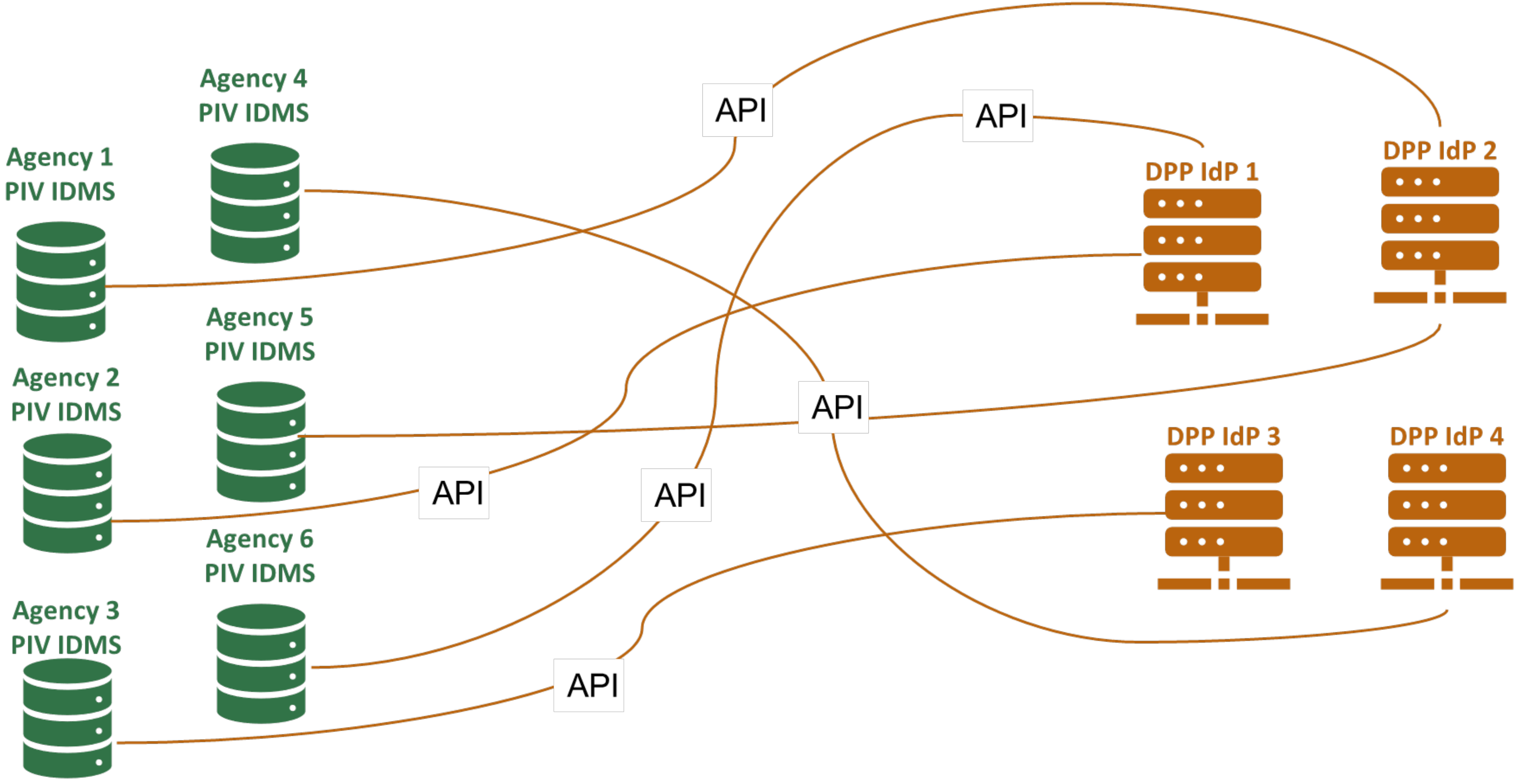
❹ Relying Party provides Services to User

User A from Agency X

Model #2: Benefits/Drawbacks

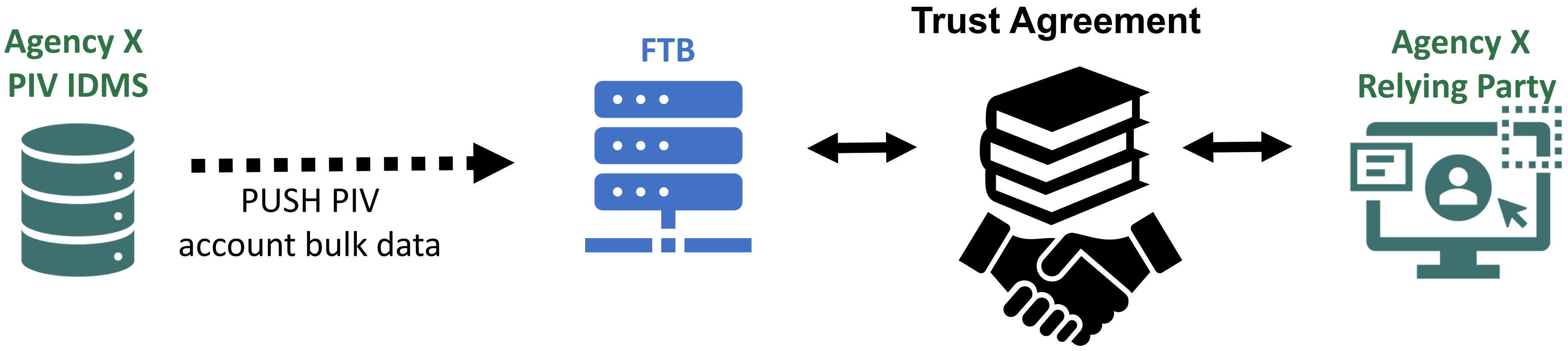
- **Benefits**
  - **Agency outsources**
    - **Complexity of federation**
    - **Complexity of FIDO2 issuance**
    - **O&M responsibility of DPP IdP**
- **Drawbacks**
  - **Federation Trust Agreements more complex**
    - **Between Vendor DPP IdP and Agency RPs**
  - **Special APIs needed to provide Vendor access to Agency PIV Repository**
  - **Creates spaghetti connections between Agencies and Vendors if DPPs are implemented widely**

Model #2 – Potential Scenario in Federal Government

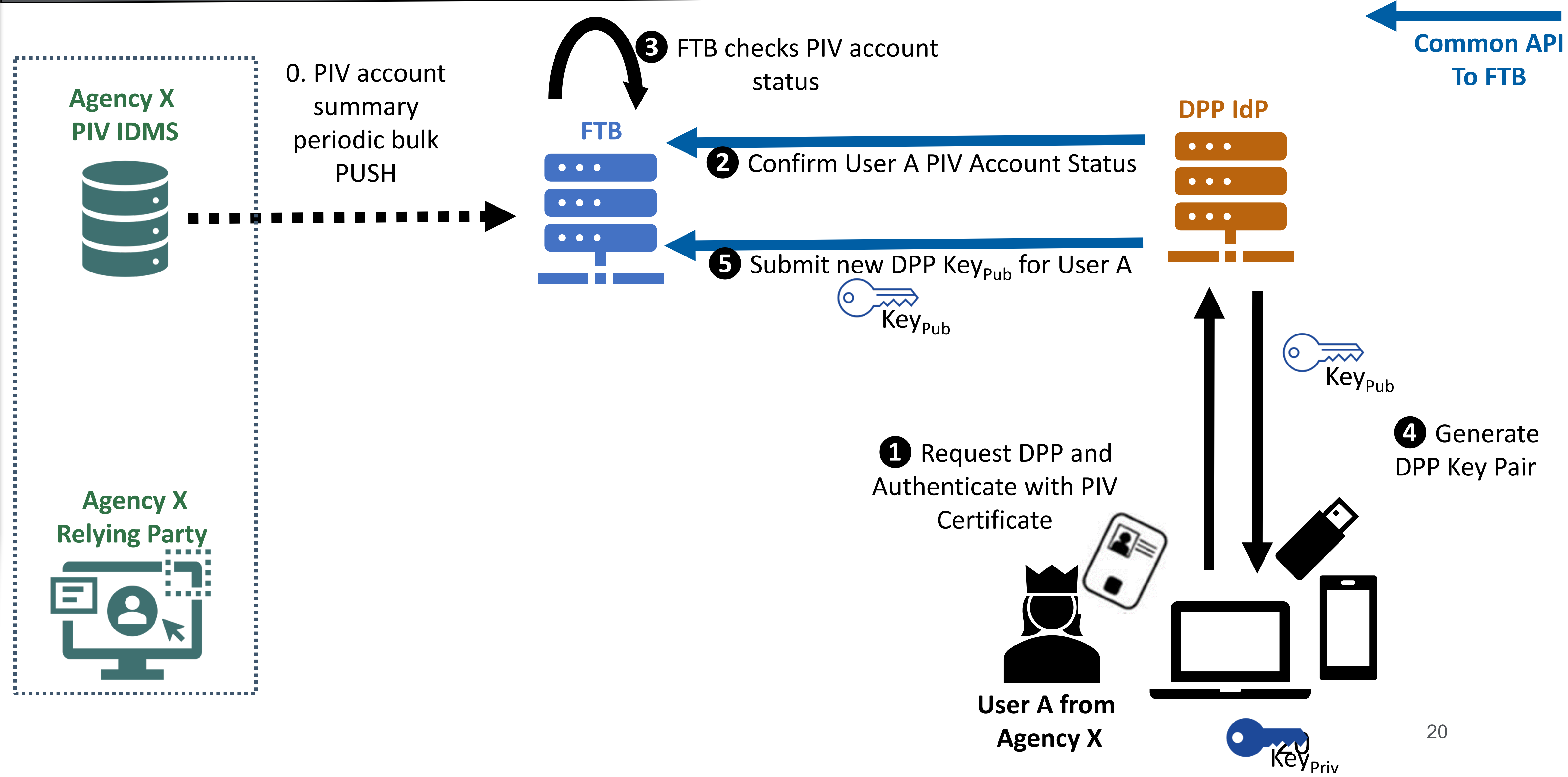


Model #3: Federal Trust Broker (FTB)

- FTB acts as Trusted Intermediary and Vetting Agent
  - Between Agency PIV IDMS to Vendor DPP IdPs
- Agency X Setup to use FTB:
  - Selects an approved Vendor as their DPP IdP
  - Agrees to PUSH PIV Account bulk data to FTB periodically
  - Establishes Identity Federation Trust Agreement
    - Between Agency X Relying Parties and FTB



Model #3: DPP Issuance



Agency X PIV IDMS

0. PIV account summary periodic bulk PUSH

FTB

3 FTB checks PIV account status

Common API To FTB

DPP IdP

2 Confirm User A PIV Account Status

5 Submit new DPP Key_{Pub} for User A

Key_{Pub}

Key_{Pub}

4 Generate DPP Key Pair

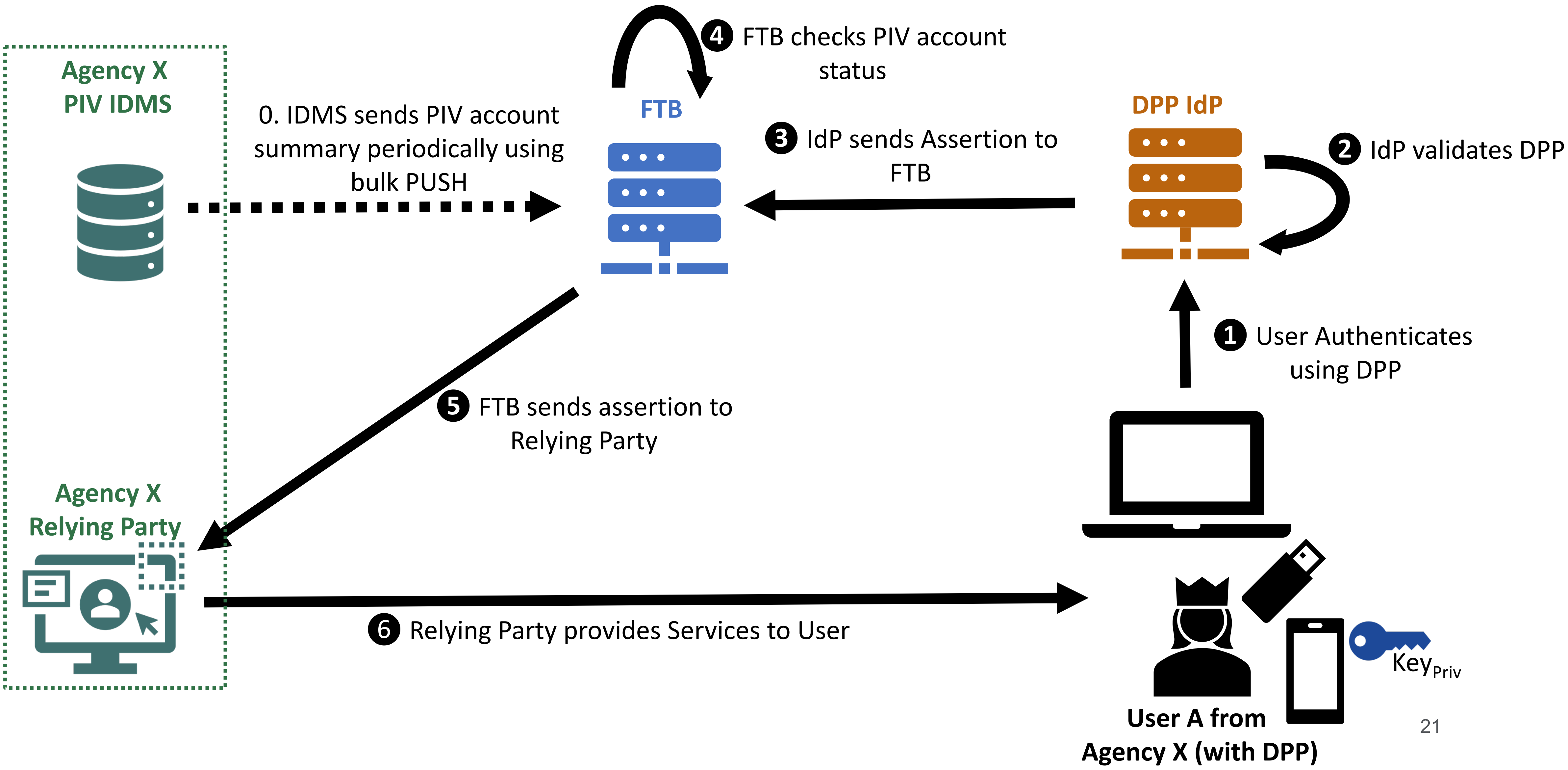
1 Request DPP and Authenticate with PIV Certificate

Agency X Relying Party

User A from Agency X

Key_{Priv}

Model #3: DPP Authentication



0. IDMS sends PIV account summary periodically using bulk PUSH

1 User Authenticates using DPP

2 IdP validates DPP

3 IdP sends Assertion to FTB

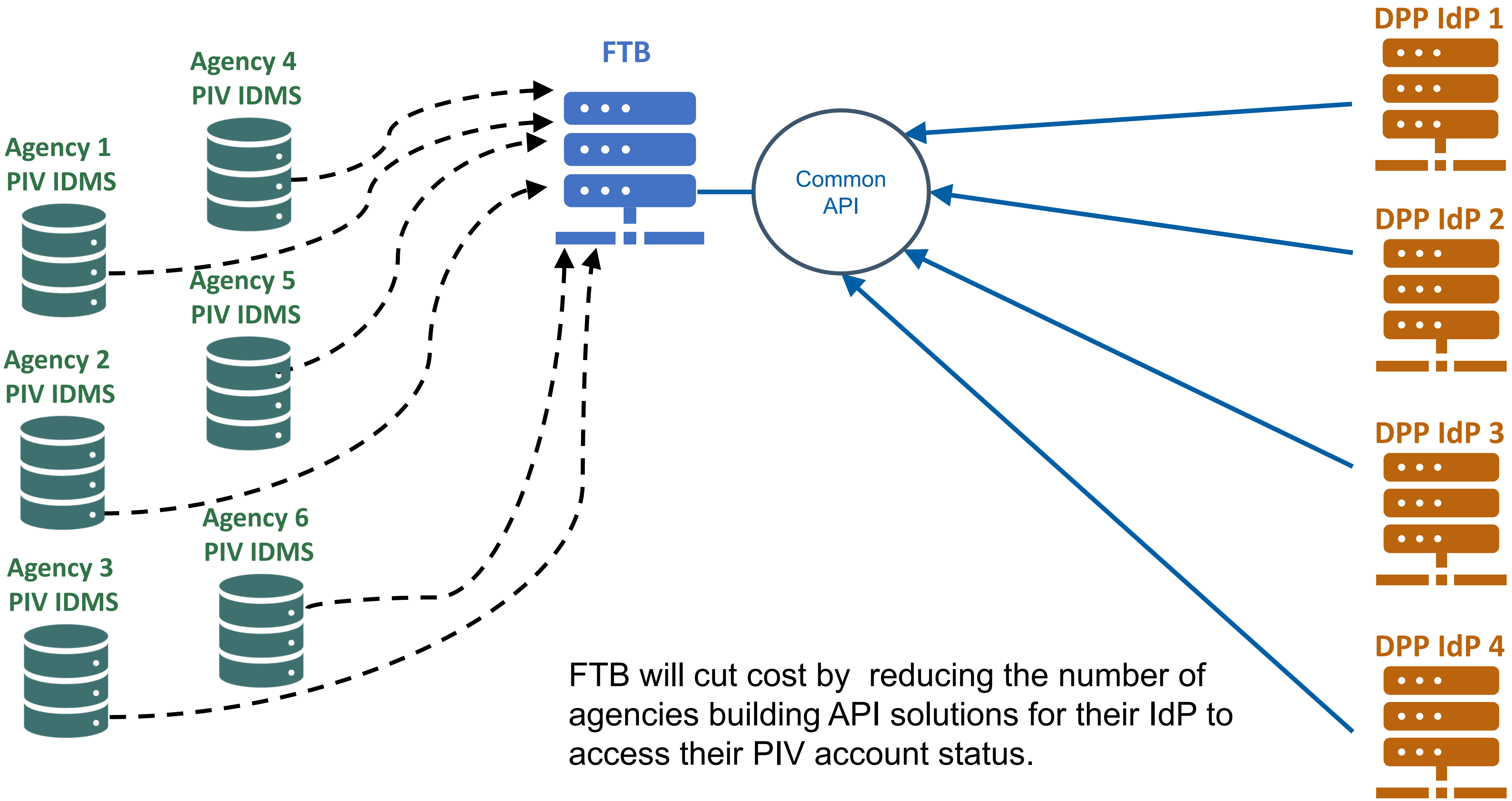
4 FTB checks PIV account status

5 FTB sends assertion to Relying Party

6 Relying Party provides Services to User

User A from Agency X (with DPP)

Model #3: Multi-Agency, Multi-DPP Scenario



FTB will cut cost by reducing the number of agencies building API solutions for their IdP to access their PIV account status.

FTB will allow for agencies to switch to any IdP for derived-credentials.

Model #3: Benefits/Considerations

- **Benefits**
  - Agency outsources DPP Implementation and Operations
  - Vendor IdPs deal with a single entity (FTB) and a *Common API*
  - Agencies establish Trust Agreement with a single (Federal) entity
- **Considerations**
  - Common API has to be developed and maintained
  - FTB has be highly scalable and high performance

Derived PIV Passkeys (DPP) – Summary

- **Combines the strengths of PIV and FIDO2/Passkey**
  - Inherits High assurance identity proofing process from PIV
  - Inherits Lifecycle management processes from PIV
  - Strong, Multi-factor, Phishing Resistant Authenticator
  - Widely supported on IT Platforms and Browsers
  - User-friendly Interfaces
  - Privacy preserving use of biometrics as a 2nd factor

- **Benefits for Agency Users**
  - Easy to use
  - Reduces need to carry PIV Cards
  - Passwordless Reduces Help Desk Calls and Cost
  - Broad support on IT platforms and browsers

- **Multiple Models of Implementation with Pros and Cons**

Contact Information

- Contact Info: Dr. Sarbari Gupta – Electrosoft
  - Email: sarbari@electrosoft-inc.com;
  - Phone: 571-489-6687
  - LinkedIn: https://www.linkedin.com/in/sarbari-gupta/

- Electrosoft
  - Web: http://www.electrosoft-inc.com
  - LinkedIn: https://www.linkedin.com/company/electrosoft/
  - Twitter: https://twitter.com/Electrosoft_Inc
  - HQ: 1893 Metro Center Drive, Suite 228
    Reston VA 20190

authenticate 2023

THE FIDO CONFERENCE

Thank you.

Signature Sponsors:

1Password | Microsoft | yubico | Google

authenticatecon.com