Electrosoft

Results That Drive Mission Success!

Non-PKI Derived Credentials – Implementation Models

IdentityWeek America 2023
Walter E. Washington Convention Center
Washington, DC

October 4, 2023

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
Fax: (703) 437-9452

Agenda

- Fundamentals – Derived PIV and FIDO2
- Implementation Models
- Summary

Electrosoft

Fundamentals – Derived PIV and FIDO2

Electrosoft

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:**
  - Requires card readers
  - PKI credentials not user-friendly

Source: fedidcard.gov

Electrosoft

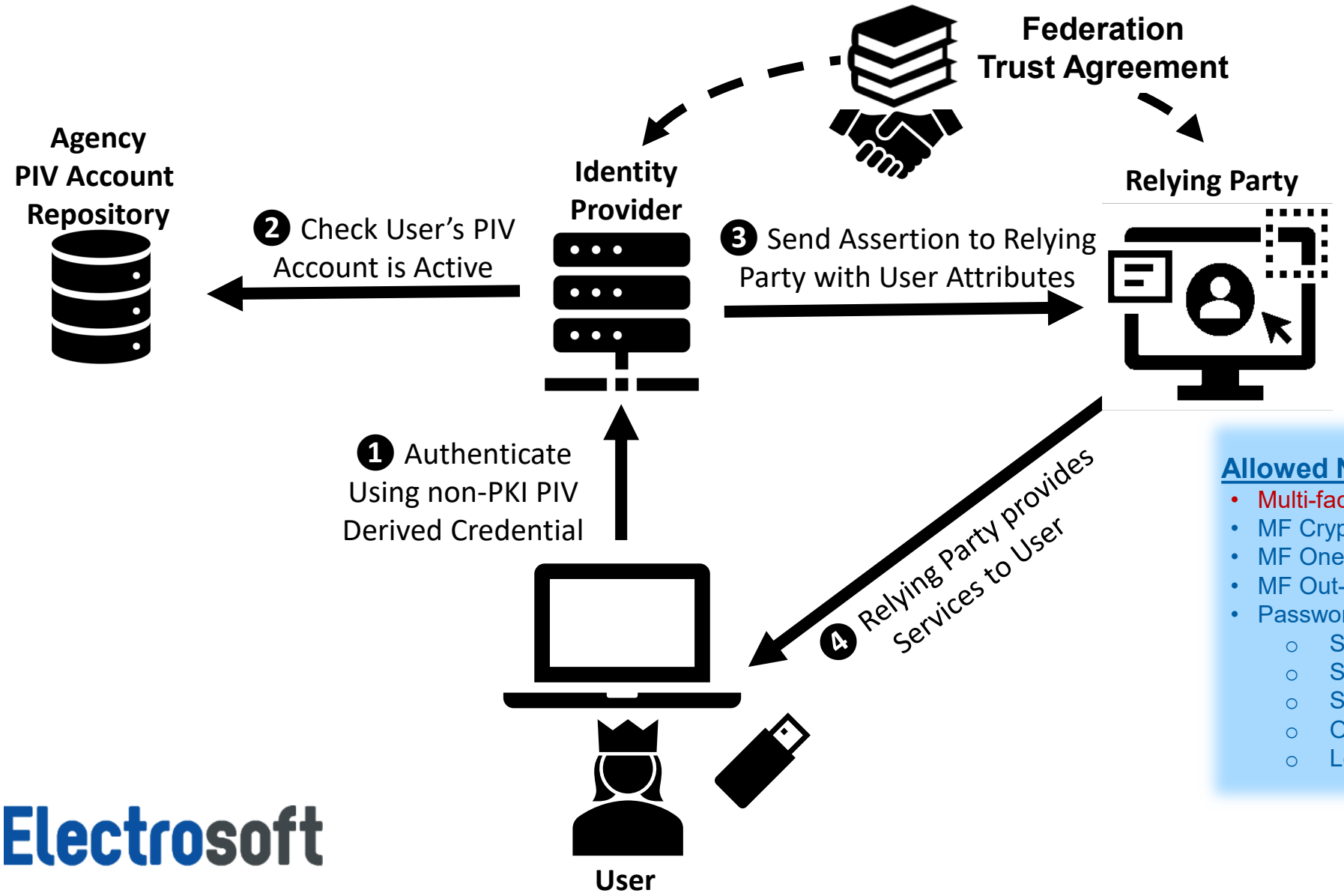
Derived PIV Credentials (IAW FIPS 201-3, NIST SP 800-157r1)

- **What are these?**
  - Additional authentication credentials issued to PIV Card holder
  - 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

- **Non-PKI Derived PIV Credential Implementation 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

Electrosoft

Identity Federation for Non-PKI Derived PIV Credentials



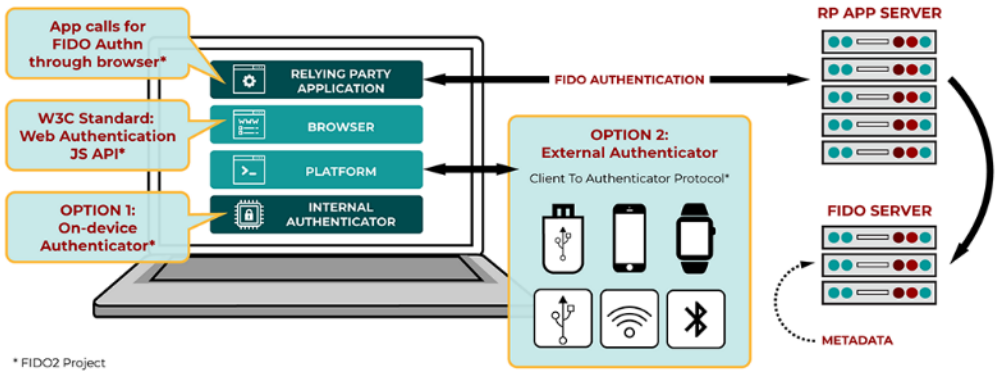
Allowed Non-PKI Derived PIV Credentials

- 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

Electrosoft

Introducing FIDO2

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



Courtesy fidoalliance.org

Electrosoft

Derived FIDO2 Credentials (DFC)

- **What are DFCs:**
  - FIDO2 Authenticators issued as Derived PIV Credentials
  - Embodies the combined strengths of PIV and FIDO2

- **DFC 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**

Electrosoft

Implementation Models

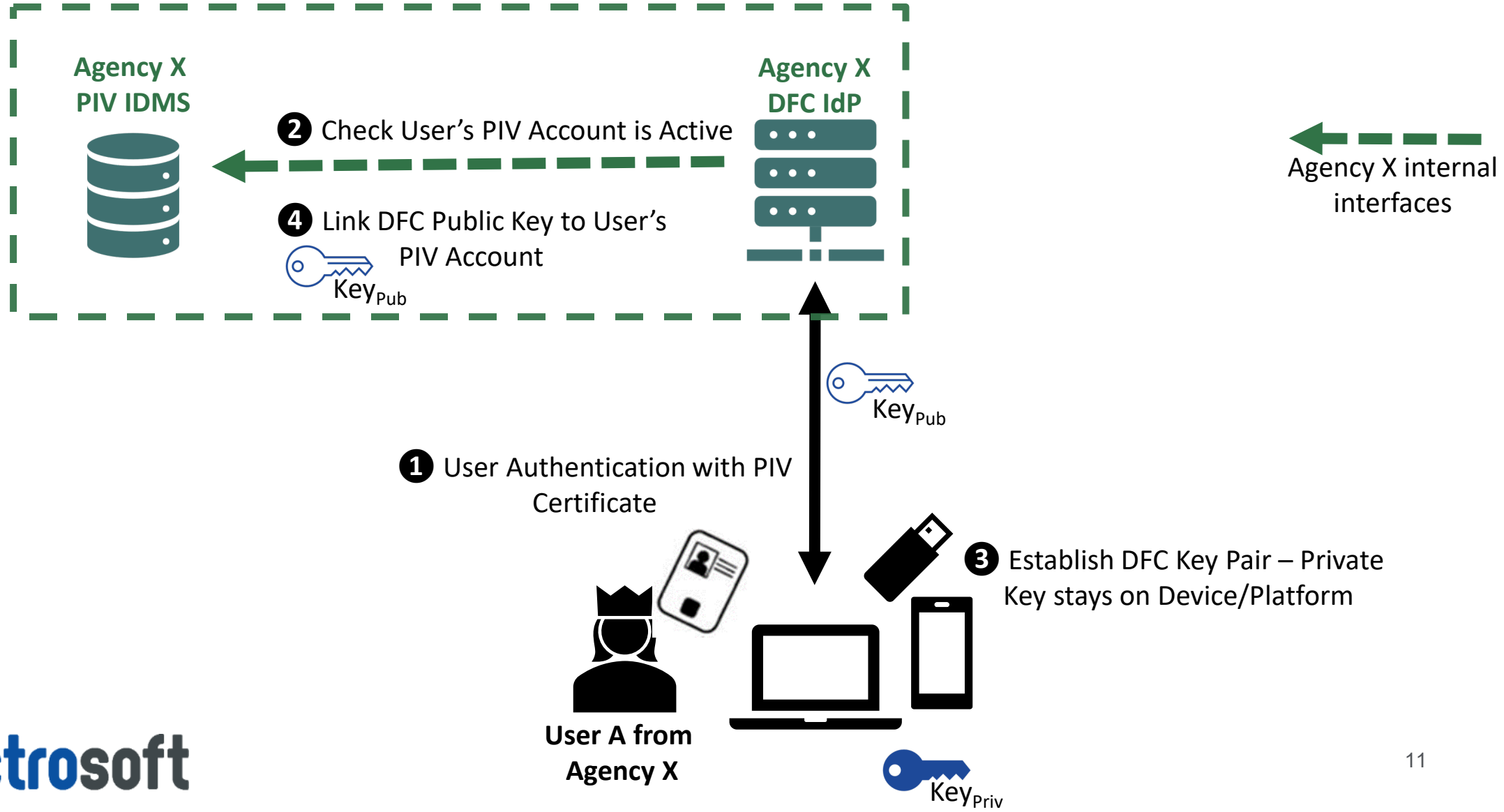
Electrosoft

Model #1: Agency as DFC Issuer

- **Agency issues DFC to User following:**
  - Successful PIV Card Authentication
  - PIV Account active status check
- **DFC used in a federated environment through Identity Federation (e.g. SAML, OIDC)**
  - Agency Identity Provider (IdP) – Issues and Verifies DFCs
  - Agency Relying Parties (RPs) – Accepts assertions from IdP
- **New DFC issued to User linked to User's PIV Account**
- **DFC lifecycle managed as part of User's PIV Account**

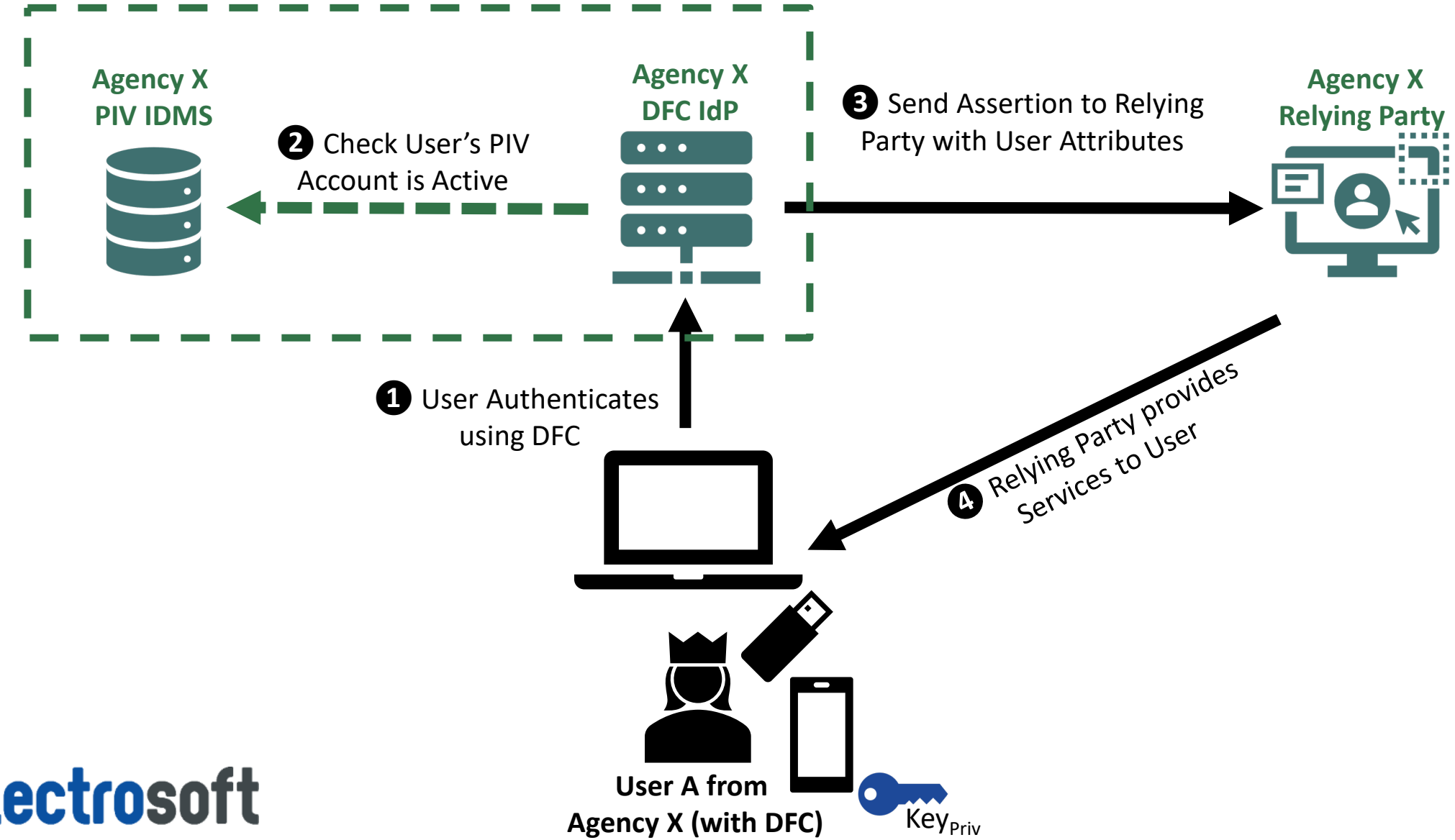
Electrosoft

Model #1: DFC Issuance



Electrosoft

Model #1: DFC Authentication & Assertion



Electrosoft

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 DFC IdP

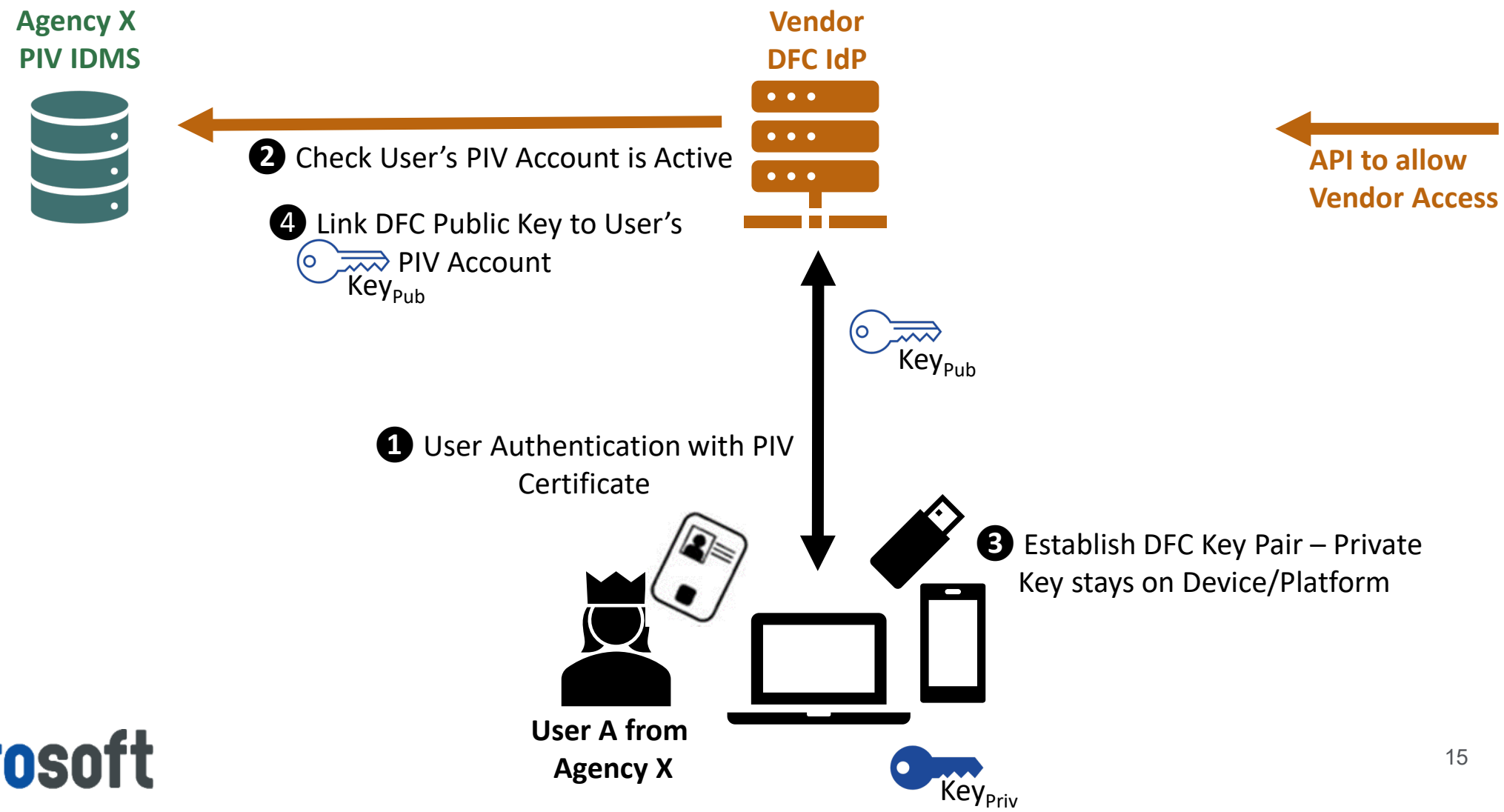
Electrosoft

Model #2: Outsource DFC IdP to Vendor

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

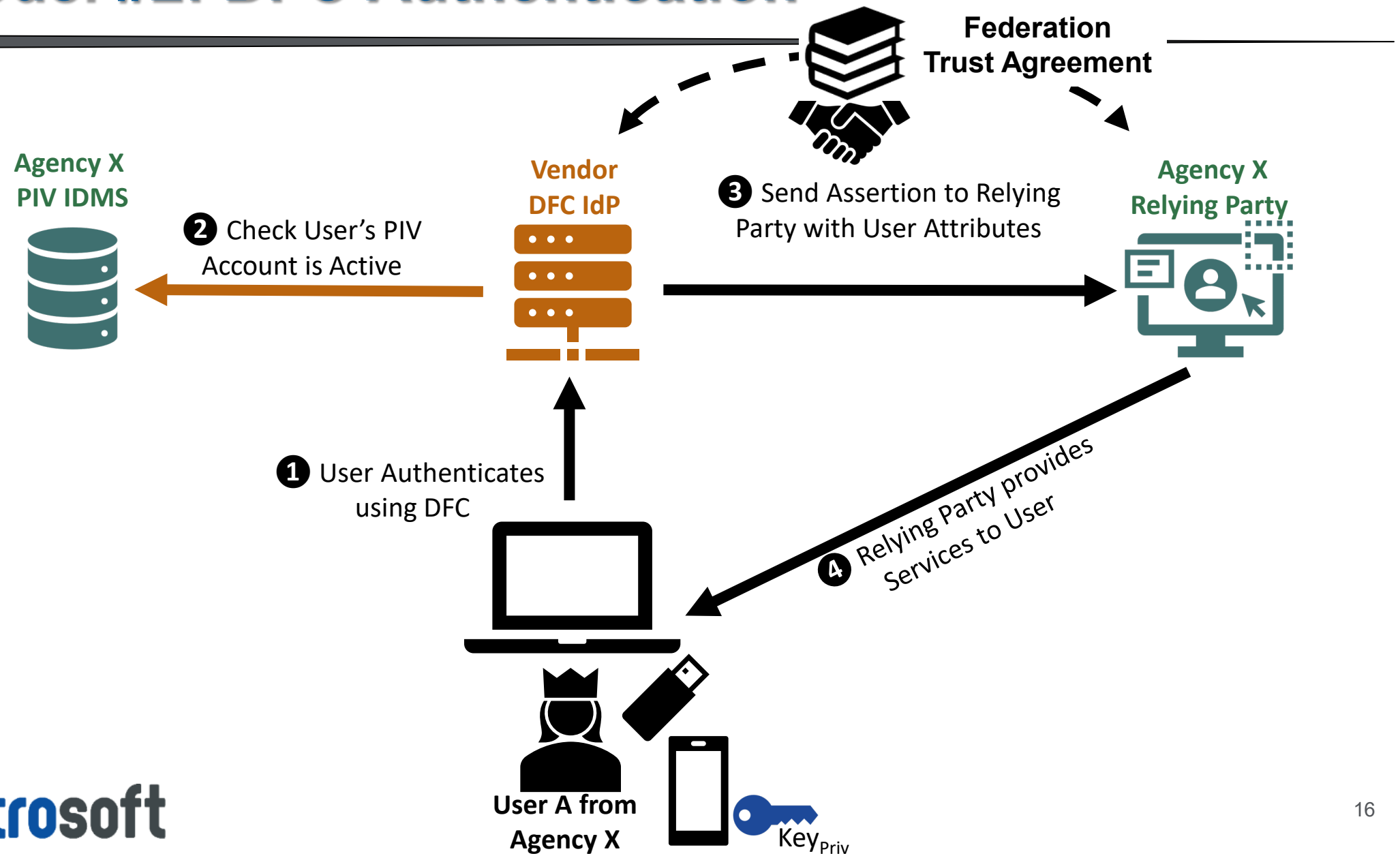
Electrosoft

Model #2: DFC Issuance



Electrosoft

Model #2: DFC Authentication



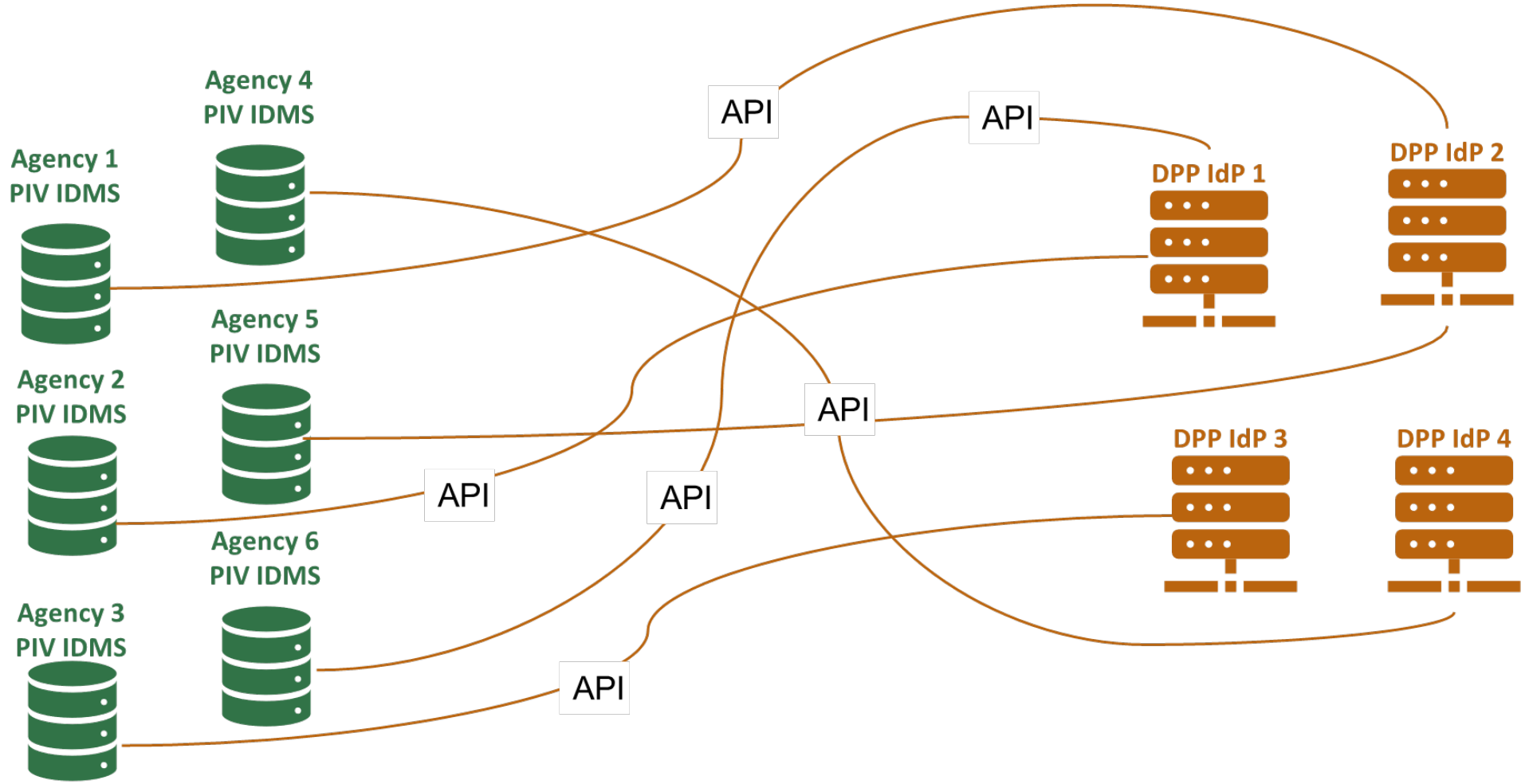
Electrosoft

Model #2: Benefits/Drawbacks

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

Electrosoft

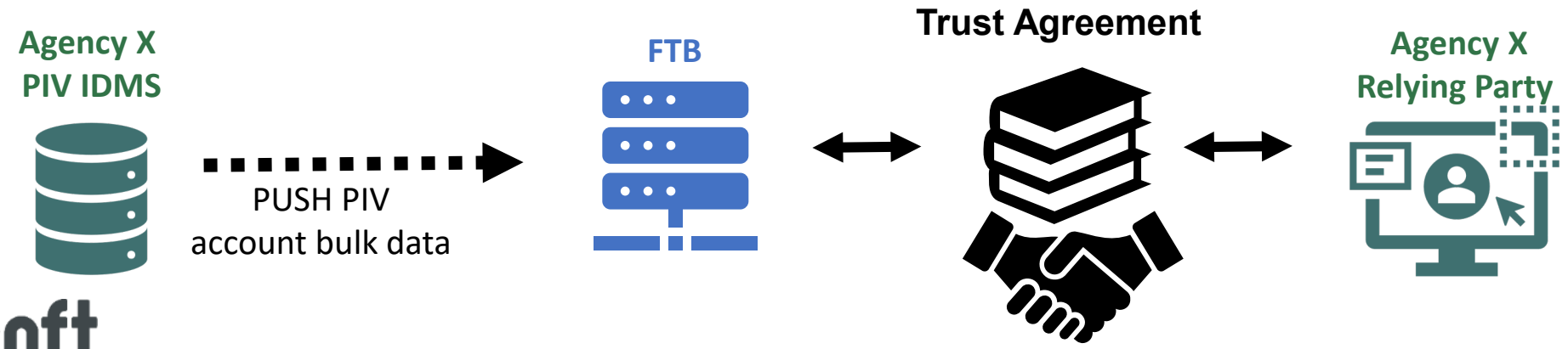
Model #2 – Potential Scenario in Federal Government



Electrosoft

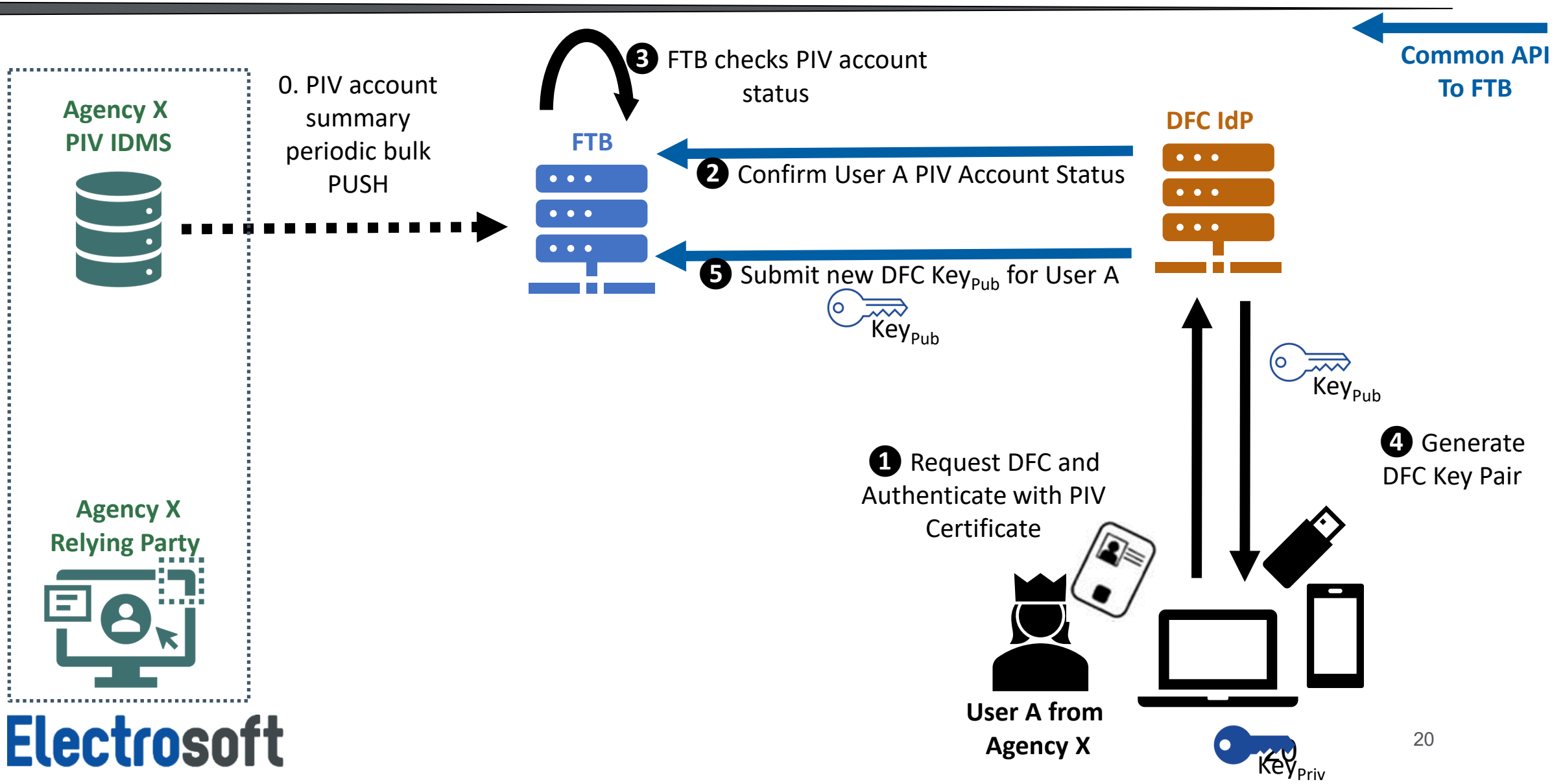
Model #3: Federal Trust Broker (FTB)

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



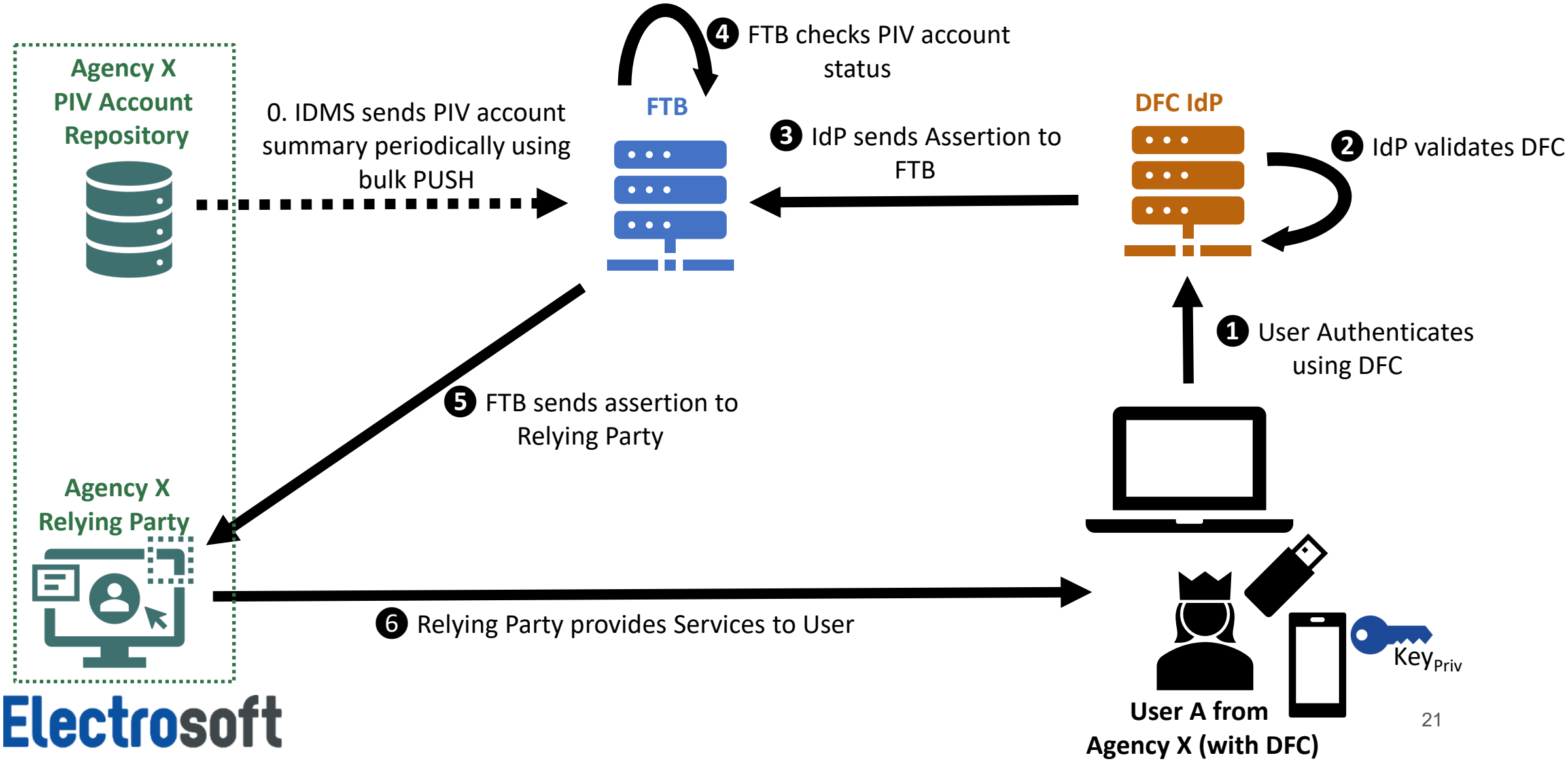
Electrosoft

Model #3: DFC Issuance



Electrosoft

Model #3: DFC Authentication



Electrosoft

Model #3: Benefits/Considerations

- **Benefits**
  - Agency outsources DFC 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

Electrosoft

Derived FIDO2 Credentials (DFC) – Summary

- **Combines the strengths of PIV and FIDO2**
  - 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
  - Easy recoverability of FIDO2 – reduces Help Desk Calls and Cost
  - Broad support on IT platforms and browsers
- **Multiple Models of Implementation with Pros and Cons**

Electrosoft

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

Electrosoft