FIDO, ID Proofing and Federation

Jerrod Chong, VP Solutions

yubico

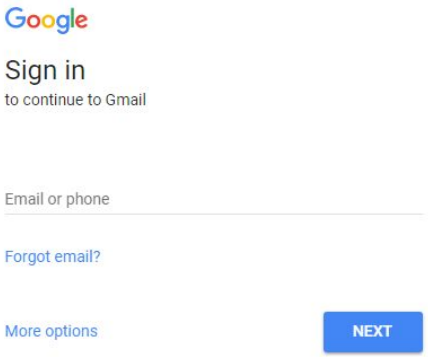
FIDO U2F AKA Security Keys

Global open authentication standard **co-created by Yubico & Google**

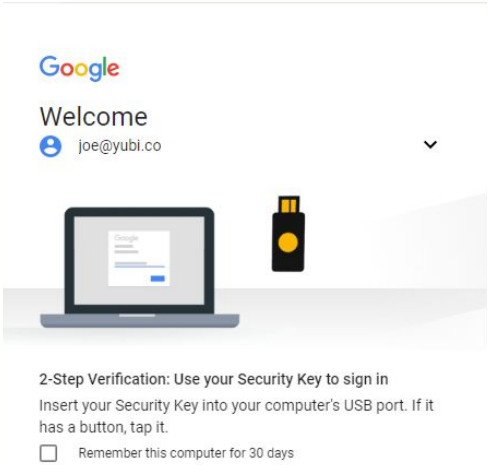
One Authenticator **Any** # of Services **No** Shared Secrets

Google Security Key Login

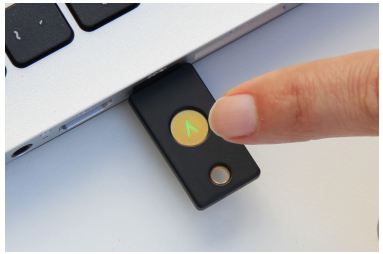
1



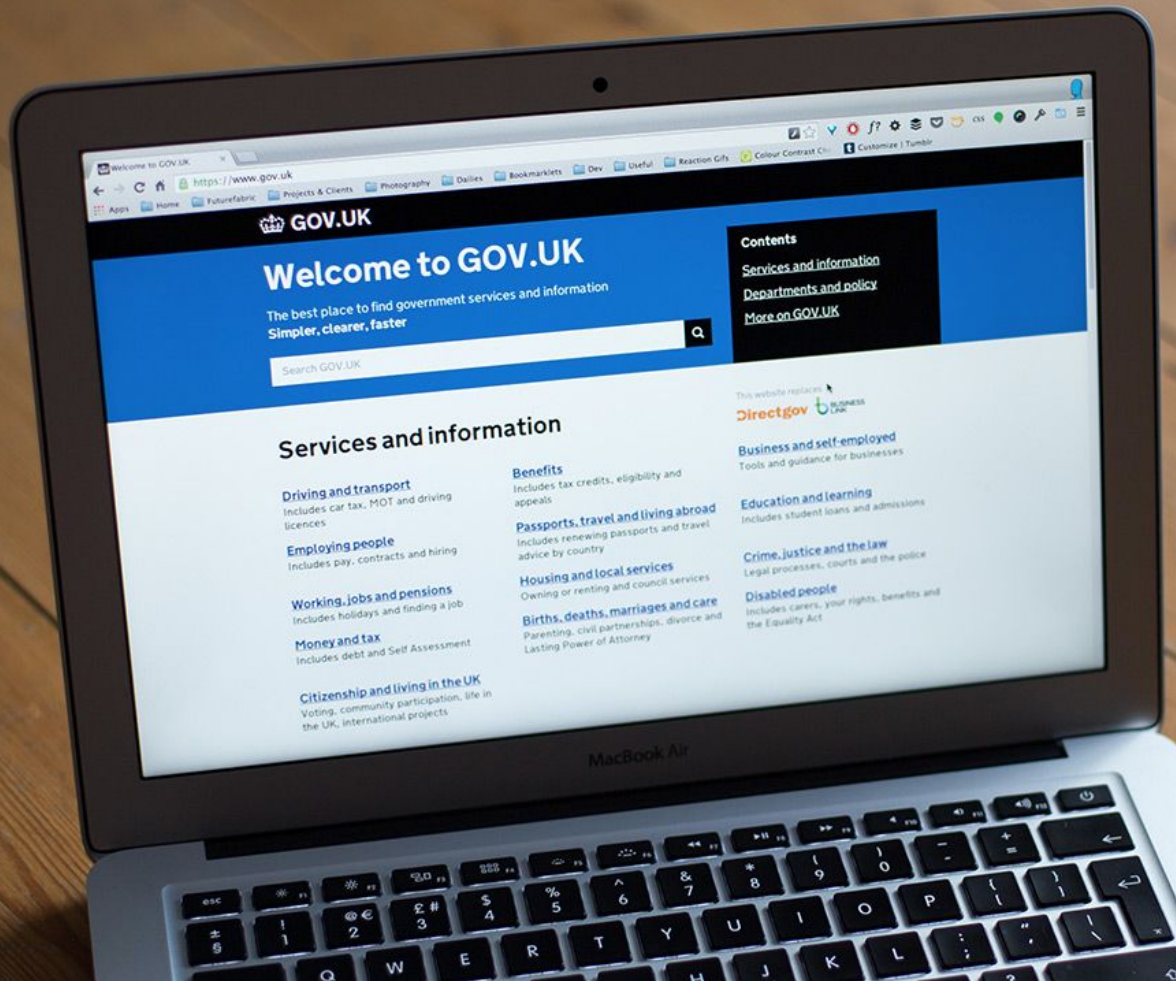
2



3



Secure Unphishable / UnMITMable
Simple Insert and press button
Scalable One device, many services
Privacy No Link-ability between services



1st Government to offer citizens opt-in U2F Secured Digital ID

Why are we solving this?

- Strong authentication not always tied to identity of user
- FIDO authentication mostly decoupled from ID Proofing
- ID Proofing required for higher assurance levels
- ID Proofing and strong authentication at odds with privacy
- Remote ID Proofing tied to Knowledge Based Verification (KBV)
- Reduce the reliance on weak recovery options

“Individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.”

-NIST Trusted Identity Group (TIG)

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP 800-63-3

Digital Identity Guidelines 800-63 Revision 3

Highlighting 3 Policy Recommendations

- Decouple Identity assurance from Authenticator assurance
- Deprecate the use of SMS as Out-of-Band verifier
- Approves FIDO U2F for use at highest Authenticator assurance level (AAL3)

The Project

Yubico awarded US NIST grant collaborating with various Identity Providers

- Extend benefits of FIDO U2F to federated identity environments
- Integrate ID Proofing with FIDO U2F authentication
- Share attributes securely, conveniently and privacy-enhancing

ID verified FIDO Authenticators

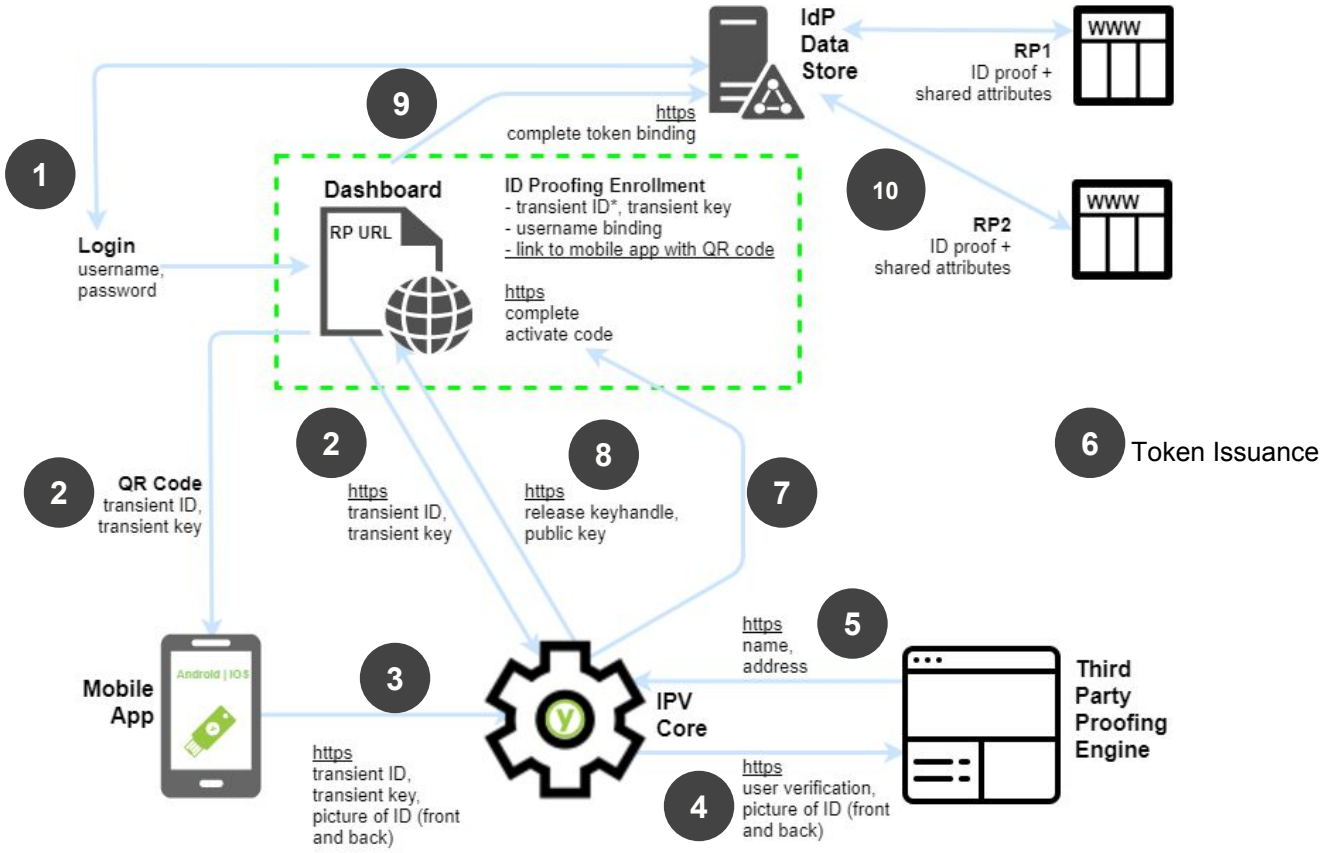
- **Successful Remote Proofing issues Pre-registered authenticator**
- **Pre-registration of authenticator ensures authenticity and integrity (first FIDO credential must be ID verified)**

Mobile ID scanning,
Driver's license or state ID

U2F Authenticator sent to
the address on ID

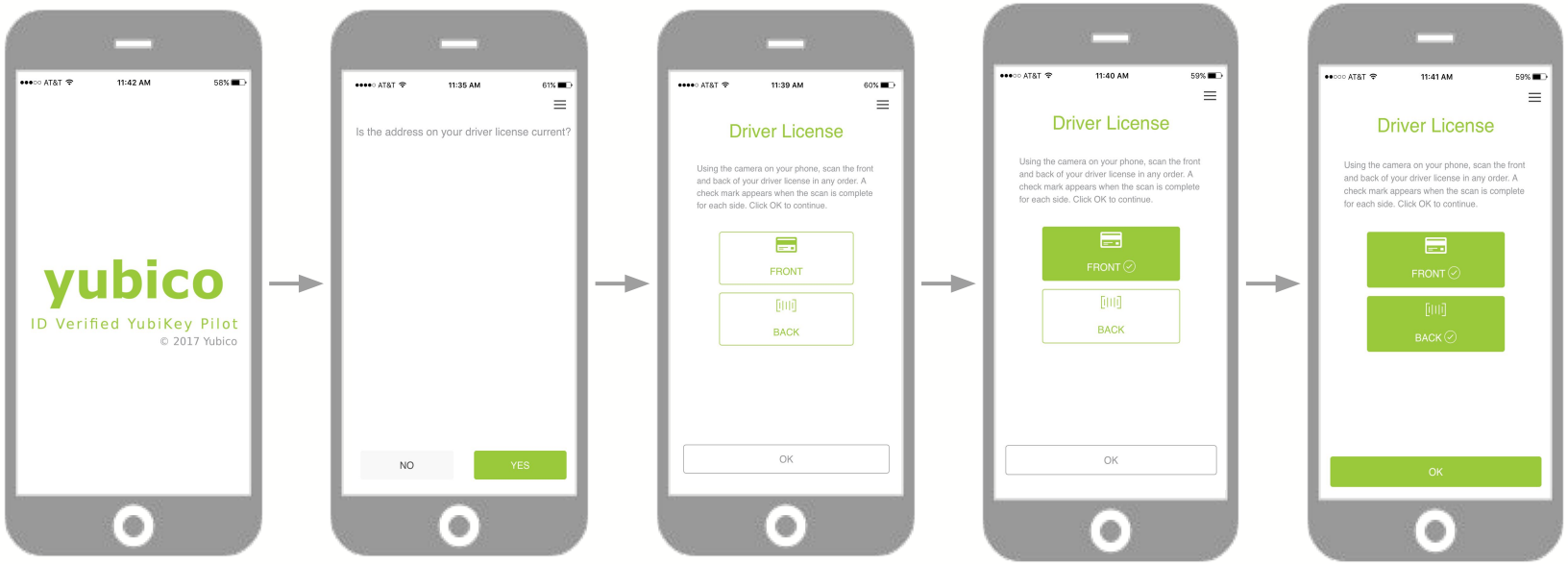
Secure access to any
number of services

ID Proofing and Verification (IPV)

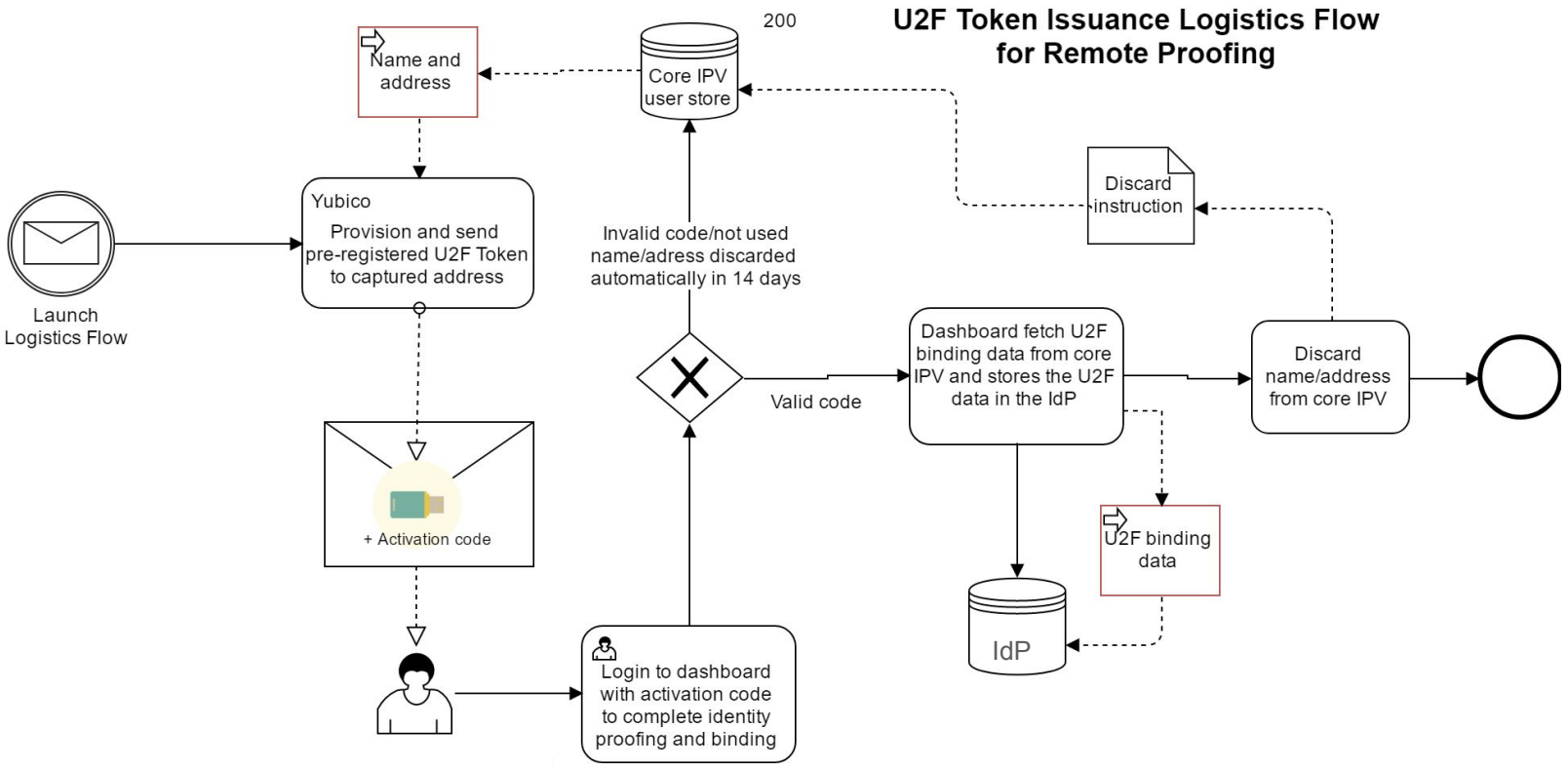


yubico

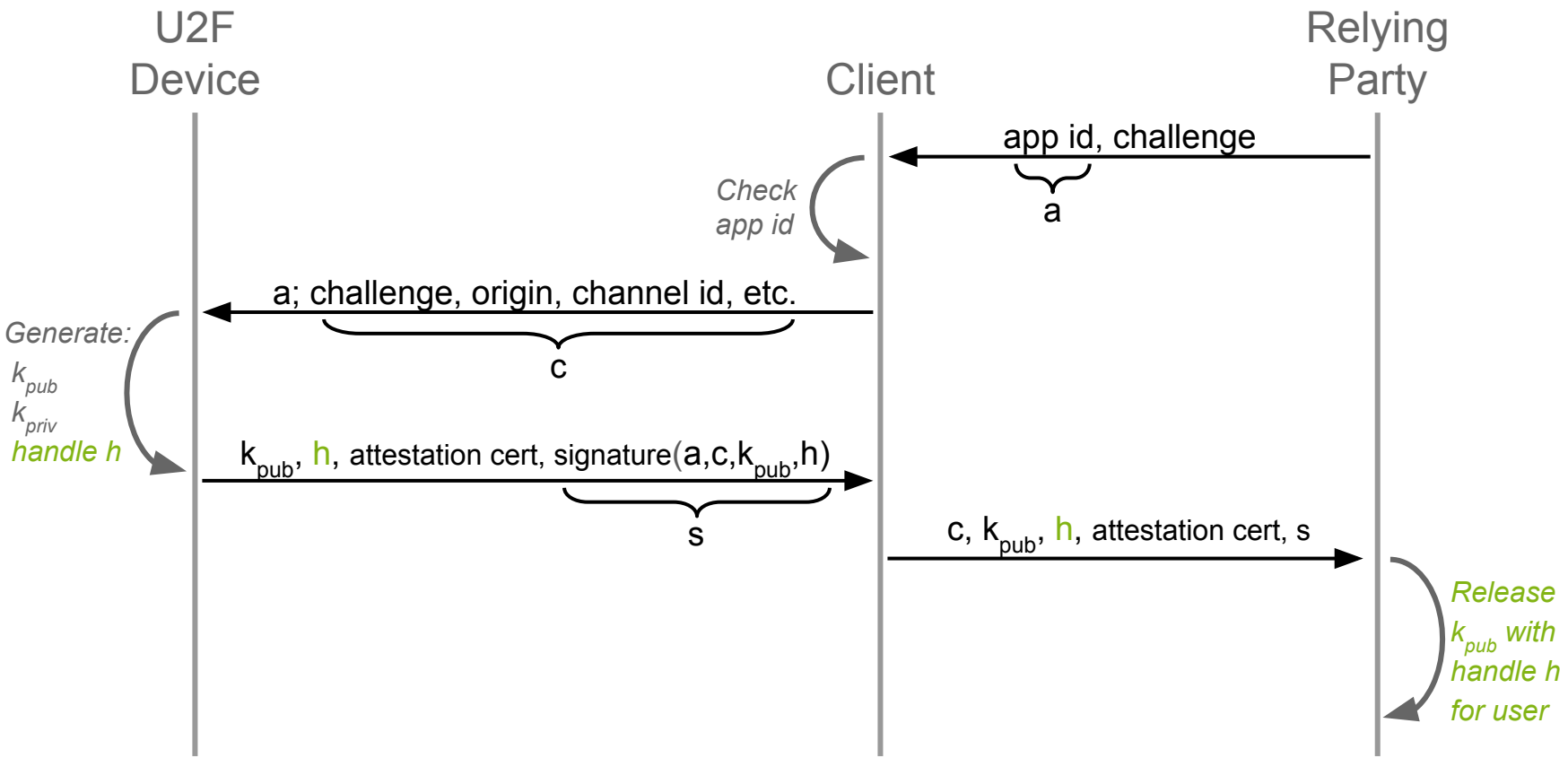
Remote ID Proofing Mobile App



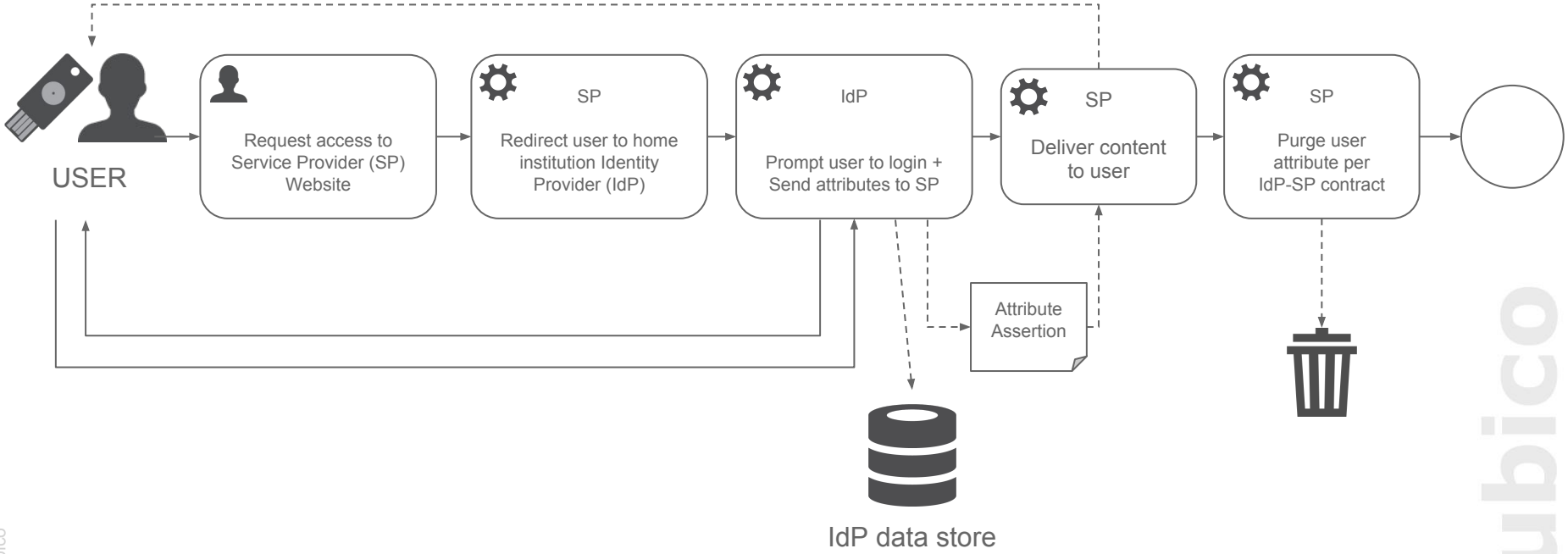
Token Issuance with Pre-Registration



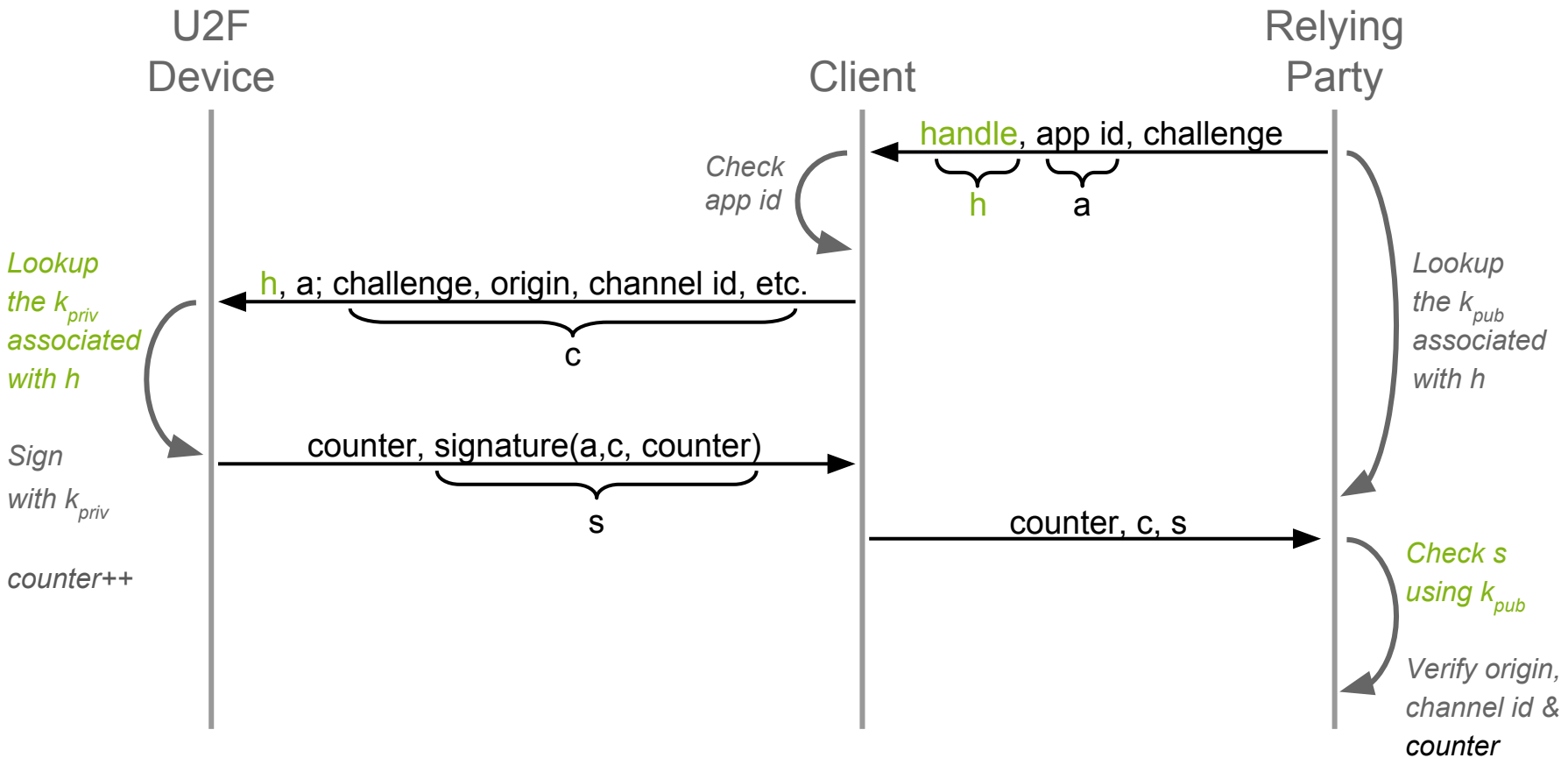
Pre-Registration of Key Handle



Authentication Flow



Authentication



Identity Ecosystem using Open Standards

- **Extend FIDO to services connected via these federation protocols**
  - U2F Shibboleth (SAML) and OpenID Connect plug-in
  - Open source reference implementation
- **Build ID Proofing engine using OpenID Connect**
  - Allows for multiple proofing solutions/providers
  - Part of the Identity toolkit

Lessons Learned

- Protecting PII is time and resource intensive
- Difficult to achieve highest identity assurance with Remote ID proofing
- High level of trust required in integrations with third-party vendors
- Compatibility challenges across diverse operating systems and devices
- Additional techniques needed to onboard special needs individuals

Questions?

yubico

Trust the Net