Is Consumer-Oriented Strong Authentication Finally Here to Stay?

Arshad Noor, CTO, StrongAuth, Inc.

Professional Strategies – S22

Historical Perspective

- Password-based authentication invented at least 4-5 decades ago
  - Primarily for charge-back accounting
- Over the years
  - “Yellow Pages” (NIS), NIS+, Kerberos, LDAP, OTP, Biometrics, Liberty Alliance, SAML, Higgins, CardSpace, Smartcards, SSL with ClientAuth, OAUTH, ……..

Historical Perspective

- Single-Factor Authentication
  - "What you know"
  - "What you are"
  - "What you have"
- Identity Protection Factor (IPF)*

  ".. a measure of the ability of a technology to resist attack from unauthorized entities"

* http://middleware.internet2.edu/idtrust/2008/papers/01-noor-ipf.pdf

StrongAuth
Securing the Core

IPF Scale

IPF	Description
0	No identification or authentication
1	**Shared-secret** based authentication on a local system, or a network **without** any network encryption
2	**Shared-secret** based authentication **with** network encryption
3	**Multiple shared-secret** based authentication **without** an external token, but with network encryption
4	**Asymmetric-key** based authentication with **Private Key in a file**
5	**Multiple shared-secret** based authentication with **external token** and network encryption
6	Asymmetric-key based authentication with **Private Key** generated and stored **on cryptographic hardware token** and using **keyboard** for authentication to token
7	Asymmetric-key based authentication with Private Key generated and stored on cryptographic hardware token and using an **external PIN-pad** for authentication to token
8	Asymmetric-key based authentication with Private Key generated and stored on cryptographic hardware token using an external PIN-pad and **being physically present at the machine** where the resource exists and where authentication is performed
9	Asymmetric-key based authentication with Private Key generated and stored on hardware cryptographic token, using an external PIN-pad, being physically present at the machine where authentication is performed and using **M of N control** for authentication to token
10	Non-existent/Unknown

Strong Authentication

- Existed for nearly 2 decades
- Asymmetric key-pair based
- **NO** secrets on server-side
- Dynamic challenge
- Hardware-based key-gen and storage
- Smartcard-based SSL ClientAuth
- Difficult and expensive

What is FIDO?

- **F**ast **ID**entity **O**nline
- An alliance of more than 125 companies
  - Alibaba, Google, PayPal, Netflix, Visa, MC, AMEX, WF, BofA, LG, Samsung, Microsoft, Lenovo, RSA, eTrade, SFDC, StrongAuth, ...
- Goal:
  - To make *strong-authentication* simple for consumers
  - Freedom to use choice of *Authenticators* (tokens)
  - Freedom to use choice of local-authentication mechanism to unlock key on token: physical presence, iris scan, fingerprint, voice, facial-recognition, PINs, etc.
  - Freedom to use one Authenticator for many websites
  - Freedom to use *many* Authenticators for *one* website

What is FIDO?

- Two strong-authentication protocols *
  - **Universal 2nd Factor (U2F)**
  - **Universal Authentication Framework (UAF)**
- Why two protocols?

* StrongAuth has implemented the U2F as the open-source StrongKey CryptoEngine; UAF is a work-in-progress

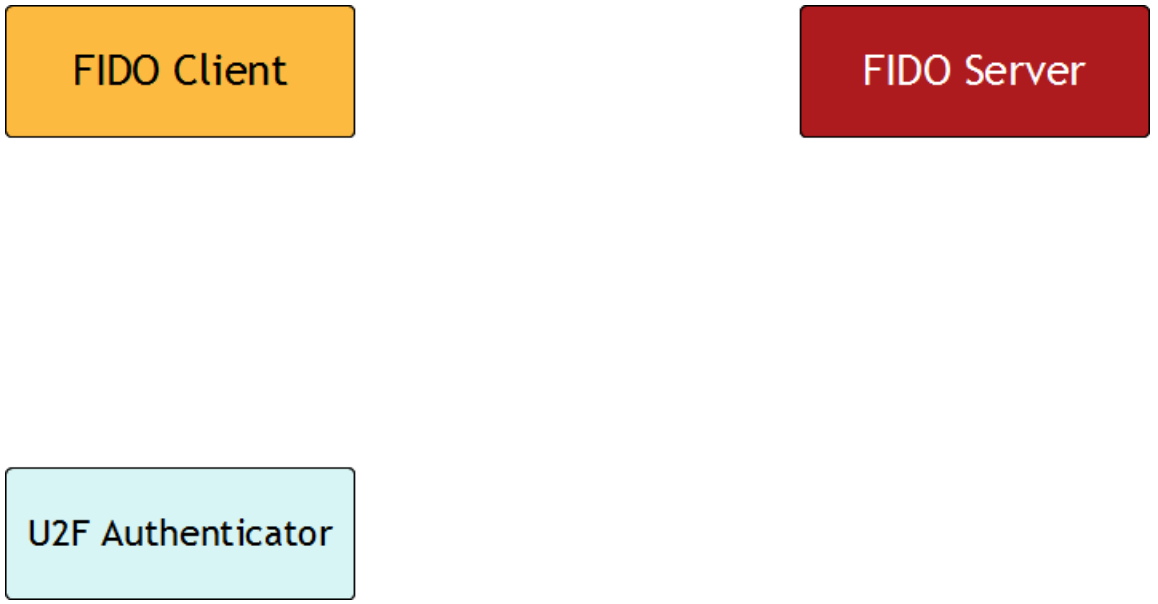
Universal 2nd Factor (U2F)

- Adds second-factor strong-authentication (2FA)
  - Can eliminate password to userid, if desired
- Each cryptographic key-pair is unique per web-site
  - Privacy is built into the FIDO protocol
- No secure display, policy assertions or “business transaction confirmation”
- Allows sharing a single Authenticator
  - User-separation is maintained by username
- Allows use of many Authenticators for single website
  - Separation is maintained in Authenticator

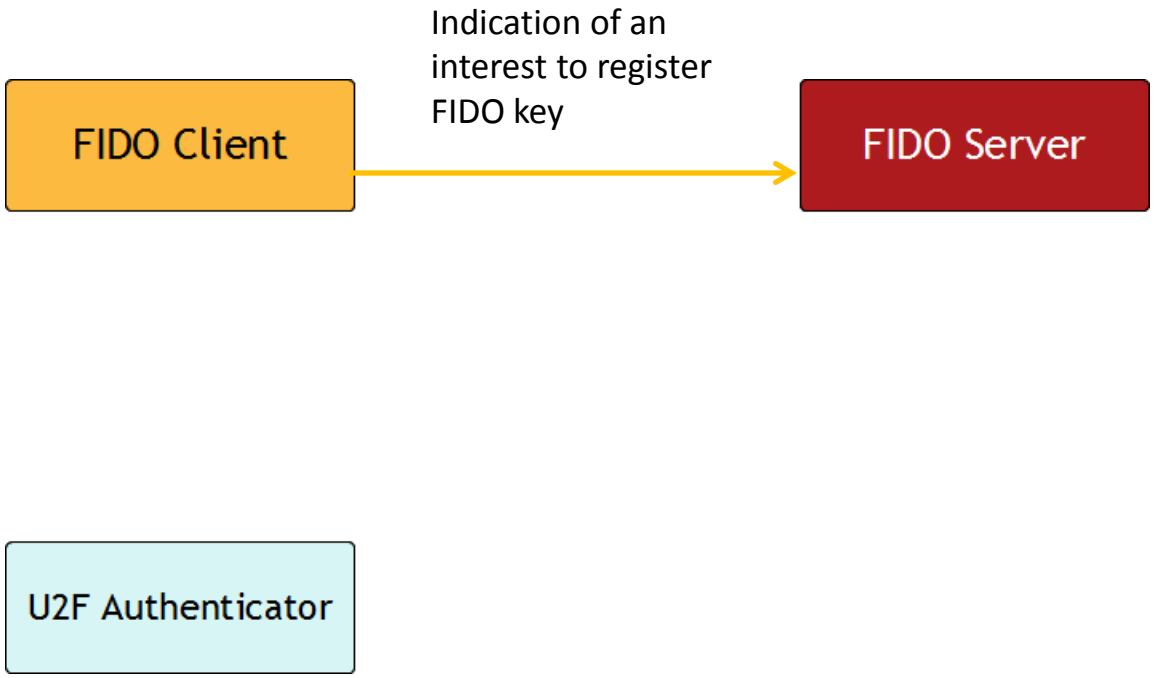
Universal Authentication Framework (UAF)

- Eliminates Password (1FA) authentication
  - Must create unique userid during registration, though
- Adds second-factor strong-authentication (2FA)
- Each cryptographic key-pair is unique per web-site
  - Privacy is built into the FIDO protocol
- Business transaction confirmation + Secure display
- Cannot share Authenticators
- Allows use of many Authenticators for single website

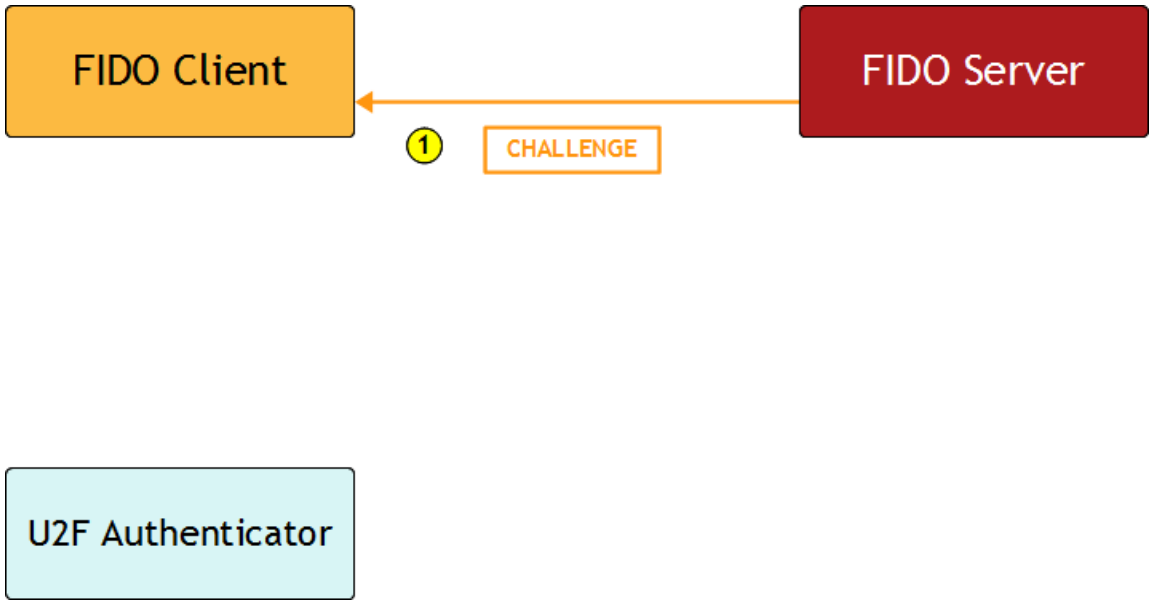
U2F Actors



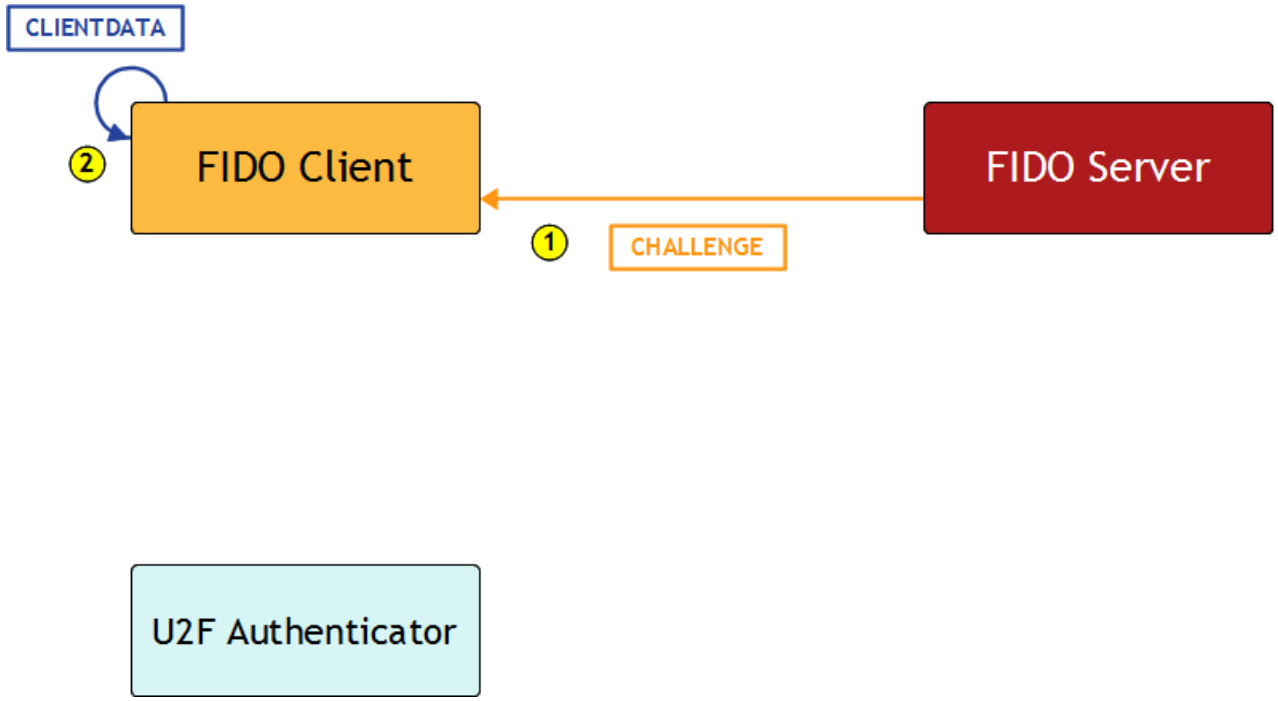
U2F Protocol Initiation



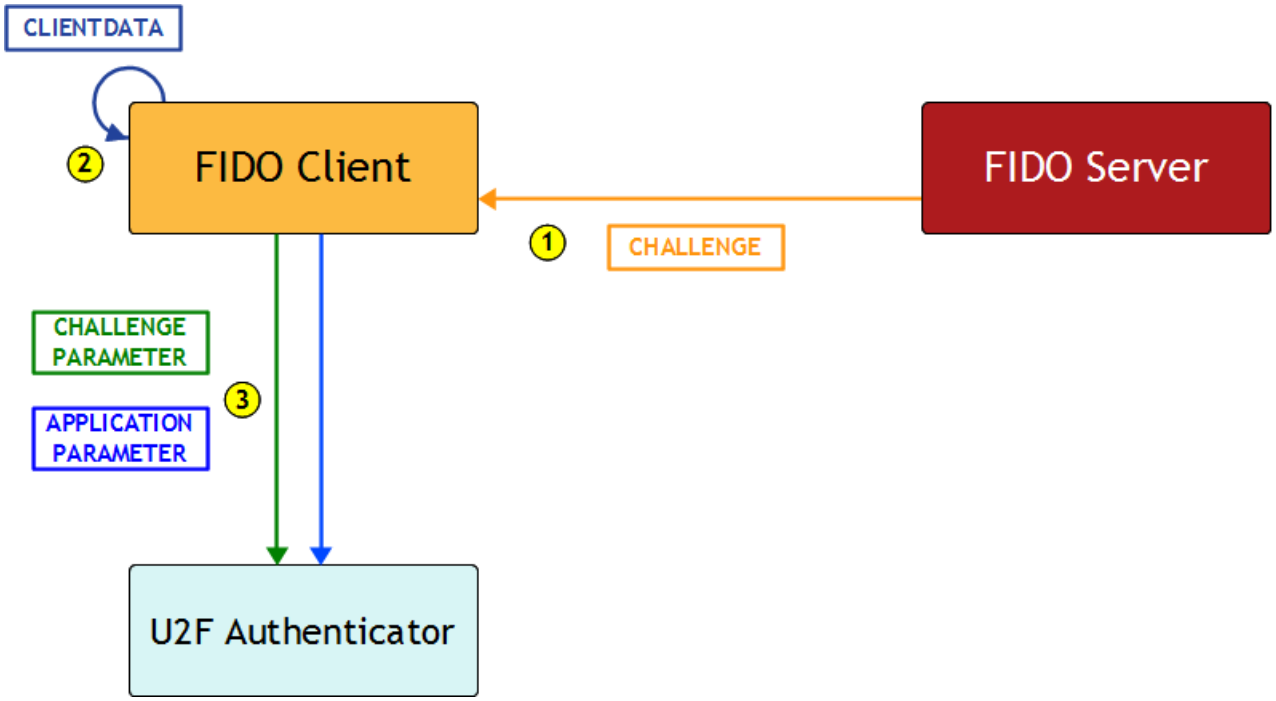
U2F Protocol Detail



U2F Protocol Detail

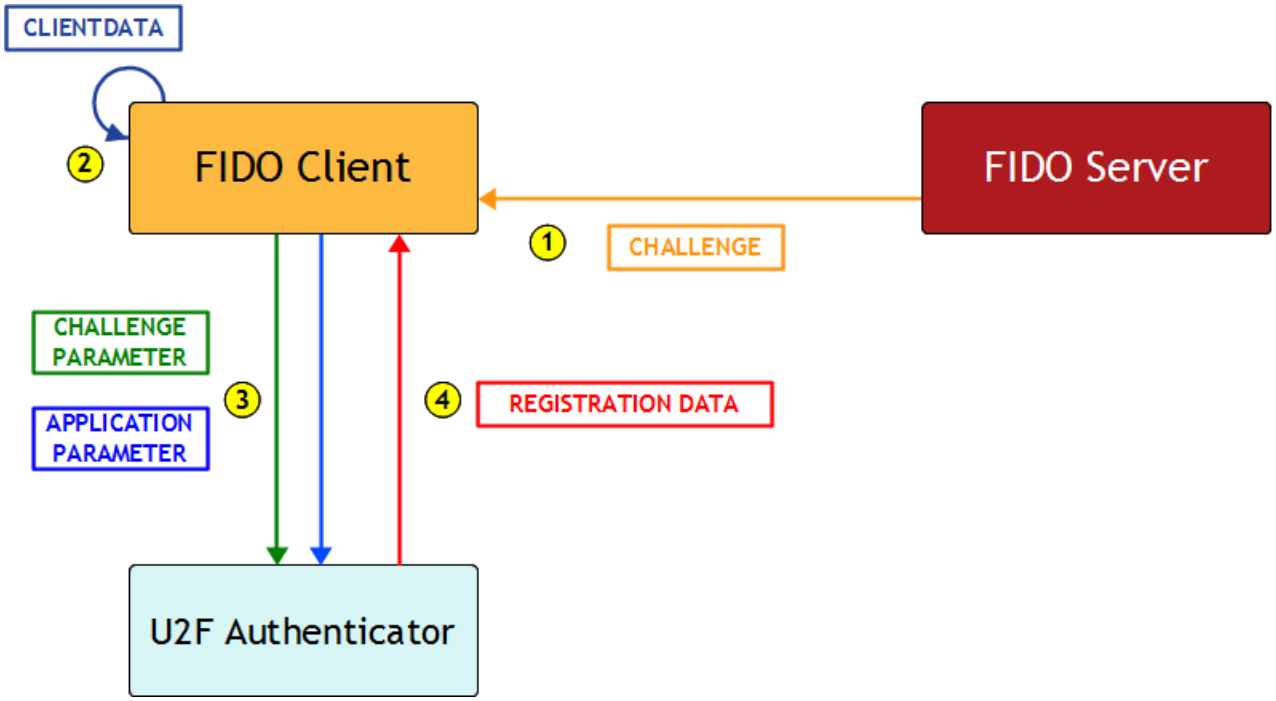


U2F Protocol Detail



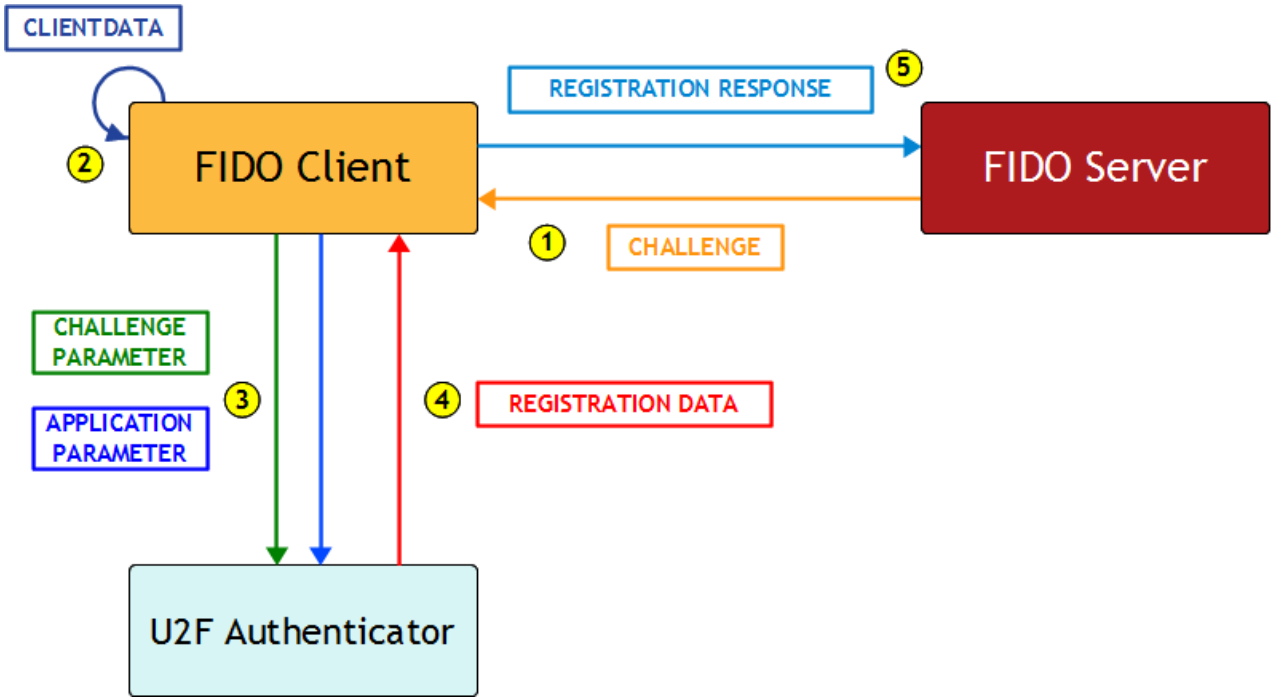
StrongAuth
Securing the Core

U2F Protocol Detail

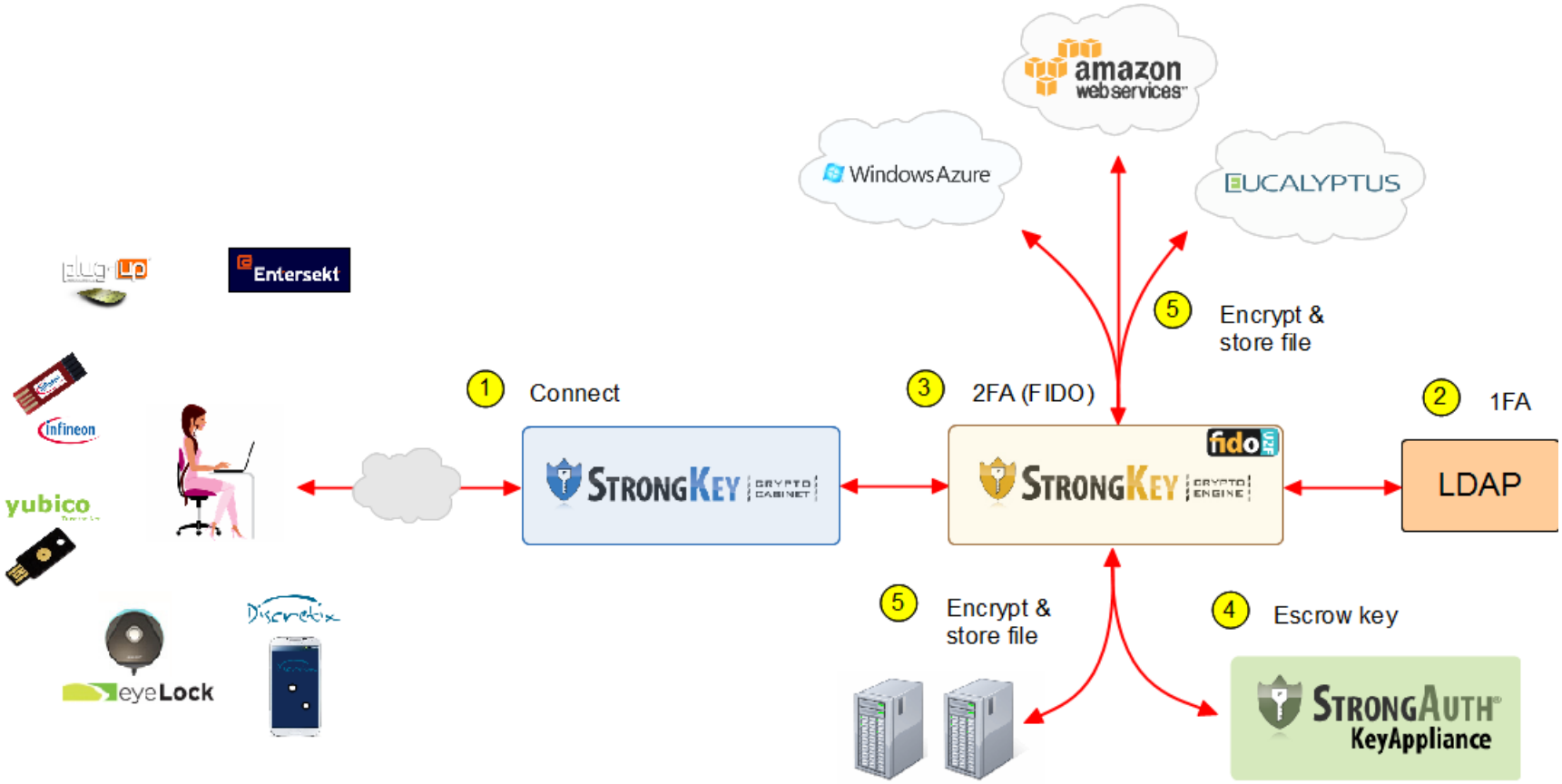


StrongAuth
Securing the Core

U2F Protocol Detail



U2F Demonstration



Questions for Auditors

- Is it an “internal-customer” or “external-customer” focused deployment?
- Are the Authenticators FIDO-certified?
- Are the Authenticators hardware- or software-based?
- Are the Authenticators security-tested?
- What controls does the Authenticator manufacturer have around the “Attestation” key(s)?
- How will the Relying Party (RP) Operations staff learn of “revoked” Authenticators and/or manufacturers?

Questions for Auditors

- What controls exist for protecting “Key Handles” on the FIDO Server?
  - Pay special attention if the FIDO Server is hosted in a public cloud like AWS, Azure, etc.
    - *ISACA Fall Conference 2012 - RC3 presentation*
- What account-recovery process exists for customers who have lost their Authenticators, or forgotten them at home?
- Does that account-recovery process address the company's security policy for identification and authentication?

Questions?

- Arshad Noor
- arshad.noor@strongauth.com
- +1 (408) 331-2000
- www.strongauth.com
- fidoalliance.org