An Introduction to FIDO
And Why it Matters

Arshad Noor

November 18, 2016

Certified

About Me

- CTO, StrongAuth, Inc. (15+ years)
- Sun Microsystems, Citibank, BASF, NY Life Insurance, Port Authority of NY/NJ (Total of 15 years)
- Programmer, Designer, UNIX Administrator, IT Architect, Project Manager, Writer, Speaker, .. (Total of 30+ years)
- PKI Architecture, Design & Deployment Experience (17+ years)
- FIDO Alliance Member (Almost 3 years)

About FIDO Alliance*

- Non-Profit Standards Group
- 250+ Members world-wide
  - Platforms, Banks, Governments, Technology companies, ..
- Currently two (2) standard protocols
  - Proposed 3rd submitted to W3C for standardization
- More than 250 FIDO Certified** products on market

* https://fidoalliance.org/

** https://fidoalliance.org/certification/fido-certified/

StrongAuth® Securing the Core

fido U2F™ Certified

Why is FIDO necessary?

- The explosion of password-based authentication
  - Business models of social-networking, search-engines, …
- The weakness of shared-secrets
- The failure of network-based security
- The failure of client-side PKI strong-authentication
- The balkanization of MFA/2FA

Why is FIDO necessary?

- The failure of federated identity models
  - Most are based on password-based-authentication
- The cost of consumer adoption to secure the internet
  - Who bears this cost?
  - What about taxpayer-funded National ID cards?
- The need for privacy in authentication protocols
- The need for simplicity

FIDO's benefits?

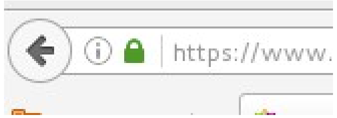
- No shared secrets – passwords, OTP tokens, etc.
  - Public-key cryptography
- Designed for the web
- Designed with privacy at the core
- Choice of standardized protocols
- Multitude of certified implementations

FIDO's benefits?

- No need for a trusted third-party
- Pervasive distribution in mobile world
  - 1.53B Android phones by 2019 (IDC)
- Low barrier to FIDO-enablement
  - Can FIDO-enable applications in less than a week
- Can co-exist with legacy web-authentication schemes
  - Passwords, OTP … and even TLS ClientAuth

FIDO's problems?

- Three (3) protocols
  - Scope creep
- Apple is not at the table
- No standard for consumer education
- No standard for how to tell when FIDO is being used
  - Recognize the SSL/TLS Lock symbol?



https://www.

- No standard for server-side security

FIDO vs. PKI

- ECDSA keys only
- Client authentication only
- No digital certificates
  - No need to trust 3rd party
  - Every key-pair is independent
  - Every RP can manage their own FIDO Keys

- DSA, RSA, ECDSA keys
- Server and ClientAuth
- X.509 digital certificates
  - Certification Authorities
  - Certificate Chains
  - Cross-certification
  - Bridges

FIDO vs. PKI

- Designed for web-apps
- Designed for privacy
- Trust enabled at individual key level in FIDO Server

- Web-app independent
- Privacy is not the goal
- Trust enabled at CA level
  - Unless Client certificate is revoked, application must determine authorization for individual owner of key

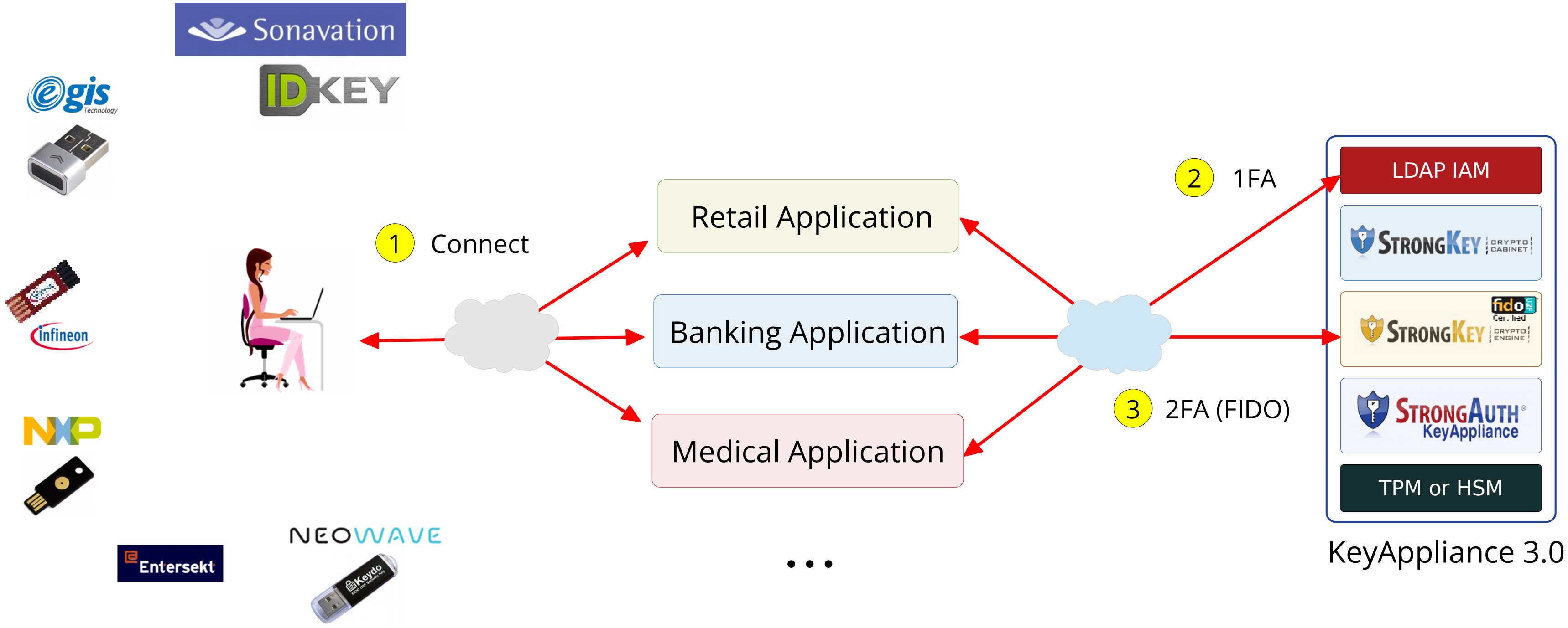
FIDO vs. PKI

- Metadata Service
- USB, BLE, NFC, Embedded Tokens
- U2F, UAF, FIDO 2.0
- ClientAuth success TBD
  - Gmail, Github, …
  - UK National Cyber Security Strategy*

- CRL, OCSP
- Smartcards, USB Tokens, Embedded Tokens
- TLS, PKCS, DSig, XMLEnc.
- ClientAuth a failure
  - With minor exceptions in some industries

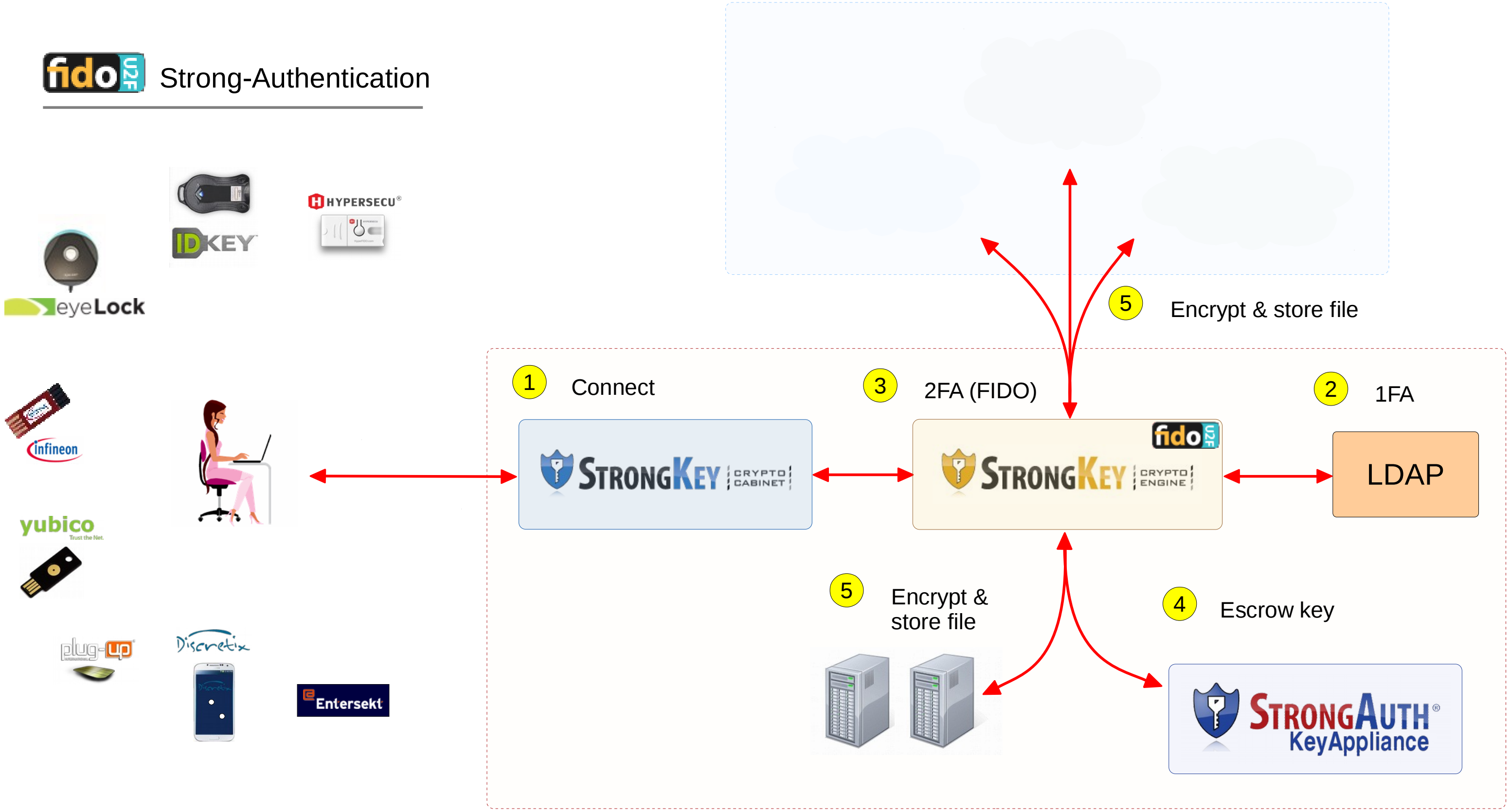
* https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

FIDO Big Picture



StrongKey CryptoCabinet

***Note**: Secure cloud-storage is a standard feature of CryptoEngine, and may be used to store encrypted documents in the cloud if desired. However, cryptographic keys are **never** stored in the cloud.*



Strong-Authentication

5 Encrypt & store file

1 Connect

3 2FA (FIDO)

2 1FA

LDAP

5 Encrypt & store file

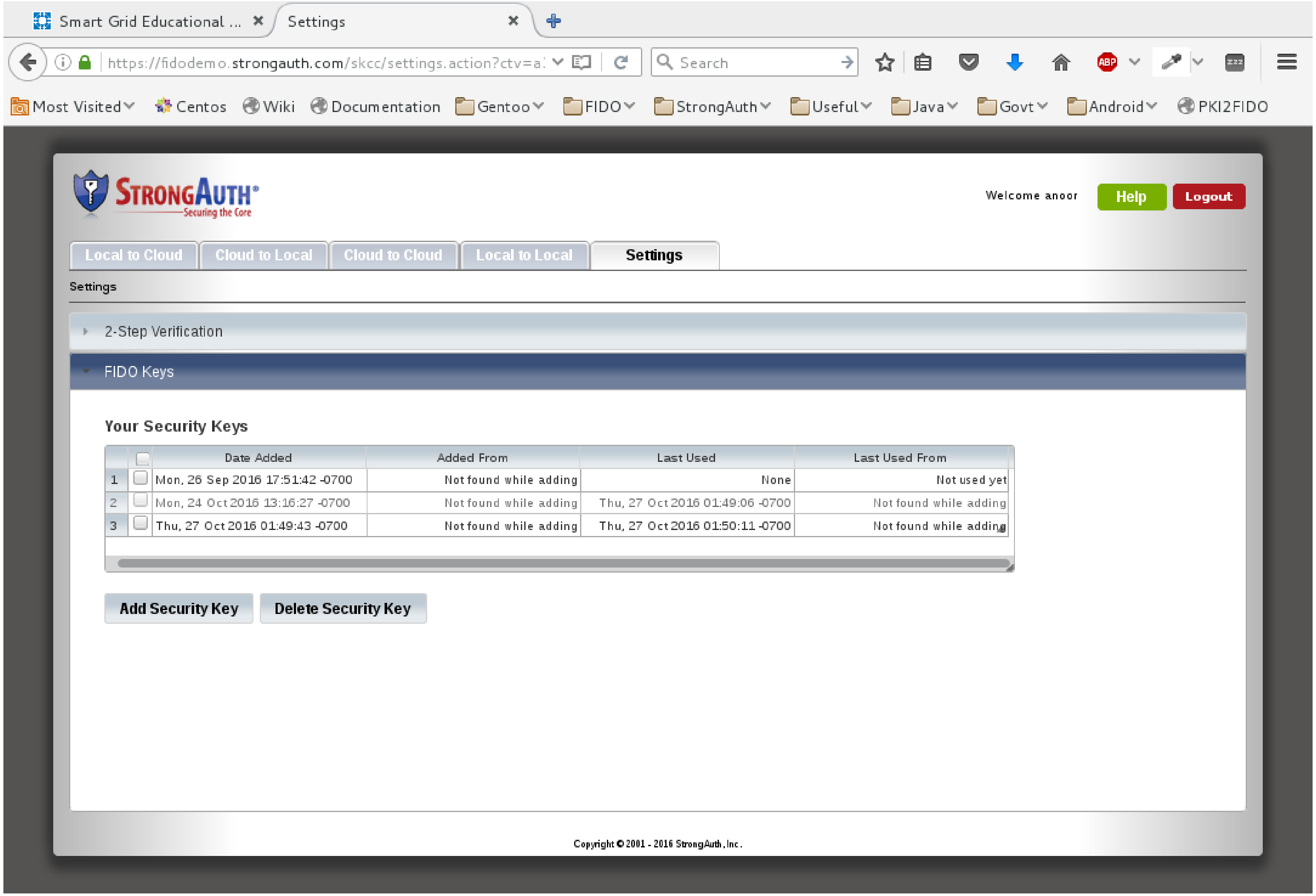
4 Escrow key

On-premises infrastructure

StrongKey CryptoCabinet

STRONGAUTH® Securing the Core

fido U2F™ Certified



Settings

2-Step Verification

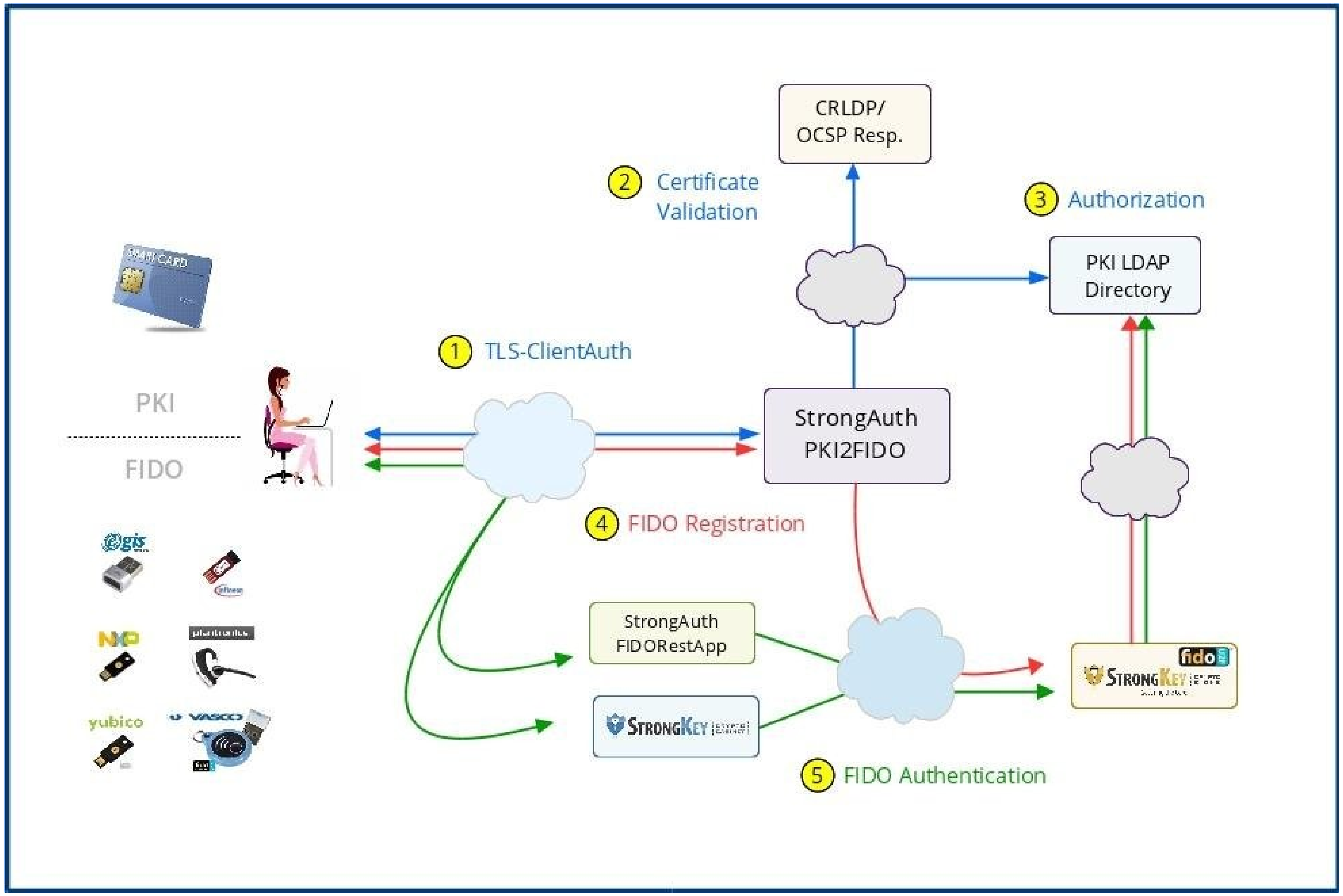
FIDO Keys

Your Security Keys

	□	Date Added	Added From	Last Used	Last Used From
1	□	Mon, 26 Sep 2016 17:51:42 -0700	Not found while adding	None	Not used yet
2	□	Mon, 24 Oct 2016 13:16:27 -0700	Not found while adding	Thu, 27 Oct 2016 01:49:06 -0700	Not found while adding
3	□	Thu, 27 Oct 2016 01:49:43 -0700	Not found while adding	Thu, 27 Oct 2016 01:50:11 -0700	Not found while adding

Copyright © 2001 - 2016 StrongAuth, Inc.

StrongAuth PKI2FIDO



U2F: Universal 2nd Factor

- Presumes 1FA to web-app exists for key-registration
  - Intent: Supplement 1FA with 2nd factor strong authentication
- Originally targeted for desktop web-applications
  - Supported in Chrome, Opera and *Firefox*; but not in IE, Edge or Safari
  - Can be used by desktop and mobile RCA too, if programmed to do so

Certified

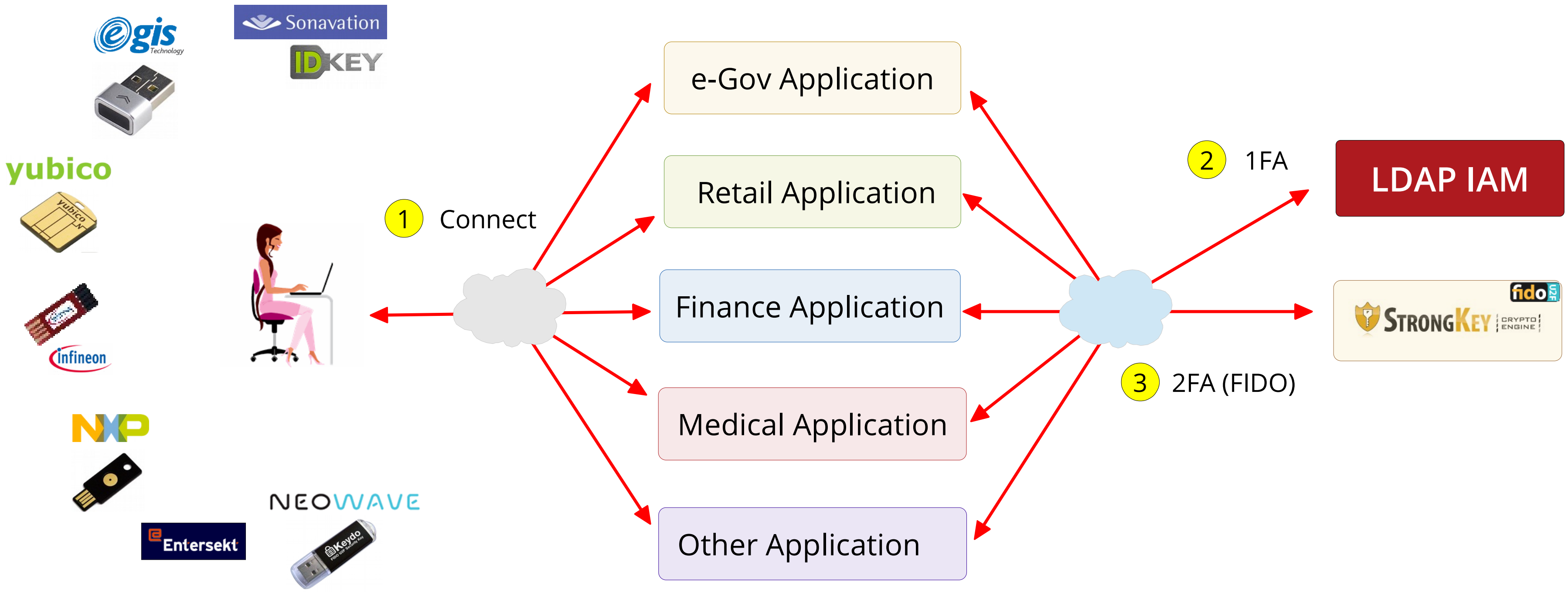
U2F Actors

- Authenticator/Token
  - The device that generates ECDSA key-pairs and signs challenges
  - "Test of human-presence" must exist
  - Supported standard transports: HID, BLE and NFC
- FIDO Client
  - The application on the client platform communicating between Authenticator and Relying Party web-application

U2F Actors

- Relying Party Web-Application
  - The business application with which User interacts
- FIDO Server
  - Software that responds to User's FIDO actions
  - Can be part of RP Web-Application or an independent server

U2F Actors


egis Technology
Sonavation
IDKEY
yubico
Infineon
NXP
Entersekt
NEOWAVE
Keydo
1 Connect
e-Gov Application
Retail Application
Finance Application
Medical Application
Other Application
2 1FA
LDAP IAM
3 2FA (FIDO)
StrongKey Crypto Engine
fido U2F

U2F Actions

- Registration
  - The act of generating a new ECDSA key-pair for a site
  - Username, Authenticator, Site Origin combination must be unique
- Authentication
  - The act of signing a challenge for a web-application
  - Same key *may* be used to authenticate to multiple apps at a site if part of the same web-origin (TLD + 1)

U2F Actions

- *Deregistration**
  - *The act of deleting an ECDSA public-key for a site*
- *Authorization**
  - *The act of digitally signing a derived-challenge for an application transaction*

** Vendor-specific capabilities – not official U2F protocol specifications*

UAF

- Universal Authentication Framework
- Presumes the following:
  - Local device-authentication exists for human verification
  - Secure Display exists for (optional) transaction authorization
  - 1FA *may* be presumed to (optionally) exist
  - Intent: Replace 1FA with device and strong-authentication

UAF

- Originally targeted for native mobile applications
  - Can be used by desktop RCA too, if programmed to do so
  - Not supported by any browser or mobile OS, natively
  - Supported by some Android OEM licensees and 3rd party vendors
  - Supported on iOS by 3rd party vendors

Unique to UAF

- Allows for RP's to specify policies about acceptable Authentications
  - Must be in specific location
  - Must be between 09:00 and 17:00
  - Must present (fingerprint, facial image or iris) and PIN
  - …
- Allows for RP's to receive confirmation for transactions displayed on the Secure Display

UAF Actors

- Authenticator/Token
  - The device that generates ECDSA key-pairs and signs challenges
  - Usually embedded in mobile device
- Authenticator Specific Module
  - Software provided by Authenticator manufacturer to provide a uniform API to FIDO Client
  - Usually, a vendor library on mobile device

UAF Actors

- FIDO Client
  - The application on client platform communicating between ASM and Relying Party web-application
  - Usually, a library to abstract FIDO-specific operations from mobile application
  - Can be RP client-application if programmed to do so

UAF Actors

- Relying Party Web-Application
  - The business application with which User interacts
- FIDO Server
  - Software that responds to User's FIDO actions
  - Can be part of RP Web-Application or an independent server

UAF Actors

- FIDO Metadata Service
  - Online service to verify status of Authenticator
  - Loosely, analogous to Certificate Revocation List in PKI
  - Currently, only a single provider: FIDO Alliance
  - RP's may ignore Metadata Service if they manage risk (of using a bad/compromised/unknown Authenticator) in other ways

UAF Actions

- Registration
  - The act of generating a new ECDSA key-pair for a site
  - Username, Authenticator, Site Origin combination must be unique
- Authentication
  - The act of signing a challenge for a web-application
  - Same key *may* be used to authenticate to multiple apps at a site if part of the same web-origin (TLD + 1)

UAF Actions

- Deregistration
  - The act of deleting an existing ECDSA key-pair for a site
- Secure Transaction Confirmation
  - The act of confirming a transaction on a Secure Display
  - Message on Secure Display is determined by Relying Party web-application

FIDO 2.0

- Web Authentication: An API for accessing Scoped Credentials
  - https://www.w3.org/TR/webauthn/
  - Intent to support protocol announced publicly:
    - Mozilla Firefox
    - Google Chrome
    - Microsoft Edge

Deployment Decisions

- Which protocol?
- Which Authenticators?
- Which Platform?
- Which FIDO Server?
  - Build vs. Buy
    - Business focus
    - High Availability, Disaster Recovery
    - Scalability
    - Security

FIDO Security

- What's the issue? Aren't FIDO protocols supposed to be secure?
  - Yes, but.....
- If *KeyHandle* includes a private-key, security of Key-Encrypting-Key matters
- *Attestation Certificate'* private-key protection always matters
- "Substitution of Keys" Attack

FIDO Security – SuKS - 1

Jack

Jill

ID	User	....	Key Handle	Public Key
1234	Jack	....	CAFEBEEF	FEDCBA
1357	Jill	....	CAFEBABE	ABCDEF
...	....	....	....	....

FIDO Security – SuKs - 2

Jack

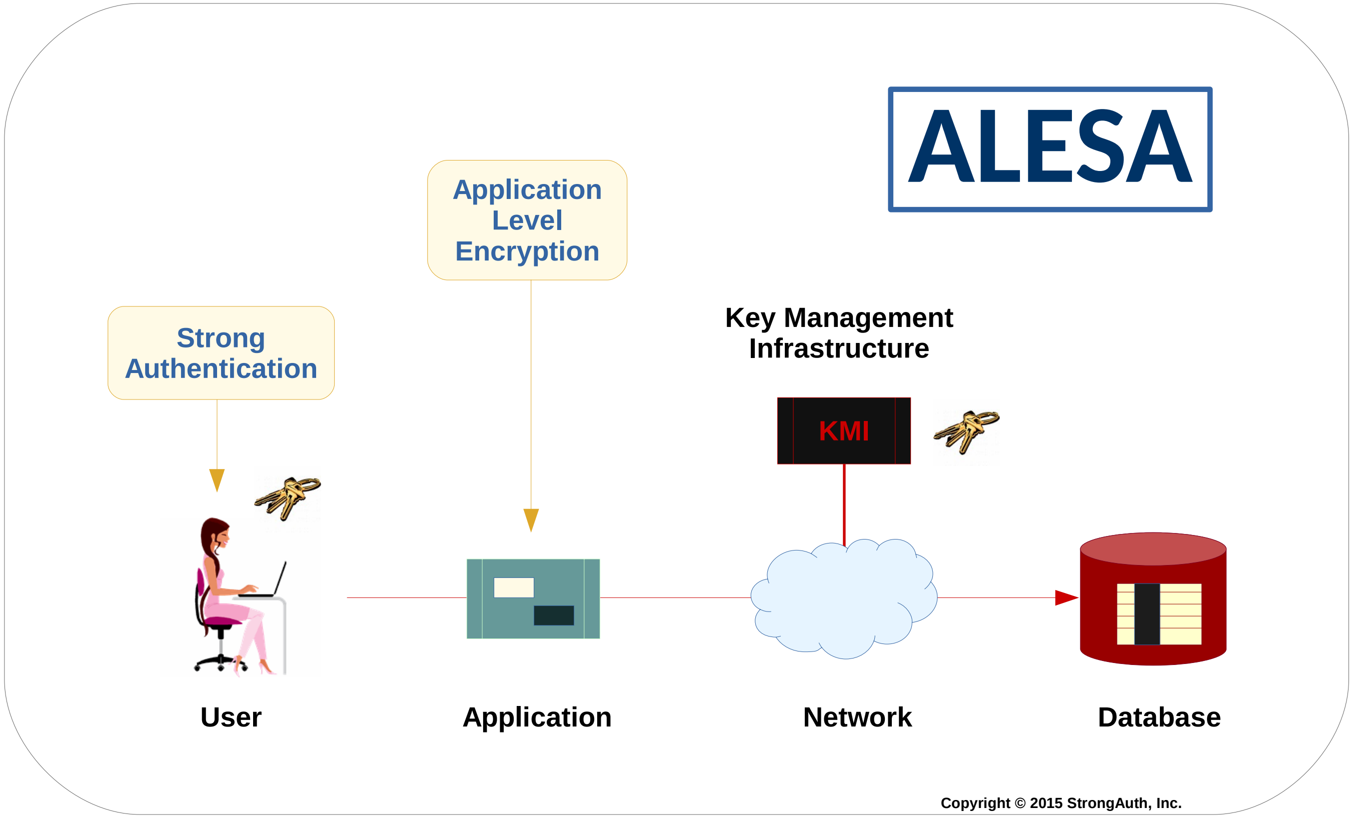
Jill

ID	User	....	Key Handle	Public Key
1234	Jack	....	CAFEBEEF	FEDCBA
1357	Jill	....	CAFEBEEF	FEDCBA
...	....	....	....	....

FIDO Enablement

- Pick a web-application – any application
- Pick an Account Recovery mechanism
- Pick a few FIDO U2F Authenticators
- Pick a FIDO U2F Server – any server ;-)
- Get their FIDO-enablement Tutorial
- Modify the web-application
- Test, test, test,……
- Plan for productionalization

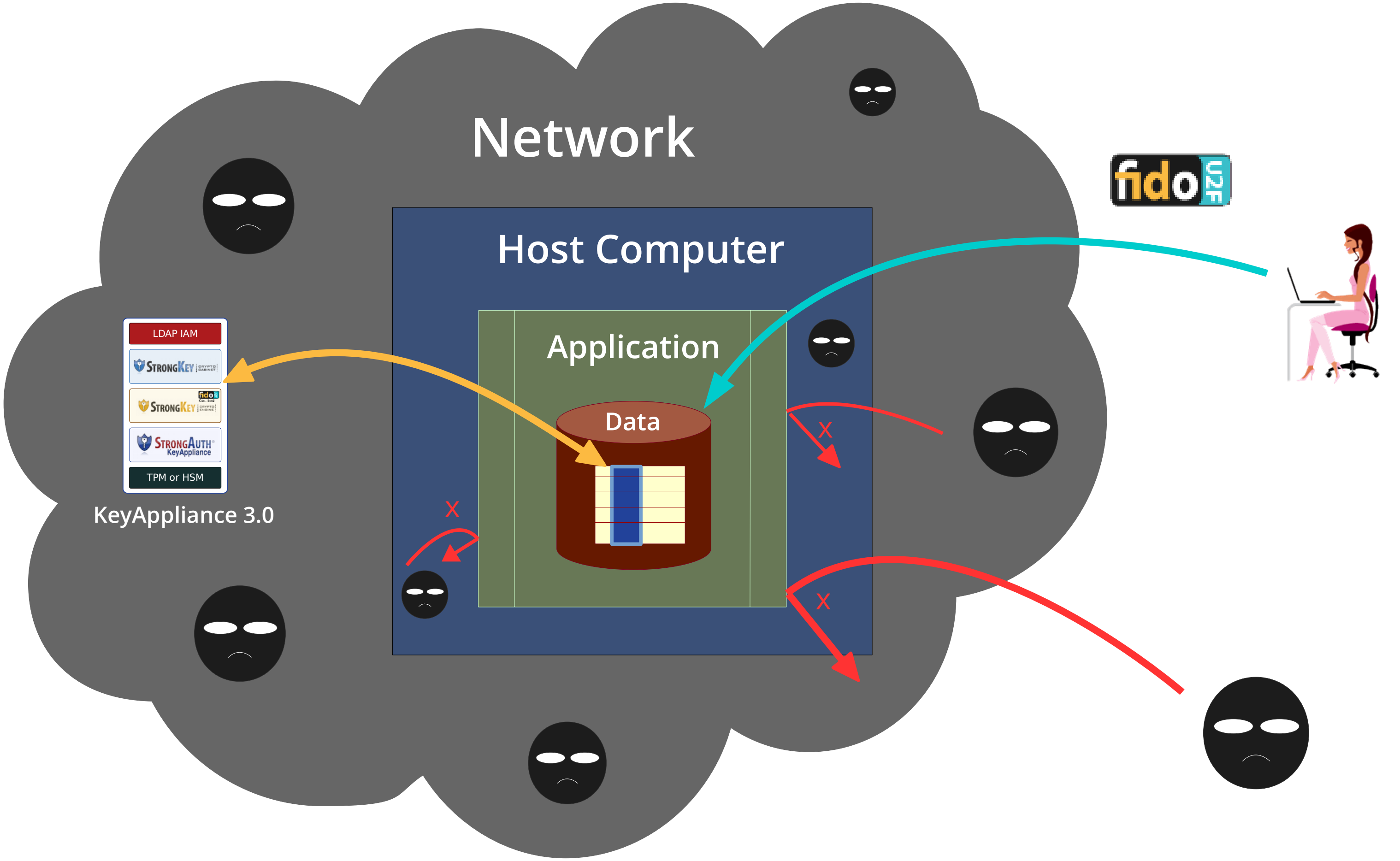
Why does FIDO matter?


ALESA
Application Level Encryption
Strong Authentication
Key Management Infrastructure
KMI
User
Application
Network
Database
Copyright © 2015 StrongAuth, Inc.

https://alesa.website

StrongAuth® Securing the Core — fido U2F Certified

Why does FIDO matter?



Resources

- FIDO Alliance
- FIDO Certified(TM) Products
- FIDO-DEV Mailing List
- Open-source FIDO Certified(TM) U2F Server - StrongKey CryptoEngine
- Open-source FIDO-enabled web-application - StrongKey CryptoCabinet
- Open-source FIDO-enabled web-application – StrongAuth PKI2FIDO
- StrongAuth's FIDO Demo Guide – You need a U2F Authenticator to use this
- StrongAuth's FIDO Demo and Tutorial site
- Status of Federal PKI Activities at Major Federal Departments & Agencies – US GAO

Questions?

- Contact information
  - Arshad Noor
  - (408) 331-2000
  - arshad.noor@strongauth.com