




FIDO-enabling a web-application using Universal 2nd Factor (U2F)

Arshad Noor
CTO, StrongAuth, Inc.

- Introduction
- Business Issues
- Operational Issues
- Technical Issues
- Security Issues
- Enablement Process
- Questions

- Founded in July 2001
- Silicon Valley-based, privately-held
- Open-source cryptographic solutions company
 - Public Key Infrastructure (PKI)
 - Symmetric Key Management System (SKMS)
 - Strong-Authentication
 - FIDO Alliance member with open-source  server
- Customers on 6 continents in:
 - Finance, Healthcare, e-Commerce, Medical Devices, Pharmaceutical, Entertainment, Manufacturing,



Business Issues

- Multiple authentication schemes
- Account Recovery
- FIDO Authenticator acquisition/support
- Which applications to FIDO-enable first?
- Protocol decision

Multiple Auth. Schemes

- UserID/Password
- LDAP/AD
- Biometric
- OTP
- 2-Step Verification
- Smartcard
- and now FIDO

- Forgotten/Lost/Stolen FIDO Authenticators
 - Policy
 - Internal vs. External customers
 - What security policy applies to them?
 - What applications must be accessible to them?
 - What is the intersection?
 - Recovery Process
 - Internal customers
 - External customers



Authenticator Acquisition

- FIDO Certified™ or “Go your own way”
- Should you standardize on one?
- A small set?
- All?
- Who pays for the Token?
- Support for “unsupported” FIDO Certified™ Tokens
 - Users are going to end up with multiple Tokens sooner or later



Which applications to enable first?

- Web-applications
 - Mission-critical vs. Nice-to-have
 - What authentication does it support currently?
 - Desired user experience?
 - FIDO with Password
 - FIDO with CAPTCHA (Password-less)
 - FIDO with Token Authentication (Password-less)
- Chrome 43 or greater
- Firefox...



FIDO with Password

Browser title: Login | StrongKey CryptoCabinet™ - Mozilla Firefox

Address bar: https://fidodemo.strongauth.com/skcc/login.jsp

Page content:

STRONGAUTH
Securing the Core

Help

Please login

Username

Password

[Not Registered? Create an account now](#)

Copyright © 2001 - 2015 StrongAuth, Inc.



FIDO + CAPTCHA (Password-less)

Login with CAPTCHA | StrongKey CryptoCabinet™ - Mozilla Firefox

https://fidodemo.strongauth.com/pno/captchalogin.jsp

Most Visited Centos Wiki Documentation Forums Gentoo StrongAuth FIDO Useful Java

STRONGAUTH
Securing the Core

Help

Login with FIDO Ready™ Authenticator

Username

Enter Code

dk02KL8

Login without a FIDO Token (password and 2-step)
Not Registered? [Create an account now](#)

Copyright © 2001 - 2015 StrongAuth, Inc.



FIDO U2F Password-less

Login with CAPTCHA | StrongKey CryptoCabinet™ - Mozilla Firefox

Login with CAPTCHA | Str... x +

https://fidodemo.strongauth.com/pnoc/captchalgin.jsp

Most Visited ▾ Centos Wiki Documentation Forums Gentoo ▾ StrongAuth ▾ FIDO ▾ Useful ▾ Java ▾

STRONGAUTH
Securing the Core

Help

Login with FIDO Ready™ Authenticator

Username

Login **Reset**

Login without a FIDO Token (password and 2-step)
[Not Registered? Create an account now](#)

Copyright © 2001 - 2015 StrongAuth, Inc.

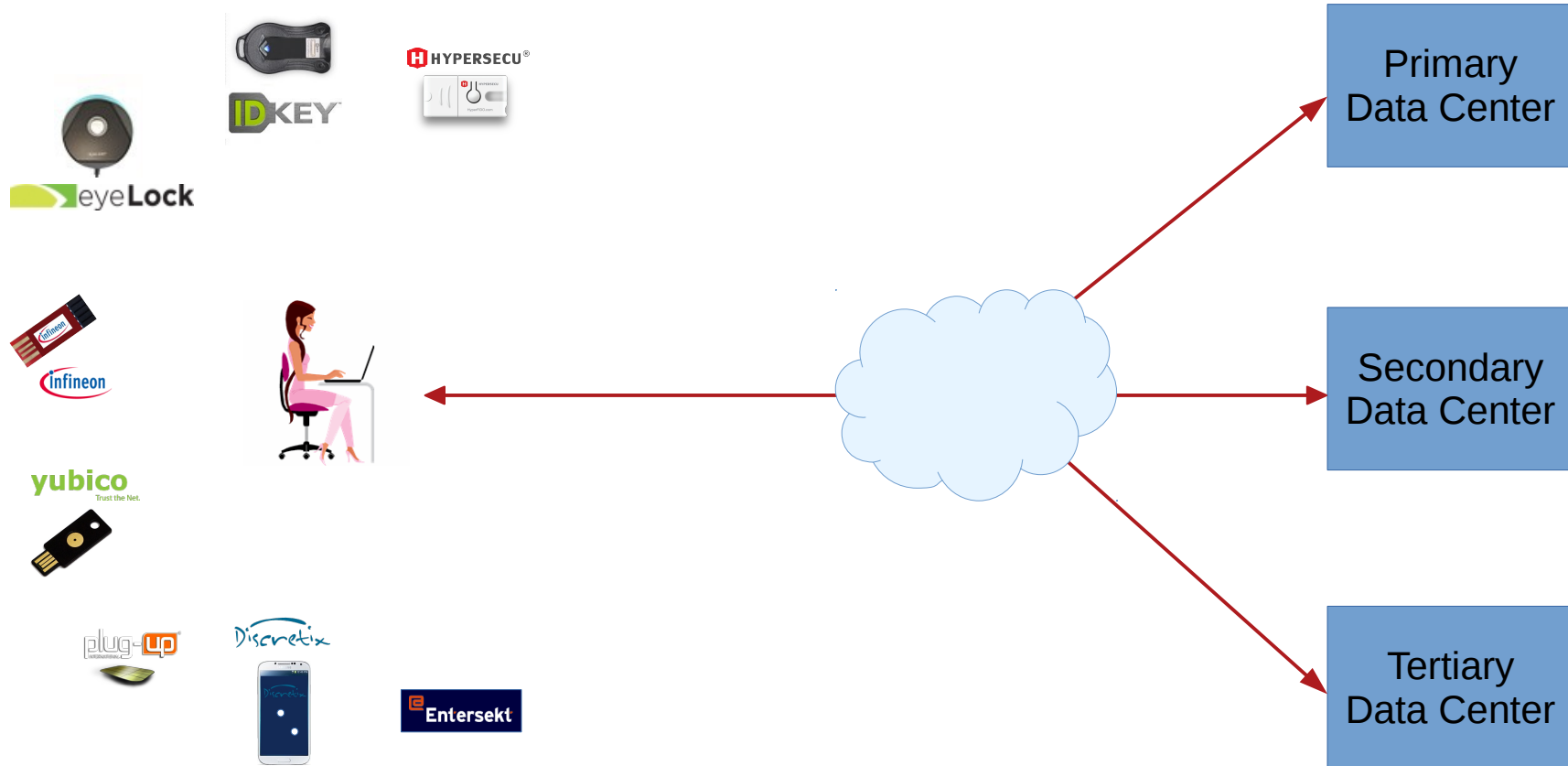
- Universal 2nd Factor (U2F)
- Universal Authentication Framework (UAF)
- FIDO 2.0



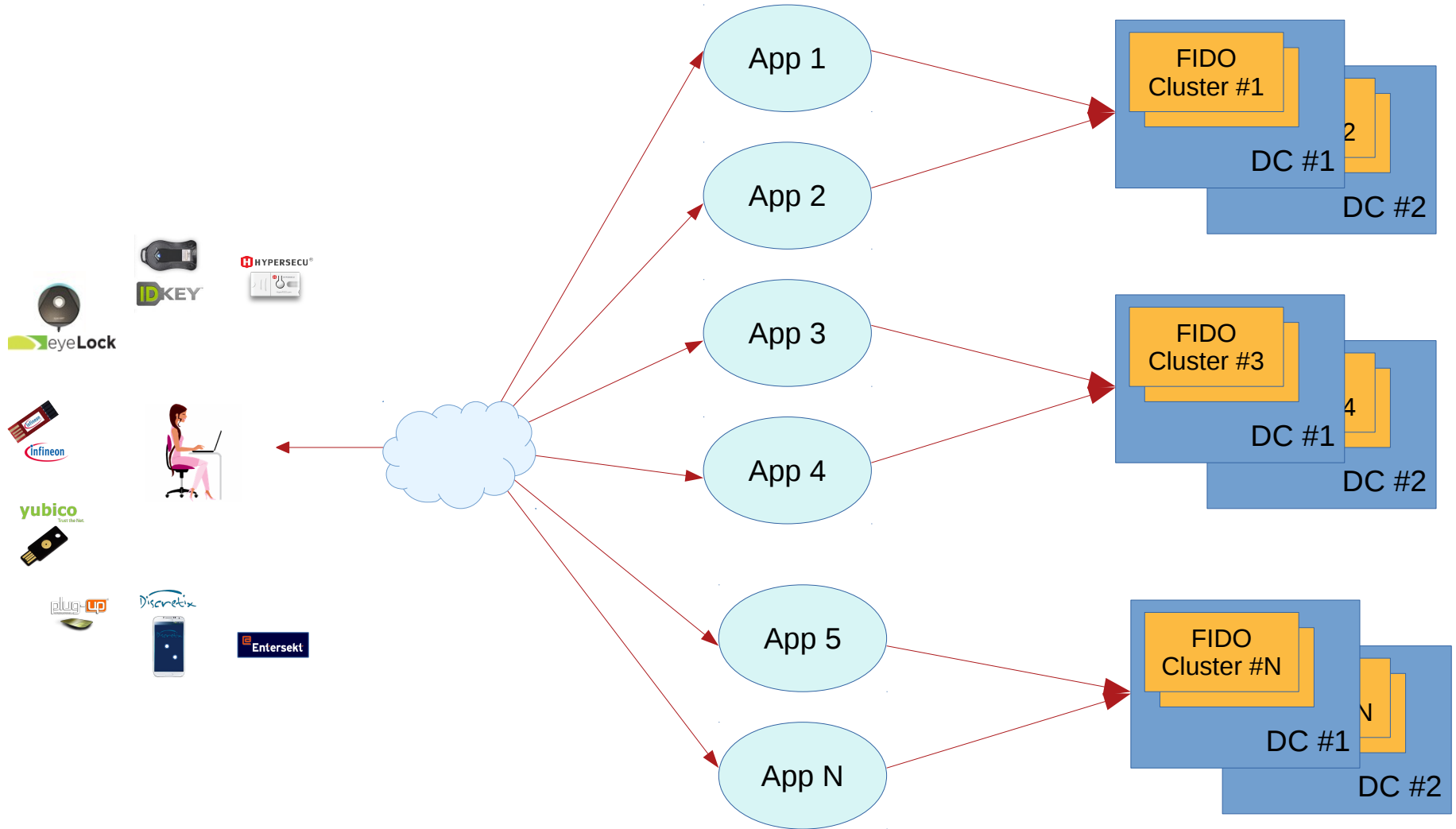
Operational Issues

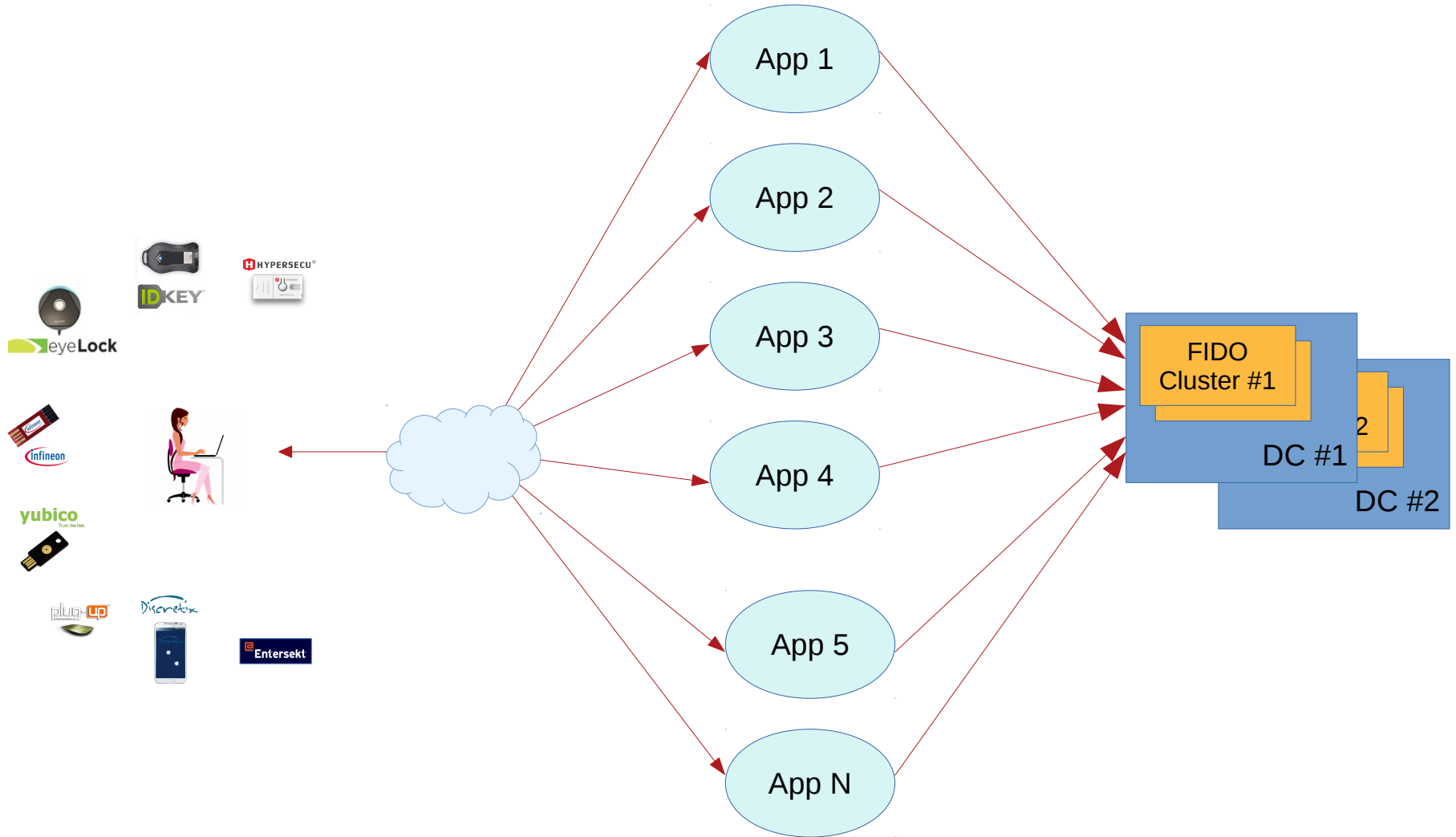
- Availability
- Scalability
- Security

Availability



Scalability - 1







Technical Issues

- Web-application framework
 - More than 90; Java (24), PHP (26), ...
- JavaScript
- Chrome dependency
- USB-port access

- 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
- “**S**ubstitution of **K**eys” Attack

Security - SuKs - 1

Jack



Jill



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

Jack



Jill



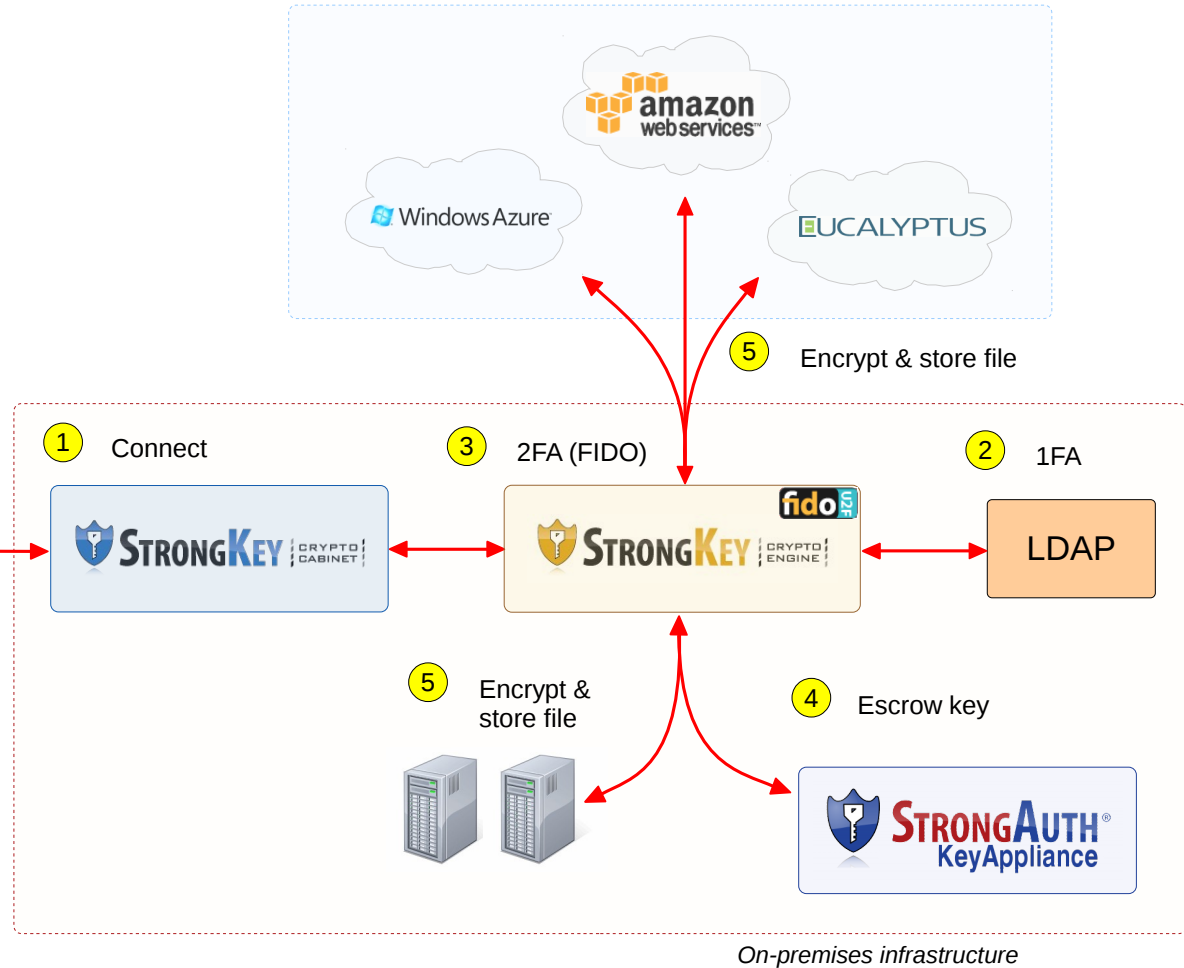
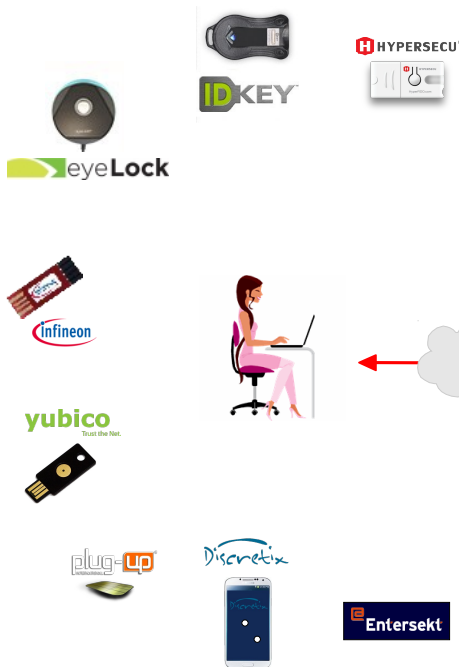
ID	User	Key Handle	Public Key
1234	Jack	CAFEBEEF	FEDCBA
1357	Jill	CAFEBEEF	FEDCBA
...

Enablement Process

- 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
- That's all, folks!

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.

fido U2F Strong-Authentication





Questions?

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