



Standards for
Simpler Stronger Authentication

Rajiv Dholakia – VP Products, Nok Nok Labs

rajiv@noknok.com

Context & Aspirations

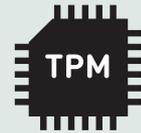
Taking lessons from History

Communication



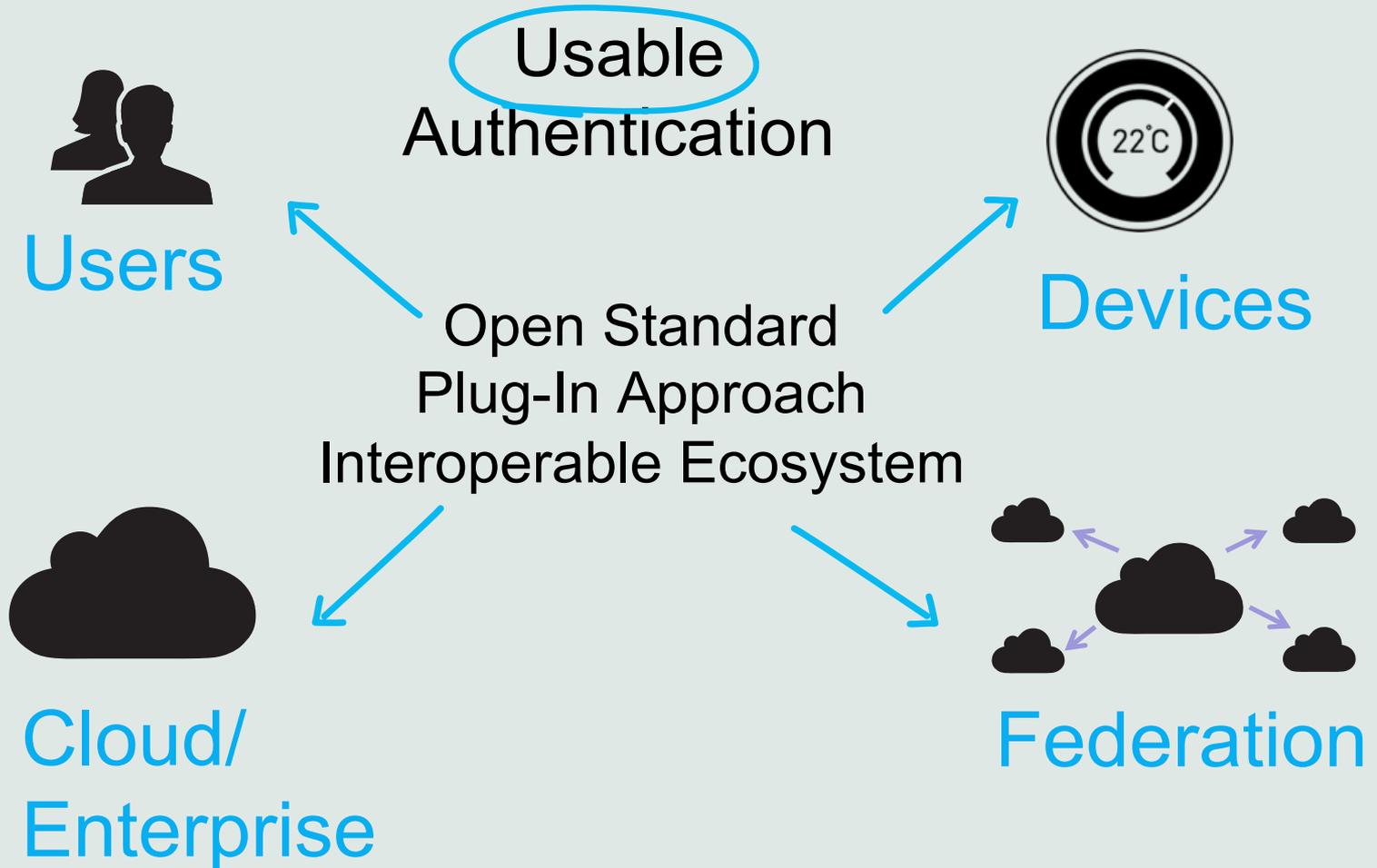
SSL

Authentication



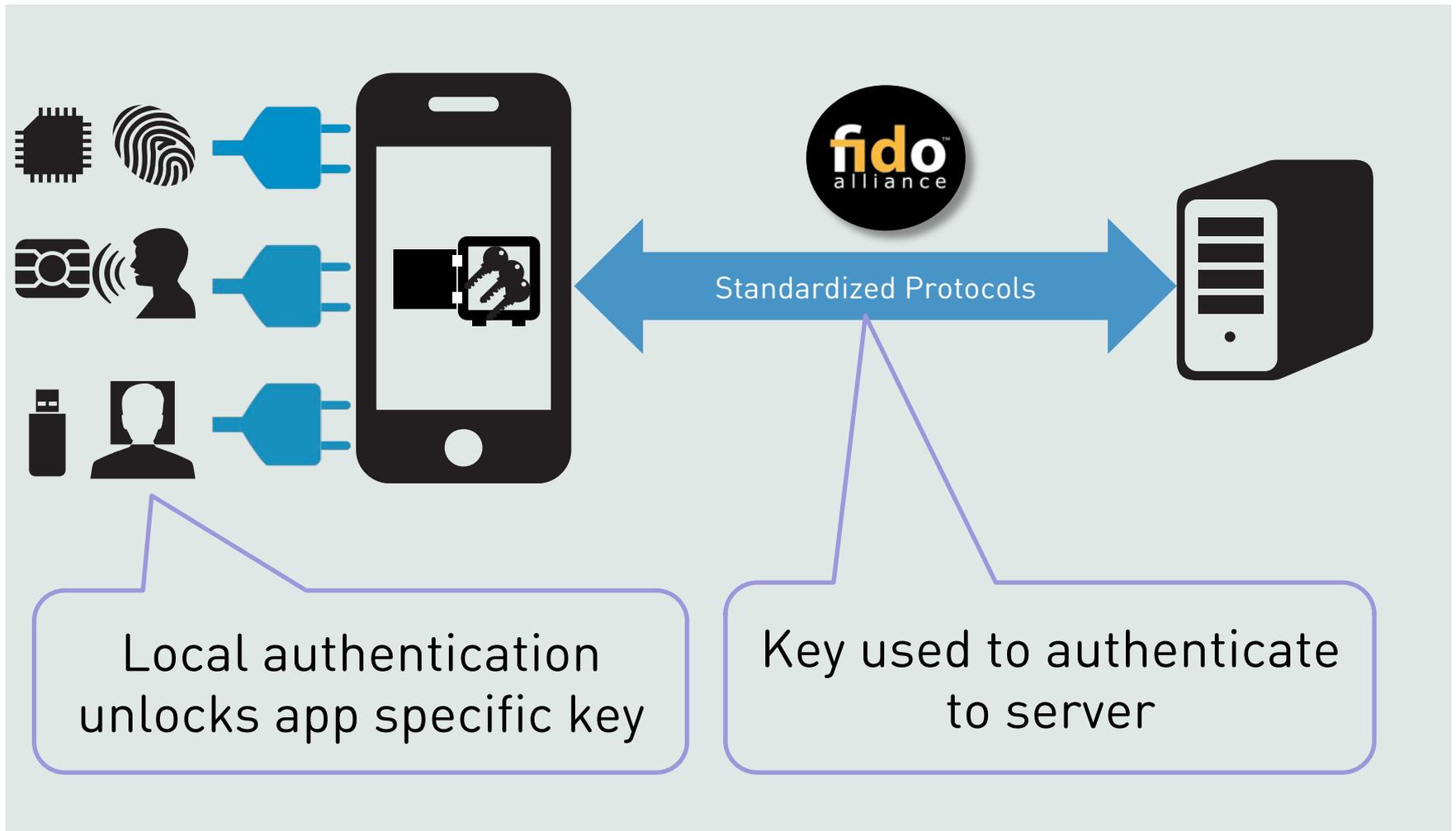
WHAT IS NEEDED

Common authentication plumbing

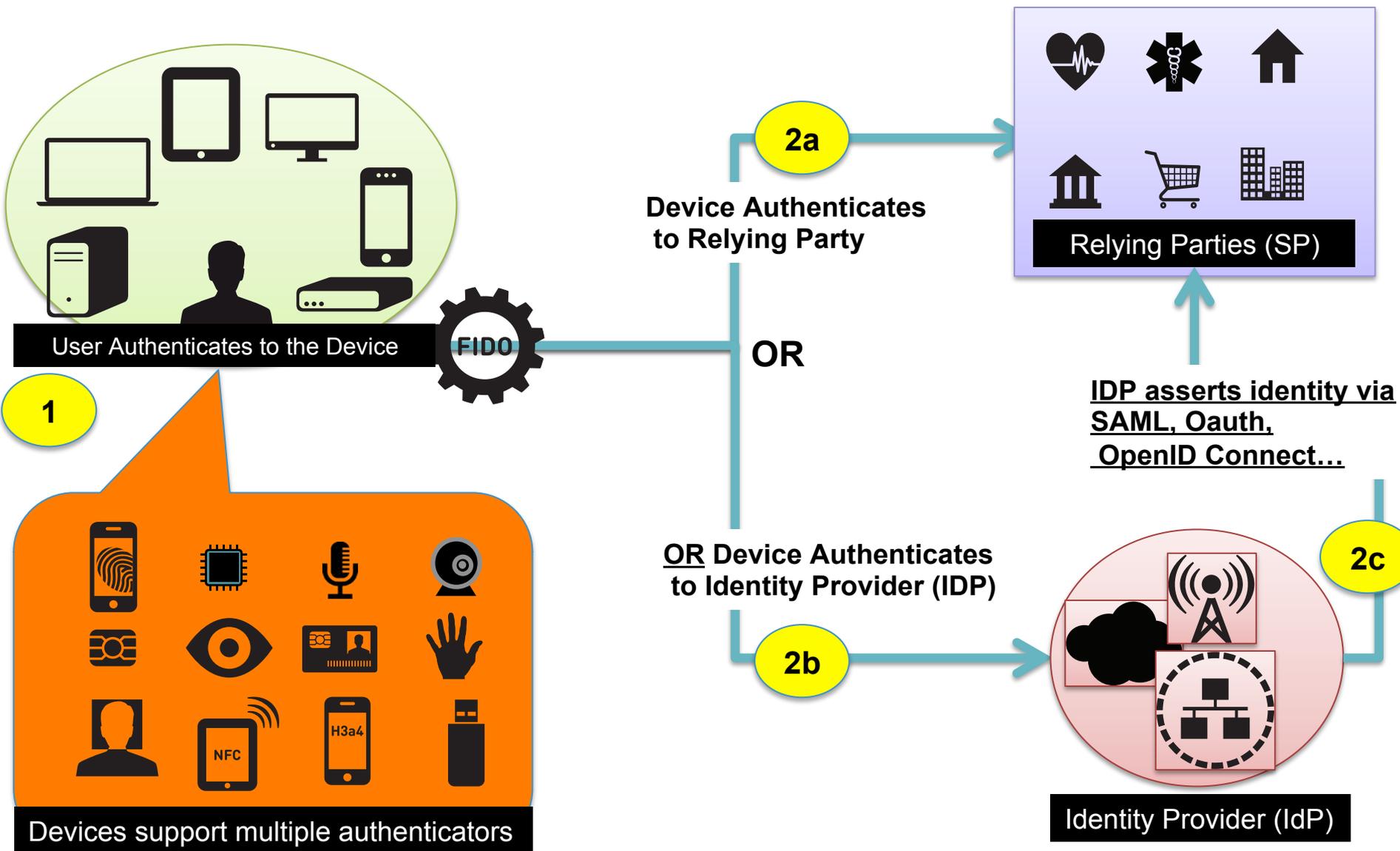


Simplifying and Scaling Authentication

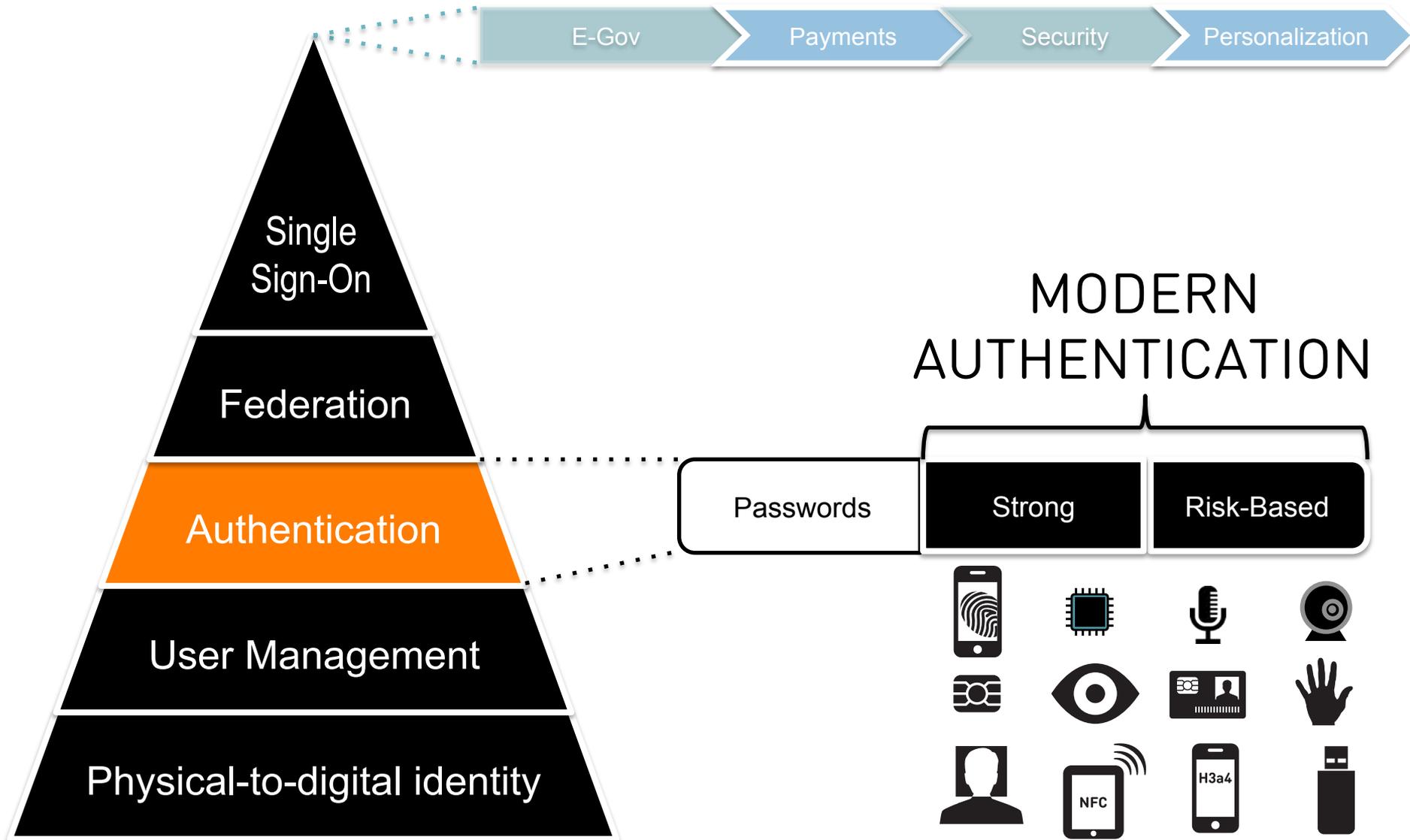
Any Device. Any Application. Any Authenticator.



FIDO Model: Direct to Relying Party OR through IdP



Identity & Authentication



FIDO Snapshot

May 2014

Goal: Simpler, Stronger Authentication

Mission: To Change Authentication Online by:

- (a) Developing unencumbered Specifications that define interoperable mechanisms that supplant reliance on passwords
- (b) Operating programs to help ensure industry adoption
- (c) Submitting mature Specifications for formal standardization

fidoTM
alliance
member

>120 Members and growing

19 Board Members (16+3)

up from 6 at launch in Feb '13



FIDO Alliance Role

- Paper Specifications, Interop and Conformance testing, Trademark licensing against criteria, thought leadership, nurture ecosystem of vendors delivering FIDO implementations to market
- Alliance does not ship products (only specifications)
 - Implementations left to commercial vendors
- FIDO Alliance designs core protocol
 - Like SSL, FIDO has no domain semantics
 - Relying parties and Vendors may adapt FIDO into commercial solutions
 - Vendors may deliver FIDO specification as product or service, standalone or as part of a solution stack
 - Extended use cases may be explored by vendors long before imported into protocol

Version 1.0 is in Public Review

**2014 V1.0 SPECS
NOW AVAILABLE.**

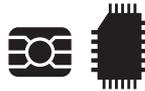
Be the first on your block.

Download now!



FIDO at Industry Events – Readiness

FIDO-Ready Products & Deployment for Mobile & More



SIM + Secure Element



Fingerprint, Mobile



Speaker Recognition



Mobile via NFC*



PIN + MicroSD, USB



OEMs SHIPPING FIDO-READY™ PRODUCTS

New and existing devices are supported



**OEM Enabled: Lenovo ThinkPads with
Fingerprint Sensors**



OEM Enabled: Samsung Galaxy S5



Clients available for these operating systems :



Software Authenticator Examples:
Voice/Face recognition, PIN, QR Code, etc.

Aftermarket Hardware Authenticator Examples:
USB fingerprint scanner, MicroSD Secure Element

First FIDO Deployment already live...

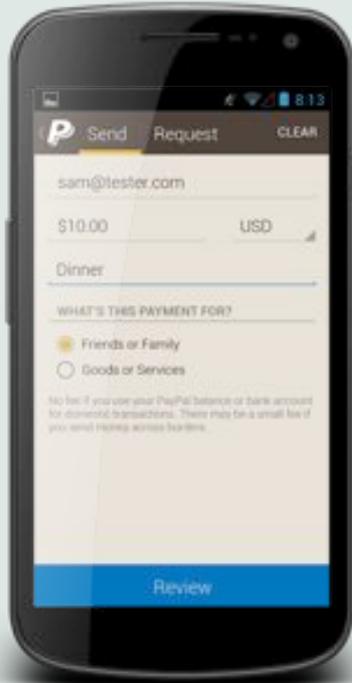
- Customers can use their finger to pay with PayPal from their new Samsung Galaxy S5 because the FIDO Ready™ software on the device securely communicates between the fingerprint sensor on their device and PayPal's service in the cloud. **The only information the device shares with PayPal is a unique cryptographic “public key”** that allows PayPal to verify the identity of the customer **without having to store any biometric information on PayPal's servers.**



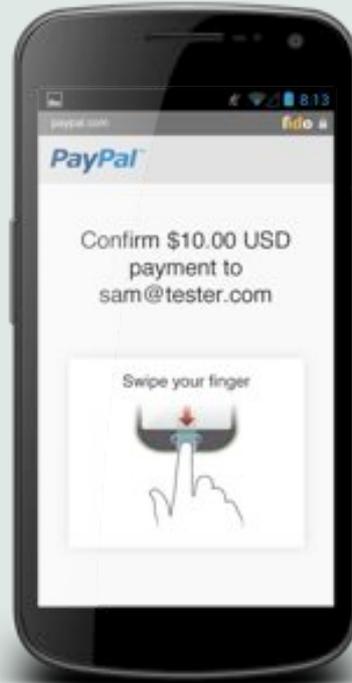
Better Security, Better User Experience

Going beyond "Risk, Regulation, Reputation"

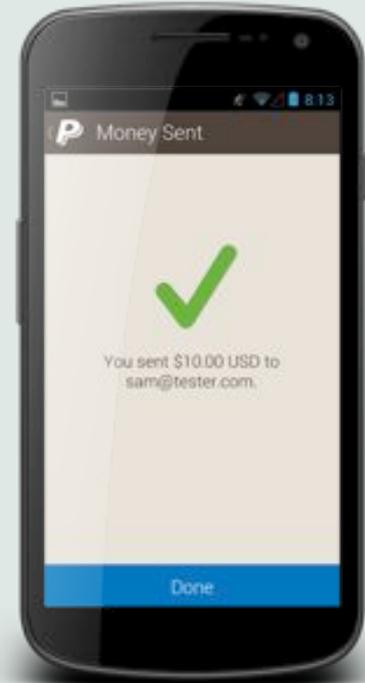
DESIGN, DELIGHT & DOLLARS!



Setup



Confirm



Sent

Appendix

FIDO 101

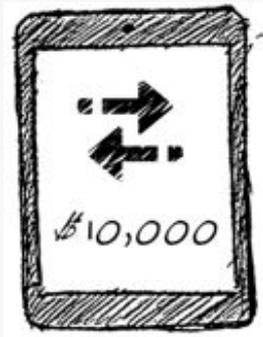
FIDO Experiences

ONLINE AUTH REQUEST

LOCAL DEVICE AUTH

SUCCESS

PASSWORDLESS EXPERIENCE (UAF standards)



Transaction Detail



Show a biometric



Done

SECOND FACTOR EXPERIENCE (U2F standards)



Login & Password



Insert Dongle, Press button

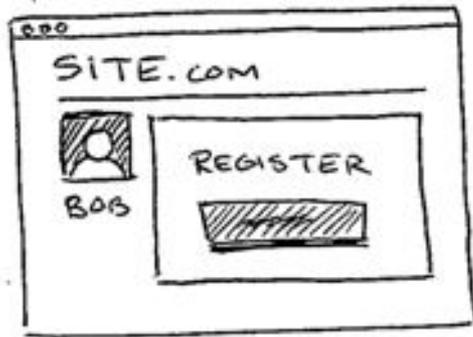


Done

FIDO Registration

1

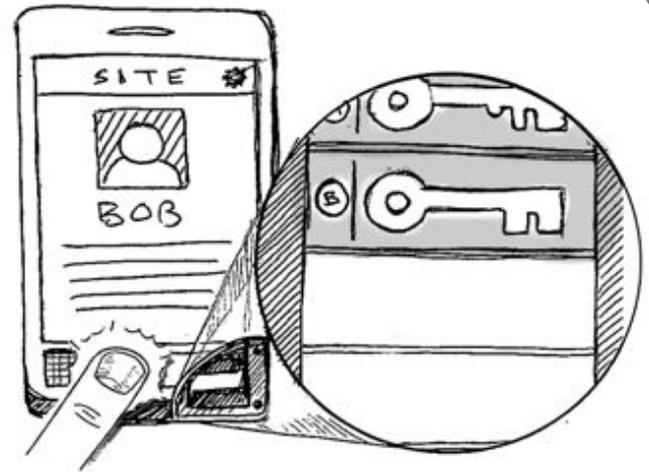
REGISTRATION BEGINS



USER APPROVAL

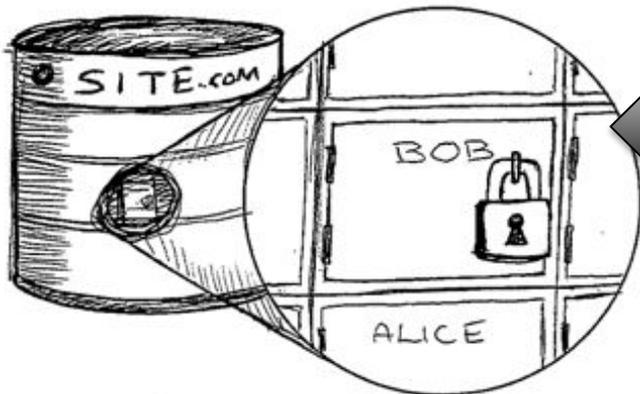
USER APPROVAL

2



4

REGISTRATION COMPLETE

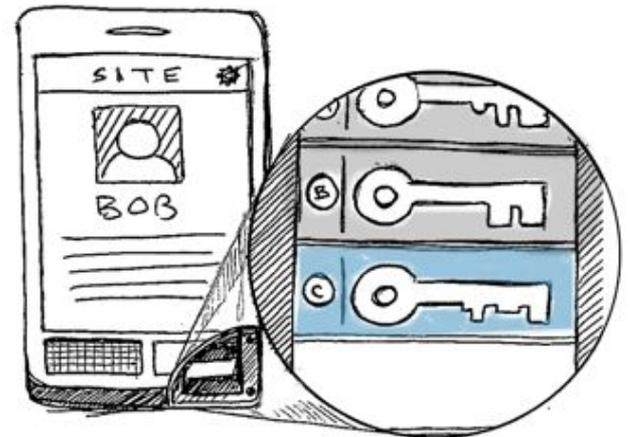


KEY REGISTERED

Using
Public key
Cryptography

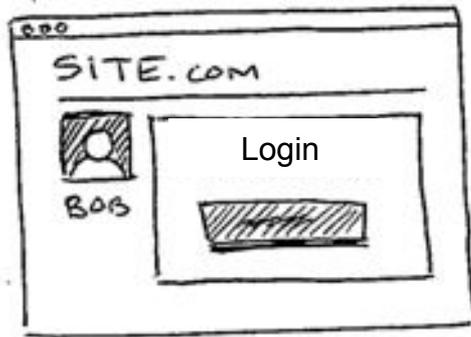
NEW KEY CREATED

3

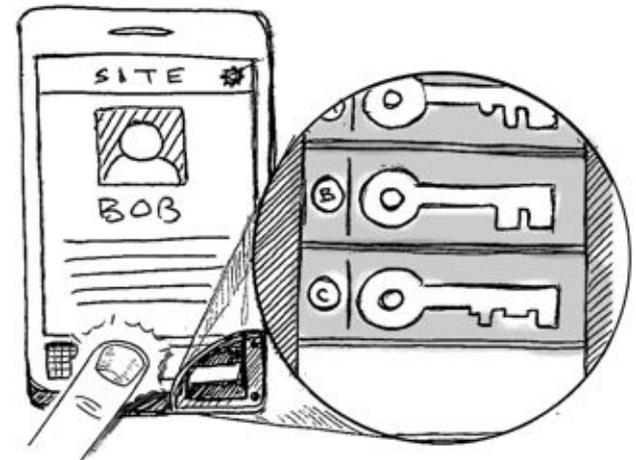


FIDO Login

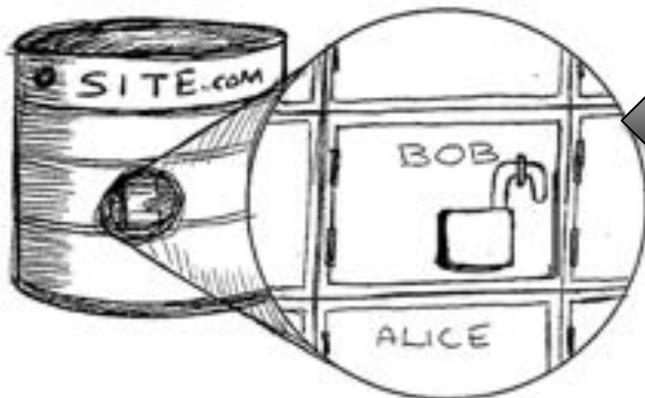
1 LOGIN



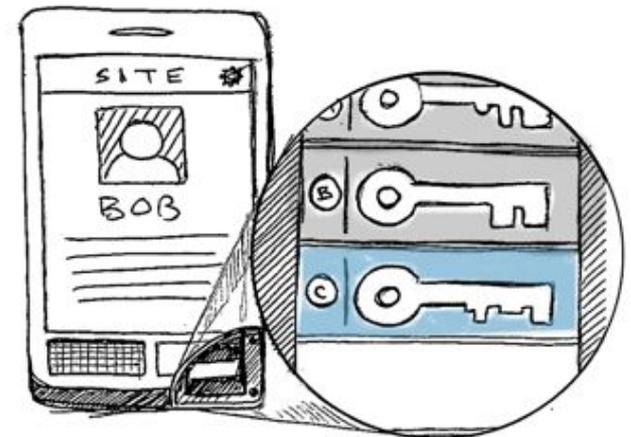
2 USER APPROVAL



4 LOGIN COMPLETE



3 KEY SELECTED



LOGIN CHALLENGE

LOGIN RESPONSE

Using
Public key
Cryptography

Decouple User Verification Method from Authentication Protocol

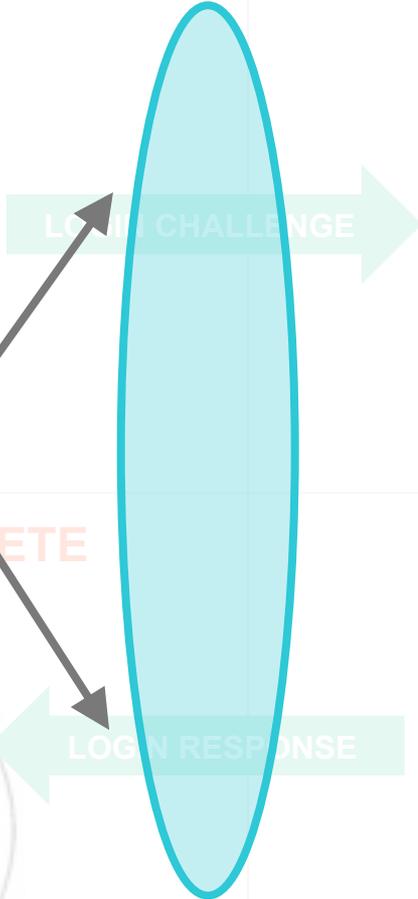
1

LOGIN

USER APP

PLUGGABLE LOCAL AUTH

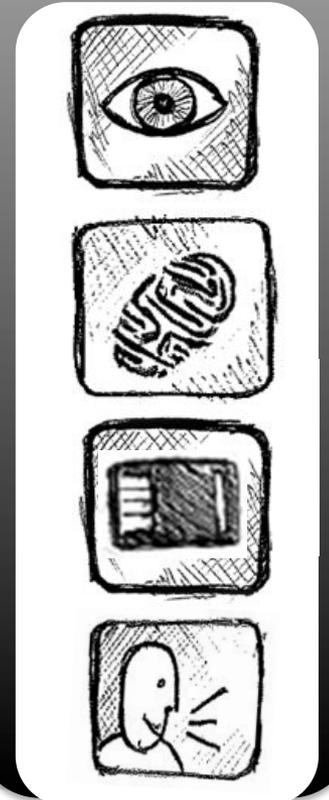
ONLINE SECURITY PROTOCOL



4

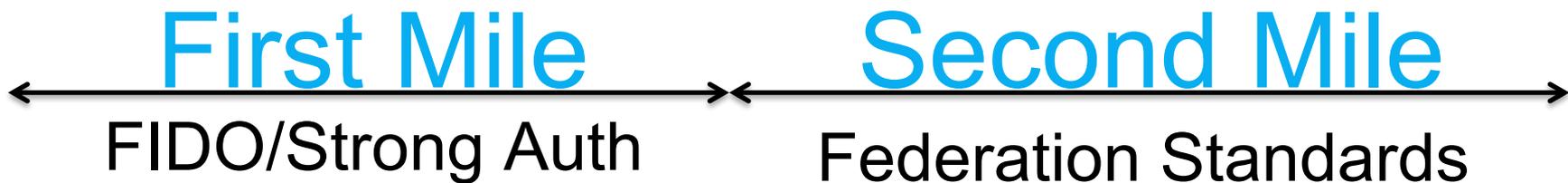
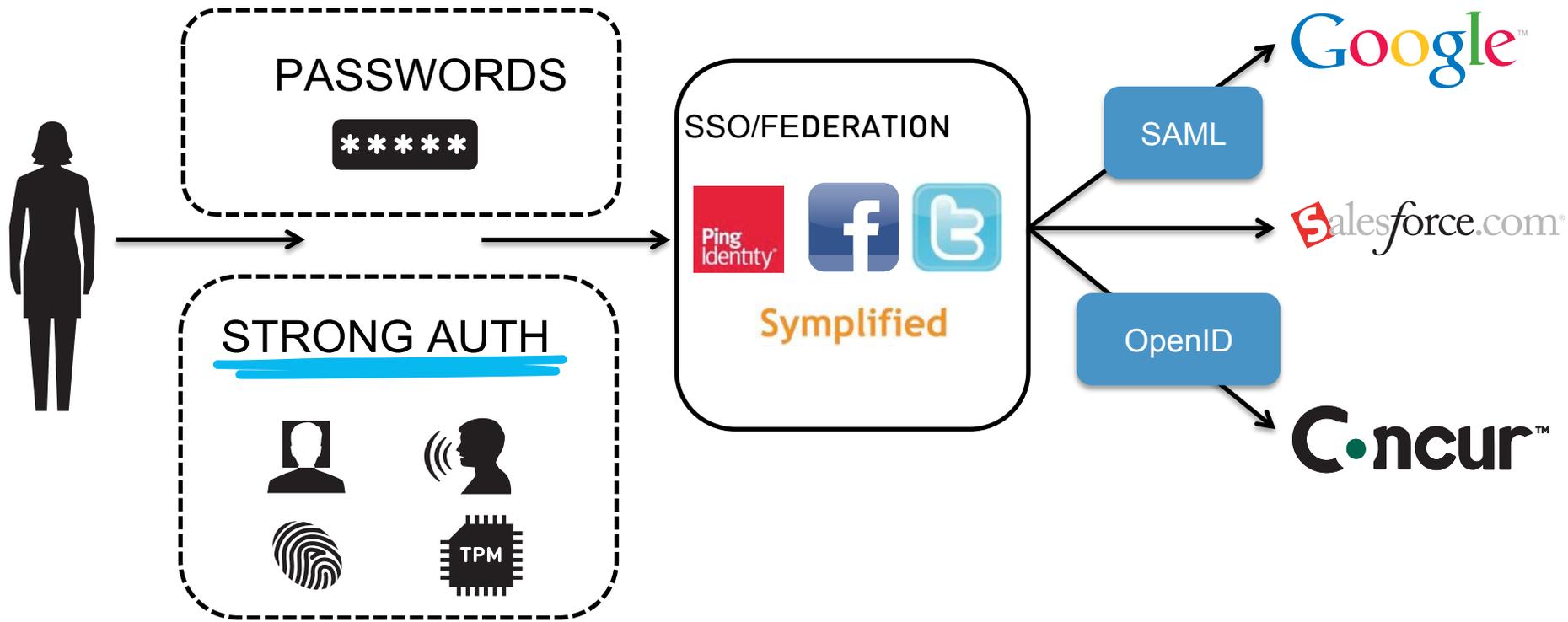
COMPLETE

KEY SELECTION

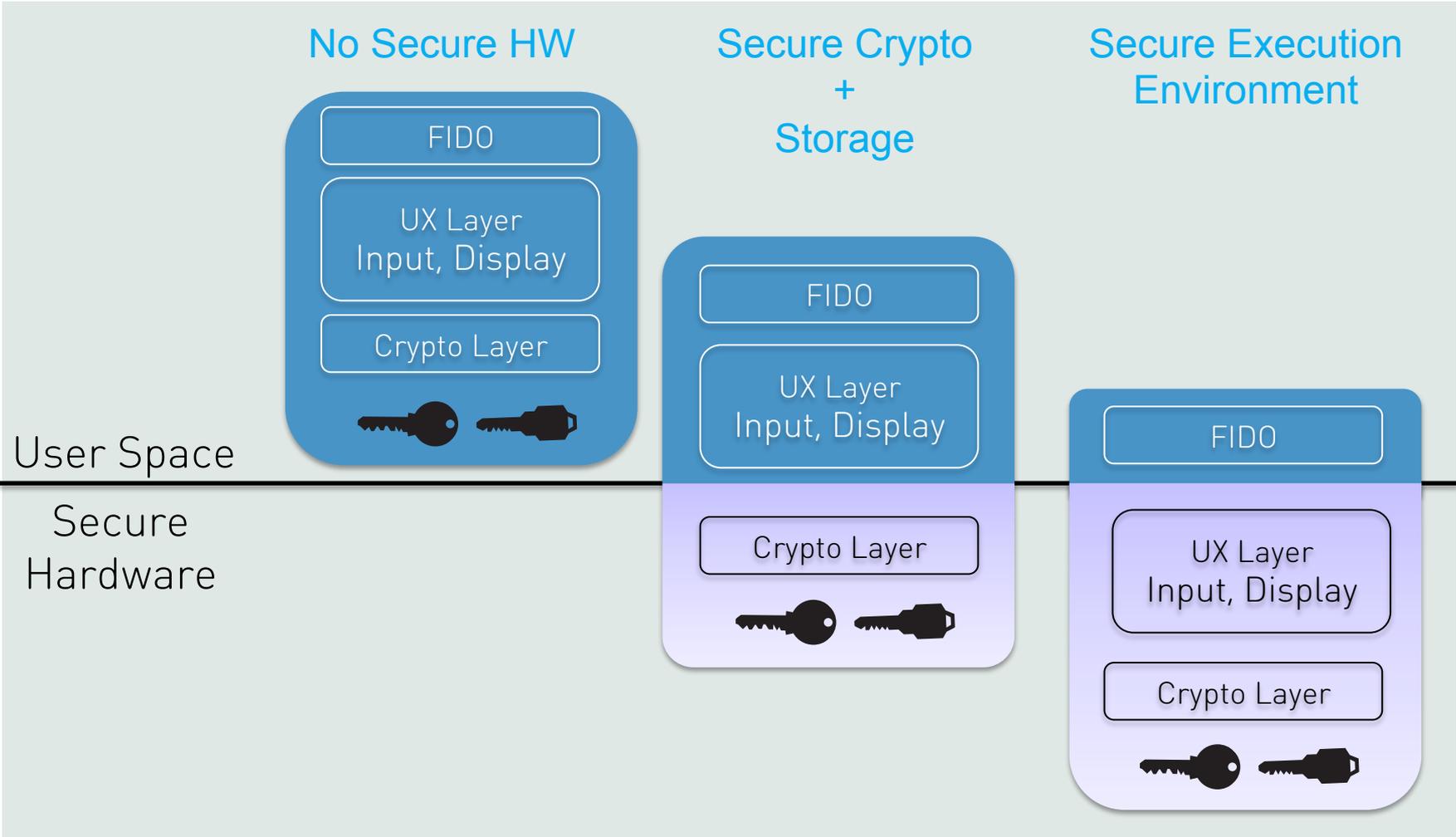


Leverage public key cryptography

COMPLEMENTS IDENTITY & FEDERATION STANDARDS



Choice of Security Profiles

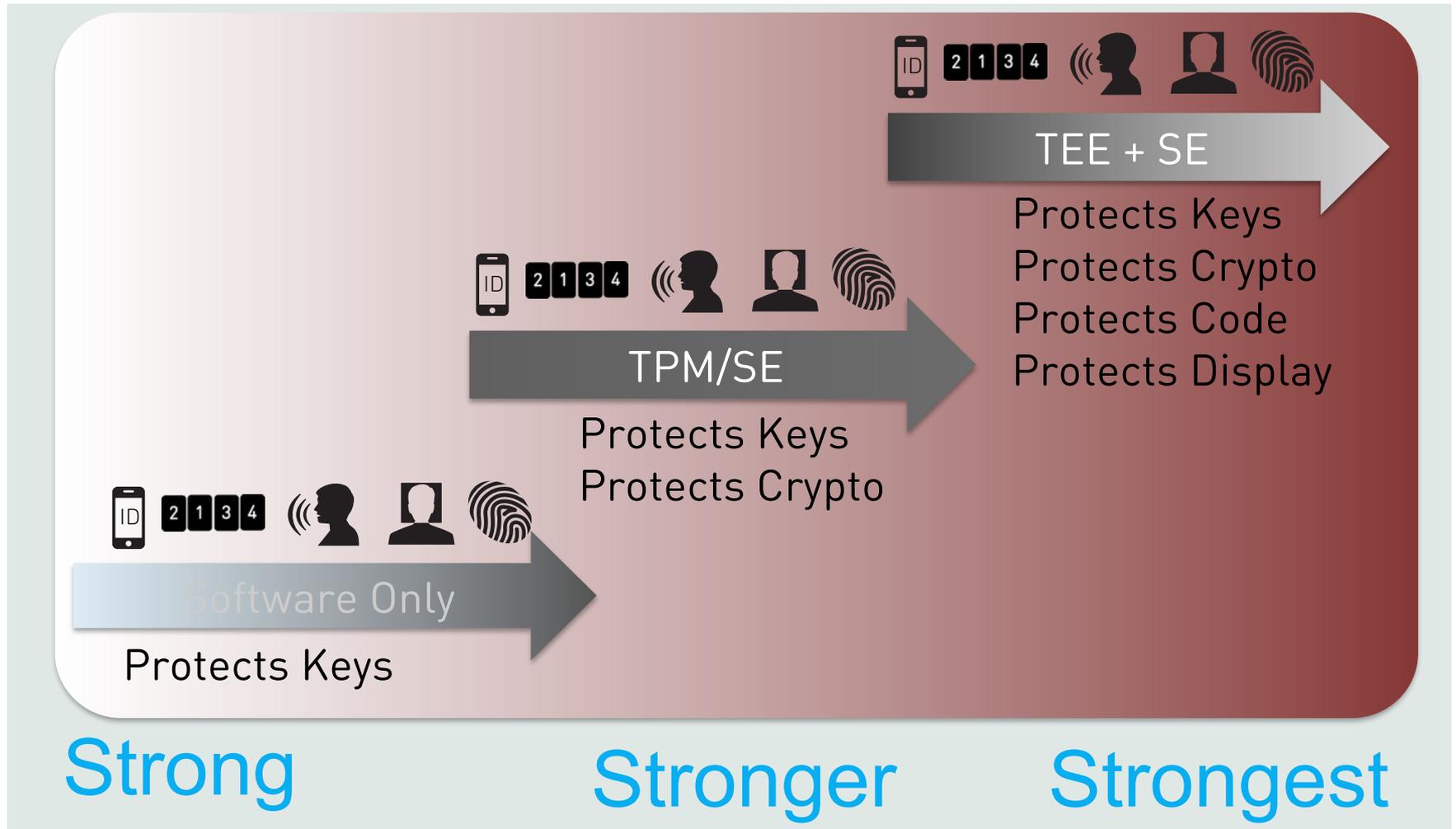


DESIGN CONSIDERATIONS

- No 3rd party in the protocol flow required
- No shared symmetric secrets on server
 - Stops scalable attacks
- Biometric data never leaves personal device
- Unique key-pair per site/app you interact with
 - No linkability between sites – privacy measures
- Embrace all authenticators
- Risk appropriate authentication choices

Risk Appropriate Authentication

FIDO Security Spectrum



CONCLUSIONS

- The enemy is symmetric shared secrets
- The enemy is poor user experiences and friction
- FIDO is a building block
- Even simple software-based authenticator with a pin offers many advantages over passwords
- FIDO complements your investments in federation and improves your security and ease of use



THANK YOU