



Cloud Security, OCT 2014

Sami Nassar
VP & GM Authentication
NXP Semiconductors



Online Authentication

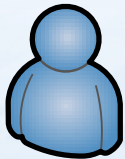
Username and password prevalent for the past 40 years: Still adapted?

Although I connect to 8 different services per day, I use some of them very seldom and sometimes

I own 25 online accounts.

Do you expect me to

remember a password re-initialization costs \$15 to the service provider



User



Service
Provider

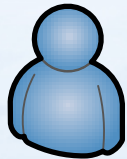
- **Account takeover rose by 50% in 2012** (Javelin March 2013)
- **Average 25 accounts per user**
- **6.5 different passwords**
- **8 services used per day in average**
- **\$15 per password re-initialization**
- *Passwords are being*
 - **Reused**
 - **Phished**
 - **Keylogged**

Online Authentication

Multi-factors authentication proved efficiency in reducing fraud

Multi-Factor Authentication, e.g. a token and a secret (Pin or password) proved very secure

I don't want to carry one physical token for each of my accounts.



User



Service
Provider

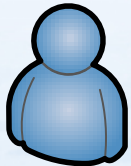
- With Chip-and-PIN card introduction in UK, fraud has decreased by 69%
- For user convenience, tokens should be shared between services

Online Authentication

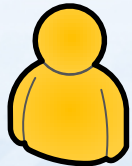
PC is no longer the only access platform

- 64% of Facebook users via Smartphone, up by 57% year-over-year (FB Q4-12)
- By 2016, 100M homes will be equipped with SmartTV in US and Western Europe (NPD In-Stat 2012)
- Must have consistent level of security through all platforms
- Solution must be user-friendly: avoid too many user manipulations

What about securing accesses through my game console? My connected car?



User



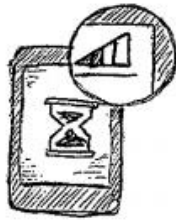
Service
Provider

Security level is defined by the weakest link. We must insure utmost security through all platforms

OTPs are not easy to use nor secure enough

One Time Codes

Improves security but not easy enough



SMS USABILITY

Coverage | Delay | Cost



DEVICE USABILITY

One per site | Fragile



USER EXPERIENCE

User confusion



STILL PHISHABLE

Known attacks today

Other topics around authentication



- ◆ Device based (Geo-location)
- ◆ Knowledge based
- ◆ Client side certificates
- ◆ Grid cards
- ◆ Out of band (e.g. SMS)
- ◆ Open ID, SAML
- ◆ Virtual keyboards
- ◆ Key stroke biometrics
- ◆ Graphical password systems
- ◆ Password Manager
- ◆ Voice, facial,...
- ◆ One time password systems
- ◆ SQRL-Secure, Quick, Reliable, L.
- ◆ Apps (SlickLogin (sound))



FIDO Simpler Stronger Authentication

A total of >140 partners engaged in making online authentication more secure.

INTERNET SERVICES



COMPONENT & DEVICE VENDORS



SOFTWARE & STACKS



FIDO Value Proposition

Key Feature: Standard Public Key Cryptography

- User device generates new key pair and provides public key to server
- Server asks user device to sign data to verify user

Easy to deploy:

BYOD registration model(no issuance), no middleware, no PKI

Interoperability:

Open standard and alliance (client and server)



Security:

Public key crypto, no phishing, no MITM, tamper resistant(SE)

Privacy:

Site specific keys, no unique ID per device

MITM: Man-in-the-middle

FIDO is promoting two authentication protocols

UAF

ONLINE AUTH REQUEST

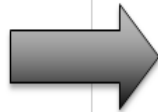
LOCAL DEVICE AUTH

SUCCESS

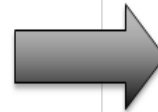
PASSWORDLESS EXPERIENCE



Transaction Detail



Show a biometric



Done

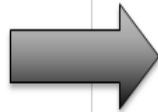


U2F

SECOND FACTOR EXPERIENCE



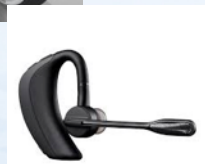
Login & Password



Insert Dongle, Press button



Done



Several keys in different form factors can access same service



Embedded SE



Bluetooth Dongle



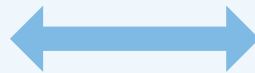
NFC Wearable
Tap and access



USB/NFC Key
Tap and access



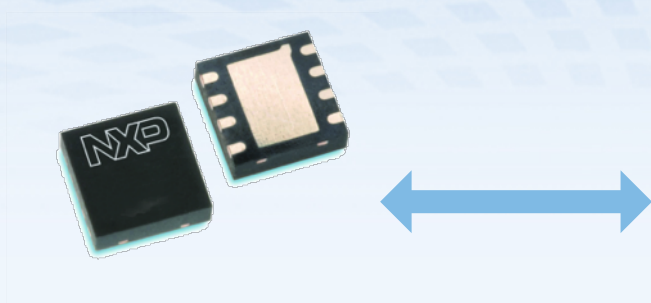
USB/ Key
Always in your PC



EXTRADE®

For example

One key for many services / Bring your own Key



- . The key is static and only holds the private key
- . The user registers the key to access the relevant cloud services

Confirmation for DentistryForFun.com

Please confirm that you want to share your dental records with Dr. Payne.

FIDO PIN

Or cancel the transaction

fido

Confirmation for DentistryForFun.com

Please confirm that you want to share your dental records with Dr. Payne.

FIDO PIN

Or cancel the transaction

fido

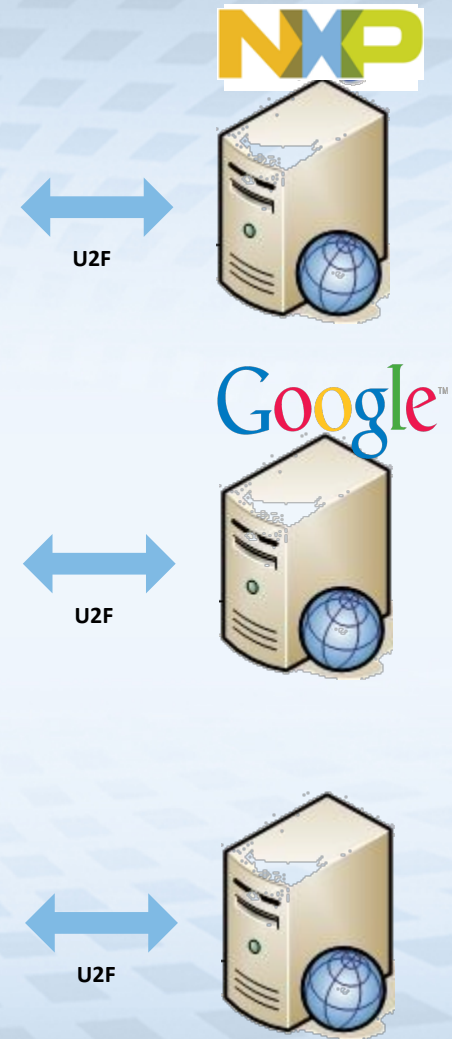
Confirmation for DentistryForFun.com

Please confirm that you want to share your dental records with Dr. Payne.

FIDO PIN

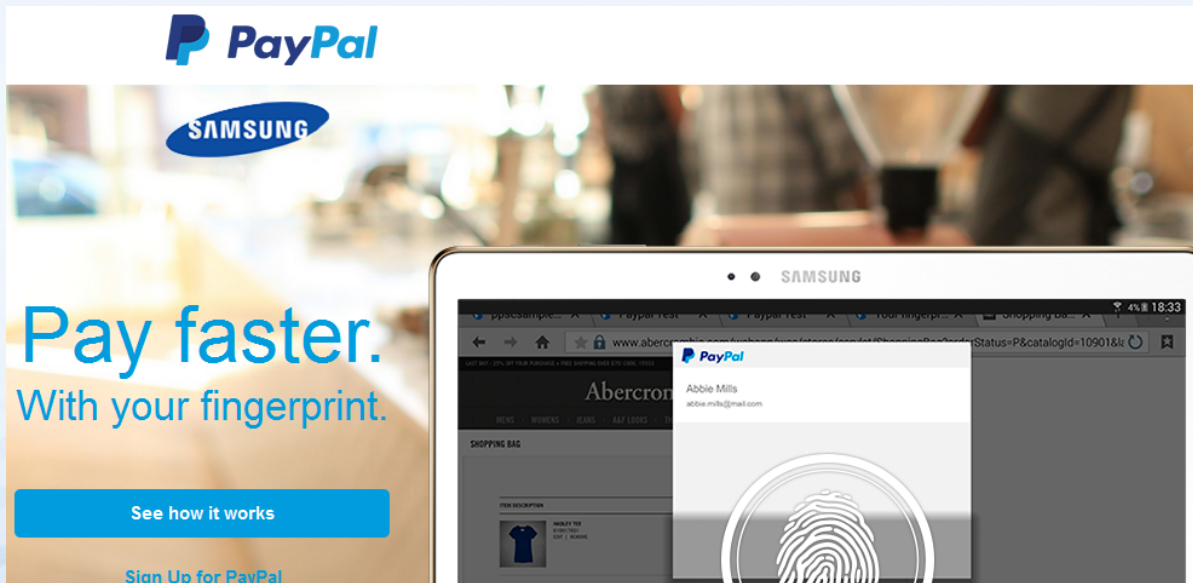
Or cancel the transaction

fido



First FIDO UAF deployment

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.**



First FIDO U2F deployment/

FIDO U2F focusses on consumer use cases with Online Services. Its standard functionality supports enterprise use cases e.g. web services. To support additional features so sort of middleware might be required

- ▶ Google
- ▶ Web services
- ▶ Enterprise Security Applications
 - Windows Logon
 - HD encryption
 - Email encryption
- ▶ Mobile device support (NFC, Bluetooth)

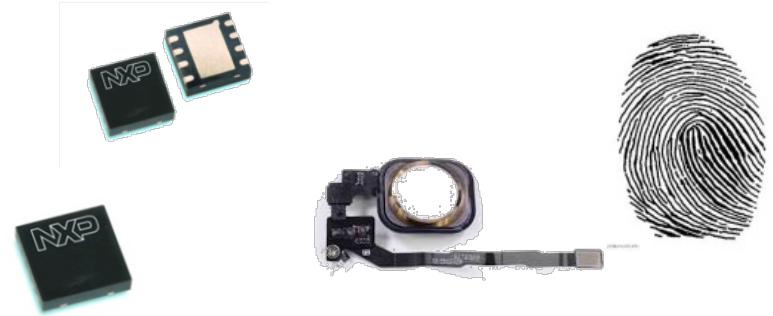


FIDO U2F Authenticators

USB keys



Embedded



BLE keys

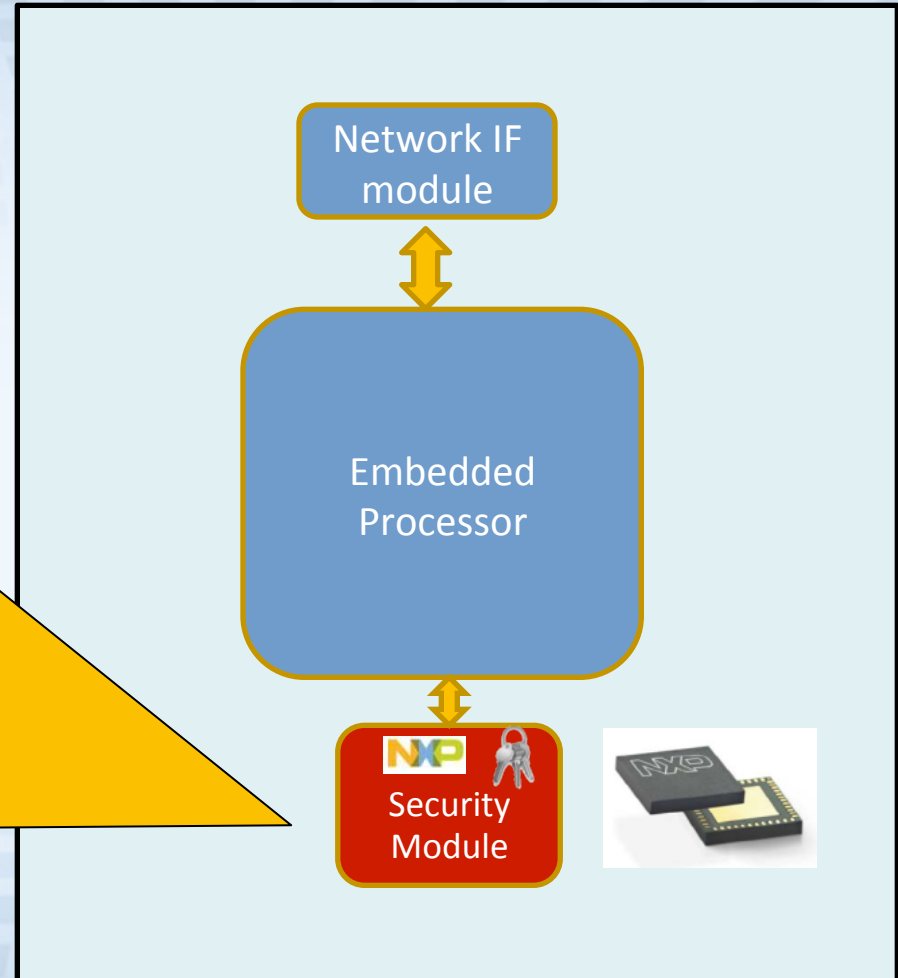


Wearables



Secure Element provides key security functions

- Strong Authentication
- Key agreement
- Data Encryption
- Digital signature generation/verification
- Secure storage
- True Random Number Generation
- Cryptographic accelerators
- Tamper resistance
- Strong Root of Trust



NXP Semiconductor



Thank you

Customer-focused passion to win

