INTRODUCTION TO FIDO AUTHENTICATION

Brett McDowell, Executive Director, FIDO Alliance
brett@fidoalliance.org
The world has a **PASSWORD PROBLEM**
Data Breaches...

781 data breaches in 2015

170 million records in 2015 (up 50%)

$3.8 million cost/breach (up 23% from 2013)
“95% of these incidents involve harvesting credentials stolen from customer devices, then logging into web applications with them.”

2015 Data Breach Investigations Report
ONE-TIME PASSCODES

Improve security but aren’t easy enough to use

- SMS Reliability
- Token Necklace
- User Confusion
- Still Phishable
The world has a “SHARED SECRETS” PROBLEM
WE NEED A NEW MODEL
THE NEW MODEL

Fast IDentity Online

online authentication using public key cryptography
THE FIDO PARADIGM
HOW FIDO WORKS

The user authenticates “locally” to their device (by various means)

The device authenticates the user online using public key cryptography
FIDO Registration

1. User is in a Session Or New Account Flow

2. Invitation Sent

3. New Keys Created

4. Public Key Registered With Online Server

Registration Complete
FIDO Authentication

User needs to login or authorize a transaction

1. FIDO Challenge
2. User Approval
3. Key Selected & Signs
4. Signed Response verified using Public Key Cryptography

Login Complete
OPEN STANDARDS R.O.I.

- FIDO-ENABLE ONCE
- GAIN EVERY DEVICE YOU TRUST
- NO MORE ONE-OFF INTEGRATIONS
USABILITY, SECURITY, R.O.I. and PRIVACY
No 3rd Party in the Protocol

No Secrets on the Server Side

Biometric Data (if used) Never Leaves Device

No Link-ability Between Services

No Link-ability Between Accounts
The FIDO Alliance is an open industry association of over 250 organizations with a focused mission: authentication standards.
Board Members

aetna®
Alibaba Group
American Express
ARM®
Bank of America.
BCcard
CrucialTec
Daon
egis Technology
FEITIAN
Google
Infineon
ING
Intel®
Lenovo
MasterCard
Microsoft
Nak Nak LABS
NTT docomo
NXP
oberthur TECHNOLOGIES
PayPal
Qualcomm®
RSA
Samsung
Synaptics®
USAA®
VASCO
VISA
yubico

All Rights Reserved. FIDO Alliance. Copyright 2016.
Government Members
Liaison Partners
FIDO Adoption
Deployments are enabled by over 250 FIDO® Certified products available today
# of Certified FIDO Products since program launch

- Apr-15: 32
- Jul-15: 62
- Sep-15: 74
- Dec-15: 108
- Mar-16: 162
- May-16: 216
- Aug-16: 253
Leading OEMs Shipping FIDO Certified Devices

Samsung
- S5, Mini
- Alpha
- Note 4,5
- Note Edge
- Tab S, Tab S2
- S6, S6 Edge
- S7, S7 Edge

Sharp
- Aquos Zeta

Sony
- Xperia Z5
- Xperia Z5 Compact
- Xperia Z5 Premium

Sharp
- V1
- G5

Sony
- Phab2
- Phab2 Pro

Fujitsu
- Arrows NX
- Arrows Fit
- Arrows Tab

Huawei
- Mate 8

Lenovo
- ZUK

All Rights Reserved. FIDO Alliance. Copyright 2016.

23
FIDO Applications Now Run on iOS

Supported iOS Fingerprint Devices

- iPhone SE
- iPhone
- iPhone+
- iPad Air
- iPad Mini
- iPad Pro
Better security for online services
Reduced cost for the enterprise
Simpler and safer for consumers
POLICY DISCUSSION
FIDO specifications offer governments newer, better options for strong authentication – but governments may need to update some policies to support the ways in which FIDO is different.

As technology evolves, policy needs to evolve with it.
1. Recognize that two-factor authentication no longer brings higher burdens or costs.

“another commenter pointed out that current approaches to multi-factor authentication are costly and burdensome to implement”


- While this statement was true of most “old” MFA technology, FIDO specifically addresses these cost and usability issues.
  - FIDO enables simpler, stronger authentication capabilities that governments, businesses and consumers can easily adopt at scale.
2. Recognize technology is now mature enough to enable two secure, distinct auth. factors in a single device.

- Recognized by the US government (NIST) in 2014...

- "OMB (White House) to update guidance on remote electronic authentication" to remove requirements that one factor be separate from the device accessing the resource

- The evolution of mobile devices - in particular, hardware architectures that offer highly robust and isolated execution environments (such as TEE, SE and TPM) - has allowed these devices to achieve high-grade security without the need for a physically distinct token
2. Recognize technology is now mature enough to enable two secure, distinct auth. factors in a single device.

European Banking Authority (EBA)

Draft Regulatory Technical Standards on PSD2 Strong Authentication

Article 6
Requirements related to the independence of the elements

1. The use of the elements of strong customer authentication referred to in Article 3, 4 and 5 shall be subject to procedures in terms of the technology, algorithms and parameters, ensuring that the breach of one of the elements does not compromise the reliability of the other elements.

2. Where any of the elements of strong customer authentication or the authentication code, is used through a multi-purpose device including, but not limited to, mobiles phones and tablets, the authentication procedure shall provide measures to mitigate the risk of the multi-purpose device being compromised.

3. For the purposes of paragraph 2, the mitigating measures shall include, but not be limited to:
   a. the implementation of separated trusted execution environments inside the multi-purpose device;
   b. mechanisms to ensure that the software or device have not been altered by the payer or by a third party or mechanisms to mitigate the risks related to such alteration where this has taken place.
3. As governments promote or require strong auth., make sure it is the “right” strong auth..

The market is in the midst of a burst of innovation around authentication technology - some solutions are better than others. Don’t build rules focused on old authentication technology.

- Old authentication technologies impose significant costs and burdens on the user - which decreases adoption

- Old authentication technologies have security (i.e., phishable) and privacy issues - putting both users and online service providers at risk
FIDO Delivers on Key Policy Priorities

**Security**
- Authentication using strong asymmetric Public Key cryptography
- Superior to old “shared secrets” model – there is nothing to steal on the server
- Biometrics as second factor

**Privacy**
- Privacy architected in up front; No linkability or tracking
- Biometric data never leaves device
- Consumer control and consent

**Interoperability**
- Open standards: FIDO 2.0 specs are in W3C standardization process
- FIDO compliance/conformance testing to ensure interoperability of “FIDO certified” products

**Usability**
- Designed with the user experience (UX) first – with a goal of making authentication as easy as possible.
- Security built to support the user’s needs, not the other way around

All Rights Reserved. FIDO Alliance. Copyright 2016.
THANK YOU!

QUESTIONS?

brett@fidoalliance.org  |  info@fidoalliance.org