

An aerial, black and white photograph of the Chicago skyline, showing a dense cluster of skyscrapers and buildings. The image is used as a background for the event title.

CYBER SECURITY CHICAGO

18-19 October 2017, McCormick Place, Chicago

ADAM LEWIS

Motorola Solutions, Office of the CTO
Cybersecurity Lead





THE NEW MODEL

Fast
IDentity
Online

open standards for
simpler, stronger authentication
using public key cryptography



THE WORLD HAS A PASSWORD PROBLEM

THE WORLD HAS A PASSWORD PROBLEM



81%

Data breaches in 2016 that involved **weak, default, or stolen passwords**¹



65%

Increase in **phishing attacks** over the number of attacks recorded in 2015²



1,093

Breaches in 2016, a **40% increase over 2015**³



CLUMSY | HARD TO REMEMBER | NEED TO BE CHANGED ALL THE TIME

¹Verizon 2017 Data Breach Report | ²Anti-Phishing Working Group | ³Identity Theft Resource Center 2016

ONE-TIME PASSCODES

Improve security but aren't easy enough to use



SMS
Reliability



Token
Necklace



User
Confusion



Still
Phishable

ATTACKS AGAINST SMS OTPS ON THE RISE

SS7 routing protocol vulnerability let thieves drain 2FA-protected bank accounts



**SECURITY NEWS THIS WEEK:
OH GOOD, HACKERS BEAT TWO-
FACTOR TO ROB BANK
ACCOUNTS**



Two-factor security is so broken, now hackers can drain bank accounts

"Whenever possible, people should also avoid using text messages to receive one-time passwords. Instead, they should rely on cryptographically based security keys as a second authentication factor"

Ars Technica, April 2017

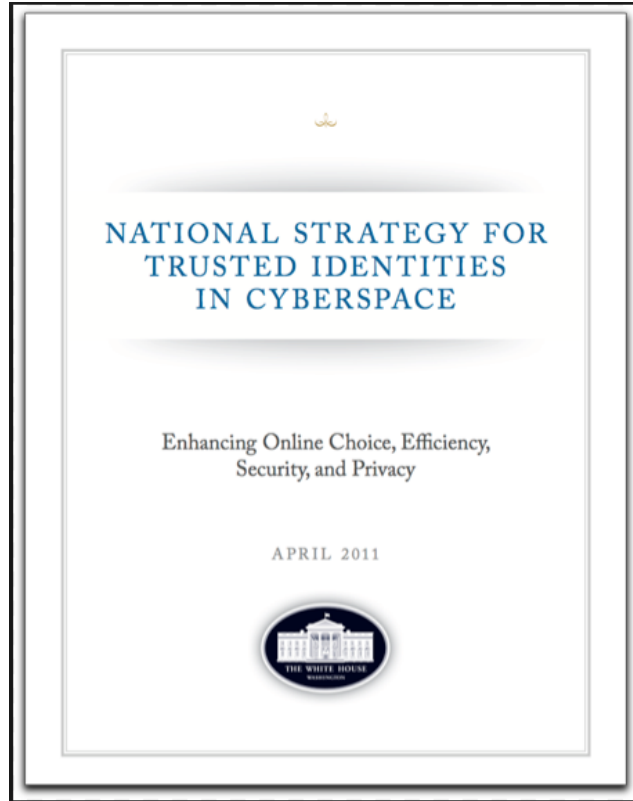


THE WORLD HAS A “SHARED SECRETS” PROBLEM

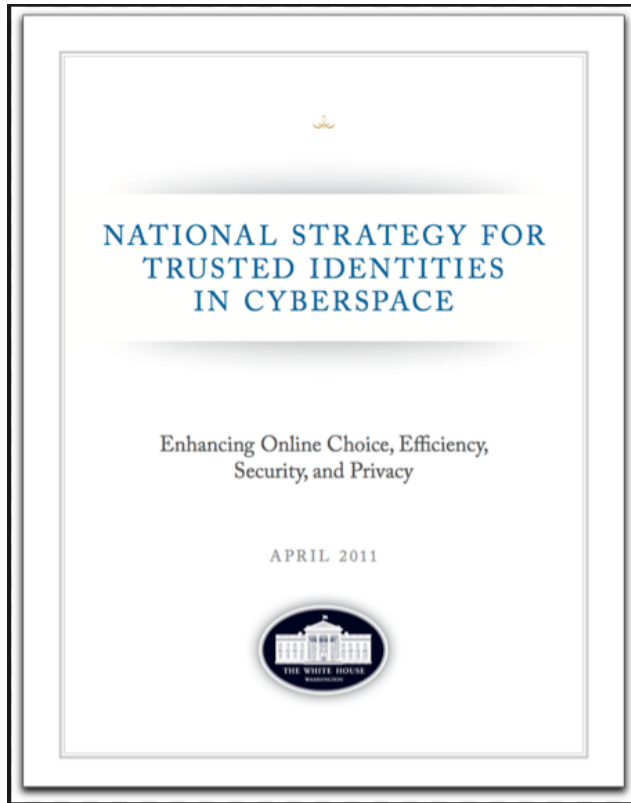


WE NEED A NEW MODEL

Let's Agree on Some Things.

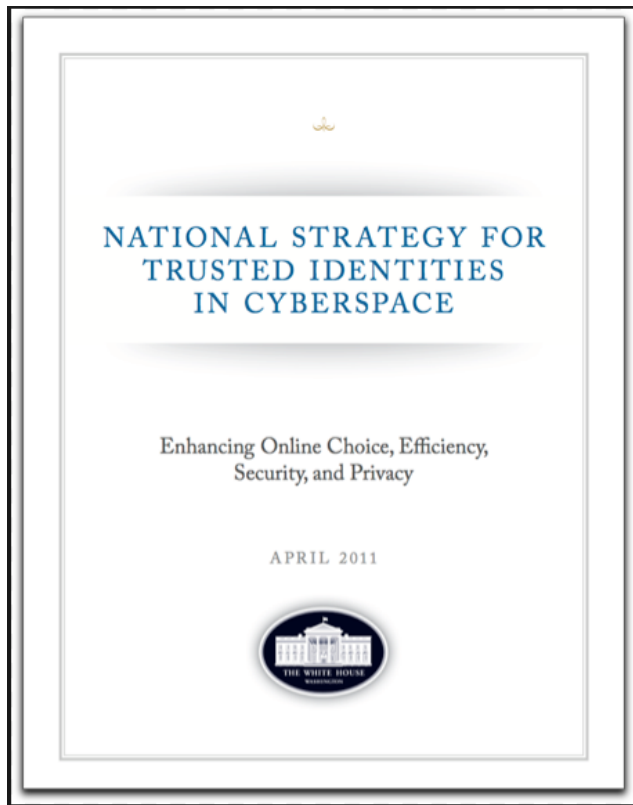


Let's Agree on Some Things.



SECURE

Let's Agree on Some Things.

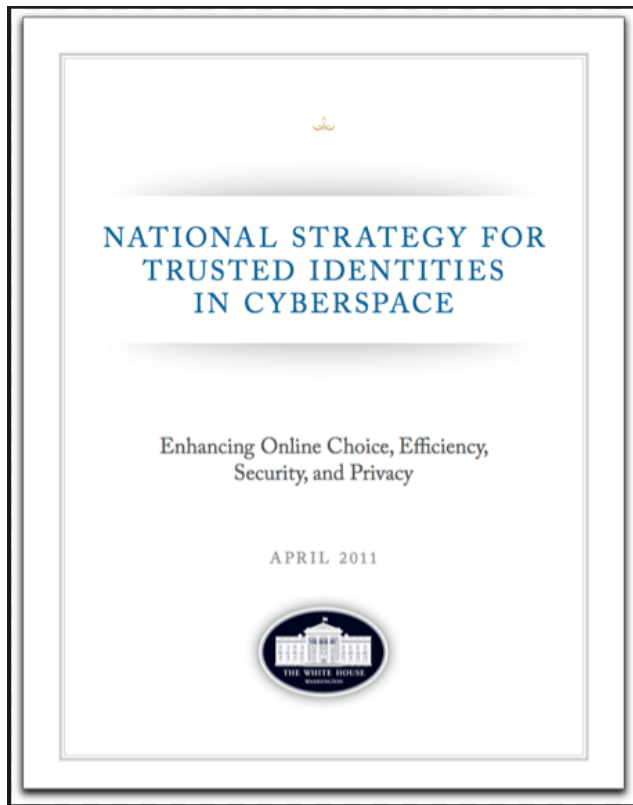


SECURE



**PRIVACY
ENHANCING**

Let's Agree on Some Things.



SECURE

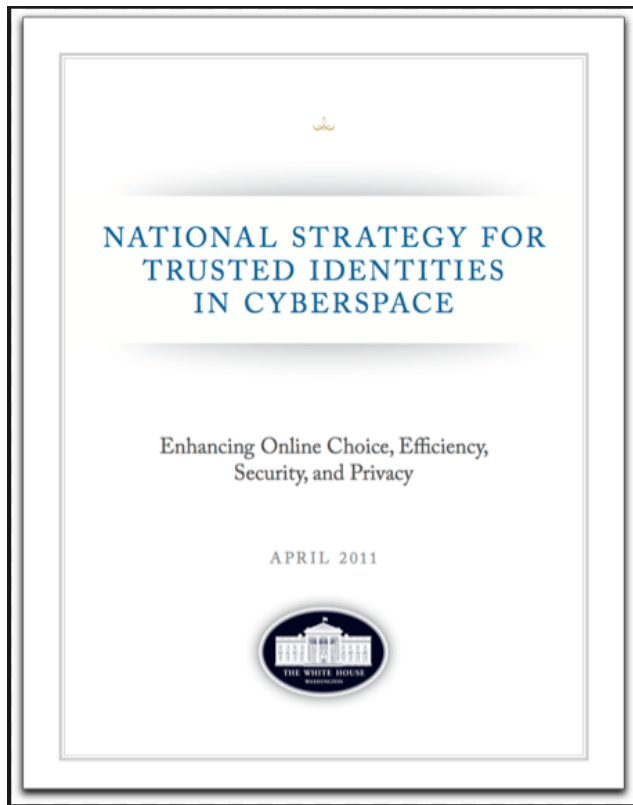


**PRIVACY
ENHANCING**



INTEROPERABLE

Let's Agree on Some Things.



SECURE



**PRIVACY
ENHANCING**

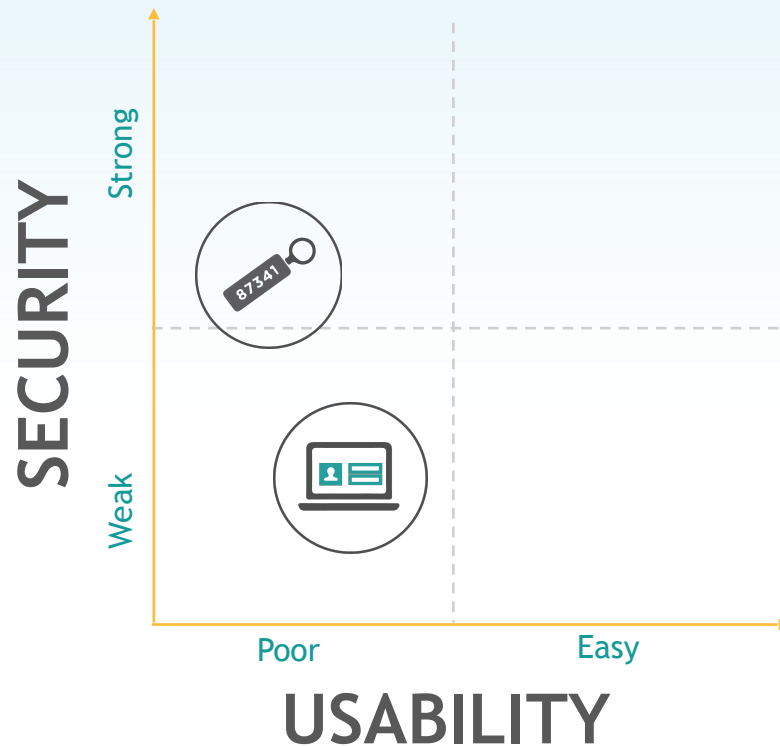


INTEROPERABLE

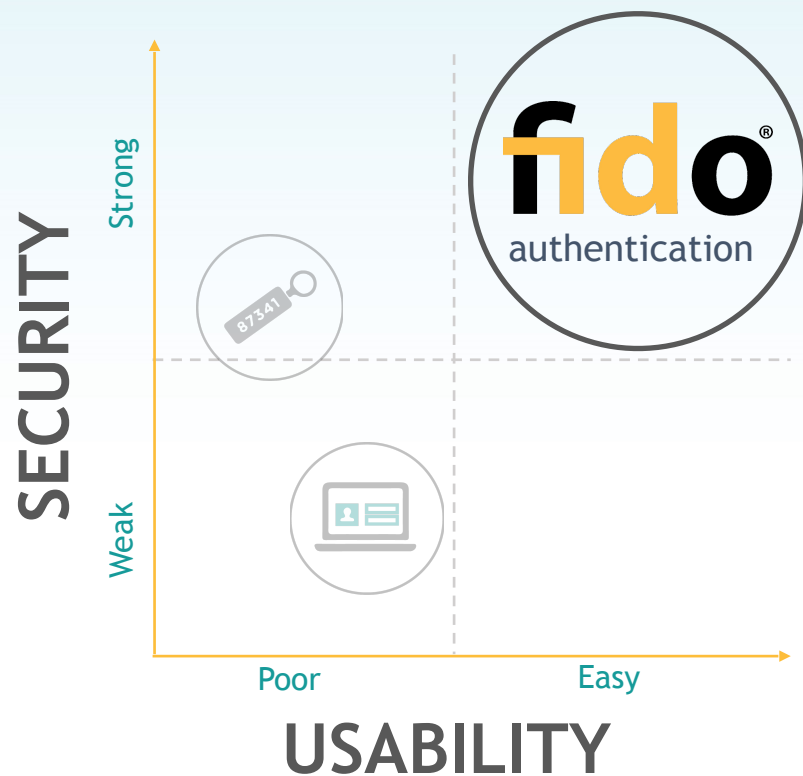


USABLE

THE OLD PARADIGM



THE FIDO PARADIGM



A MODEL THAT TAKES ADVANTAGE OF COMMODITIZED SECURE HARDWARE

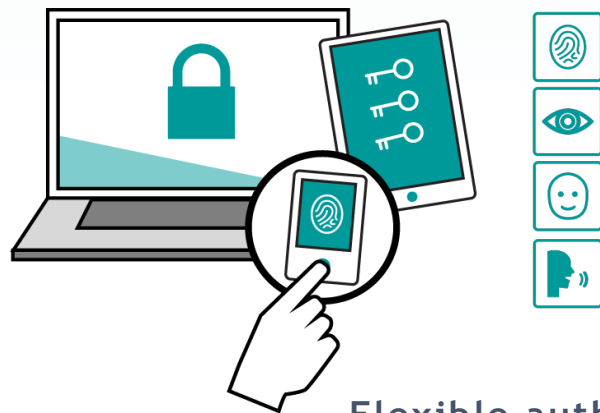
- Secure, hardware-based isolated execution environments (TPM/TEE/SE) – capable of generating, securing and applying cryptographic keys
- Multiple biometric sensors (finger/face/iris/voice)
- Other sensors and capabilities



UAF

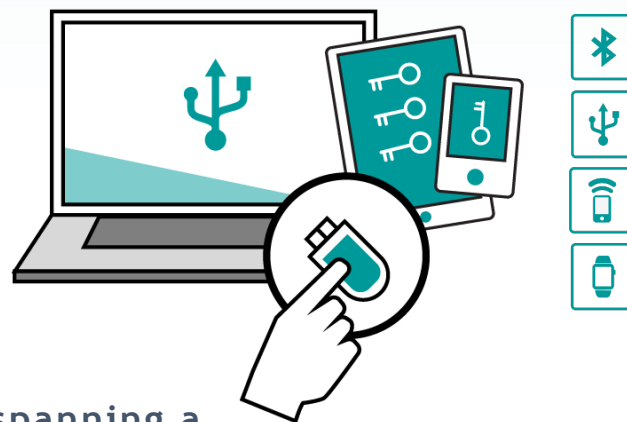
U2F

Passwordless Experience



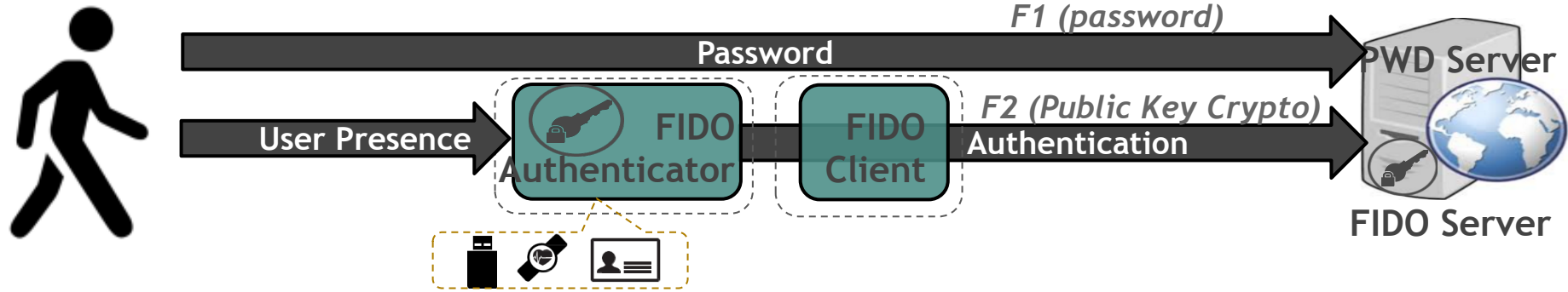
Flexible authentication spanning a
myriad of service providers

Second Factor Experience

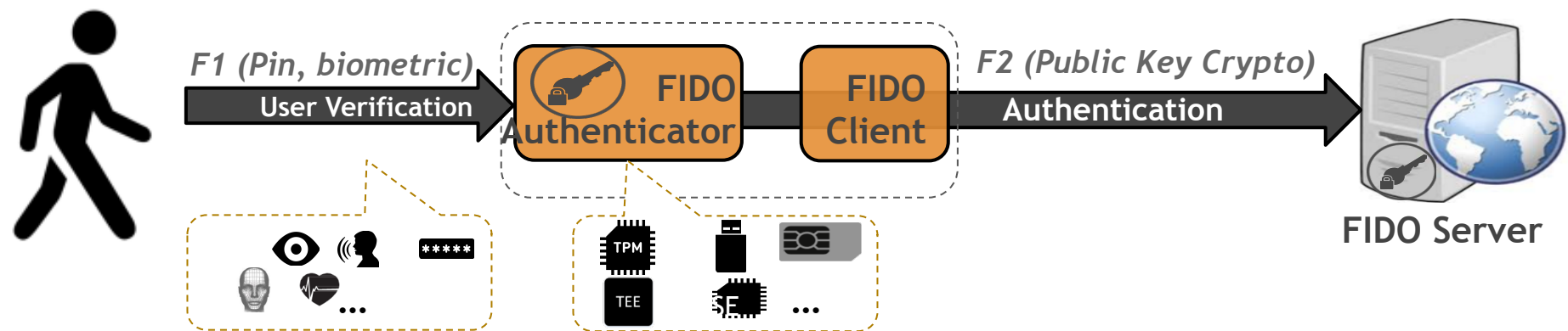




FIDO U2F (Second Factor Experience)



FIDO UAF (Passwordless Experience)



EXPERIENCES ADDRESS ARRAY OF USE CASES

FIDO standards provide support for user-friendly, privacy-aware user experiences across platforms to meet varying requirements

PASSWORDLESS EXPERIENCES

- Biometrics authn via mobile device
- Biometric authn via PC
- Biometrics authn to PC via mobile device

SECOND FACTOR EXPERIENCES

- External token to PC (USB, BLE)
- External token to mobile device (NFC/BLE)
- Embedded second factor on PC



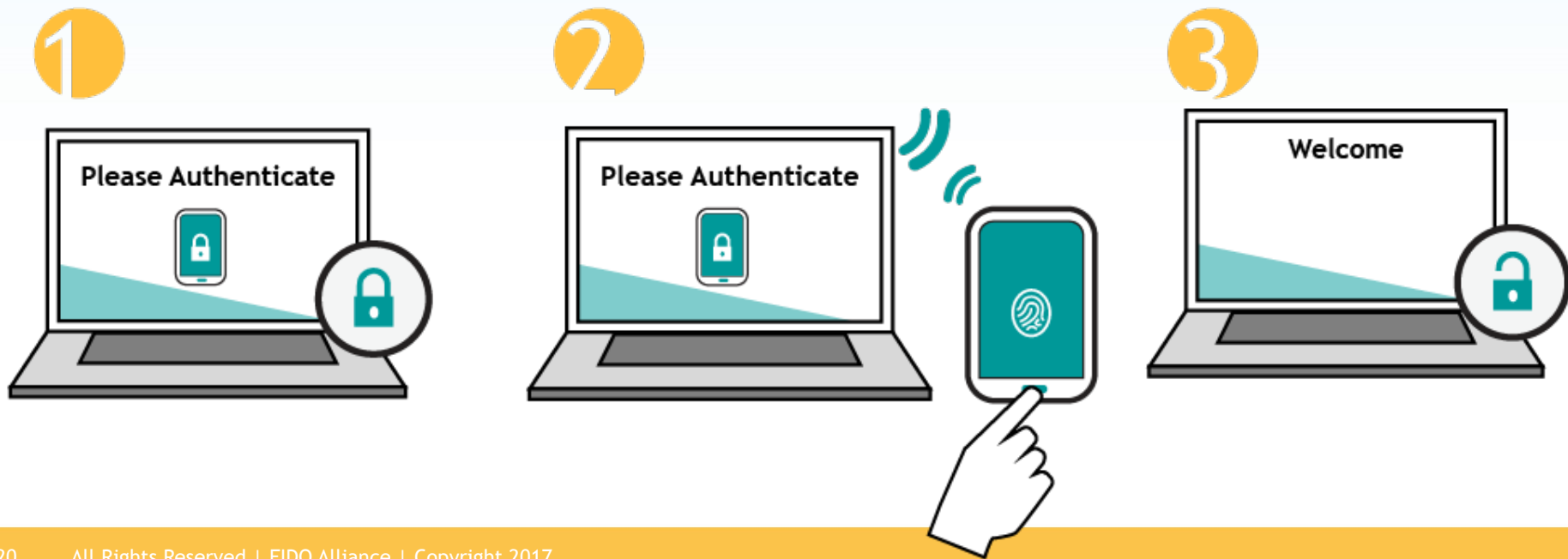
PASSWORDLESS AUTHENTICATION TO MOBILE APPLICATIONS USING BUILT-IN AUTHENTICATORS



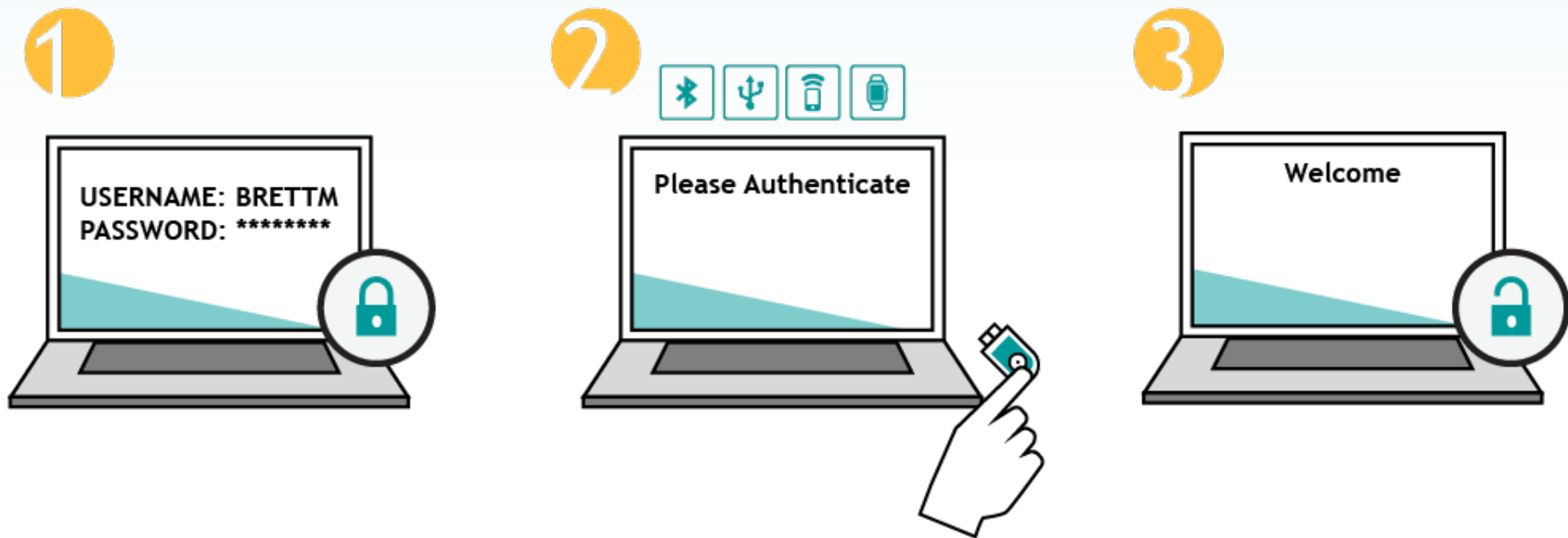
PASSWORDLESS AUTHENTICATION TO WEB APPLICATIONS/ PLATFORMS ON A PC USING BUILT-IN AUTHENTICATORS



PASSWORDLESS AUTHENTICATION TO WEB APPLICATIONS/PLATFORMS ON A PC USING EXTERNAL AUTHENTICATOR



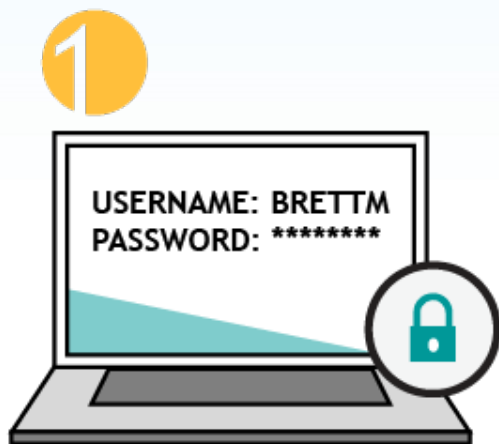
SECOND FACTOR AUTHENTICATION TO WEB APPLICATIONS/ PLATFORMS ON A PC USING EXTERNAL AUTHENTICATOR



SECOND FACTOR AUTHENTICATION TO MOBILE APPLICATIONS USING EXTERNAL AUTHENTICATORS



SECOND FACTOR AUTHENTICATION TO WEB APPLICATIONS ON A PC USING BUILT-IN AUTHENTICATORS





Who is driving FIDO?



Who is driving FIDO?



Who is driving FIDO?



Who is driving FIDO?



Who is driving FIDO?



Who is driving FIDO?



Who is driving FIDO?



Who is driving FIDO?



aetna®



Google



Lenovo



NTT
docomo



VISA

Who is driving FIDO?



aetna®



ARM



Google



Lenovo



NTT
docomo



QUALCOMM®



VISA

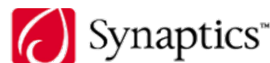
Who is driving FIDO?



aetna®



ARM



Who is driving FIDO?



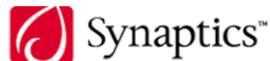
aetna®



ARM



FEITIAN
WE BUILD SECURITY



+ SPONSOR MEMBERS

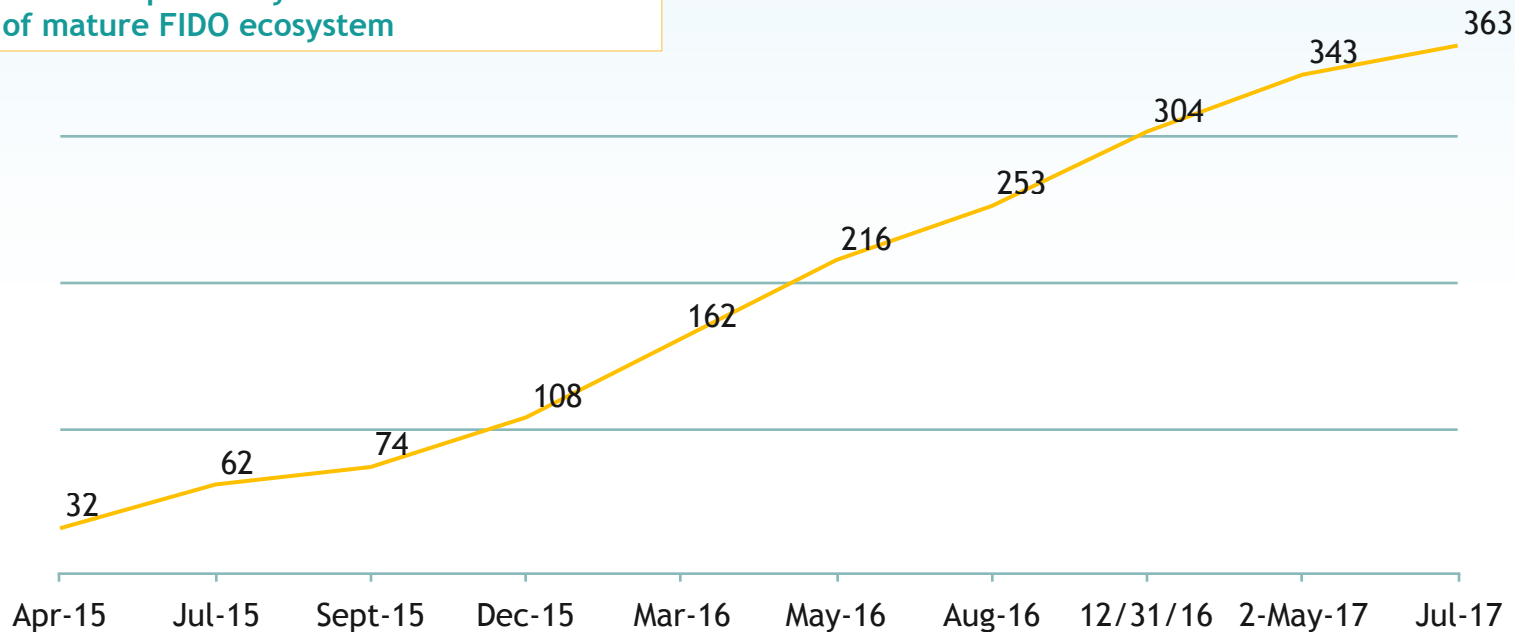
+ ASSOCIATE MEMBERS

+ LIAISON MEMBERS

360+ FIDO® CERTIFIED PRODUCTS



- ✓ An open competitive market
- ✓ Ensures interoperability
- ✓ Sign of mature FIDO ecosystem



FIDO CROSS-PLATFORM SUPPORT

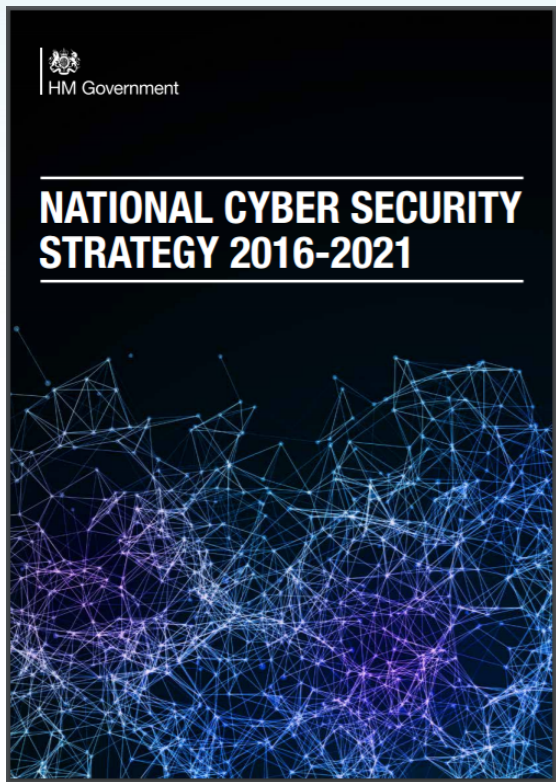


FIDO IMPACT ON POLICY



As technology evolves,
policy needs to evolve with it.

FIDO IS IMPACTING HOW GOVERNMENTS THINK ABOUT AUTHENTICATION



Priorities:

- Ensuring that future online products and services coming into use are “secure by default”
- Empowering consumers to “choose products and services that have built-in security as a default setting.”

“[We will] invest in technologies like Trusted Platform Modules (TPM) and emerging industry standards such as Fast IDentity Online (FIDO), which do not rely on passwords for user authentication, but use the machine and other devices in the user’s possession to authenticate. The Government will test innovative authentication mechanisms to demonstrate what they can offer, both in terms of security and overall user experience.”

FIDO IS IMPACTING HOW GOVERNMENTS THINK ABOUT AUTHENTICATION

U.S. Commission on Enhancing National Cybersecurity:

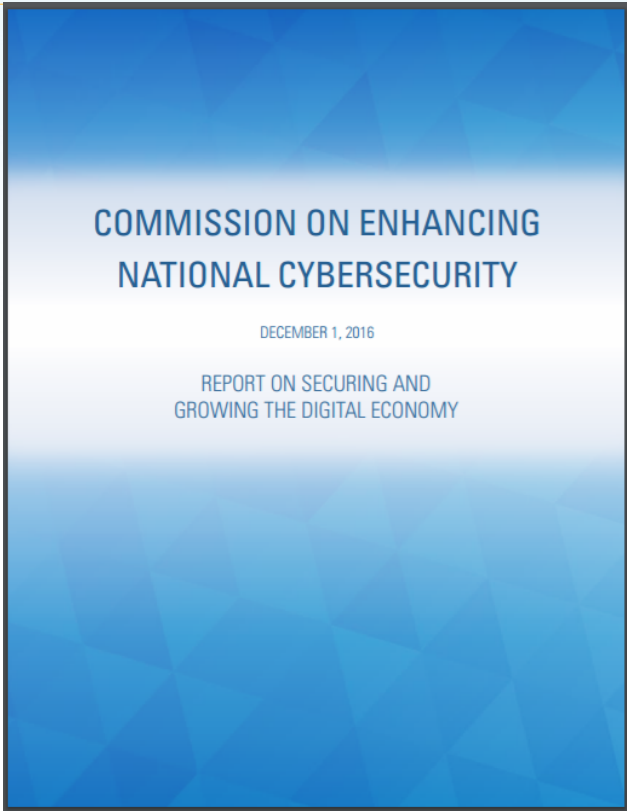
- Bipartisan commission established by the White House in April - charged with crafting recommendations for the next President
- Major focus on Authentication



An ambitious but important goal for the next administration should be to see no major breaches by 2021 in which identity—especially the use of passwords—is the primary vector of attack.

**U.S. COMMISSION ON ENHANCING
NATIONAL CYBERSECURITY**

US COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

The image shows the front cover of a report. The background is a solid blue color with a subtle, abstract pattern of lighter blue geometric shapes. The title "COMMISSION ON ENHANCING NATIONAL CYBERSECURITY" is centered in a white, uppercase, sans-serif font. Below the title, the date "DECEMBER 1, 2016" is printed in a smaller white font. At the bottom, the subtitle "REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY" is also centered in a white font.

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

DECEMBER 1, 2016

REPORT ON SECURING AND
GROWING THE DIGITAL ECONOMY

*“Other important work that must be undertaken to overcome identity authentication challenges includes the development of open-source standards and specifications like those developed by the **Fast IDentity Online (FIDO) Alliance**. FIDO specifications are focused largely on the mobile smartphone platform to deliver multifactor authentication to the masses, all based on industry standard public key cryptography.*

Windows 10 has deployed FIDO specifications (known as Windows Hello), and numerous financial institutions have adopted FIDO for consumer banking. Today, organizations complying with FIDO specifications are able to deliver secure authentication technology on a wide range of devices, including mobile phones, USB keys, and near-field communications (NFC) and Bluetooth low energy (BLE) devices and wearables.

This work, other standards activities, and new tools that support continuous authentication provide a strong foundation for opt-in identity management for the digital infrastructure.”

TECHNOLOGY IS NOW MATURE ENOUGH TO ENABLE TWO SECURE, DISTINCT AUTHN FACTORS IN A SINGLE DEVICE

Article 9

Independence of the elements

1. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 shall be subject to measures in terms of technology, algorithms and parameters, which ensure 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 mobile phones and tablets, payment service providers shall adopt security measures to mitigate the risk resulting from the multi-purpose device being compromised.
3. For the purposes of paragraph 2, the mitigating measures shall include each of the following:
 - (a) the use of separated secure execution environments through the software installed inside the multi-purpose device;
 - (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party or mechanisms to mitigate the consequences of such alteration where this has taken place.

FINAL REPORT ON DRAFT RTS ON SCA AND CSC



EBA/RTS/2017/02

23 February 2017

Final Report

Draft Regulatory Technical Standards

on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)

TECHNOLOGY IS NOW MATURE ENOUGH TO ENABLE TWO SECURE, DISTINCT AUTHN FACTORS IN A SINGLE DEVICE



SP 800-63-3

Digital Identity Guidelines



SP 800-63A

Enrollment & Identity Proofing



SP 800-63B

Authentication & Lifecycle Management



SP 800-63C

Federation & Assertions

NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi
James L. Fenton
Elaine M. Newton
Ray A. Perlner
Andrew R. Regenscheid
William E. Burr
Justin P. Richer

Privacy Authors:
Naomi B. Lefkowitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-63b>

**FIDO recognized at the highest
Authenticator Assurance Level
(AAL3) by NIST**

NCCoE for First Responder Mobile SSO



PROJECT DESCRIPTION

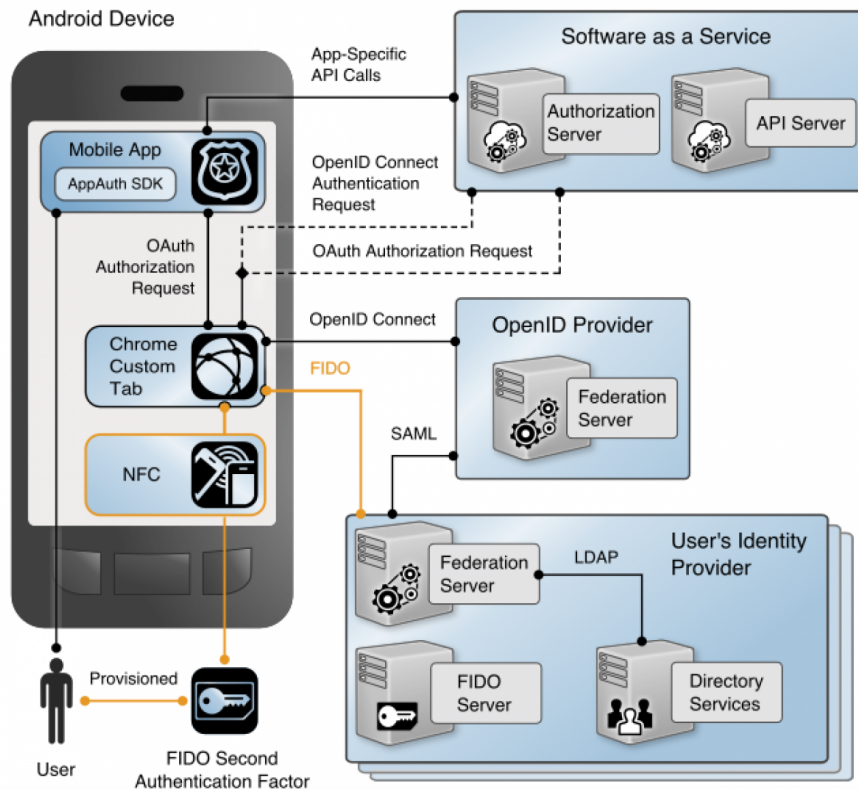
MOBILE APPLICATION SINGLE SIGN-ON

For Public Safety and First Responders

Paul Grassi
NIST Applied Cybersecurity Division

William Fisher
NIST National Cybersecurity Center of Excellence

FINAL DRAFT
November 2016
PSFR-NCCoE@nist.gov



We Can Do It!



J. Howard Miller

POST FEB. 15 TO FEB. 22



WAR PRODUCTION CO-ORDINATING COMMITTEE



THANK YOU!

e: adam.lewis@motorolasolutions.com

t: [@lewiada](https://twitter.com/lewiada)

