FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

# FIDO Alliance: Standards-based Solutions for Simpler, Strong Authentication

Jeremy Grant
Managing Director, Technology Business Strategy
Venable LLP

jeremy.grant@venable.com
@jgrantindc


fido™ ALLIANCE

# Digital: The Opportunity and the Challenge


***"Identity is a precursor to access to fintech, yet identity continues to languish in analog forms that are difficult to build upon for the provision of digital services."***

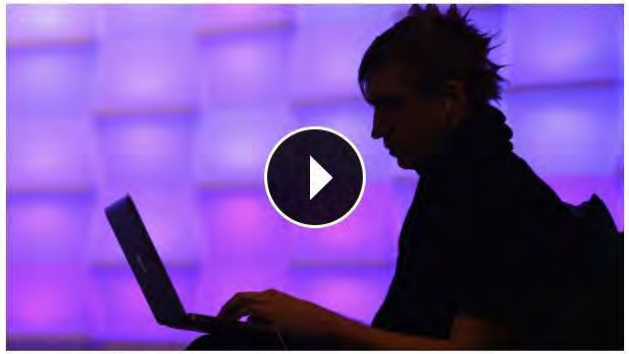
# THE PROBLEM


# THE WORLD HAS A PASSWORD PROBLEM

# HOW SECURE IS AUTHENTICATION?

## Criminals steal 1.2 billion paswords

By James O'Toole and Jose Pagliery @CNNTech August 6, 2014: 6:56 AM ET



**Hackers know your password**

NEW YORK (CNNMoney)

Criminals have stolen 1.2 billion Internet user names and passwords, amassing what could be the largest collection of stolen digital credentials in history, a respected security firm said Tuesday.

There's **no need to panic at this point** -- Hold Security, the firm that discovered the theft, says the gang isn't in the business of stealing your bank account information. Instead, they make their money by sending out spam for bogus products like

Posted August 27, 2014 EMAIL PRINT SHARE

## Chase Bank Customers Targeted by Massive Phishing Attack

By Hal M. Bundrick

Pin It

NEW YORK (MainStreet) — A new trend in cyber attacks may be unfolding: the "smash and grab" campaign. One such attack recently targeted a massive number of JPMorgan Chase customers on August 19. While most phishing perpetrators attempt to disguise their efforts and extend the shelf life of their attacks, this exploit was fearless – disregarding stealth measures and launching a multi-pronged attack that wasn't concerned about the threat of detection.

The FBI is looking into cyber attacks on U.S. banks, reportedly as possible cases of Russian retaliation for U.S.-backed sanctions enacted over the crisis in Ukraine. According to Bloomberg, investigators are considering the possibility that recent hacking of JPMorgan is connected to a series of data breaches at European banks. These infiltrations are said to have exploited "a similar vulnerability," and required enough technical expertise to raise the possibility of government involvement. The timing has also raised suspicions: since Vladimir Putin's government became heavily involved in Ukraine's civil conflict, there has been a reported increase in cyber attacks on U.S. banks launched from Russia and Eastern Europe.

## How the Eurograbber attack stole 36 million euros

Posted on 05.12.2012

Check Point has revealed how a sophisticated malware attack was used to steal an estimated €36 million from over 30,000 customers of over 30 banks in Italy, Spain, Germany and Holland over summer this year.

The theft used malware to target the PCs and mobile devices of banking customers. The attack also took advantage of SMS messages used by banks as part of customers' secure login and authentication process.

The attack worked by infecting victims' PCs and mobiles with a modified

# AUTHENTICATION IS OUR BIGGEST PROBLEM

WIRED

SO, UH, THAT BILLION-ACCOUNT YAHOO BREACH WAS ACTUALLY 3 BILLION

The New York Times

*Target to Pay $18.5 Million to 47 States in Security Breach Settlement*

The Register

**Sensitive client emails, usernames, passwords exposed in Deloitte hack**

Fortune

LinkedIn Lost 167 Million Account Credentials in Data Breach

Mashable

Someone is selling 33 million Twitter passwords on the dark web

ars technica

Cluster of "megabreaches" compromises a whopping 642 million passwords

# 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 2015[2]

**1,579**

Breaches in 2017, a 45% increase over 2016[3]

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

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

# 2017 DATA BREACHES

## Number of Data Breaches Continues to Soar over 2016 Figures

**1579**

Breaches in 2017, an increase of 44.7 percent over last year's record pace

[1]*Identity Theft Resource Center 2017*

# 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

ars technica

ZDNet

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

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

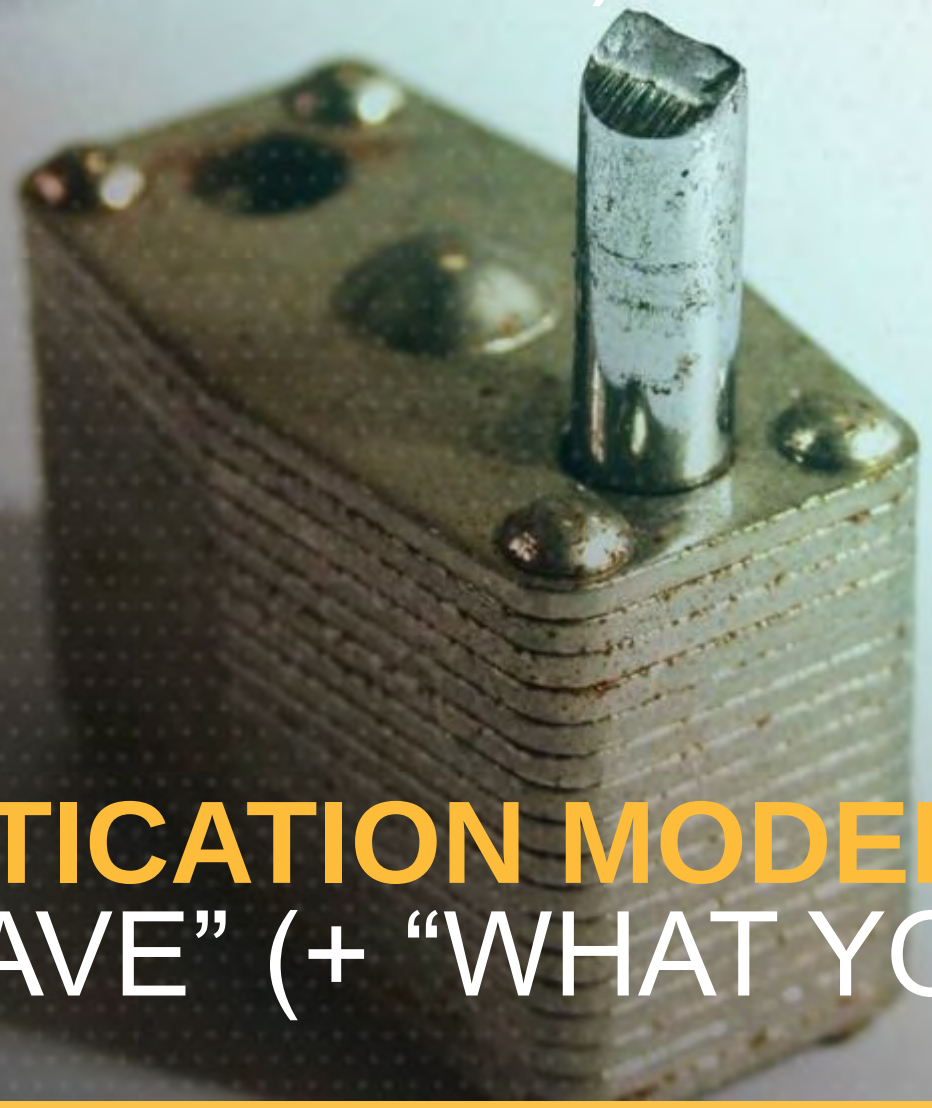
WIRED

*"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**

# THE “SHARED SECRET” (AKA “WHAT YOU KNOW”) **IS BROKEN**



# WE NEED A **NEW AUTHENTICATION MODEL** “WHAT YOU HAVE” (+ “WHAT YOU ARE”)

# HIGH-ASSURANCE STRONG AUTHENTICATION

## High-assurance strong authentication =

- ✓ Use of two + factors 
- ✓ At least one leverages public key cryptography 
- ✓ Not susceptible to phishing, man-in-the-middle and/or other attacks targeting credentials

*Javelin Strategy & Research, 2017 State of Authentication Report*

# THE NEW MODEL

Fast
IDentity
Online

open standards for
simpler, stronger authentication
using public key cryptography

# THE SOLUTION: FIDO AUTHENTICATION

# VIDEO – WHAT IS FIDO?

https://youtu.be/5ZIQabDrnT0

# THE FACTS ON FIDO

The FIDO Alliance is an open industry association of over 250 organizations with a focused mission:

## AUTHENTICATION STANDARDS

based on public key cryptography to solve the password problem

Today, its members provide the world's largest ecosystem for standards-based, interoperable authentication

**500+**
FIDO Certified solutions

Available to protect
**3 BILLION**
user accounts worldwide

# LEADING THE EFFORT

fido ALLIANCE

Google
Microsoft
intel
Lenovo
NTT docomo
infineon
SAMSUNG
QUALCOMM
arm
NXP

gemalto security to be free
yubico
Synaptics
RSA
nok nok
Daon
FEITIAN WE BUILD SECURITY
RAON SECURE
IDEMIA augmented identity
FINGERPRINTS
egis Technology
vmware
OneSpan

aetna
LINE
VISA
amazon
facebook
Alibaba.com
AMERICAN EXPRESS
PayPal
Bank of America
mastercard
ING
USAA
BCcard

CONSUMER ELECTRONICS

SECURITY & BIOMETRICS

HIGH-ASSURANCE SERVICES

# INDUSTRY PARTNERSHIPS

fido ALLIANCE

Asia PKI Consortium

Australian Payments Network

Biometrics Institute

Bluetooth

CARCONNECTIVITY consortium

carin

DIACC

ETA ELECTRONIC TRANSACTIONS ASSOCIATION

EMVCo

EUROSMART The Voice of the Smart Security Industry

FIDO FORUM KOREA

GLOBAL CYBER ALLIANCE

GLOBALPLATFORM

GSMA

ibia INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

IDPRO incubated by KANTARA

IESA INDIA ELECTRONICS & SEMICONDUCTOR ASSOCIATION Taking India to ESDM Leadership

India PKI Forum

ISO JTC1 IEC INFORMATION TECHNOLOGY STANDARDS

ITU

kantara INITIATIVE

NATIONAL CYBERSECURITY ALLIANCE

NFC FORUM

NH-ISAC

OpenID

SAFE-BioPharma SECURITY. IDENTITY. TRUST.

SECURE TECHNOLOGY ALLIANCE

TeleTrusT Pioneers in IT security. IT Security Association Germany

TRUSTED COMPUTING GROUP

US PAYMENTS FORUM

W3C

# FIDO Standards

**FIDO2 Project**

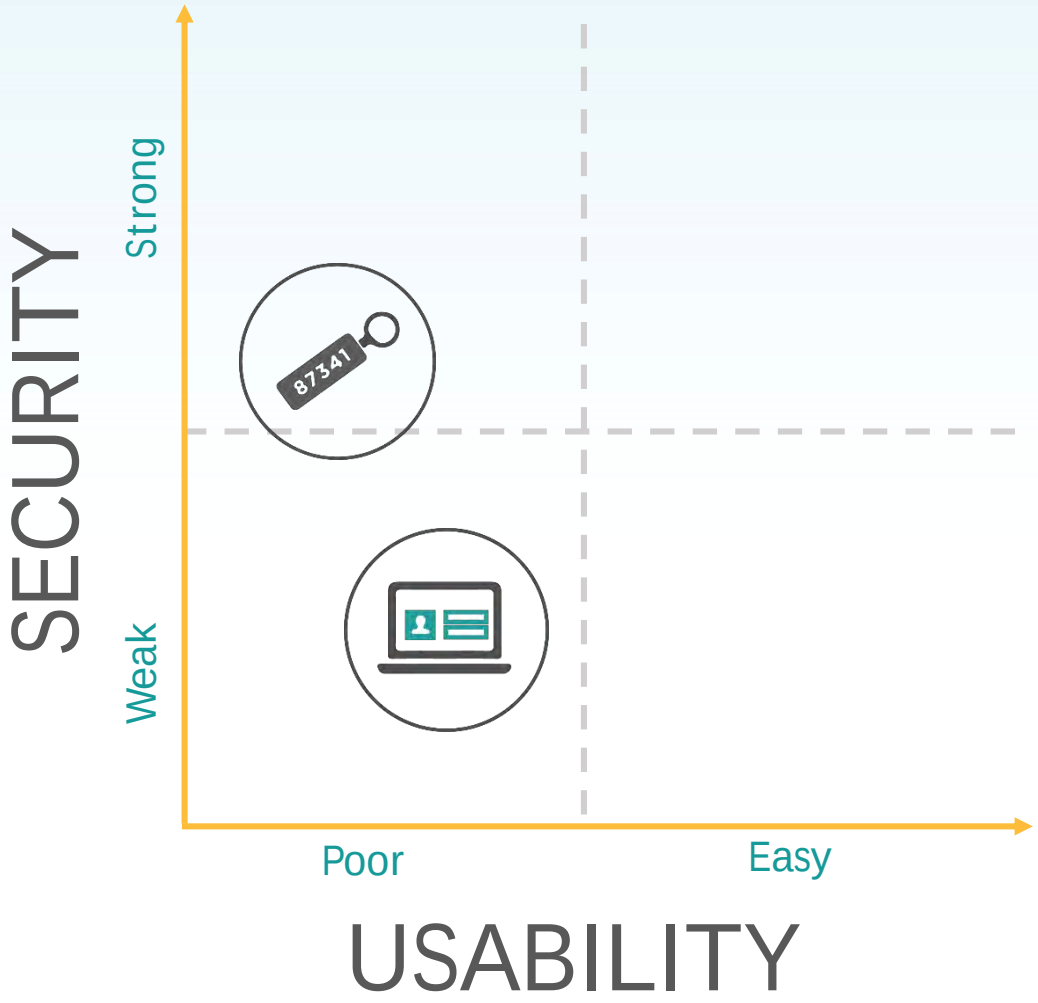
**FIDO UAF**
**(ITU x.1277)**

**FIDO U2F**
**(ITU x.1278)**

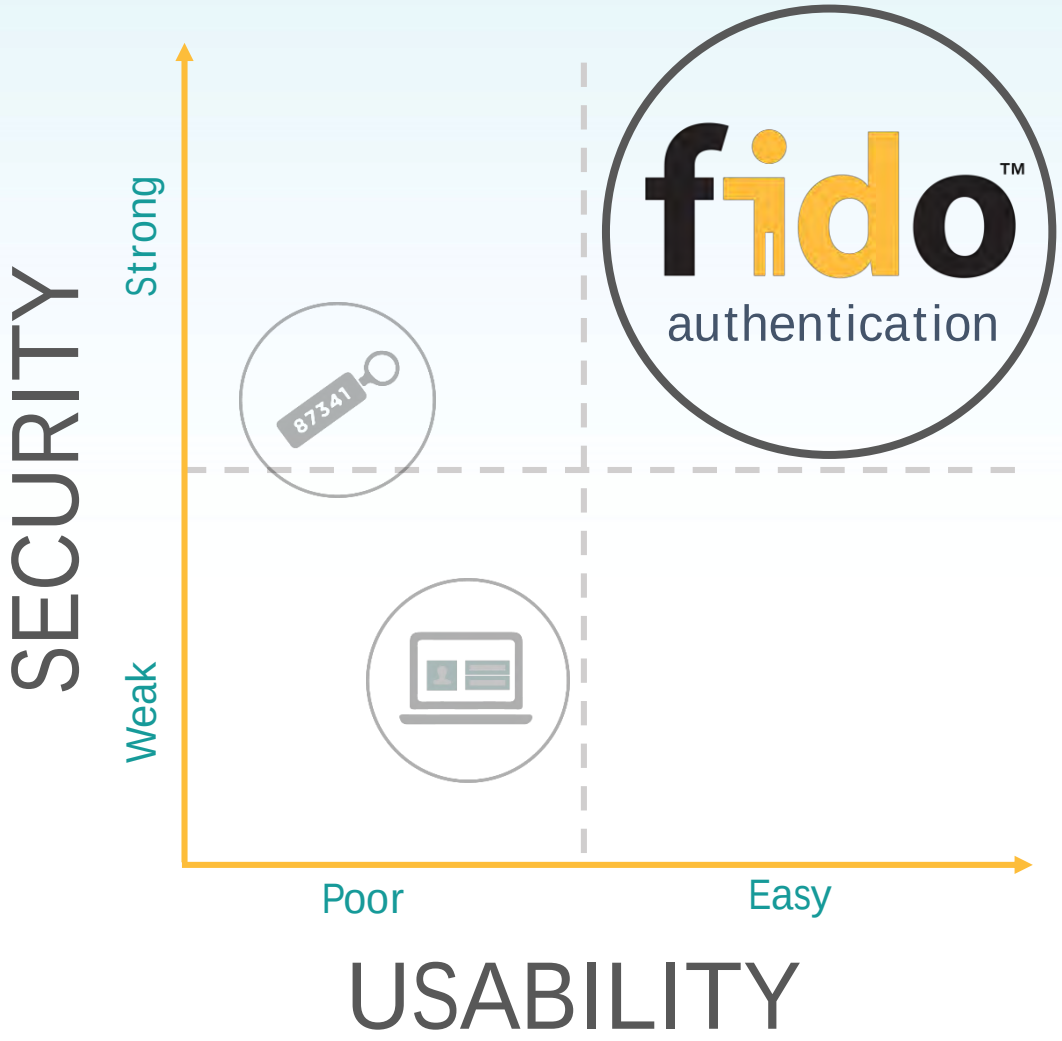
**CTAP**
**(ITU x.1278)**

**WebAuthn**
**(W3C Standard)**

# THE OLD PARADIGM

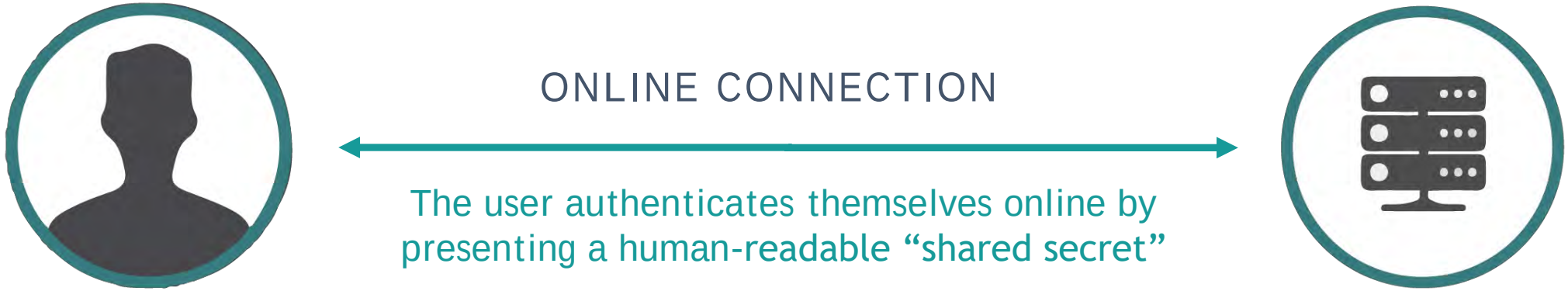


# THE FIDO PARADIGM



# HOW FIDO WORKS

# HOW OLD AUTHENTICATION WORKS



# HOW FIDO AUTHENTICATION WORKS

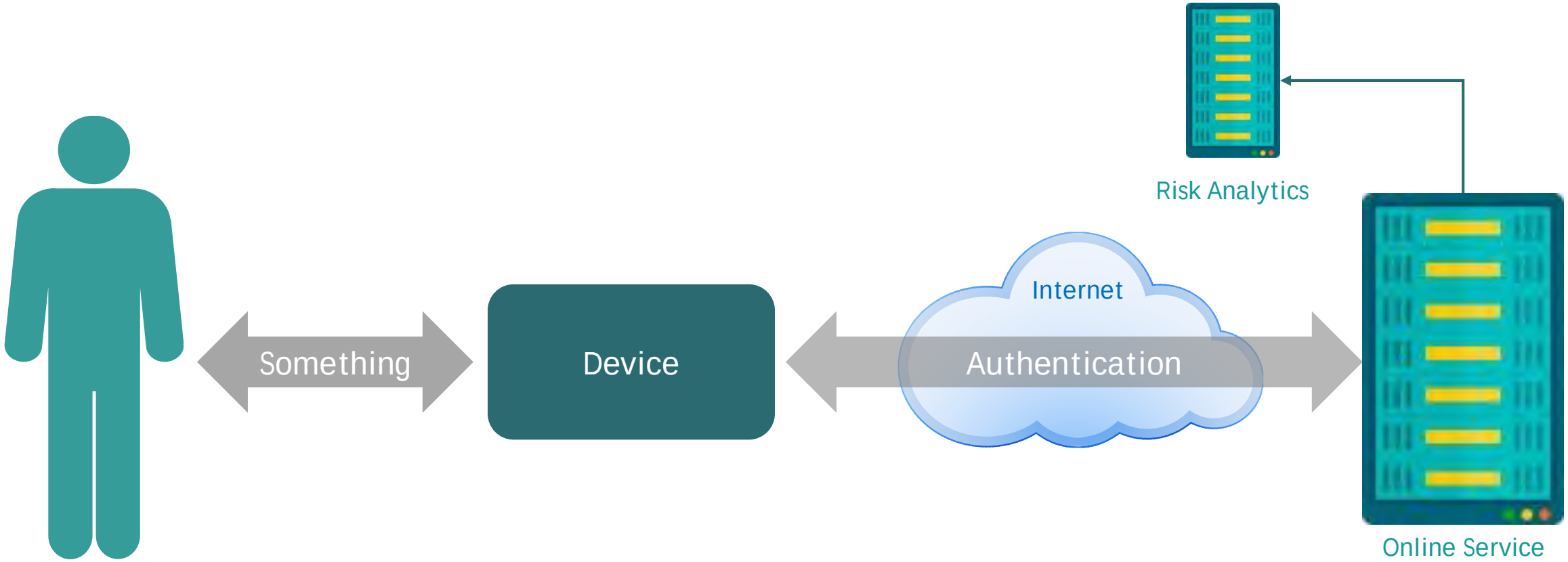
LOCAL CONNECTION

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

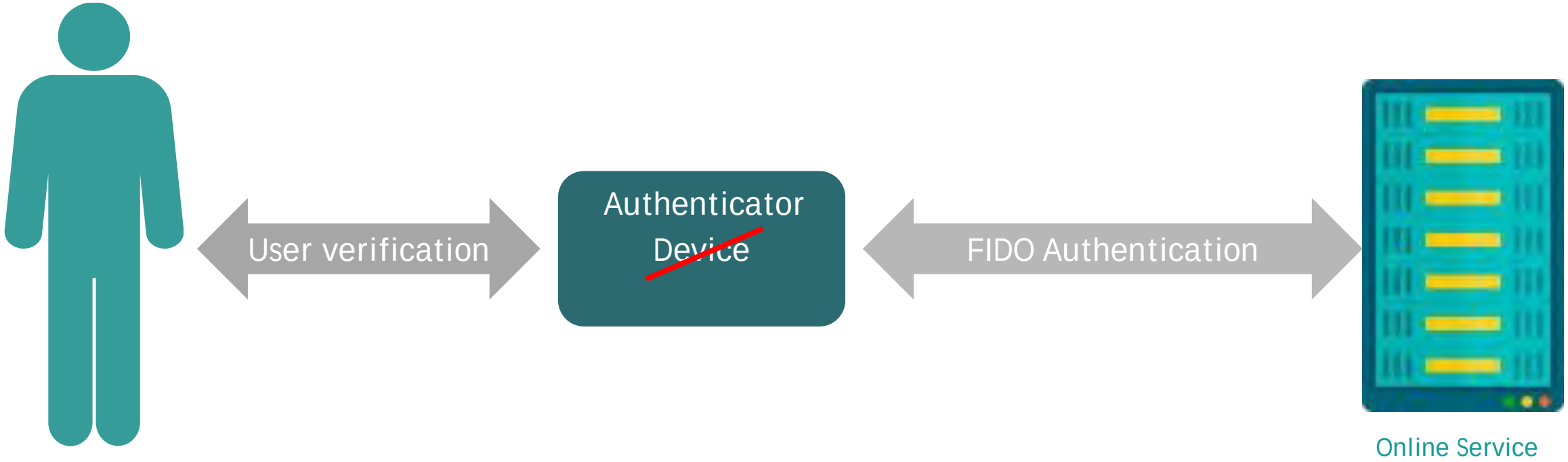

The device authenticates the user online using public key cryptography

ONLINE CONNECTION

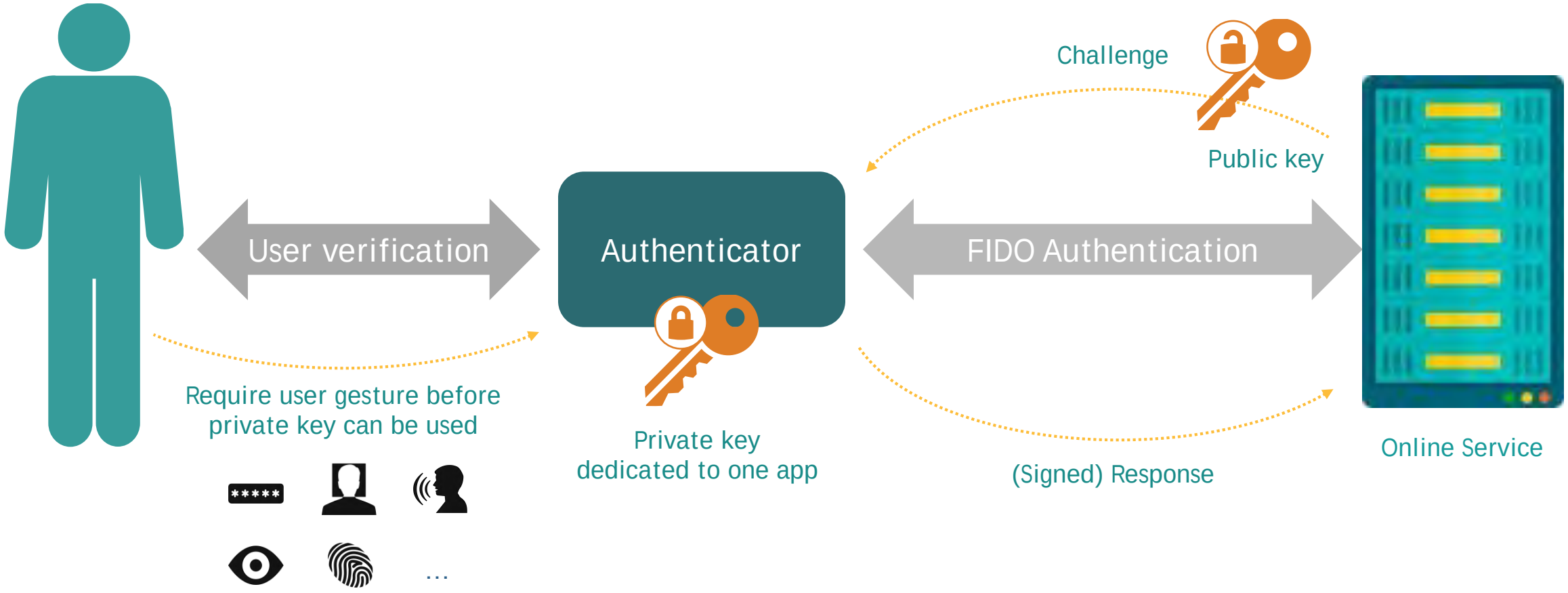
# CLOUD AUTHENTICATION



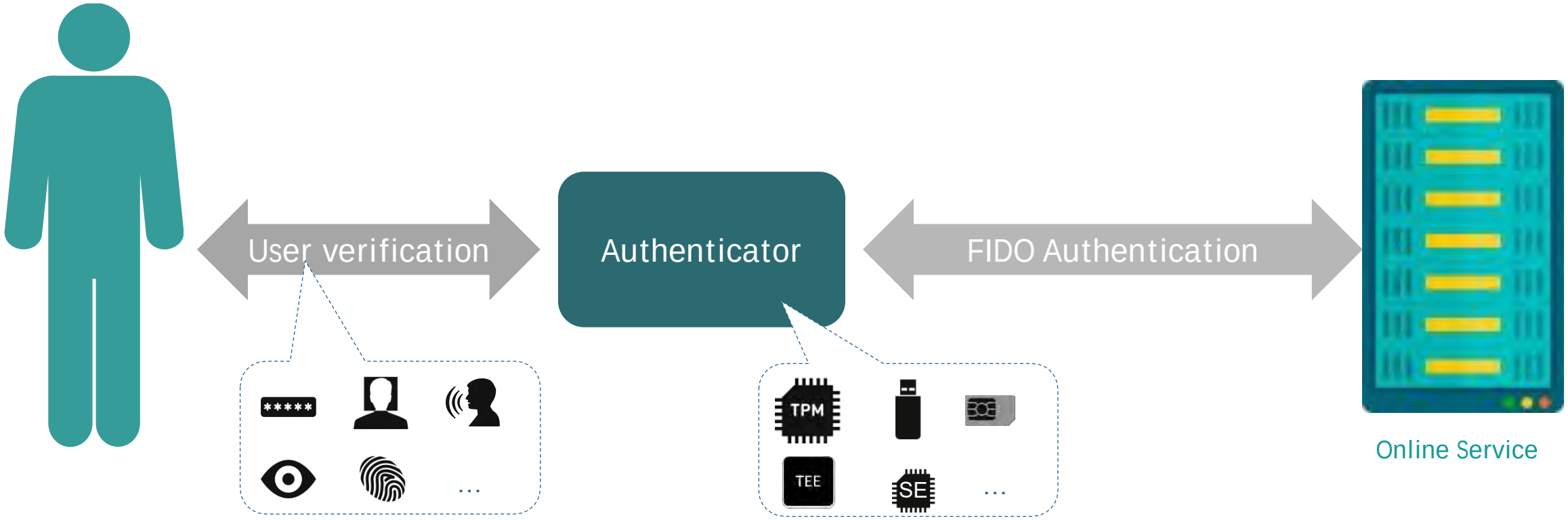
# HOW DOES FIDO WORK?



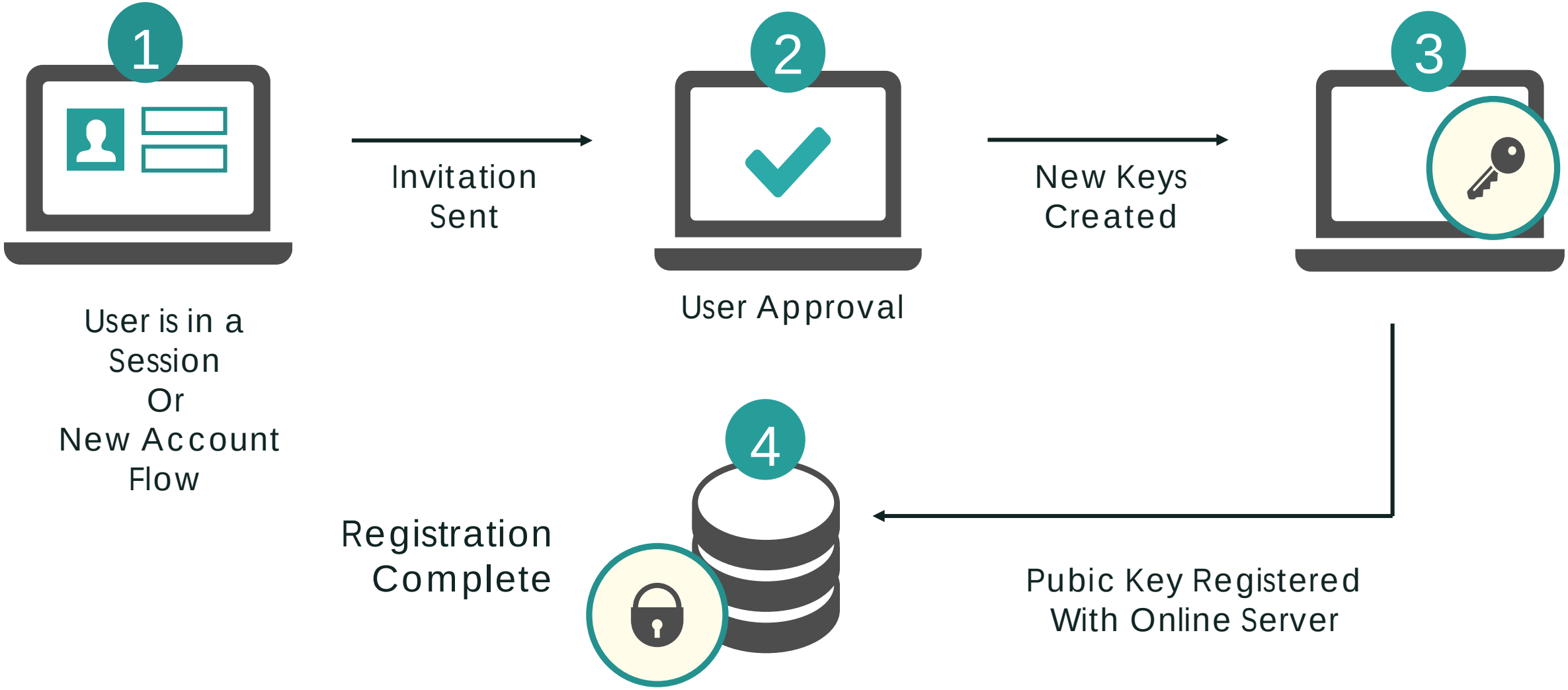
# HOW DOES FIDO WORK?



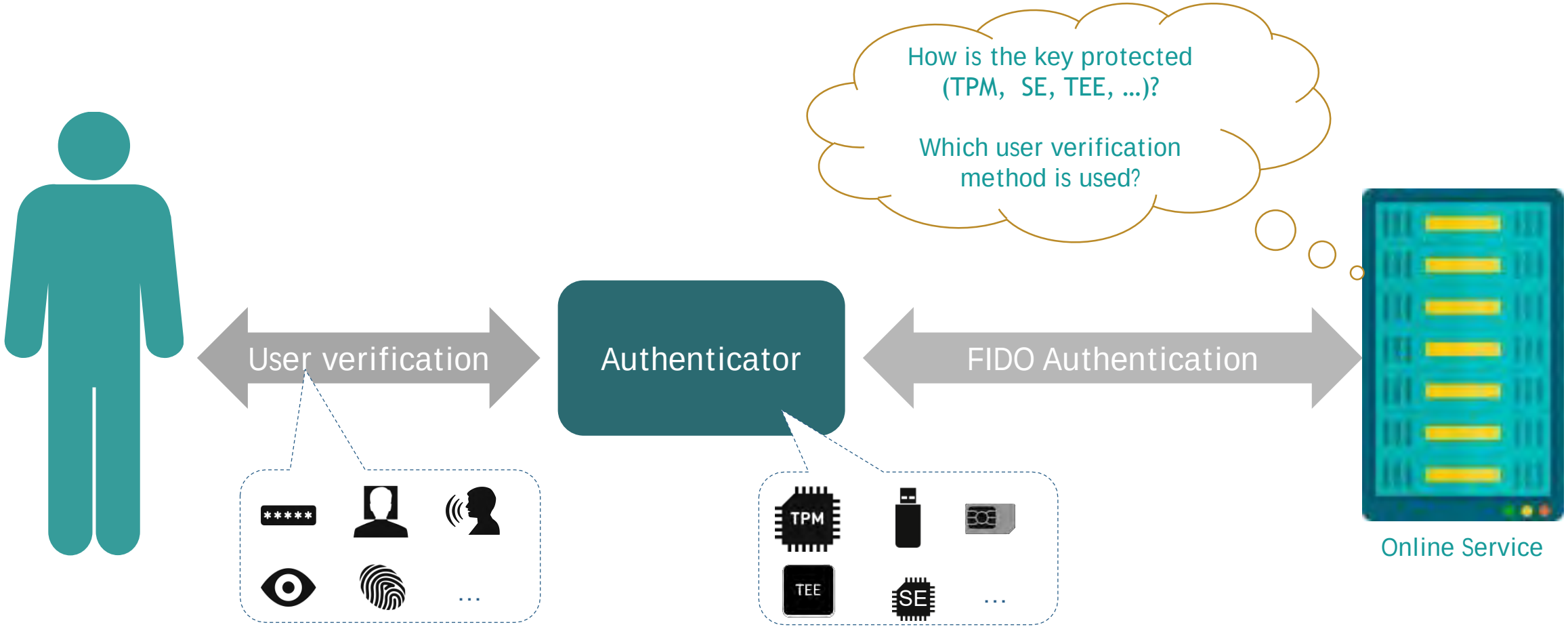
# HOW DOES FIDO WORK?



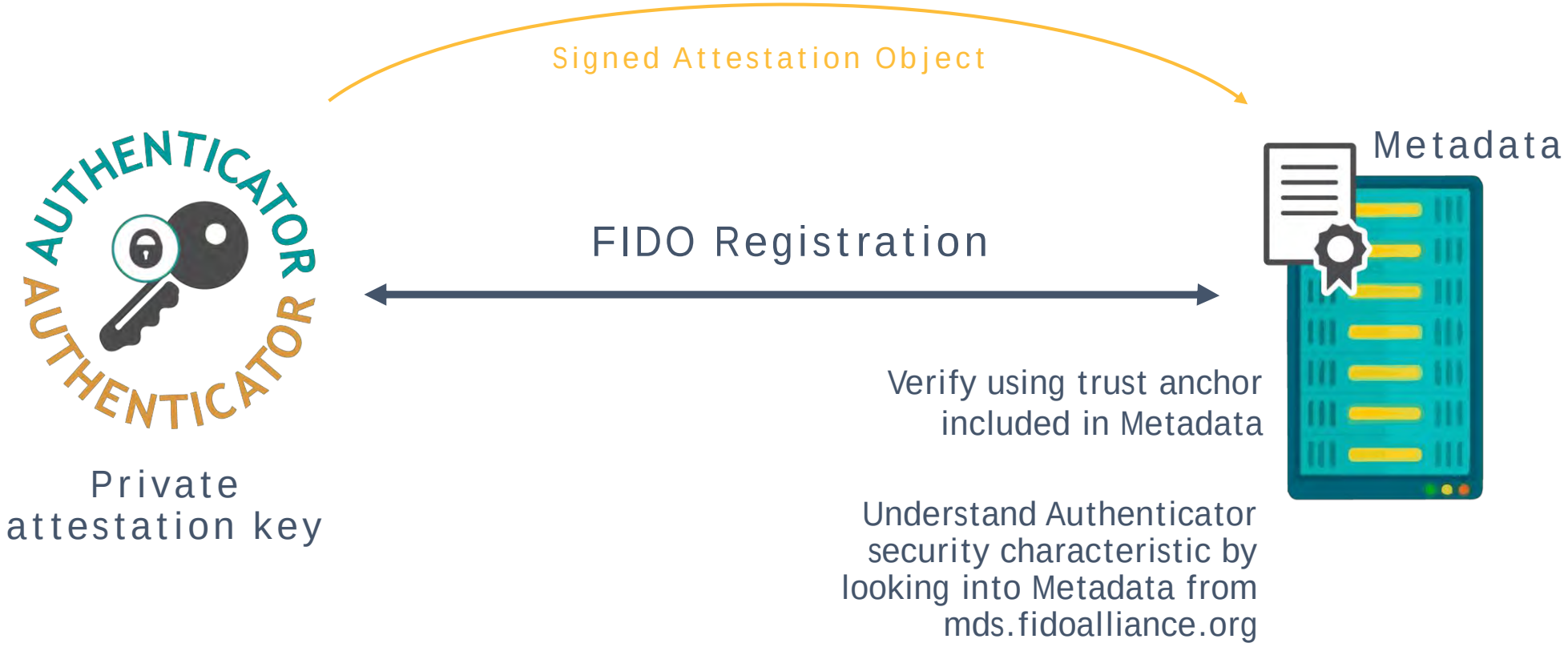
# FIDO REGISTRATION



# IMPORTANT DATA FOR SERVICE PROVIDERS



# ATTESTATION + METADATA



# USER EXPERIENCES

# EXPERIENCES ADDRESS ARRAY OF USE CASES

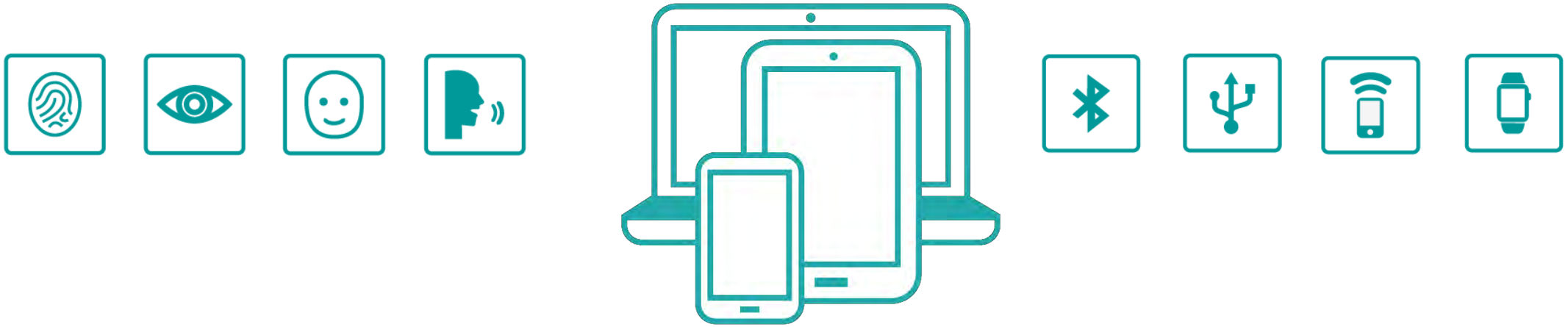
FIDO standards provide support for user-friendly, privacy-aware user experiences across platforms to meet varying requirements

## PASSWORDLESS EXPERIENCES

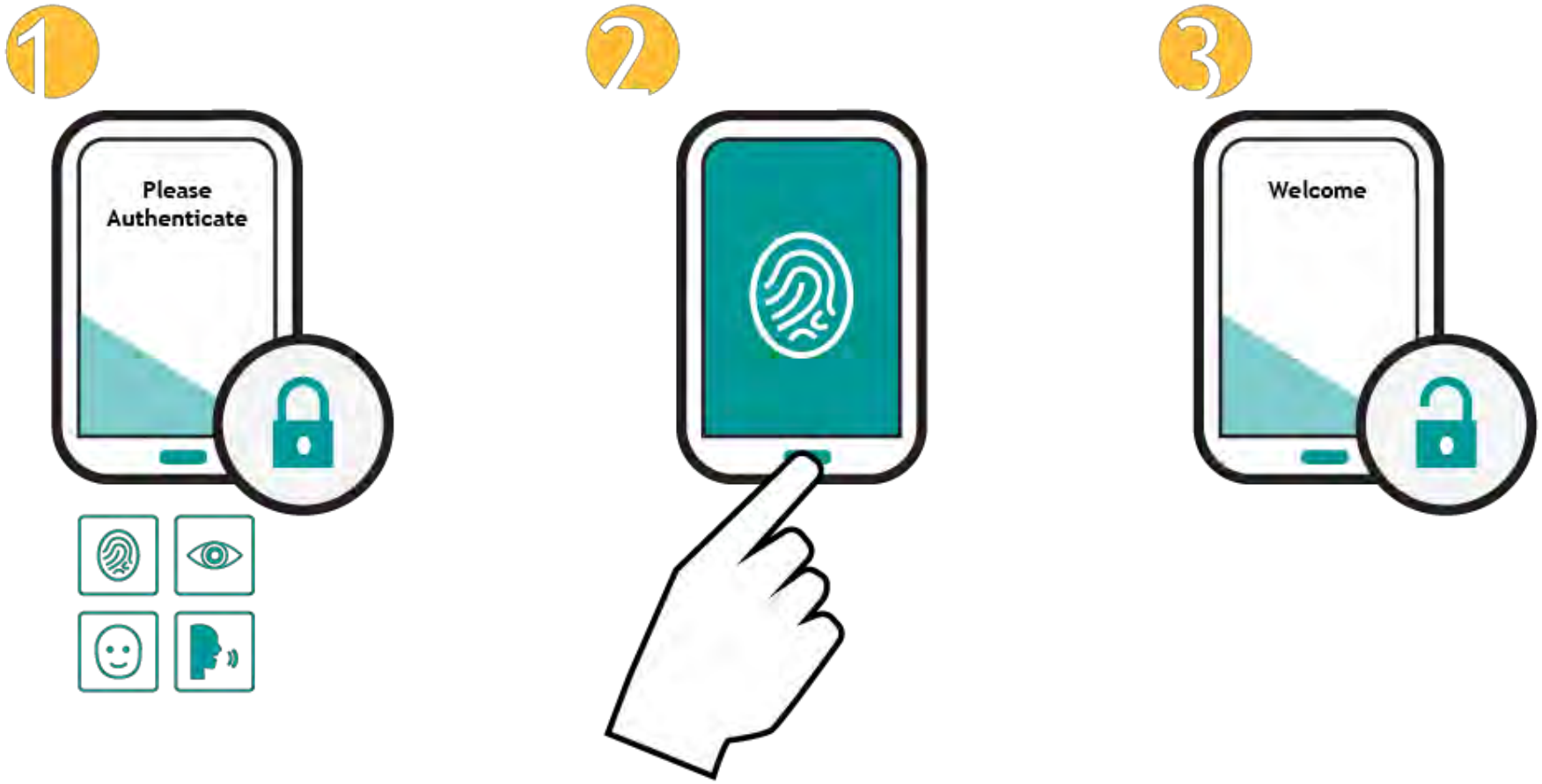
- Biometrics authn via mobile device
- Biometric authn via PC
- Biometrics authn to PC via mobile device

## 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

## Client-to-Authenticator Protocol (CTAP)

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

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

# SECOND FACTOR AUTHENTICATION TO MOBILE APPLICATIONS USING EXTERNAL AUTHENTICATORS

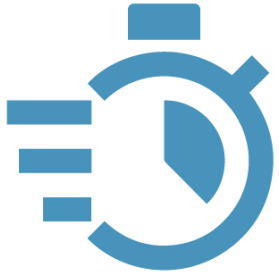
# SIMPLER AUTHENTICATION


Reduces reliance on complex passwords

Single gesture to log on

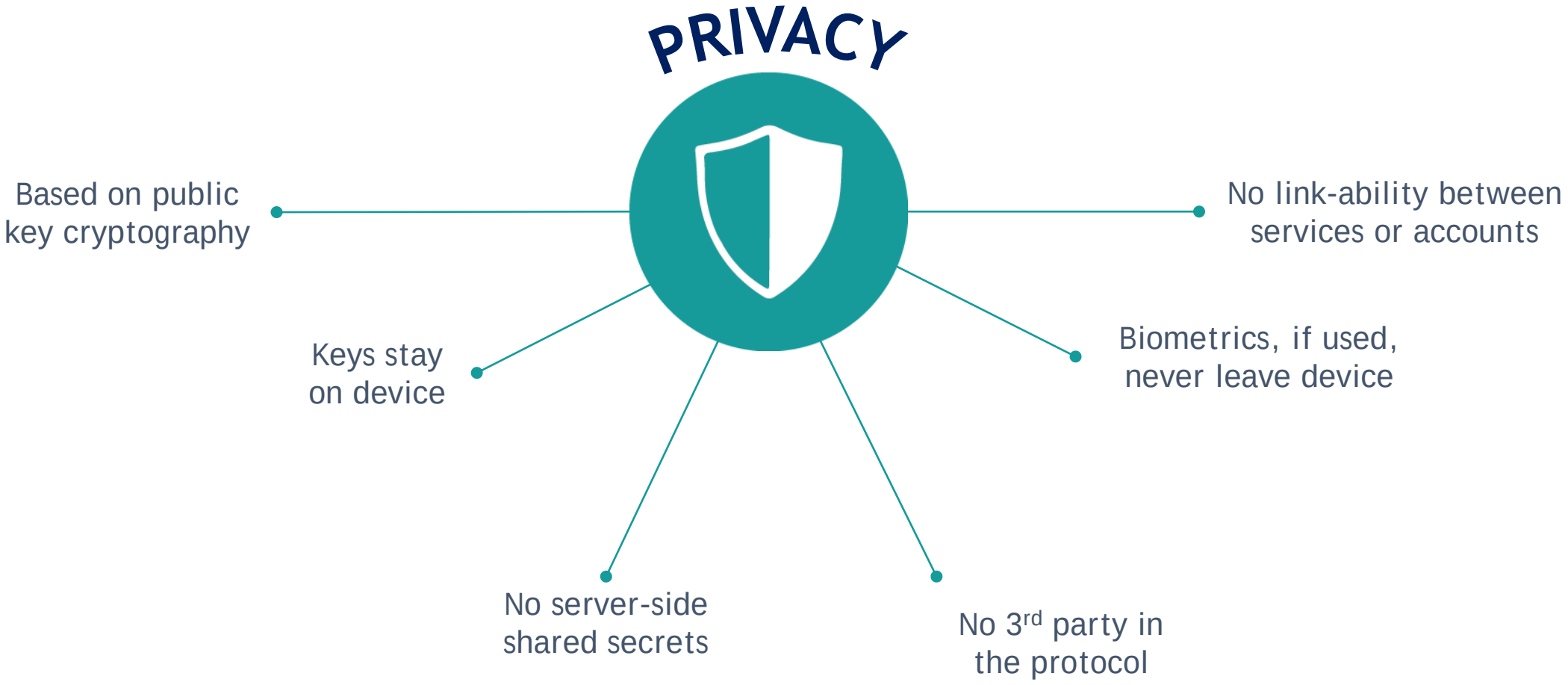
Works with commonly used devices

Same authentication on multiple devices



Fast and convenient

# STRONGER AUTHENTICATION



# FIDO DELIVERS ON KEY PRIORITIES

Security

Usability

Privacy

Interoperability

# ADVANTAGES FOR DEPLOYING ORGANIZATIONS

## Open Standards ROI

FIDO-enable services once

Securely access from any trusted device

No more one-off integrations

Increases future-proofing

## Unique FIDO Benefits

Lower total cost of ownership

Lower breach risks and potential damages

Increases choice of authenticators for users

Low-friction user experience

# WHERE'S FIDO IN THE MARKET?

# FIDO CROSS-PLATFORM SUPPORT

# SAMPLE: FIDO-ENABLED SERVICES

fido ALLIANCE

Google

LOGIN.GOV

ebay

facebook

salesforce

Bank of America

中国银行 BANK OF CHINA

NTT docomo

aetna

AVAILABLE TO PROTECT

**3.5 BILLION**

ACCOUNTS WORLDWIDE

T·Mobile

GitHub

PayPal

BCcard

Dropbox

dashlane

intuit

Microsoft

YAHOO! JAPAN

Cigna

# BACKED BY CERTIFICATION (>500)

- Functional Certification (End-to-End):
  - Conformance Testing
  - Interoperability Testing

- Authenticator Security Certification Levels
  - How well do you protect the private key?
  - 3rd-party laboratory verification
  - Complimented by new Biometric Component certification

- Universal Server:
  - Ensures compatibility with all FIDO Certified Authenticators

# FIDO CERTIFIED ECOSYSTEM (SAMPLE)

PHONES, PCs, & BROWSERS

SECURITY KEYS

CLOUD/SERVER SOLUTIONS

# FIDO AND REGULATION

# AUTHENTICATION IS IMPORTANT TO GOVERNMENT

1) Protects access to government assets
2) Enables more high-value citizen-facing services
3) Empowers private sector to provide a wider range of high value services to consumers
4) Secures critical assets and infrastructure

Governments seek identity solutions that can deliver not just improved SECURITY - but also PRIVACY, INTEROPERABILITY and better CUSTOMER EXPERIENCES

# FIDO IMPACT ON POLICY

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.

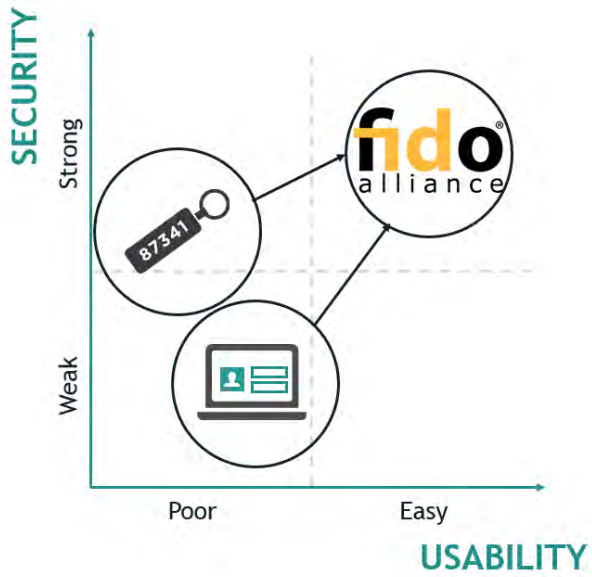
As technology evolves,
policy needs to evolve with it.

# 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"*

*–US Department of Health and Human Services 2015 Edition Health Information Technology (Health IT) Certification Criteria, October, 2015*

- 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 AUTHN FACTORS IN A SINGLE DEVICE

- Recognized by the U.S. 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

ITL BULLETIN FOR DECEMBER 2014

RELEASE OF NIST SPECIAL PUBLICATION 800-157,
*GUIDELINES FOR DERIVED PERSONAL IDENTITY VERIFICATION (PIV) CREDENTIALS*

Hildegard Ferraiolo, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

**Background**

Members of the federal government are increasingly using Personal Identity Verification (PIV) cards that uniquely identify the cardholder through verification of electronically stored credentials. PIV smart cards are used to allow the cardholder access to government facilities or to access federal computer systems (e.g., desktops and laptops) equipped with smart card readers. In the last decade, the mobile computing device market has skyrocketed, with a resulting desire by both employers and employees to enable remote access from these devices.

NIST has recently released Special Publication (SP) 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, to provide the technical details for a system by which mobile devices such as smart phones and tablets are provisioned with PIV credentials, allowing these credentials to take the place of the smart card for remote authentication to federal systems. The publication describes how a user with a valid PIV card could obtain a derived credential on an integrated security token using either hardware or software cryptographic modules. This approach is in response to the mobile device authentication credential outlined in Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, published in August 2013.

NIST SP 800-157 does not address use of the PIV Card with mobile devices, but does provide an alternative in cases where using a PIV Card would be impractical. In lieu of the PIV Card, the alternative security token described in SP 800-157 can be implemented and deployed directly with mobile devices. The PIV credential associated with this alternative token is called a Derived PIV Credential. The use of a different type of token greatly improves the usability of electronic authentication from mobile devices to remote IT resources.

**Introduction to Special Publication 800-157**

The new Special Publication describes the life-cycle activities associated with derived PIV credentials, including aspects of issuance, usage, and maintenance. It describes the methods for adhering to Homeland Security Presidential Directive 12 (HSPD-12), including the requirement that the credential be established through an official accreditation process.

SP 800-157 Chapter 3 describes the technical requirements related to certificate policies, cryptographic specifications, and the security token types that may be used with mobile devices. It lists guidelines for cases in which the use of PIV Cards with mobile devices—using either contact card readers or Near Field Communication (NFC)—is deemed impractical. The guideline specifies the use of tokens with alternative form factors to the PIV Card that may either be inserted into mobile devices—such as Secure Digital (SD) cards, Universal Serial Bus (USB)

1

# 2. RECOGNIZE 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

EBA/RTS/2017/02
23 February 2017

Final Report

Draft Regulatory Technical Standards

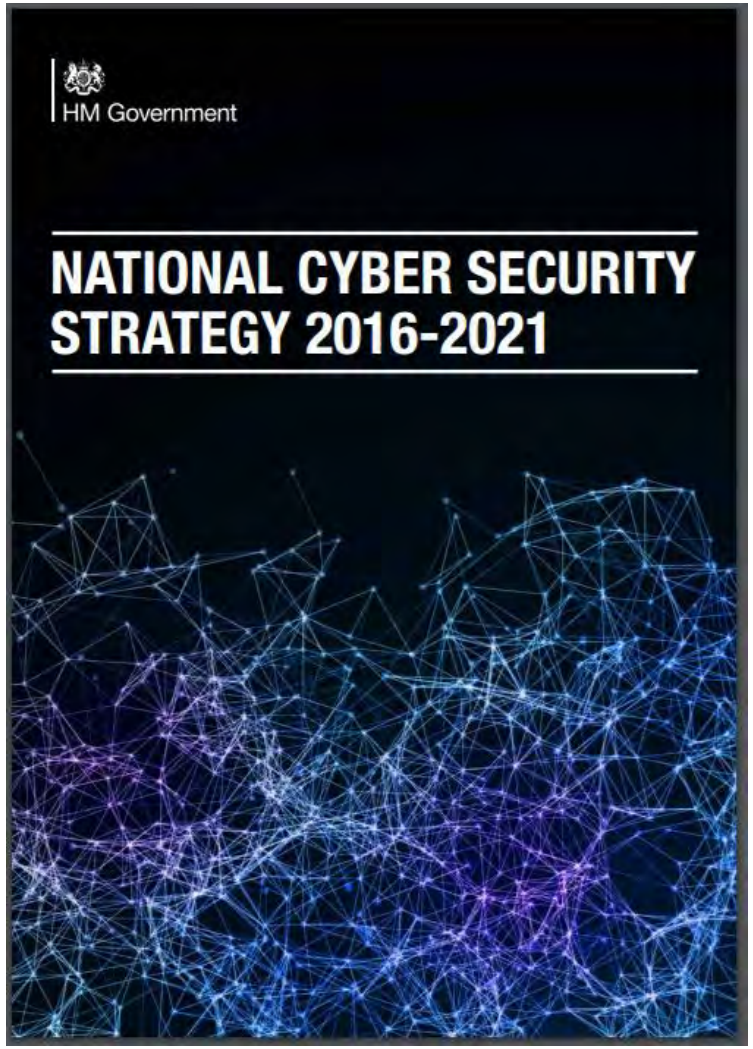
on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)

1

# 3. AS GOVERNMENTS PROMOTE OR REQUIRE STRONG AUTHENTICATION, MAKE SURE IT IS THE "RIGHT" AUTHENTICATION

- 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 IS IMPACTING HOW GOVERNMENTS THINK ABOUT AUTHENTICATION



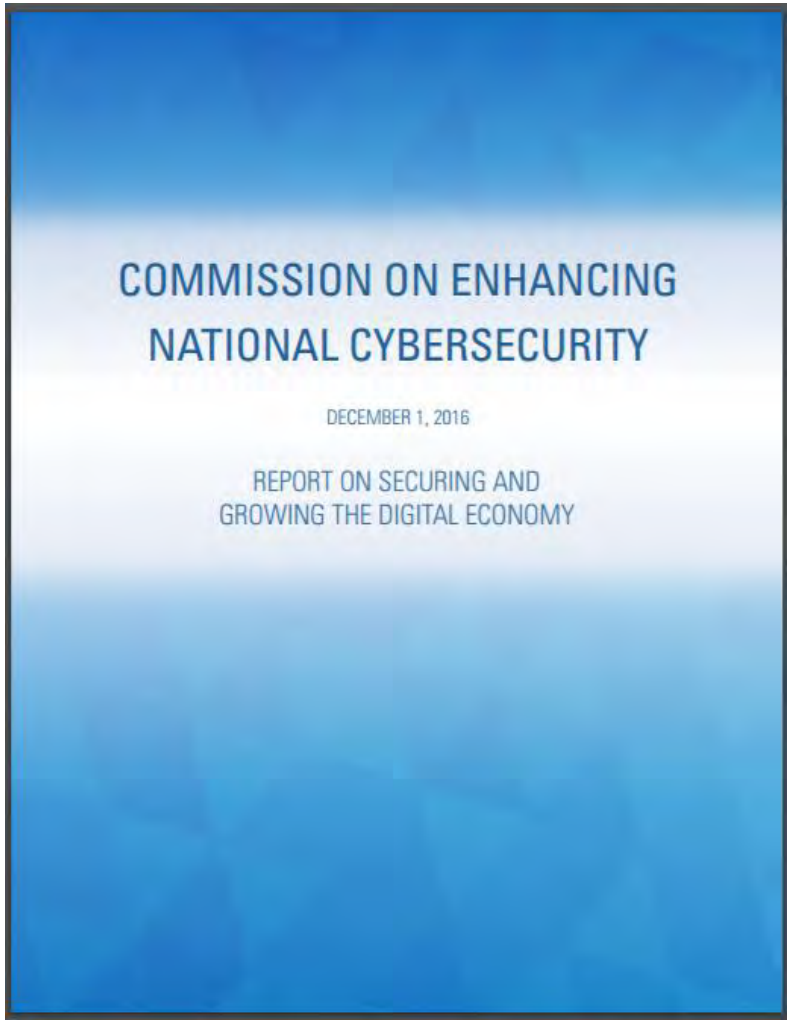

## Priorities:

- 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."*

# US COMMISSION ON ENHANCING NATIONAL CYBERSECURITY




*"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."*

# NEW NIST GUIDANCE (SP 800-63-3)

NIST AUTHENTICATOR ASSURANCE LEVEL 1

NIST AUTHENTICATOR ASSURANCE LEVEL 2

NIST AUTHENTICATOR ASSURANCE LEVEL 3


- SMS OTPs now RESTRICTED

- Easily compromised credentials
- Credentials stored in the cloud
- Example: passwords (“memorized secrets”)

- Public Key Cryptography
- Credentials stored ON DEVICE
- Example: FIDO Authentication

# SOUTH KOREA

## South Korea has moved away from Internet Explorer/ActiveX mandate for online financial services and is embracing open standards

- South Korea policy that any person using online financial services or payments had to obtain a digital certificate tied specifically to use of Internet Explorer and ActiveX controls was limiting and created cybersecurity risk

- The Korean Internet Security Agency (KISA) has since embraced the FIDO specifications as part of a broader way to get to a more modern, vendor-neutral approach to authentication

- Lesson learned: locking in to a single technology, as opposed to vendor-neutral solutions rooted in standards, meant that efforts to migrate to a more modern solution took many years and introduced significant levels of complexity

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

# Questions?

## FIDO Alliance: Standards-based Solutions for Simpler, Strong Authentication

Jeremy Grant
Managing Director, Technology Business Strategy
Venable LLP

jeremy.grant@venable.com
@jgrantindc


fido™ ALLIANCE