



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

Jeremy Grant
Managing Director, Technology Business Strategy
Venable LLP

jeremy.grant@venable.com
@jgrantindc



Digital: The Opportunity and the Challenge

Fintech from the Frontlines:

The Opportunity for Technology
to Improve Financial Services for All

 PayPal

“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

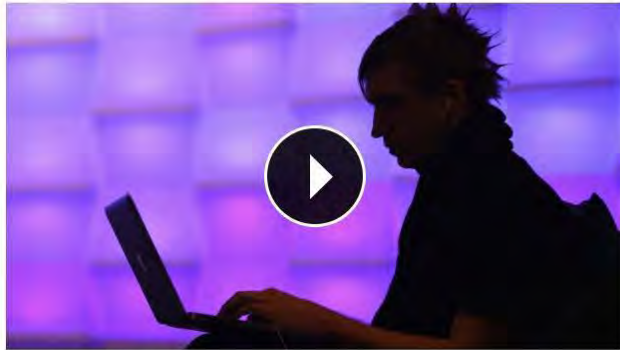


THE WORLD HAS A PASSWORD PROBLEM

HOW SECURE IS AUTHENTICATION?

Criminals steal 1.2 billion passwords

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 Register

Sensitive client emails, usernames,
passwords exposed in Deloitte hack

Mashable

Someone is selling 33 million Twitter
passwords on the dark web

The New York Times

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

Fortune

LinkedIn Lost 167 Million Account Credentials in Data
Breach

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 passwords¹



65%

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



1,579

Breaches in 2017, a 45% increase over 2016³



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

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

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

¹Identity 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



**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

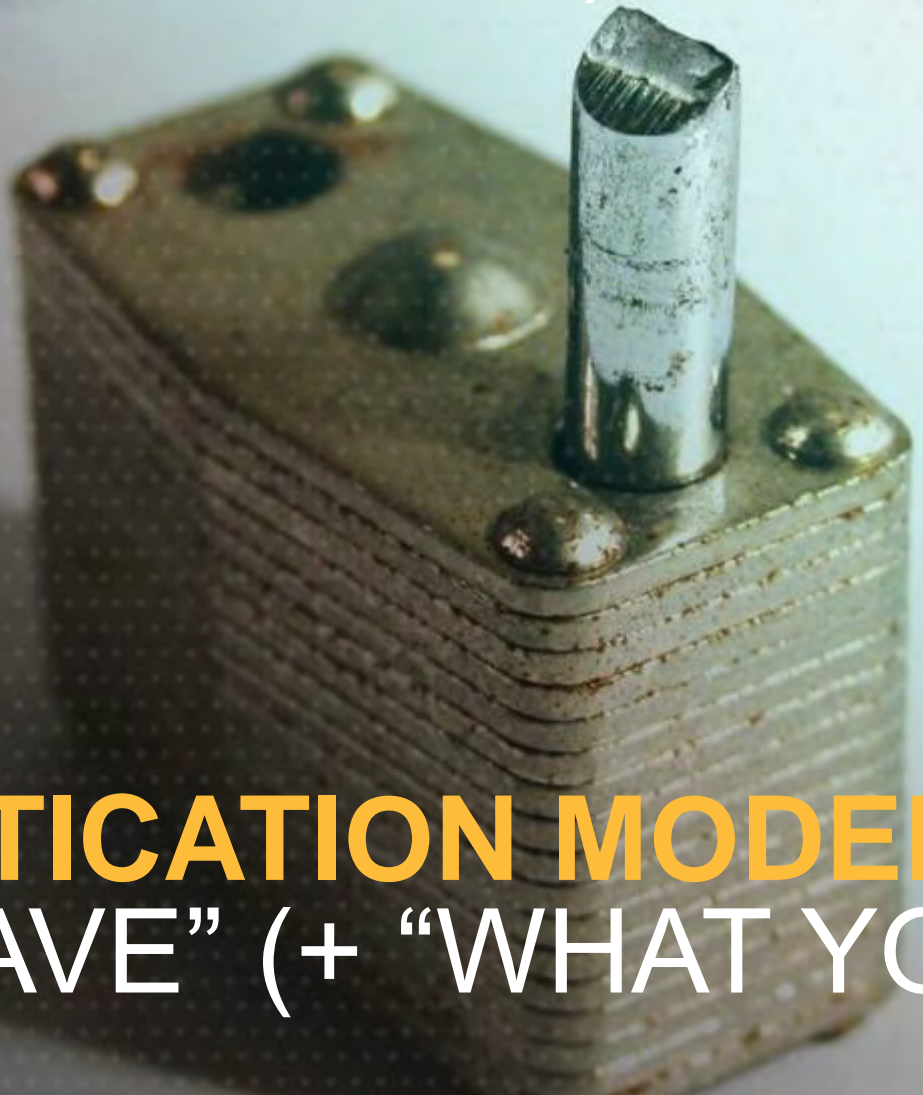
“Whenever possible, people should also avoid using text messages to receive one-time passwords. Instead, they should rely on cryptographically based security keys as a second authentication factor”

Ars Technica, April 2017






THE WORLD HAS A “SHARED SECRETS” PROBLEM

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 =

- ✓ 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

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



CONSUMER ELECTRONICS



SECURITY & BIOMETRICS



HIGH-ASSURANCE SERVICES

INDUSTRY PARTNERSHIPS



SECURITY. IDENTITY. TRUST.



FIDO Standards

FIDO2 Project

FIDO UAF

(ITU x.1277)

FIDO U2F

(ITU x.1278)

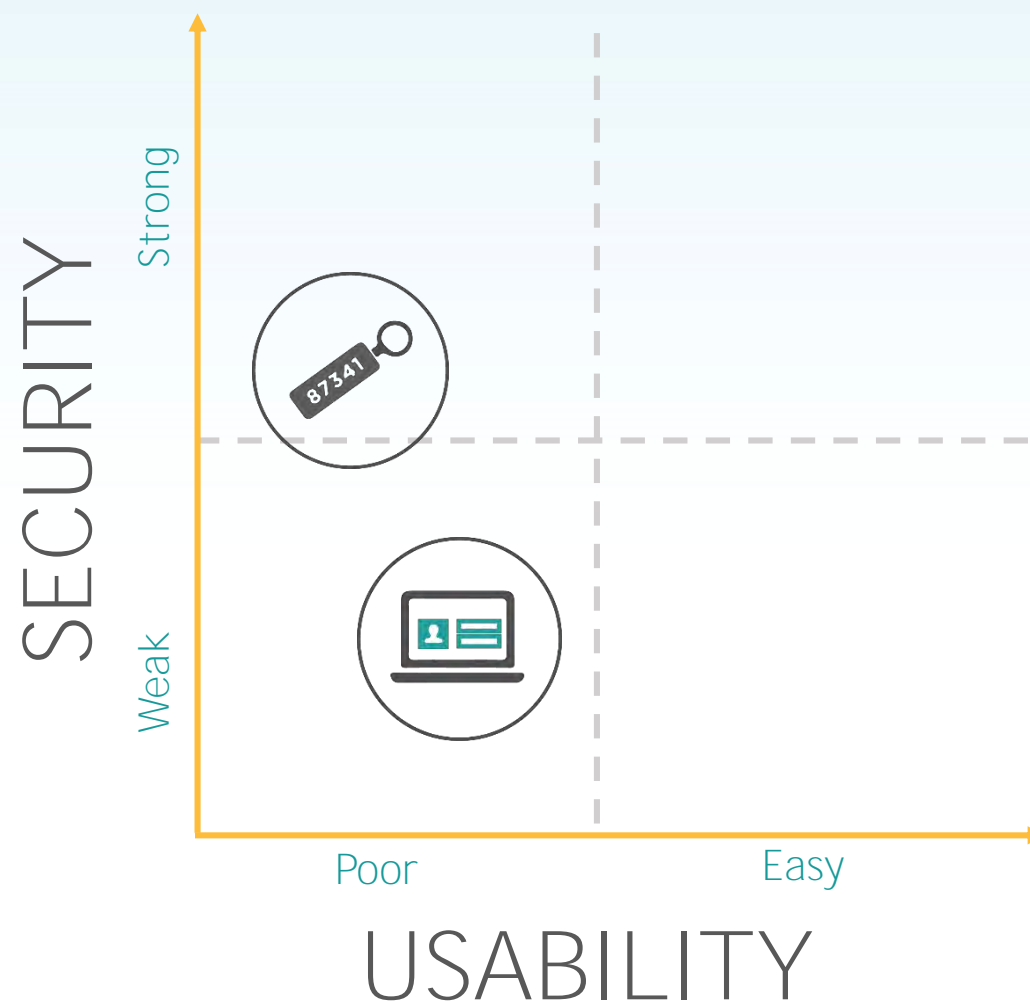
CTAP

(ITU x.1278)

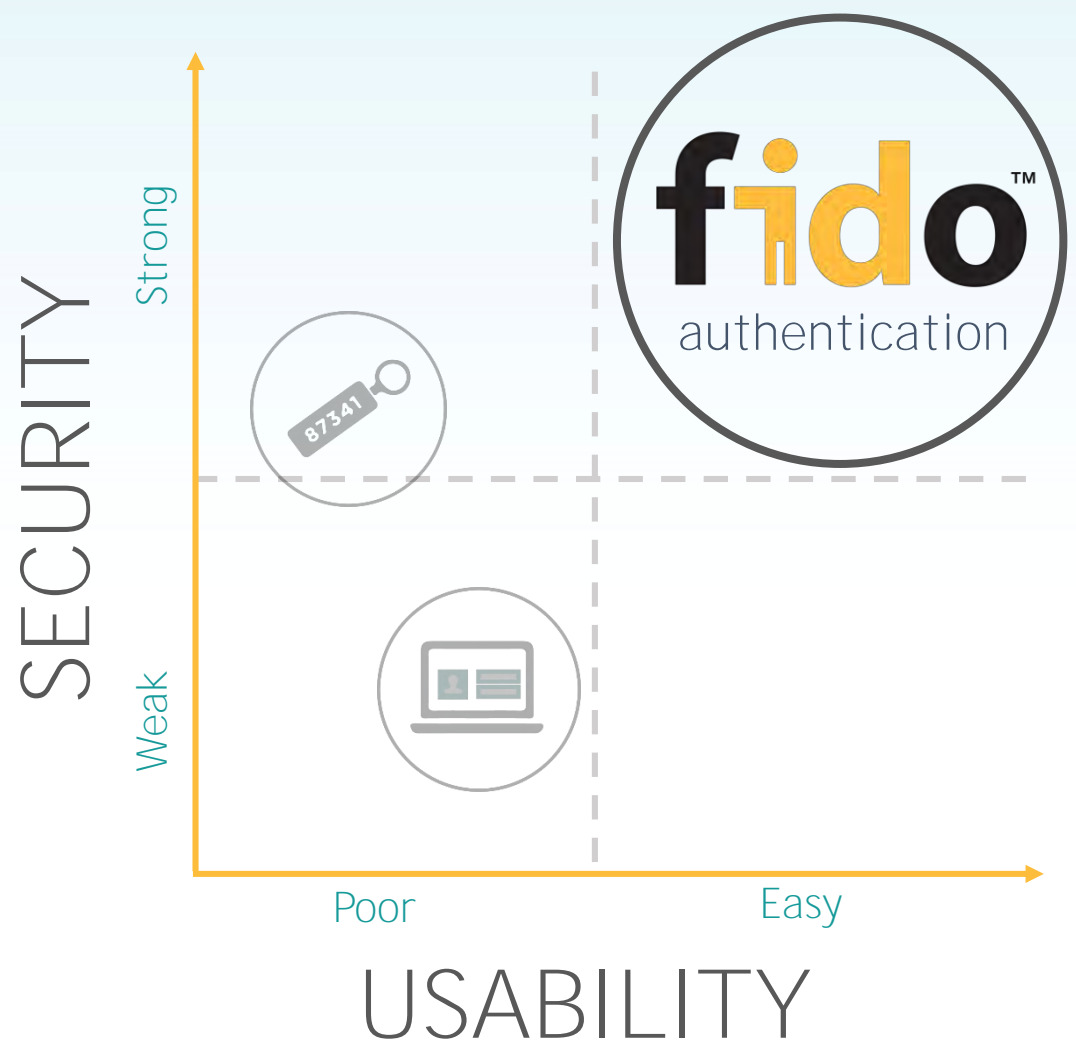
WebAuthn

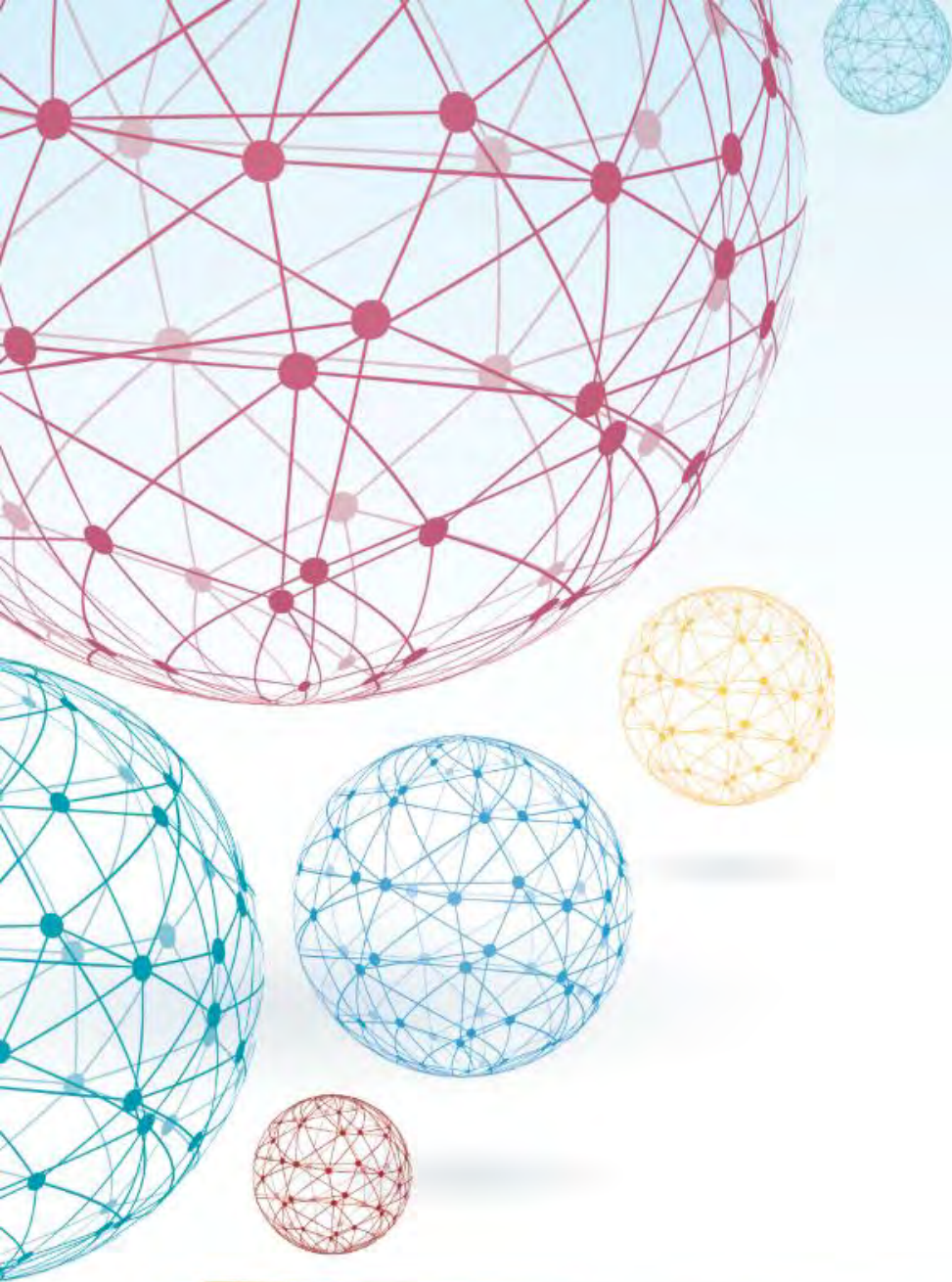
(W3C Standard)

THE OLD PARADIGM



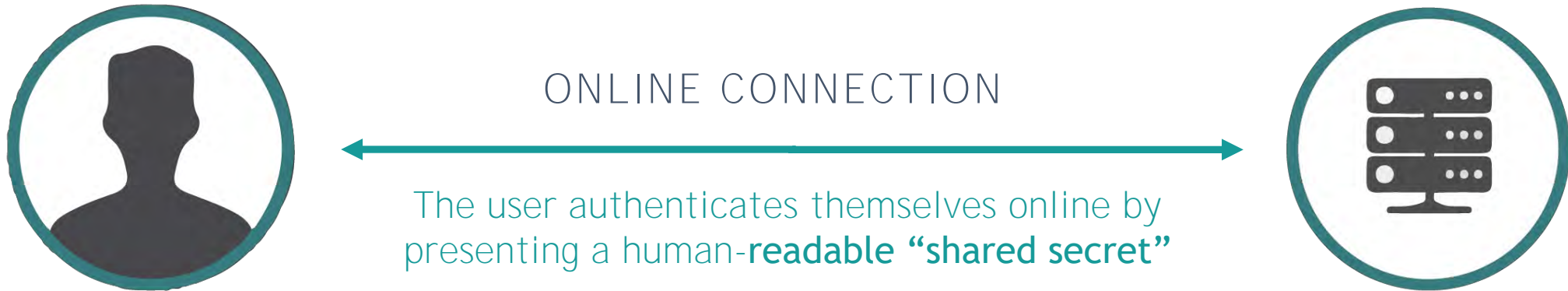
THE FIDO PARADIGM



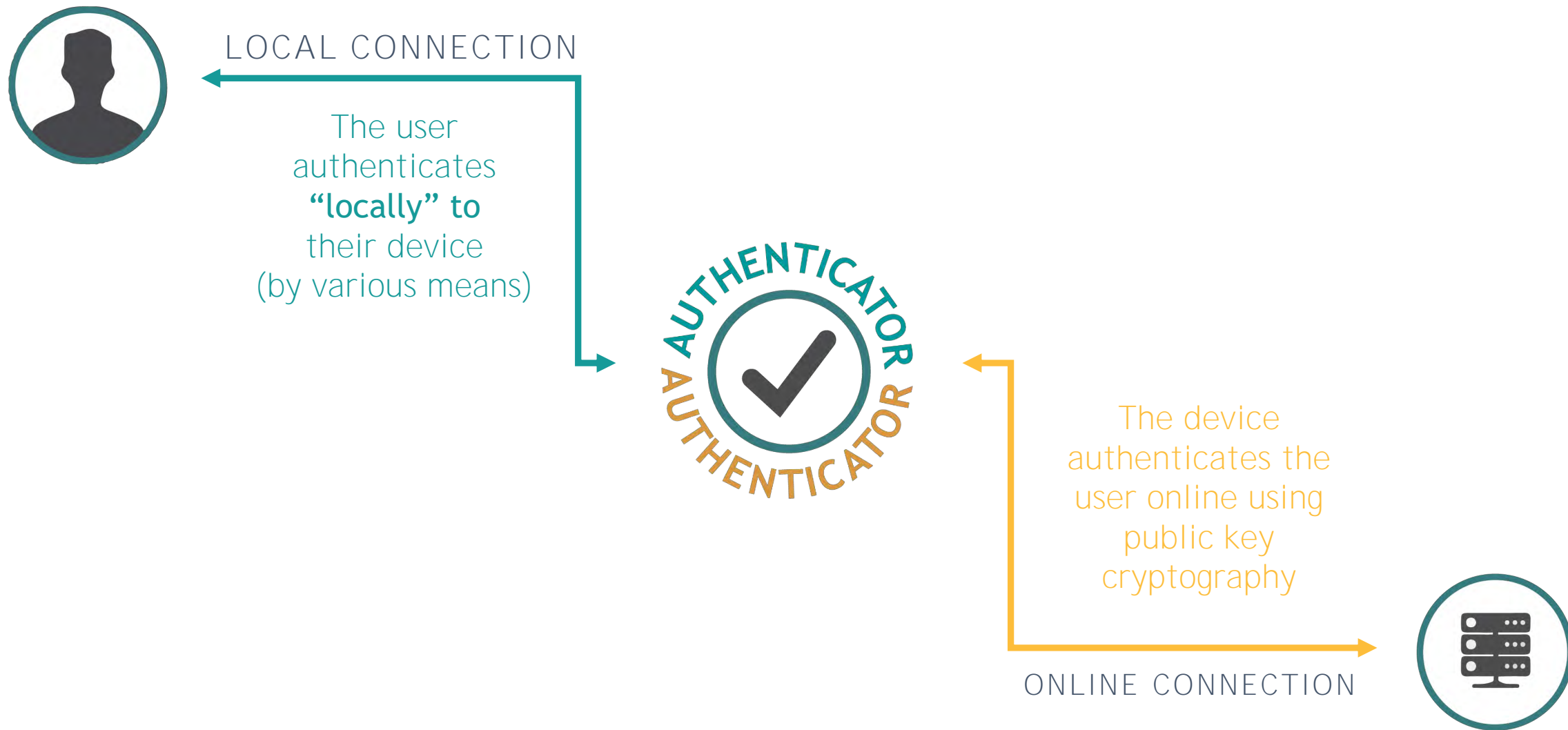


HOW FIDO WORKS

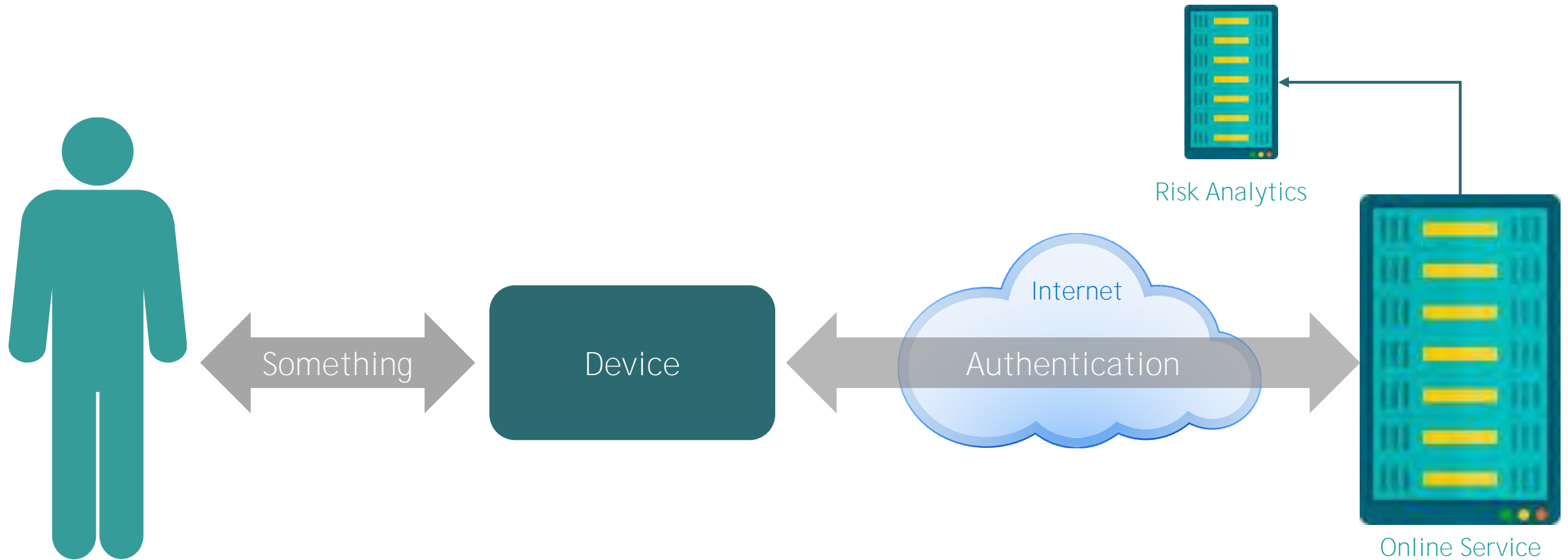
HOW OLD AUTHENTICATION WORKS



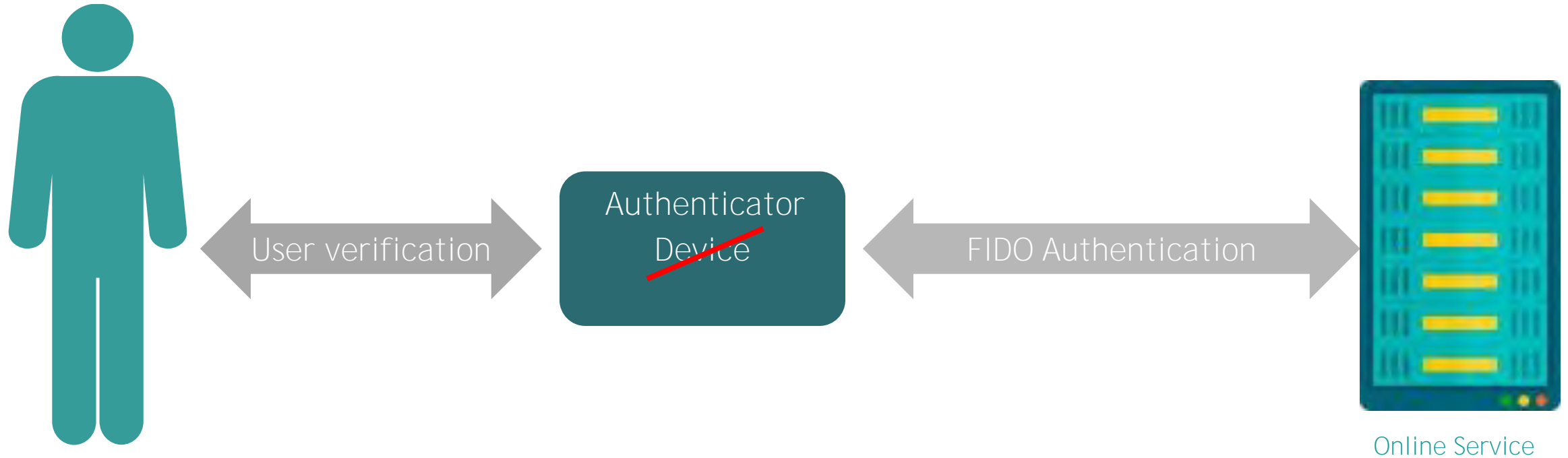
HOW FIDO AUTHENTICATION WORKS



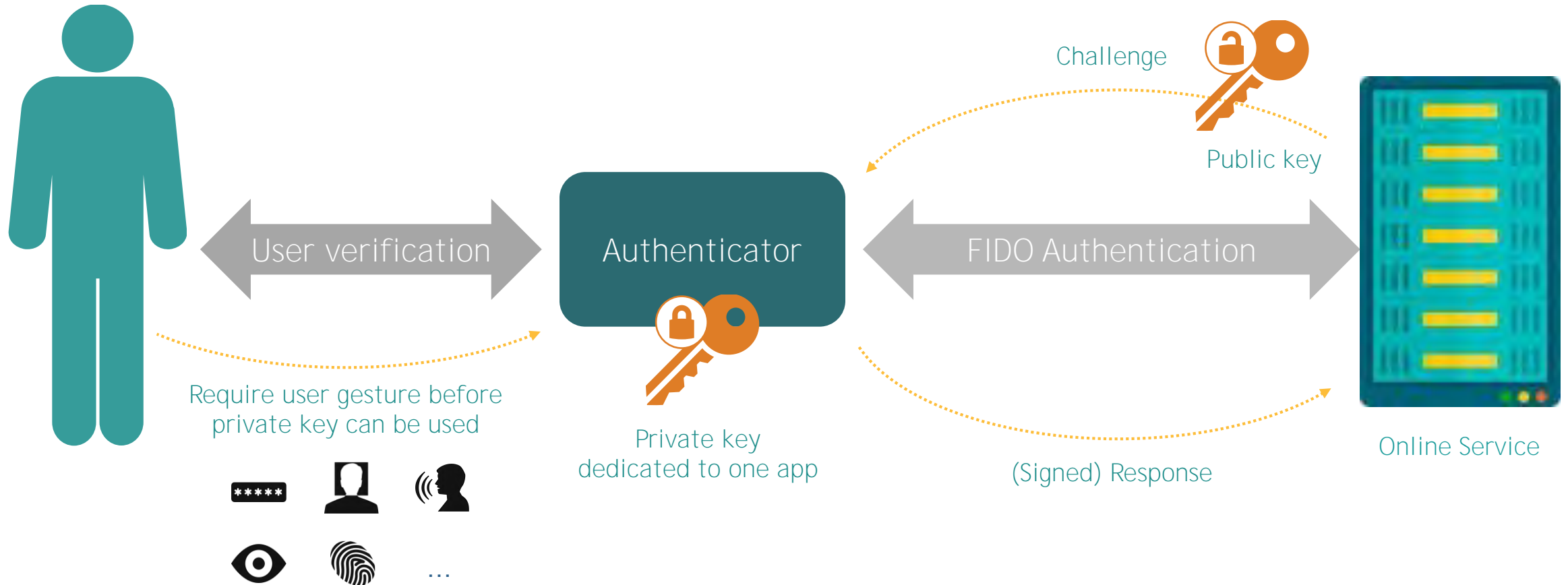
CLOUD AUTHENTICATION



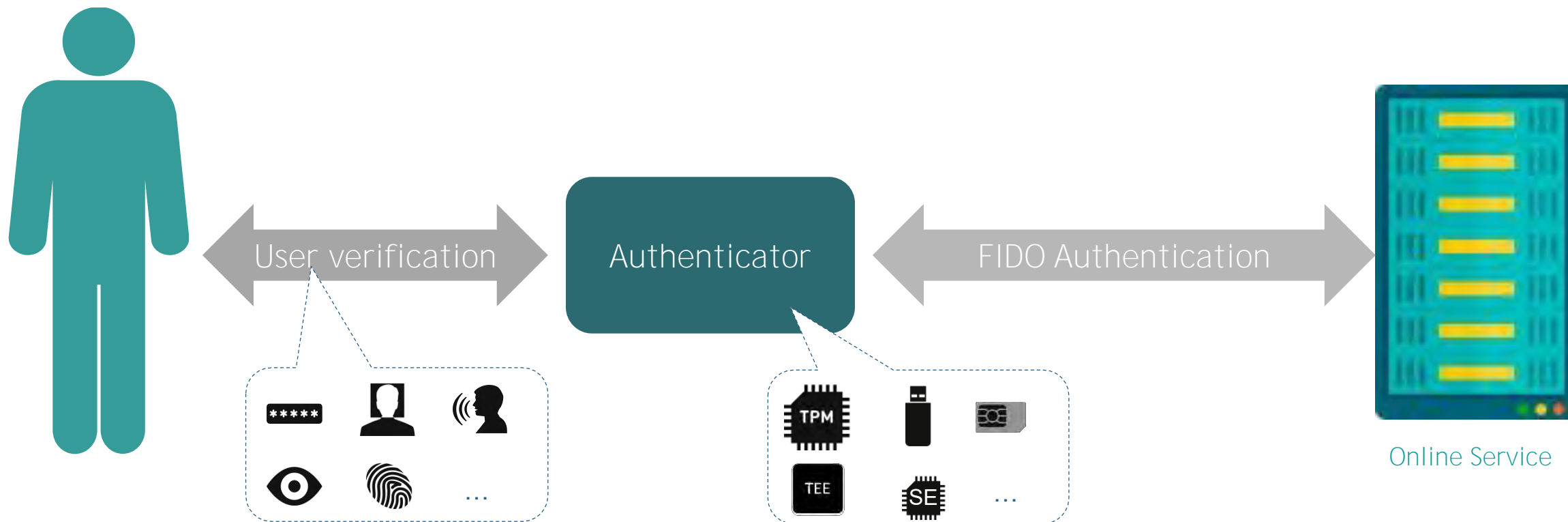
HOW DOES FIDO WORK?



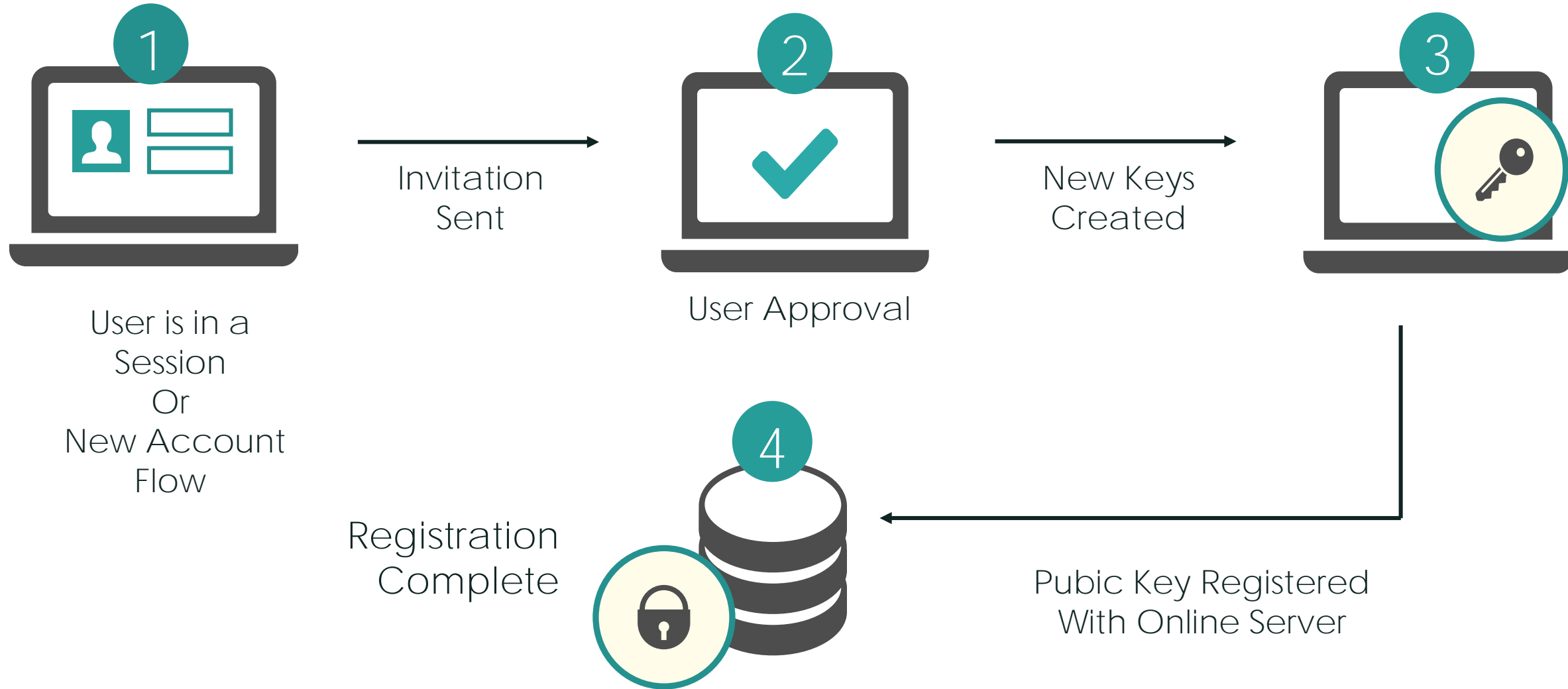
HOW DOES FIDO WORK?



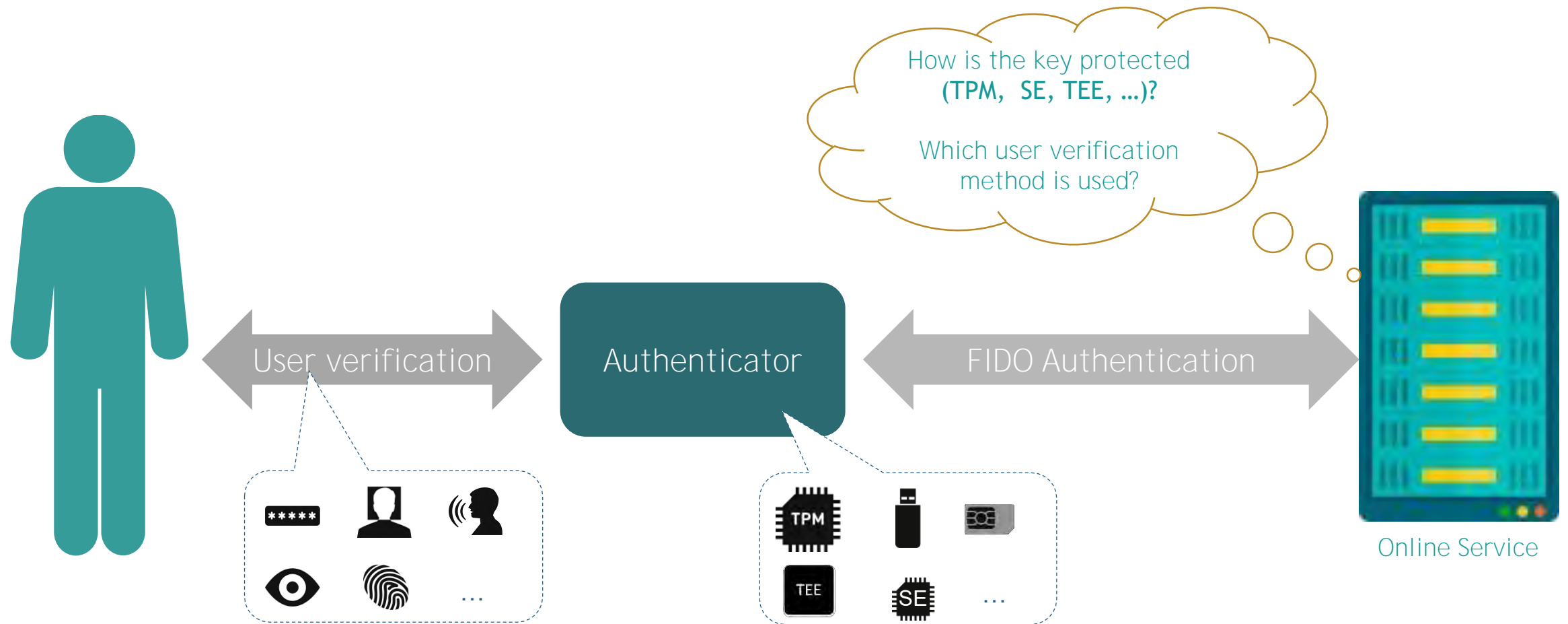
HOW DOES FIDO WORK?



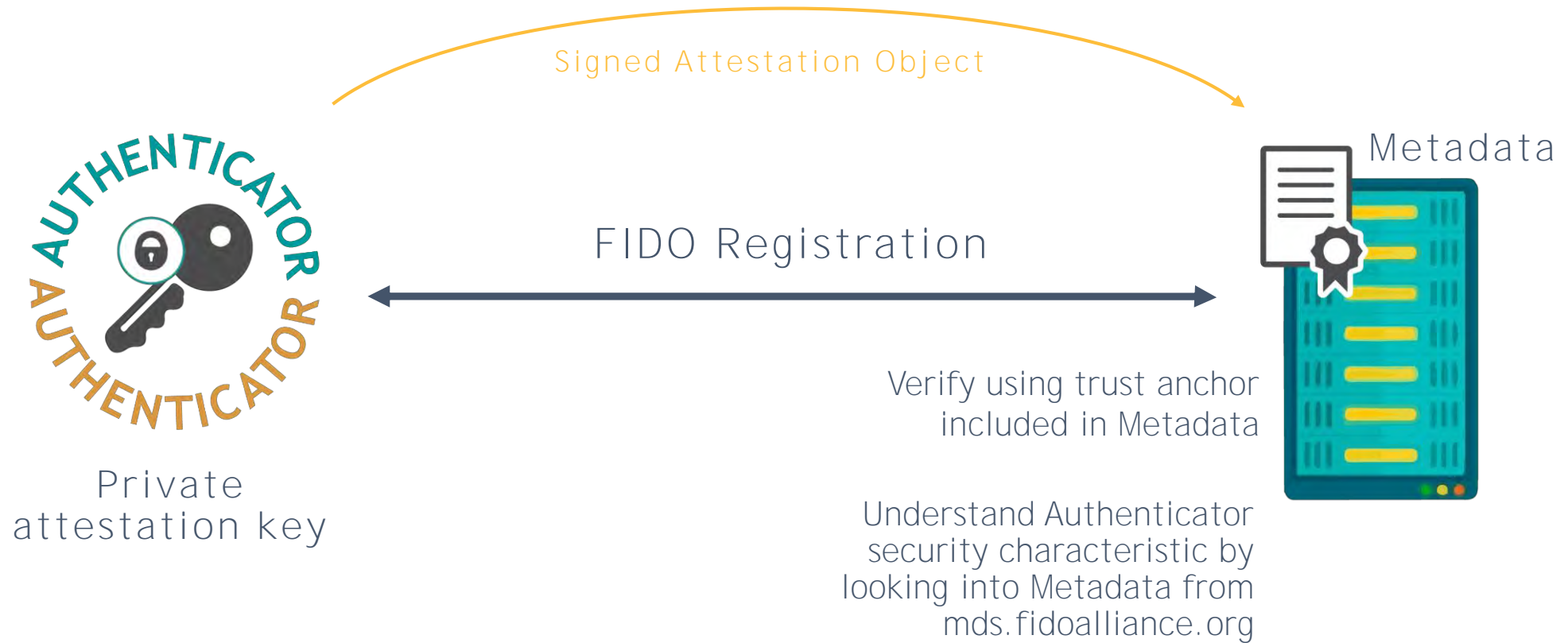
FIDO REGISTRATION

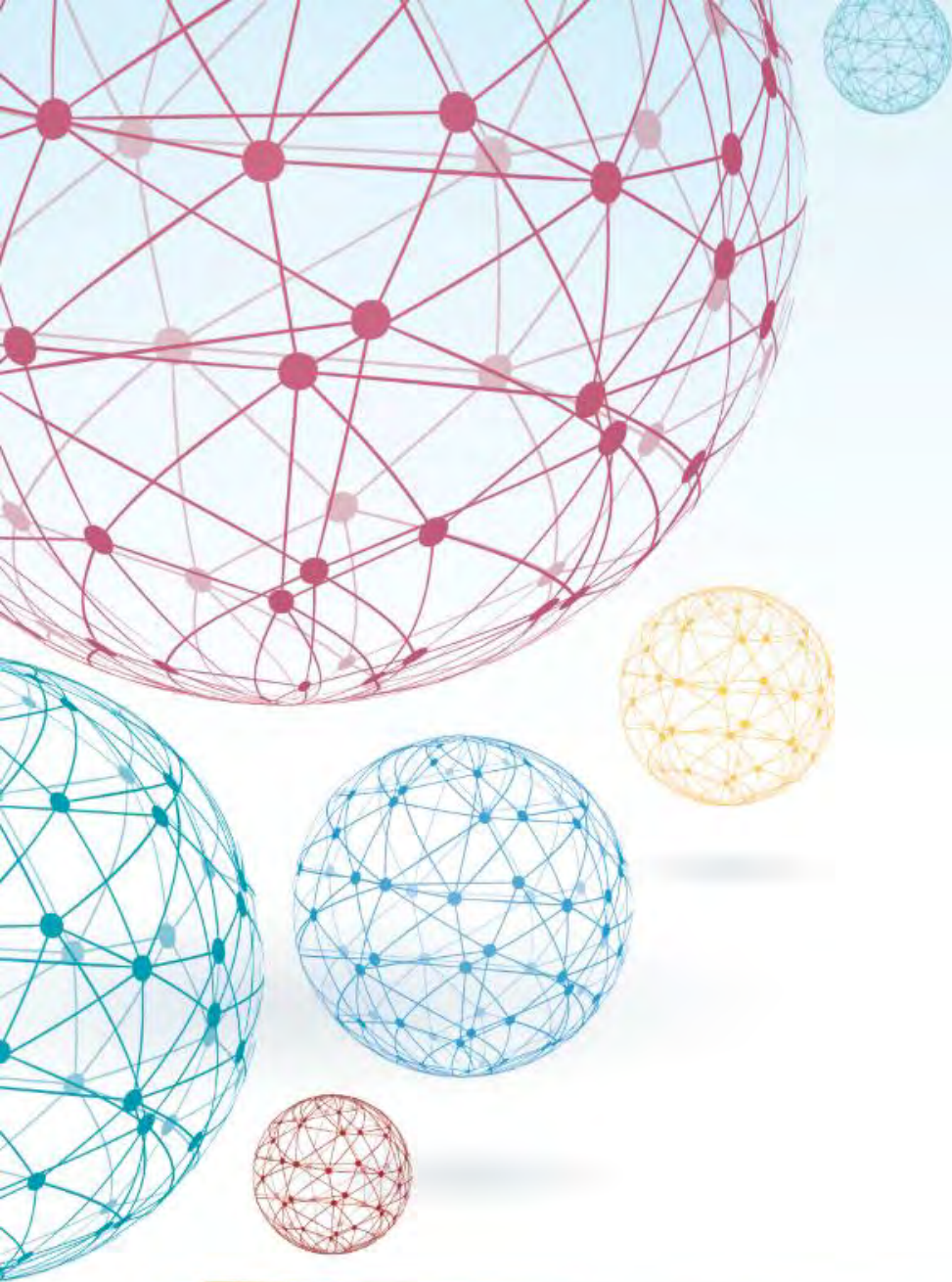


IMPORTANT DATA FOR SERVICE PROVIDERS



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



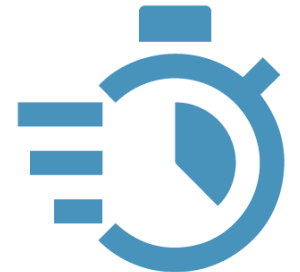
Single gesture to log on



Works with commonly used devices

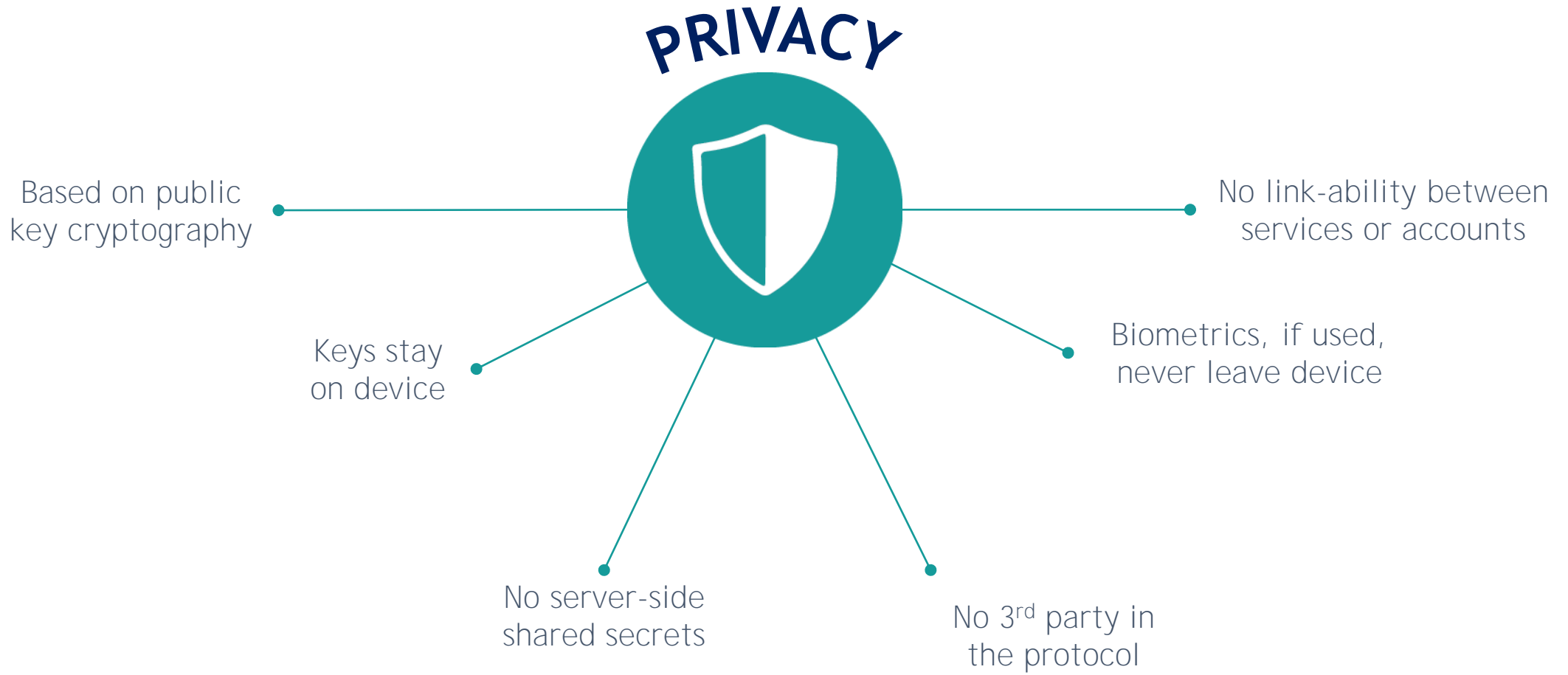


Same authentication on multiple devices



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



AVAILABLE TO PROTECT



3.5 BILLION

ACCOUNTS WORLDWIDE



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)



SONY



FEITIAN
WE BUILD SECURITY

Google



FUJITSU

SurePass 

 Ledger



ING 



SHARP

 OneSpan

 Daon

RSA

Lenovo



yubico



nok
nok

RAON
SECURE



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.

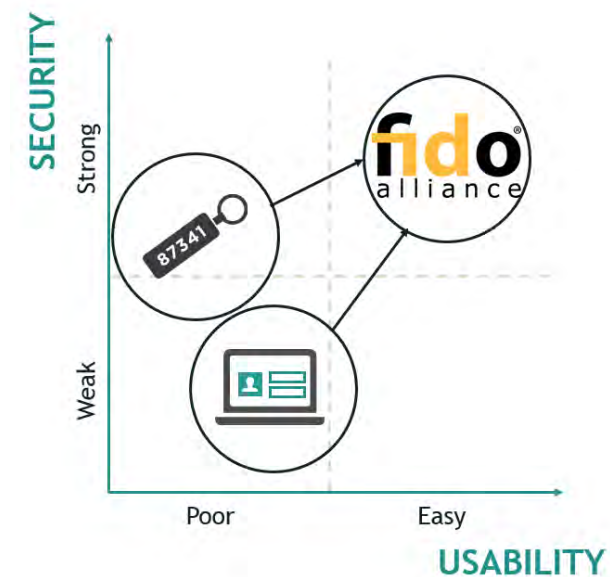


1. RECOGNIZE THAT TWO-FACTOR AUTHENTICATION NO LONGER BRINGS HIGHER BURDENS OR COSTS

“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

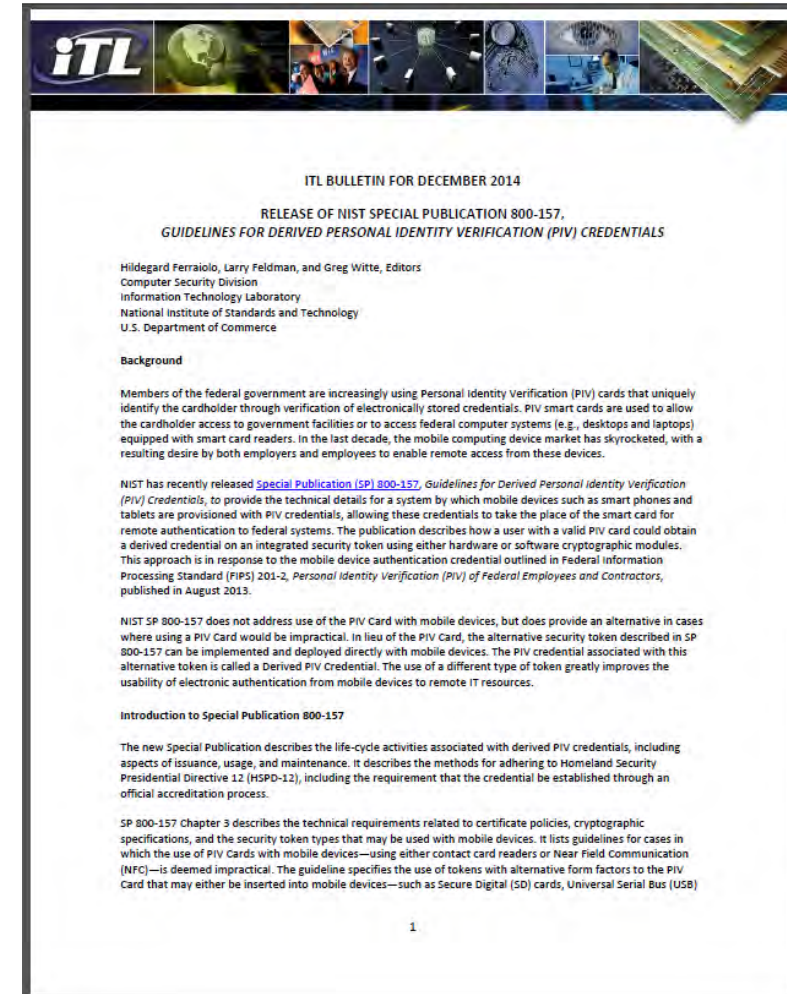
- While this statement was true of most “old” MFA technology, FIDO specifically addresses these cost and usability issues
- FIDO enables simpler, stronger authentication capabilities that governments, businesses and consumers can easily adopt at scale





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



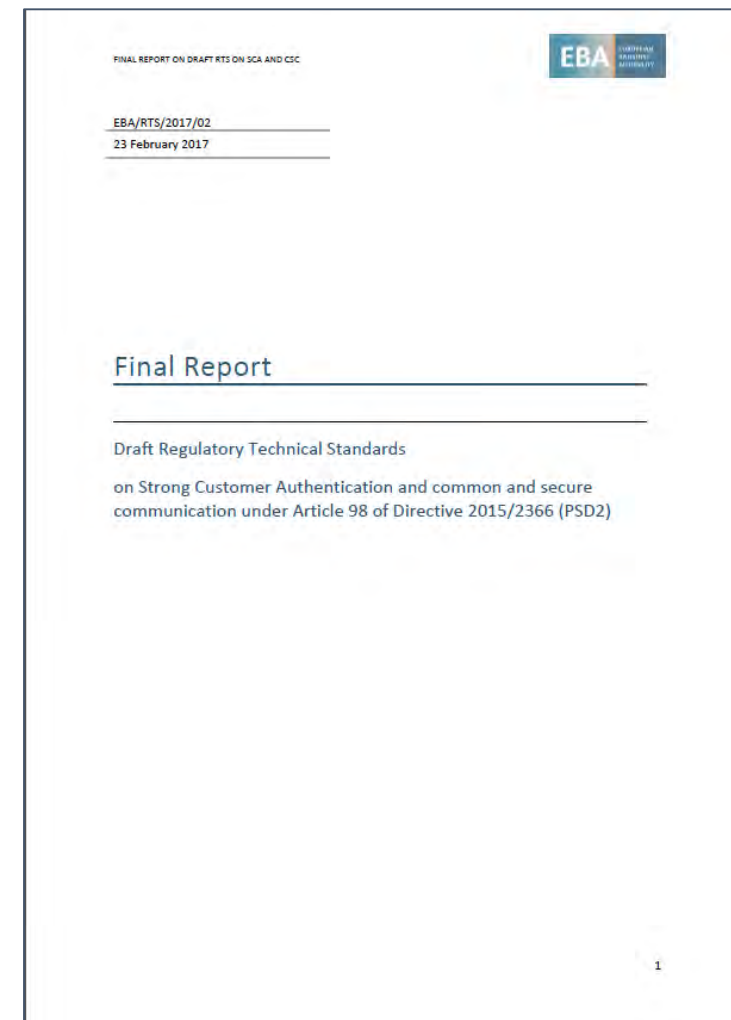


2. RECOGNIZE TECHNOLOGY IS NOW MATURE ENOUGH TO ENABLE TWO SECURE, DISTINCT AUTHN FACTORS IN A SINGLE DEVICE

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.



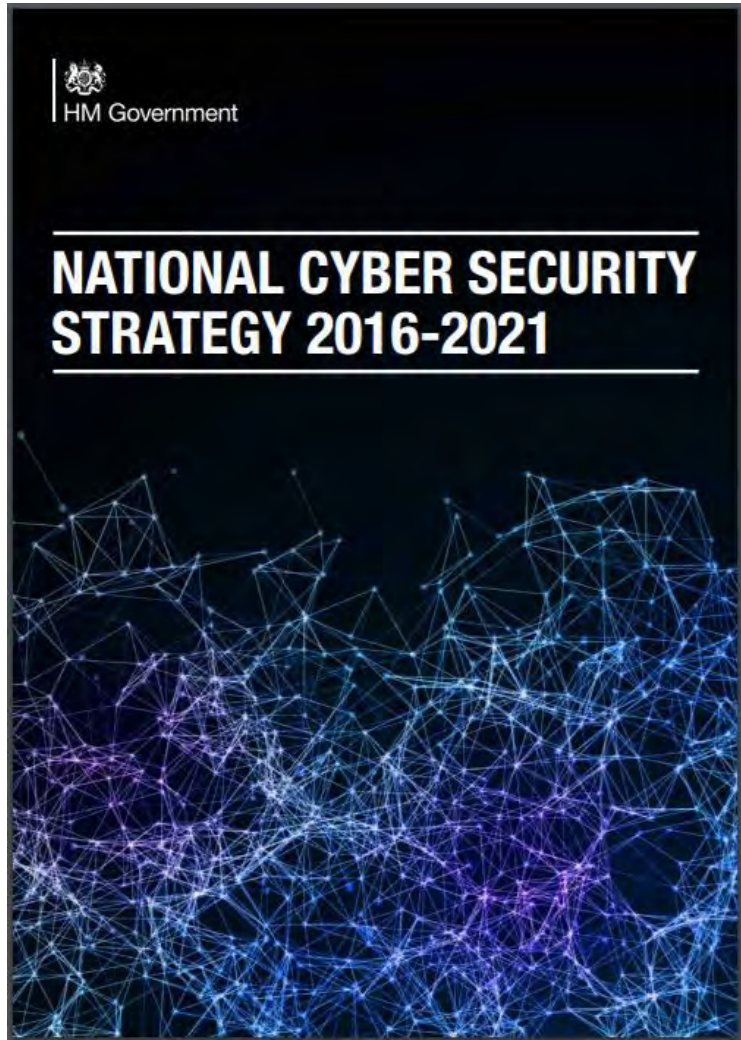


3. AS GOVERNMENTS PROMOTE OR REQUIRE STRONG AUTHENTICATION, MAKE SURE IT IS THE “RIGHT” AUTHENTICATION



- 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



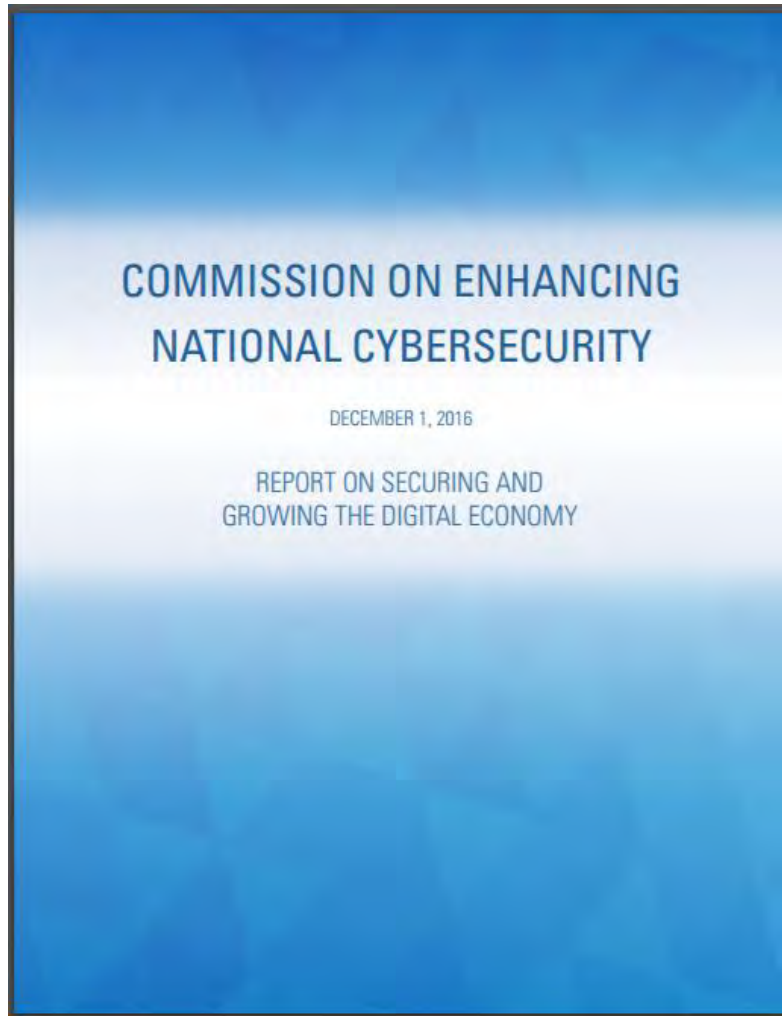
Priorities:

- 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



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

- SMS OTPs now RESTRICTED

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

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



Questions?

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

Jeremy Grant
Managing Director, Technology Business Strategy
Venable LLP

jeremy.grant@venable.com

@jgrantindc

