



A NEW MODEL FOR AUTHENTICATION

ENABLING MORE EFFICIENT DIGITAL SERVICE DELIVERY

Jeremy Grant

jeremy.grant@chertoffgroup.com



The world has a **PASSWORD PROBLEM**

The world has a **PASSWORD PROBLEM**

AMERICAN BANKER

Seven Ways Yahoo's 500M-User Data Breach
Affects Banks

FORTUNE

LinkedIn Lost 167 Million
Account Credentials in Data
Breach

*Data breaches
expected to reach
1,000 in 2016*

up 22% from 2015
-Identity Theft Resource
Center

*63% of data breaches
in 2015 involved
weak, default, or
stolen passwords*

-Verizon 2016 Data
Breach Report

*Each data breach
costs \$3.8 million
on average*

up 23% from 2013
-Ponemon Institute

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

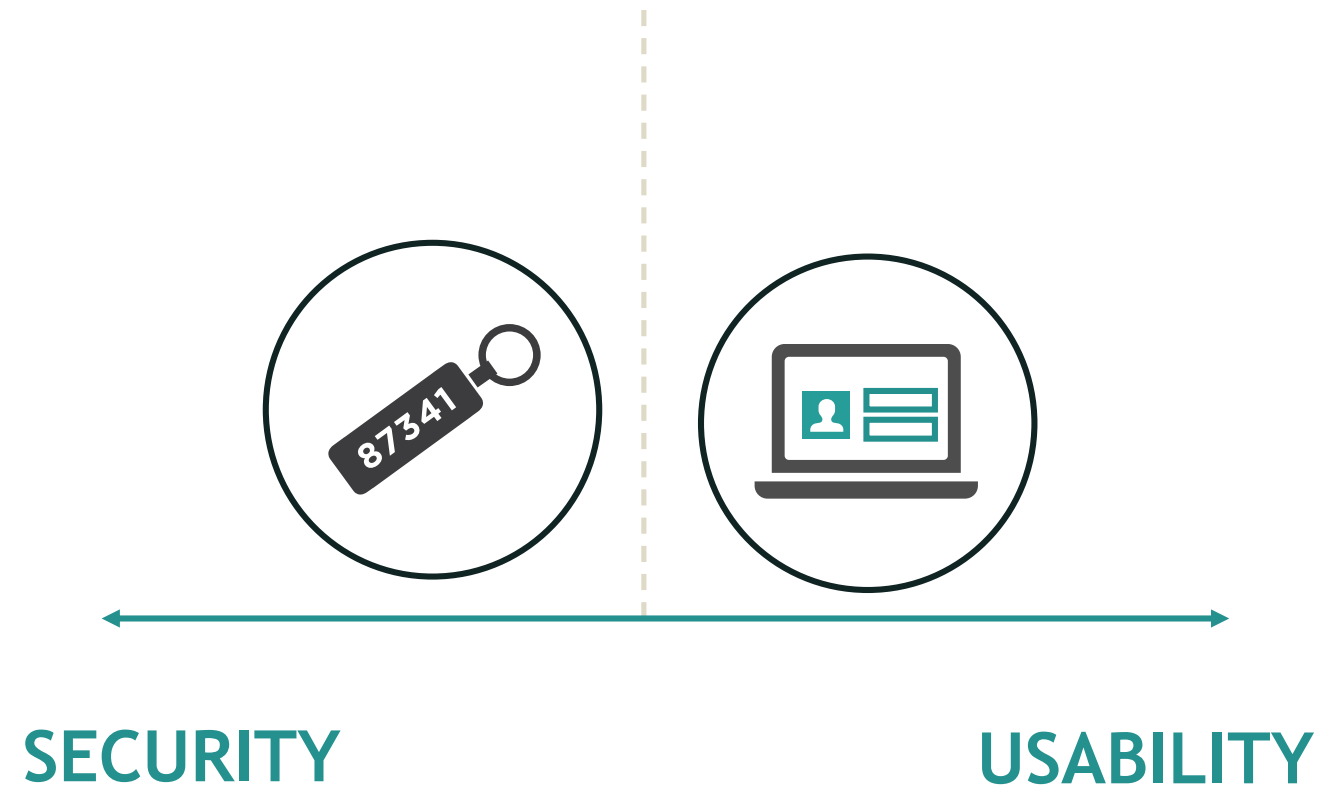


THE NEW MODEL

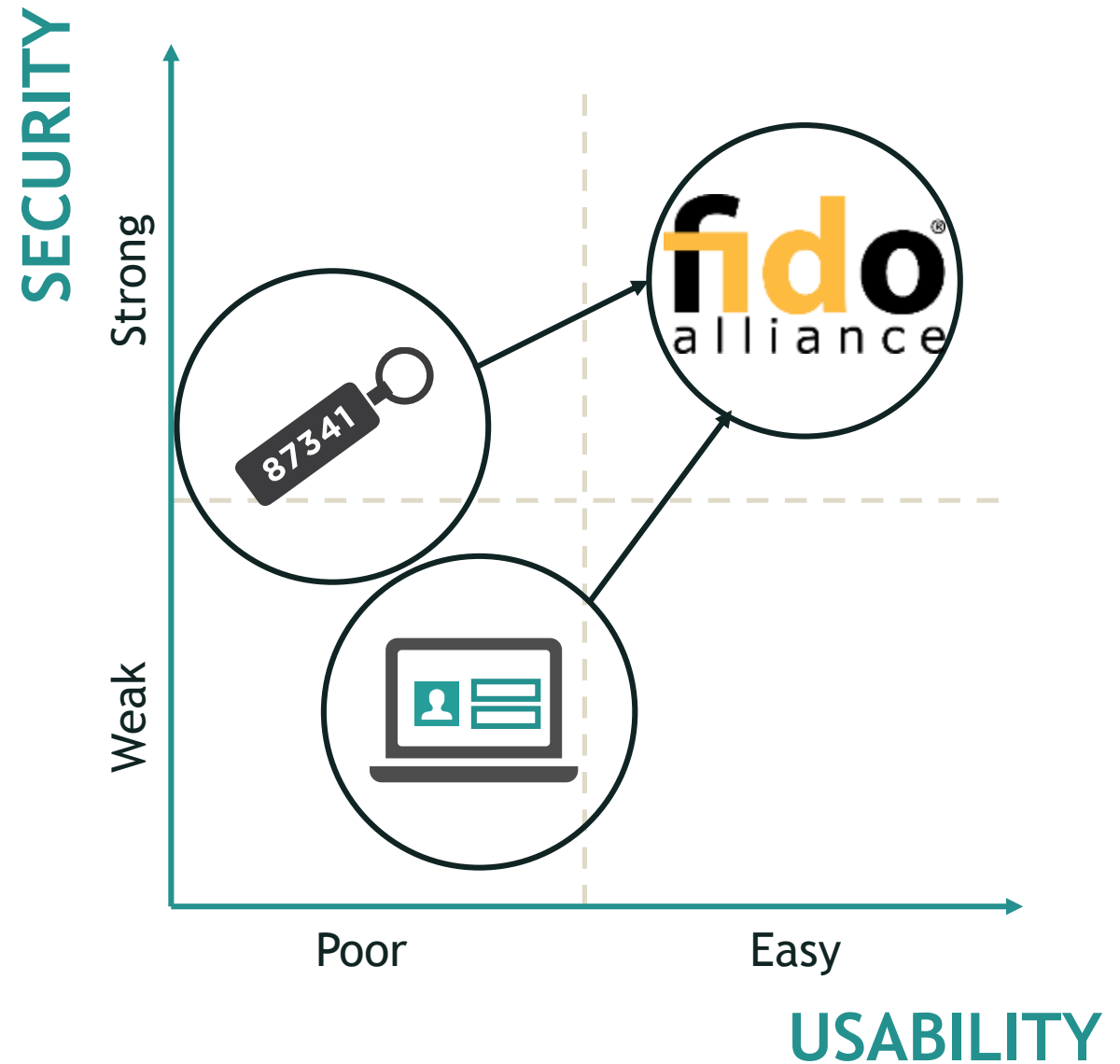
Fast IDentity Online

online authentication using
public key cryptography

THE OLD PARADIGM

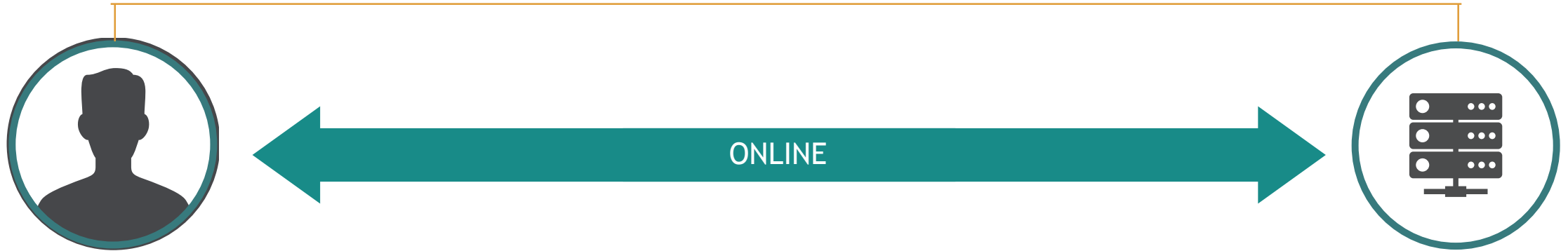


THE FIDO PARADIGM

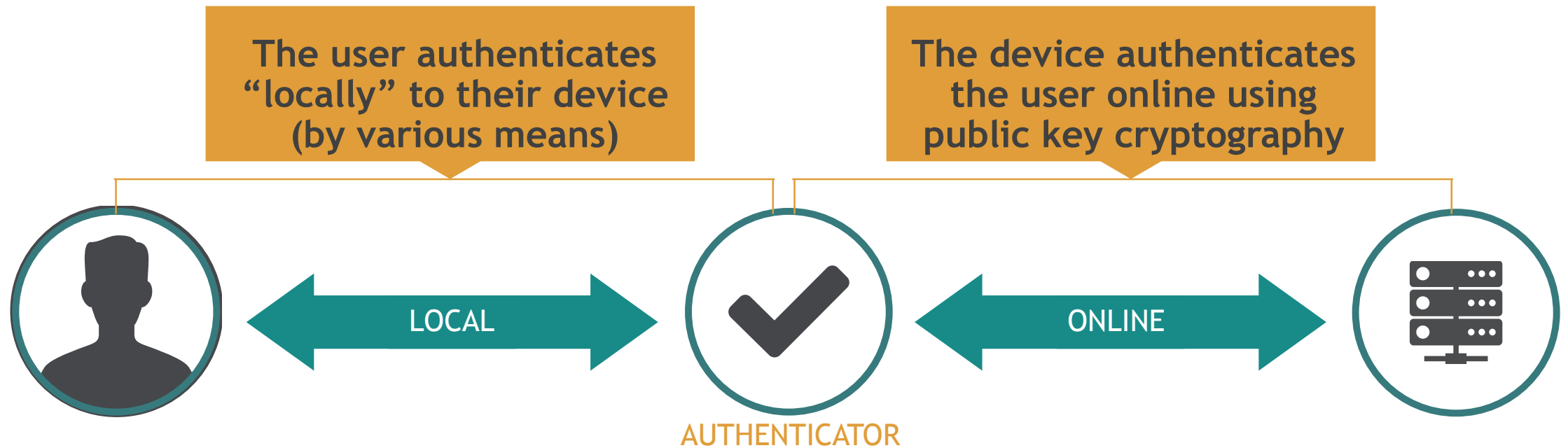


HOW “Shared Secrets” WORK

The user authenticates themselves online by presenting a human-readable “shared secret”



HOW FIDO WORKS



Support for Two Authentication Experiences

Passwordless Experience

FIDO UAF (Universal Authentication Framework)



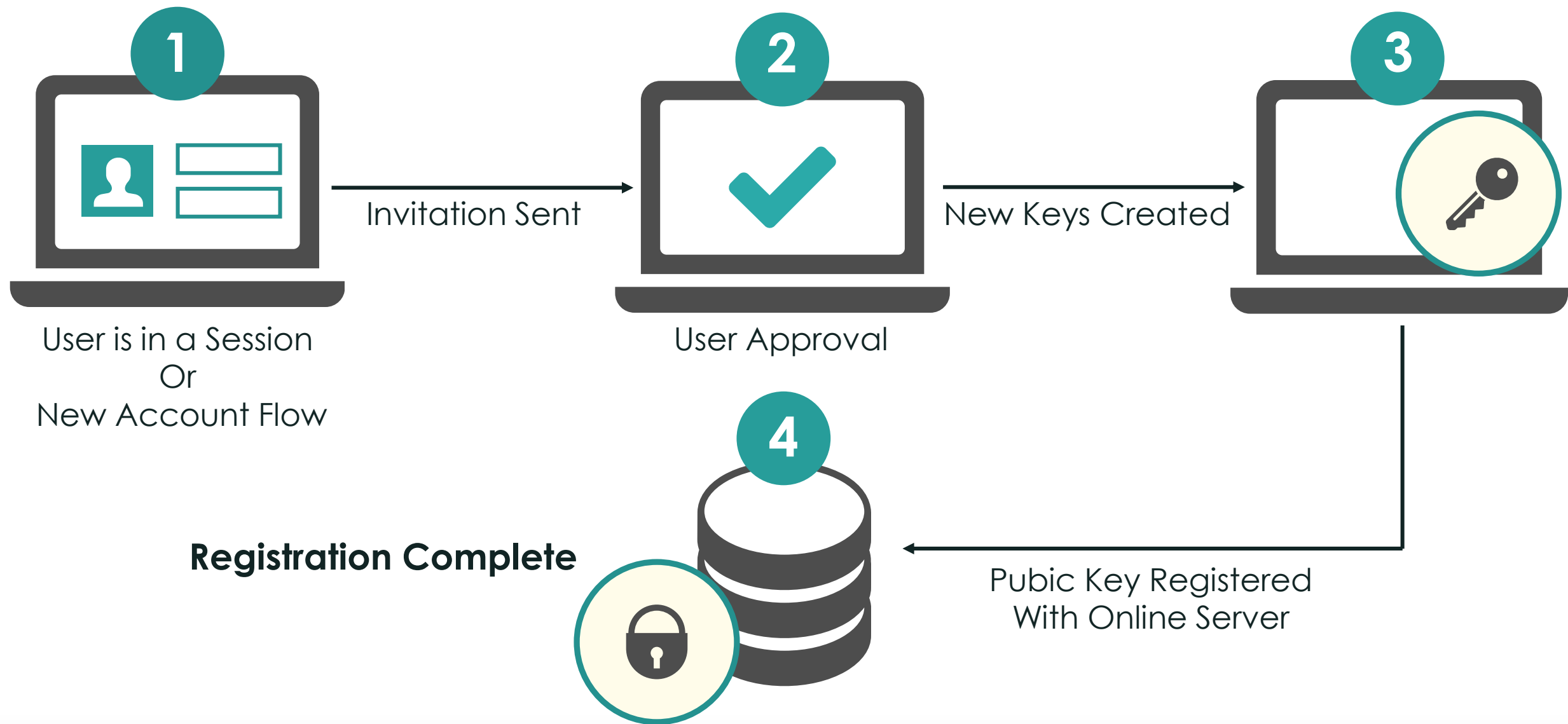
Second Factor Experience

FIDO U2F (Universal Second Factor)

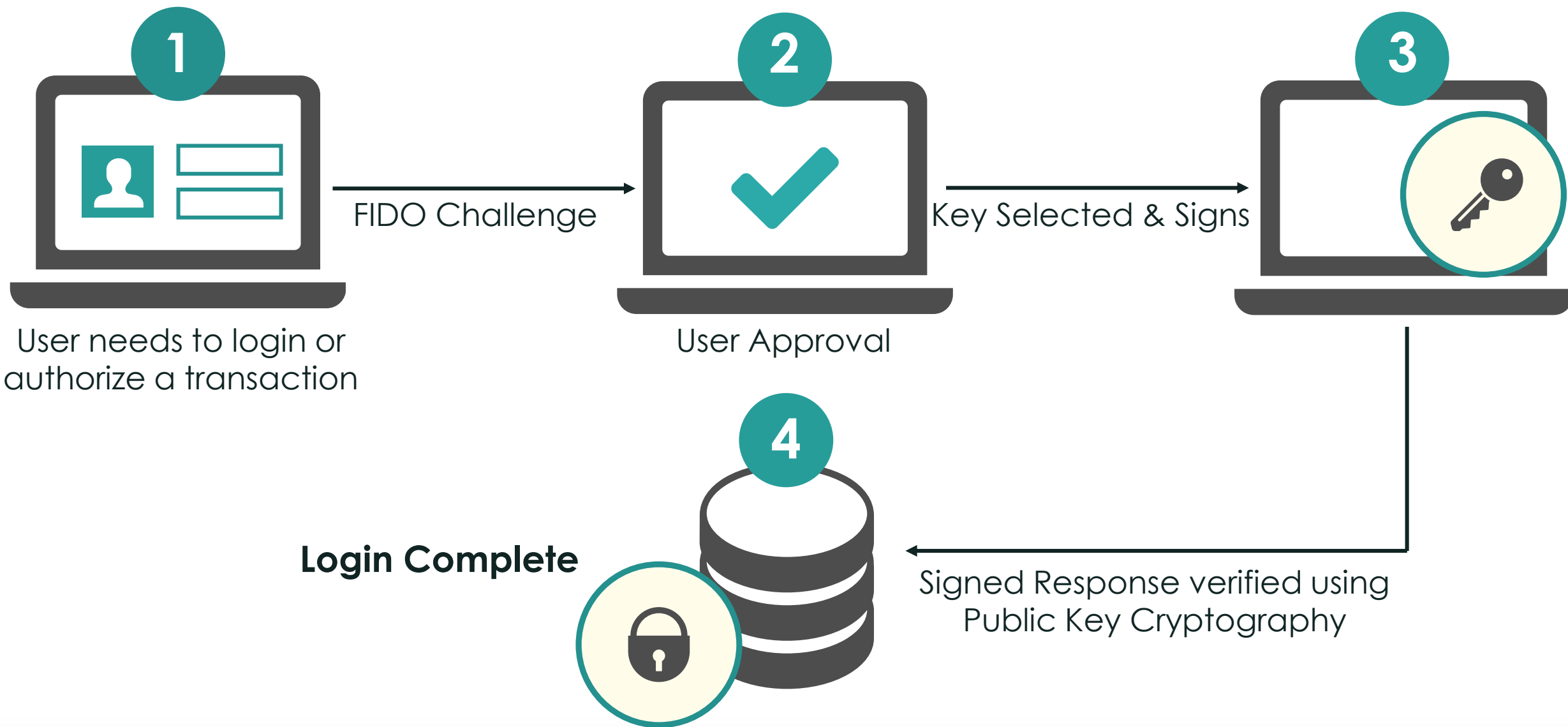


ENABLES MANY AUTHENTICATION OPTIONS | EACH SERVICE PROVIDER HAS ITS OWN UNIQUE SECURITY KEYS

FIDO Registration



FIDO Authentication





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

FIDO was designed from the start to support the Privacy Principles of the European Data Protection Directive



EU Privacy Principle	FIDO Implementation of EU Privacy Principle
Personal data must be processed fairly and lawfully	For a User to access a Relying Party's services through FIDO Authentication, the User must first agree to register with that Relying Party. When the User wishes to access the online service, they must execute the User Verification step, e.g. touching a sensor, entering a passcode, or providing their fingerprint, in order to execute the cryptographic computation. This ensures that malware installed on the User's device is unable to autonomously perform FIDO operations.
Personal data can only be processed for one or more specified lawful purpose(s)	The Personal Data required to access an online service, such as a fingerprint, can only be accessed by the FIDO Authenticator which is part of the User's device. The FIDO Authenticator can only access such data when it is required to perform an Authentication. The FIDO protocol requires a minimum amount of data stored by the Relying Party, for which the user is required to provide consent.
Personal data must be adequate, relevant, and not excessive in relation to the purposes for which it is being used	<p>The data needed to perform an Authentication is collected by the Relying Party when the User registers with it. This data is:</p> <ul style="list-style-type: none">• A public key: This allows the Relying Party to verify that the FIDO Authenticator being used is the one previously registered by the User.• Authenticator Attestation ID (AAID): This is a reference that allows the Relying Party to look-up the characteristics of the used FIDO Authenticator.• Key Handle: An identifier created by a FIDO Authenticator, potentially containing an encrypted private key, to refer to a specific key maintained the FIDO Authenticator.
Personal data must be accurate and up to date	The data used for FIDO Authentication, such as the registered public key, must be accurate since cryptographic verification fails otherwise. If the data becomes corrupted for any reason, the User needs to re-register with the Relying Party. Re-registration changes the registered public key.
Personal data must not be kept for longer than necessary to fulfil the purposes for which it was collected	The User may de-register from a Relying Party at any time. Once de-registration has taken place the Public key held by the Relying Party is of no further use.
Personal data must be kept secure	Allowing users to authenticate using FIDO Authentication provides a greater level of security around accessing personal data than passwords alone. Data required for local User Verification is stored locally on the FIDO Authenticator. FIDO-related data stored at the Relying Party is not confidential by itself. The FIDO Authenticator is required to protect data required for User Verification and FIDO-related data, such as cryptographic keys, against unauthorized access by third parties.
Personal data must be processed in accordance with rights of data subjects	Personal data used to authenticate a User can only be accessed by that User when the User wishes to be authenticated.
Personal data cannot be transferred outside a given geographical area, such as the EEA, without specific circumstances being in place.	Personal data held in a FIDO Authenticator will be protected by the same mechanisms irrespective of the device's location and the device can only leave the EEA if the owner wishes it to do so. The FIDO Server used by the Relying Party does not contain personal data.



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



FIDO Alliance Mission

1

Develop
Specifications

2

Operate
Adoption Programs

3

Pursue Formal
Standardization

Board Members

aetna®


Alibaba Group



ARM®

Bank of America.


 BCcard

CrucialTec 

 Daon



FEITIAN
WE BUILD SECURITY

Google



ING 

intel®

Lenovo™


MasterCard

 Microsoft

Nok Nok
LABS

NTT
docomo

NXP

 oberthur
TECHNOLOGIES
THE M COMPANY

PayPal™

QUALCOMM®

RSA®

SAMSUNG

 Synaptics®


USAA®

 VASCO®

VISA

yubico

Sponsor Members



Government Members



Australian Government
Digital Transformation Office

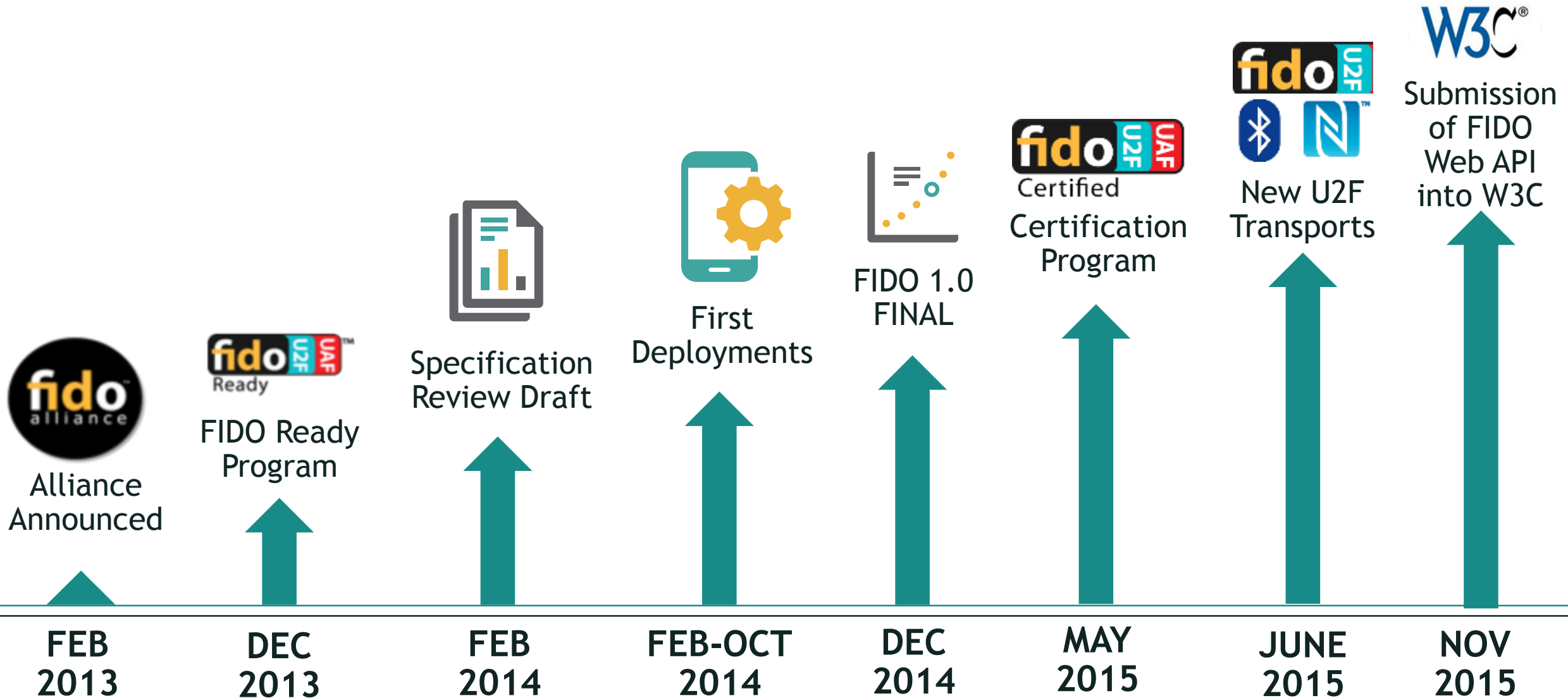


Bundesamt
für Sicherheit in der
Informationstechnik



Note: if you are not listed here, we'd like you to be.

FIDO DEVELOPMENT TIMELINE



FIDO Adoption



A photograph of a server room with rows of black server racks. The racks are filled with various electronic components and cables. The lighting is dim, with some blue and green indicator lights visible on the equipment. The text is overlaid on the left side of the image.

Deployments are enabled by over 250
FIDO® Certified products
available today

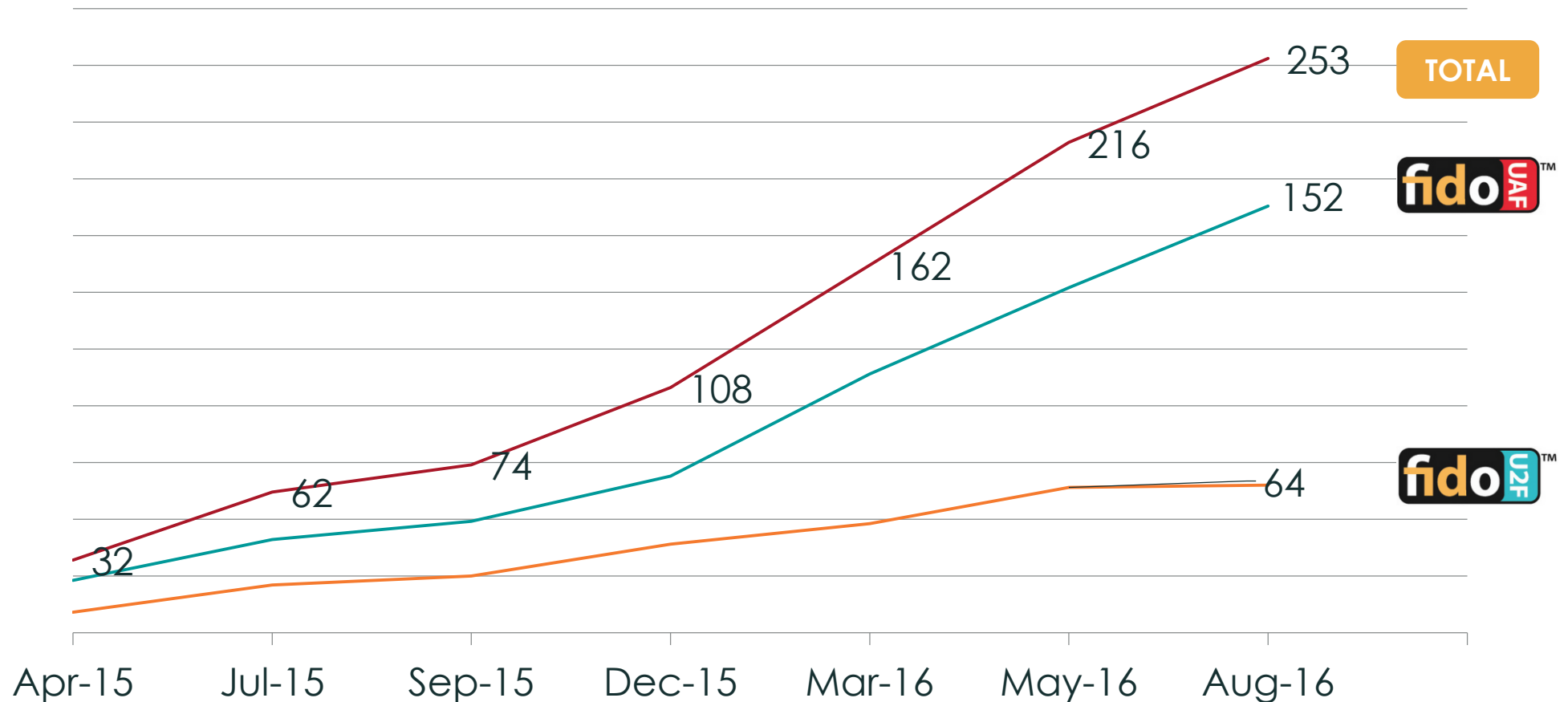
Certification Growth



250+

*FIDO® Certified
products available
today*

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



FIDO in the Android Ecosystem



S5, Mini



Alpha



Note 4, 5



Note Edge



Tab S,
Tab S2



S6,
S6 Edge



S7,
S7 Edge



Vernee
Thor



Aquos Zeta



Xperia Z5



Xperia Z5
Compact



Xperia Z5
Premium



LG Electronics



V10



G5



Arrows
NX



Arrows
Fit



Arrows
Tab



Mate 8



Phab2 Pro
Phab2 Plus



Z2, Z2 Pro

FIDO in the Apple Ecosystem



Supported iOS Fingerprint Devices

Bank of America



NTT
docomo

ebay



iPhone SE



iPhone & iPhone+



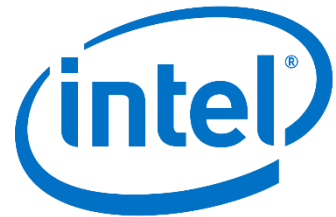
iPad Air, Mini



iPad Pro

FIDO in the Windows and Web Ecosystems

Windows Platforms



Web



mozilla





HOW FIDO CAN HELP GOVERNMENTS

How FIDO Can Help Governments



- **Support for “BYOC” (Bring Your Own Credential)**
 - Take advantage of the growing ecosystem of FIDO solutions and standards
 - No need to create passwords for digital government services
 - No requirement to issue a separate token or app for MFA
- **Better Security, Privacy + Interoperability**
- **Better Customer Experiences - simpler and safer**
- **Reduced Cost for the Government Enterprise**

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.

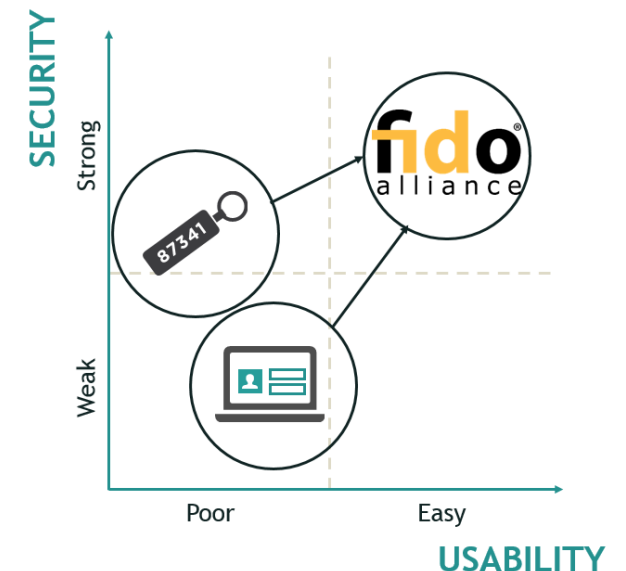
1. Recognize that two-factor authentication no longer brings higher burdens or costs



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

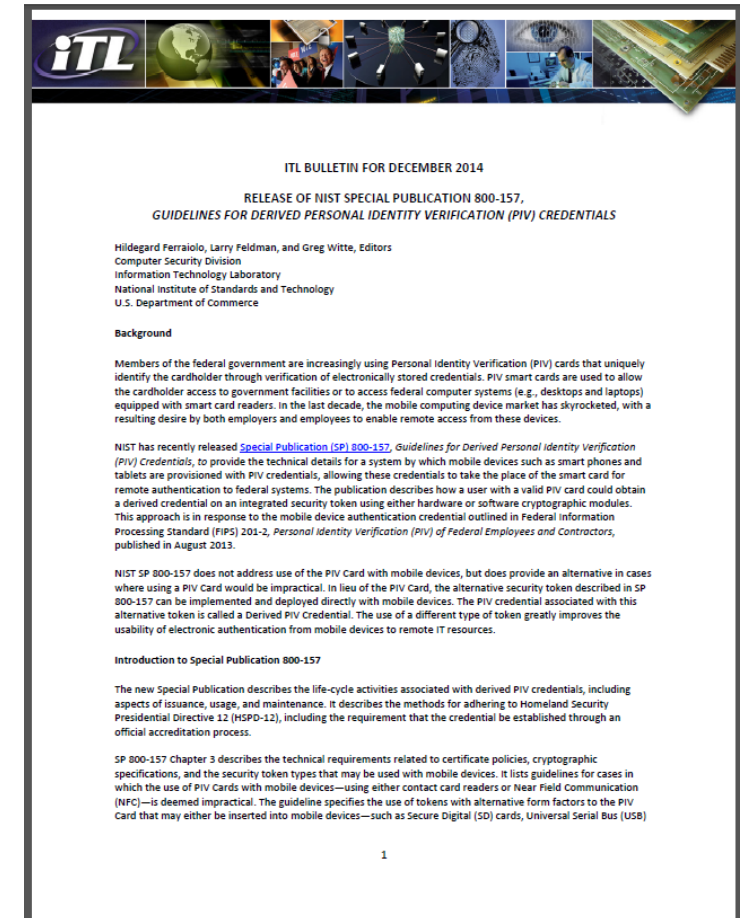
–US Department of Health and Human Services 2015 Edition Health Information Technology (Health IT) Certification Criteria, October, 2015

- 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 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 AuthN 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 AuthN, make sure it is the “right” strong AuthN

The market is in the midst of a burst of innovation around authentication technology - some solutions are better than others. Don't build rules and systems 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
- Designed to support Privacy Principles of the European Data Protection Directive
- 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

Come learn more: FIDO in Vancouver!



- FIDO Seminar - Monday, January 23
- FIDO Plenary - January 24-26



THANK YOU!

QUESTIONS?

jeremy.grant@chertoffgroup.com | info@fidoalliance.org