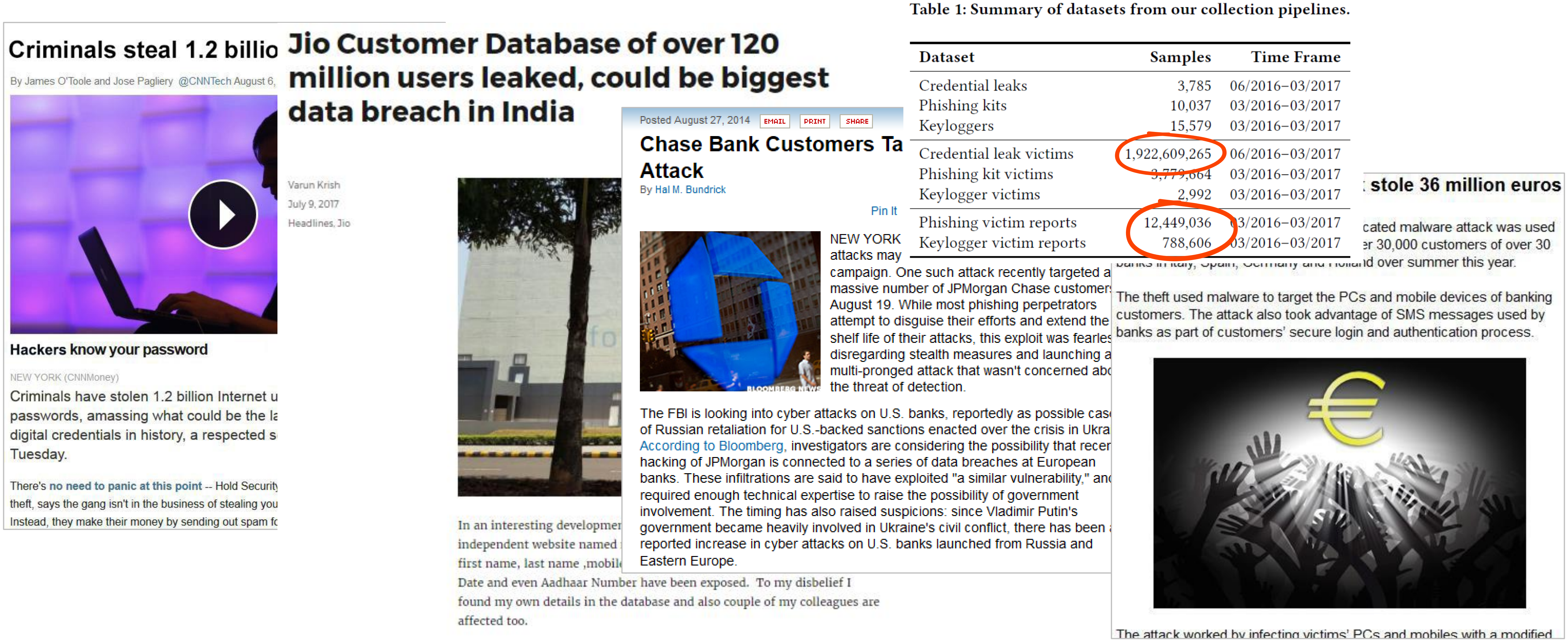
FIDO TECHNICAL OVERVIEW

REVISED JUNE 29TH 2018

HOW SECURE IS AUTHENTICATION?



Criminals steal 1.2 billio

By James O'Toole and Jose Pagliery @CNNTech August 6,

Hackers know your password

NEW YORK (CNNMoney)

Criminals have stolen 1.2 billion Internet u passwords, amassing what could be the la digital credentials in history, a respected s Tuesday.

There's no need to panic at this point -- Hold Securit theft, says the gang isn't in the business of stealing you Instead, they make their money by sending out spam fc

Jio Customer Database of over 120 million users leaked, could be biggest data breach in India

Varun Krish
July 9, 2017
Headlines, Jio

In an interesting developmen independent website named first name, last name ,mobil Date and even Aadhaar Number have been exposed. To my disbelief I found my own details in the database and also couple of my colleagues are affected too.

Posted August 27, 2014 EMAIL PRINT SHARE

Chase Bank Customers Ta Attack

By Hal M. Bundrick

Pin It

NEW YORK attacks may campaign. One such attack recently targeted a massive number of JPMorgan Chase customer August 19. While most phishing perpetrators attempt to disguise their efforts and extend the shelf life of their attacks, this exploit was fearles disregarding stealth measures and launching a multi-pronged attack that wasn't concerned abo the threat of detection.

The FBI is looking into cyber attacks on U.S. banks, reportedly as possible cas of Russian retaliation for U.S.-backed sanctions enacted over the crisis in Ukra According to Bloomberg, investigators are considering the possibility that rece hacking of JPMorgan is connected to a series of data breaches at European banks. These infiltrations are said to have exploited "a similar vulnerability," an 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 reported increase in cyber attacks on U.S. banks launched from Russia and Eastern Europe.

Table 1: Summary of datasets from our collection pipelines.

Dataset	Samples	Time Frame
Credential leaks	3,785	06/2016–03/2017
Phishing kits	10,037	03/2016–03/2017
Keyloggers	15,579	03/2016–03/2017
Credential leak victims	1,922,609,265	06/2016–03/2017
Phishing kit victims	3,779,664	03/2016–03/2017
Keylogger victims	2,992	03/2016–03/2017
Phishing victim reports	12,449,036	03/2016–03/2017
Keylogger victim reports	788,606	03/2016–03/2017

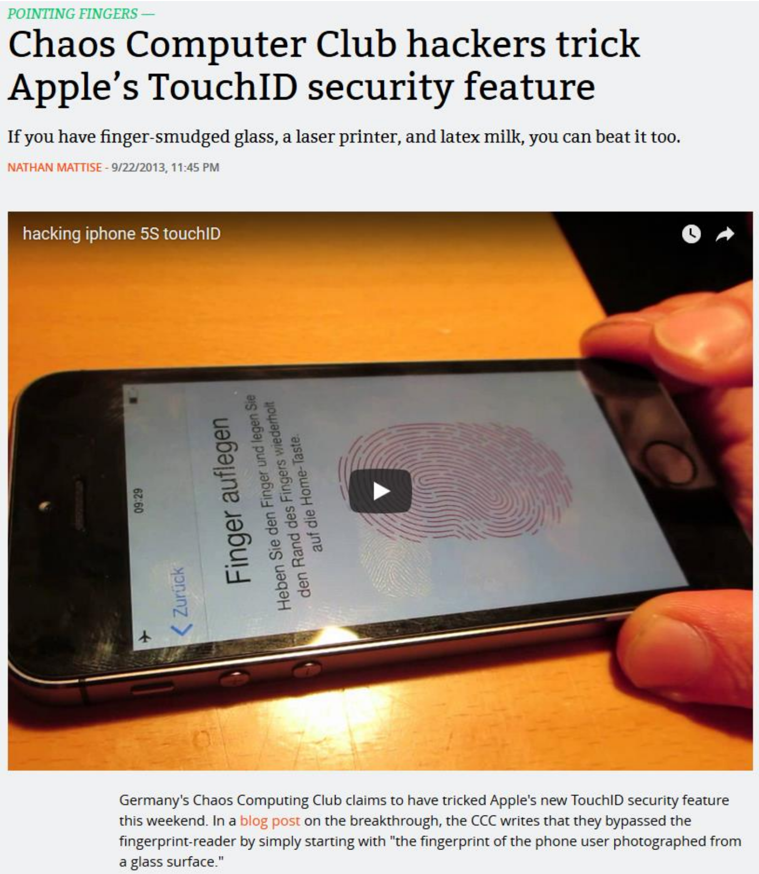
stole 36 million euros

cated malware attack was used er 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

HOW SECURE IS AUTHENTICATION?


hacking iphone 5S touchID
09:29
Finger auflegen
Heben Sie den Finger und legen Sie den Rand des Fingers wiederholt auf die Home-Taste.
Zurück

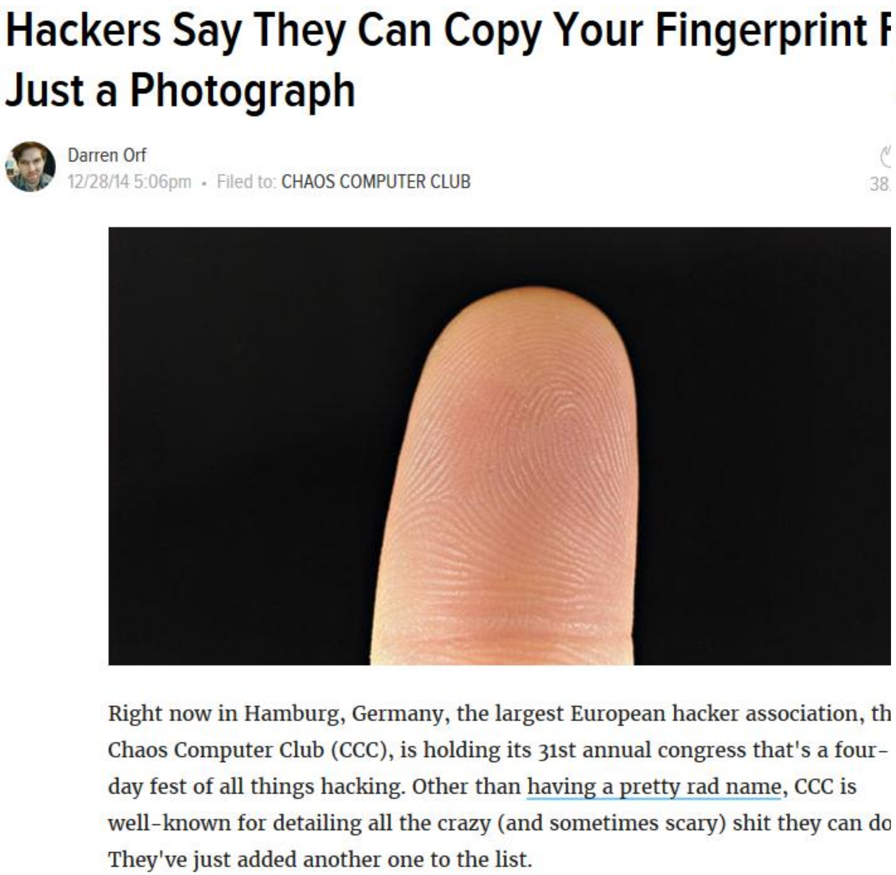
POINTING FINGERS —

Chaos Computer Club hackers trick Apple's TouchID security feature

If you have finger-smudged glass, a laser printer, and latex milk, you can beat it too.

NATHAN MATTISE - 9/22/2013, 11:45 PM

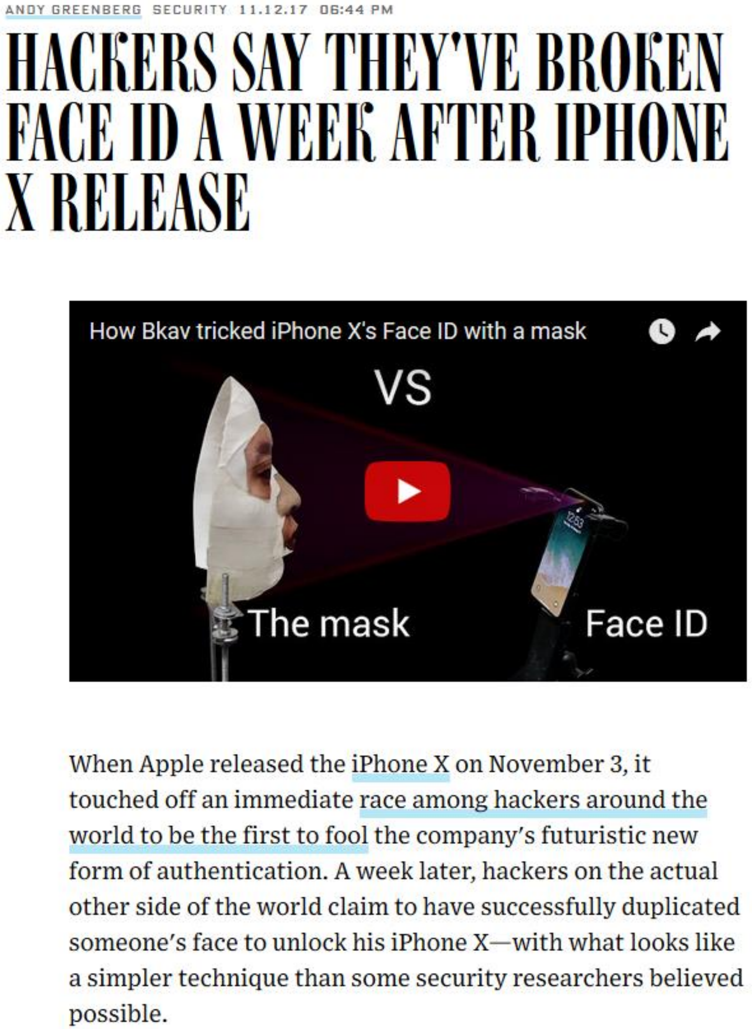
Germany's Chaos Computing Club claims to have tricked Apple's new TouchID security feature this weekend. In a blog post on the breakthrough, the CCC writes that they bypassed the fingerprint-reader by simply starting with "the fingerprint of the phone user photographed from a glass surface."



Hackers Say They Can Copy Your Fingerprint F Just a Photograph

Darren Orf
12/28/14 5:06pm · Filed to: CHAOS COMPUTER CLUB
38

Right now in Hamburg, Germany, the largest European hacker association, th Chaos Computer Club (CCC), is holding its 31st annual congress that's a four-day fest of all things hacking. Other than having a pretty rad name, CCC is well-known for detailing all the crazy (and sometimes scary) shit they can do They've just added another one to the list.

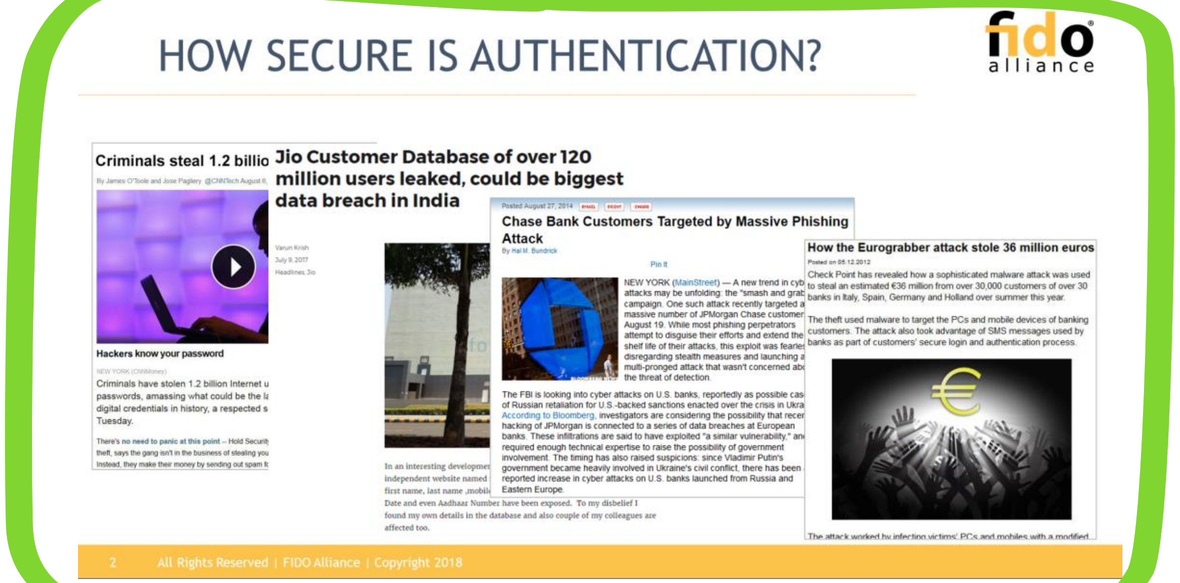


ANDY GREENBERG SECURITY 11.12.17 06:44 PM

HACKERS SAY THEY'VE BROKEN FACE ID A WEEK AFTER IPHONE X RELEASE

When Apple released the iPhone X on November 3, it touched off an immediate race among hackers around the world to be the first to fool the company's futuristic new form of authentication. A week later, hackers on the actual other side of the world claim to have successfully duplicated someone's face to unlock his iPhone X—with what looks like a simpler technique than some security researchers believed possible.

HOW SECURE IS AUTHENTICATION?



HOW SECURE IS AUTHENTICATION?

Criminals steal 1.2 billio

By James O'Toole and Jose Pagliery @CNNTech August 6,

Hackers know your password

NEW YORK (CNNMoney)

Criminals have stolen 1.2 billion Internet u passwords, amassing what could be the l digital credentials in history, a respected s Tuesday.

There's no need to panic at this point -- Hold Securit theft, says the gang isn't in the business of stealing you Instead, they make their money by sending out spam f

Jio Customer Database of over 120 million users leaked, could be biggest data breach in India

Varun Krish
July 9, 2017
Headlines, Jio

In an interesting developme independent website named first name, last name ,mobil Date and even Aadhaar Number have been exposed. To my disbelief I found my own details in the database and also couple of my colleagues are affected too.

Posted August 27, 2014

Chase Bank Customers Targeted by Massive Phishing Attack

By Hal M. Bundrick

Pin It

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

The FBI is looking into cyber attacks on U.S. banks, reportedly as possible cas of Russian retaliation for U.S.-backed sanctions enacted over the crisis in Ukra According to Bloomberg, investigators are considering the possibility that rece hacking of JPMorgan is connected to a series of data breaches at European banks. These infiltrations are said to have exploited "a similar vulnerability," an 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 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

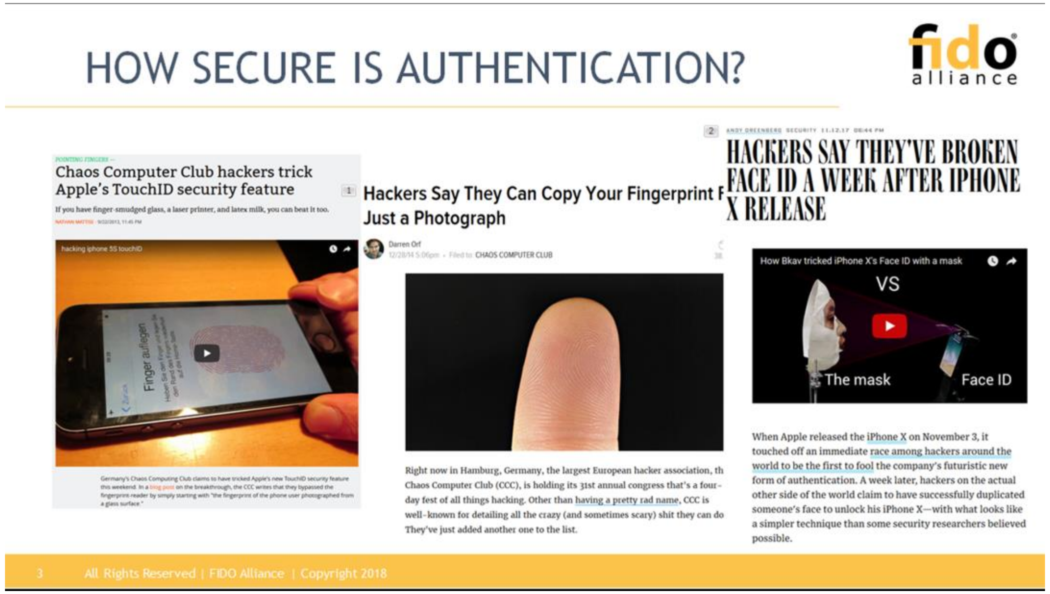
Check Point has revealed how a sophisticated malware attack was used to steal an estimated €36 million from over 30,000 customers of over 30 banks in Italy, Spain, Germany and Holland over summer this year.

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

2 All Rights Reserved | FIDO Alliance | Copyright 2018

Scalable Attacks



HOW SECURE IS AUTHENTICATION?

POINTING FINGERS —

Chaos Computer Club hackers trick Apple's TouchID security feature

If you have finger-smudged glass, a laser printer, and latex milk, you can beat it too.

NATHAN MATTISE - 9/22/2013, 11:45 PM

Germany's Chaos Computing Club claims to have tricked Apple's new TouchID security feature this weekend. In a blog post on the breakthrough, the CCC writes that they bypassed the fingerprint-reader by simply starting with "the fingerprint of the phone user photographed from a glass surface."

1

Hackers Say They Can Copy Your Fingerprint F Just a Photograph

Darren Orf
12/28/14 5:06pm · Filed to: CHAOS COMPUTER CLUB

Right now in Hamburg, Germany, the largest European hacker association, th Chaos Computer Club (CCC), is holding its 31st annual congress that's a four-day fest of all things hacking. Other than having a pretty rad name, CCC is well-known for detailing all the crazy (and sometimes scary) shit they can do They've just added another one to the list.

2

ANDY GREENBERG SECURITY 11.12.17 08:44 PM

HACKERS SAY THEY'VE BROKEN FACE ID A WEEK AFTER IPHONE X RELEASE

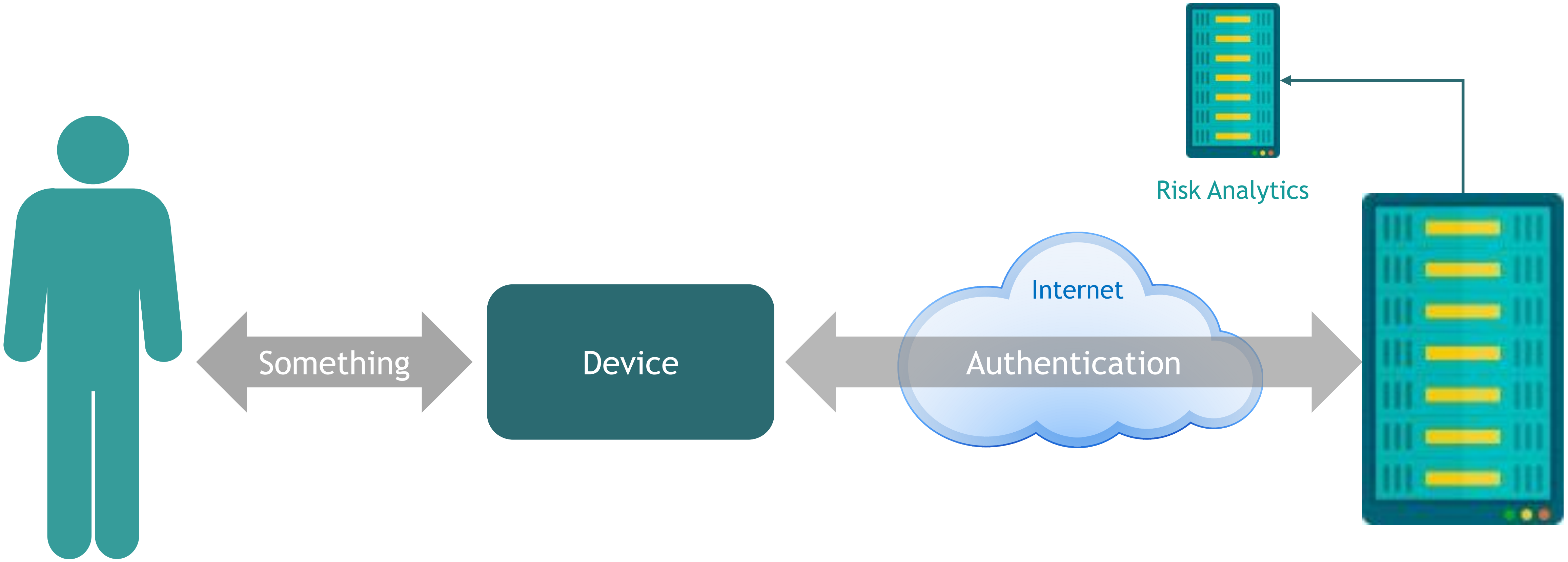
When Apple released the iPhone X on November 3, it touched off an immediate race among hackers around the world to be the first to fool the company's futuristic new form of authentication. A week later, hackers on the actual other side of the world claim to have successfully duplicated someone's face to unlock his iPhone X—with what looks like a simpler technique than some security researchers believed possible.

3 All Rights Reserved | FIDO Alliance | Copyright 2018

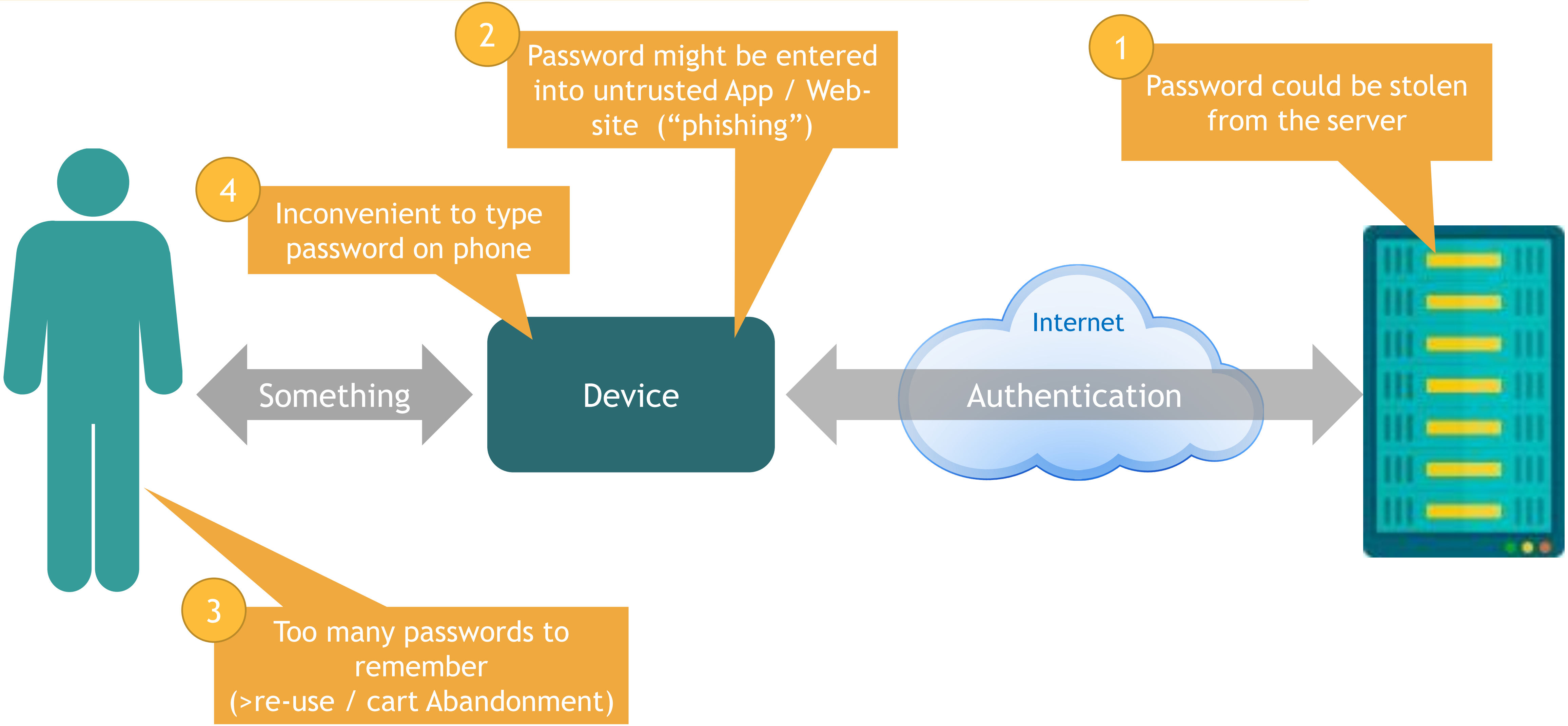
Attacks require physical action → not scalable

Things are never 100% secure, so focus on adequate security.
Focus on the scalable attacks first.

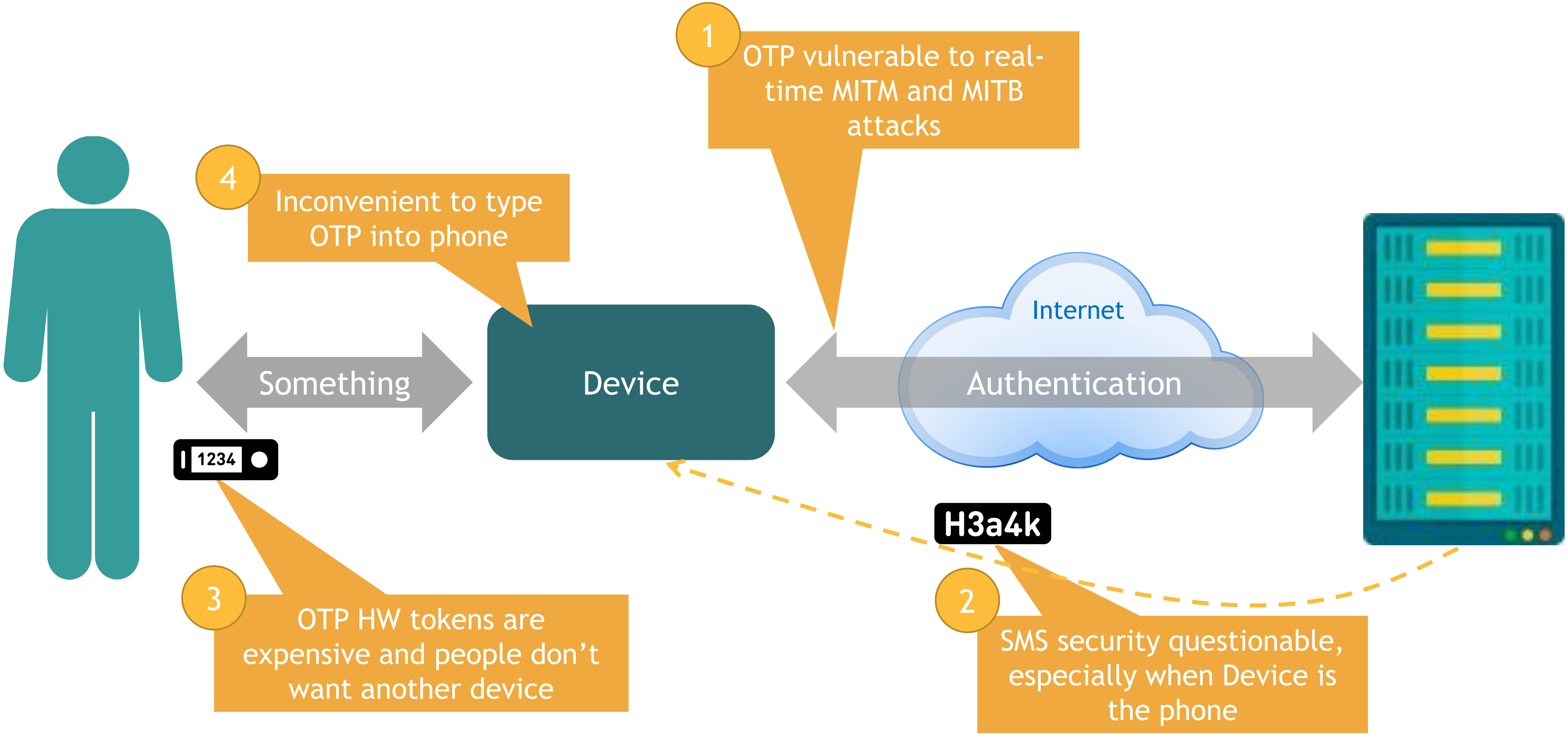
CLOUD AUTHENTICATION



PASSWORD ISSUES


2
Password might be entered into untrusted App / Website ("phishing")
1
Password could be stolen from the server
4
Inconvenient to type password on phone
Something
Device
Internet
Authentication
3
Too many passwords to remember
(>re-use / cart Abandonment)

OTP ISSUES



1 OTP vulnerable to real-time MITM and MITB attacks

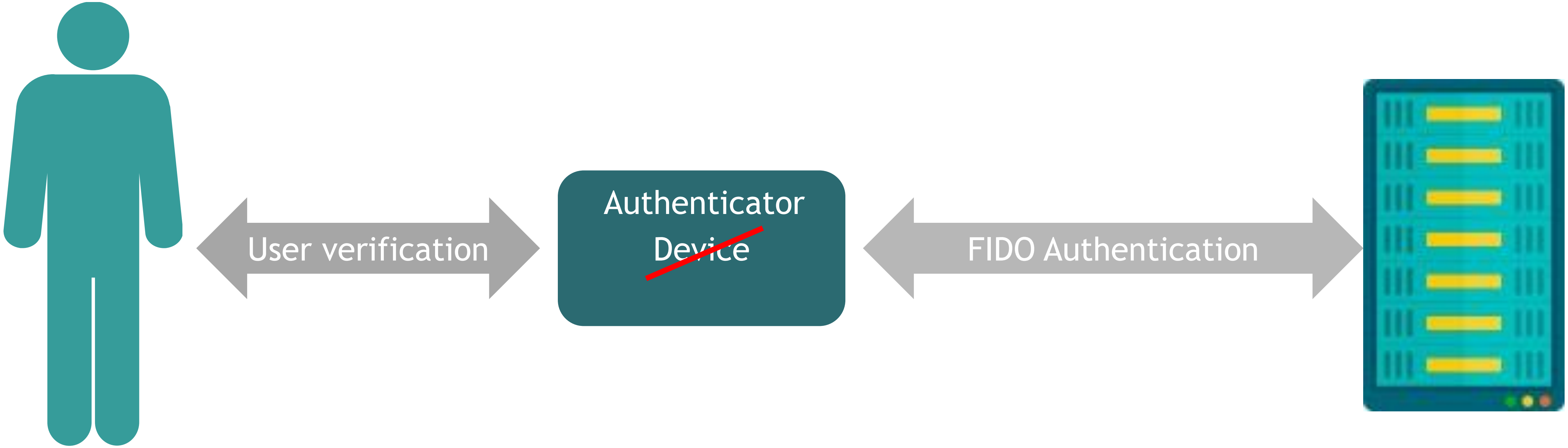
2 SMS security questionable, especially when Device is the phone

3 OTP HW tokens are expensive and people don’t want another device

4 Inconvenient to type OTP into phone

HOW DOES FIDO WORK?

HOW DOES FIDO WORK?

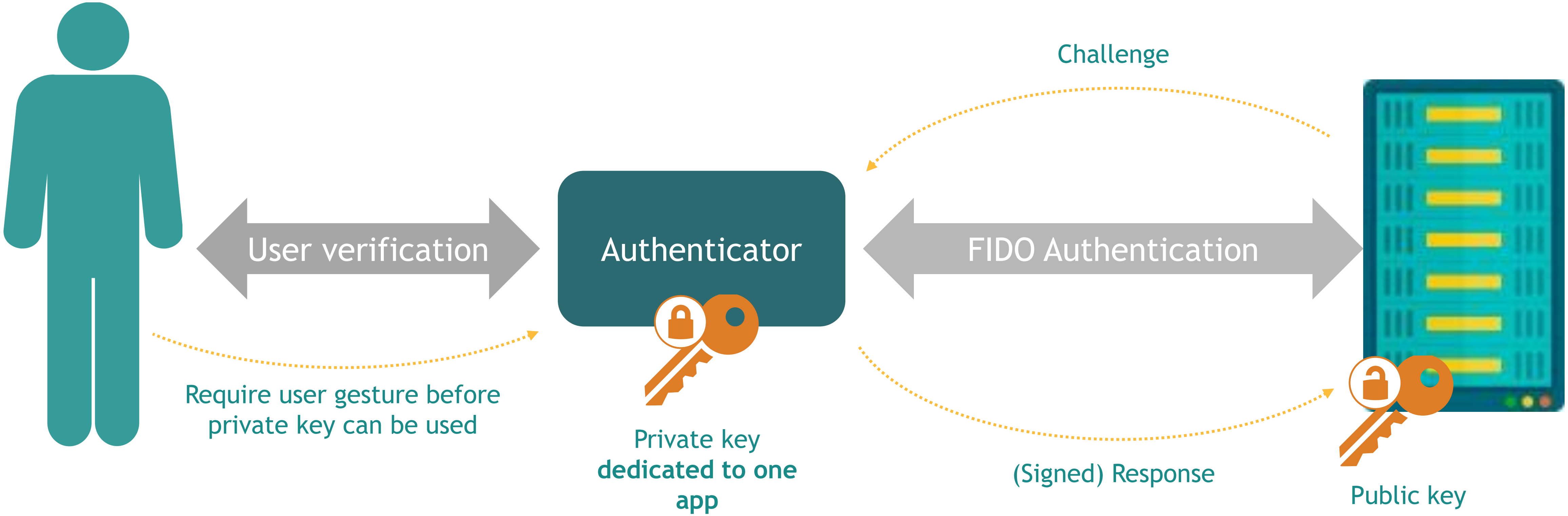


User verification

Authenticator ~~Device~~

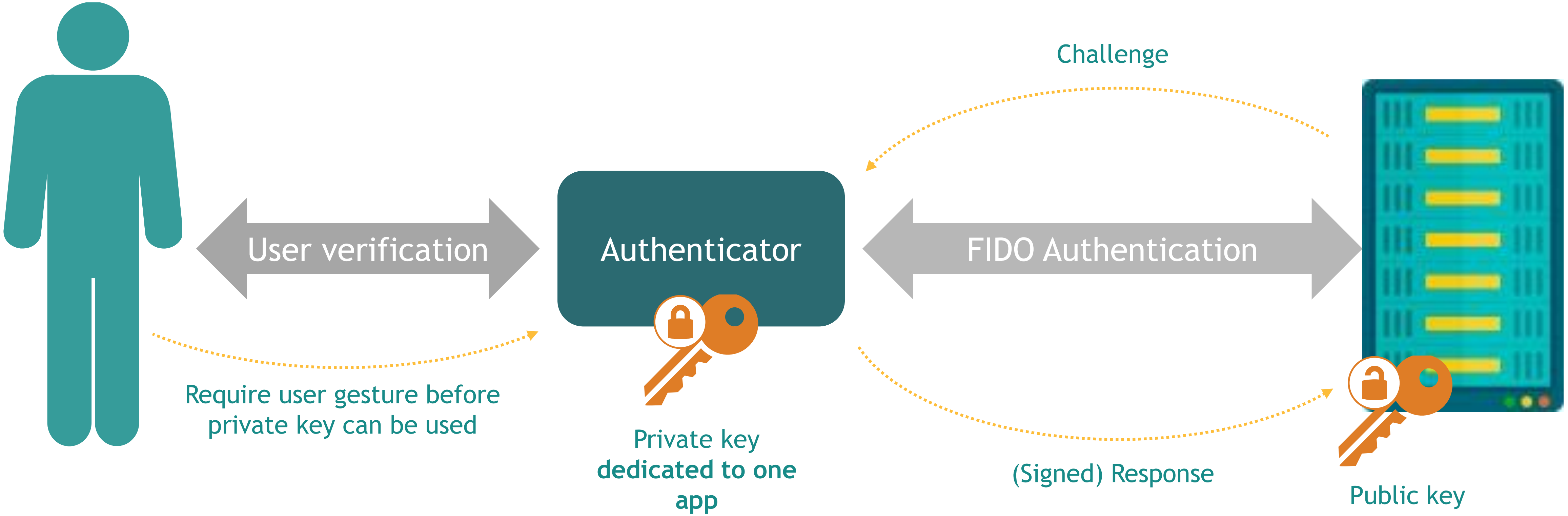
FIDO Authentication

HOW DOES FIDO WORK?

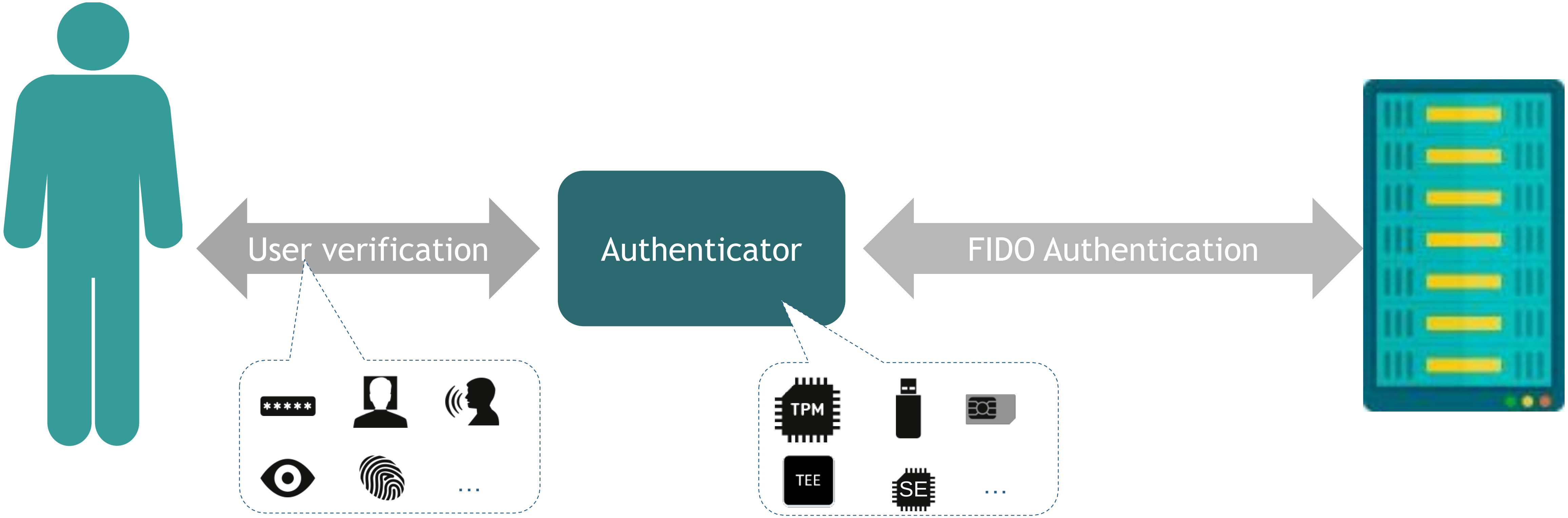


Challenge
User verification
Authenticator
FIDO Authentication
Require user gesture before private key can be used
Private key **dedicated to one app**
(Signed) Response
Public key

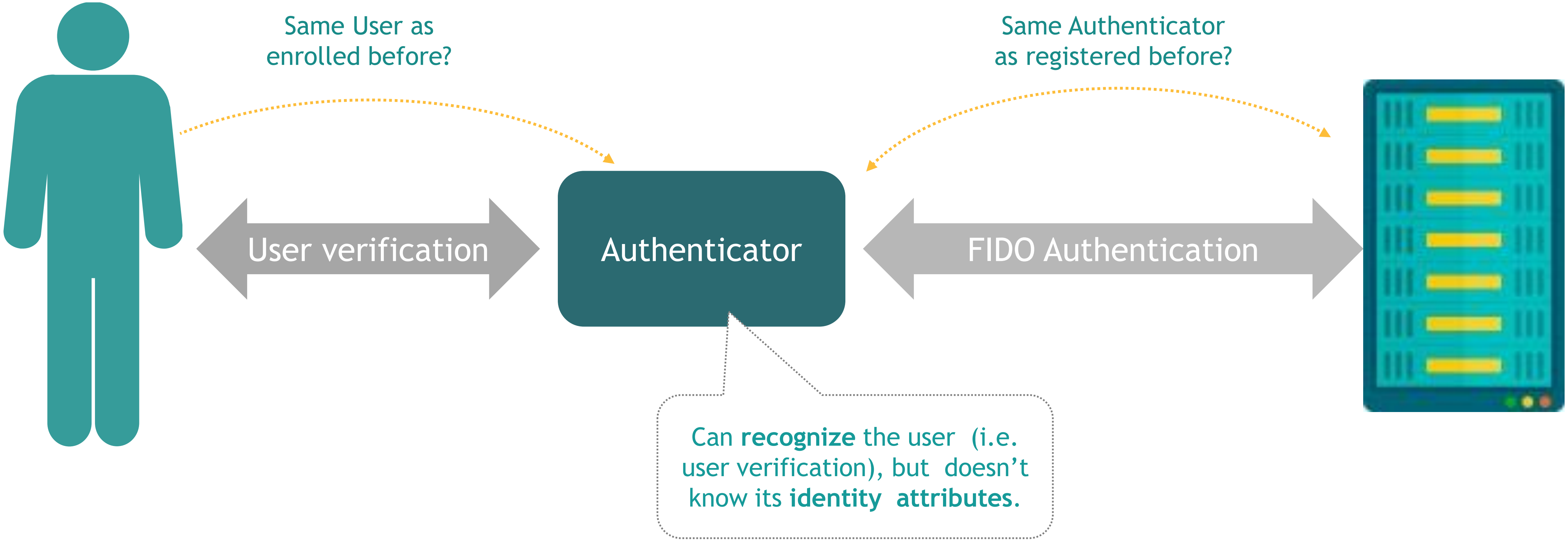
HOW DOES FIDO WORK?


Challenge
User verification
Authenticator
FIDO Authentication
Require user gesture before private key can be used
Private key **dedicated to one app**
(Signed) Response
Public key

HOW DOES FIDO WORK?



HOW DOES FIDO WORK?



Same User as enrolled before?

Same Authenticator as registered before?

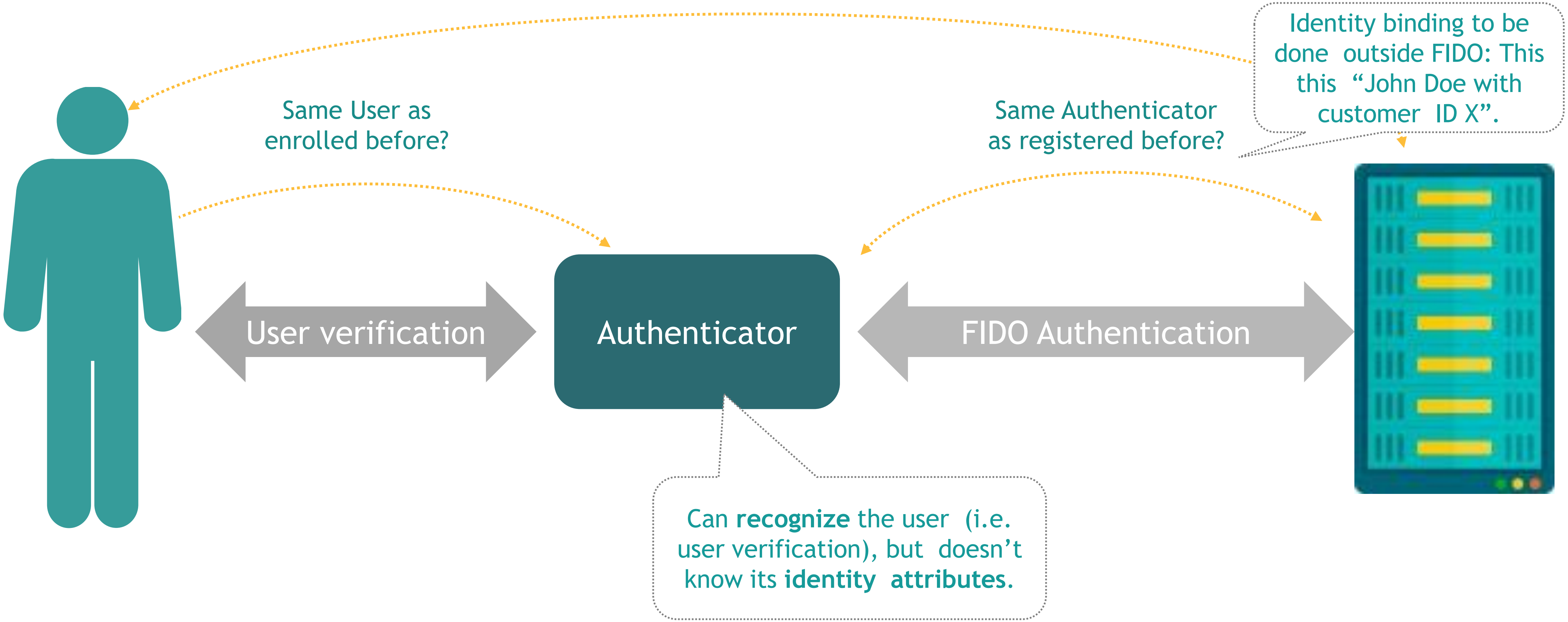
User verification

Authenticator

FIDO Authentication

Can **recognize** the user (i.e. user verification), but doesn’t know its **identity attributes**.

HOW DOES FIDO WORK?



Same User as enrolled before?

Same Authenticator as registered before?

Identity binding to be done outside FIDO: This this "John Doe with customer ID X".

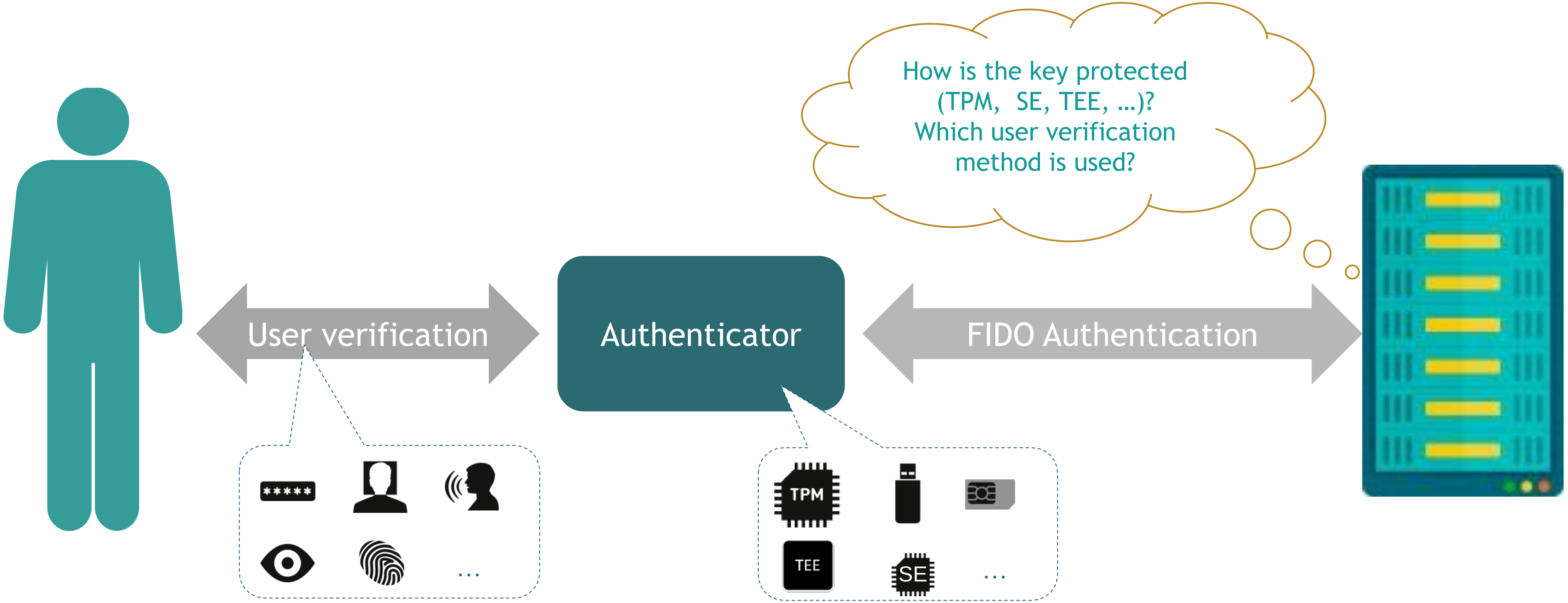
User verification

Authenticator

FIDO Authentication

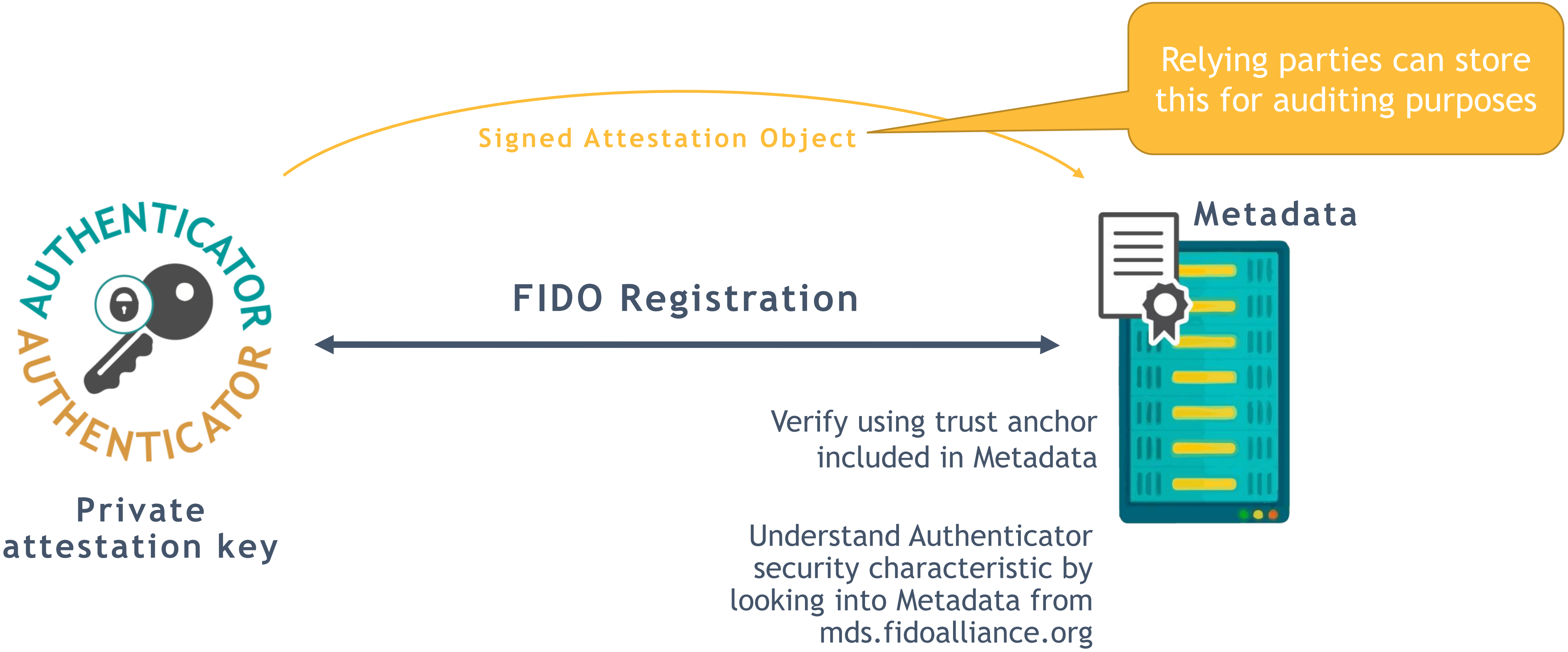
Can **recognize** the user (i.e. user verification), but doesn't know its **identity attributes**.

HOW DOES FIDO WORK?



How is the key protected (TPM, SE, TEE, …)? Which user verification method is used?
User verification
Authenticator
FIDO Authentication
*****
…
TPM
TEE
SE
…

ATTESTATION + METADATA



Relying parties can store this for auditing purposes

Signed Attestation Object

Metadata

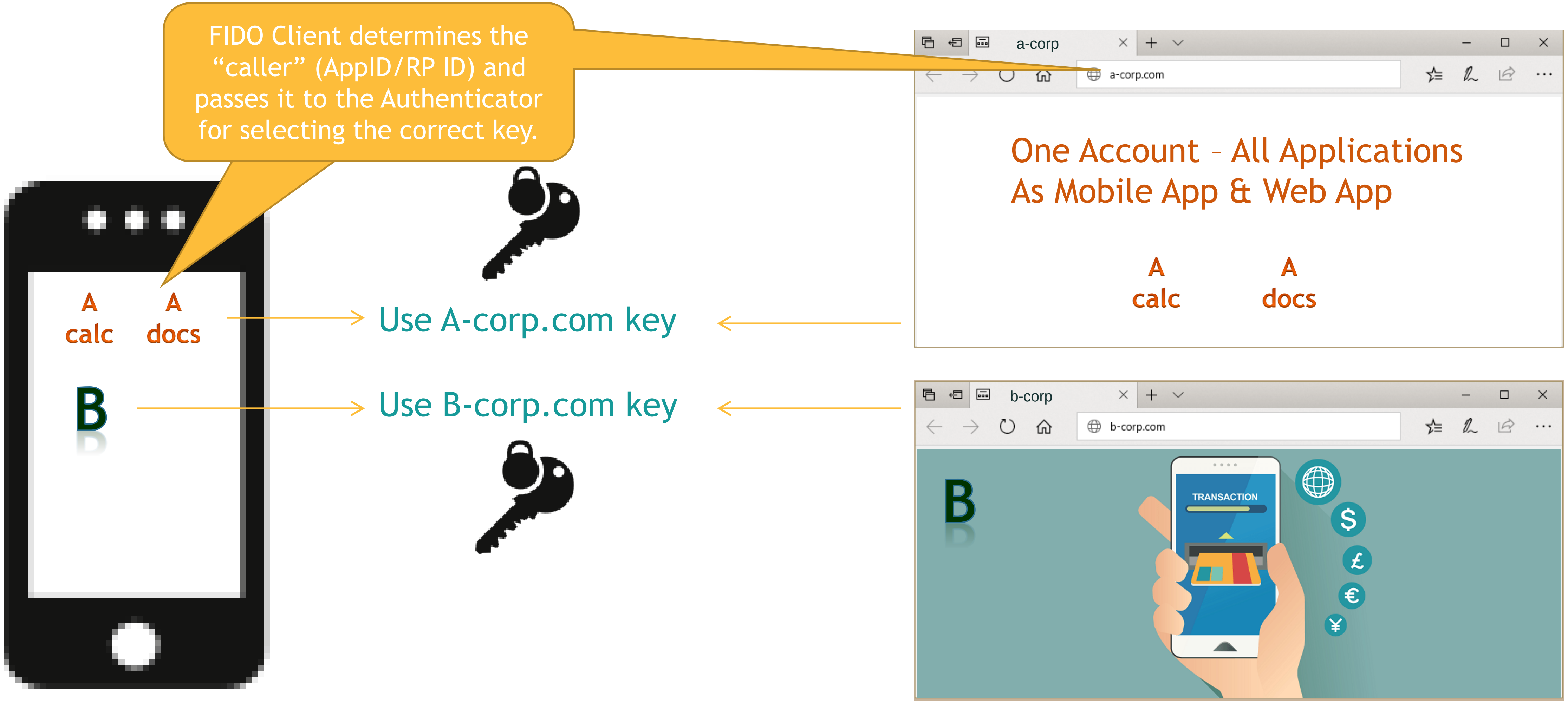
FIDO Registration

Private attestation key

Verify using trust anchor included in Metadata

Understand Authenticator security characteristic by looking into Metadata from mds.fidoalliance.org

BINDING KEYS TO RELYING PARTIES



FIDO Client determines the “caller” (AppID/RP ID) and passes it to the Authenticator for selecting the correct key.

A calc

A docs

B

Use A-corp.com key

Use B-corp.com key

a-corp

a-corp.com

One Account – All Applications
As Mobile App & Web App

A calc

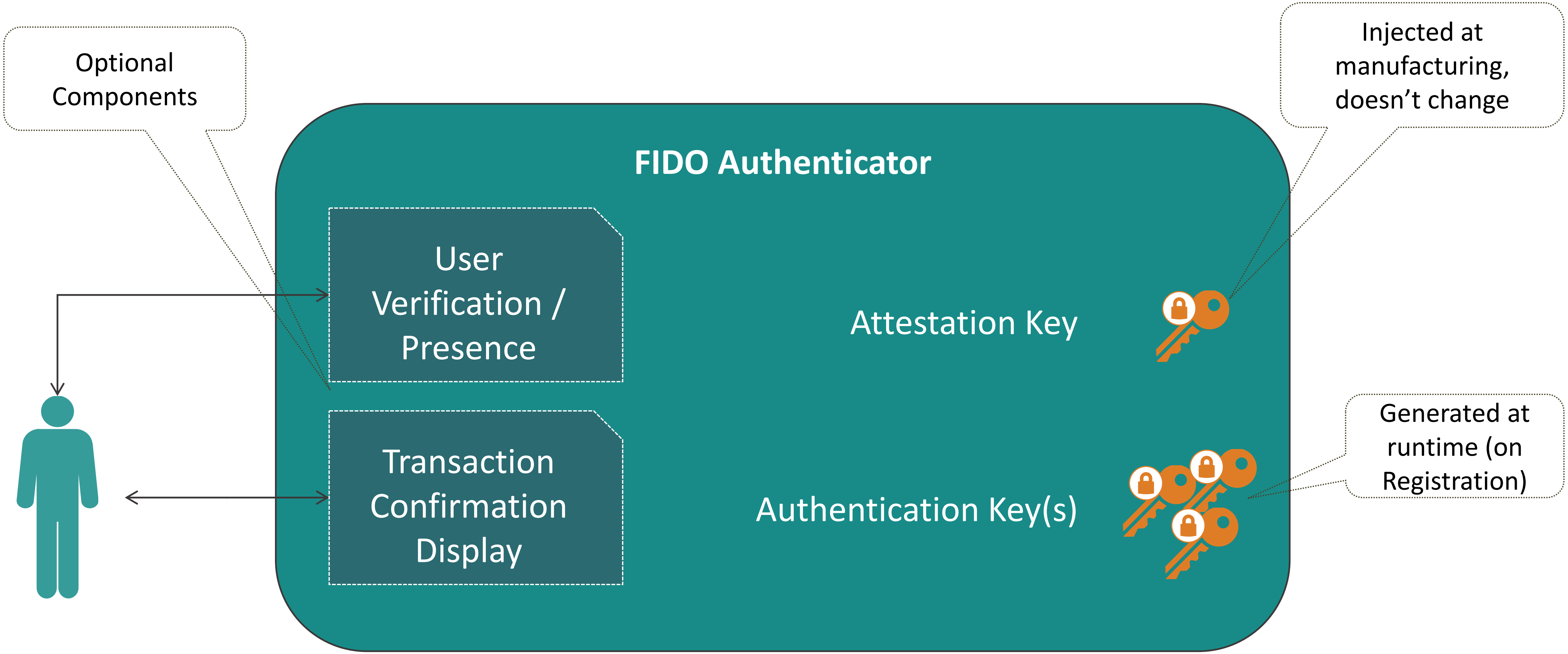
A docs

b-corp

b-corp.com

B

FIDO AUTHENTICATOR CONCEPT

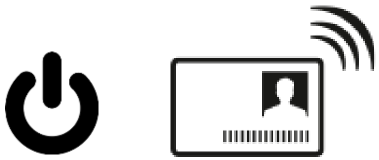

Optional Components
Injected at manufacturing, doesn't change
FIDO Authenticator
User Verification / Presence
Attestation Key
Transaction Confirmation Display
Authentication Key(s)
Generated at runtime (on Registration)

FIDO AUTHENTICATORS

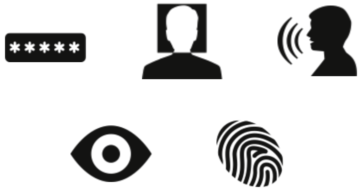
We see "Bound" Authenticators,
i.e. authenticators that are an
integral part of a smartphone or laptop.

We see "Roaming" Authenticators,
i.e. authenticators that can be connected to
different smartphones or laptops using CTAP.

In both categories you find support for different modalities

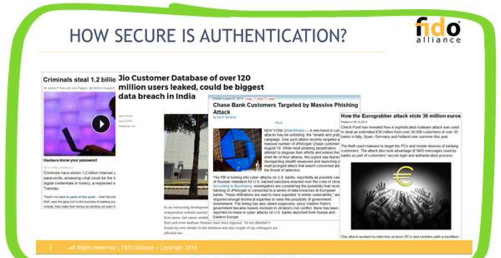


Verify User Presence



Verify User

FIDO AUTHENTICATORS


HOW SECURE IS AUTHENTICATION?
Criminals steal 1.2 billio
Jio Customer Database of over 120 million users leaked, could be biggest data breach in India
Chase Bank Customers Targeted by Massive Phishing Attack
How the Eurograbber attack stole 36 million euros
Hackers know your password

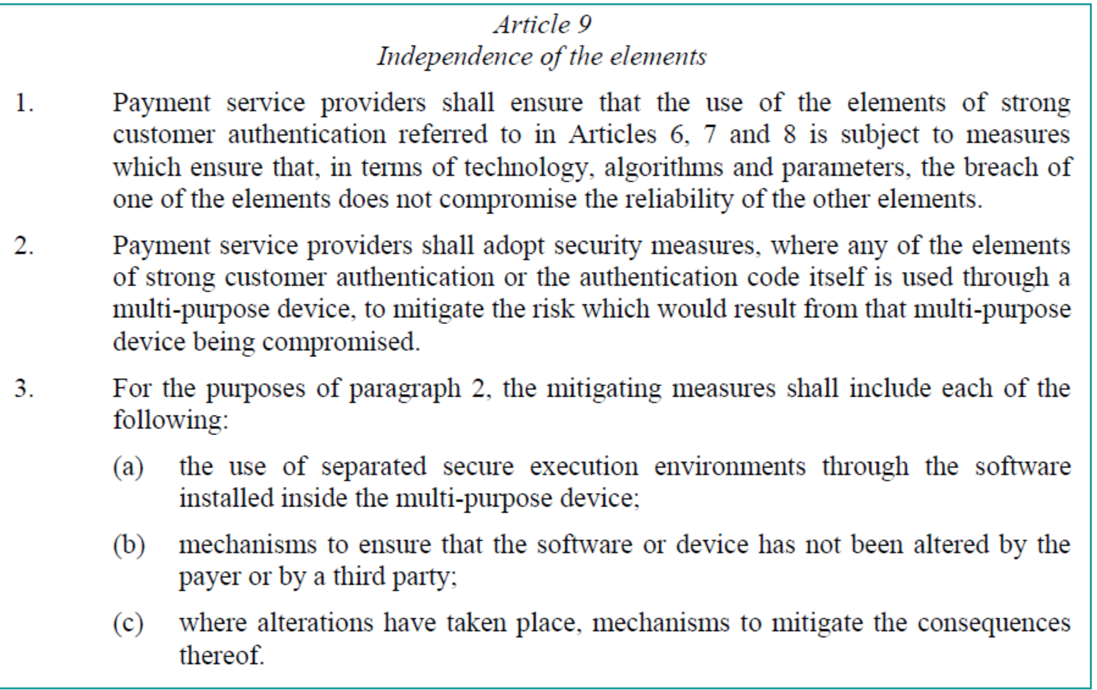
Scalable Attacks

HOW SECURE IS AUTHENTICATION?
Chaos Computer Club hackers trick Apple's TouchID security feature
Hackers Say They Can Copy Your Fingerprint F Just a Photograph
HACKERS SAY THEY'VE BROKEN FACE ID A WEEK AFTER IPHONE X RELEASE
VS
The mask
Face ID

Attacks require physical action → not scalable

FIDO has an Authenticator Certification program. Different certification levels address the needs to protect against scalable and physical attacks.

Things are never 100% secure, so focus on adequate security.
Focus on the scalable attacks first.



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 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.

2. Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.

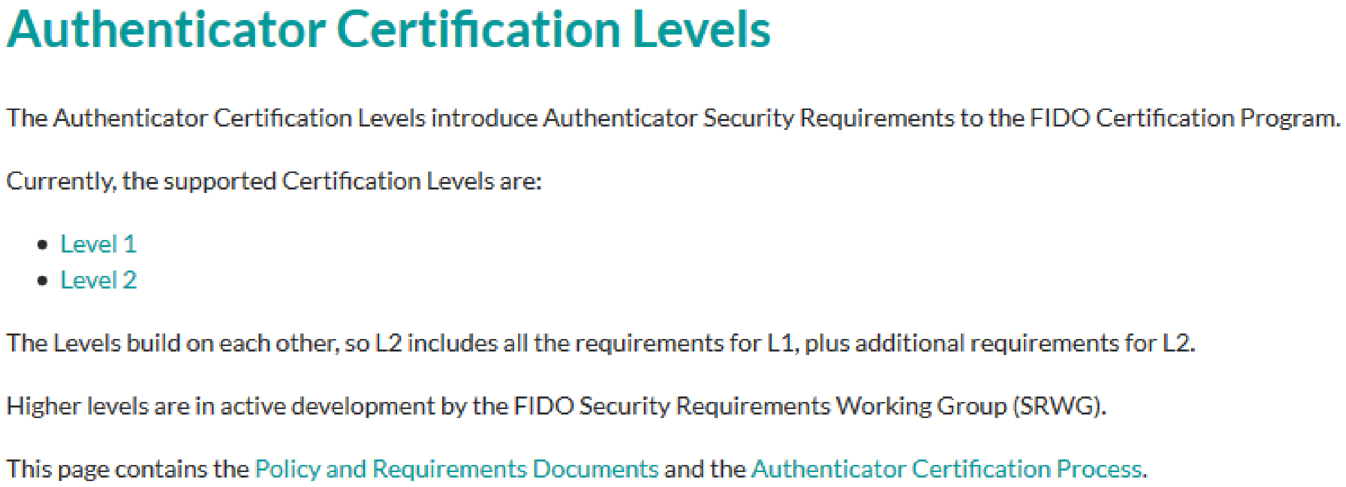
3. For the purposes of paragraph 2, the mitigating measures shall include each of the following:

   (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;

   (c) where alterations have taken place, mechanisms to mitigate the consequences thereof.

See https://fidoalliance.org/certification/authenticator-certification-levels/



Authenticator Certification Levels

The Authenticator Certification Levels introduce Authenticator Security Requirements to the FIDO Certification Program.

Currently, the supported Certification Levels are:

- Level 1
- Level 2

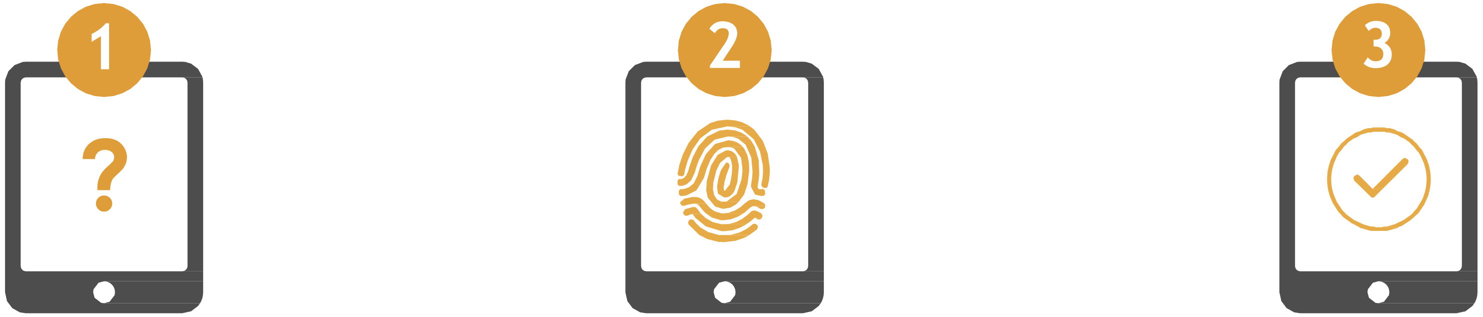
The Levels build on each other, so L2 includes all the requirements for L1, plus additional requirements for L2.

Higher levels are in active development by the FIDO Security Requirements Working Group (SRWG).

This page contains the Policy and Requirements Documents and the Authenticator Certification Process.

FIDO USE CASES

Passwordless Experience

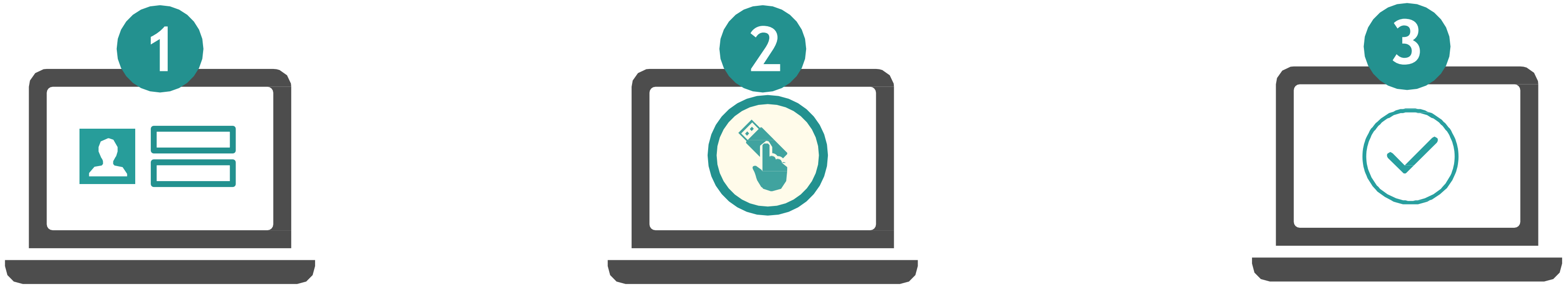


Authentication Challenge

Biometric User Verification*

Authenticated Online

Second Factor Experience



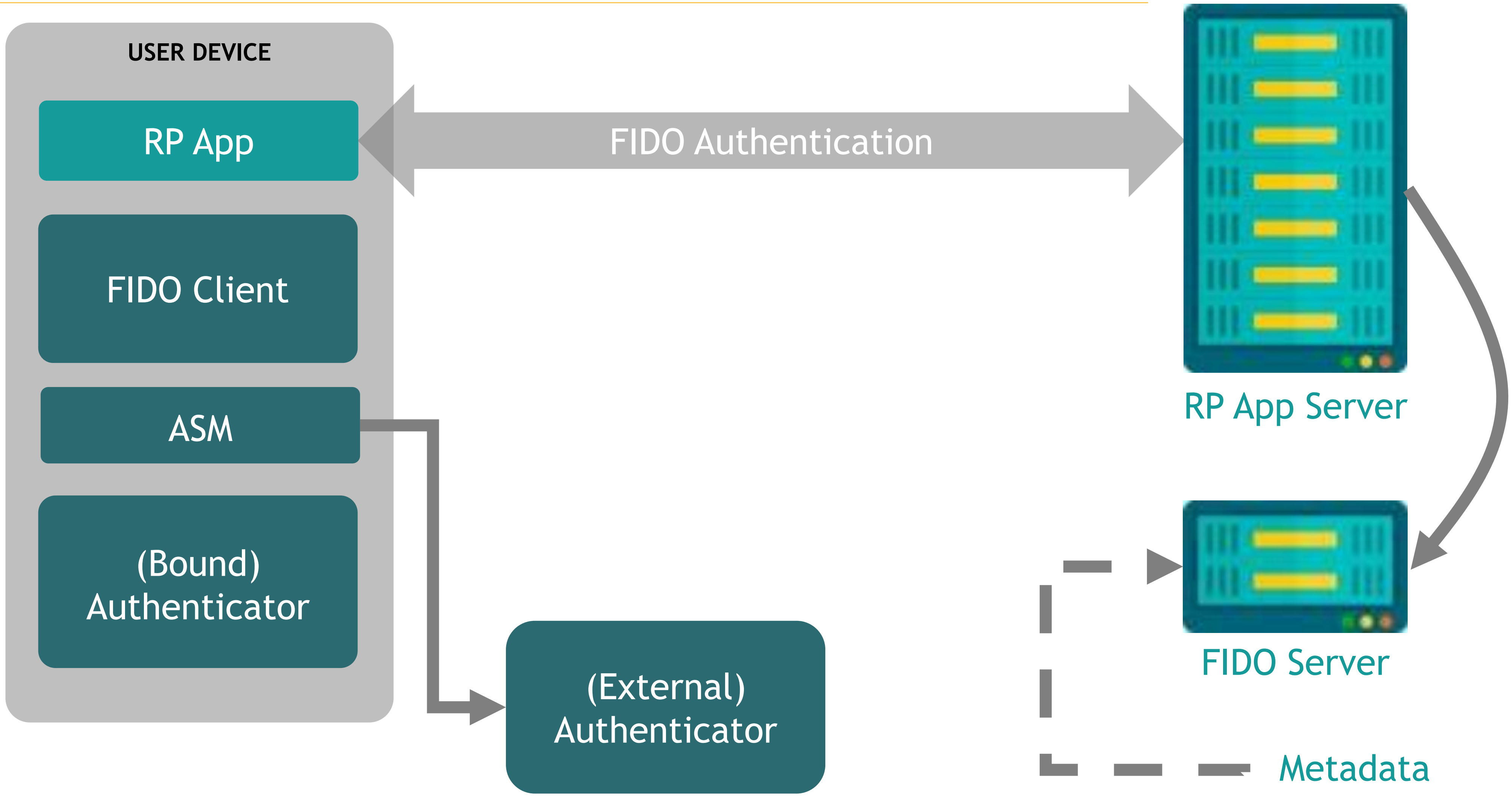
Second Factor Challenge

Insert Dongle* / Press Button

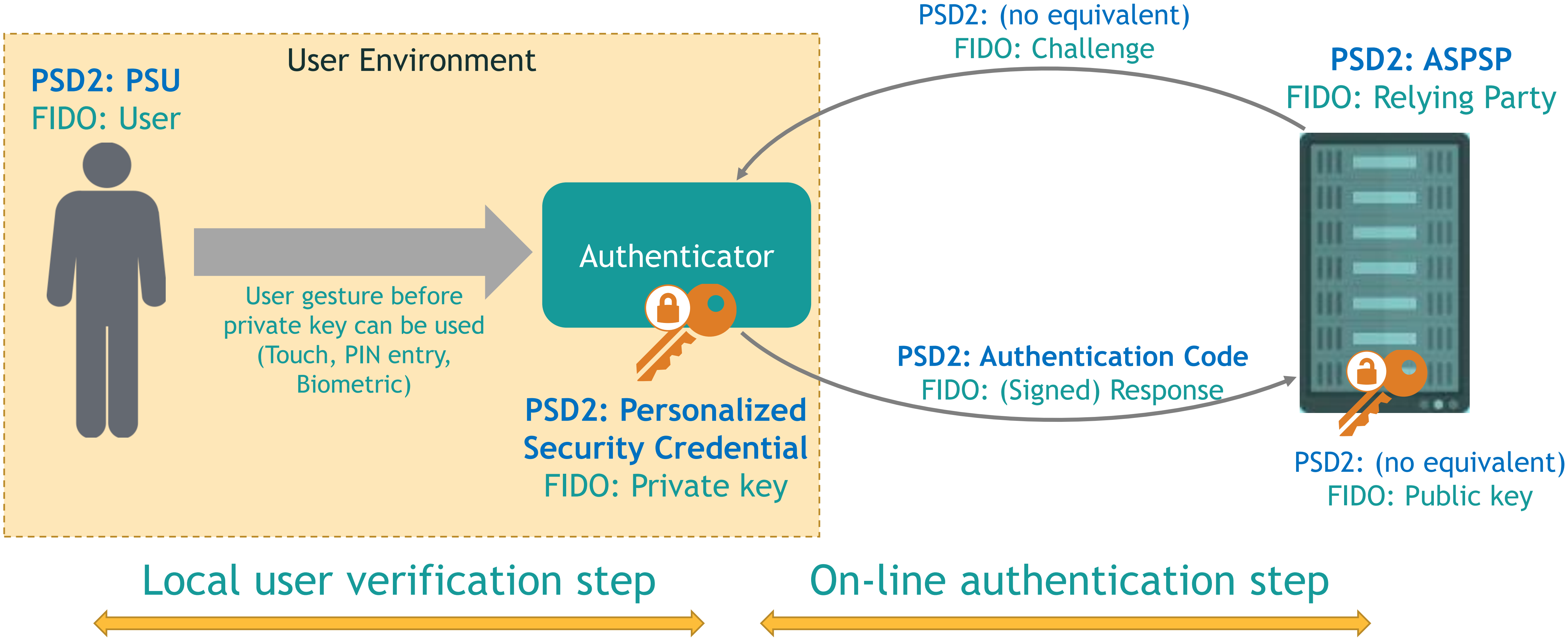
Authenticated Online

*There are other types of authenticators (e.g. PIN)

FIDO BUILDING BLOCKS



HOW DOES FIDO WORK?



User Environment

PSD2: PSU
FIDO: User

User gesture before private key can be used (Touch, PIN entry, Biometric)

Authenticator

PSD2: Personalized Security Credential
FIDO: Private key

PSD2: (no equivalent)
FIDO: Challenge

PSD2: ASPSP
FIDO: Relying Party

PSD2: Authentication Code
FIDO: (Signed) Response

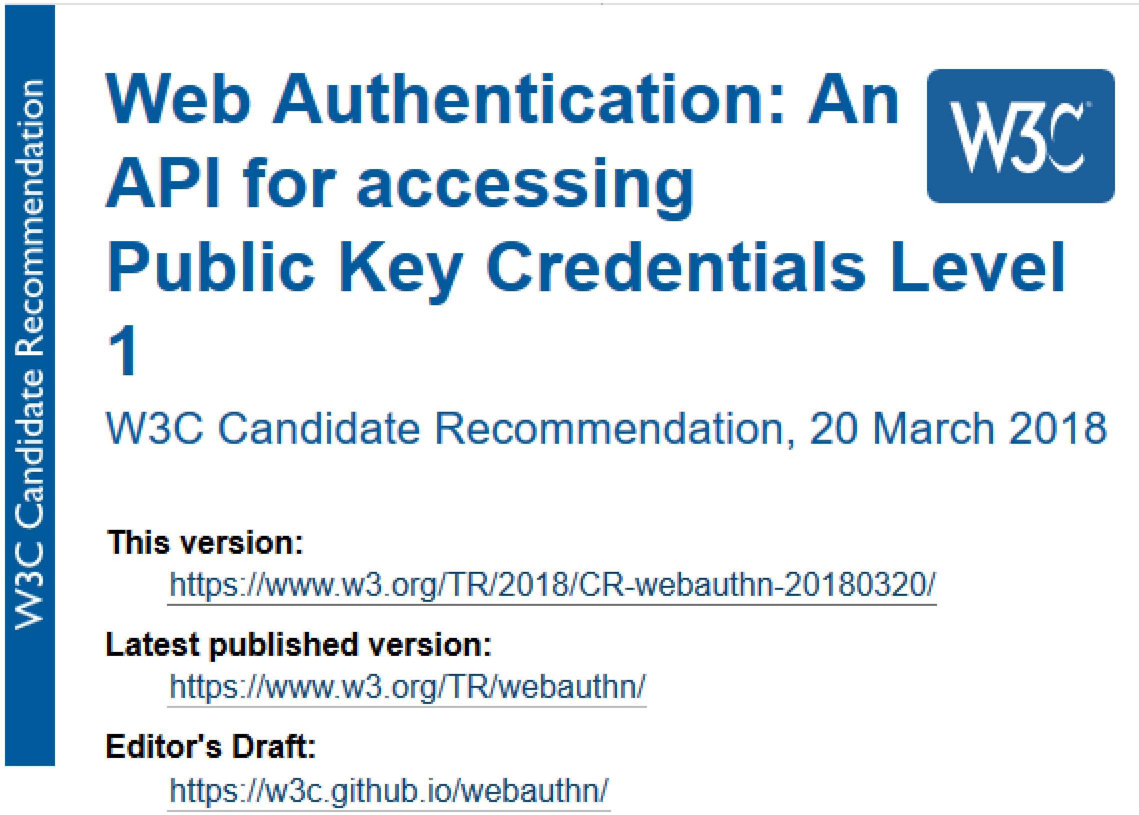
PSD2: (no equivalent)
FIDO: Public key

Local user verification step

On-line authentication step

WEB AUTHENTICATION

JavaScript API that enables
FIDO Authentication directly in web browsers



W3C Candidate Recommendation

Web Authentication: An API for accessing Public Key Credentials Level 1

W3C Candidate Recommendation, 20 March 2018

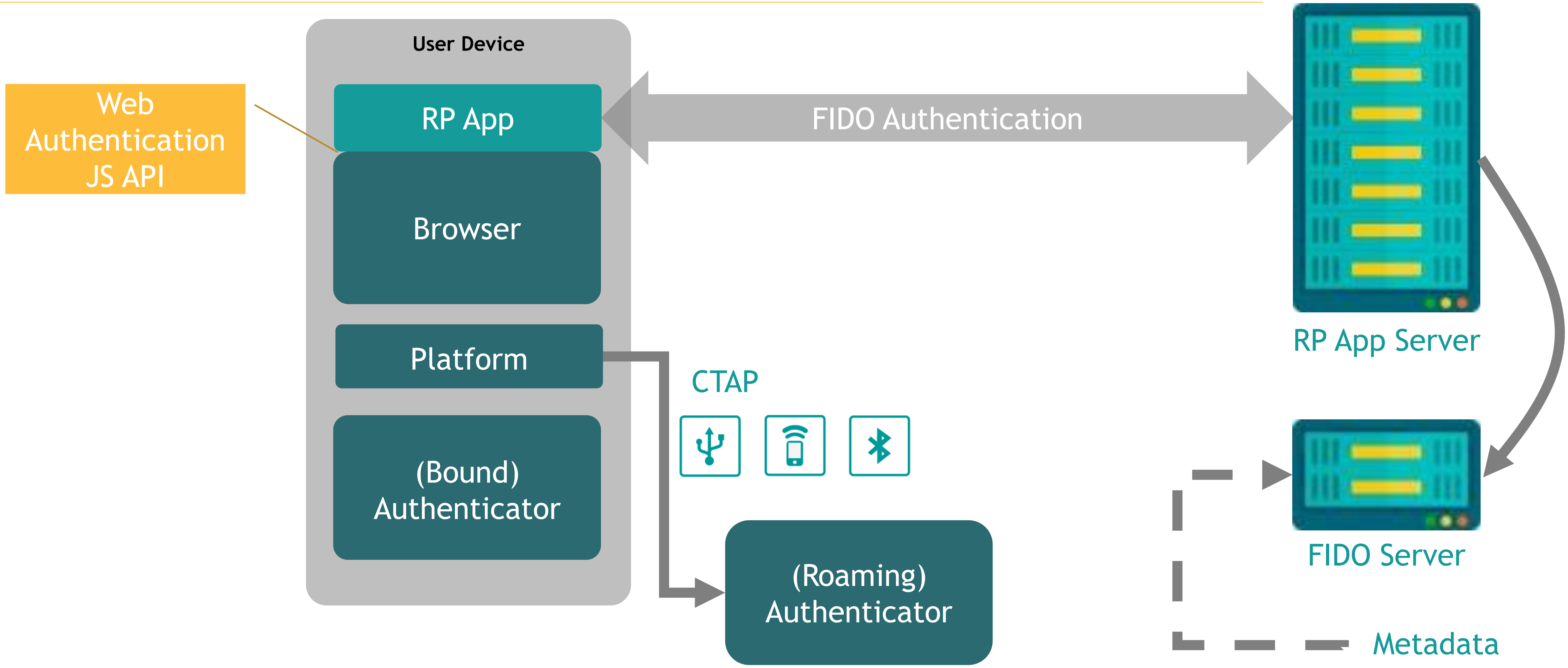
This version:
https://www.w3.org/TR/2018/CR-webauthn-20180320/

Latest published version:
https://www.w3.org/TR/webauthn/

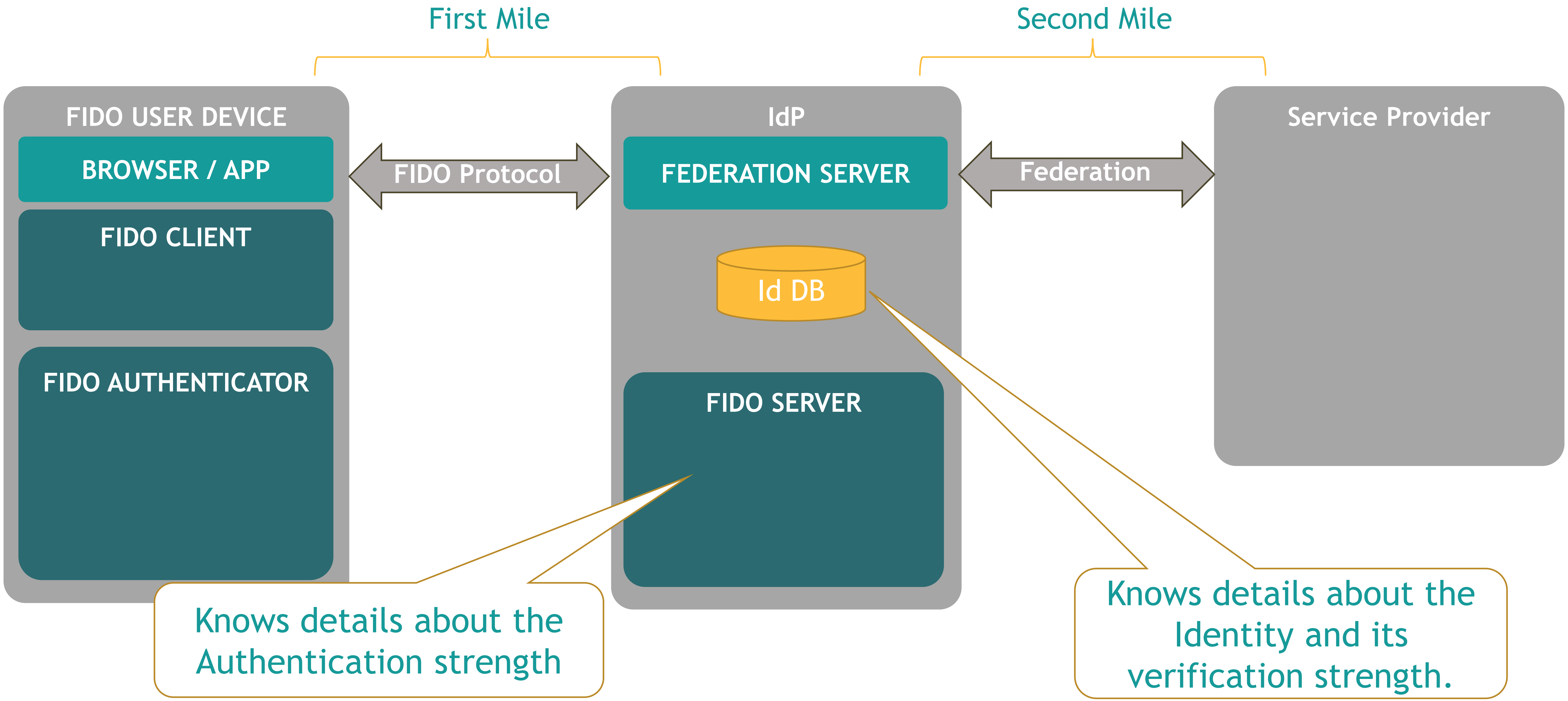
Editor's Draft:
https://w3c.github.io/webauthn/

Supported In:

FIDO BUILDING BLOCKS



FIDO & Federation

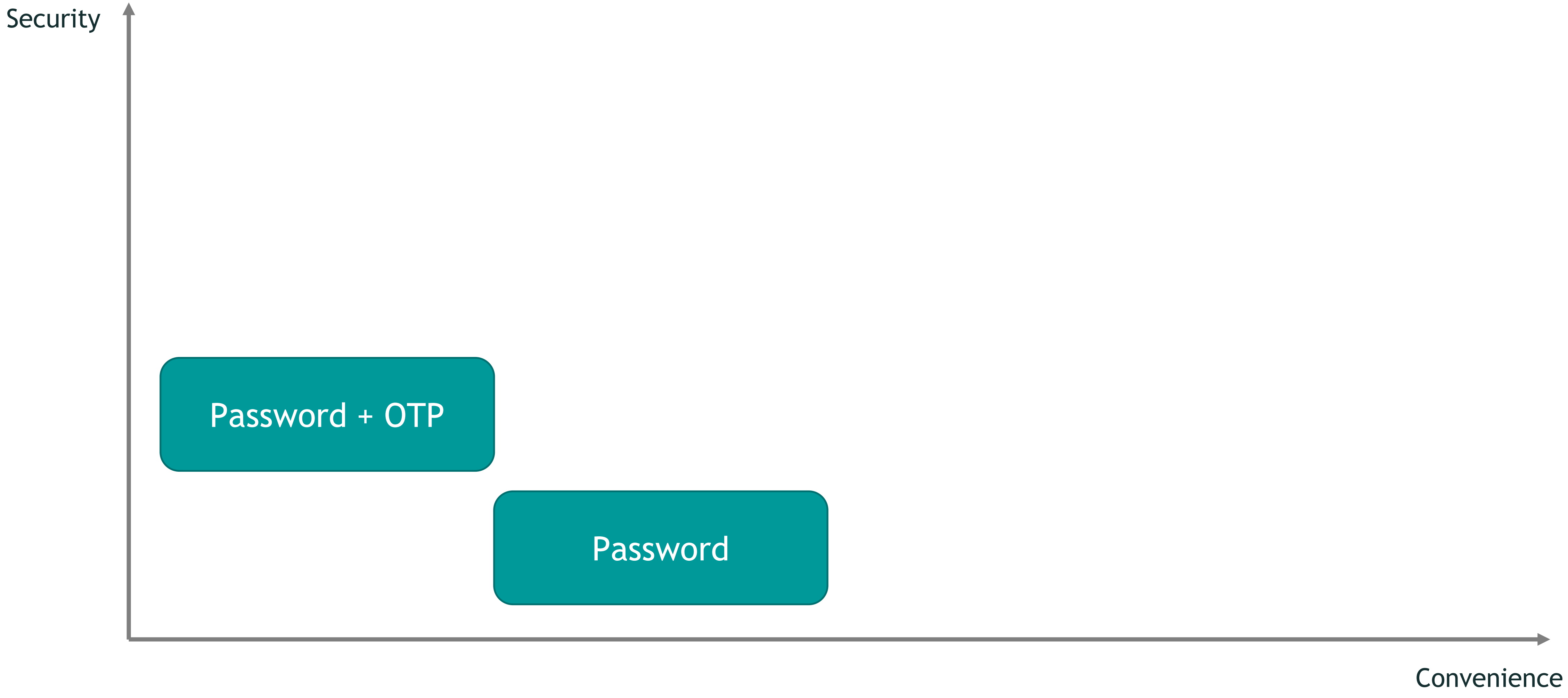


Knows details about the Authentication strength

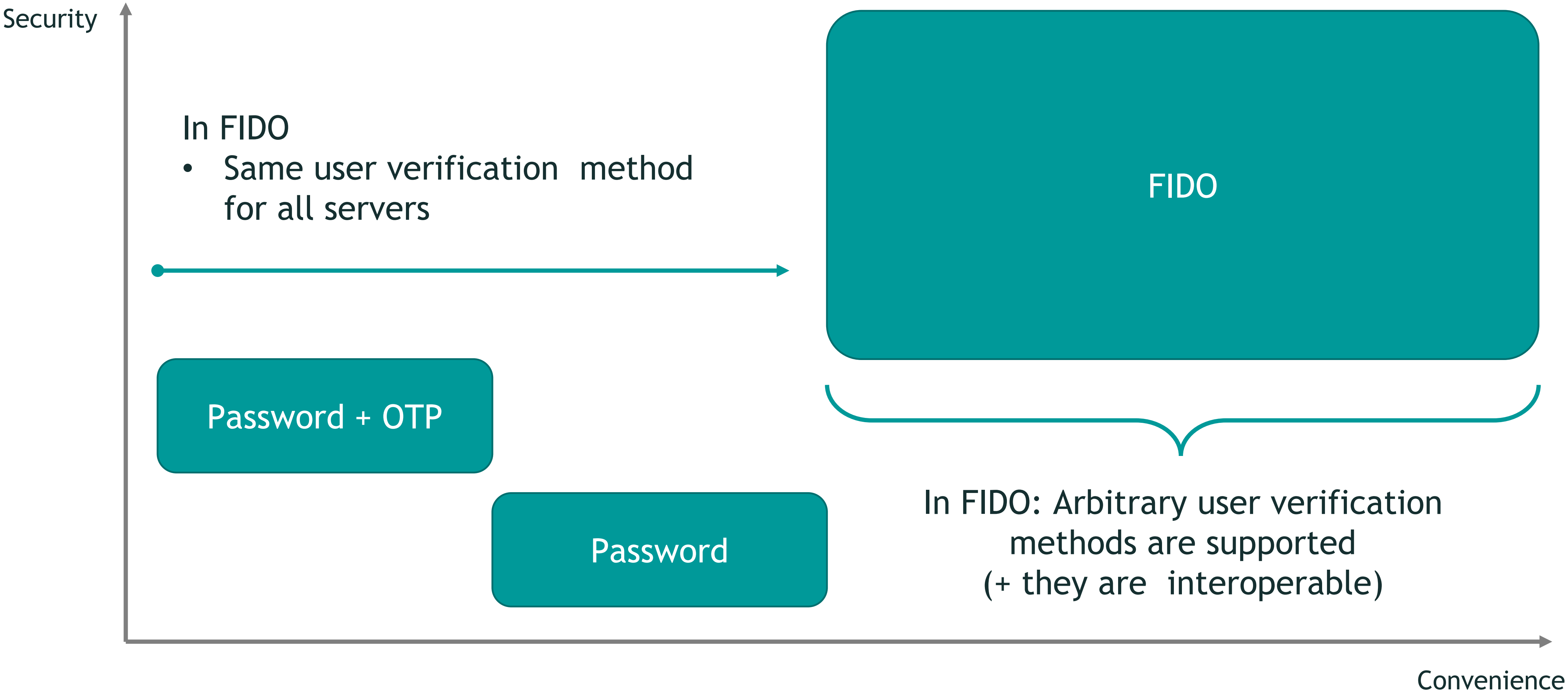
Knows details about the Identity and its verification strength.

FIDO AUTHENTICATION: SECURITY & CONVENIENCE

CONVENIENCE & SECURITY



CONVENIENCE & SECURITY



Security

In FIDO
- Same user verification method for all servers

FIDO

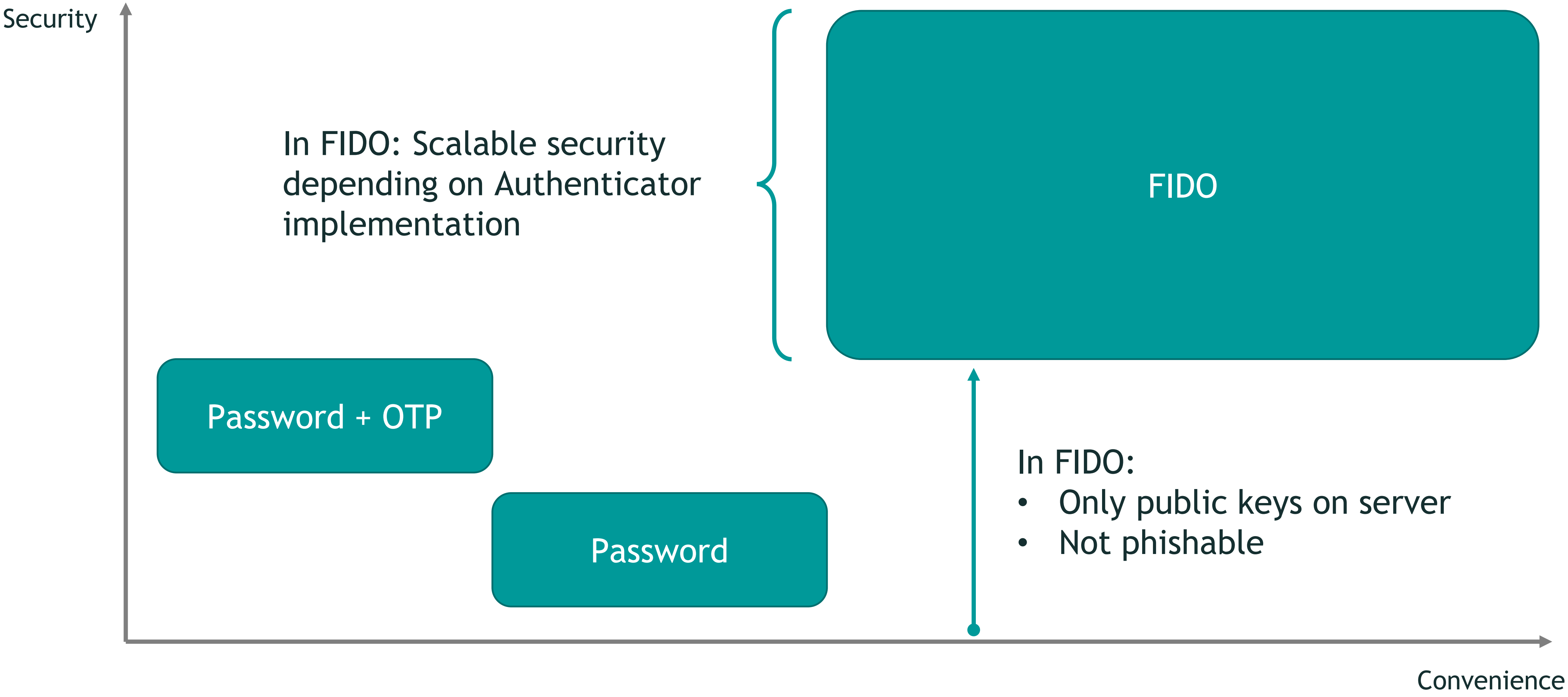
Password + OTP

Password

In FIDO: Arbitrary user verification methods are supported
(+ they are interoperable)

Convenience

CONVENIENCE & SECURITY



Security

In FIDO: Scalable security depending on Authenticator implementation

FIDO

Password + OTP

Password

In FIDO:
- Only public keys on server
- Not phishable

Convenience

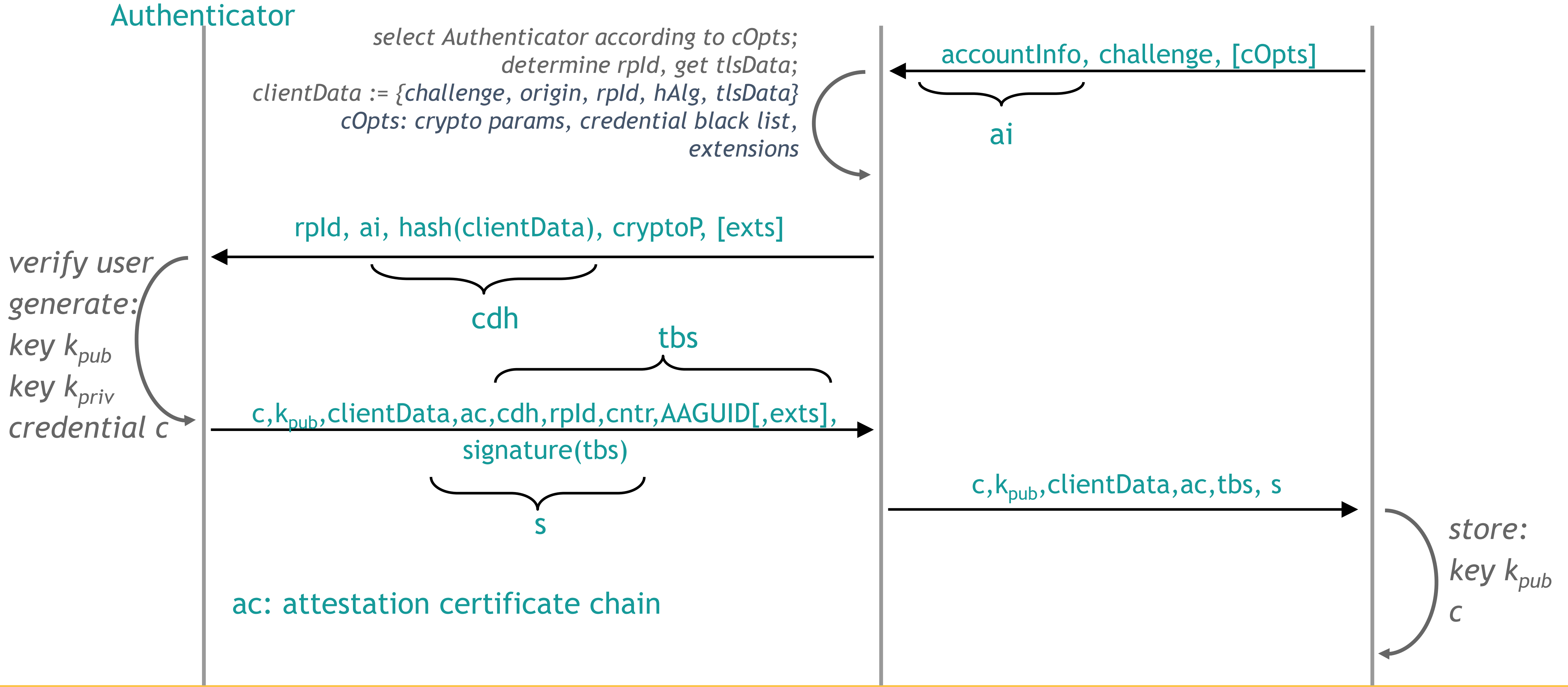
CONCLUSION

- Different authentication use-cases lead to different authentication requirements
- FIDO separates user verification from authentication and hence supports all user verification methods
- FIDO supports scalable convenience & security
- User verification data is known to Authenticator only
- FIDO complements federation

@FIDOalliance

#FIDOseminar

FIDO REGISTRATION



Authenticator

select Authenticator according to cOpts;
determine rpId, get tlsData;
clientData := {challenge, origin, rpId, hAlg, tlsData}
cOpts: crypto params, credential black list,
extensions

accountInfo, challenge, [cOpts]

ai

rpId, ai, hash(clientData), cryptoP, [exts]

cdh

verify user
generate:
key k_{pub}
key k_{priv}
credential c

tbs

c,k_{pub},clientData,ac,cdh,rpId,cntr,AAGUID[,exts],
signature(tbs)

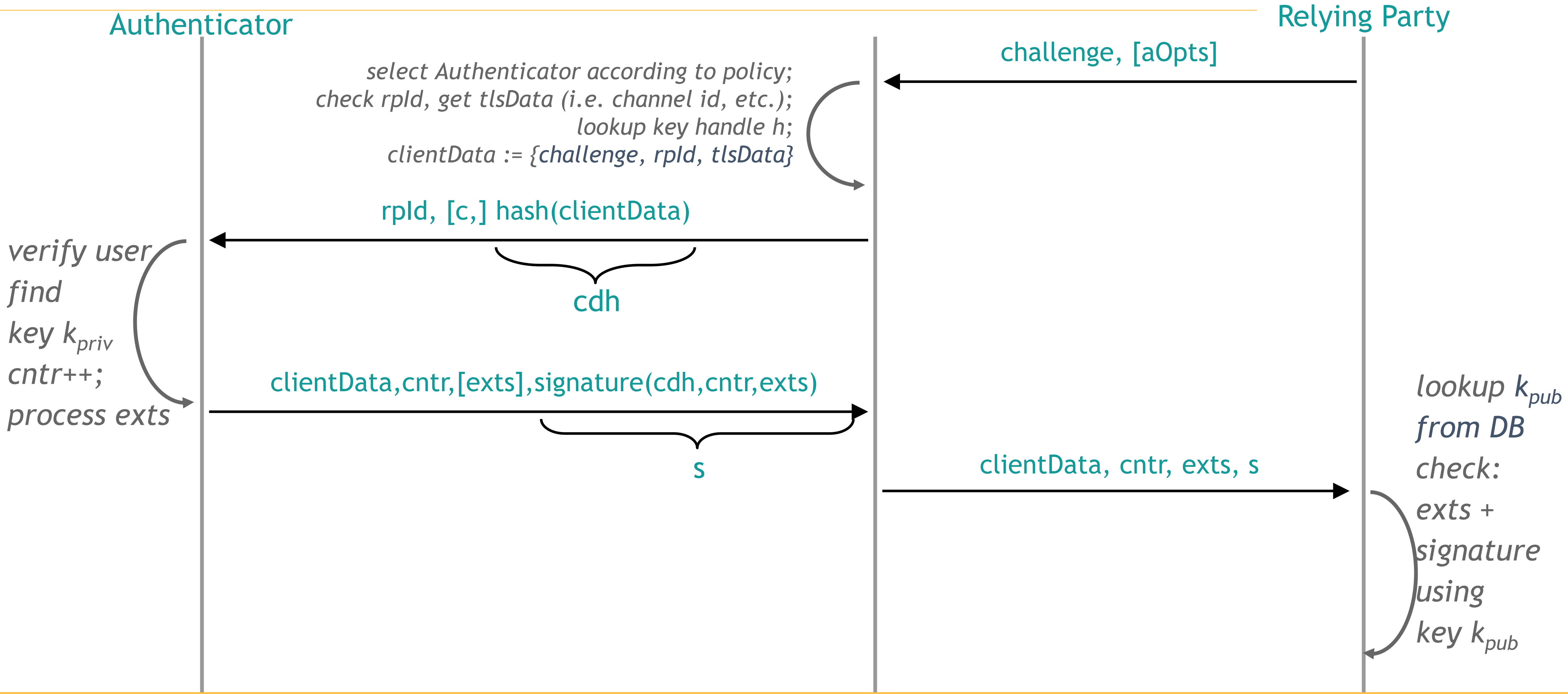
s

c,k_{pub},clientData,ac,tbs, s

store:
key k_{pub}
c

ac: attestation certificate chain

FIDO AUTHENTICATION



Authenticator

Relying Party

challenge, [aOpts]

select Authenticator according to policy;
check rpId, get tlsData (i.e. channel id, etc.);
lookup key handle h;
clientData := {challenge, rpId, tlsData}

rpId, [c,] hash(clientData)

cdh

verify user
find
key k_{priv}
cntr++;
process exts

clientData,cntr,[exts],signature(cdh,cntr,exts)

s

clientData, cntr, exts, s

lookup k_{pub}
from DB
check:
exts +
signature
using
key k_{pub}