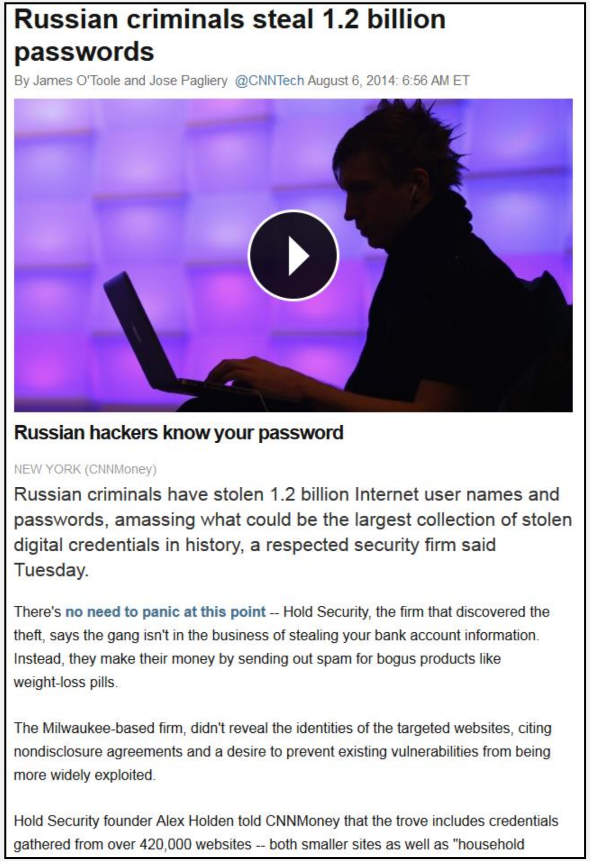
fido™ alliance

simpler
stronger
authentication

FIDO UAF Tutorial

How Secure is Authentication?



Russian criminals steal 1.2 billion passwords

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

Russian hackers know your password

NEW YORK (CNNMoney)

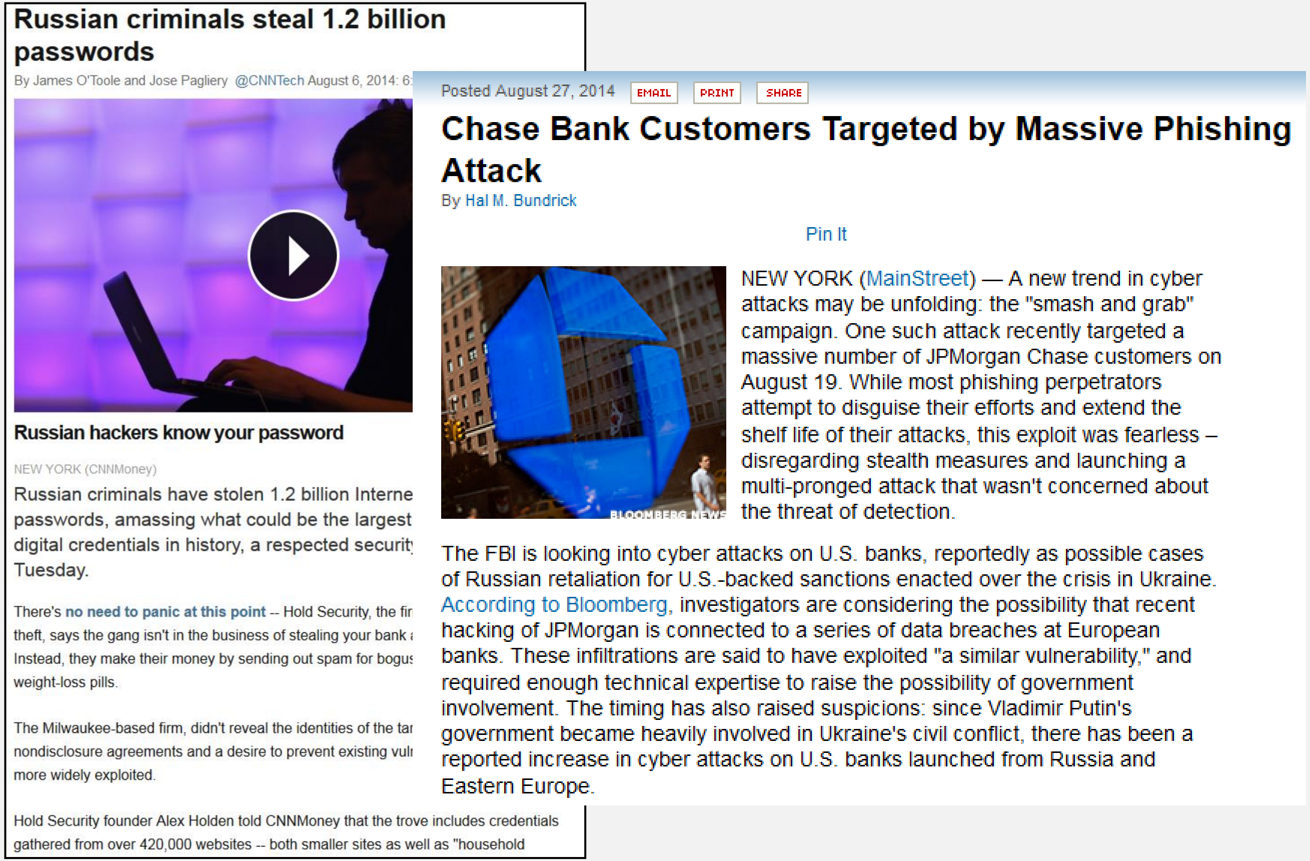
Russian criminals have stolen 1.2 billion Internet user names and passwords, amassing what could be the largest collection of stolen digital credentials in history, a respected security firm said Tuesday.

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 weight-loss pills.

The Milwaukee-based firm, didn't reveal the identities of the targeted websites, citing nondisclosure agreements and a desire to prevent existing vulnerabilities from being more widely exploited.

Hold Security founder Alex Holden told CNNMoney that the trove includes credentials gathered from over 420,000 websites -- both smaller sites as well as "household

How Secure is Authentication?



Russian criminals steal 1.2 billion passwords

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

Russian hackers know your password

NEW YORK (CNNMoney)

Russian criminals have stolen 1.2 billion Interne passwords, amassing what could be the largest digital credentials in history, a respected securit Tuesday.

There's **no need to panic at this point** -- Hold Security, the fir theft, says the gang isn't in the business of stealing your bank a Instead, they make their money by sending out spam for bogus weight-loss pills.

The Milwaukee-based firm, didn't reveal the identities of the tar nondisclosure agreements and a desire to prevent existing vuln more widely exploited.

Hold Security founder Alex Holden told CNNMoney that the trove includes credentials gathered from over 420,000 websites -- both smaller sites as well as "household

Posted August 27, 2014 EMAIL PRINT SHARE

Chase Bank Customers Targeted by Massive Phishing Attack

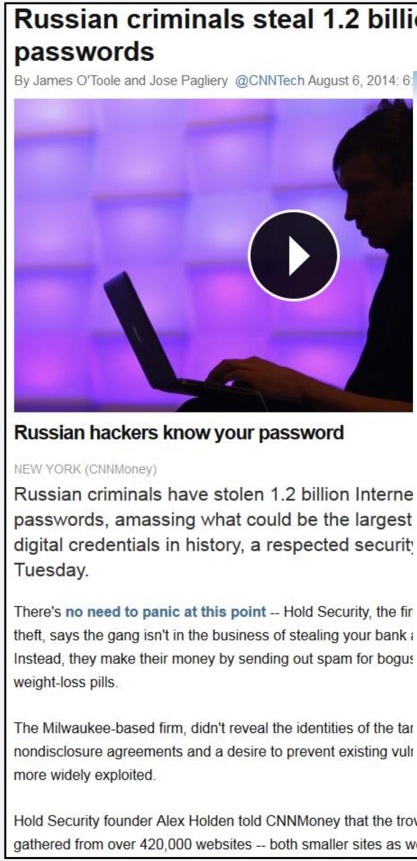
By Hal M. Bundrick

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 Secure is Authentication?



Russian criminals steal 1.2 billion passwords

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

Russian hackers know your password

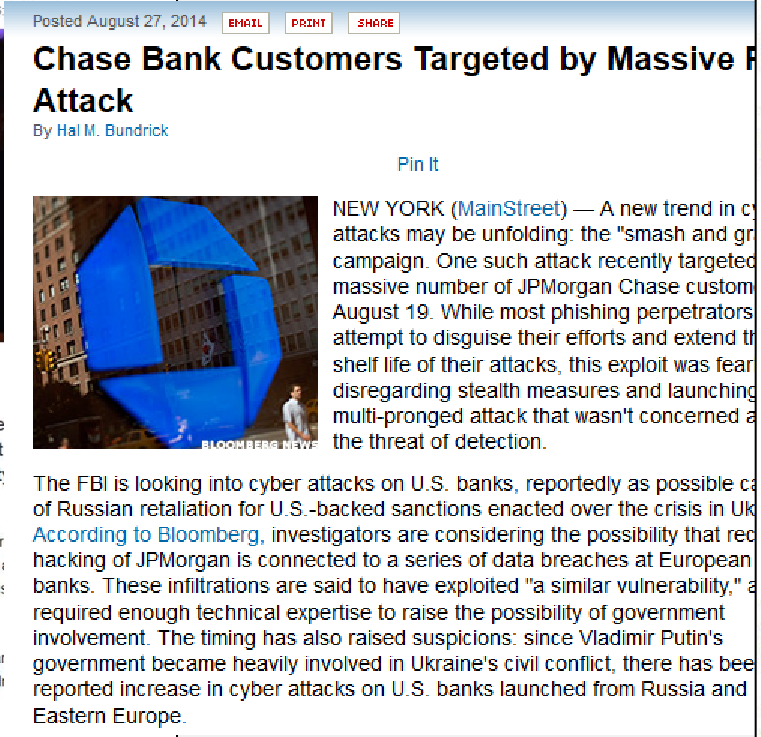
NEW YORK (CNNMoney)

Russian criminals have stolen 1.2 billion Interne passwords, amassing what could be the largest digital credentials in history, a respected securit Tuesday.

There's **no need to panic at this point** -- Hold Security, the fir theft, says the gang isn't in the business of stealing your bank a Instead, they make their money by sending out spam for bogus weight-loss pills.

The Milwaukee-based firm, didn't reveal the identities of the tar nondisclosure agreements and a desire to prevent existing vul more widely exploited.

Hold Security founder Alex Holden told CNNMoney that the trove includes credentials gathered from over 420,000 websites -- both smaller sites as well as "household



Posted August 27, 2014 EMAIL PRINT SHARE

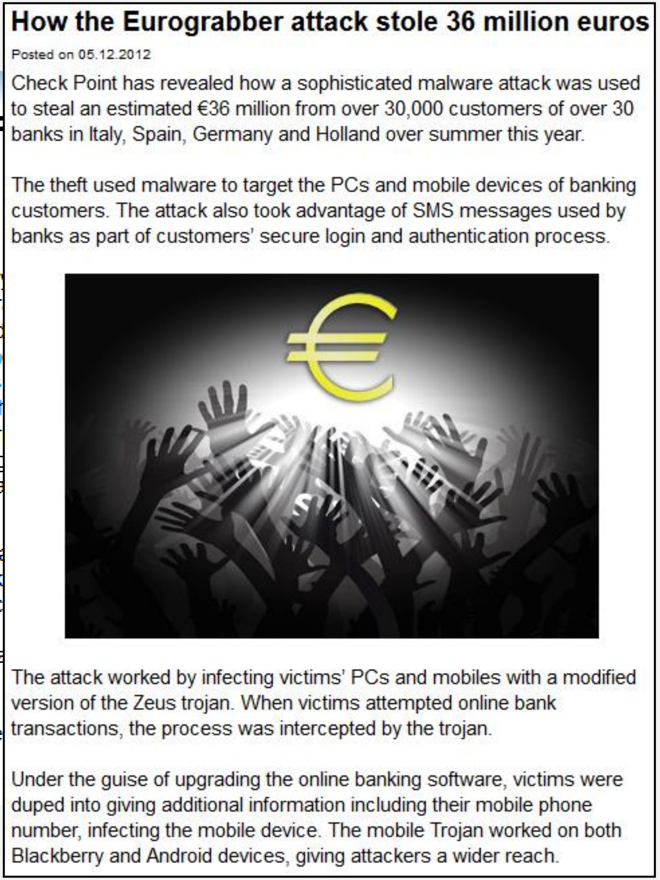
Chase Bank Customers Targeted by Massive P Attack

By Hal M. Bundrick

Pin It

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

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

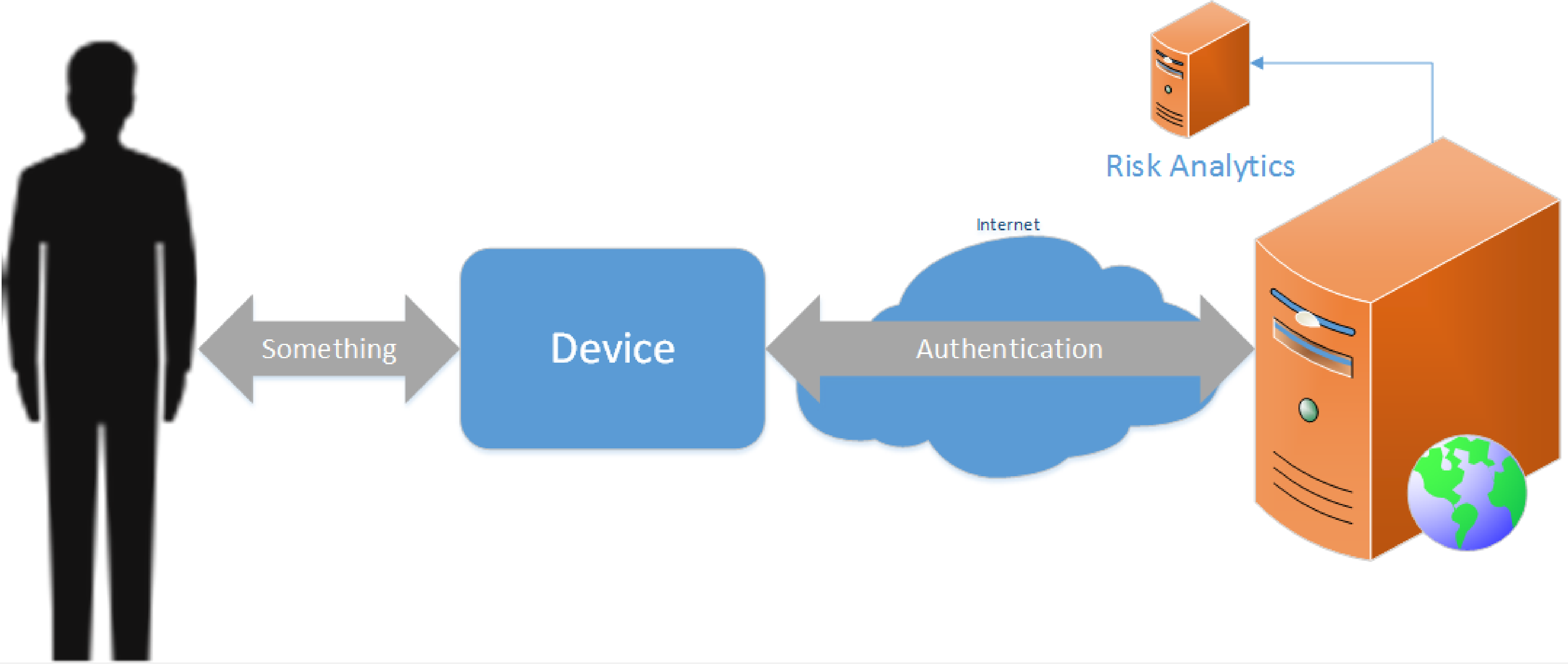
Check Point has revealed how a sophisticated malware attack was used to steal an estimated €36 million from over 30,000 customers of over 30 banks in Italy, Spain, Germany and Holland over summer this year.

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.

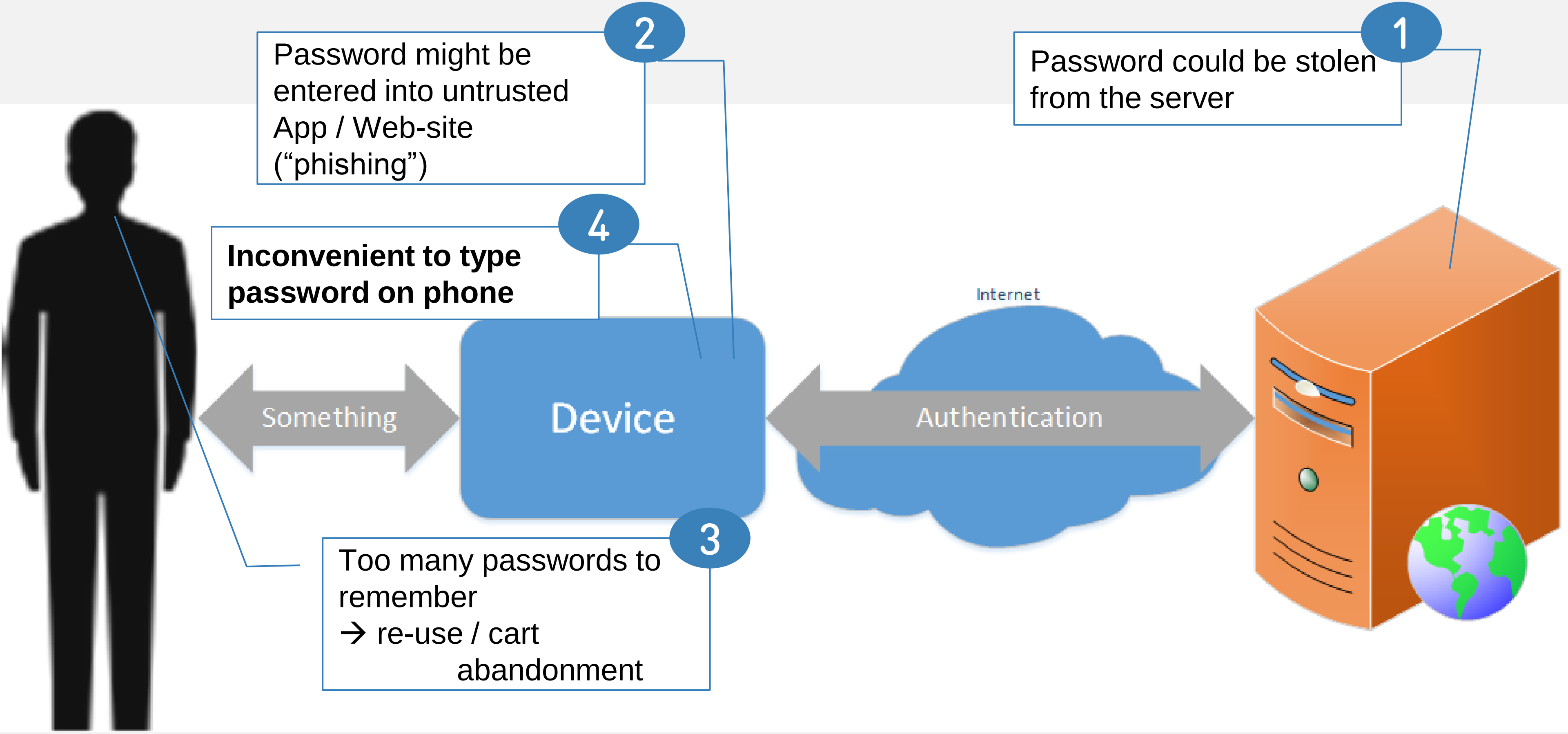
The attack worked by infecting victims' PCs and mobiles with a modified version of the Zeus trojan. When victims attempted online bank transactions, the process was intercepted by the trojan.

Under the guise of upgrading the online banking software, victims were duped into giving additional information including their mobile phone number, infecting the mobile device. The mobile Trojan worked on both Blackberry and Android devices, giving attackers a wider reach.

Cloud Authentication



Password Issues



1 Password could be stolen from the server

2 Password might be entered into untrusted App / Web-site ("phishing")

3 Too many passwords to remember
→ re-use / cart abandonment

4 **Inconvenient to type password on phone**

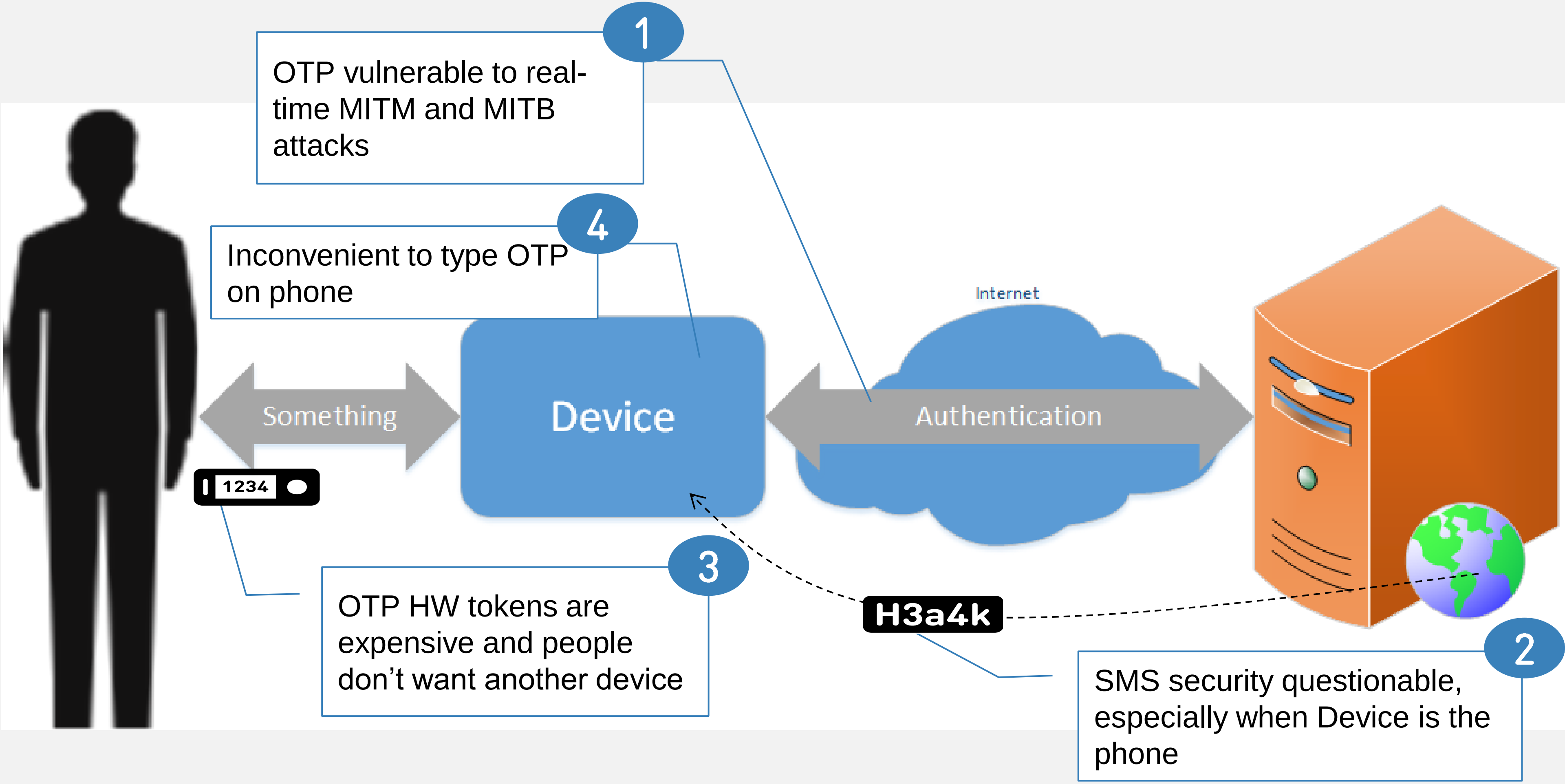
Something

Device

Internet

Authentication

OTP Issues



1 OTP vulnerable to real-time MITM and MITB attacks

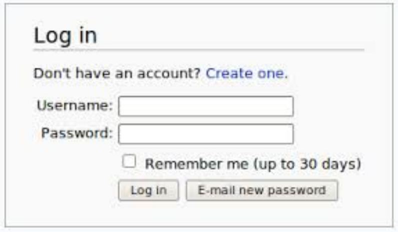
2 SMS security questionable, especially when Device is the phone

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

4 Inconvenient to type OTP on phone

Authentication Needs

Do you want to login? 1



Log in

Don't have an account? Create one.

Username:

Password:

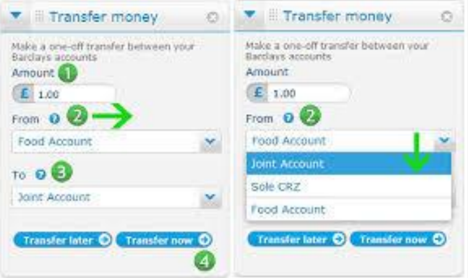
□ Remember me (up to 30 days)

Do you want to delete all of your emails? 2

Do you want to change your shipping address? 3

Do you want to share your dental records? 4

Do you want to transfer $100 to Frank? 5



Transfer money

Make a one-off transfer between your Barclays accounts

Amount: £ 1.00

From: Food Account

To: Joint Account

Transfer money

Make a one-off transfer between your Barclays accounts

Amount: £ 1.00

From: Food Account

Joint Account

Sole CRZ

Food Account

6

Do you want to transfer $10,000 to mymerchant.com?

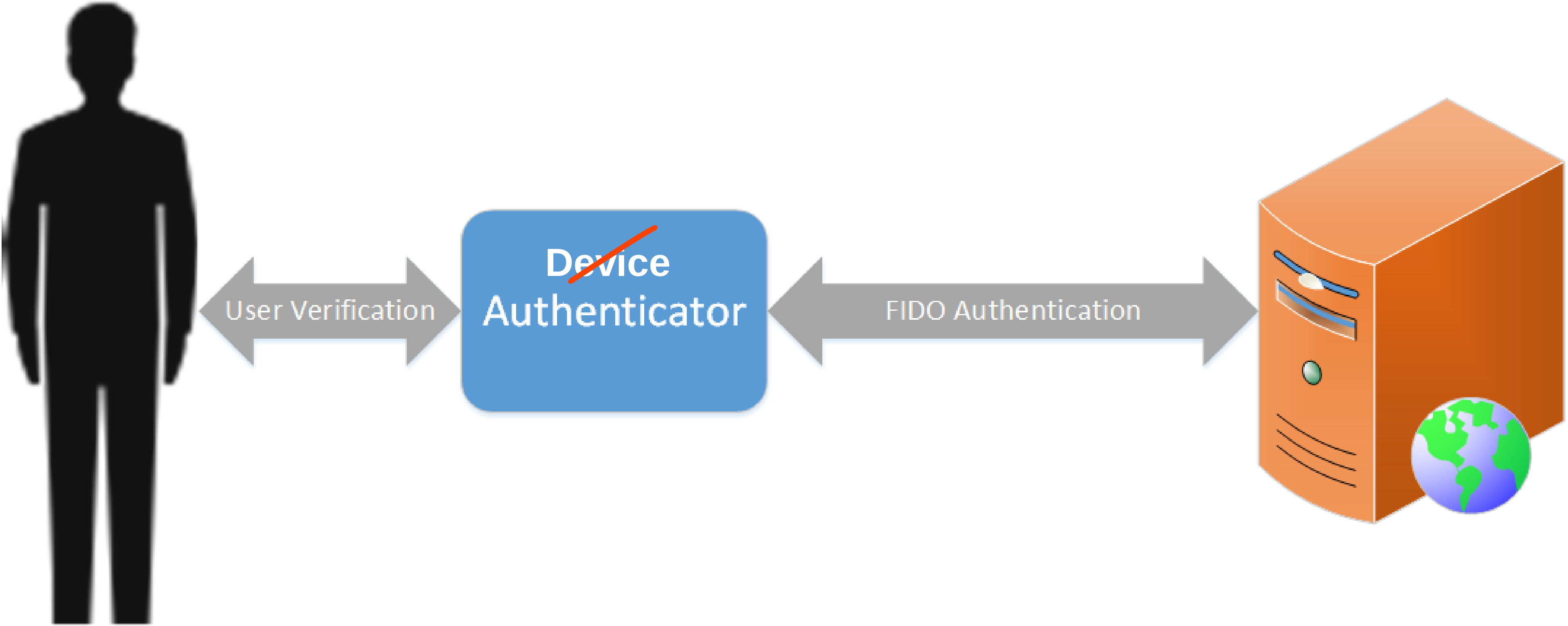
Authentication today:

Ask user for a password… (and perhaps a one time password)

Summary

1. Passwords are insecure and inconvenient especially on mobile devices
2. Alternative authentication methods are silos and hence don‘t scale to large scale user populations
3. The required security level of the authentication depends on the use
4. Risk engines need information about the explicit authentication security for good decision

How does FIDO work?

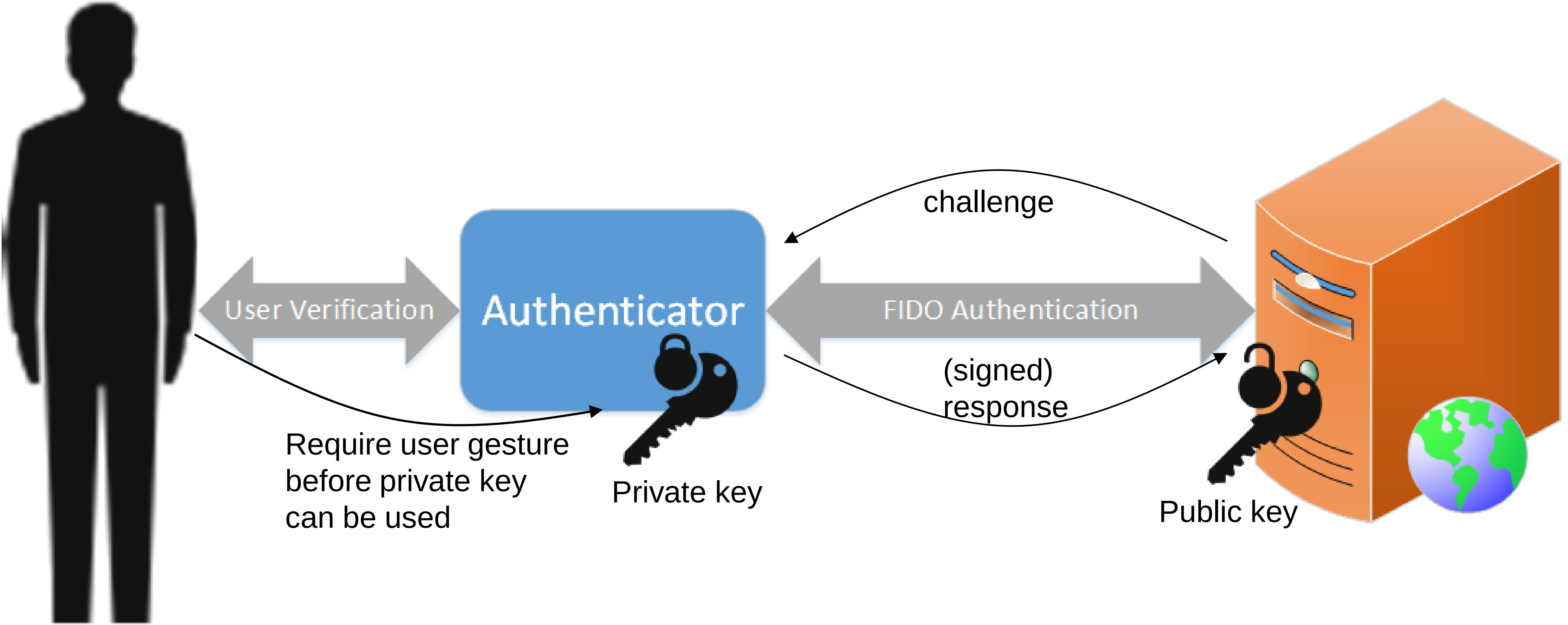


User Verification

~~Device~~ Authenticator

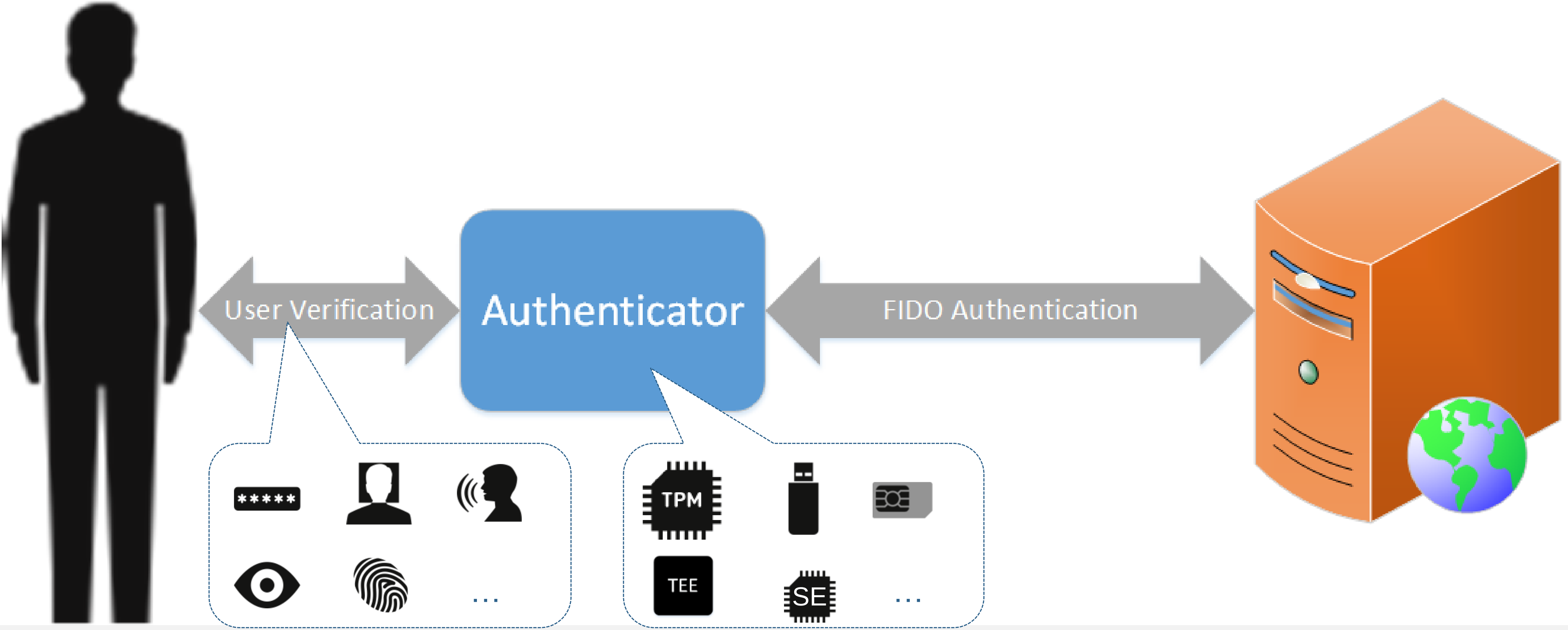
FIDO Authentication

How does FIDO work?

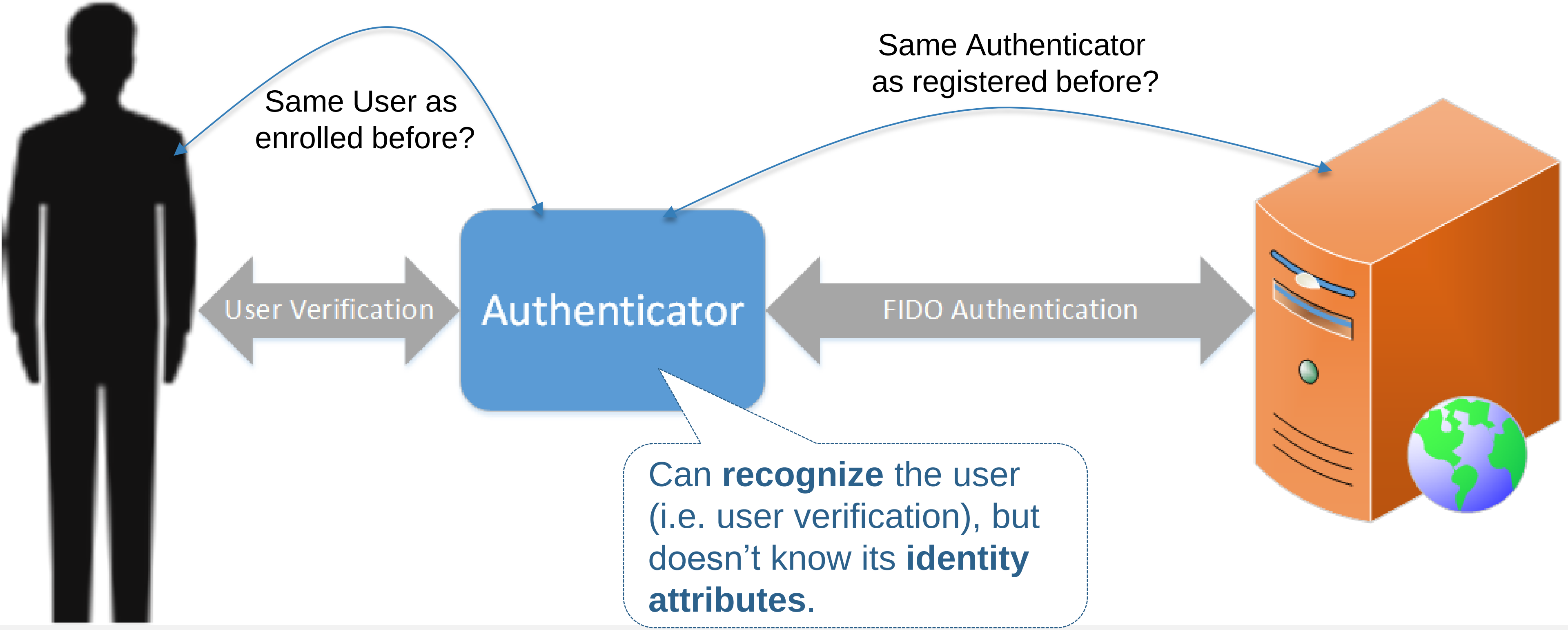


Require user gesture before private key can be used

How does FIDO UAF work?

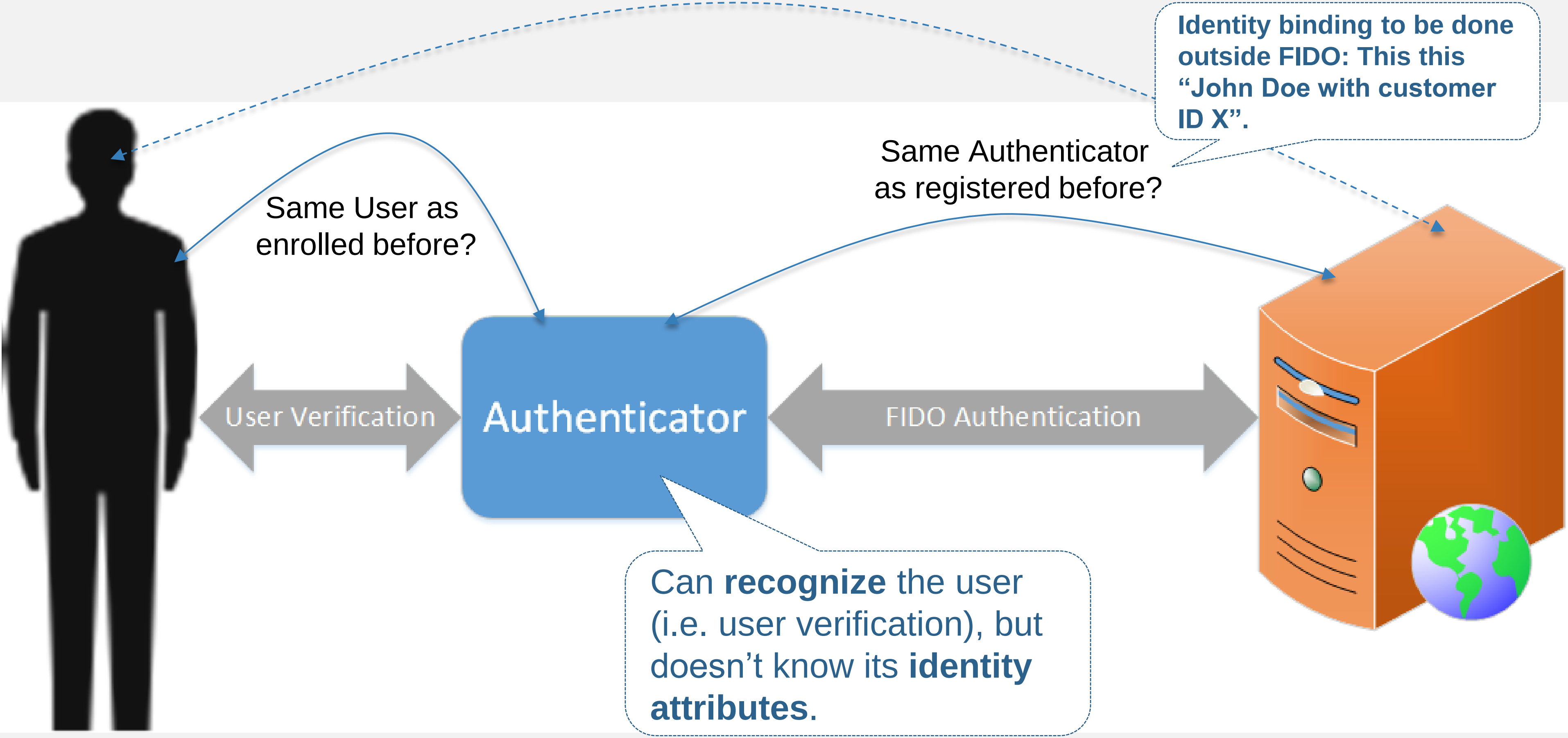


How does FIDO UAF work?


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 UAF work?



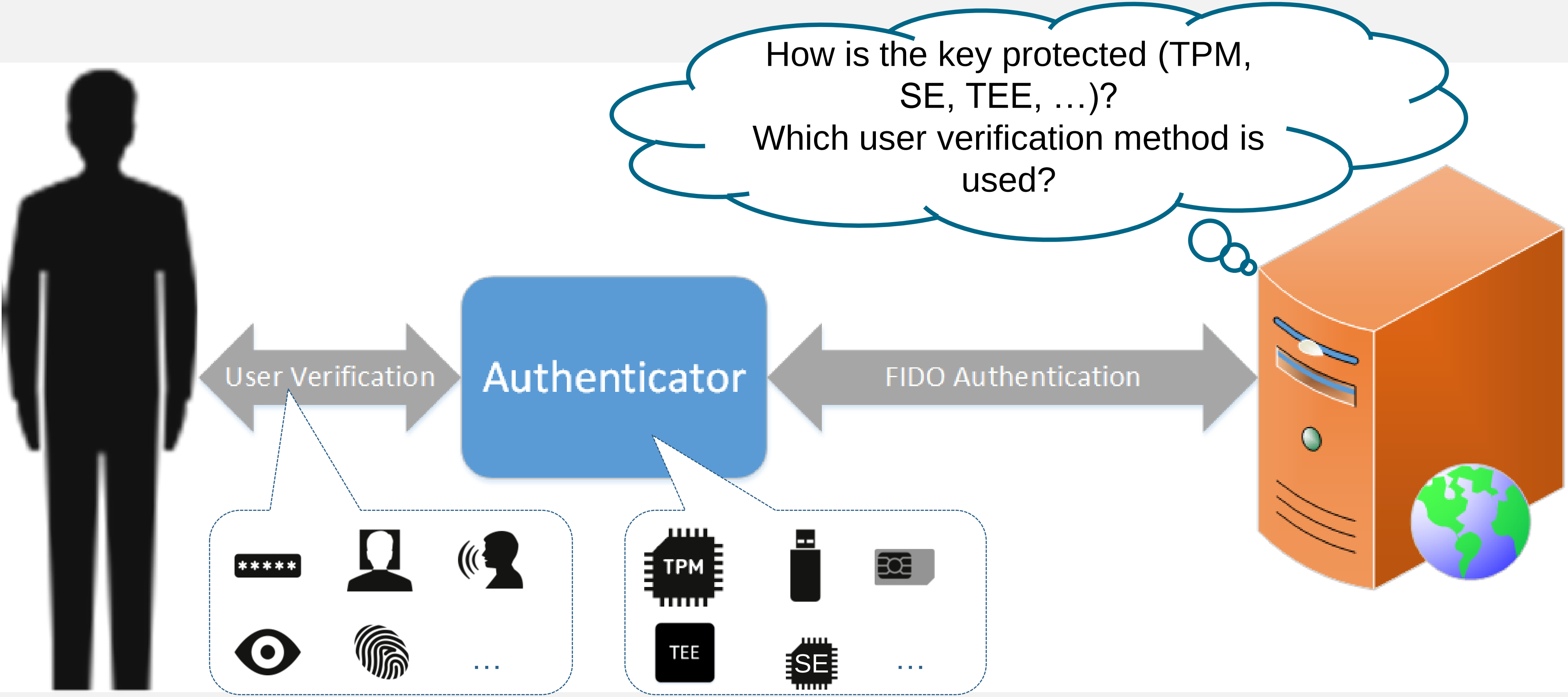
Identity binding to be done outside FIDO: This this "John Doe with customer ID X".

Same User as enrolled before?

Same Authenticator as registered before?

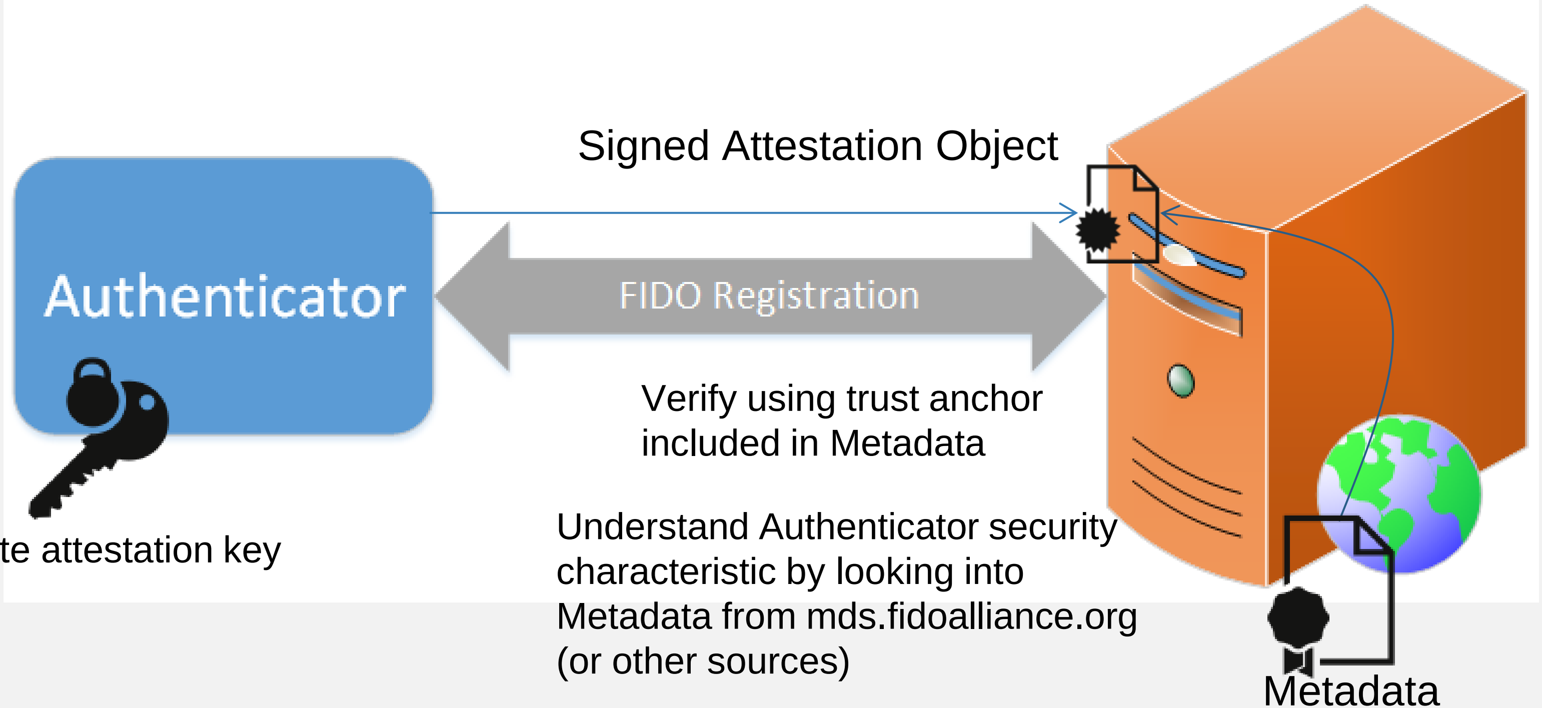
Can **recognize** the user (i.e. user verification), but doesn't know its **identity attributes**.

How does FIDO UAF work?



How is the key protected (TPM, SE, TEE, …)?
Which user verification method is used?

Attestation & Metadata



Signed Attestation Object

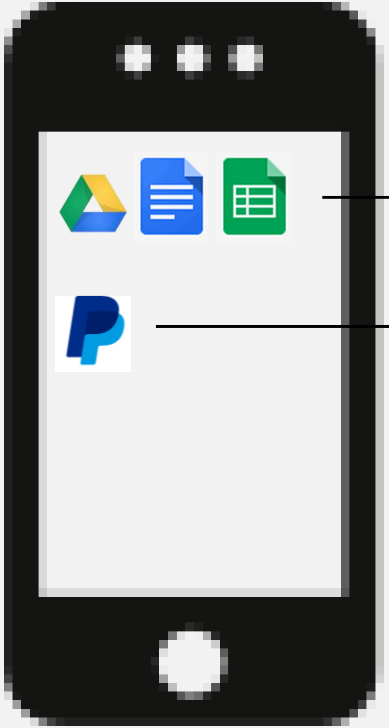
Private attestation key

Verify using trust anchor
included in Metadata

Understand Authenticator security
characteristic by looking into
Metadata from mds.fidoalliance.org
(or other sources)

Metadata

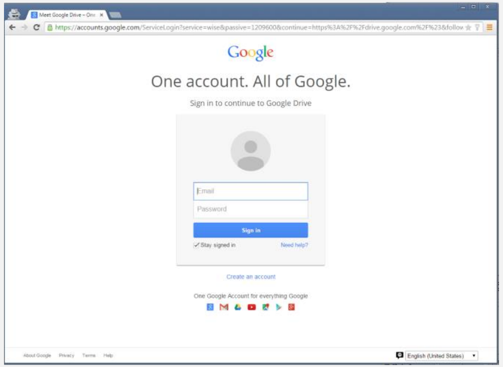
Binding Keys to Apps



Use google.com key

Use paypal.com key

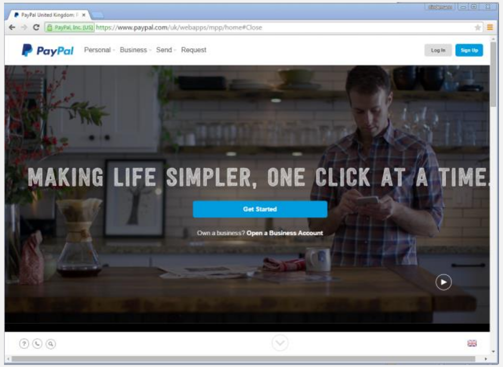
Use same user gesture
(e.g. same finger or PIN)
for unlocking each private key.



One account. All of Google.

Sign in to continue to Google Drive

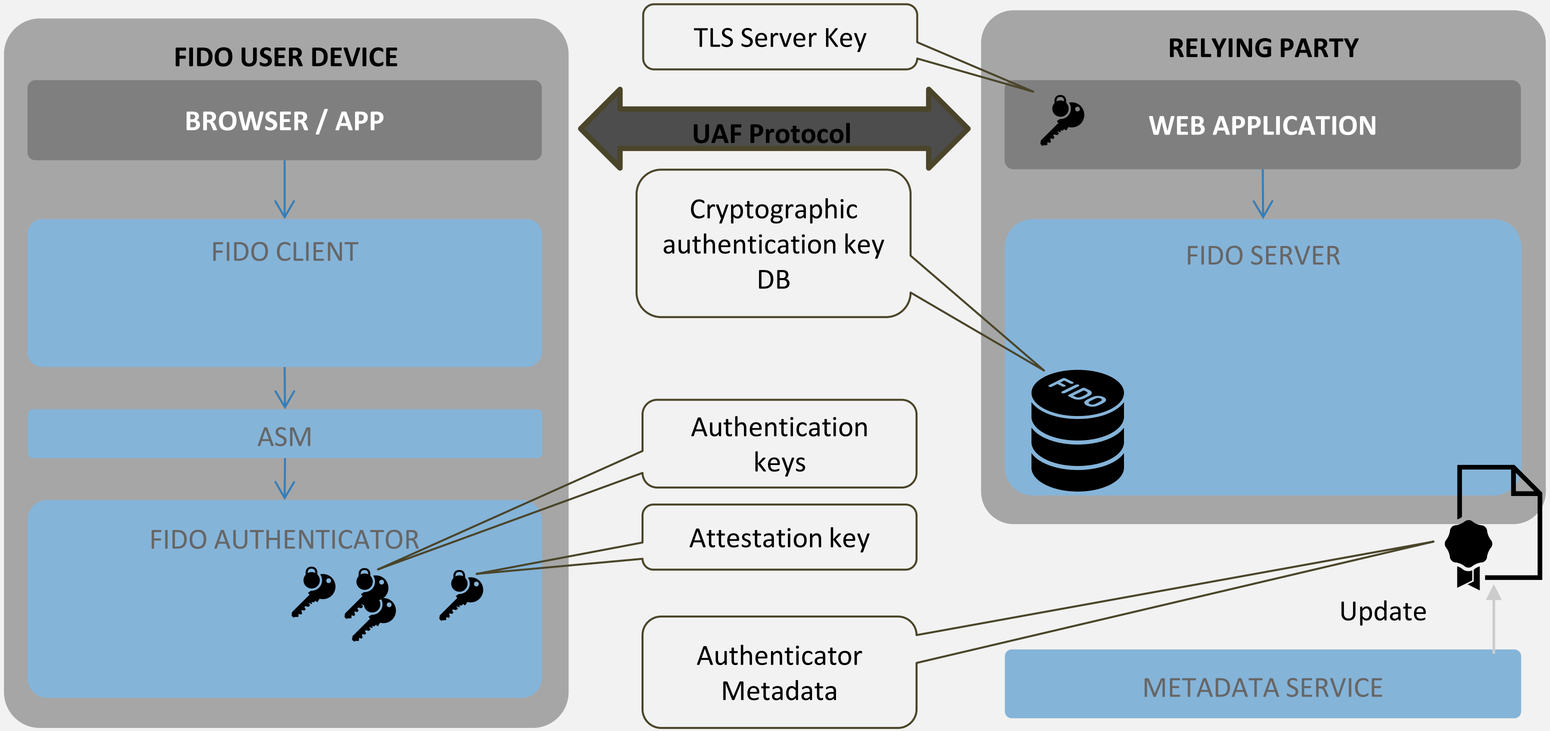
One Google Account for everything Google



MAKING LIFE SIMPLER, ONE CLICK AT A TIME.

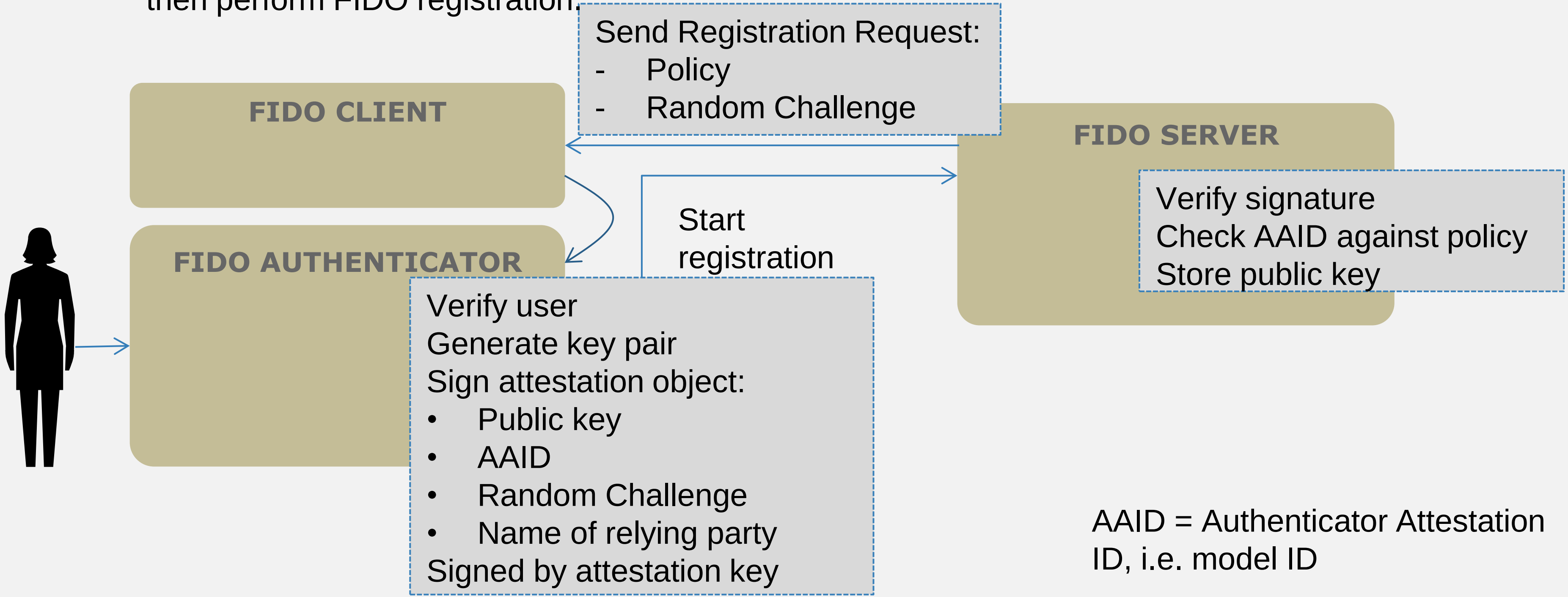
Own a business? Open a Business Account

FIDO Building Blocks



Registration Overview

Perform legacy authentication first, in order to bind authenticator to an electronic identity, then perform FIDO registration.



Send Registration Request:

- Policy
- Random Challenge

Verify user
Generate key pair
Sign attestation object:

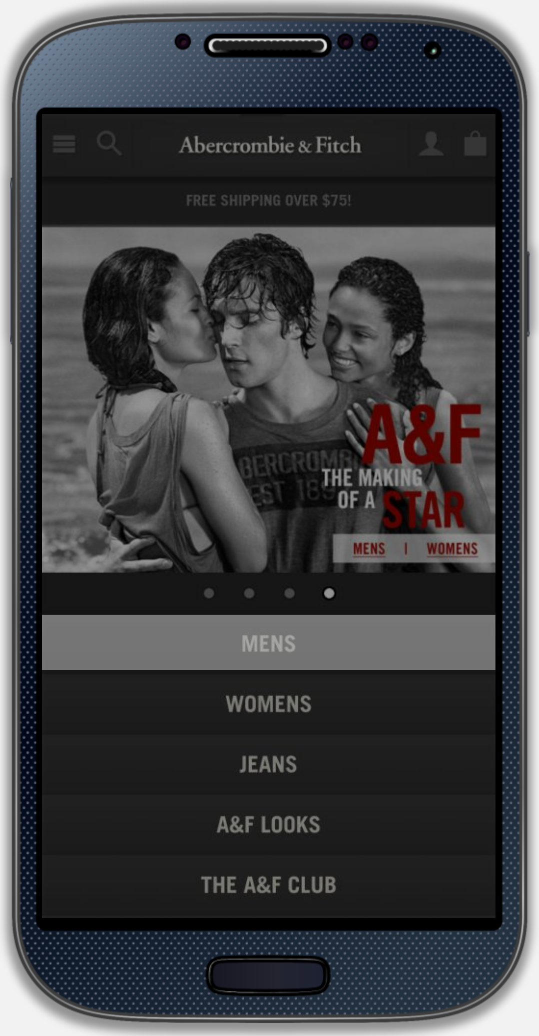
- Public key
- AAID
- Random Challenge
- Name of relying party

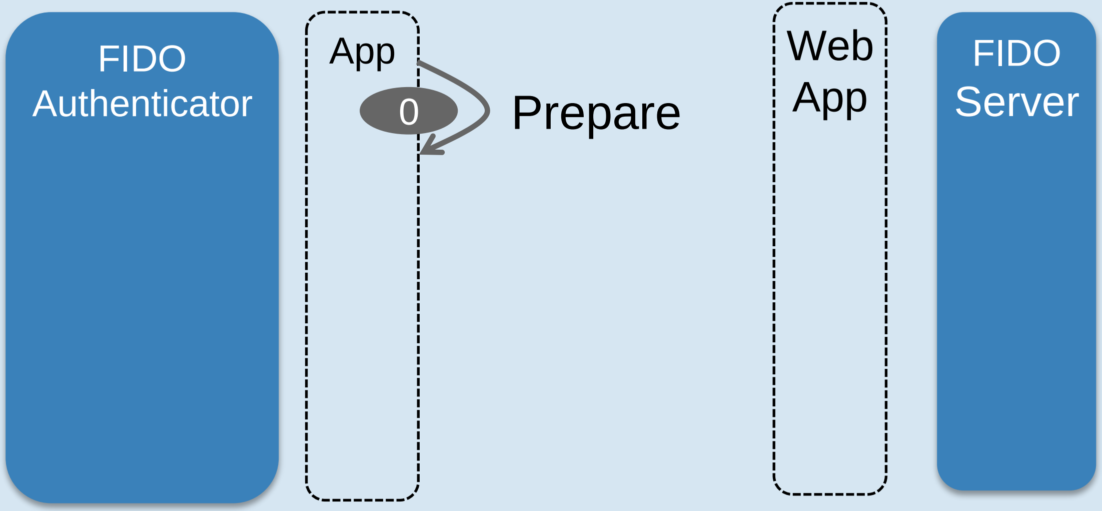
Signed by attestation key

Verify signature
Check AAID against policy
Store public key

AAID = Authenticator Attestation ID, i.e. model ID

UAF Authentication




FIDO Authenticator

App

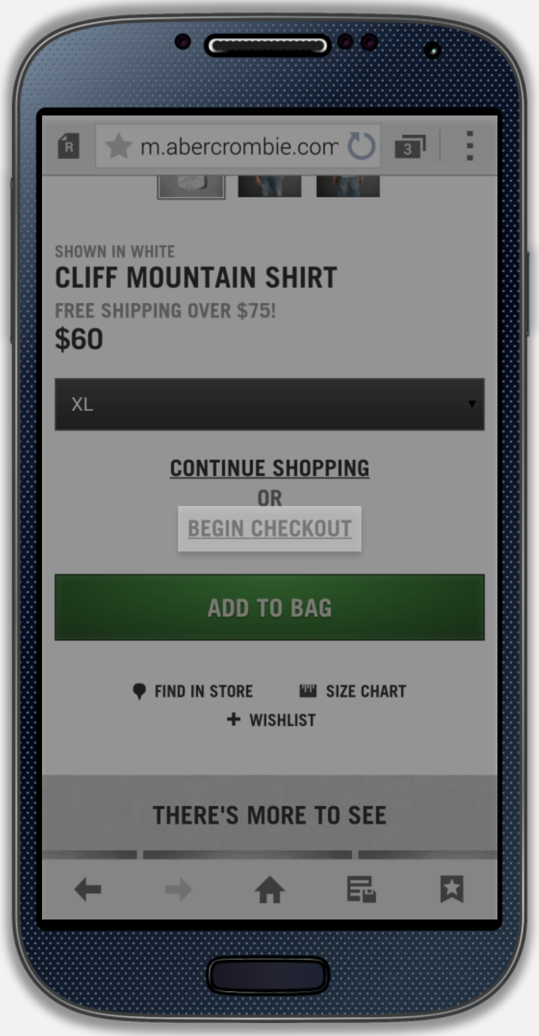
0

Prepare

Web App

FIDO Server

UAF Authentication



m.abercrombie.com

SHOWN IN WHITE

CLIFF MOUNTAIN SHIRT

FREE SHIPPING OVER $75!

$60

XL

CONTINUE SHOPPING

OR

BEGIN CHECKOUT

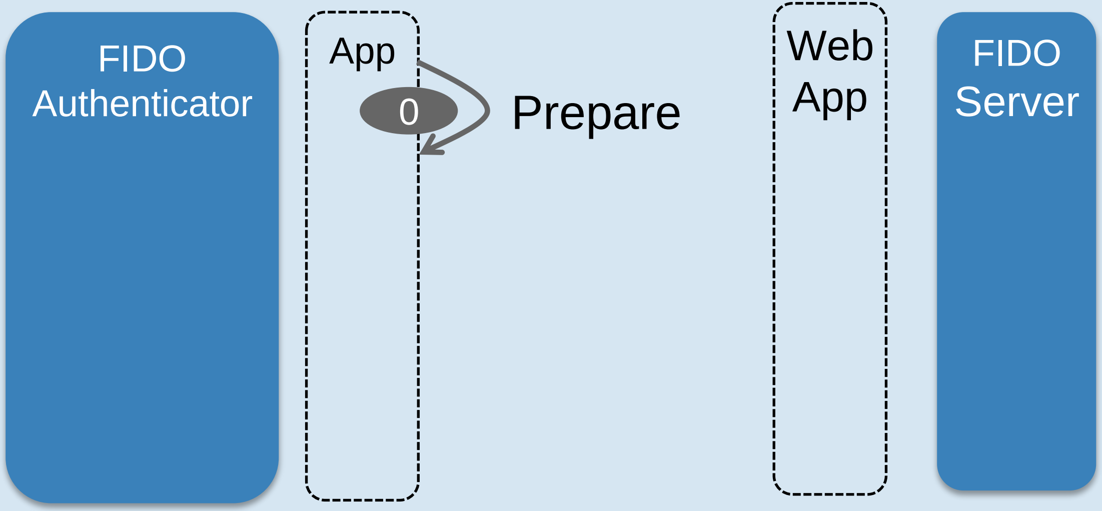
ADD TO BAG

FIND IN STORE

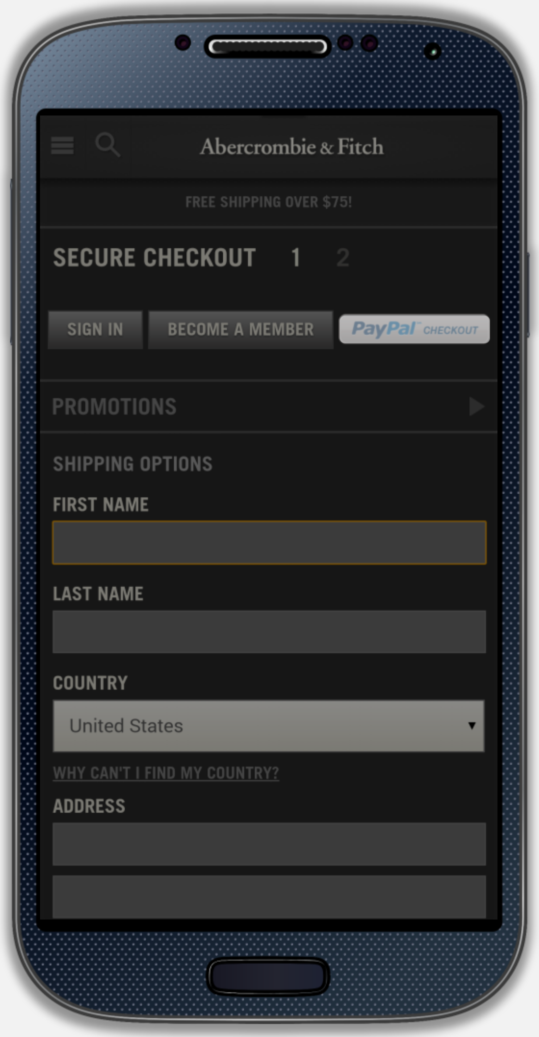
SIZE CHART

WISHLIST

THERE'S MORE TO SEE



UAF Authentication



Abercrombie & Fitch

FREE SHIPPING OVER $75!

SECURE CHECKOUT 1 2

SIGN IN | BECOME A MEMBER | PayPal CHECKOUT

PROMOTIONS

SHIPPING OPTIONS

FIRST NAME

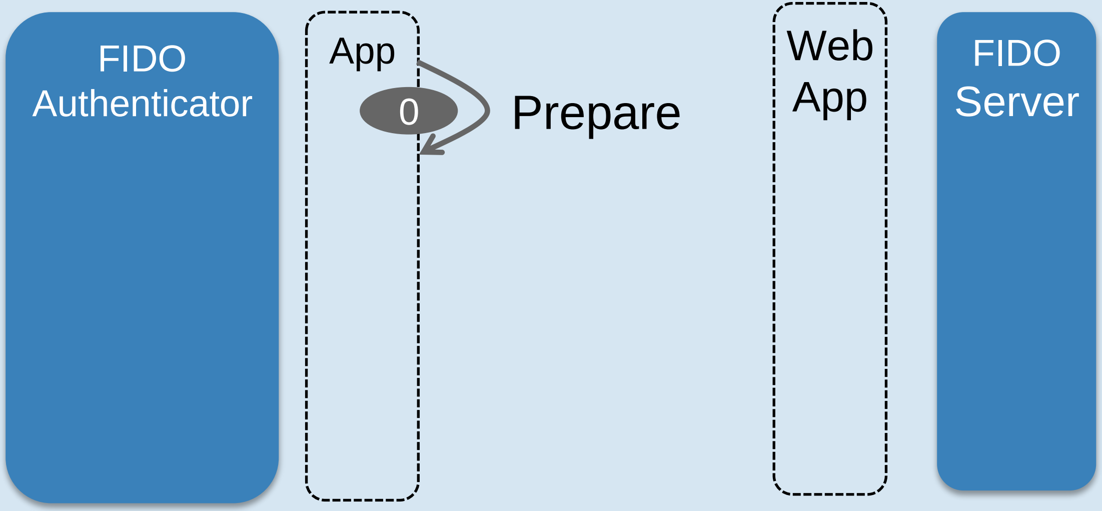
LAST NAME

COUNTRY

United States

WHY CAN'T I FIND MY COUNTRY?

ADDRESS



FIDO Authenticator

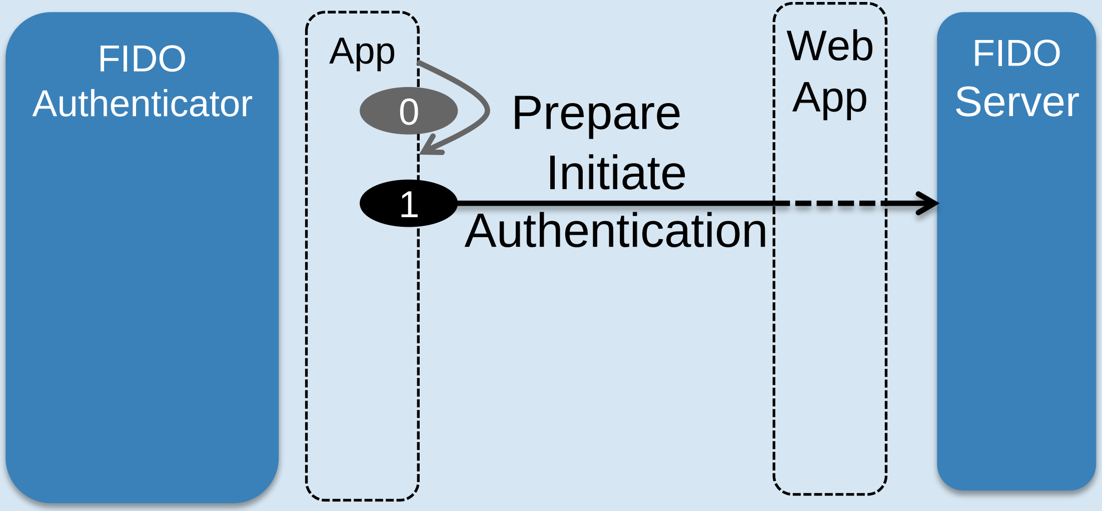
App

0 Prepare

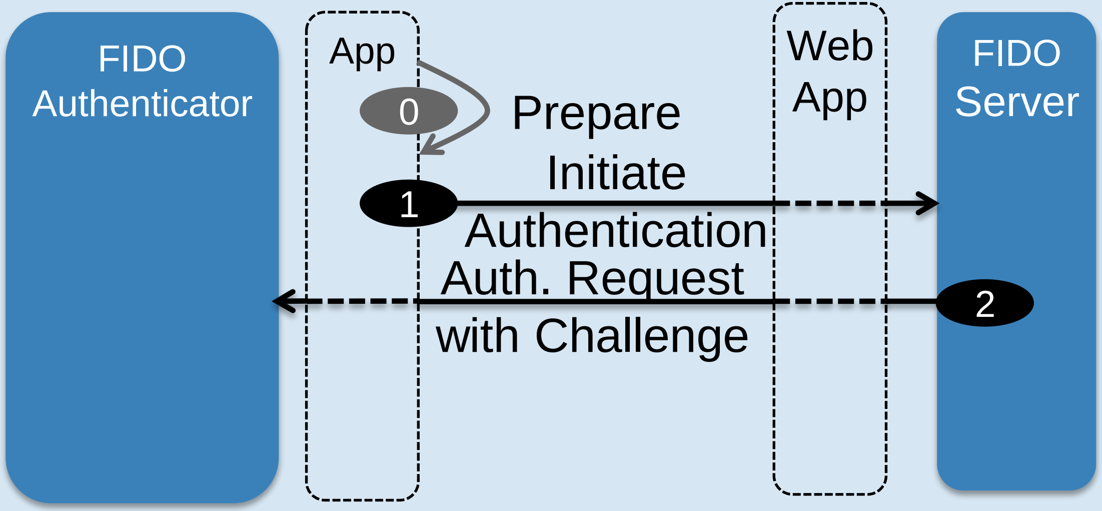
Web App

FIDO Server

UAF Authentication



UAF Authentication

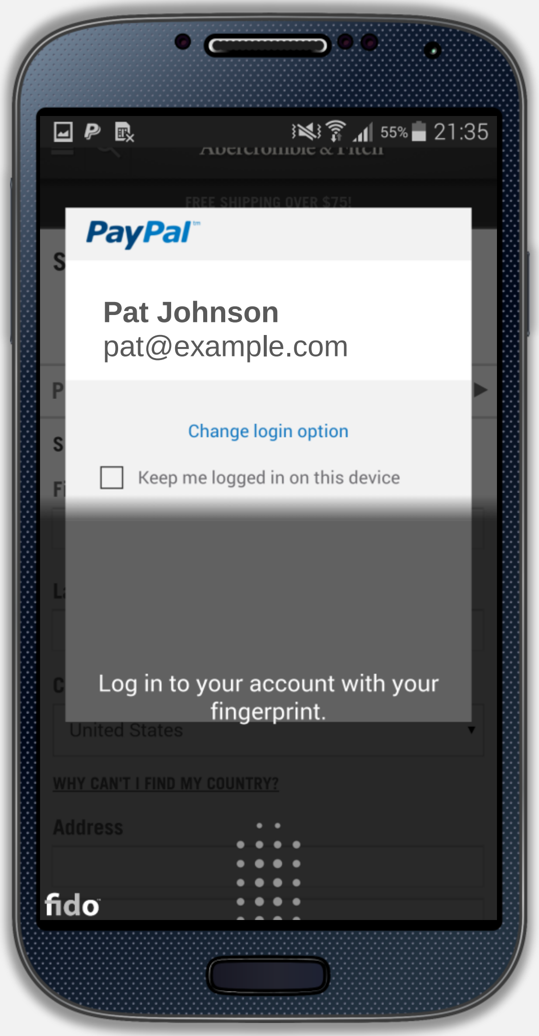


0 Prepare

1 Initiate Authentication

2 Auth. Request with Challenge

UAF Authentication



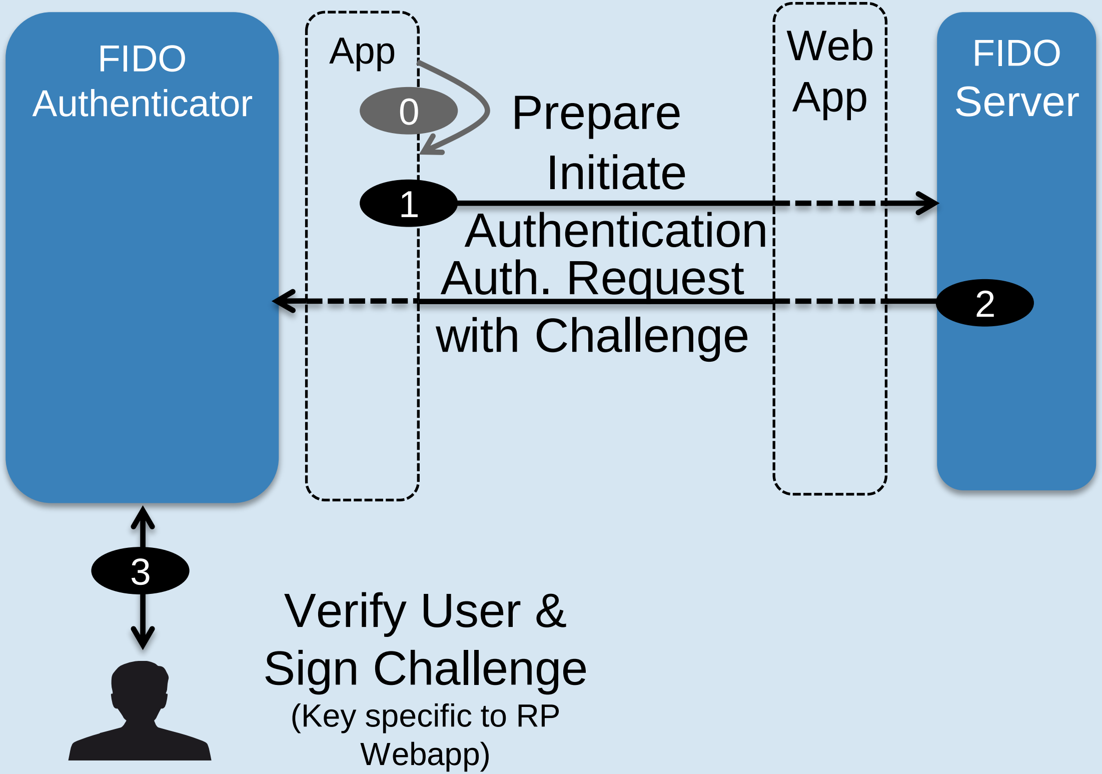
PayPal

Pat Johnson
pat@example.com

Change login option

□ Keep me logged in on this device

Log in to your account with your fingerprint.



FIDO Authenticator

App

Web App

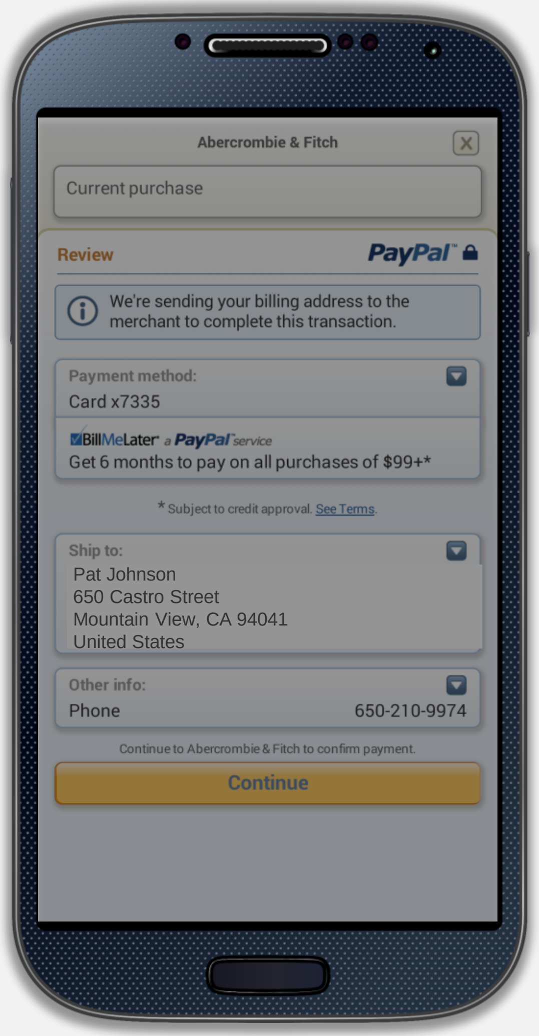
FIDO Server

0 Prepare

1 Initiate Authentication

2 Auth. Request with Challenge

3 Verify User & Sign Challenge (Key specific to RP Webapp)



Abercrombie & Fitch

Current purchase

Review

PayPal

We're sending your billing address to the merchant to complete this transaction.

Payment method:
Card x7335

BillMeLater a PayPal service
Get 6 months to pay on all purchases of $99+*

* Subject to credit approval. See Terms.

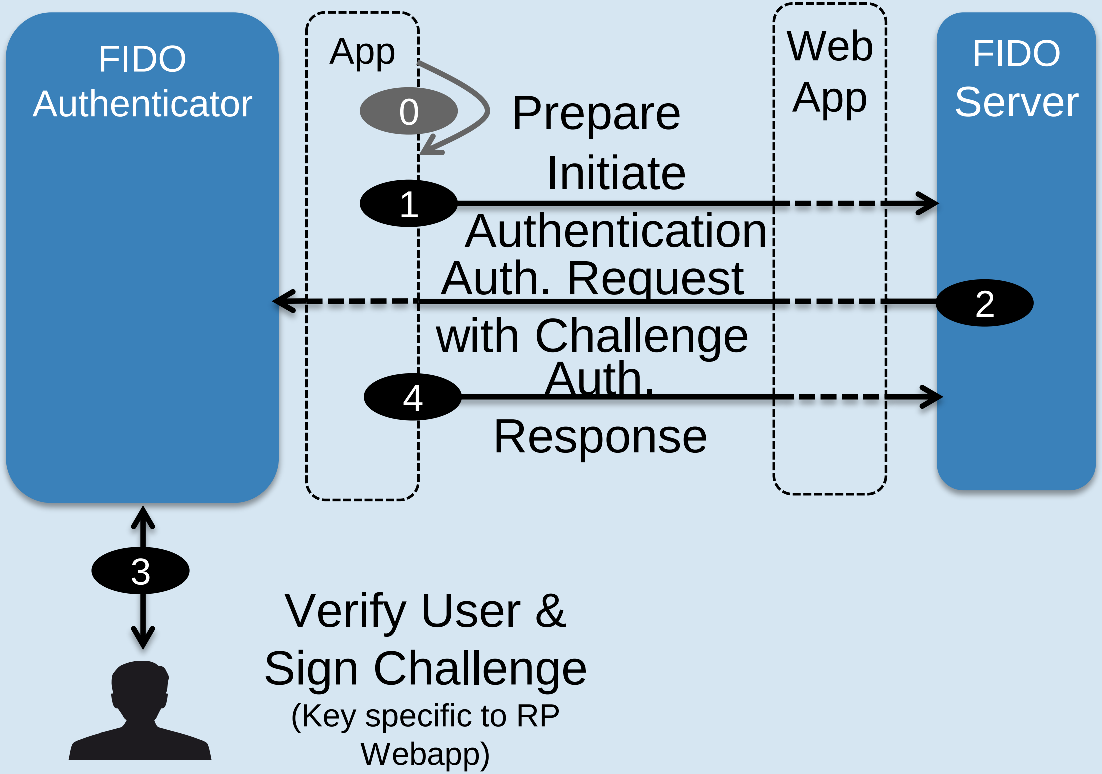
Ship to:
Pat Johnson
650 Castro Street
Mountain View, CA 94041
United States

Other info:

Phone	650-210-9974

Continue to Abercrombie & Fitch to confirm payment.

UAF Authentication



FIDO Authenticator

App

Web App

FIDO Server

0 Prepare

1 Initiate Authentication

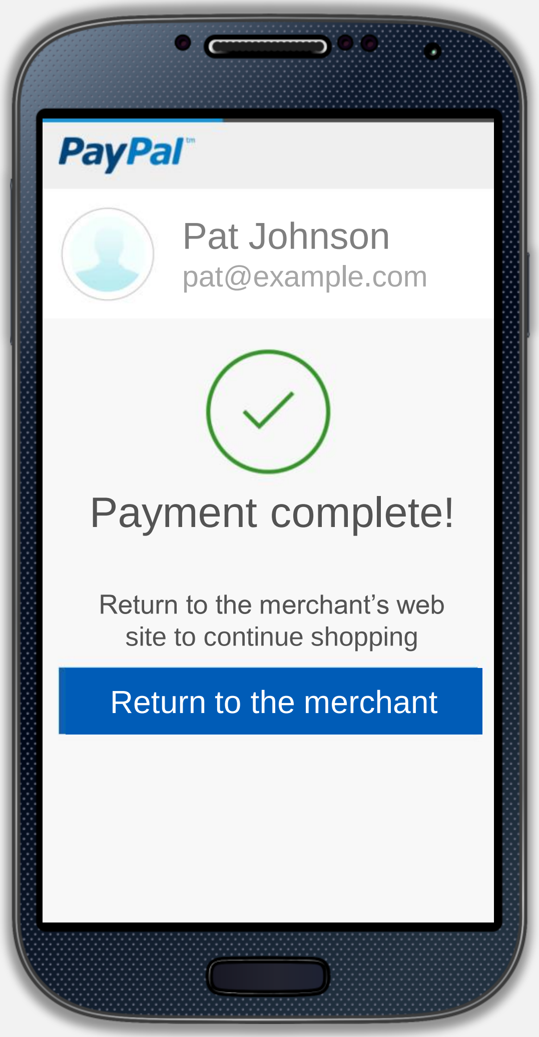
2 Auth. Request with Challenge

4 Auth. Response

3

Verify User & Sign Challenge
(Key specific to RP Webapp)

UAF Authentication



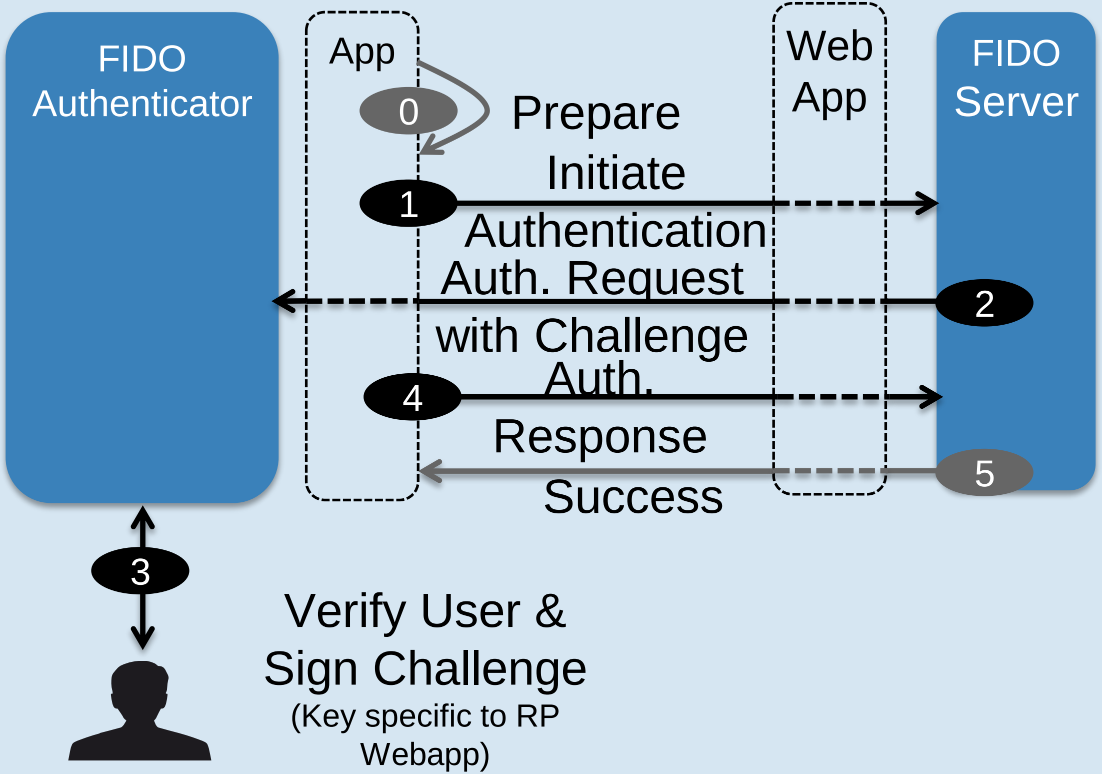
PayPal

Pat Johnson
pat@example.com

Payment complete!

Return to the merchant’s web site to continue shopping

Return to the merchant



FIDO Authenticator

App

Web App

FIDO Server

0 Prepare

1 Initiate Authentication

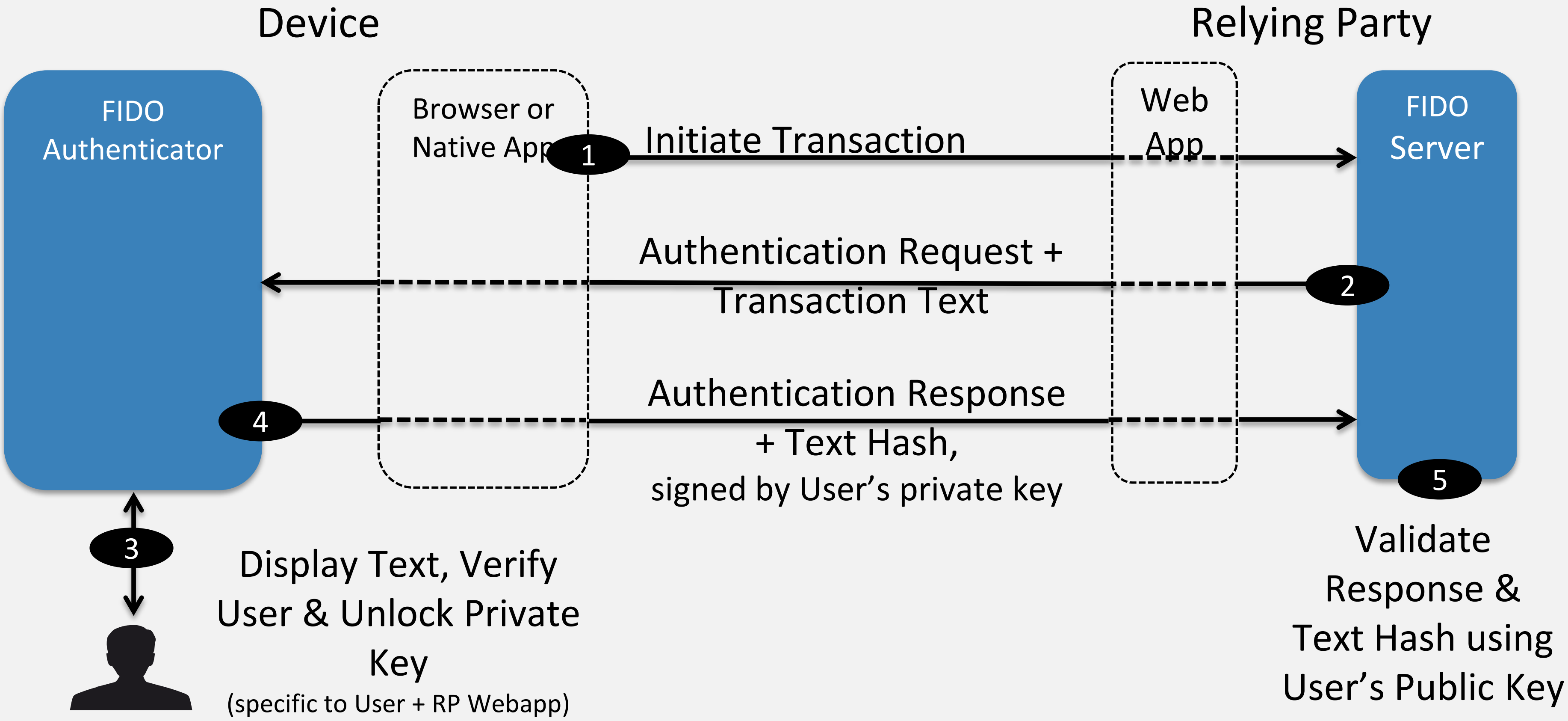
2 Auth. Request with Challenge

3 Verify User & Sign Challenge
(Key specific to RP Webapp)

4 Auth. Response

5 Success

Transaction Confirmation



Device

Relying Party

FIDO Authenticator

Browser or Native App

Web App

FIDO Server

1 Initiate Transaction

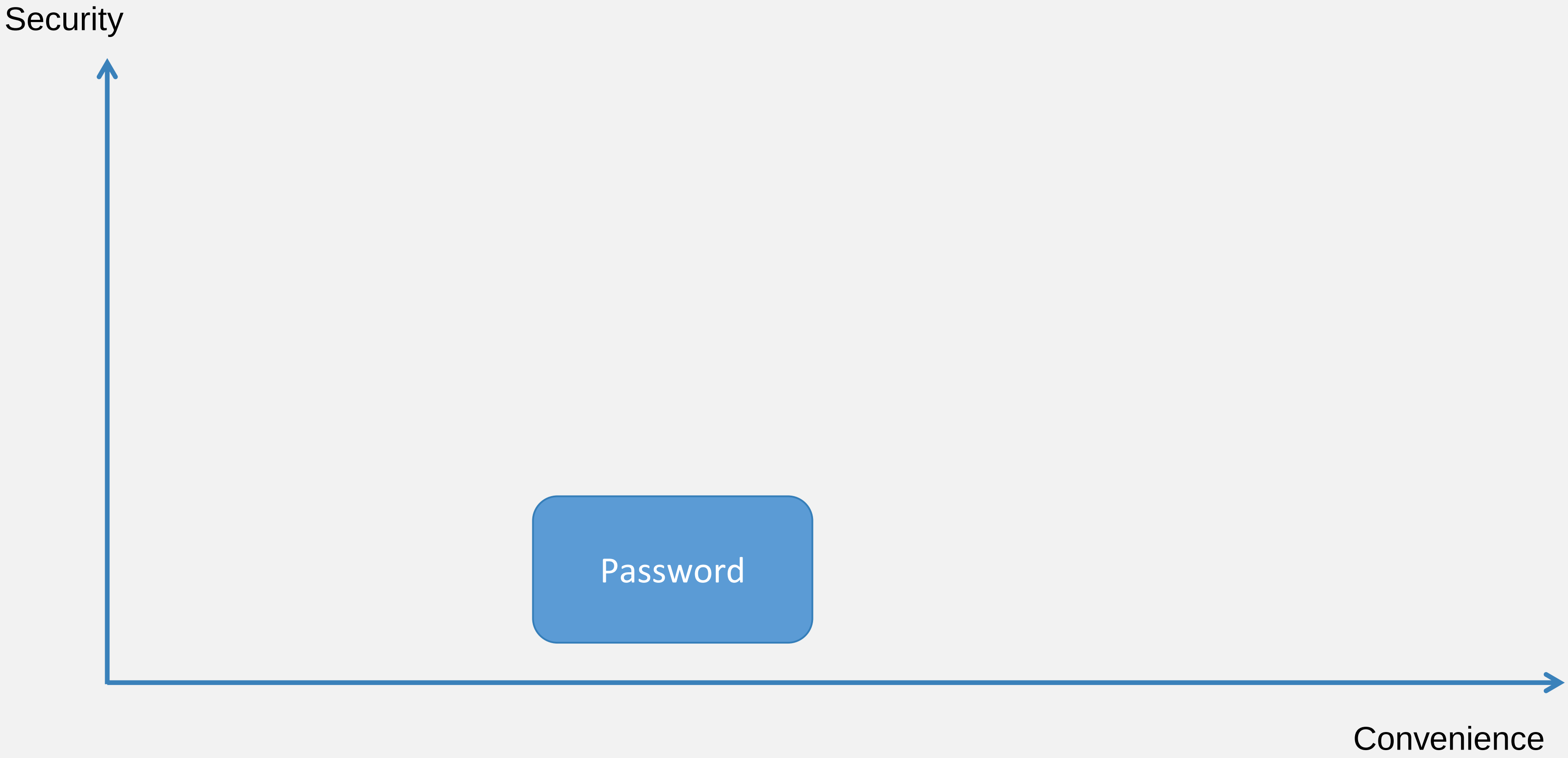
2 Authentication Request + Transaction Text

3 Display Text, Verify User & Unlock Private Key (specific to User + RP Webapp)

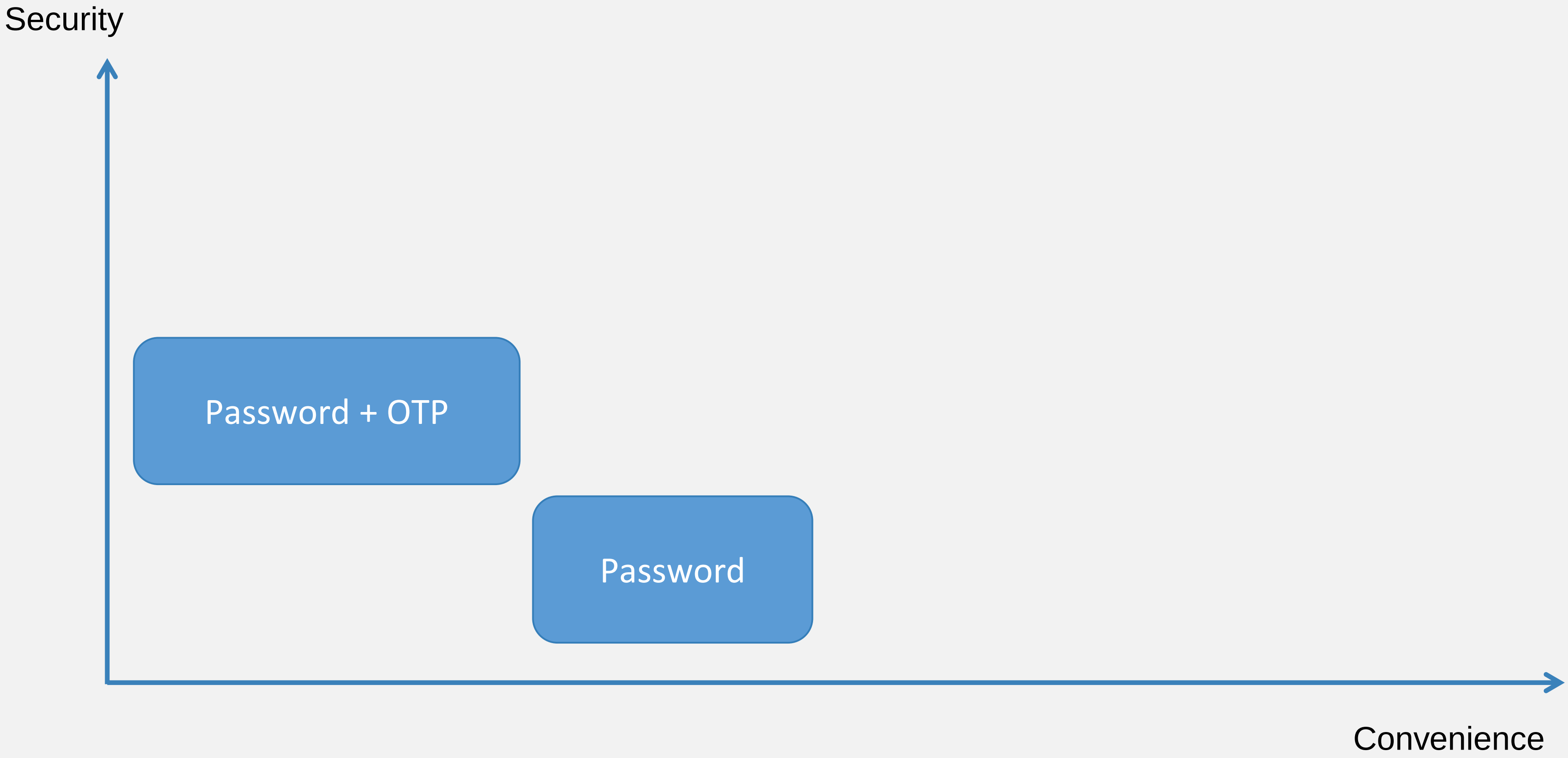
4 Authentication Response + Text Hash, signed by User’s private key

5 Validate Response & Text Hash using User’s Public Key

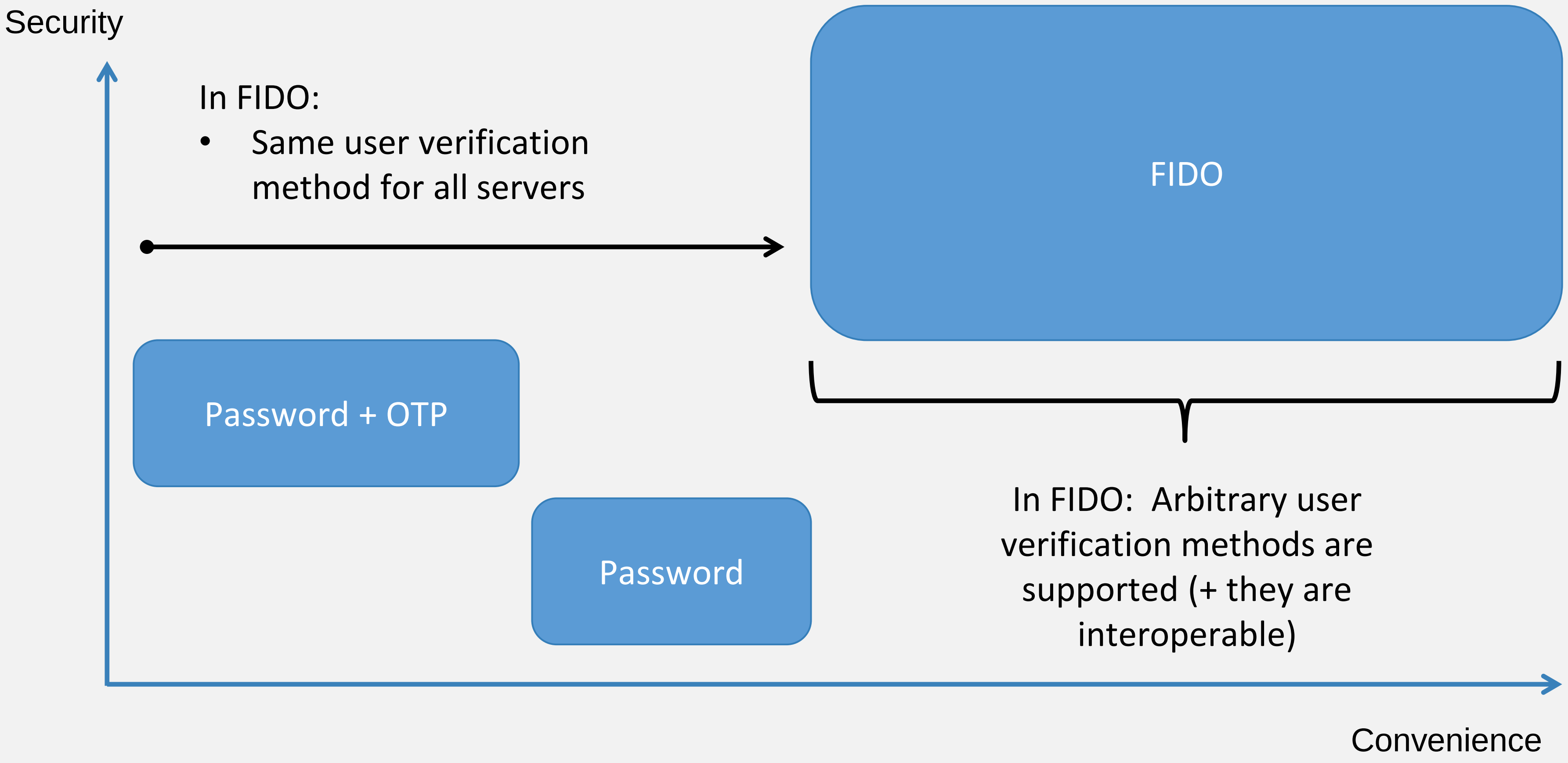
Convenience & Security



Convenience & Security



Convenience & Security



Security

In FIDO:

- Same user verification method for all servers

FIDO

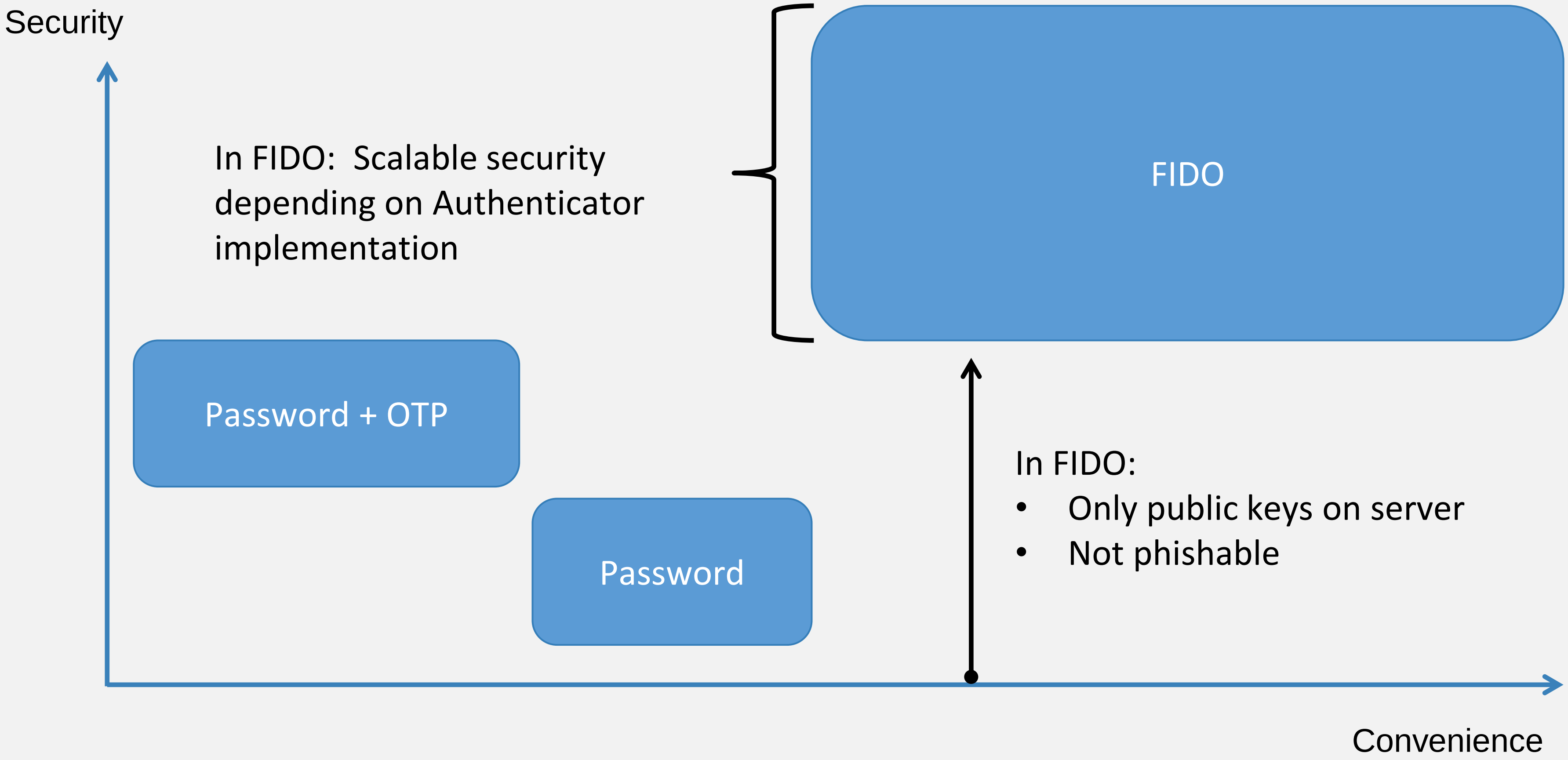
Password + OTP

Password

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

Convenience

Convenience & Security

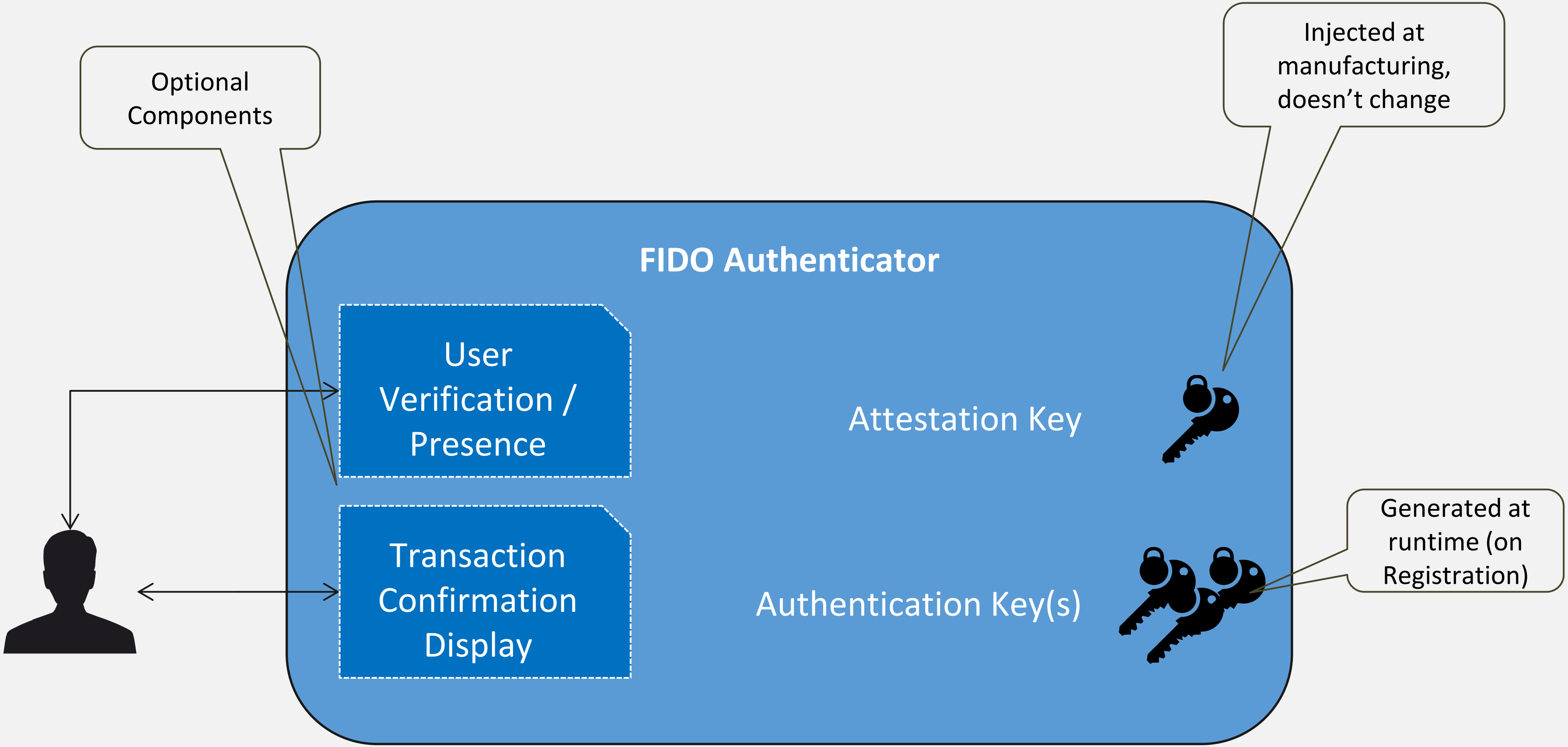


In FIDO: Scalable security depending on Authenticator implementation

In FIDO:

- Only public keys on server
- Not phishable

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)

What about rubber fingers?

Protection methods in FIDO

1. Attacker needs access to the Authenticator and swipe rubber finger on it. This makes it a non-scalable attack.
2. Authenticators might implement presentation attack detection methods.

Remember:

Creating hundreds of millions of rubber fingers + stealing the related authenticators is expensive. Stealing hundreds of millions of passwords from a server has low cost per password.

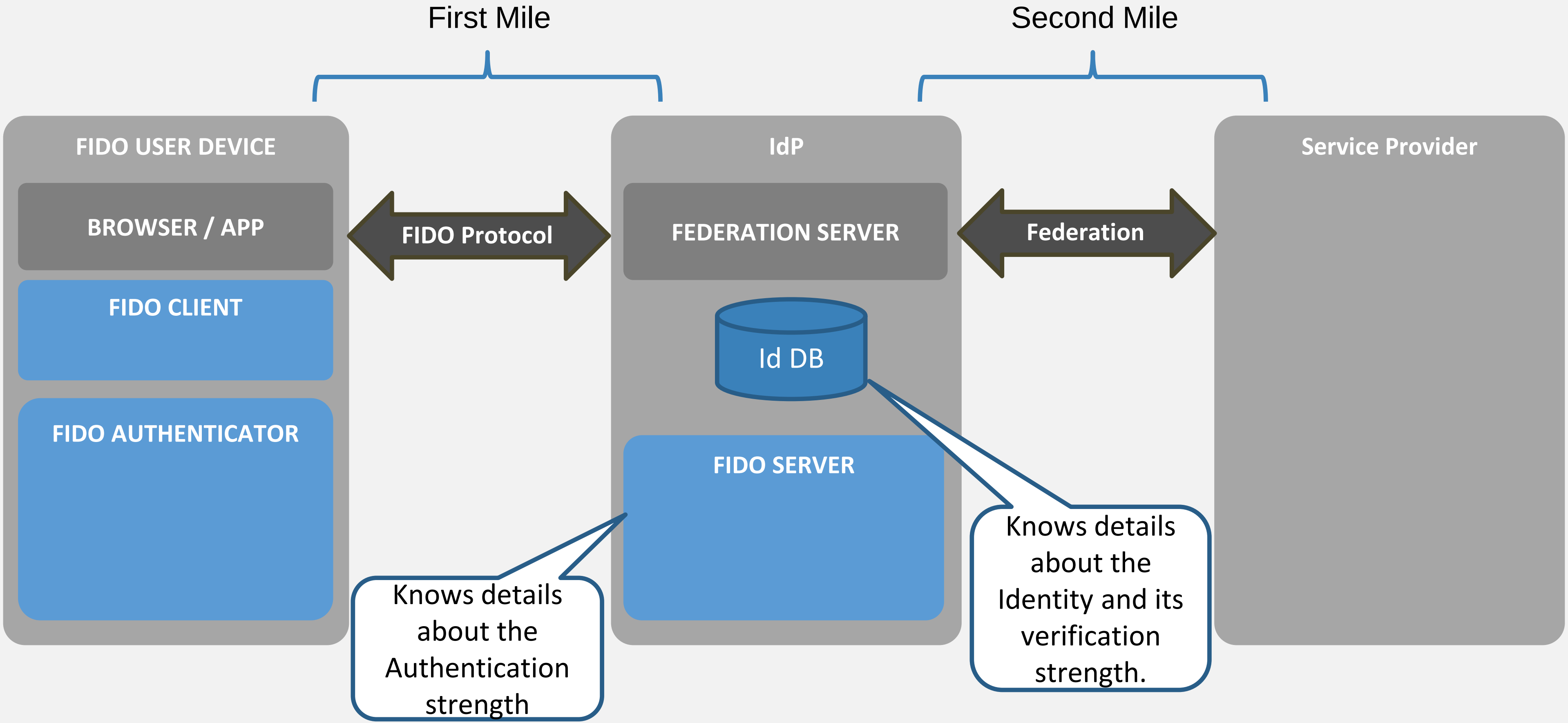
But I can’t revoke my finger…

- Protection methods in FIDO

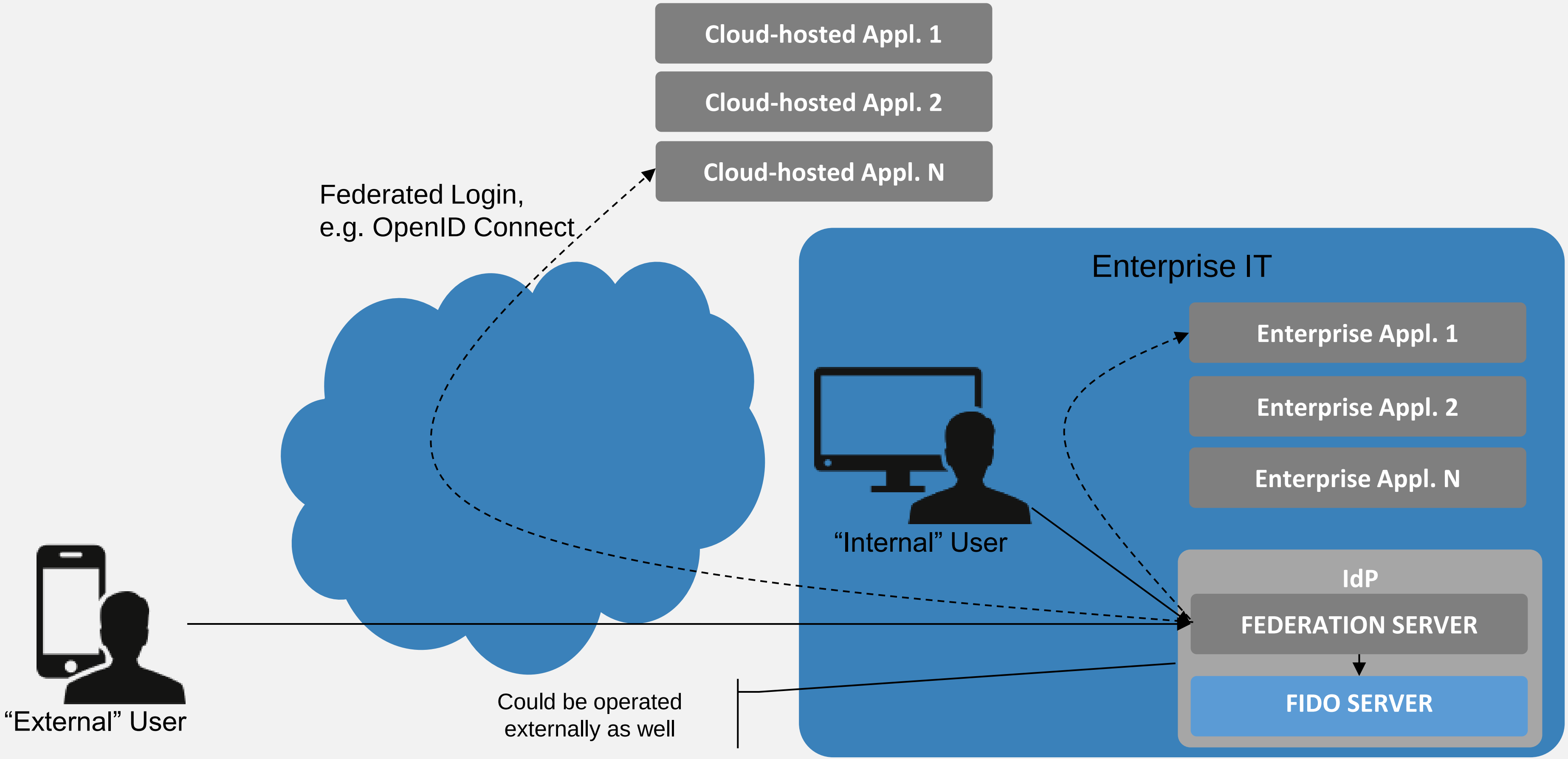
  You don’t need to revoke your finger, you can simply de-register the old (=attacked) authenticator. Then,

  1. Get a new authenticator
  2. Enroll your finger (or iris, …) to it
  3. Register the new authenticator to the service

FIDO & Federation



FIDO & Federation in Enterprise



FIDO UAF Enabled Products

Samsung

Galaxy S6, S6 Edge, S6 Edge+
Galaxy Tab S2 8“+9.7“
Galaxy Note 5

Galaxy S5, S5 Mini, S5 Plus
Galaxy Alpha
Galaxy Note 4, Note 4 Edge
Galaxy Tab S 8.4“+10.5“

Sony

Xperia Z5, Z5 Compact,
Z5 Premium

Sharp

Aquos Zeta SH-03G, SH01H

Fujitsu

Arrows NX F-04G, Fit F-01H,
NX F-02H

OEM Enabled Smartphones & Tablets

Downloads

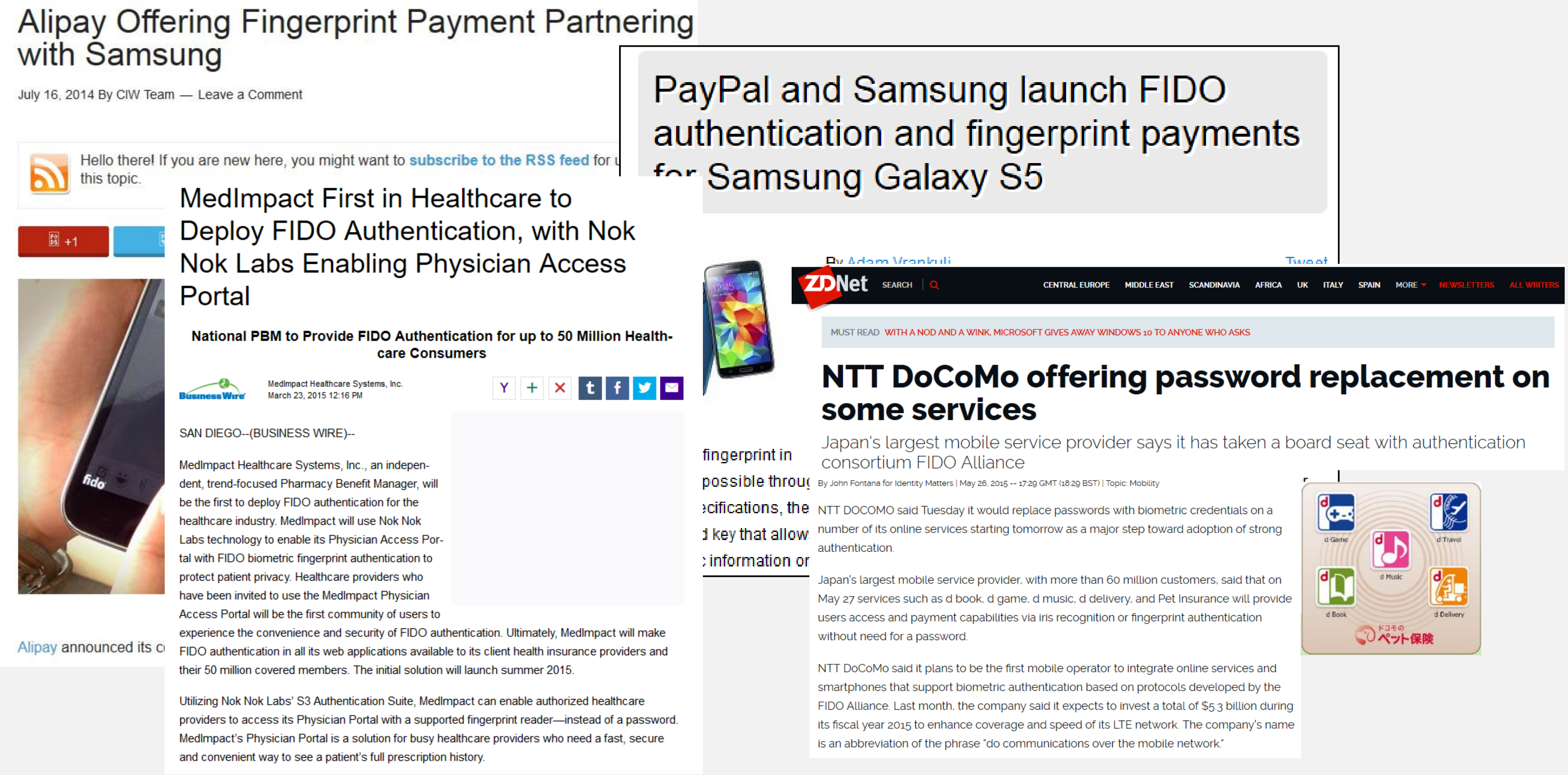
Clients available for these operating systems:

Windows 7 Windows 8 android iOS

Software Authenticator Examples:
Speaker/Face recognition, PIN, QR Code, etc.

Aftermarket Hardware Authenticator Examples:
USB fingerprint scanner, MicroSD Secure Element

FIDO is used Today



Alipay Offering Fingerprint Payment Partnering with Samsung

July 16, 2014 By CIW Team — Leave a Comment

Hello there! If you are new here, you might want to **subscribe to the RSS feed** for u this topic.

+1

Alipay announced its c

PayPal and Samsung launch FIDO authentication and fingerprint payments for Samsung Galaxy S5

By Adam Vrankulj

Tweet

fingerprint in
possible throu
ecifications, the
key that allow
information or

MedImpact First in Healthcare to Deploy FIDO Authentication, with Nok Nok Labs Enabling Physician Access Portal

National PBM to Provide FIDO Authentication for up to 50 Million Health-care Consumers

Business Wire

MedImpact Healthcare Systems, Inc.
March 23, 2015 12:16 PM

SAN DIEGO--(BUSINESS WIRE)--

MedImpact Healthcare Systems, Inc., an independent, trend-focused Pharmacy Benefit Manager, will be the first to deploy FIDO authentication for the healthcare industry. MedImpact will use Nok Nok Labs technology to enable its Physician Access Portal with FIDO biometric fingerprint authentication to protect patient privacy. Healthcare providers who have been invited to use the MedImpact Physician Access Portal will be the first community of users to experience the convenience and security of FIDO authentication. Ultimately, MedImpact will make FIDO authentication in all its web applications available to its client health insurance providers and their 50 million covered members. The initial solution will launch summer 2015.

Utilizing Nok Nok Labs' S3 Authentication Suite, MedImpact can enable authorized healthcare providers to access its Physician Portal with a supported fingerprint reader—instead of a password. MedImpact's Physician Portal is a solution for busy healthcare providers who need a fast, secure and convenient way to see a patient's full prescription history.

ZDNet SEARCH | CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ WITH A NOD AND A WINK, MICROSOFT GIVES AWAY WINDOWS 10 TO ANYONE WHO ASKS

NTT DoCoMo offering password replacement on some services

Japan's largest mobile service provider says it has taken a board seat with authentication consortium FIDO Alliance

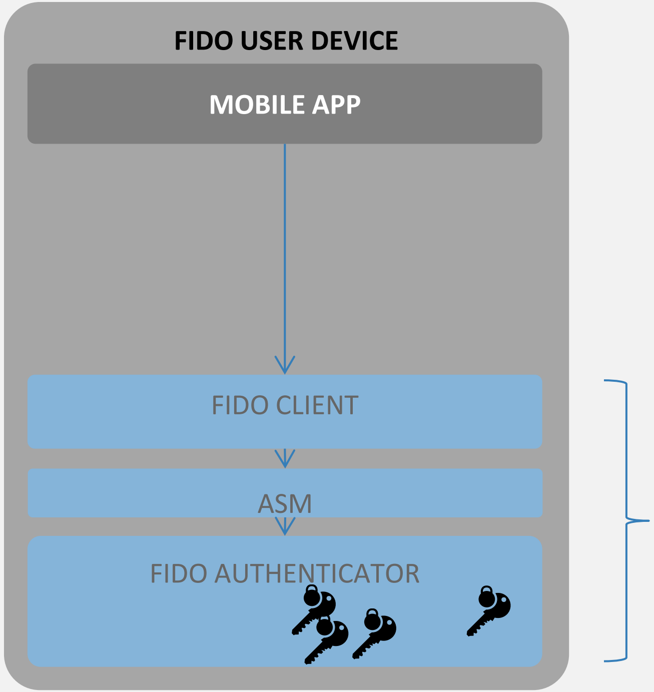
By John Fontana for Identity Matters | May 26, 2015 -- 17:29 GMT (18:29 BST) | Topic: Mobility

NTT DOCOMO said Tuesday it would replace passwords with biometric credentials on a number of its online services starting tomorrow as a major step toward adoption of strong authentication.

Japan's largest mobile service provider, with more than 60 million customers, said that on May 27 services such as d book, d game, d music, d delivery, and Pet Insurance will provide users access and payment capabilities via iris recognition or fingerprint authentication without need for a password.

NTT DoCoMo said it plans to be the first mobile operator to integrate online services and smartphones that support biometric authentication based on protocols developed by the FIDO Alliance. Last month, the company said it expects to invest a total of $5.3 billion during its fiscal year 2015 to enhance coverage and speed of its LTE network. The company's name is an abbreviation of the phrase "do communications over the mobile network."

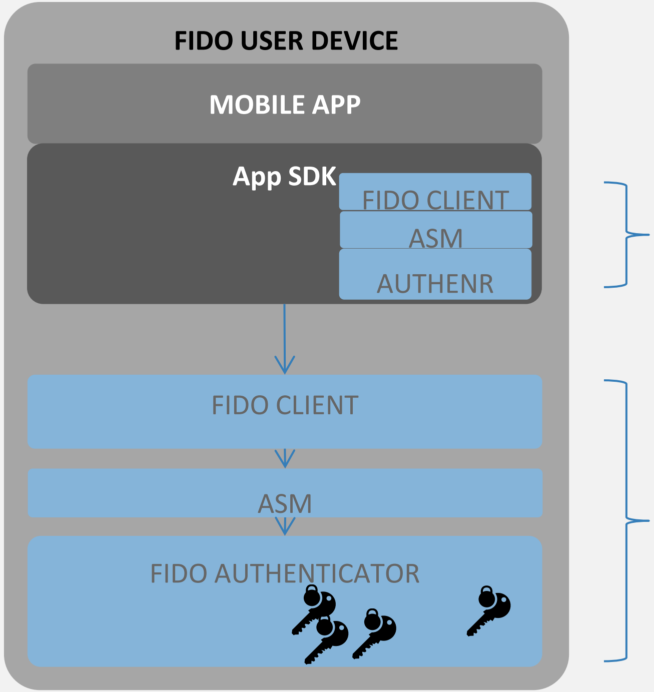
Typical RP Deployment



Challenge: Old devices do not have a native FIDO Stack

Native FIDO Stack
(not on old devices)

Typical RP Deployment

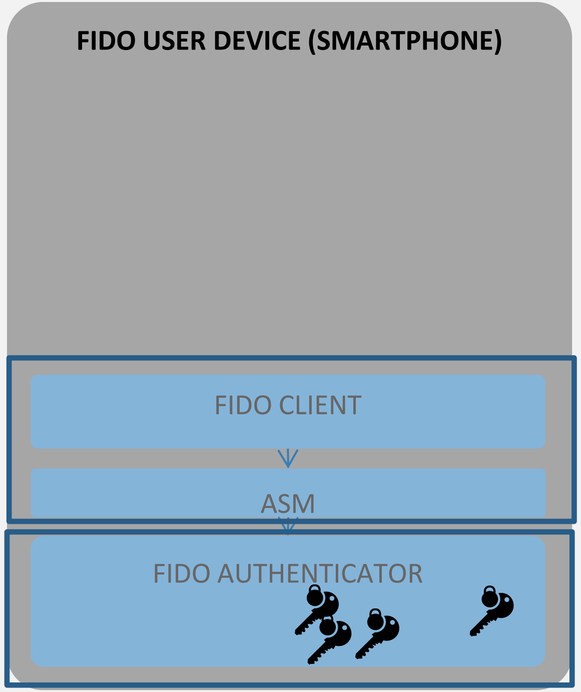


Challenge: Old devices do not have a native FIDO Stack
Solution: embed FIDO Stack in App SDK

Embedded FIDO Stack

Native FIDO Stack
(not on old devices)

Typical Native FIDO Stack



Rich Execution Environment,
e.g. Android.

Trusted Execution
Environment (TEE)

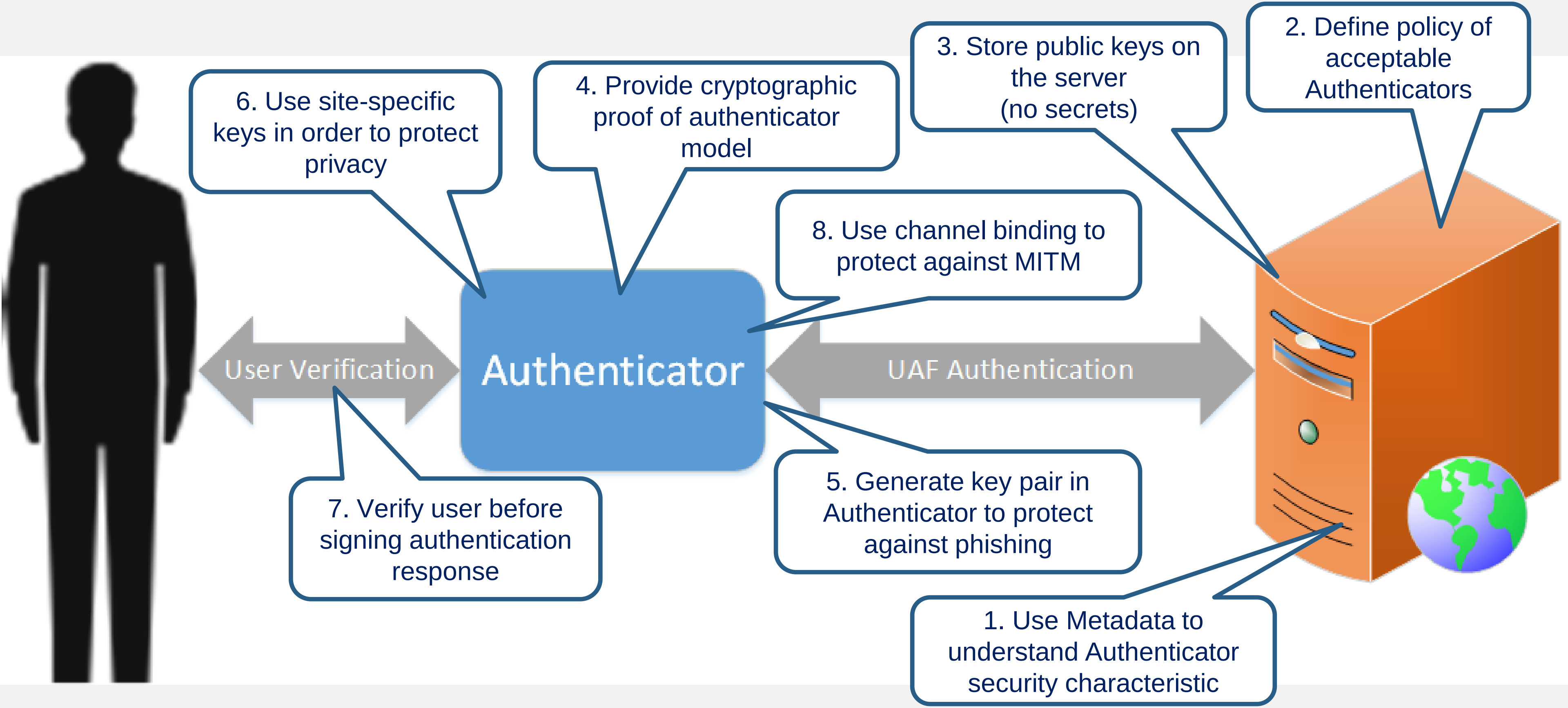
Fingerprint is mostly used today.
Typically on high-end devices.

Some devices use eye/iris as modality.
No need for expensive FP Sensors.

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

How does FIDO UAF work?



1. Use Metadata to understand Authenticator security characteristic

2. Define policy of acceptable Authenticators

3. Store public keys on the server (no secrets)

4. Provide cryptographic proof of authenticator model

5. Generate key pair in Authenticator to protect against phishing

6. Use site-specific keys in order to protect privacy

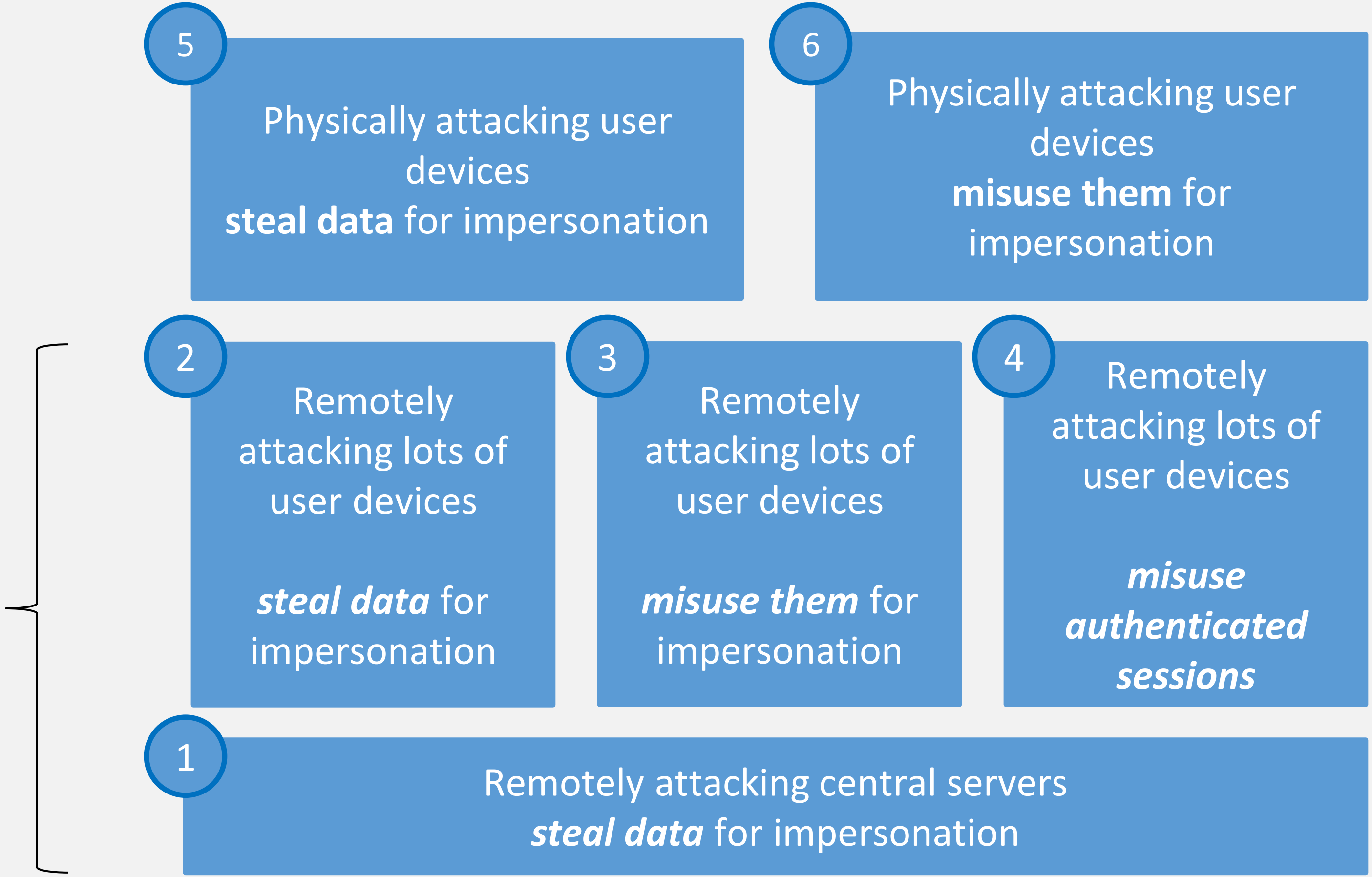
7. Verify user before signing authentication response

8. Use channel binding to protect against MITM

Classifying Threats

Physical attacks possible on lost or stolen devices
(≈3% in the US in 2013)

Scalable attacks



5

Physically attacking user devices
steal data for impersonation

6

Physically attacking user devices
misuse them for impersonation

2

Remotely attacking lots of user devices

steal data for impersonation

3

Remotely attacking lots of user devices

misuse them for impersonation

4

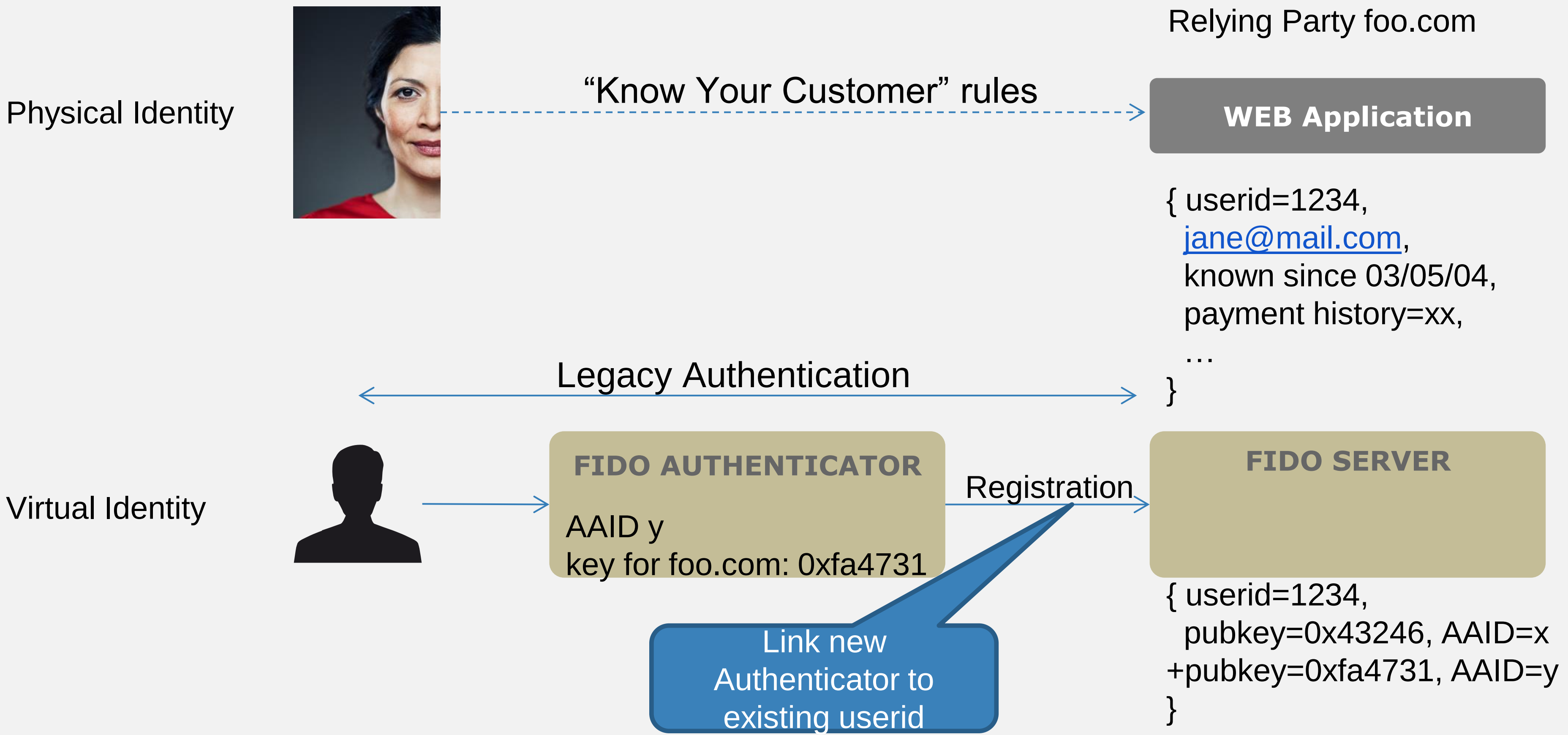
Remotely attacking lots of user devices

misuse authenticated sessions

1

Remotely attacking central servers
steal data for impersonation

Registration Overview (2)



Relying Party foo.com

Physical Identity

“Know Your Customer” rules

WEB Application

{ userid=1234,
  jane@mail.com,
  known since 03/05/04,
  payment history=xx,
  …
}

Legacy Authentication

Virtual Identity

FIDO AUTHENTICATOR

AAID y
key for foo.com: 0xfa4731

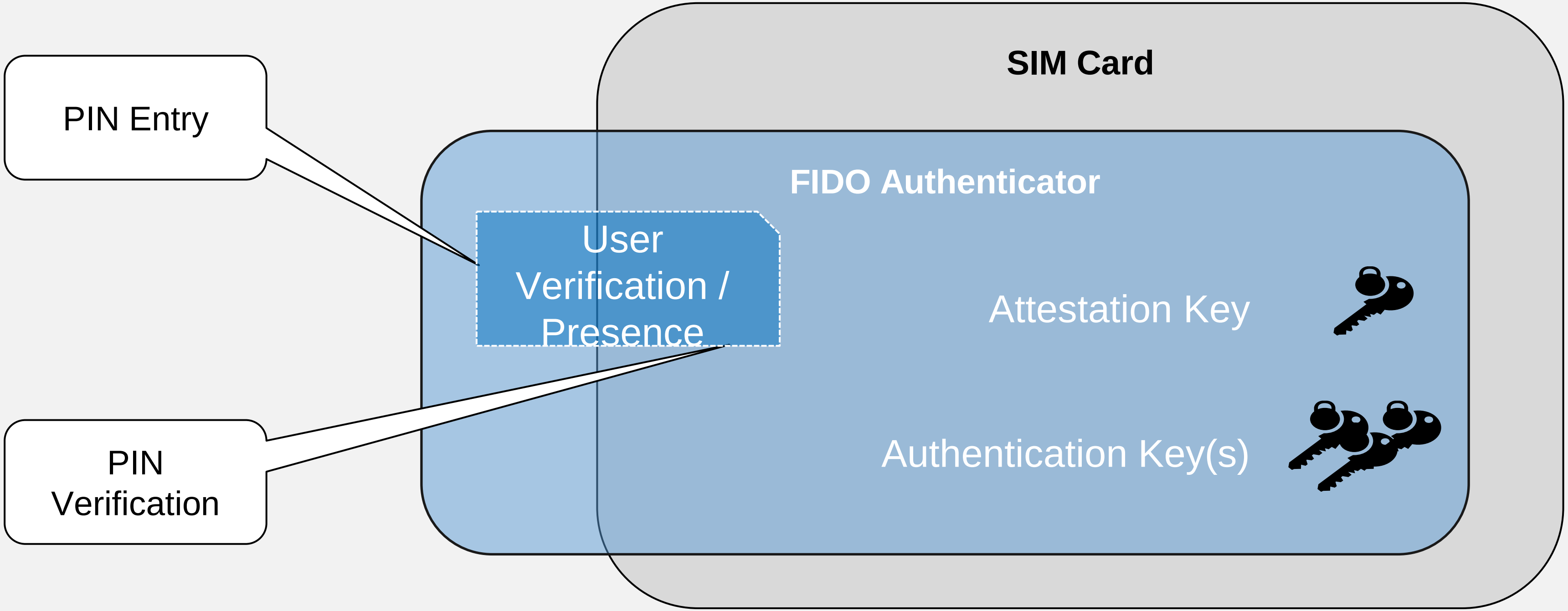
Registration

FIDO SERVER

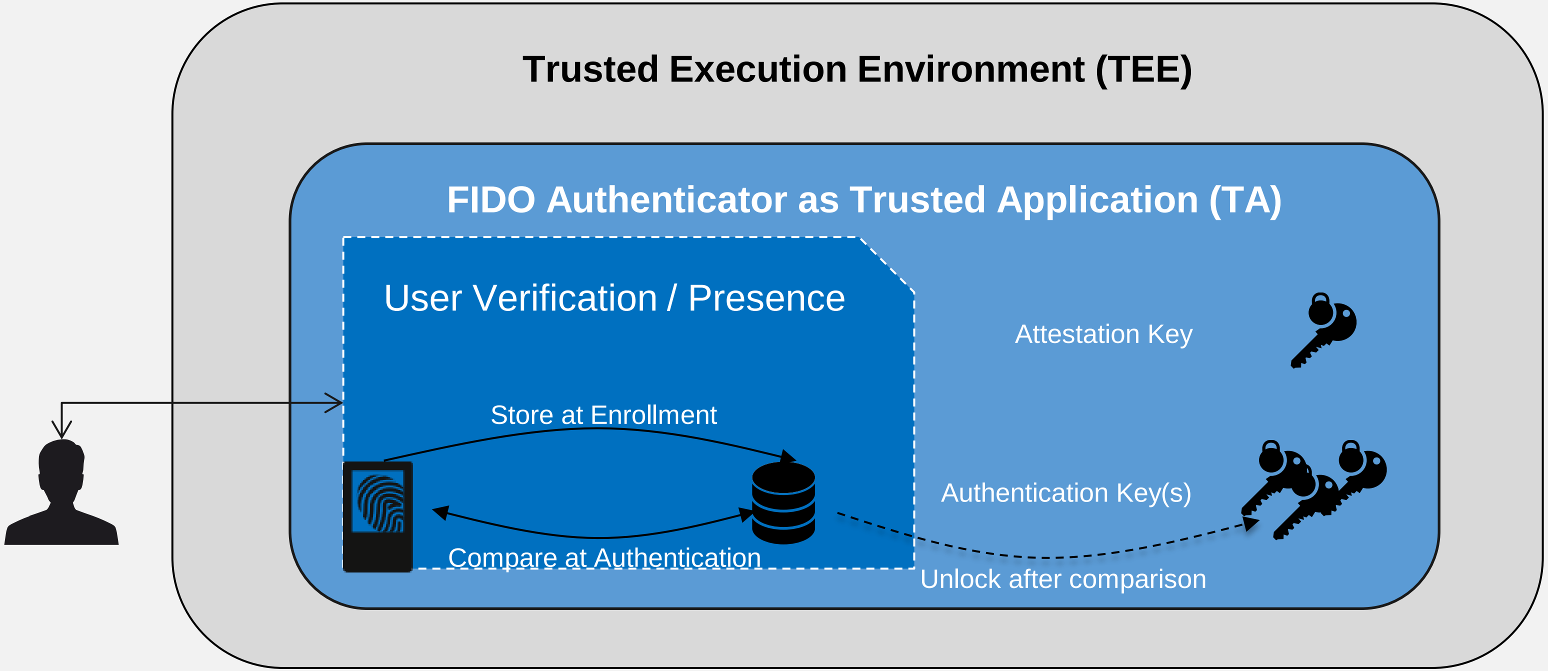
Link new Authenticator to existing userid

{ userid=1234,
  pubkey=0x43246, AAID=x
+pubkey=0xfa4731, AAID=y
}

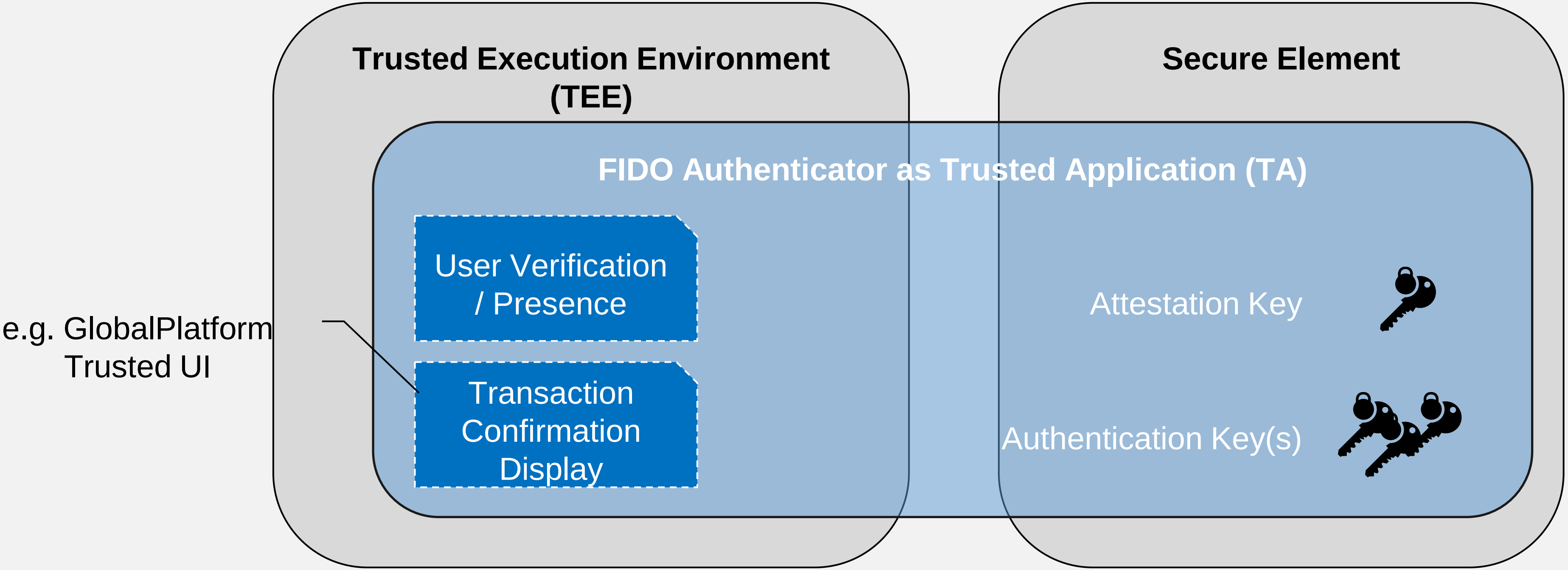
Using Secure Hardware



Client Side Biometrics


Trusted Execution Environment (TEE)
FIDO Authenticator as Trusted Application (TA)
User Verification / Presence
Store at Enrollment
Compare at Authentication
Attestation Key
Authentication Key(s)
Unlock after comparison

Combining TEE and SE


Trusted Execution Environment (TEE)
Secure Element
FIDO Authenticator as Trusted Application (TA)
User Verification / Presence
Transaction Confirmation Display
e.g. GlobalPlatform Trusted UI
Attestation Key
Authentication Key(s)