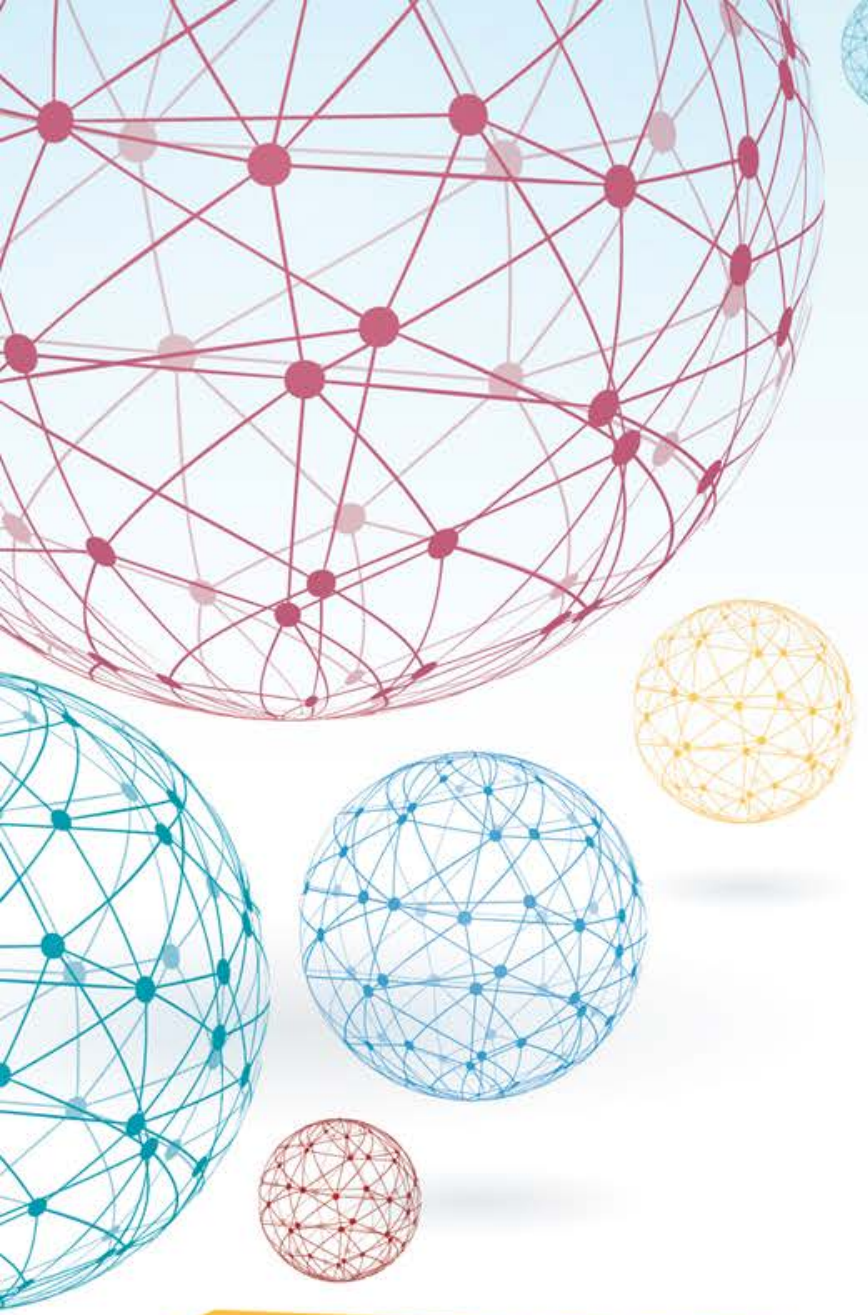
THE FUTURE OF AUTHENTICATION FOR THE INTERNET OF THINGS

FIDO ALLIANCE WEBINAR

MARCH 28, 2017

All Rights Reserved | FIDO Alliance | Copyright 2017



INTRODUCTION TO THE FIDO ALLIANCE

ANDREW SHIKIAR
SENIOR DIRECTOR OF MARKETING
MARCH 28, 2017

All Rights Reserved | FIDO Alliance | Copyright 2017

THE FACTS ON FIDO

The FIDO Alliance is an open, global industry association of 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

300+
FIDO Certified solutions

Available to protect
3 BILLION+
user accounts worldwide

All Rights Reserved | FIDO Alliance | Copyright 2017

DRIVEN BY 250 MEMBERS

Board of Directors comprised of leading global brands and technology providers

+ SPONSOR MEMBERS **+ ASSOCIATE MEMBERS** **+ LIAISON MEMBERS**

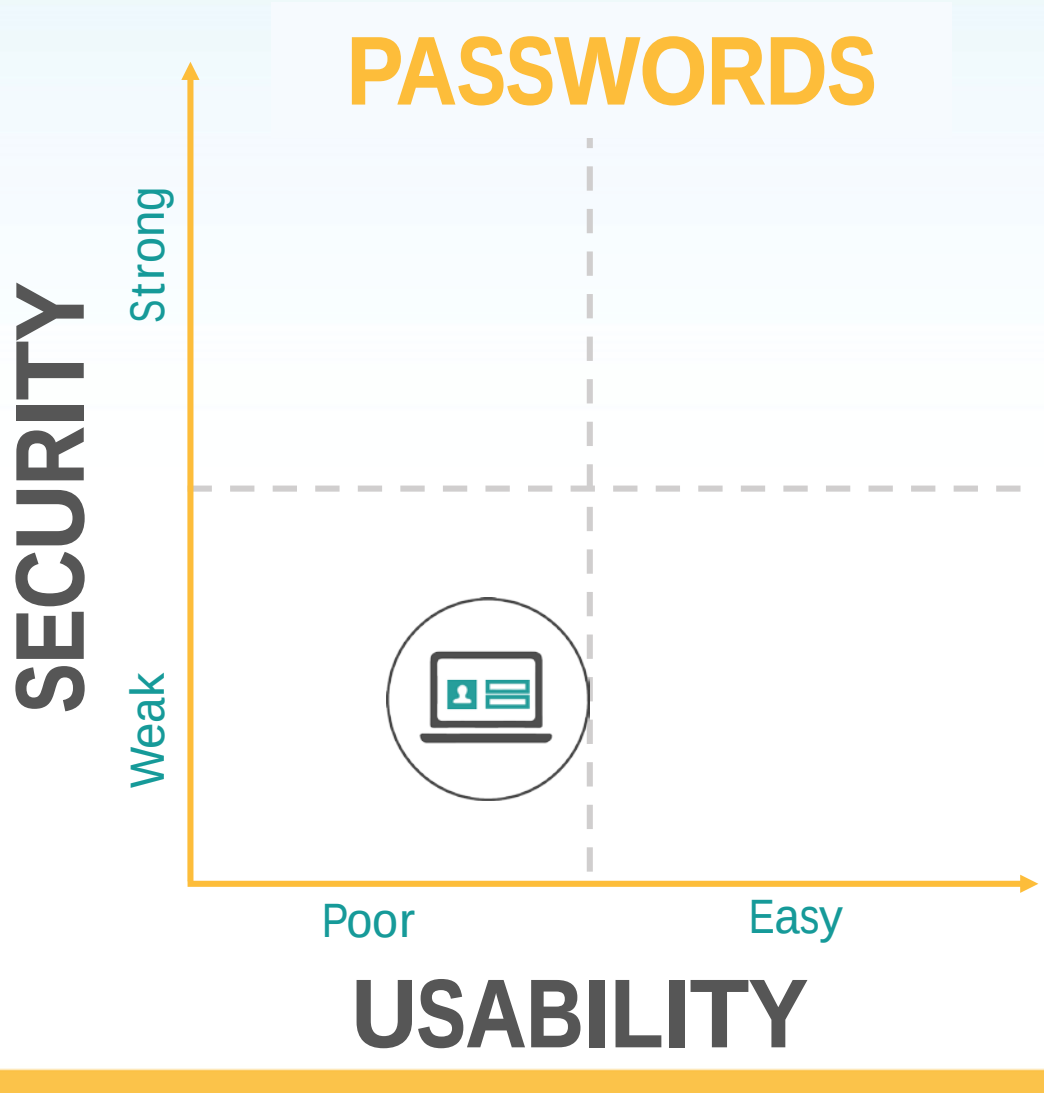
All Rights Reserved | FIDO Alliance | Copyright 2017

WHY FIDO?

The World Has a Password Problem

Usability

For users, they're **clumsy**, **hard to remember** and they **need to be changed** all the time



Security

63% of data breaches in 2015 involved weak, default, or stolen passwords
-Verizon 2016 Data Breach Report

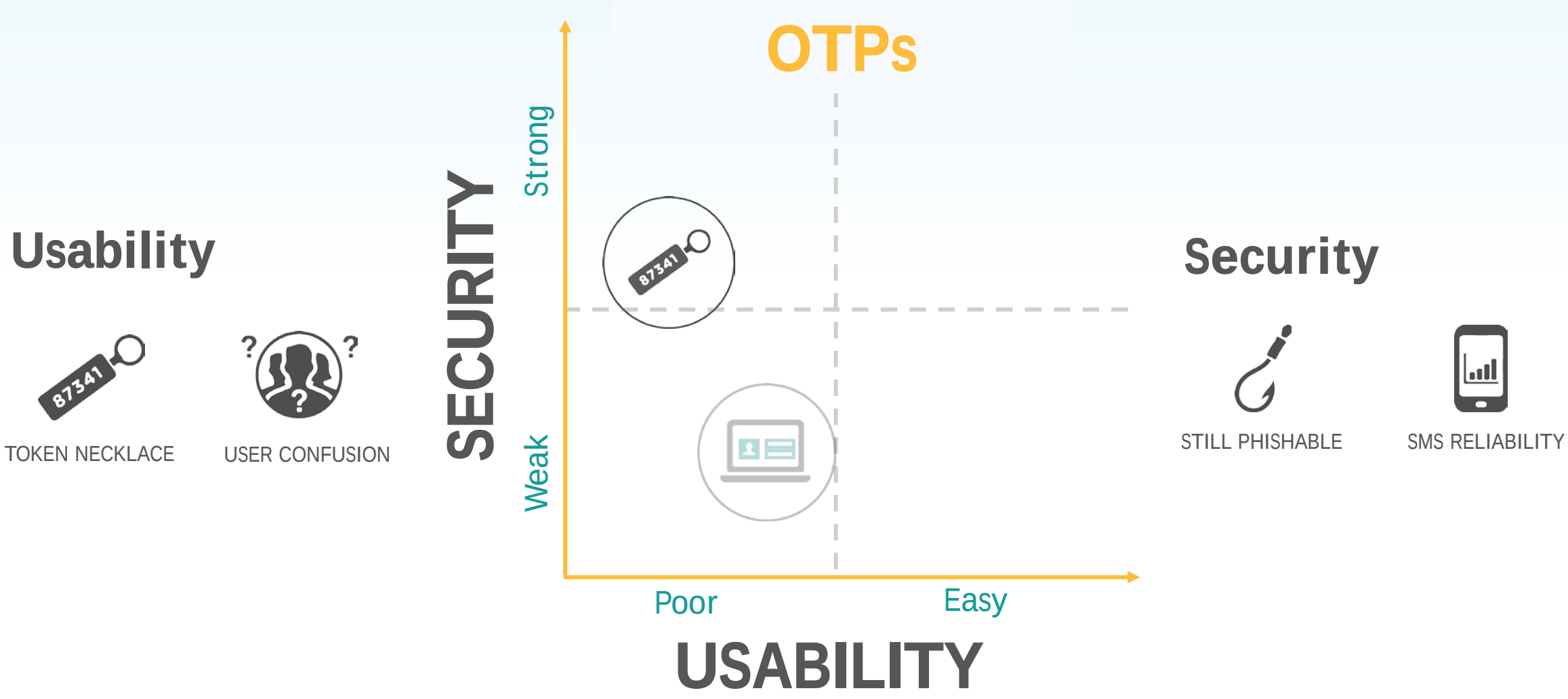
65% Increase in phishing attacks over the number of attacks recorded in 2015[2]
-Anti-Phishing Working Group

There were **1093** data breaches in 2016, **a 40% increase** from 2015
- Identity Theft Resource Center, 2016

All Rights Reserved | FIDO Alliance | Copyright 2017

WHY FIDO?

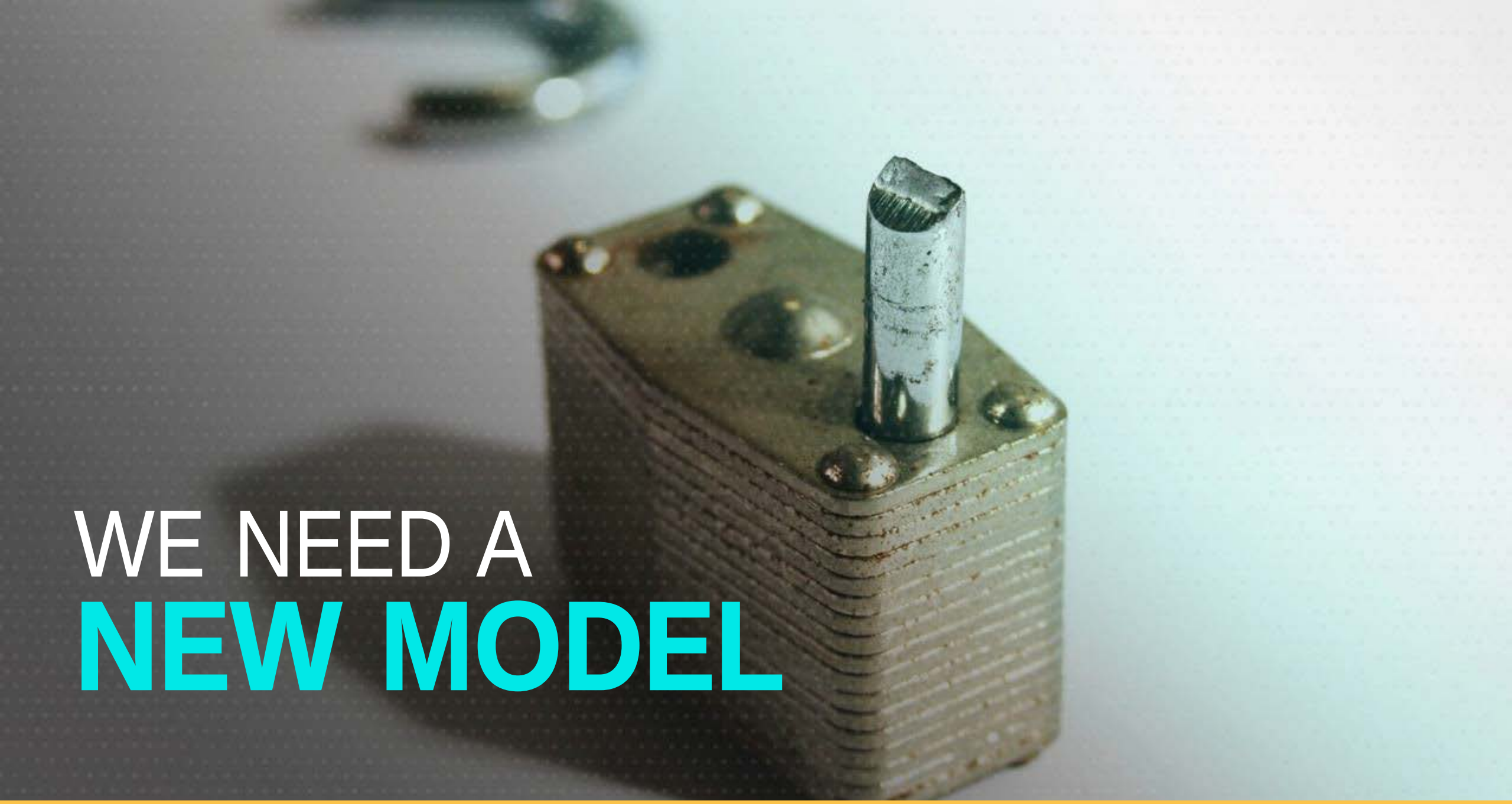
OTPs improve security but aren't easy enough to use - and are still phishable



All Rights Reserved | FIDO Alliance | Copyright 2017

THE WORLD HAS A **“SHARED SECRETS” PROBLEM**

All Rights Reserved | FIDO Alliance | Copyright 2017



All Rights Reserved | FIDO Alliance | Copyright 2017

HOW ARE WE DOING IT?

STANDARDS

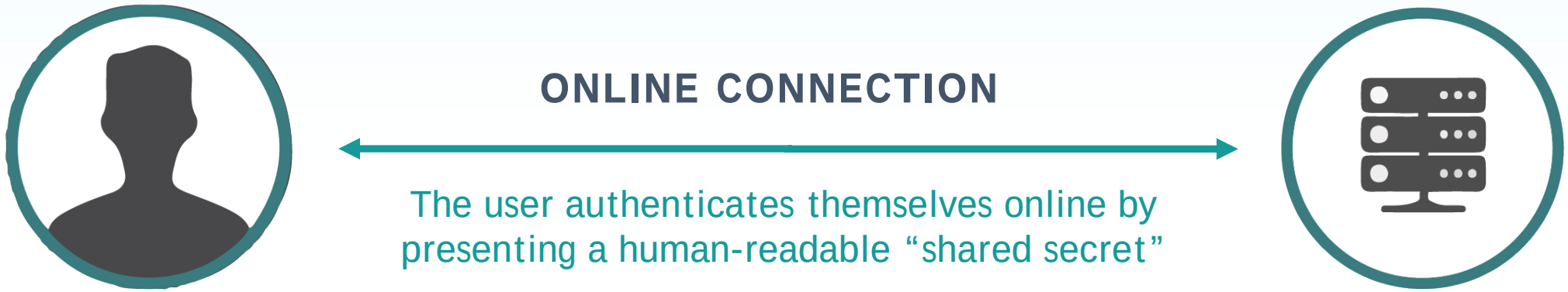
ECOSYSTEM

DEPLOYMENTS

USER EXPERIENCE

All Rights Reserved | FIDO Alliance | Copyright 2017

HOW OLD AUTHENTICATION WORKS



All Rights Reserved | FIDO Alliance | Copyright 2017

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

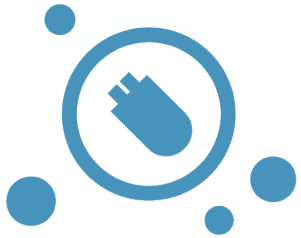
All Rights Reserved | FIDO Alliance | Copyright 2017

SIMPLER AUTHENTICATION

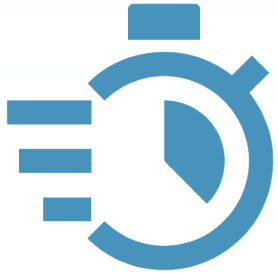
Reduces reliance on complex passwords

Single gesture to log on

Works with commonly used devices



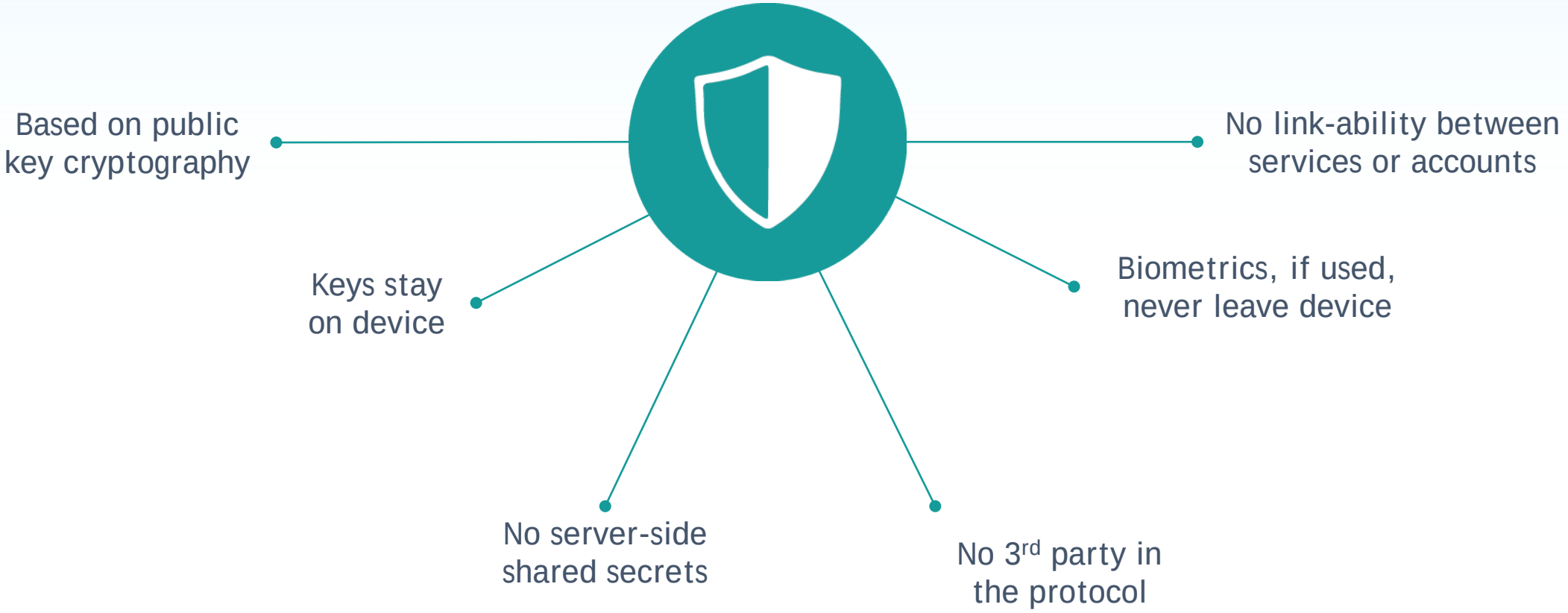
Same authentication on multiple devices



Fast and convenient

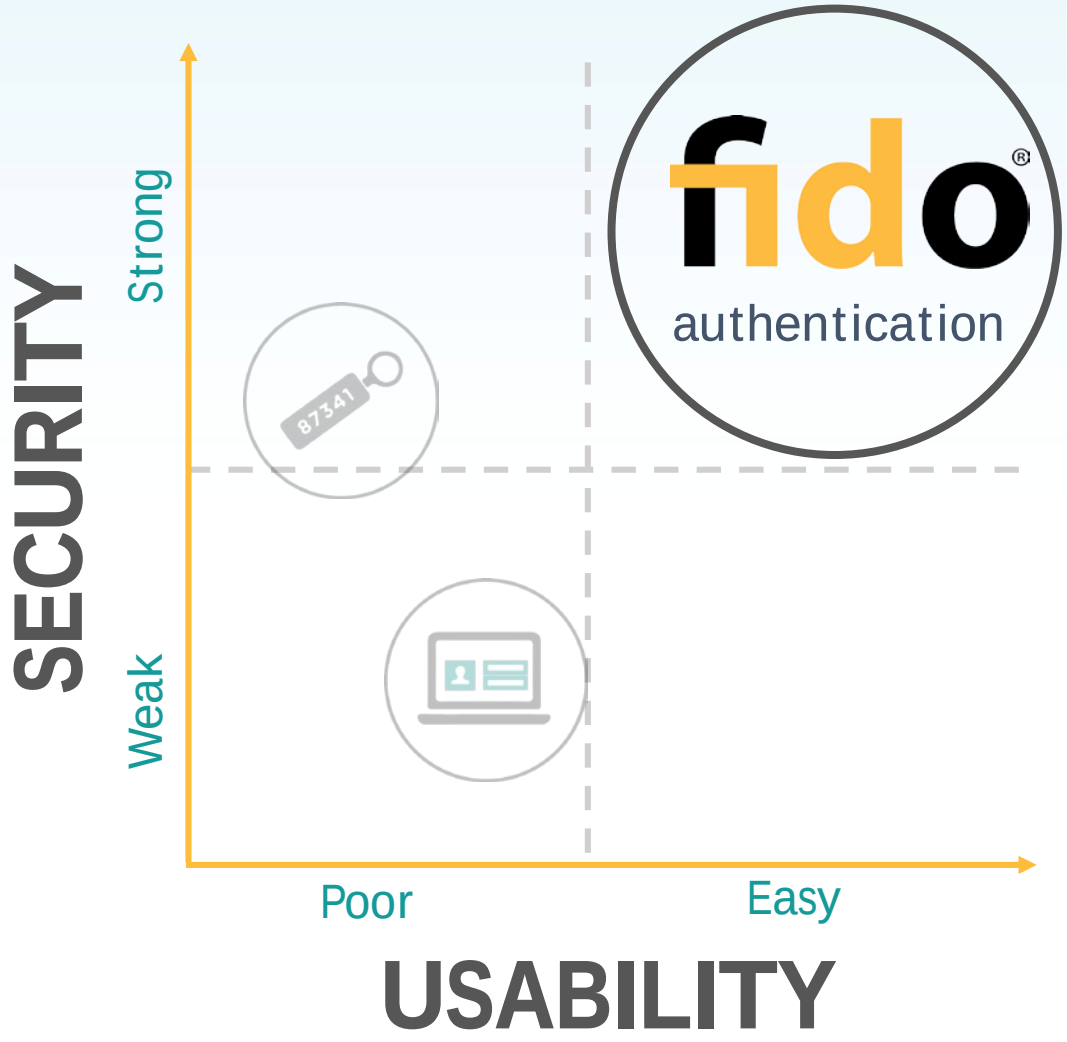
All Rights Reserved | FIDO Alliance | Copyright 2017

STRONGER AUTHENTICATION



All Rights Reserved | FIDO Alliance | Copyright 2017

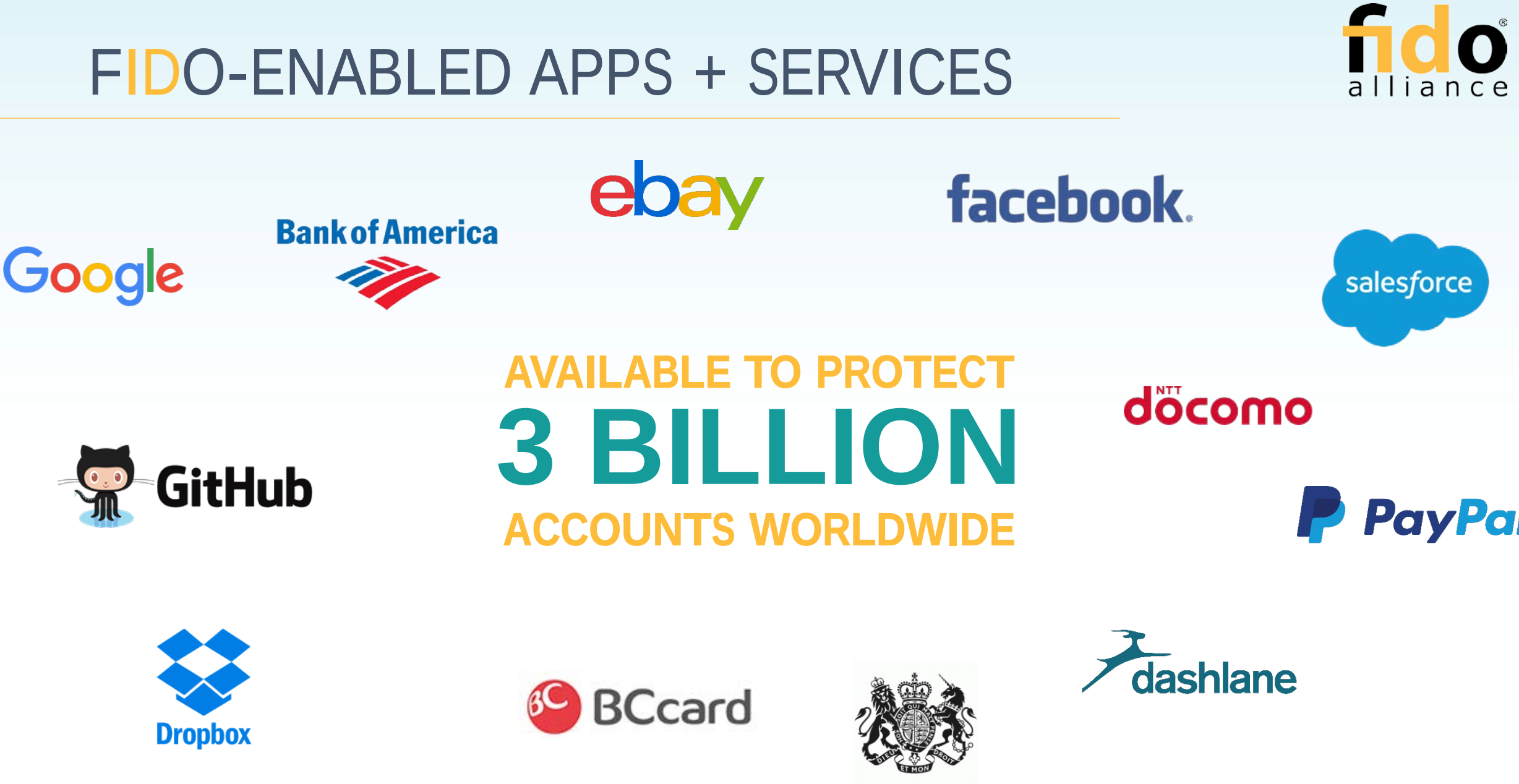
FIDO — A NEW PARADIGM:



STRONGER & SIMPLER

All Rights Reserved | FIDO Alliance | Copyright 2017

FIDO-ENABLED APPS + SERVICES

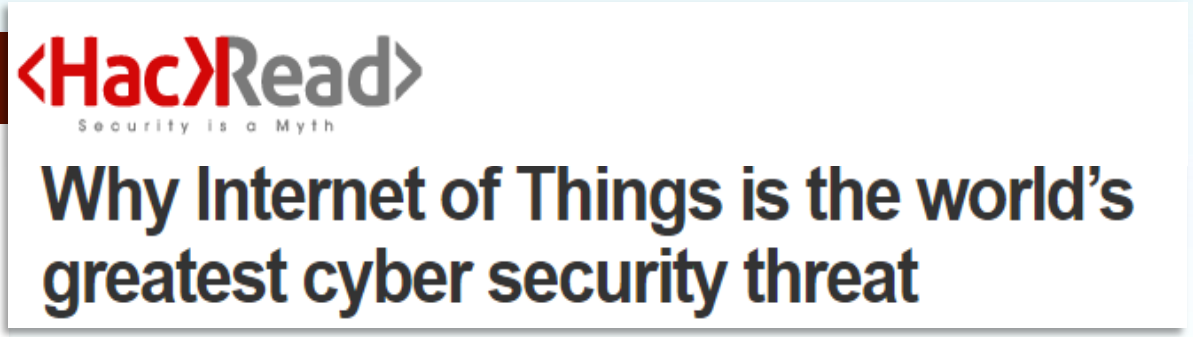


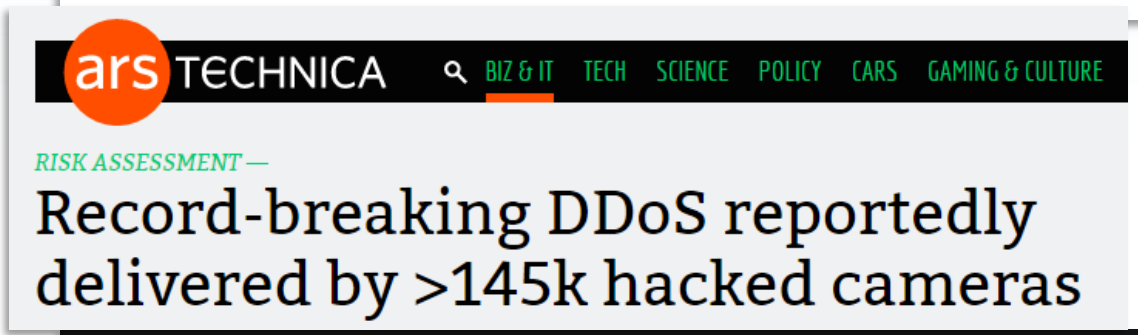
All Rights Reserved | FIDO Alliance | Copyright 2017

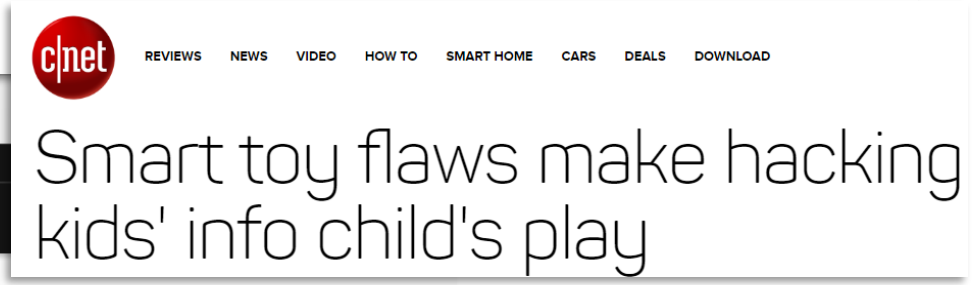
BUT WAIT…

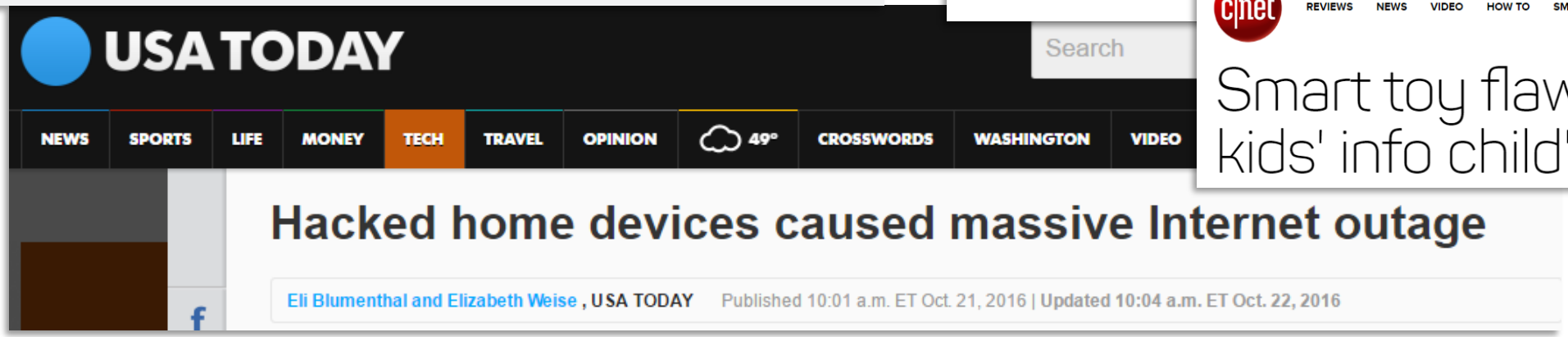
All Rights Reserved | FIDO Alliance | Copyright 2017

THE WORLD HAS AN IOT SECURITY PROBLEM





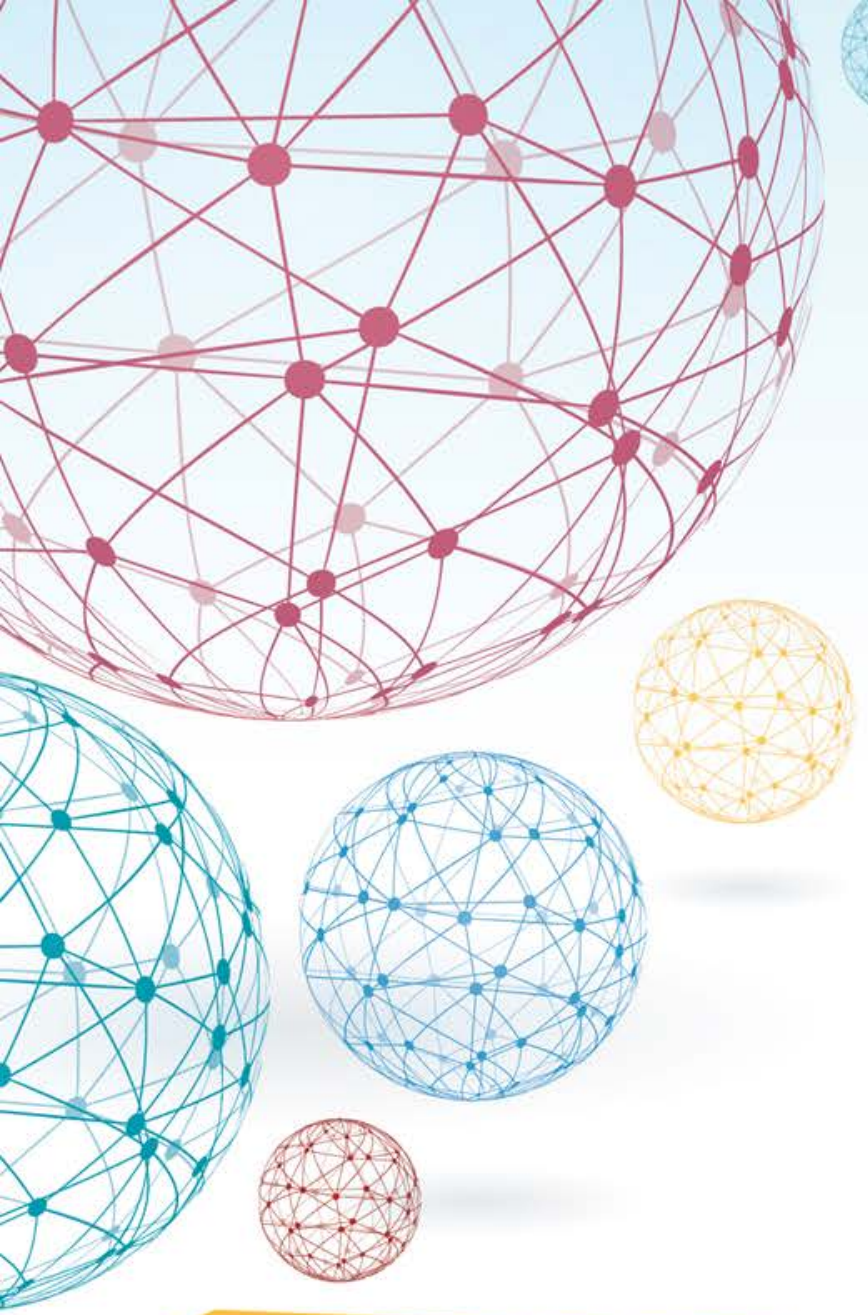




All Rights Reserved | FIDO Alliance | Copyright 2017

WE NEED A NEW AUTHENTICATION MODEL FOR CONNECTED USERS & DEVICES

All Rights Reserved | FIDO Alliance | Copyright 2017



THANK YOU

ANDREW SHIKIAR
SR. DIRECTOR OF MARKETING
ANDREW@FIDOALLIANCE.ORG

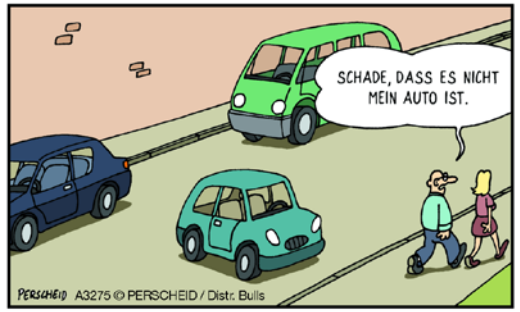
All Rights Reserved | FIDO Alliance | Copyright 2017

THE FUTURE OF AUTHENTICATION FOR THE INTERNET OF THINGS

ROLF LINDEMANN, NOK NOK LABS

Thanks to this app you can maneuver the new Forpel using your smartphone!

Too bad it's not my car.



All Rights Reserved | FIDO Alliance | Copyright 2017

What‘s the challenge

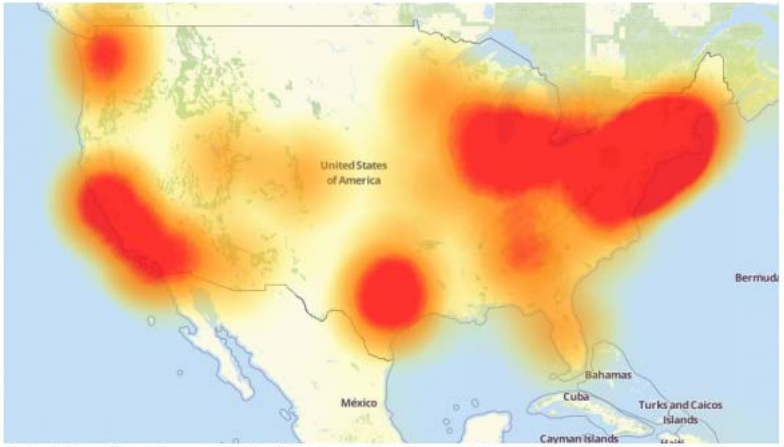
KrebsonSecurity
In-depth security news and investigation

21 Hacked Cameras, DVRs Powered Today’s Massive Internet Outage

OCT 16

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet’s top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



A depiction of the outages caused by today’s attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

At first, it was unclear who or what was behind the attack on Dyn. But over the past few hours, at least one computer security firm has come out saying the attack involved **Mirai**,

*“The issue with these particular devices is that a user cannot feasibly change this password,” Flashpoint’s **Zach Wikholm** told KrebsOnSecurity. “The password is hardcoded into the firmware, and the tools necessary to disable it are not present.*

HELPING SECURE THE INTERNET OF THINGS WITH THE
OWASP INTERNET OF THINGS TOP 10
VULNERABILITY CATEGORIES

1 Insecure Web Interface
covers IoT device administrative interfaces

Obstacles

- Default usernames and passwords
- No account lockout
- XSS, CSRF, SQLi vulnerabilites

Solutions

- Allow default usernames and password to be changed
- Enable account lockout
- Conduct web application assessments

2 Insufficient Authentication/Authorization
covers all device interfaces and services

Obstacles

- Weak passwords
- Password recovery mechanisms are insecure
- No two-factor authentication available

Solutions

- Require strong, complex passwords
- Verify that password recovery mechanisms are secure
- Implement two-factor authentication where possible

3 Insecure Network Services
covers all network services including device, cloud, web and mobile

Five of 10 mobile interfaces exhibit account enumeration issues

One system offered two-factor authentication

A **single** system implemented Apple’s Touch ID

HP Enterprise IoT Home Security Systems

All Rights Reserved | FIDO Alliance | Copyright 2017

Context

Secure firmware protects one “healthy” part from infected parts

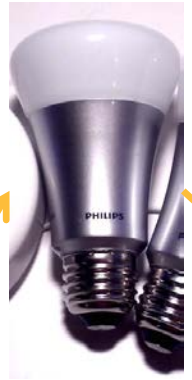
Need strong fundament, e.g. a CPU supporting ARM TrustZone, Intel SGX, etc.

Focus of today‘s presentation

Strong authentication makes sure only legitimate entities get access

All Rights Reserved | FIDO Alliance | Copyright 2017

Scope



Cloud Services

All Rights Reserved | FIDO Alliance | Copyright 2017

Scope

Devices that are not primary interaction devices, e.g. smart light bulbs, WIFI routers, smart fridges, smart thermostats, connected cars, smart door locks, …

Web

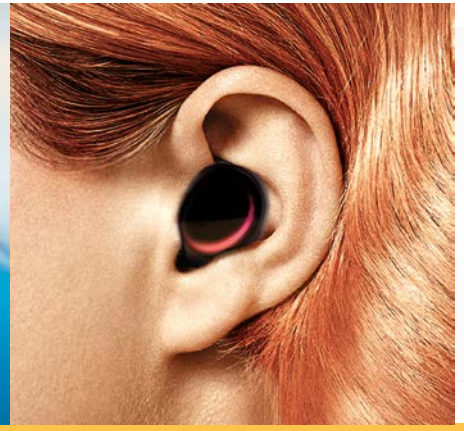
“Primary interaction” devices, i.e. devices
a) which we typically have in our possession and
b) that have a user interface

…ssed by FIDO & W3C Web Authentication, not the **core** focus of this talk

All Rights Reserved | FIDO Alliance | Copyright 2017

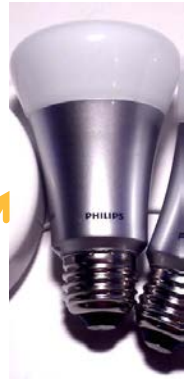
Primary Interaction Devices

- Primary interaction device have the capability to verify the user through their user interface.
- They can connect to another device or to a cloud service
- They can implement a FIDO Authenticator allowing the user to strongly and conveniently authenticate to devices or cloud services. Trust Execution Environments and/or Secure Elements add security.



All Rights Reserved | FIDO Alliance | Copyright 2017

Scope

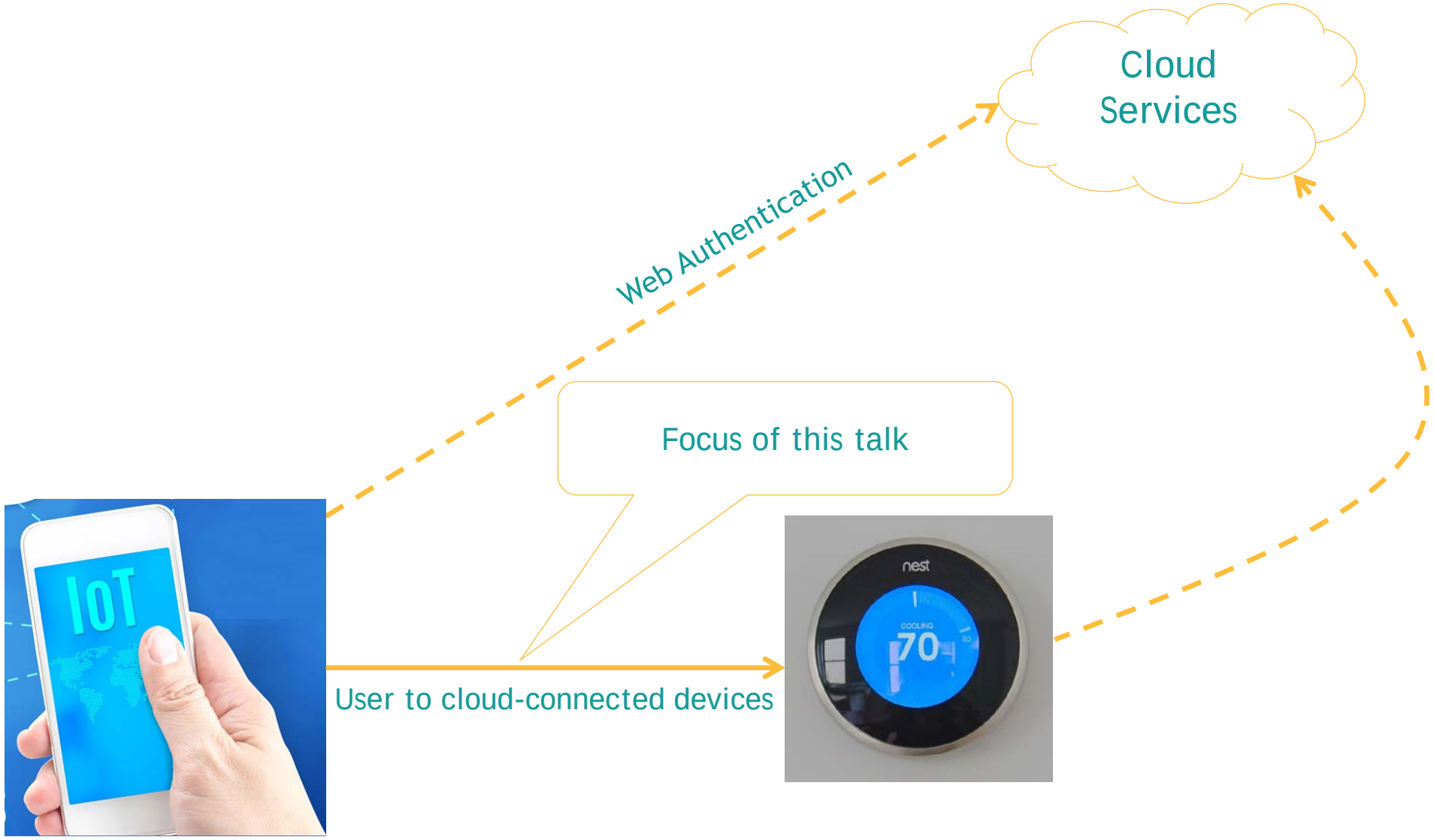


User to standalone devices

Focus of this talk

All Rights Reserved | FIDO Alliance | Copyright 2017

Scope



All Rights Reserved | FIDO Alliance | Copyright 2017

Scope

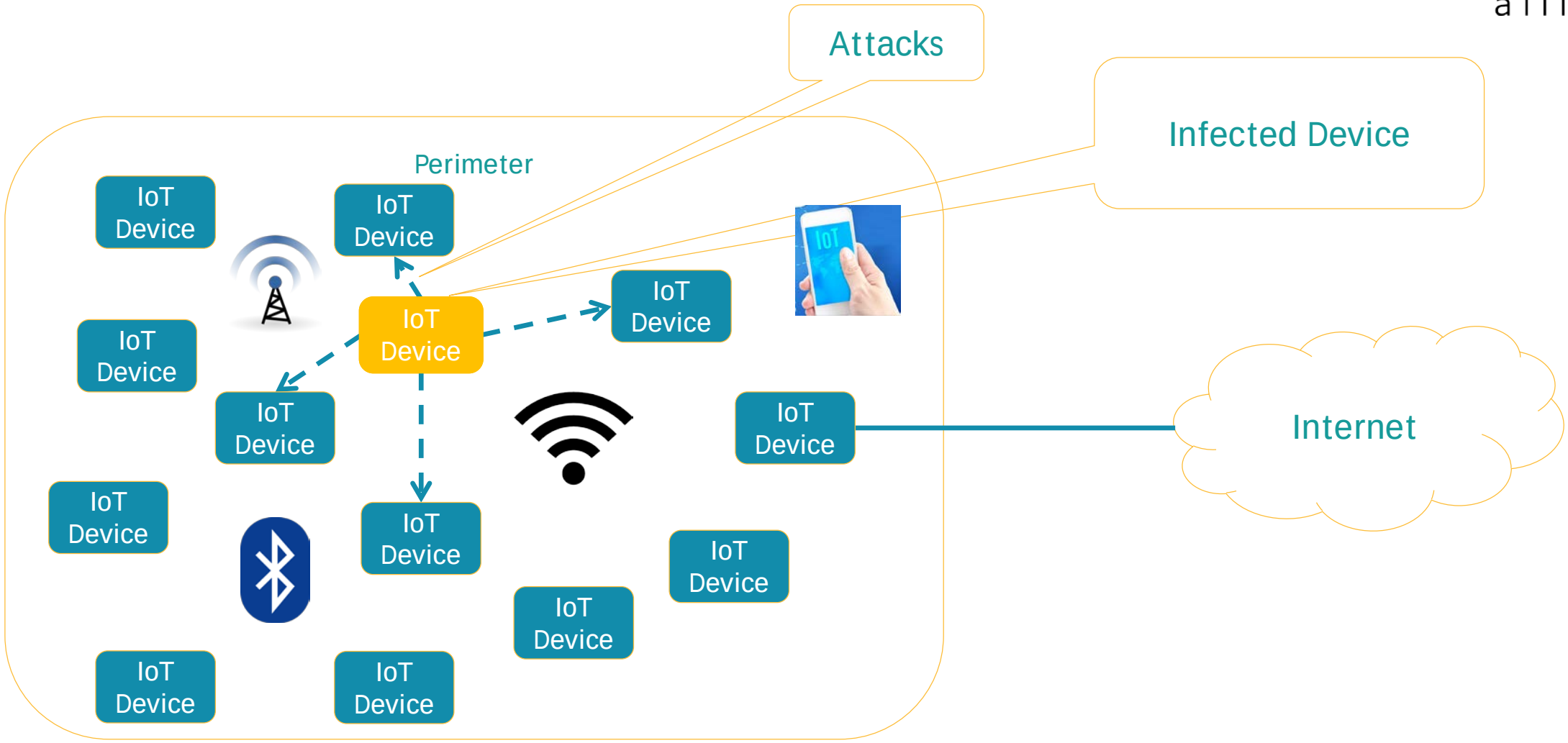
Cloud Services

Device-to-Device Authentication

Device-to-Cloud Authentication

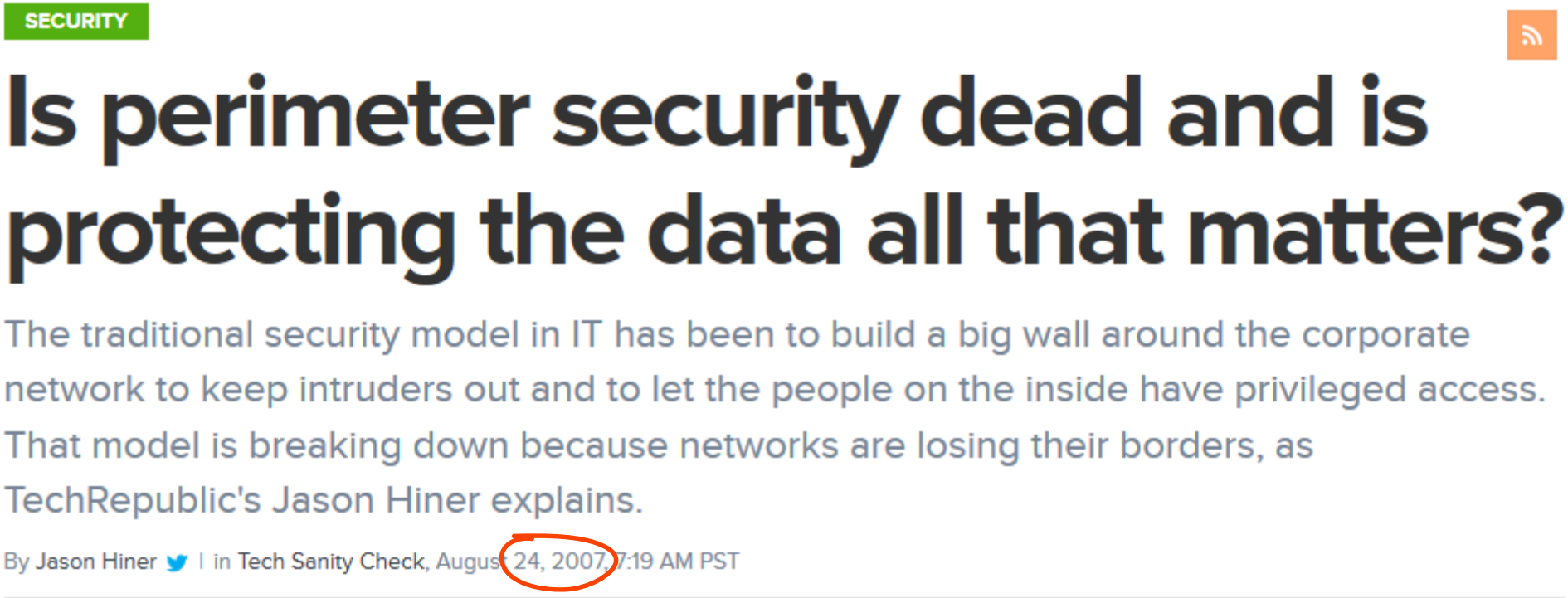
All Rights Reserved | FIDO Alliance | Copyright 2017

Background



All Rights Reserved | FIDO Alliance | Copyright 2017

Background



SECURITY

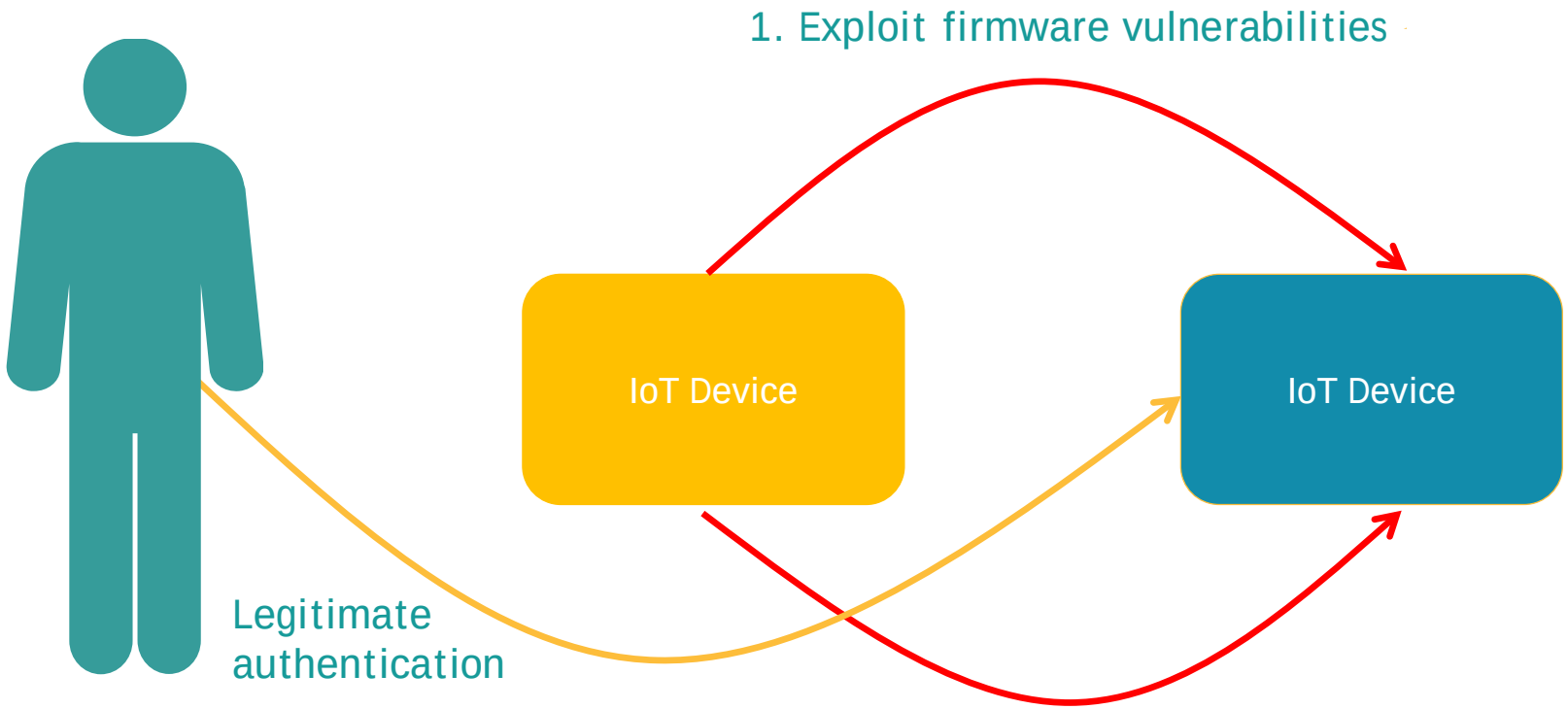
Is perimeter security dead and is protecting the data all that matters?

The traditional security model in IT has been to build a big wall around the corporate network to keep intruders out and to let the people on the inside have privileged access. That model is breaking down because networks are losing their borders, as TechRepublic's Jason Hiner explains.

By Jason Hiner | in Tech Sanity Check, August 24, 2007, 7:19 AM PST

All Rights Reserved | FIDO Alliance | Copyright 2017

Attack Scenarios



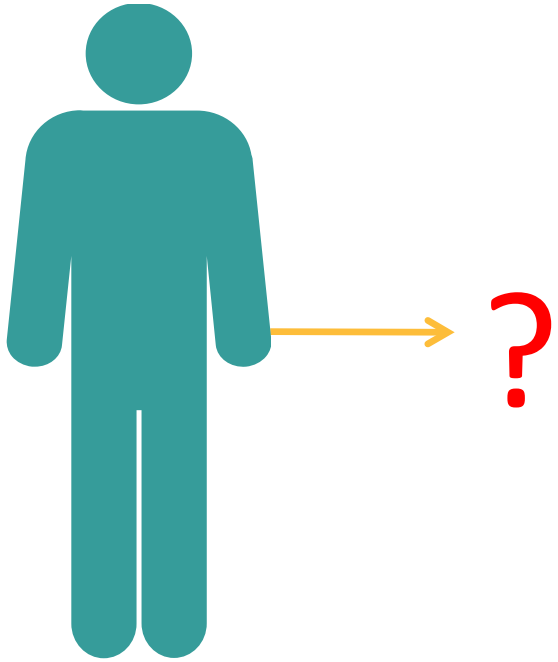
Need **Strong Authentication** to protect against such attacks. **Our focus.**

All Rights Reserved | FIDO Alliance | Copyright 2017

User to Device Authentication

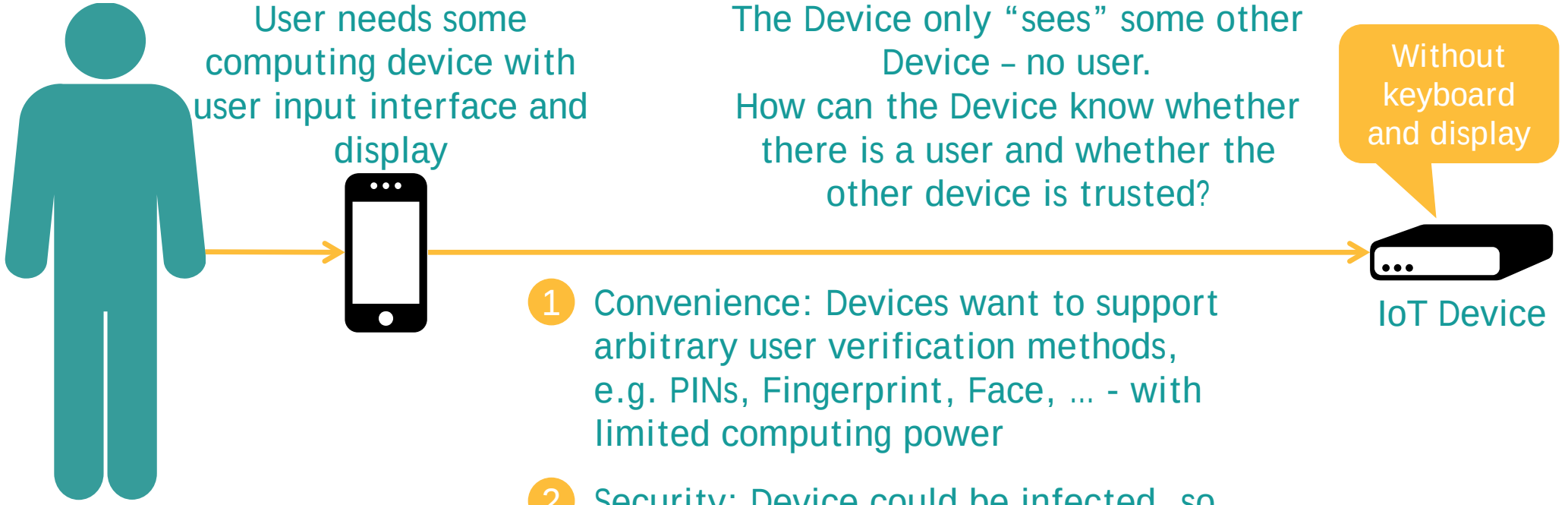
All Rights Reserved | FIDO Alliance | Copyright 2017

User to Device interaction



All Rights Reserved | FIDO Alliance | Copyright 2017

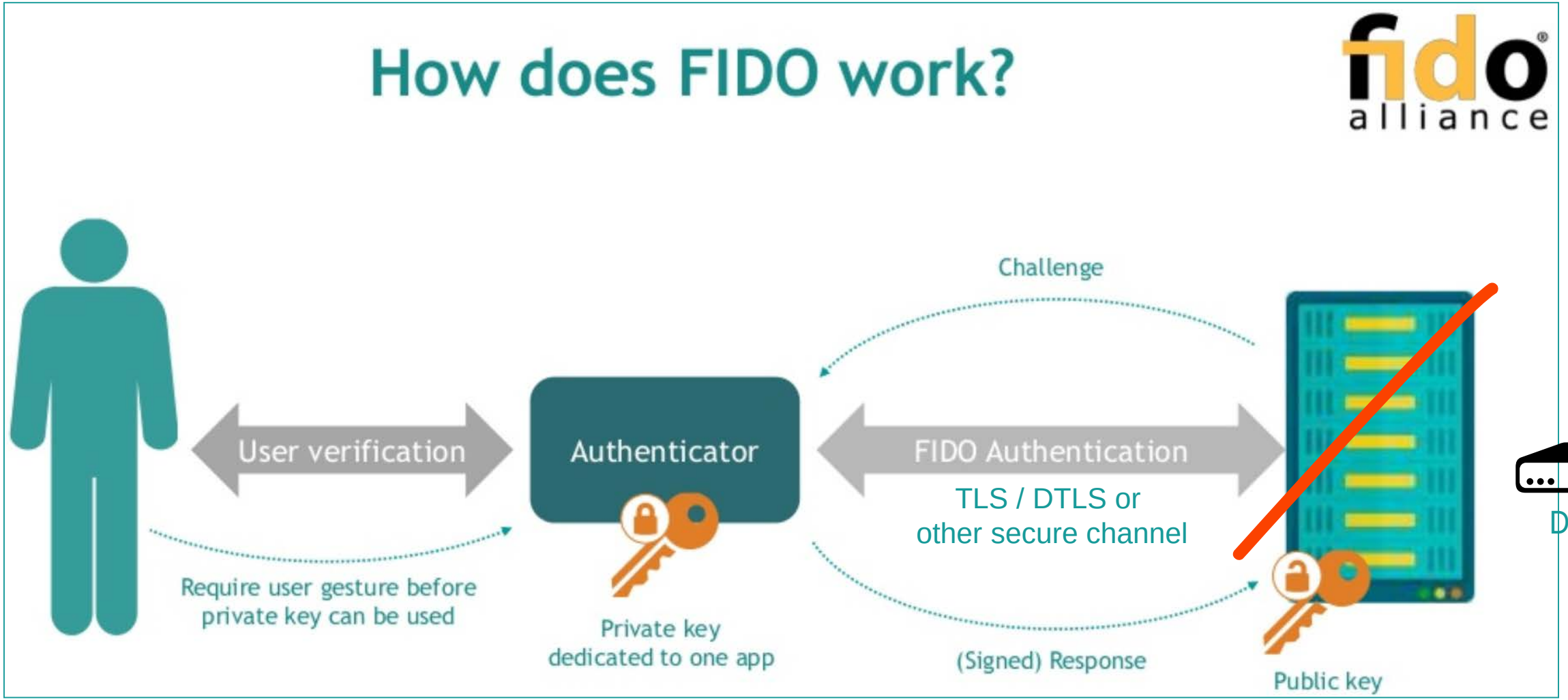
User to Device interaction



1. Convenience: Devices want to support arbitrary user verification methods, e.g. PINs, Fingerprint, Face, … - with limited computing power
2. Security: Device could be infected, so users don’t want to reveal bearer tokens (like passwords, etc.) to it

All Rights Reserved | FIDO Alliance | Copyright 2017

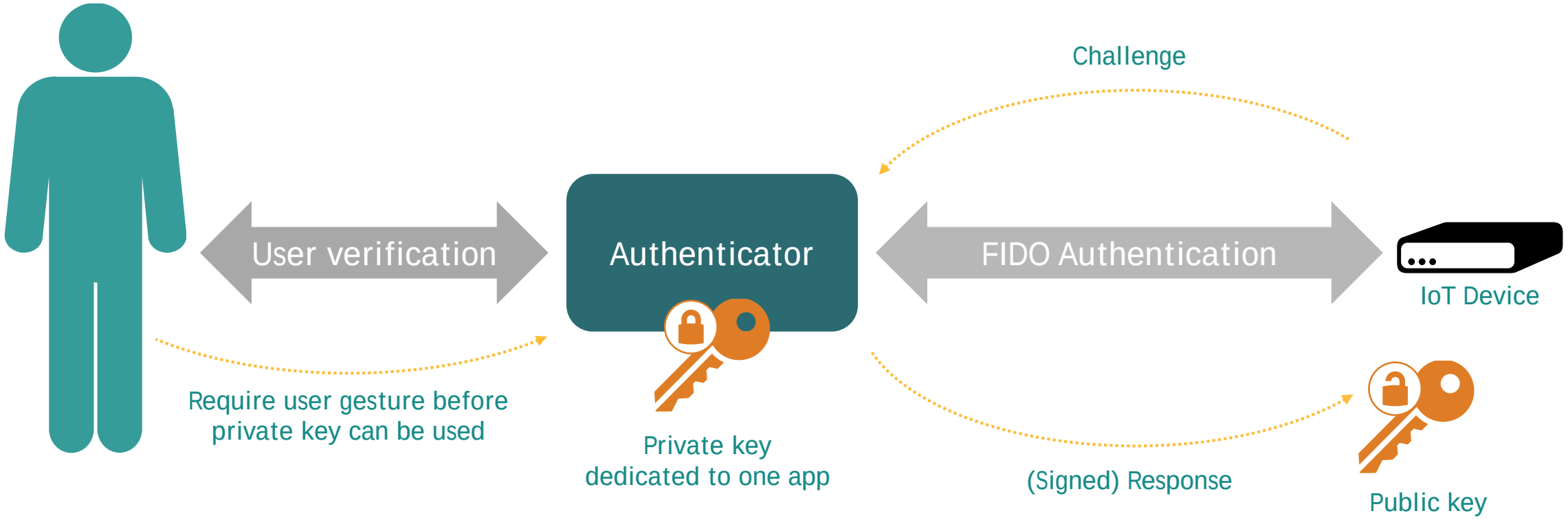
... did we see that before?



See **https://fidoalliance.org/events/fido-alliance-seminar-hongkong/**

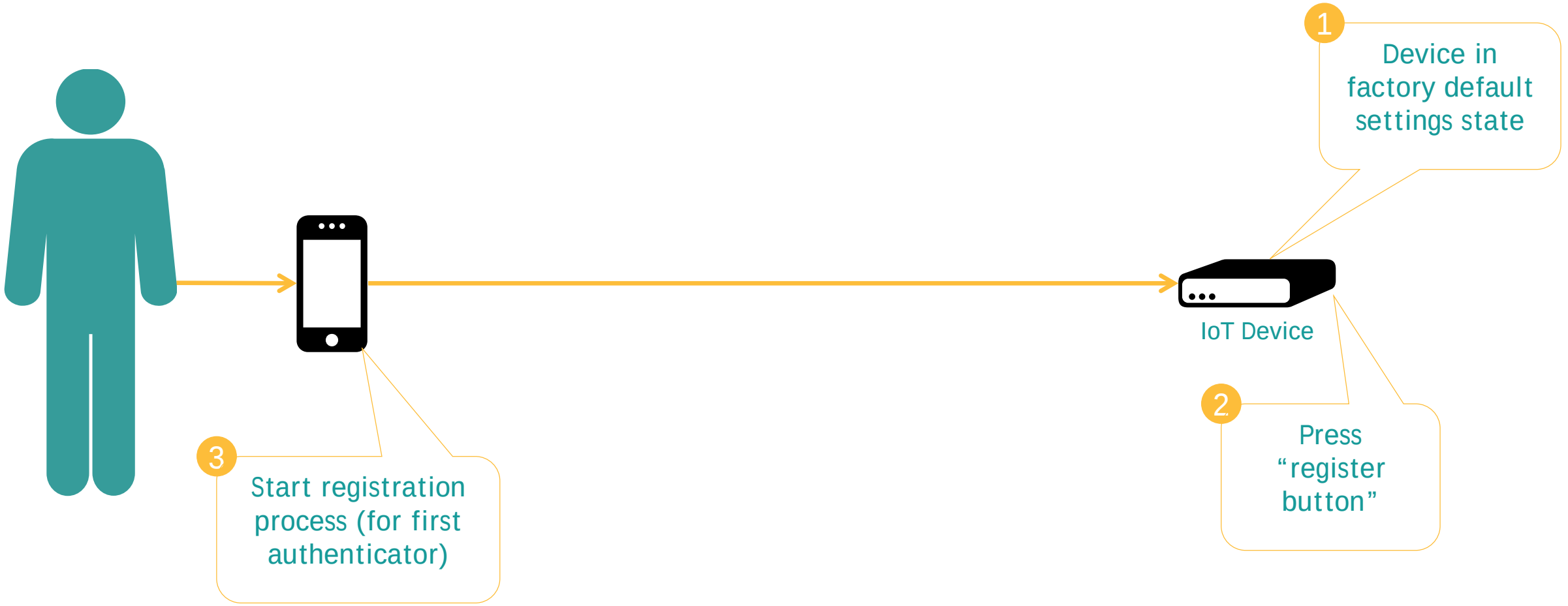
All Rights Reserved | FIDO Alliance | Copyright 2017

User to Device Authentication



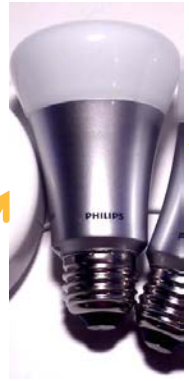
All Rights Reserved | FIDO Alliance | Copyright 2017

First Authenticator Registration (Example)



All Rights Reserved | FIDO Alliance | Copyright 2017

Standalone Devices



Smart Light Bulbs

WIFI Router

...

Cloud Services

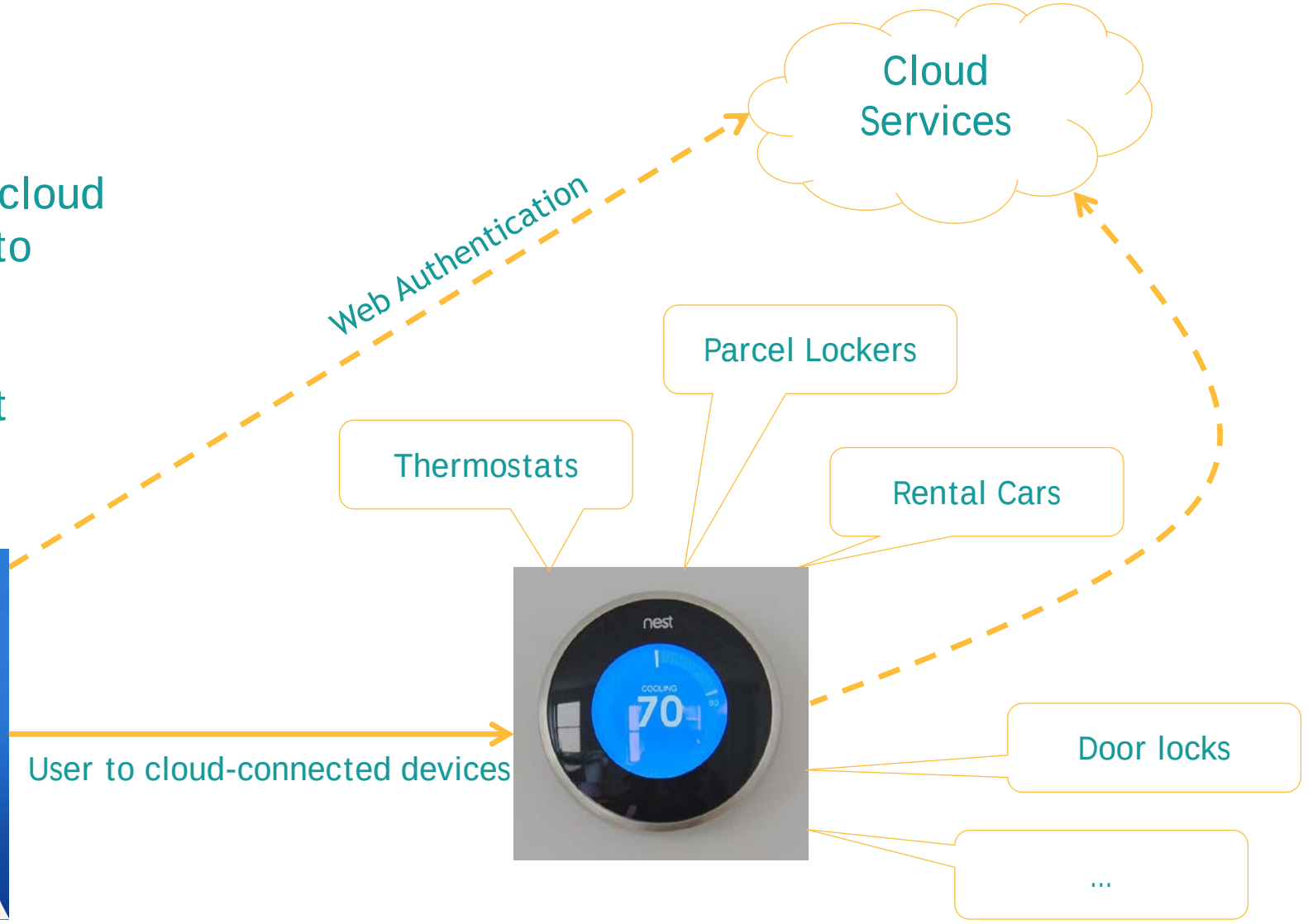
User to standalone devices

All Rights Reserved | FIDO Alliance | Copyright 2017

Devices with Cloud Dependency

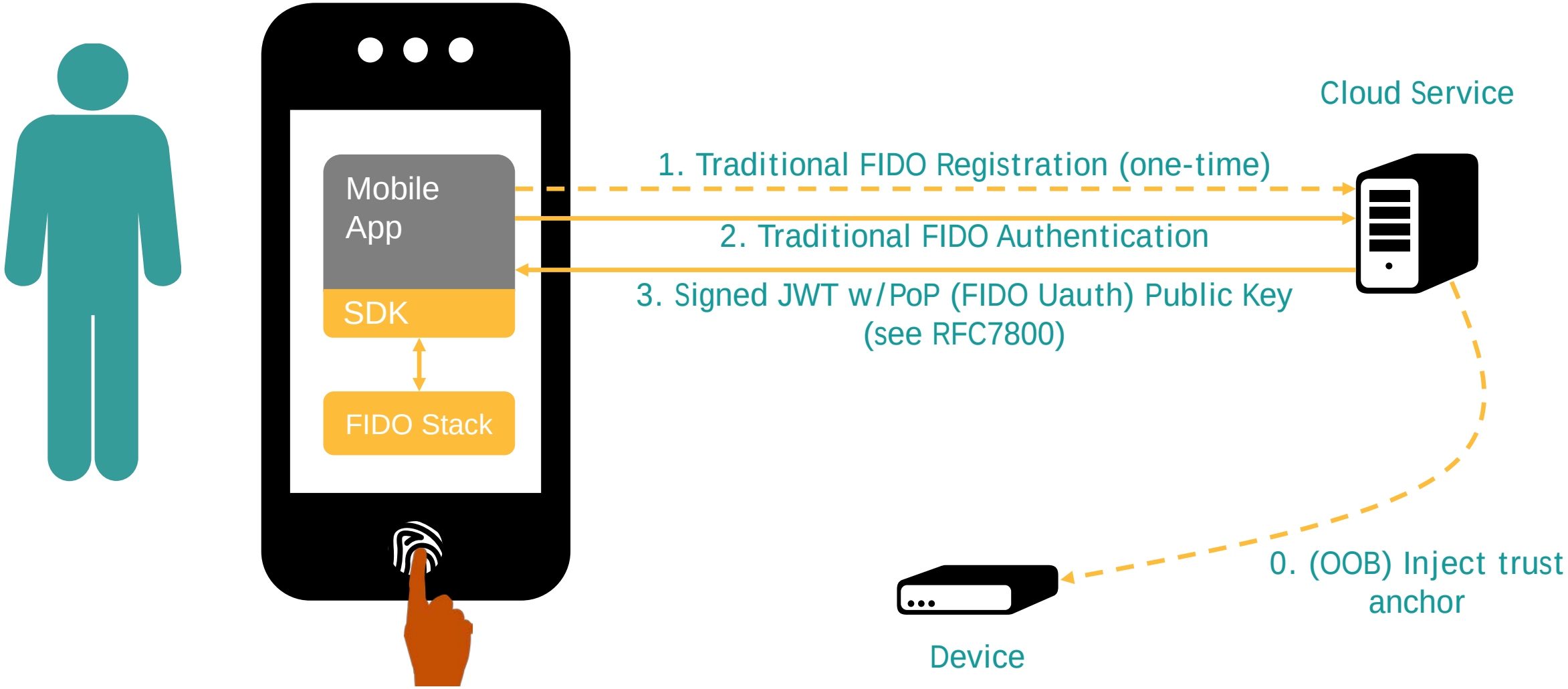
Cloud Dependency: We want the cloud service being able to grant access to the device to a specific user

But: Do not rely on stable internet connection at time of access



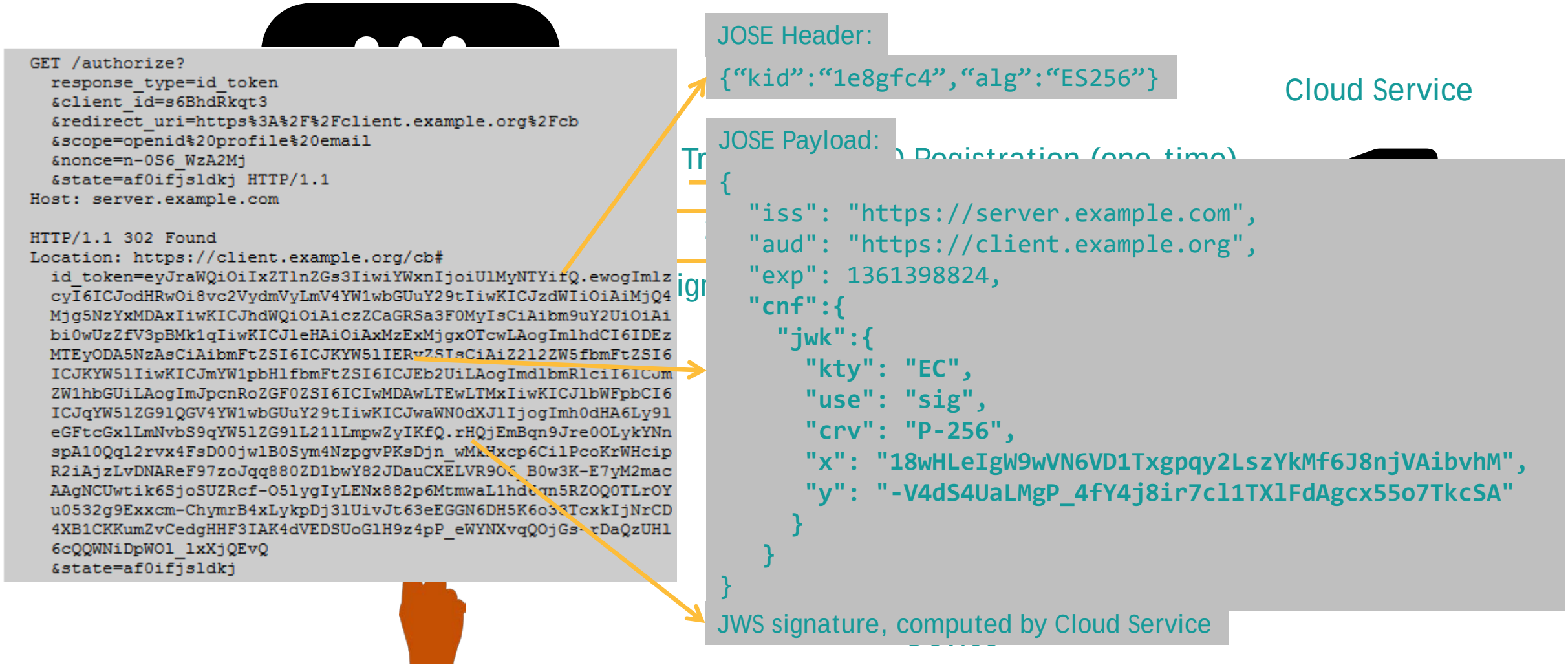
All Rights Reserved | FIDO Alliance | Copyright 2017

How does it work with central authorization infrastructure?



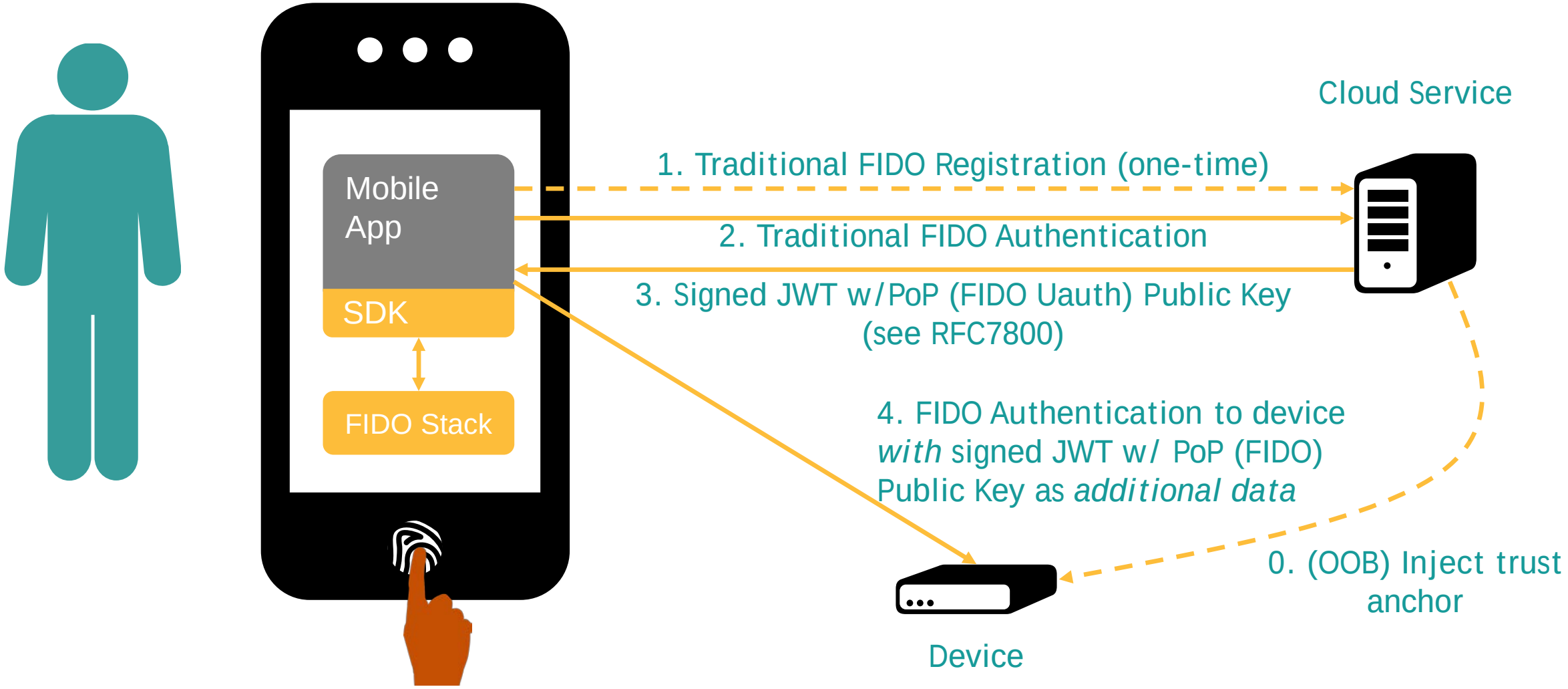
All Rights Reserved | FIDO Alliance | Copyright 2017

How does it work with central authorization infrastructure?



All Rights Reserved | FIDO Alliance | Copyright 2017

How does it work with central authorization infrastructure?



All Rights Reserved | FIDO Alliance | Copyright 2017

Gallagher Unlocks the Internet of Things with Nok Nok

GALLAGHER™

Source: Philafrenzy, Wikipedia

Source: Klaus Mueller, wikipedia

Device to Device & Device to Cloud Authentication

All Rights Reserved | FIDO Alliance | Copyright 2017

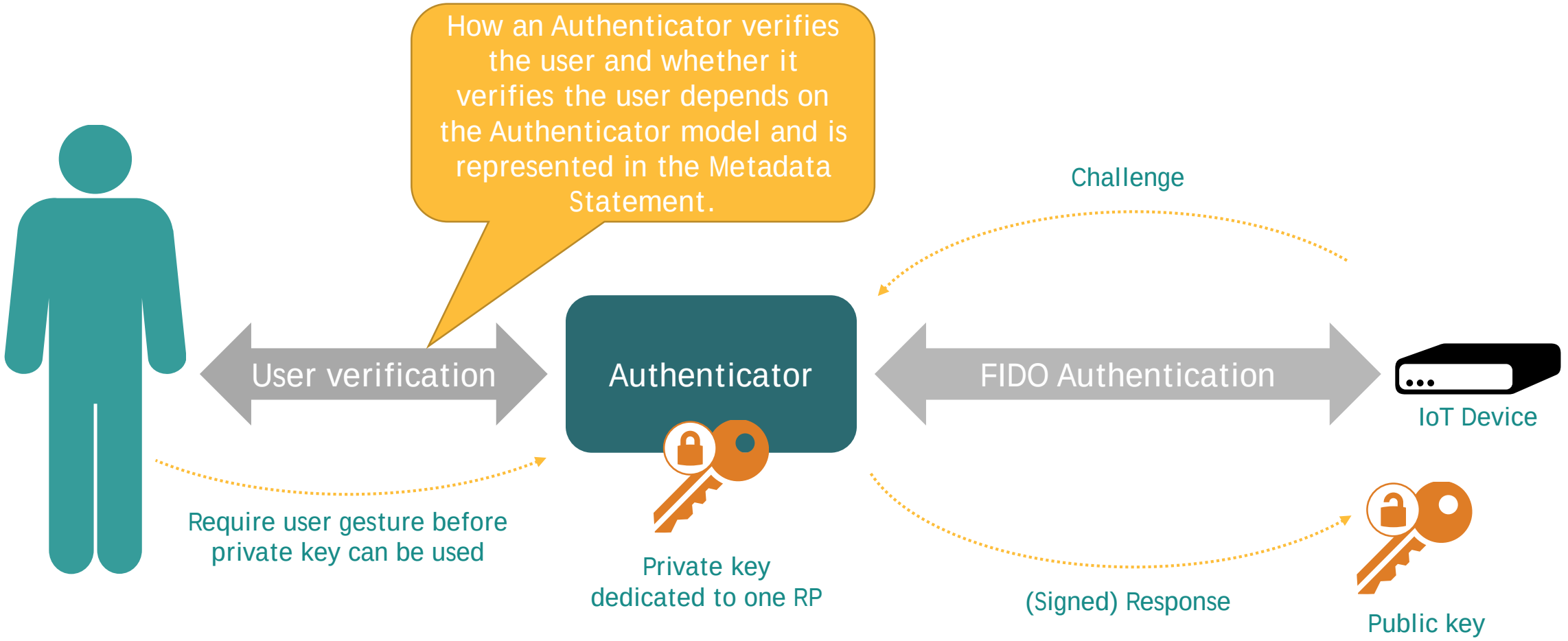
Scope

Device to device authentication

User to device authentication

All Rights Reserved | FIDO Alliance | Copyright 2017

User to Device Authentication



All Rights Reserved | FIDO Alliance | Copyright 2017

Device to Device Authentication

There are “Silent” Authenticators, never requiring any user interaction.

Challenge

Authenticator

FIDO Authentication

IoT Device

(Signed) Response

Public key

… and such Authenticator might be embedded in a device

All Rights Reserved | FIDO Alliance | Copyright 2017

Device to **Cloud** Authentication

It makes no difference to the IoT device nor to the FIDO Authenticator whether it authenticates to another device or to a cloud service

Challenge

Cloud Service

Authenticator

FIDO Authentication

(Signed) Response

Public key

All Rights Reserved | FIDO Alliance | Copyright 2017

Device to Cloud Authentication

It makes no difference to the IoT device nor to the FIDO Authenticator whether it authenticates to another device or to a cloud service

Challenge

Cloud Service

Authenticator

FIDO Authentication

(Signed) Response

Public key

… and the Authenticator can be embedded in smart fridges, smart thermostats and other IoT devices.

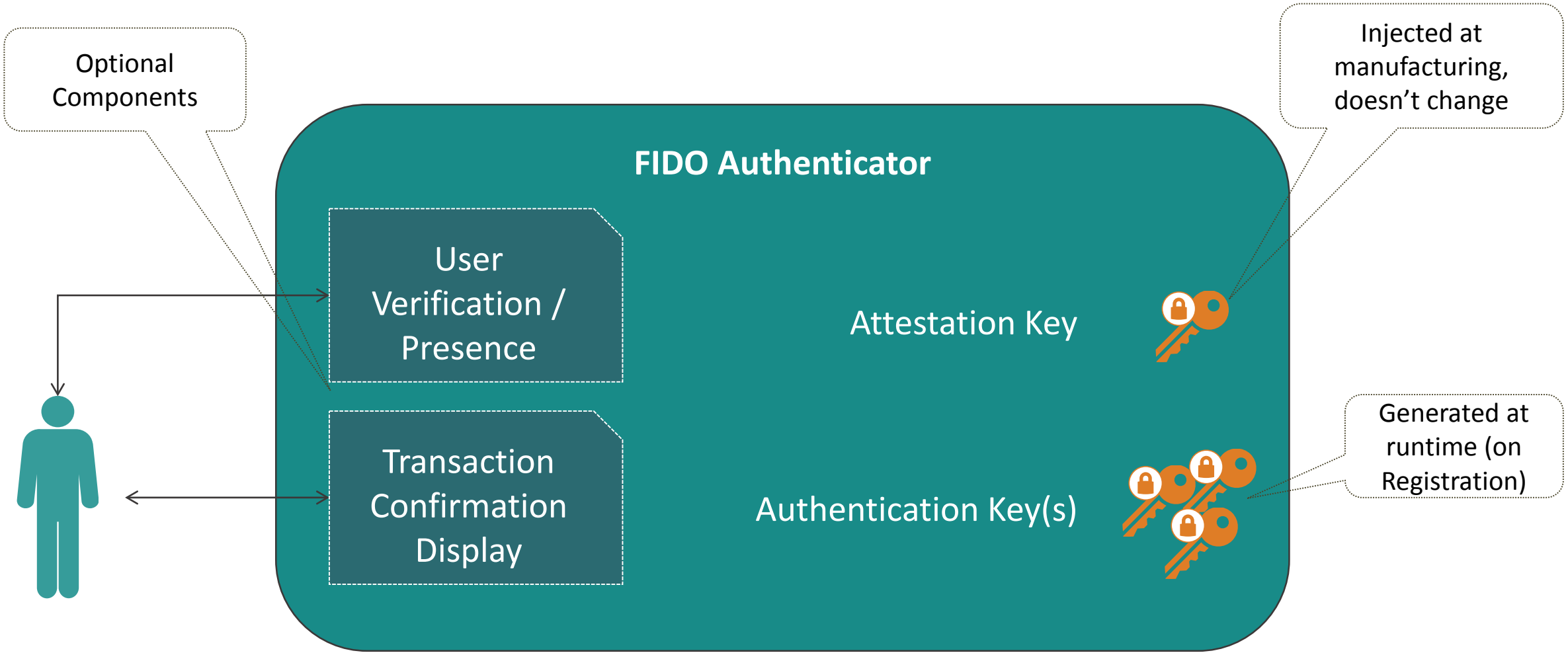
All Rights Reserved | FIDO Alliance | Copyright 2017

Conclusion

1. Authentication is the first experience of users with services and several device types.
2. Authentication needs to be convenient for the user and strong enough for the purpose.
3. We can do better than passwords + OTP. Look at the FIDO specifications for strong & convenient authentication, see www.fidoalliance.org.
4. FIDO supports “silent” Authenticators. These Authenticators can be implemented in IoT devices.
5. FIDO authentication responses can be verified in small devices, allowing FIDO authentication to those IoT device.
6. FIDO can be combined with PoP Keys (RFC7800) in order to support authentication to “cloud connected” IoT devices

All Rights Reserved | FIDO Alliance | Copyright 2017

FIDO Authenticator Concept



All Rights Reserved | FIDO Alliance | Copyright 2017

Silent Authenticators

1. Definition, see FIDO Glossary

Silent Authenticator

FIDO Authenticator that does not prompt the user or perform any user verification.

2. User Verification Method, see FIDO Registry

`USER_VERIFY_NONE` `0x00000200`

This flag MUST be set if the authenticator will respond without any user interaction (e.g. Silent Authenticator).

3. Metadata Statement, see FIDO Metadata Statements

`userVerificationDetails` of type array of required VerificationMethodANDCombinations

A list of *alternative* VerificationMethodANDCombinations. Each of these entries is one alternative user verification method. Each of these alternative user verification methods might itself be an "AND" combination of multiple modalities.

All effectively available alternative user verification methods MUST be properly specified here. A user verification method is considered effectively available if this method can be used to either:

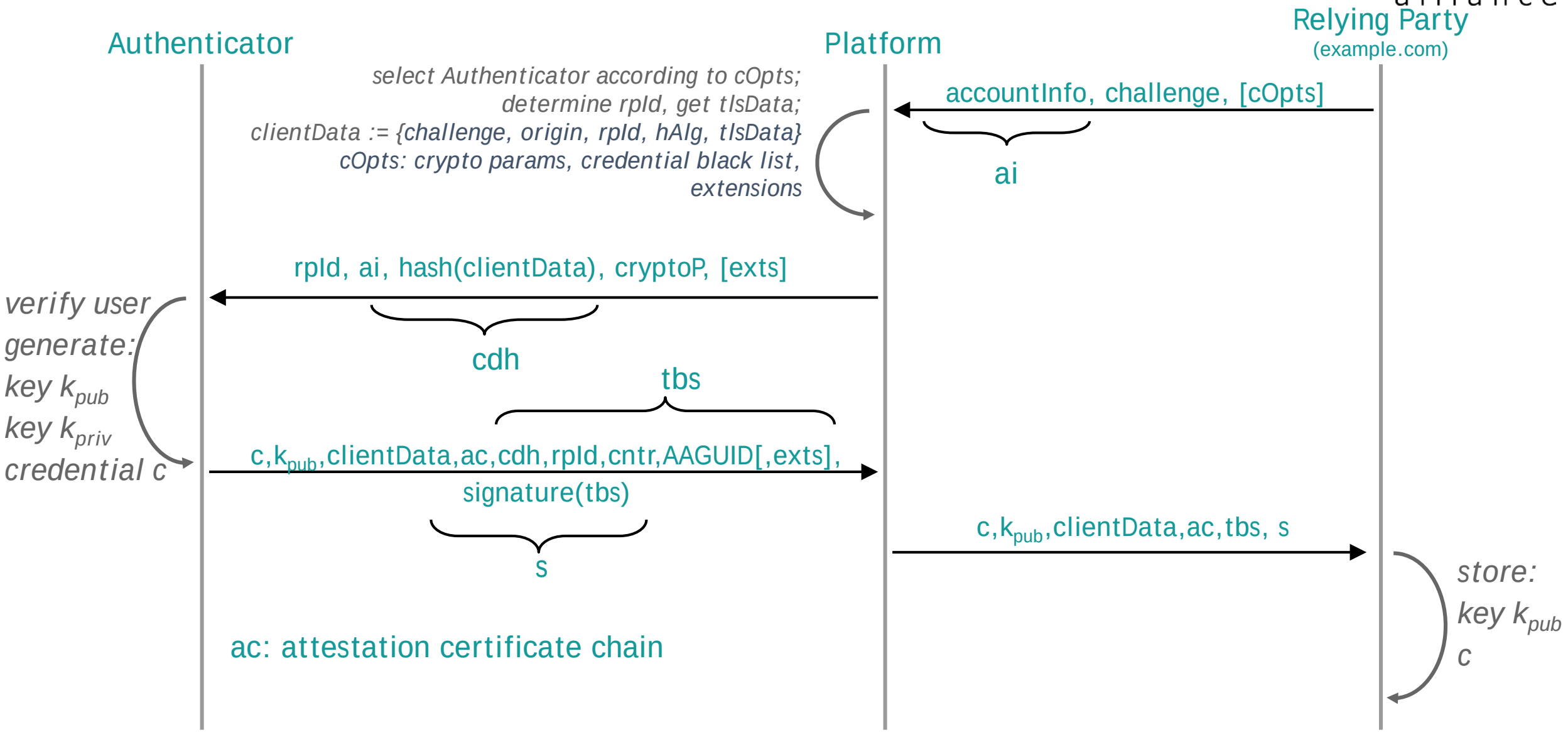
- enroll new verification reference data to one of the user verification methods

  or

- unlock the UAuth key directly after successful user verification

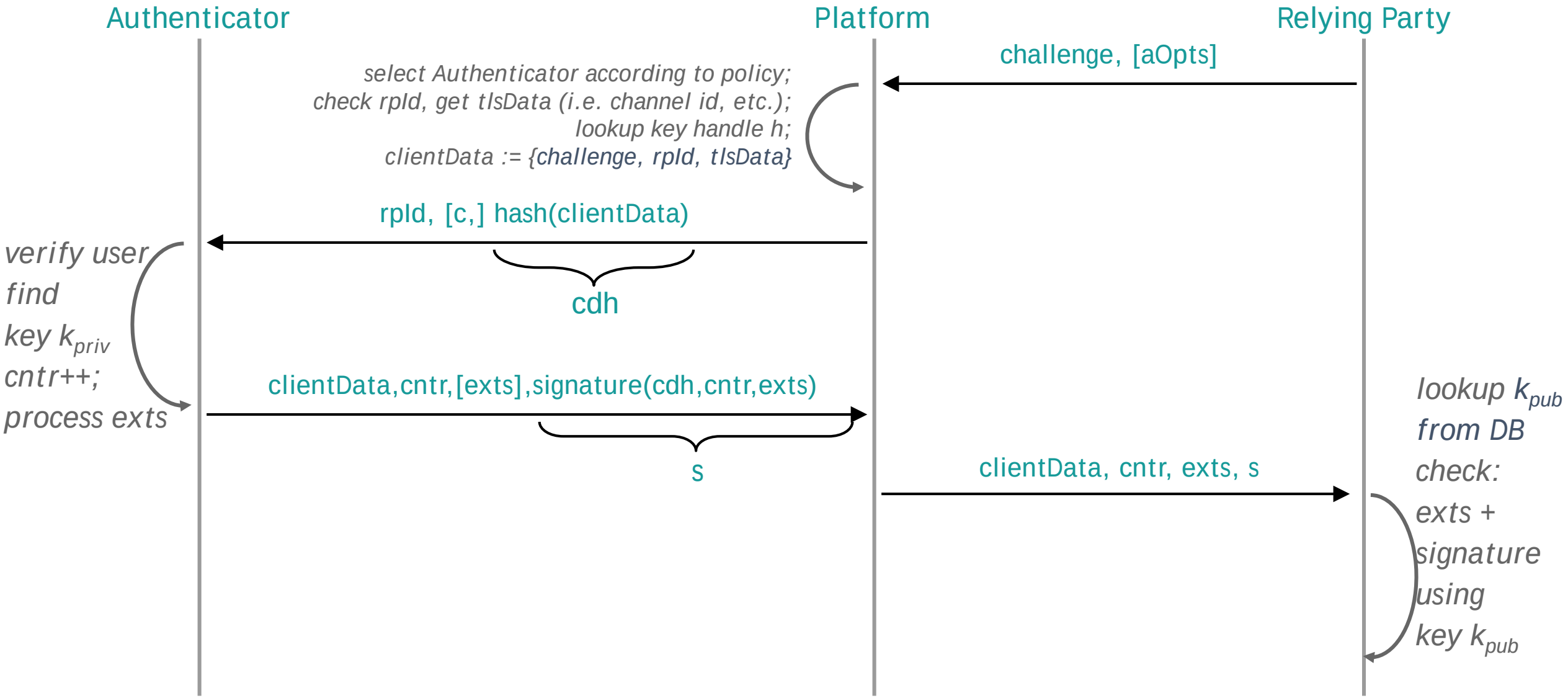
All Rights Reserved | FIDO Alliance | Copyright 2017

FIDO Registration



All Rights Reserved | FIDO Alliance | Copyright 2017

FIDO Authentication



All Rights Reserved | FIDO Alliance | Copyright 2017