FIDO and the Future of Simpler and Stronger Authentication

RISE Spring School
29 March 2018

Dr. Andrea Höller
Infineon Technologies Austria AG

Agenda

1	Introduction
2	The FIDO Standard
3	The FIDO Ecosystem
4	The Future of FIDO

Agenda

User authentication

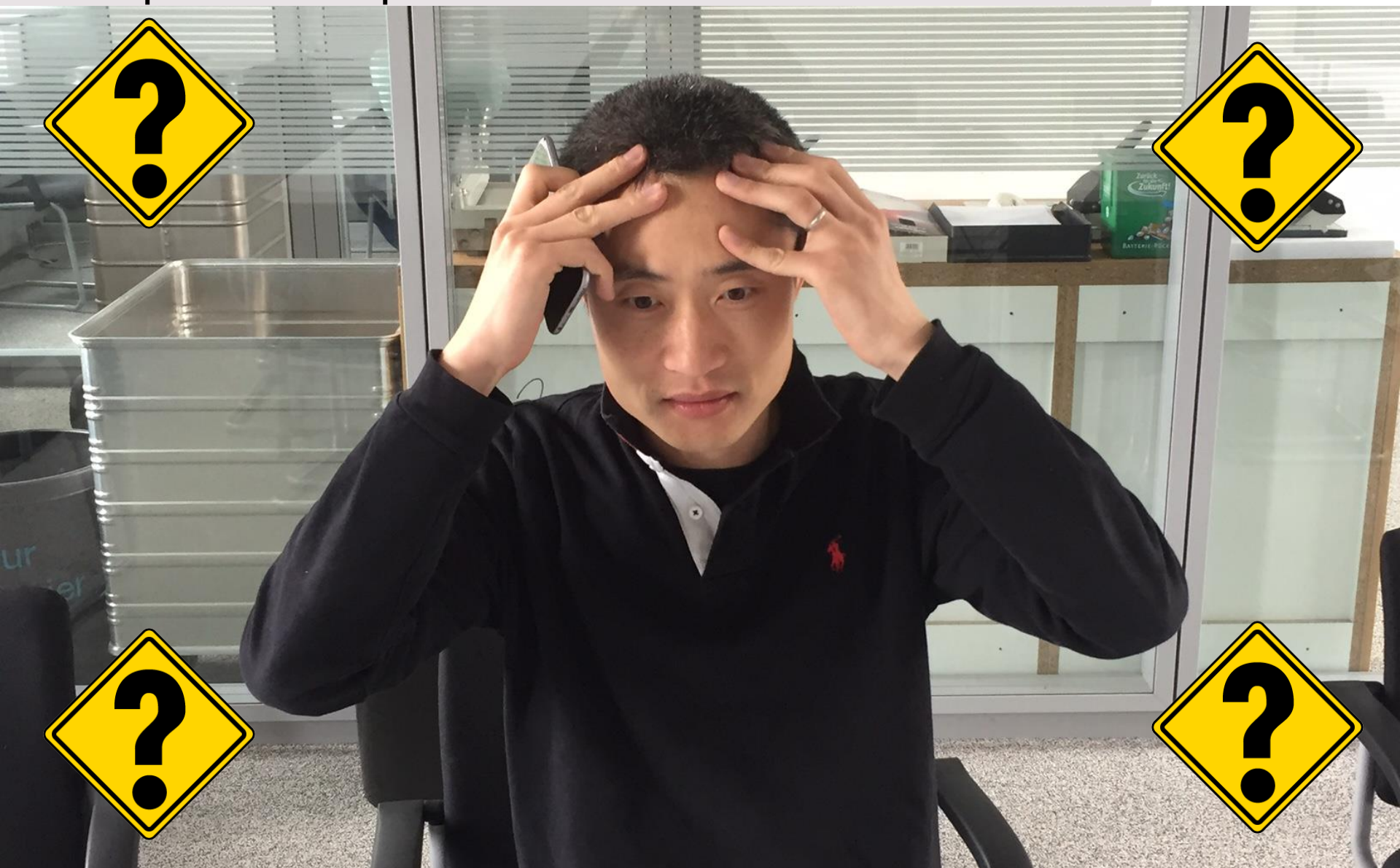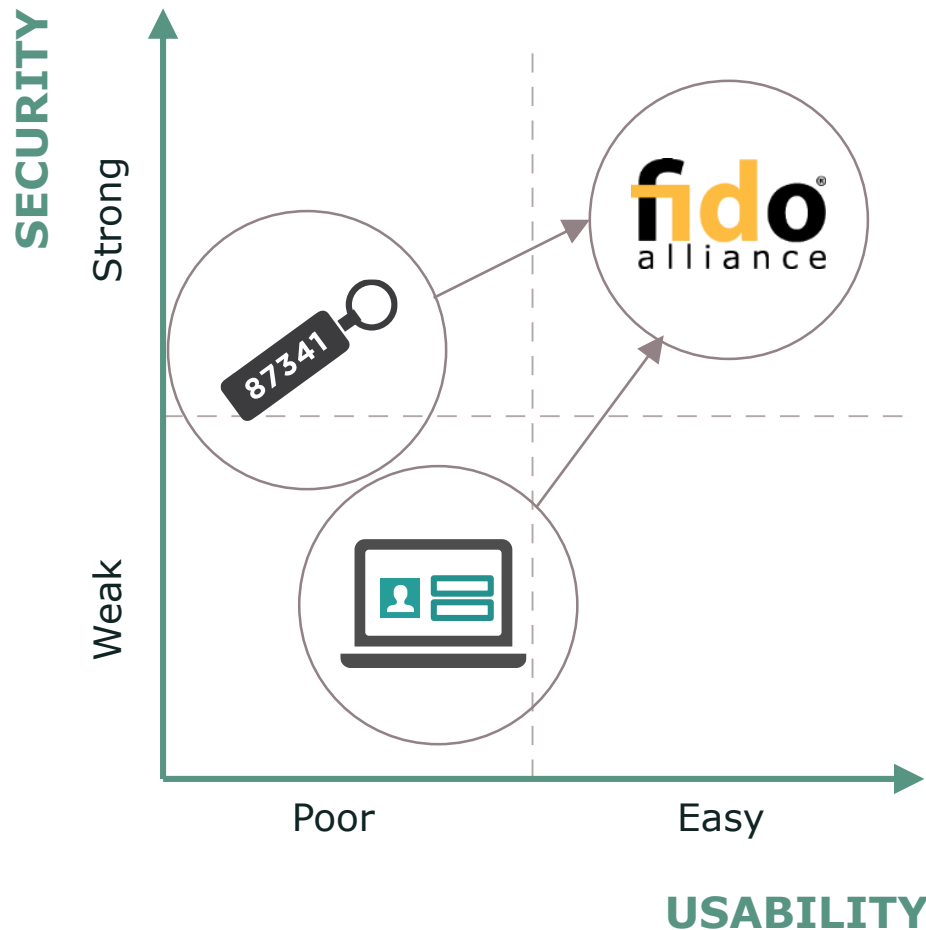| Three possible factors of user authentication		
Something you KNOW		› Password › PIN code › …
Something you ARE		› Fingerprint › Voice recognition › Face recognition › …
Something you HAVE		› SmartCard › USB token › Smartphone › Wearables › …

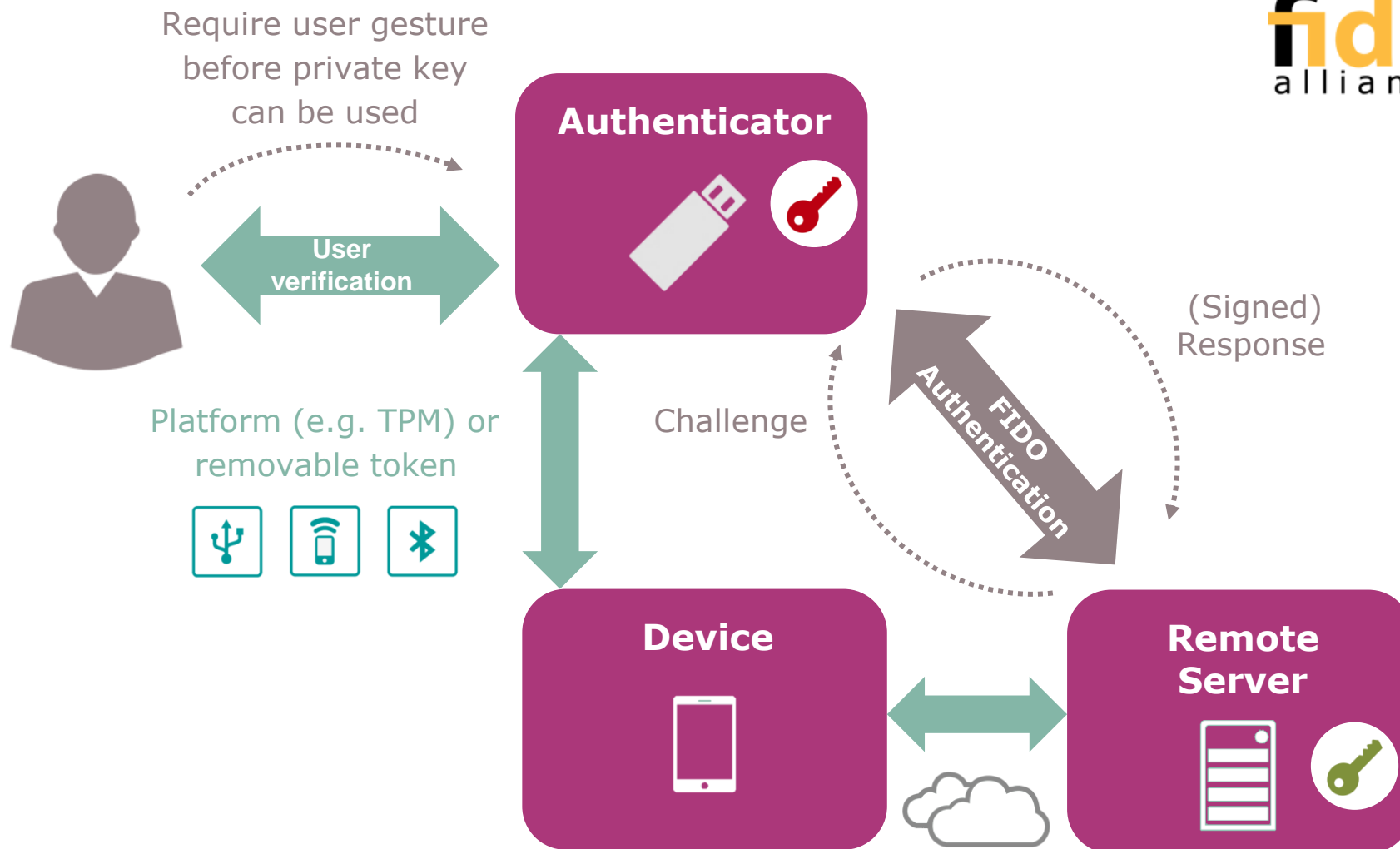# User authentication to a remote server
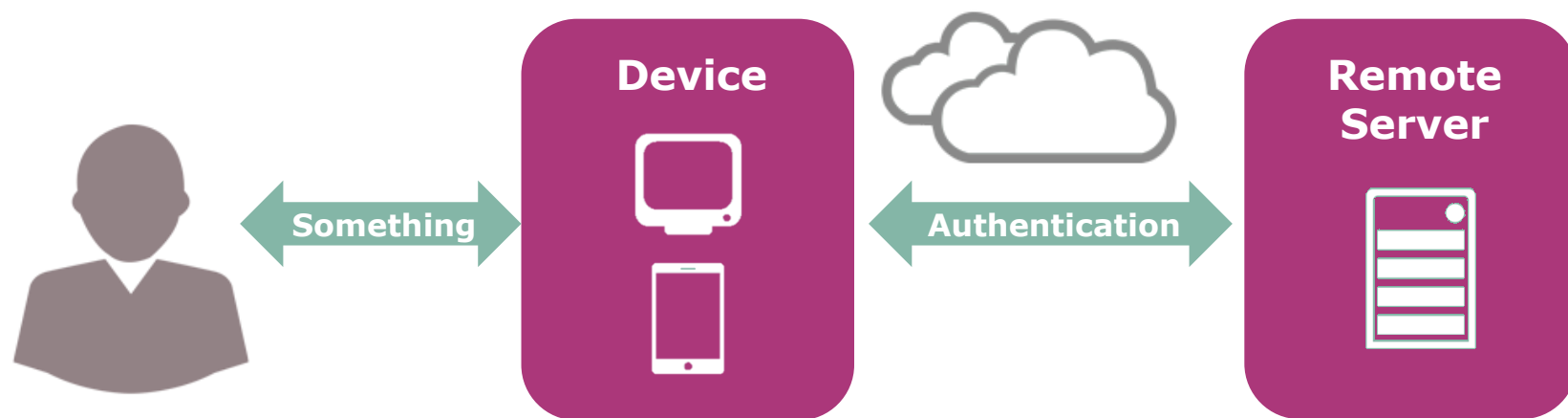
The password problem

The idea of FIDO

› **F**ast **ID**entiy **O**nline

› The core ideas of the FIDO Alliance are

  – ease of use

  – high security

  – good privacy

Basic working principle of FIDO

Require user gesture before private key can be used

Authenticator

User verification

Platform (e.g. TPM) or removable token

Challenge

FIDO Authentication

(Signed) Response

Device

Remote Server
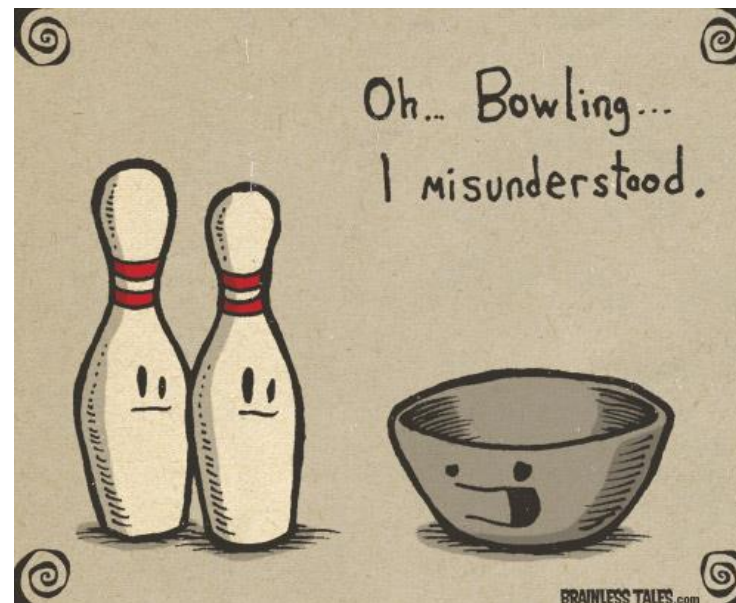
Ecosystem → **Standardization**

Agenda

FIDO 1.0

Passwordless Experience (UAF Standards)

fido®
alliance

1

?

Authentication
Challenge

2

Biometric User
Verification*

3

✓

Authenticated Online

Second Factor Experience (U2F Standards)

1

Second Factor
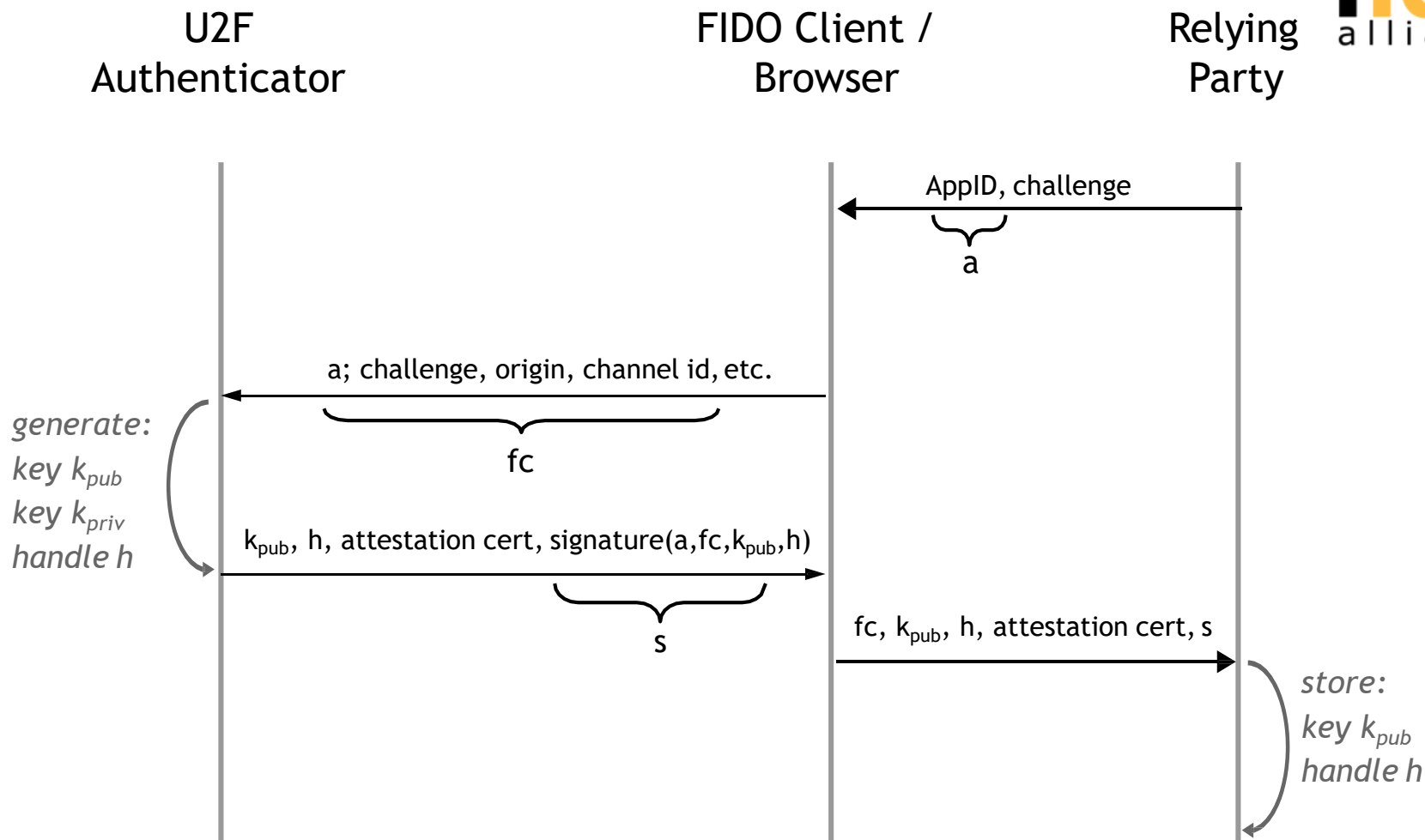Challenge

2

Insert Dongle* / Press
Button

3

✓

Authenticated
Online

*There are other types of authenticators

https://www.slideshare.net/FIDOAlliance/getting-to-know-the-fido-specifications-technical-tutorial

U2F registration

fido alliance

U2F
Authenticator

FIDO Client /
Browser

Relying
Party

AppID, challenge

a

a; challenge, origin, channel id, etc.

generate:
key k_{pub}
key k_{priv}
handle h

fc

k_{pub}, h, attestation cert, signature(a,fc,k_{pub},h)

s

fc, k_{pub}, h, attestation cert, s

store:
key k_{pub}
handle h

U2F authentication
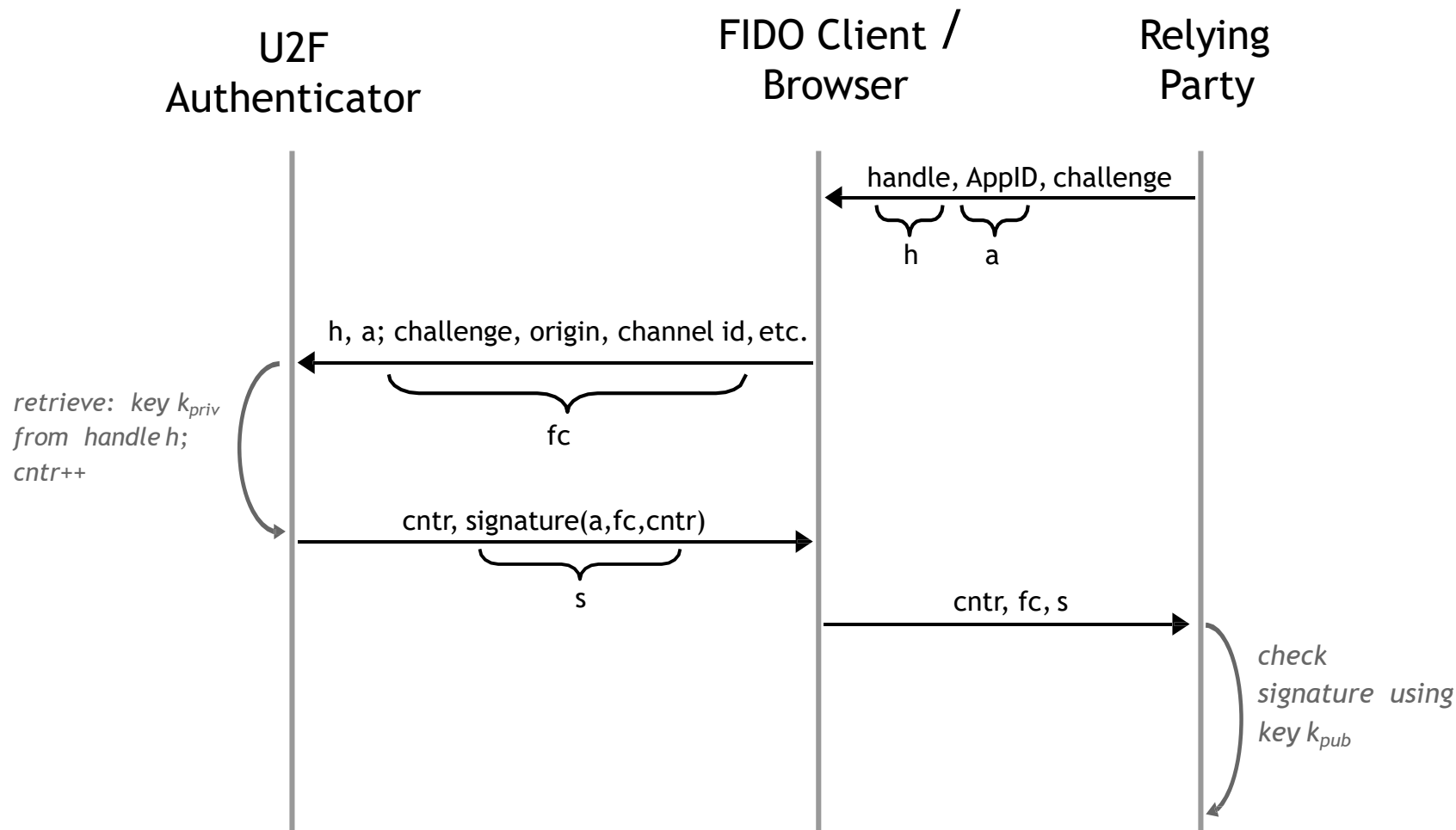
FIDO authenticator concept
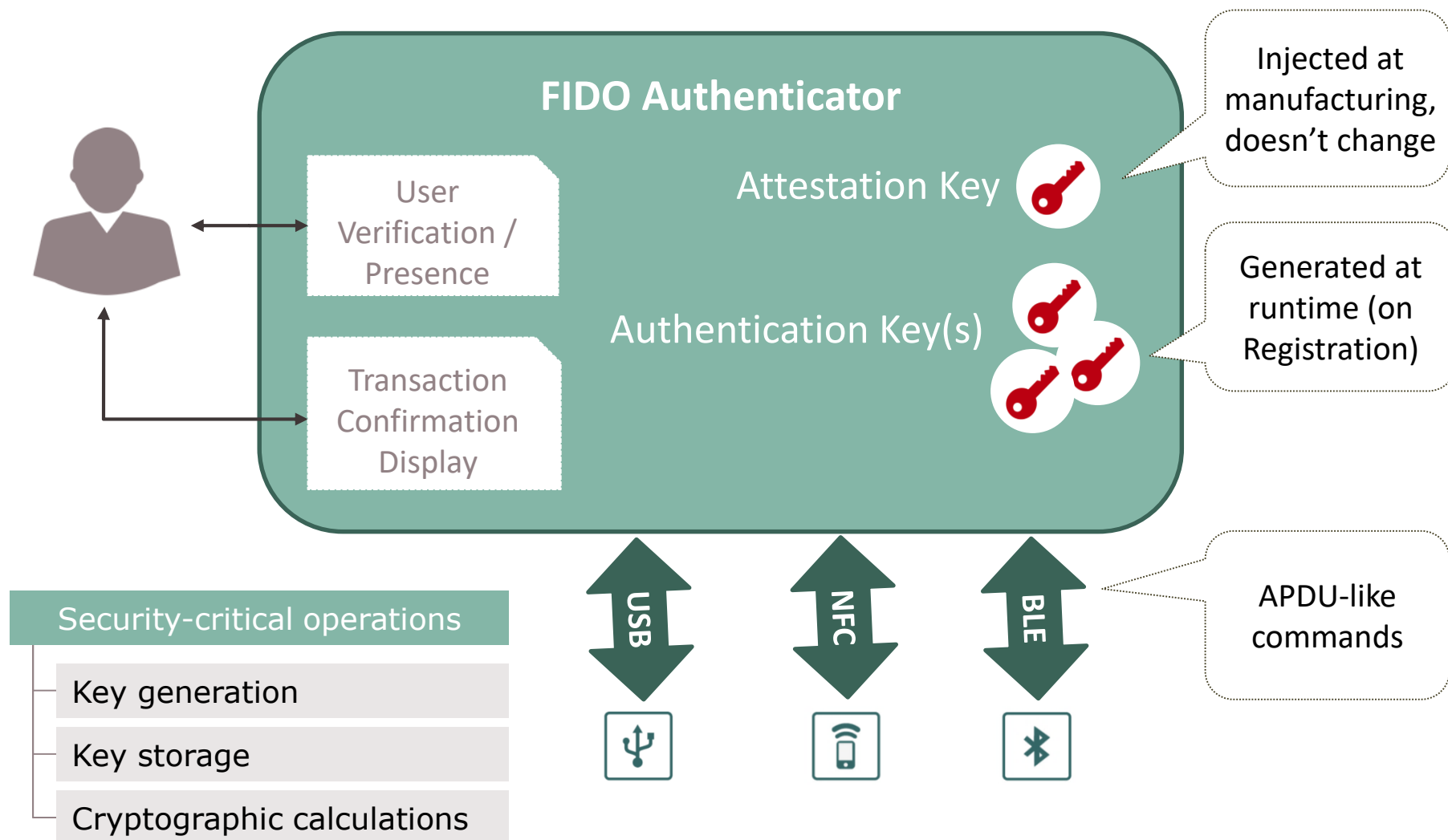
FIDO Authenticator

User Verification / Presence

Transaction Confirmation Display

Attestation Key — Injected at manufacturing, doesn't change

Authentication Key(s) — Generated at runtime (on Registration)

USB NFC BLE — APDU-like commands

Security-critical operations
- Key generation
- Key storage
- Cryptographic calculations

Agenda

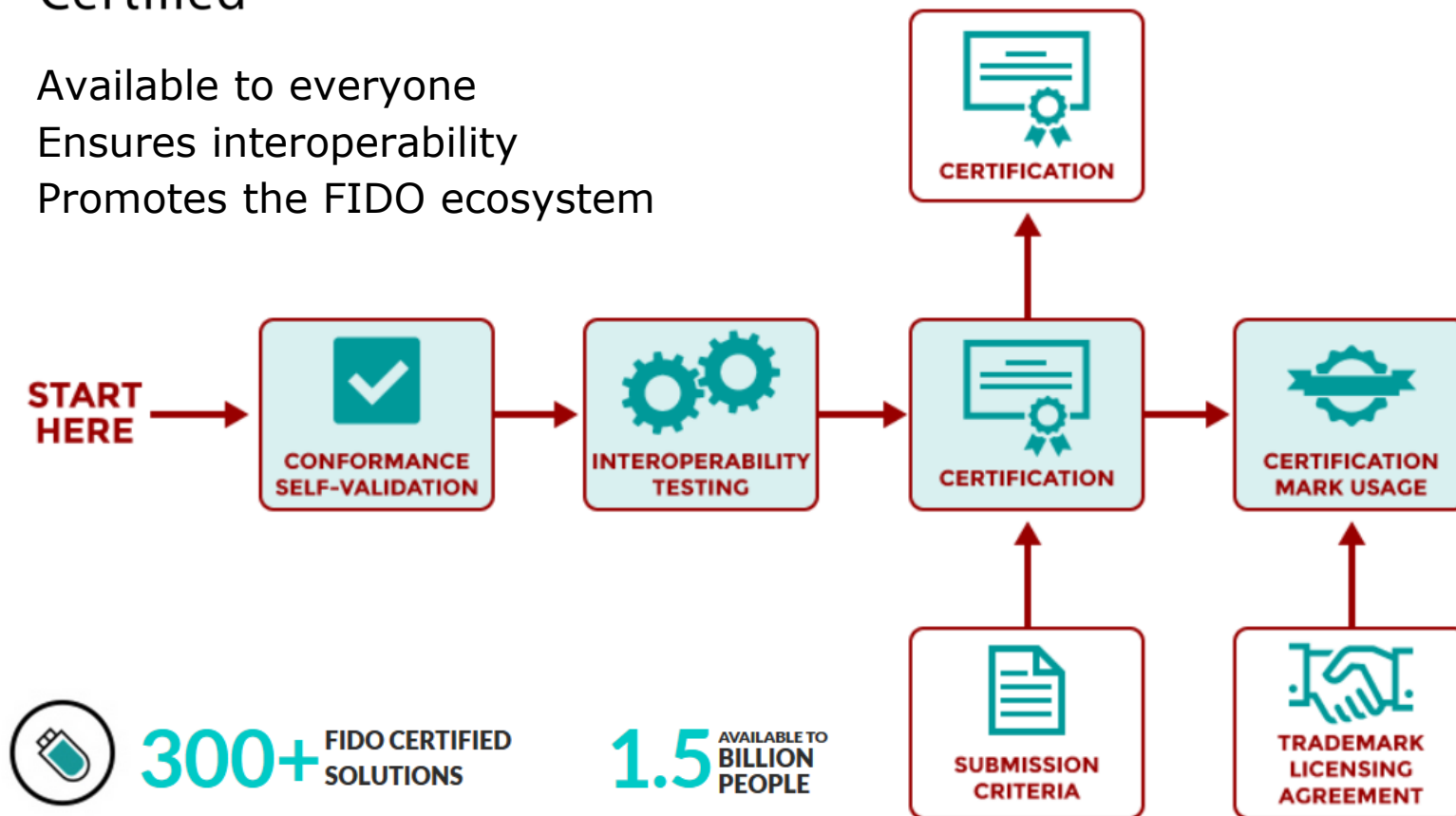– 2012: Foundation of the FIDO Alliance
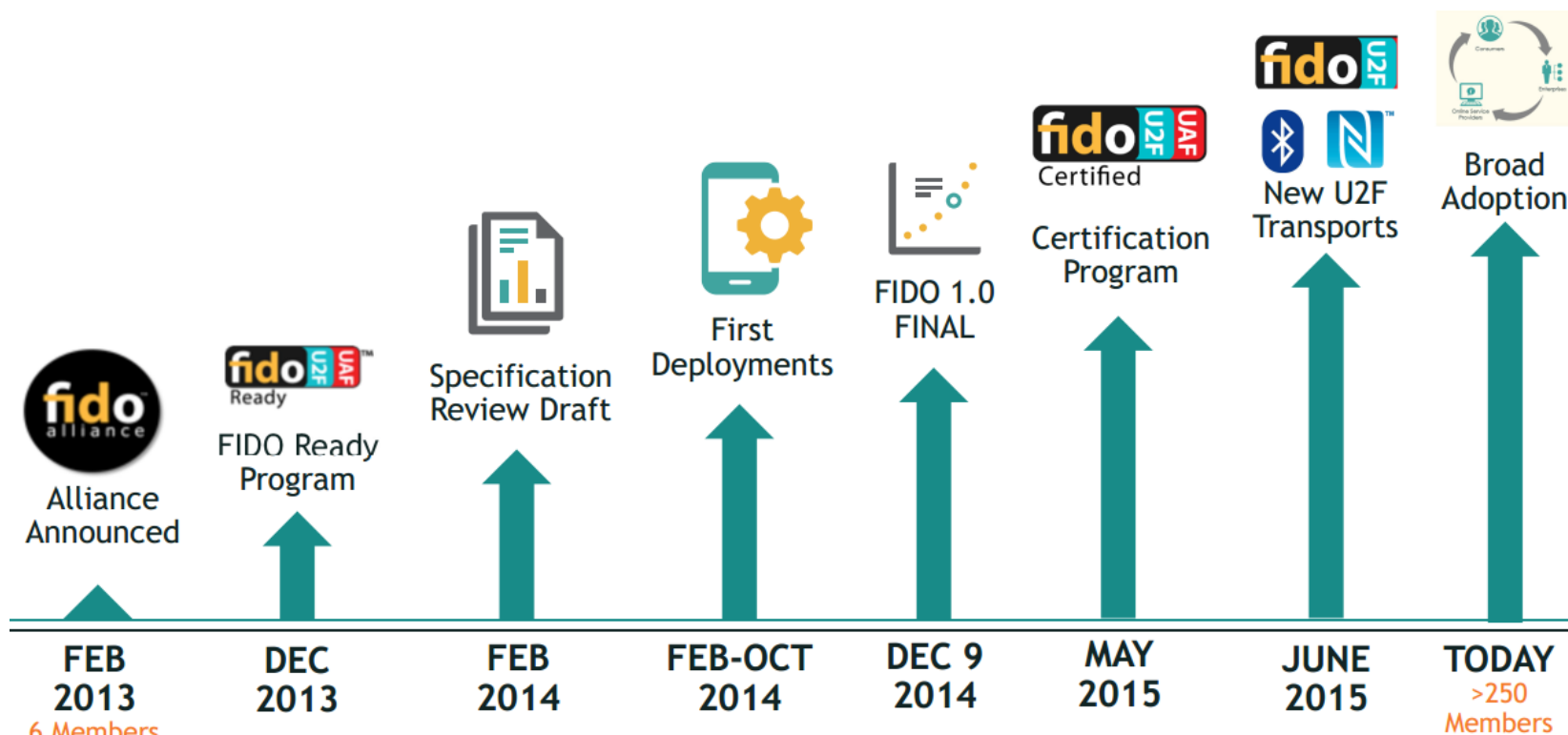
FIDO Alliance board members

FIDO certification
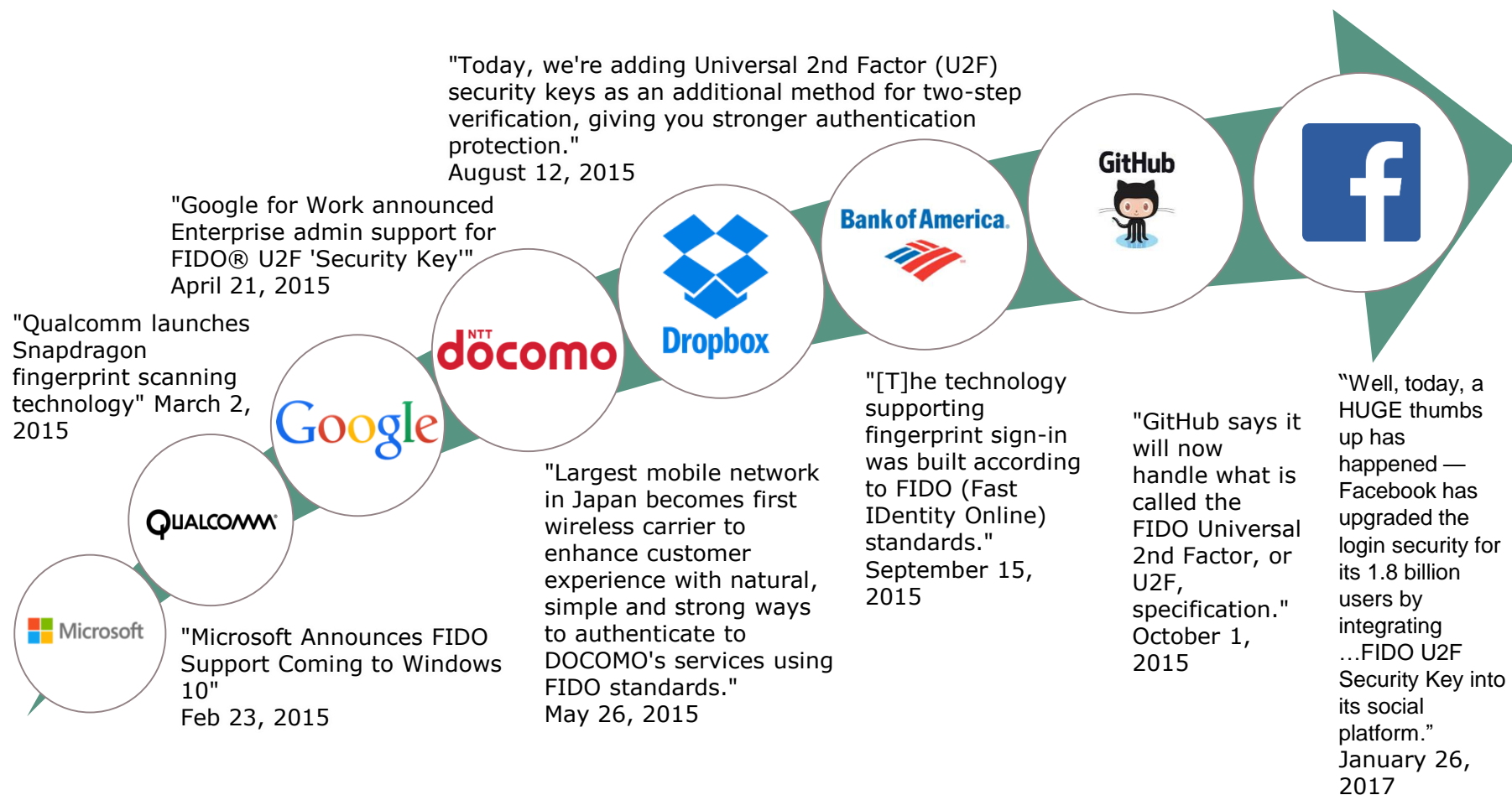

› Available to everyone
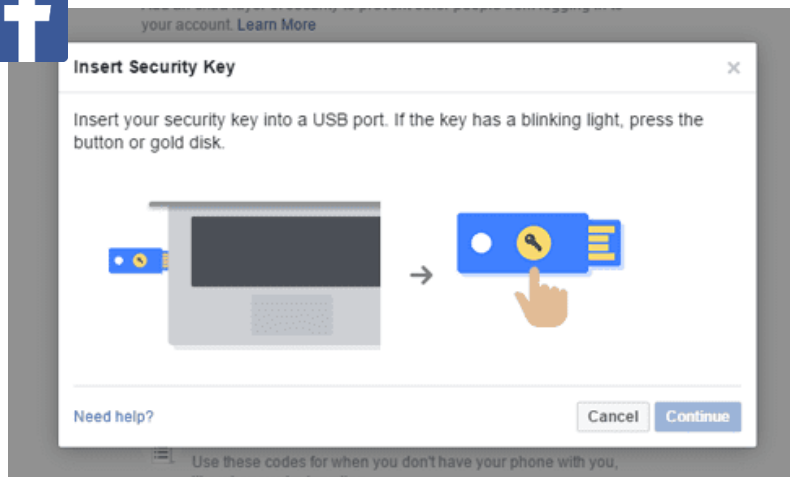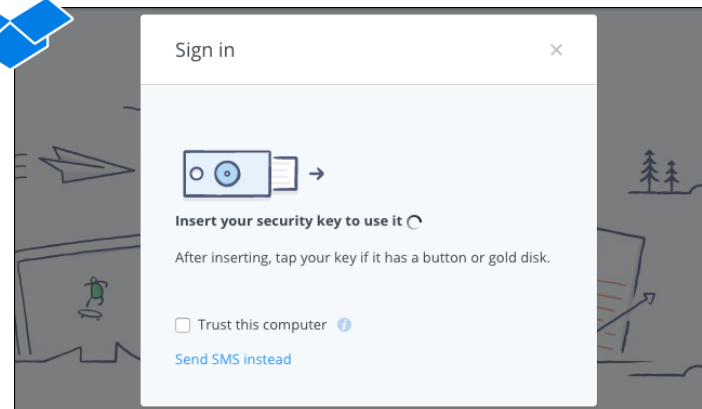› Ensures interoperability
› Promotes the FIDO ecosystem

https://fidoalliance.org/certification

"Today, we're adding Universal 2nd Factor (U2F) security keys as an additional method for two-step verification, giving you stronger authentication protection."
August 12, 2015

"Google for Work announced Enterprise admin support for FIDO® U2F 'Security Key'"
April 21, 2015

"Qualcomm launches Snapdragon fingerprint scanning technology" March 2, 2015

"Microsoft Announces FIDO Support Coming to Windows 10"
Feb 23, 2015

"Largest mobile network in Japan becomes first wireless carrier to enhance customer experience with natural, simple and strong ways to authenticate to DOCOMO's services using FIDO standards."
May 26, 2015

"[T]he technology supporting fingerprint sign-in was built according to FIDO (Fast IDentity Online) standards."
September 15, 2015

"GitHub says it will now handle what is called the FIDO Universal 2nd Factor, or U2F, specification."
October 1, 2015

"Well, today, a HUGE thumbs up has happened — Facebook has upgraded the login security for its 1.8 billion users by integrating …FIDO U2F Security Key into its social platform."
January 26, 2017

The U2F user experience

Agenda

1	Introduction
2	The FIDO Standard
3	The FIDO Ecosystem
4	The Future of FIDO

FIDO 2.0

› Developed since February 2016

› Official announcement at April 16, 2018 at the RSA Conference

RSA Conference

When: April 16, 2018 - April 20, 2018 - *All Day*
Where: Moscone Center, San Francisco, USA

RSA Conference is one of the largest and most influential events in cybersecurity. Look for the Alliance and our members in session and on the expo hall floor.

Google and Microsoft Debut: Replacing Passwords with FIDO2 Authentication

April 20, 2018 | 10:15 AM – 11:00 AM

FIDO's modern authentication ecosystem is leaping ahead in browsers and online platforms. In this panel, Google and Microsoft security team leaders will debut new authentication options based on FIDO2 and W3C standards in their browsers and other core products so online services can go beyond passwords with stronger, simpler authentication using the same devices and security people use every day. (More)

https://fidoalliance.org/events/rsac-2018/

Authentication for industrial applications

› FIDO for industry
› Robotic security
› Contactless user/device authentication

Open PhD Position

PhD Thesis: Secure Industrial IoT

Contact:
andrea.hoeller@infineon.com

At a glance

During the 3 years thesis sample system implentations in selected Industrial IoT (IIoT) use cases shall be built up ensuring system security by means of correct application of basic security components, role definitons and policies, especially in environments making use of Near Field Communication (NFC), wireless communication channels and mobile devices.

Quick info

| Location	Graz	Type	Full time
Entry level	Thesis support	Contract	Temporary
Job ID	24752		
Start	immediately		

During the 3 years thesis sample system implentations in selected Industrial IoT (IoT) use cases shall be built up ensuring system security by means of correct application of basic security components, role definitons and policies, especially in environments making use of Near Field Communication (NFC), wireless communication channels and mobile devices.

Based on these implementations **a valid projection to the future integration of new cryptographic protocols (e.g. including post quantum cryptography) and methods shall be investigated.** Parts of the thesis work will be performed in the framework of the ECSEL project PRODUCTIVE4.0 - https://productive40.eu/ conducting research on user authentication and authorization mechanisms by means of two factor authentication protocols according to the fast IDentity Online (FIDO - https://fidoalliance.org/) standard and variants thereof.

https://www.infineon.com/cms/en/careers/jobsearch/jobsearch/24752-PhD-Thesis-Secure-Industrial-IoT/

Summary

› An ecosystem and standardization are essential

› The goals of FIDO are

  – good usability

  – high privacy and security

  – standardization

› FIDO 2.0 will be presented at the RSA conference, April 16 2018
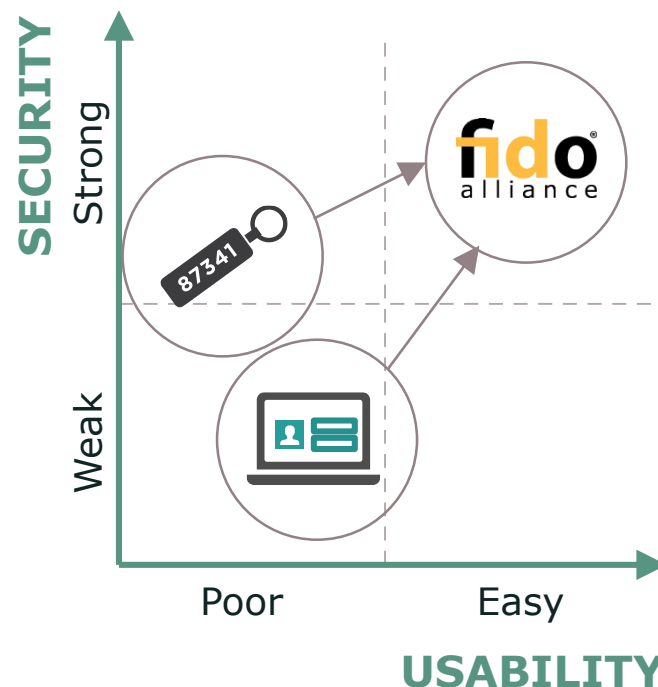
Part of your life. Part of tomorrow.

infineon