FIGI Security Clinic

How FIDO Helps Meeting Regulatory Requirements

Dr. Rolf Lindemann, Nok Nok Labs
rolf@noknok.com

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

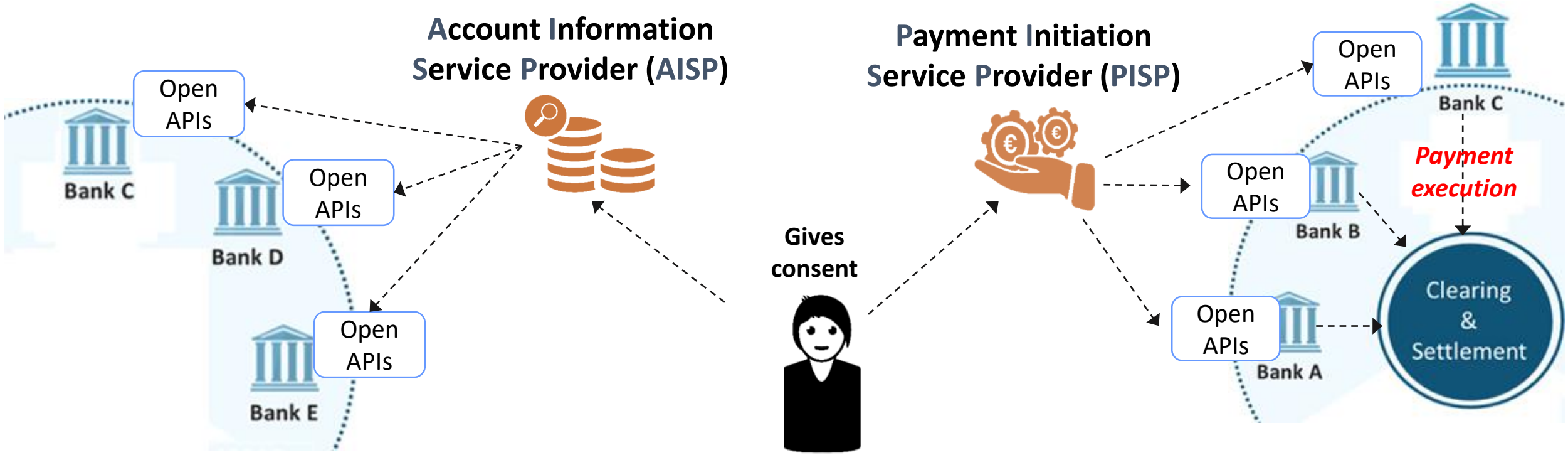
FIDO & PSD2

What is PSD2?

- “An attempt to drive innovation through regulation”
  - Regulates banks, payment services and other related financial services throughout the European Union (EU) and European Economic Area (EEA)
  - Goals:
    - Increase competition and participation in financial services and payments by creating a path for non-bank Third Party Providers (TPPs), including:
      - Account Information Service Providers (AISPs) – entities that gather data on a user’s accounts and present a unified view of finances, as well as offer advice
      - Payment Initiation Service Providers (PISPs) – entities that don’t hold payment accounts for users, but do allow users to make payments through them
    - Give consumers non-bank choices in payments and financial services
    - Improve consumer protection

PSD2 – Key Provisions

- New Access to Account mandate ➔ Open APIs
- New Strong Customer Authentication mandate
- New Third Party Provider (TPP) roles



What the EBA SCA Rules Require

Transactions require Multi-Factor Authentication (MFA) – 2 of 3 elements:

- Something you know (password or PIN)
- Something you possess (phone, token, card)
- Something you are (biometric)

Passw00rd

A "multi-purpose" device must protect the independence of authentication elements

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:

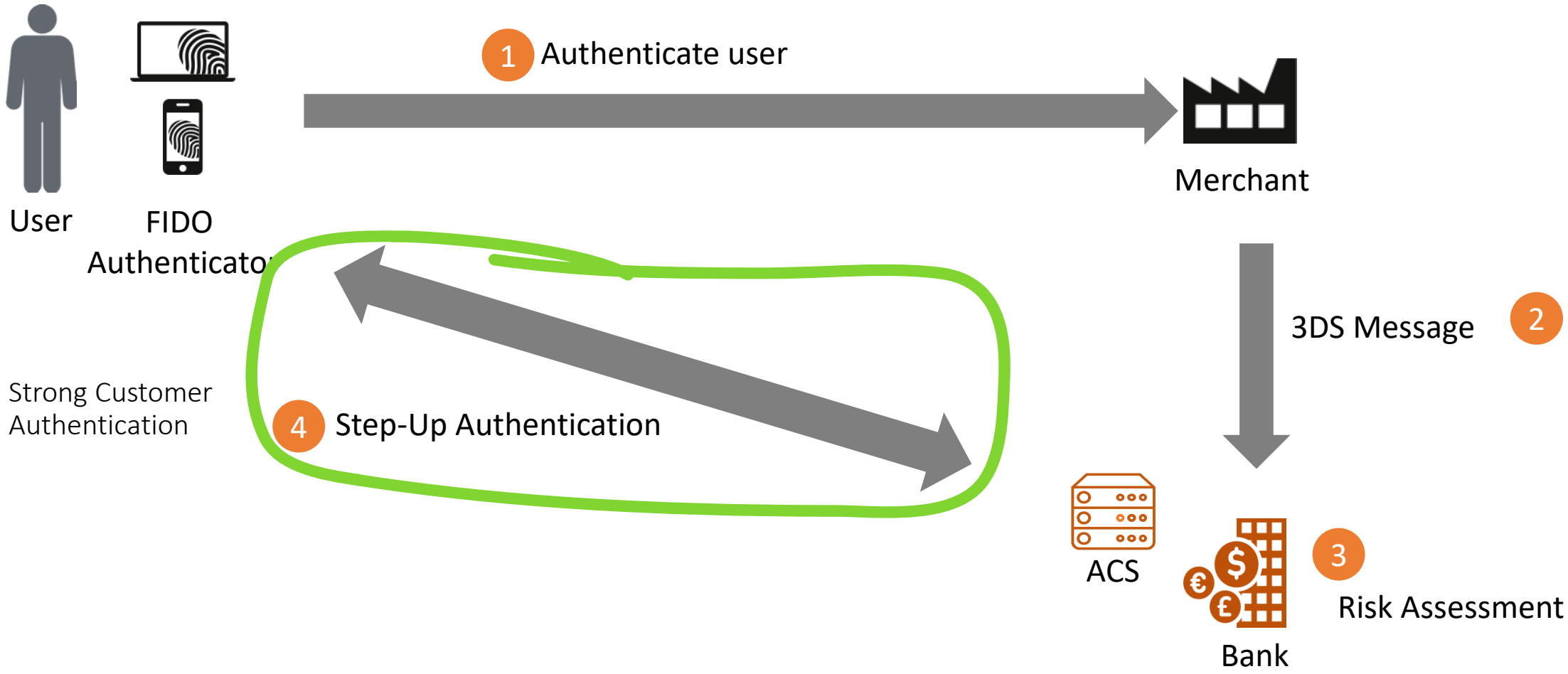
   (a) the use of separated secure execution environments through the software installed inside the multi-purpose device;

   (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party;

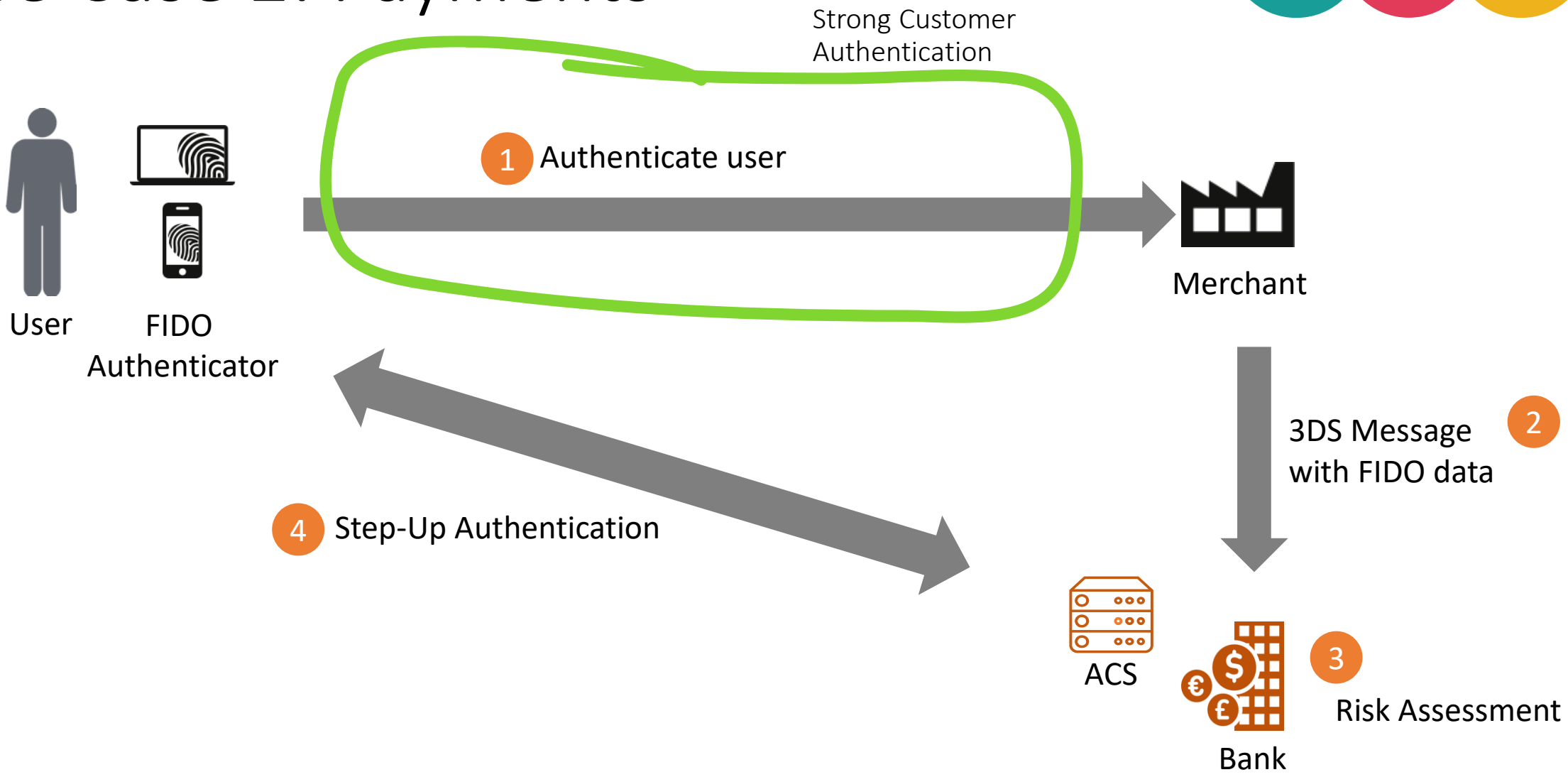
   (c) where alterations have taken place, mechanisms to mitigate the consequences thereof.

Use Case 1: Online Banking

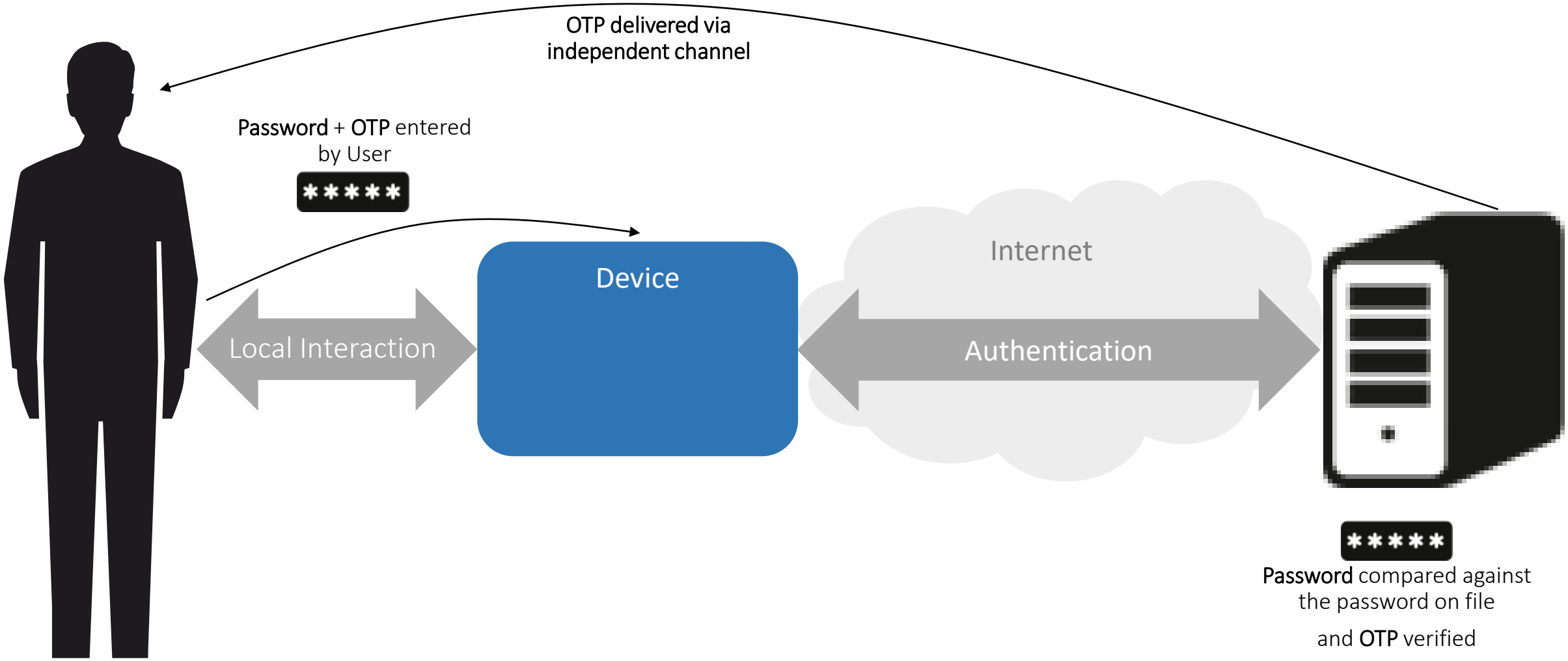
Use Case 2: Payments



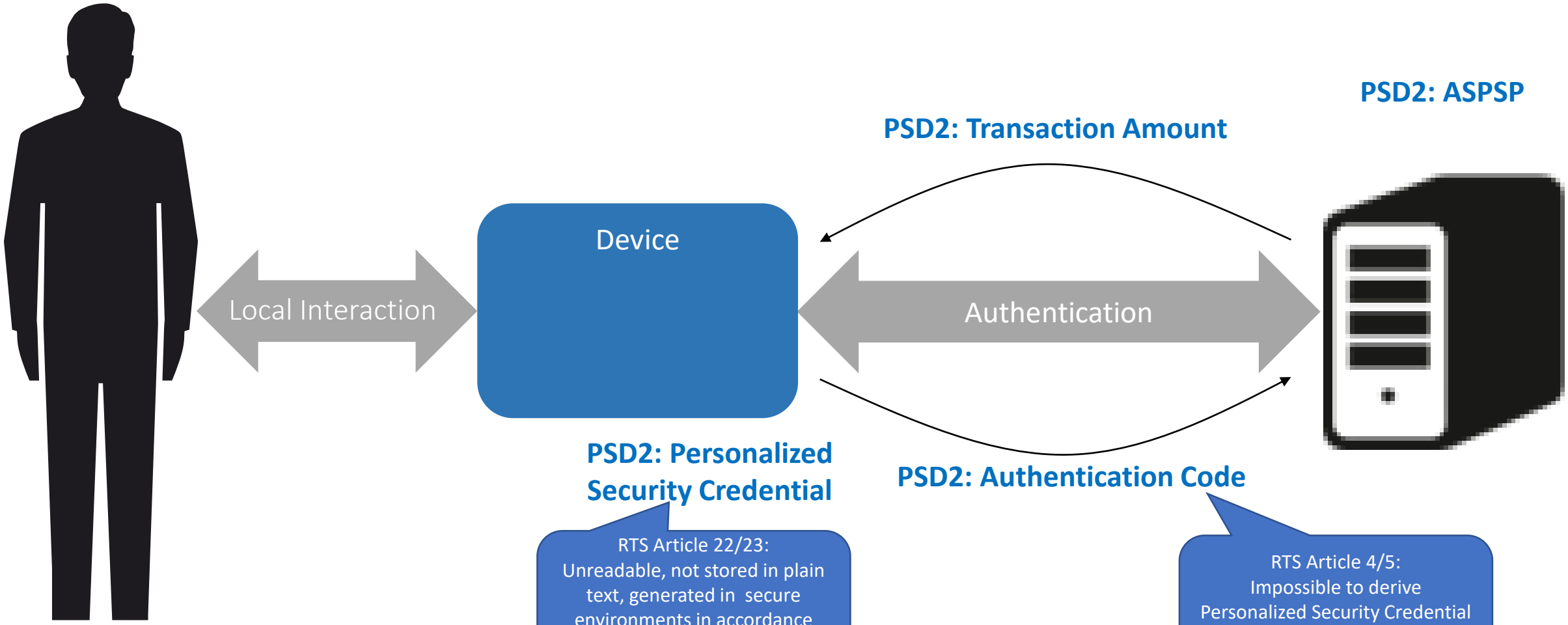
Use Case 2: Payments



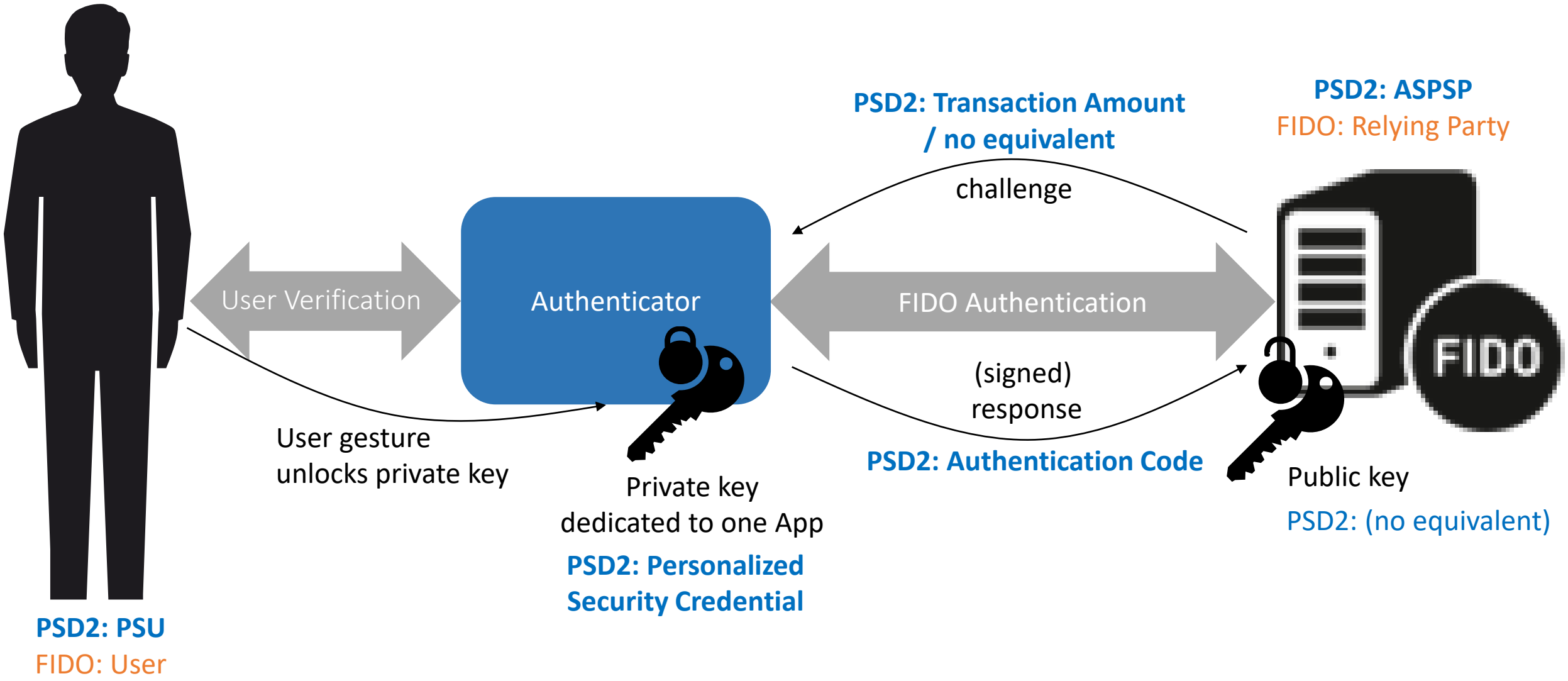
Pre-PSD2 View of Authentication



PSD2 View of Authentication



Mapping PSD2 Terminology to FIDO



FIDO & PSD2 Summary

- FIDO standards: a good solution for any of the authentication models
  - Security and Privacy by Design
  - Meet all the PSD2 RTS requirements
  - Aligned with authorization frameworks
- FIDO standards maximize reach
  - They support a large variety of devices
- FIDO standards: versatile and future proof
  - Bank can support the redirection and decoupled models
  - Bank can propose the embedded model to TPPs that integrate FIDO authenticators in their solutions

Open Banking Standards in the US

FINANCIAL SERVICES Information Sharing and Analysis Center

Want a copy?
Reach out to
Eric Guerrino at
eguerrino@fsisac.com

Press Releases

FS-ISAC Enables Safer Financial Data Sharing with API

Tuesday, February 13, 2018

FS-ISAC publishes new API to facilitate safer information sharing of consumer financial information between financial institutions and technology companies

RESTON, VA., February 13, 2018 – In an effort to keep consumer financial information and businesses safer from cyberattacks, the FS-ISAC announced today the publication of an updated application programing interface (API) for more secure, tokenized data transfer. The API is being offered free of charge to the industry.

The API and its associated Control Considerations White Paper, is the culmination of more than one year of activities of the FS-ISAC Data Aggregation Work Group, comprising more than 25 financial services firms and contributions from multiple financial technology (fintech) firms that provide data aggregation tools and services.

"Creating a standard API for secure data sharing benefits everyone in the data aggregation ecosystem," said Eric Guerrino, FS-ISAC chief operations officer. "We want to ensure that everyone from the consumer to the financial institution and the data aggregators can share information safely, quickly and accurately. The API gives consumers a more seamless and secure experience enabling greater awareness, control and peace of mind over financial data."

Over a lifetime, consumer data may be scattered throughout several financial institutions. This creates the need to log into many accounts to access loans, deposits, 401(k) or bill pay transactions. Once a financial services firm adopts and utilizes the API, the consumer will be able to access their own information seamlessly and securely, creating a higher degree of awareness, control and accuracy over sensitive data.

Financial institutions and fintech companies benefit by shifting the aggregation traffic away from the consumer login pages to a more efficient and light-weight secure format. This requires less infrastructure to support and eliminates the risk of storing credentials. Aggregators benefit by eliminating the need to maintain thousands of unique versions of screen-scraping scripts, also significantly reducing risk of stored credentials.

This API supports major enhancements to secure financial data transfer including improvements in speed and error reduction. Through tokenization, the API improves security so that financial institutions can share information with account aggregators more securely. It also facilitates faster secure transfer of tokenized information from point to point.

How it works:

- When a financial application user wishes to set up or add a bank, brokerage, or insurance account, they will be seamlessly passed to a secure server at the financial institution to begin the enrollment process.

https://www.fsisac.com/article/fs-isac-enables-safer-financial-data-sharing-api

Highlights of US FS-ISAC approach

- Standard APIs to enable secure third-party access
- When a consumer wishes to set up or add a bank, brokerage, or insurance account to a third-party service, they will be seamlessly passed to a secure server at their financial institution to begin the enrollment process.
- The consumer is presented with the financial institution's consent page, where they authorize which data or access privileges they wish to share with the financial application, giving consumers control.
- After authenticating, the consumer is then seamlessly passed back to the financial application. Data sharing between financial application servers and financial institution servers is then done securely via a unique virtual token that identifies the consumer and their respective accounts.
- Standards recommended: OAuth, OpenID Connect, FIDO

FIDO & Privacy

Berners-Lee's "Contract for the Web"

Governments

Principle 1
Ensure everyone can connect to the internet
READ MORE →

Principle 2
Keep all of the internet available, all of the time
READ MORE →

Principle 3
Respect and protect people's fundamental online privacy and data rights
READ MORE →

Companies

Principle 4
Make the internet affordable and accessible to everyone
READ MORE →

Principle 5
Respect and protect people's privacy and personal data to build online trust
READ MORE →

Principle 6
Develop technologies that support the best in humanity and challenge the worst
READ MORE →

Citizens

Principle 7
Be creators and collaborators on the Web
READ MORE →

Principle 8
Build strong communities that respect civil discourse and human dignity
READ MORE →

Principle 9
Fight for the Web
READ MORE →

Principle 5

Respect and protect people's privacy and personal data to build online trust

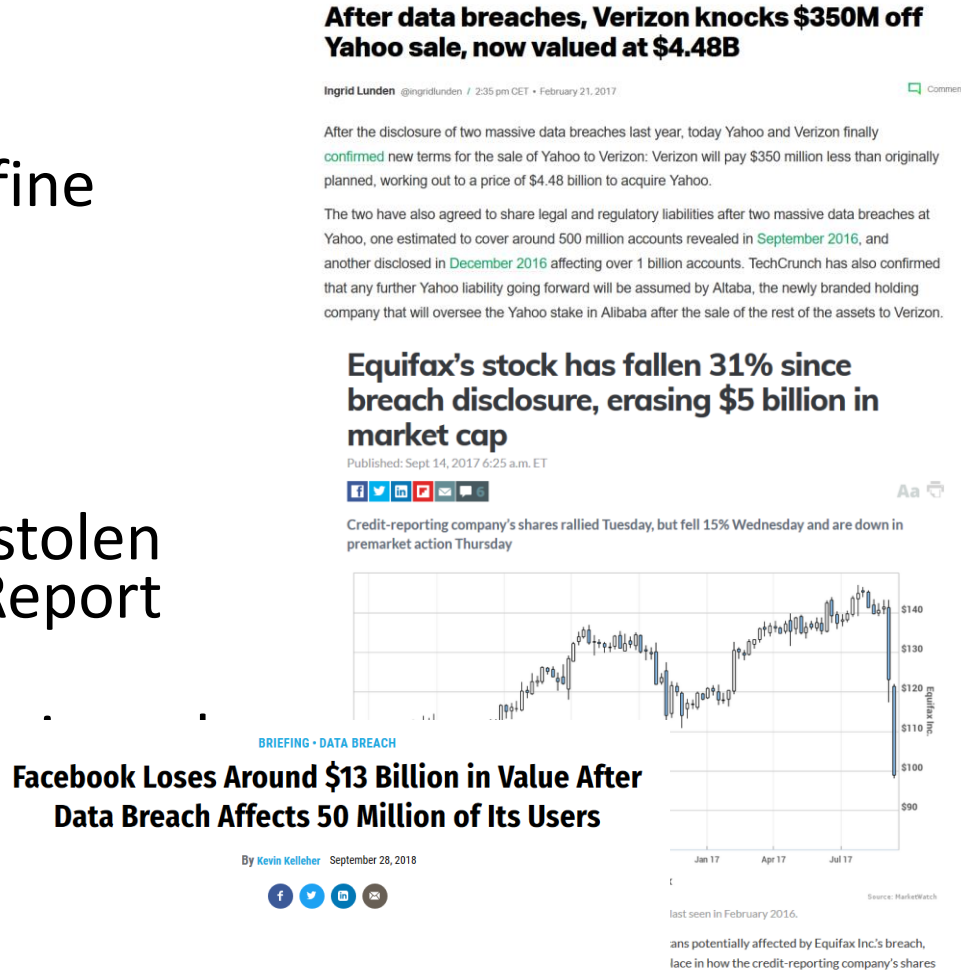
So people are in control of their lives online, empowered with clear and meaningful choices around their data and privacy

1. By giving people control over their privacy and data rights, with clear and meaningful choices to control processes involving their privacy and data
2. By supporting corporate accountability and **robust privacy and data protection by design**
3. By making privacy and data rights equally available to everyone

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Why is FIDO relevant here?

- Attackers focus on interesting attack targets (i.e. maximize value for “attack investment”)
- Data privacy regulations like GDPR and CCPA define biometric data as “personal data”.
- Failure to protect personal data appropriately
  - damages your corporate brand
  - might lead to a fine
- 81% of data breaches in 2016 involved weak or stolen passwords (Verizon Data Breach Investigations Report 2017)
- People with legitimate access need to be autl properly
  - ➔ FIDO Authentication



After data breaches, Verizon knocks $350M off Yahoo sale, now valued at $4.48B

Ingrid Lunden @ingridlunden / 2:35 pm CET • February 21, 2017

Comment

After the disclosure of two massive data breaches last year, today Yahoo and Verizon finally confirmed new terms for the sale of Yahoo to Verizon: Verizon will pay $350 million less than originally planned, working out to a price of $4.48 billion to acquire Yahoo.

The two have also agreed to share legal and regulatory liabilities after two massive data breaches at Yahoo, one estimated to cover around 500 million accounts revealed in September 2016, and another disclosed in December 2016 affecting over 1 billion accounts. TechCrunch has also confirmed that any further Yahoo liability going forward will be assumed by Altaba, the newly branded holding company that will oversee the Yahoo stake in Alibaba after the sale of the rest of the assets to Verizon.

Equifax’s stock has fallen 31% since breach disclosure, erasing $5 billion in market cap

Published: Sept 14, 2017 6:25 a.m. ET

Credit-reporting company’s shares rallied Tuesday, but fell 15% Wednesday and are down in premarket action Thursday

last seen in February 2016.

ans potentially affected by Equifax Inc.’s breach, lace in how the credit-reporting company’s shares

BRIEFING • DATA BREACH

Facebook Loses Around $13 Billion in Value After Data Breach Affects 50 Million of Its Users

By Kevin Kelleher September 28, 2018

2018 continues to be a challenging year for Facebook. The company’s stock closed down 3% Friday following reports that hackers gained access to the personal data on 50 million of its users.

EU GDPR

- In effect since May 25th 2018
- Defines data protection by design & by default
- Breaches have consequences (significant fines)
- Grants consumers the right to access, export, delete and rectify their data.
- FIDO provides privacy and strong security by design

EU GDPR

- Section 2, article 32
  - Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    - the pseudonymisation and encryption of personal data;
    - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

California: CCPA

- All companies that serve California residents and have at least $25 million in annual revenue must comply with the law.
- Companies of any size that have personal data on at least 50,000 people or that collect more than half of their revenues from the sale of personal data, also fall under the law.
- Companies have 30 days to comply with the law once regulators notify them of a violation. If the issue isn't resolved, there's a **fine of up to $7,500 per violation**.
- “Personal Information”
  - Identifiers such as a real name, alias, postal address, unique personal identifier, IP address, email address, account name, Social Security number, driver’s license number, passport number, etc.
  - Biometric information
  - Geolocation data
  - Audio, electronic, visual, thermal, olfactory or similar information

California: CCPA

CCPA grants the following rights to California consumers:

- The right to know what personal information is collected, used, shared or sold, both as to the categories and specific pieces of personal information;
- The right to delete personal information held by businesses and by extension, a business's service provider;
- The right to opt-out of sale of personal information. Consumers are able to direct a business that sells personal information to stop selling that information. Children under the age of 16 must provide opt in consent, with a parent or guardian consenting for children under 13.
- The right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA.

Privacy Summary

- FIDO's principle of no shared secrets is in line with "Privacy by Design"
- Bank keys (private & public) are generated in the authenticator
  - Only public key is uploaded to bank's server
- Local verification (of PIN, of biometric data)
  - No hackable data base of authentication credentials
- FIDO provides **state of the art** authentication

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

IoT

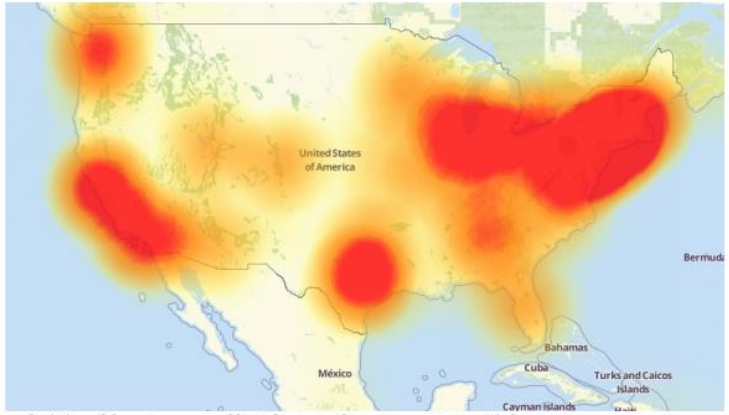
IoT Security Challenge

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.

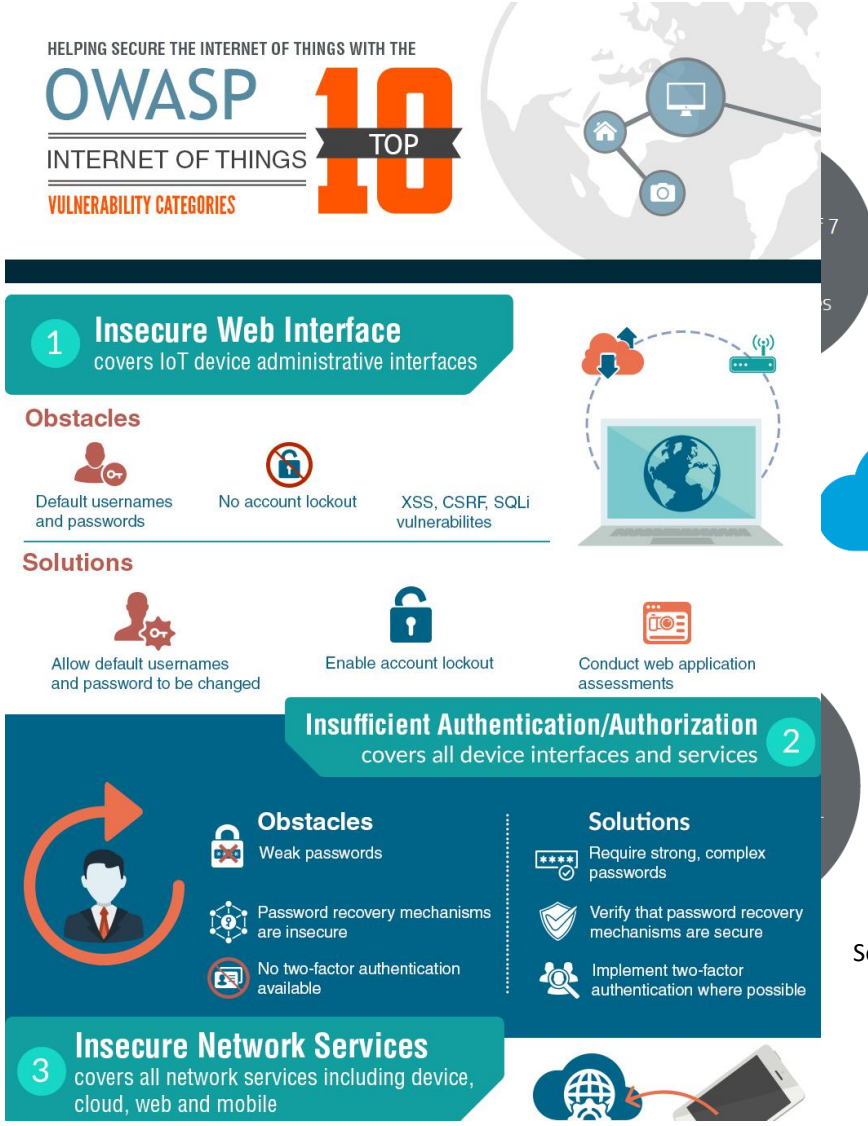
Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter,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

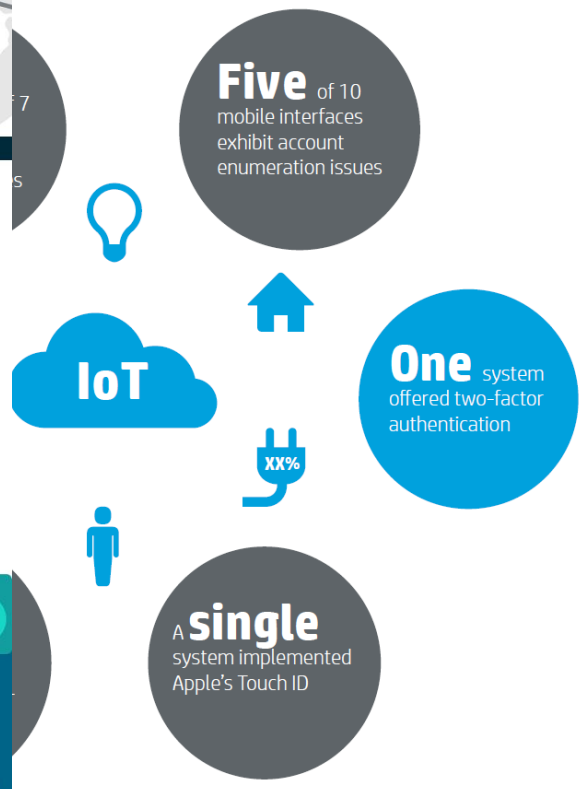


A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

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.*





Source: HP Enterprise IoT Home Security Systems

How to Secure Ecosystems

2

Isolate Applications into “rooms” from each other to prevent “eavesdropping” by malware (OS, App Store)

1

Harden the Foundation
At the CPU level e.g. TrustZone, SGX, …

3

Strong authentication makes sure only legitimate entities get access

IoT: USA

- USA President's Commission on Enhancing National Cyber Security identifies reliance on passwords as tempting target for malicious actors
- USA California Senate Bill 327 prohibits shared default passwords.

Stronger authentication of identities for interactions that require such proof must also be a key component of any approach for enhancing our nation's cybersecurity. Identity, especially the use of passwords, has been the primary vector for cyber breaches — and the trend is not improving despite our increased knowledge and awareness of this risk. Our reliance on passwords presents a tempting target for malicious actors.

Other important work that must be undertaken to overcome identity authentication challenges includes the development of open-source standards and specifications like those developed by **the Fast IDentity Online (FIDO)** Alliance. FIDO specifications are focused largely on the mobile smartphone platform to deliver multifactor authentication to the masses, all based on industry-standard public key cryptography. Windows 10 has deployed FIDO specifications (known as Windows Hello), and numerous financial institutions have adopted FIDO for consumer banking.

Today, organizations complying with FIDO specifications are able to deliver secure authentication technology on a wide range of devices, including mobile phones, USB keys, and near-field communications (NFC) and Bluetooth low energy (BLE) devices and wearables. This work, other standards activities, and new tools that support continuous authentication provide a strong foundation for opt-in identity management for the digital infrastructure.

Source: https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

IoT: EU

- EU ENISA's Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, proposes
  - countermeasures against default passwords and default usernames
  - considering use of "two-factor authentication (2FA) or multi-factor authentication (MFA), like smartphones, biometrics, etc."

Source: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

IoT: EU

- ETSI releases first globally applicable standard for consumer IoT security in Feb 19th 2019
- As more devices in the home connect to the internet, the **cyber security of the Internet of Things (IoT) is becoming a growing concern**. …
- **… Poorly secured products threaten consumer's privacy and some devices are exploited to launch large-scale DDoS (Distributed Denial of Service) cyber attacks**.
- As many IoT devices and services process and store personal data, this specification can help ensure that these are compliant with the General Data Protection Regulation (GDPR).

ETSI TS 103 645 V1.1.1 (2019-02)

CYBER;
Cyber Security for Consumer Internet of Things

4 Cyber security provisions for consumer IoT

4.1 No universal default passwords

IoT Summary

With the expected growth of IoT devices, asking users for usernames and passwords won‘t scale – not in terms of usability neither in terms of security.

FIDO Authentication is more convenient & more secure.

More resources

- The Future of Authentication for the Internet of Things (Webinar, https://www.youtube.com/watch?v=gfBDOOpZqOU)
- Interview on IoT DDoS Attack, see http://armdevices.net/2016/10/26/security-for-arm-iot-devices-milosch-meriac-arm-and-dr-rolf-lindemann-nok-nok-labs/
- FIDO Alliance recently launched the IoT Technical Working Group, see https://fidoalliance.org/internet-of-things/