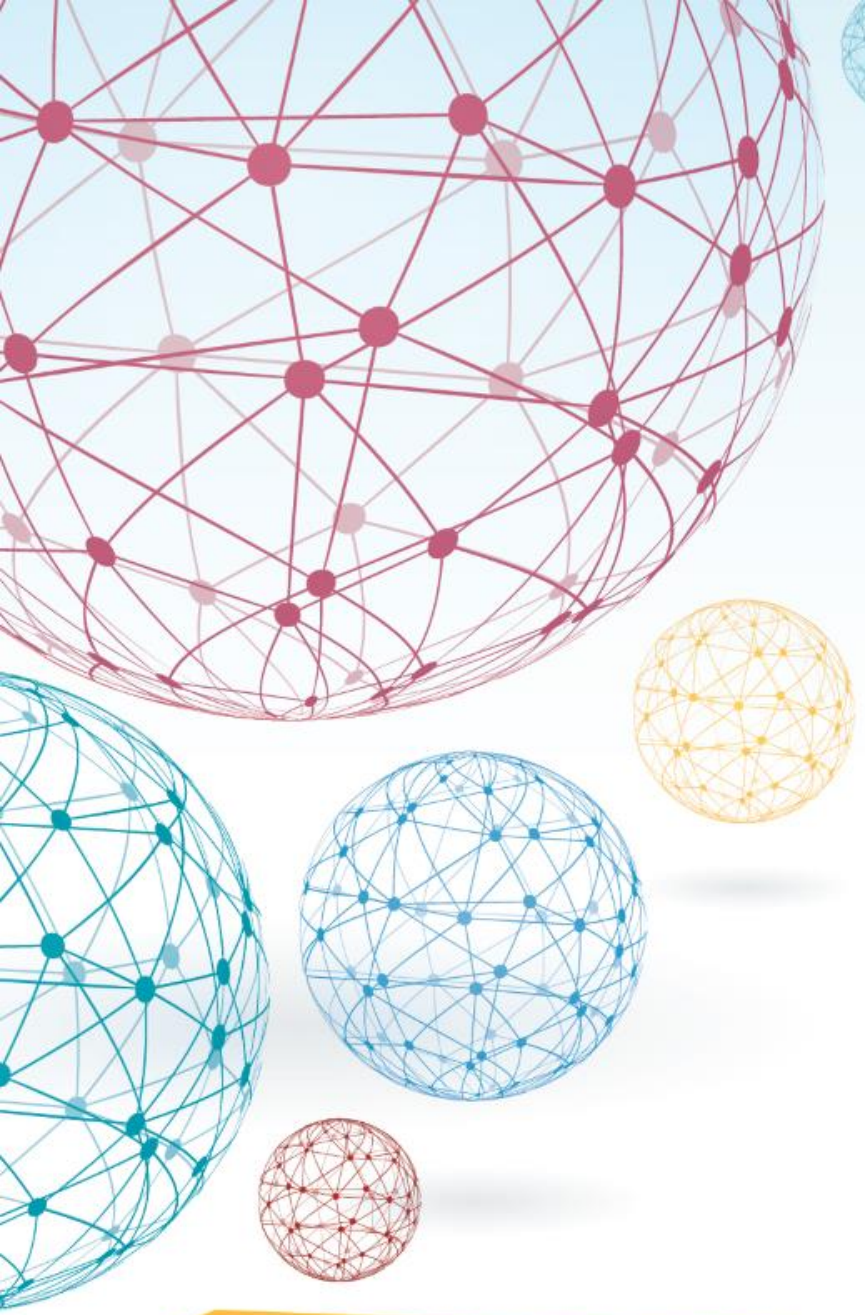


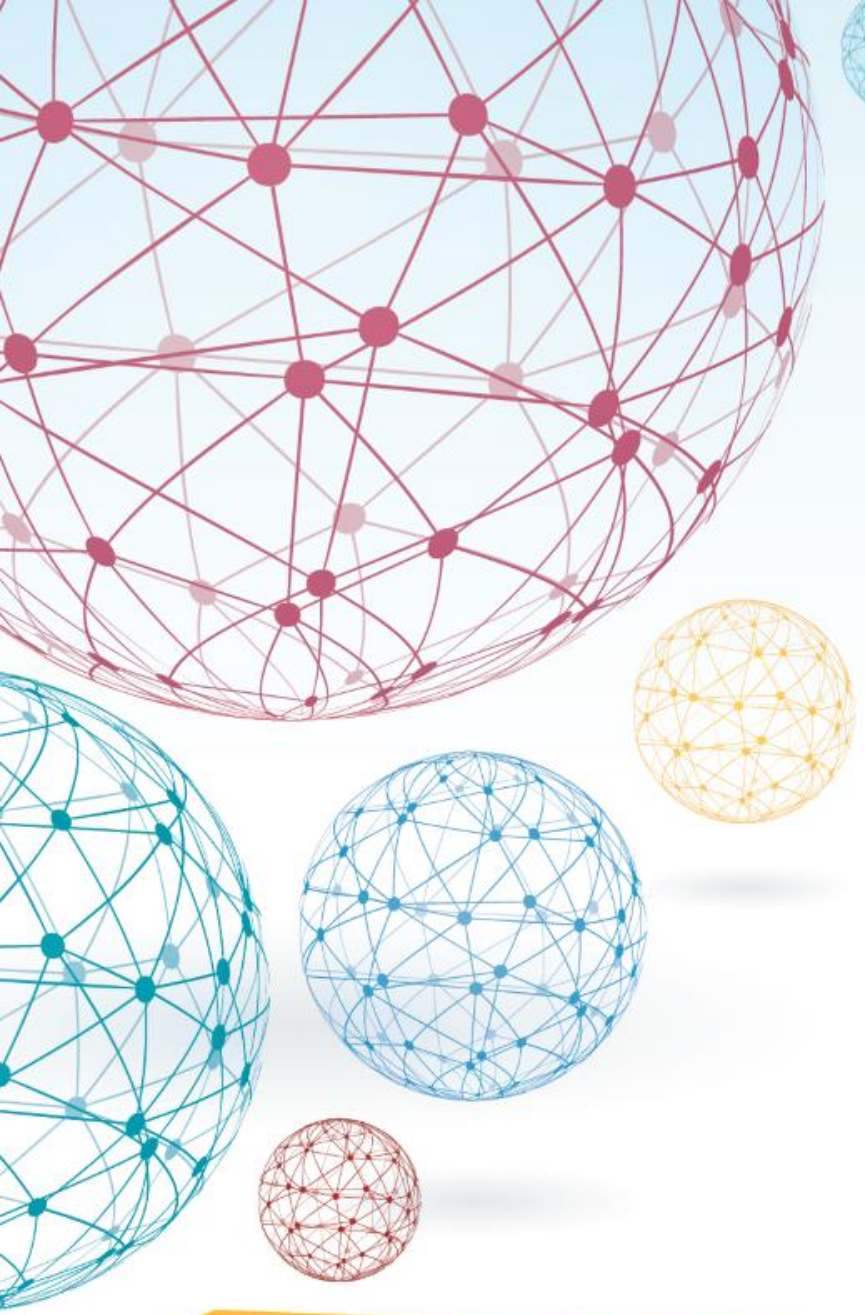
PSD2: SOLVING THE SCA CHALLENGE WHILE IMPROVING THE USER EXPERIENCE

ALAIN MARTIN – GEMALTO

FIDO EUROPE CO-CHAIR

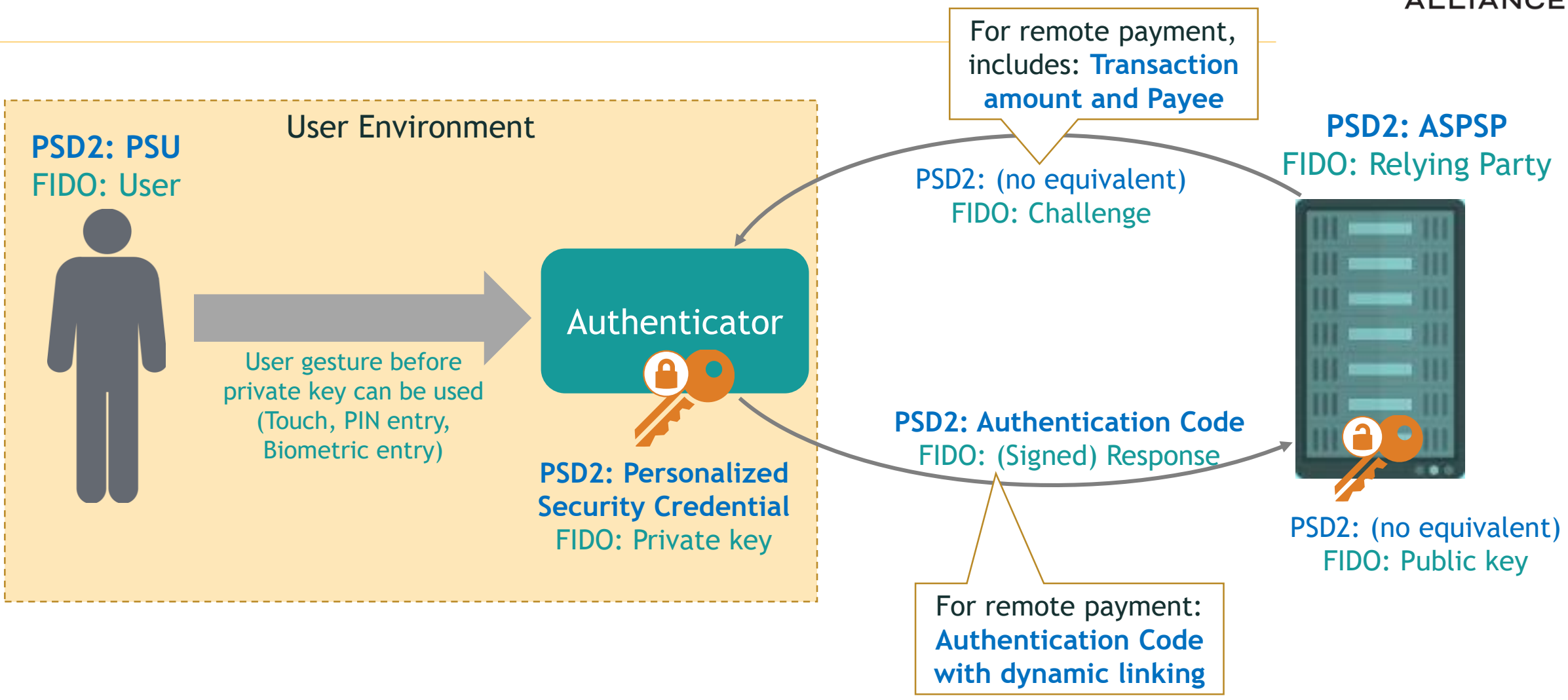
AGENDA

- FIDO and the requirements of PSD2/RTS
- The authentication models and how FIDO can help



FIDO AND THE REQUIREMENTS OF PSD2/RTS

VOCABULARY

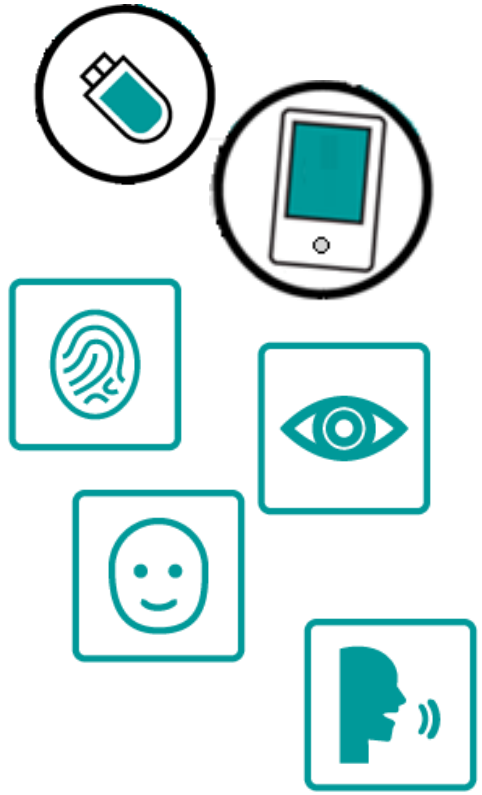


FIDO STANDARDS MEET THE PSD2/RTS REQUIREMENTS

- Based on Multi factor authentication
  ➔ Articles 4, 6, 7, 8 [RTS]

- Secure separated execution environments ranging from hardened Software to TEE to Secure Elements
  ➔ Articles 9, 22, 23, 25 [RTS]

- Support for dynamic linking
  ➔ Article 5 [RTS]



FIDO PROTECTS USER AUTHENTICATION DATA

- No shared secrets
  - Bank keys are generated in the authenticator
  - Public Key is uploaded to bank's server

  ➔ the security credential never leaves the authenticator

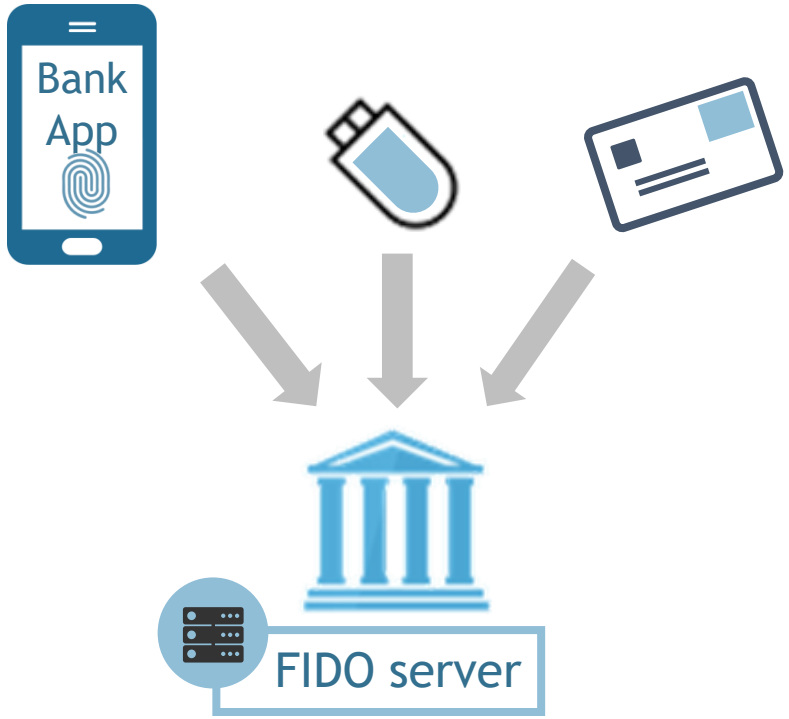
- Local verification (of PIN, of biometric data)

  ➔ In line with GDPR's "Privacy by Design"

  ➔ Facilitates deployment

FIDO SUPPORTS MULTI CHANNEL AUTHENTICATION

- Necessity to reach 100% users ➔ multiple devices may be necessary



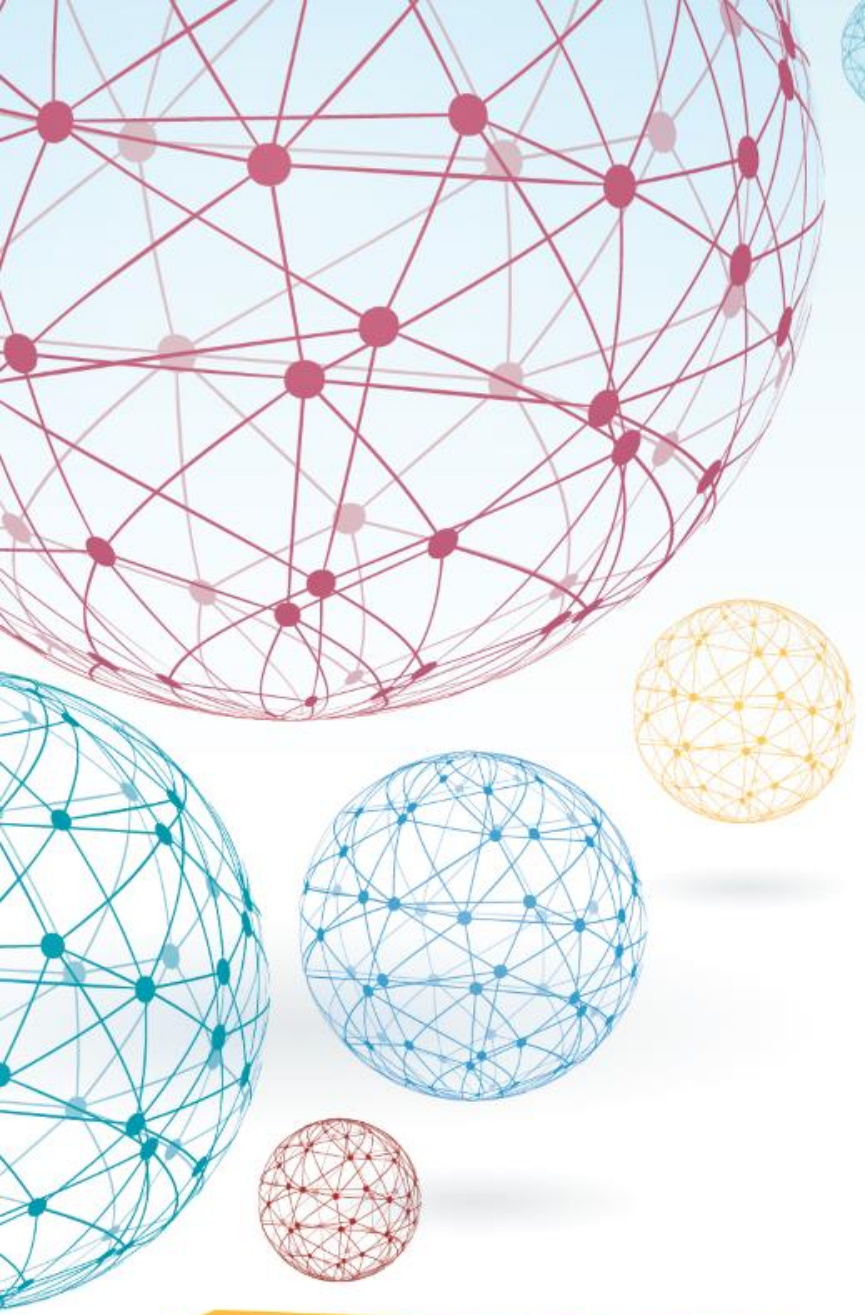
- A FIDO universal server supports *any* FIDO compliant authenticator

➔ FIDO Standards reduce the cost of deploying multiple devices

FIDO COMES WITH A CERTIFICATION PROGRAM

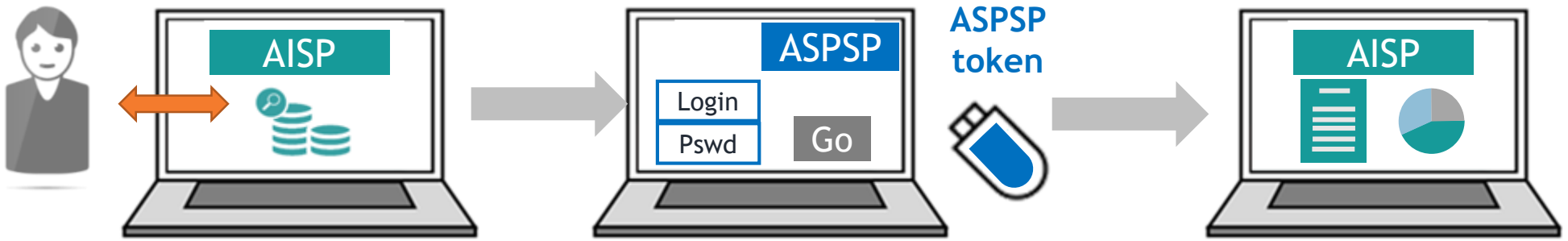
- Functional, by the FIDO Alliance
- Security, by the FIDO Alliance and independent accredited labs
- New biometrics certification

➔The RTS require security evaluation (Article 3 [RTS])

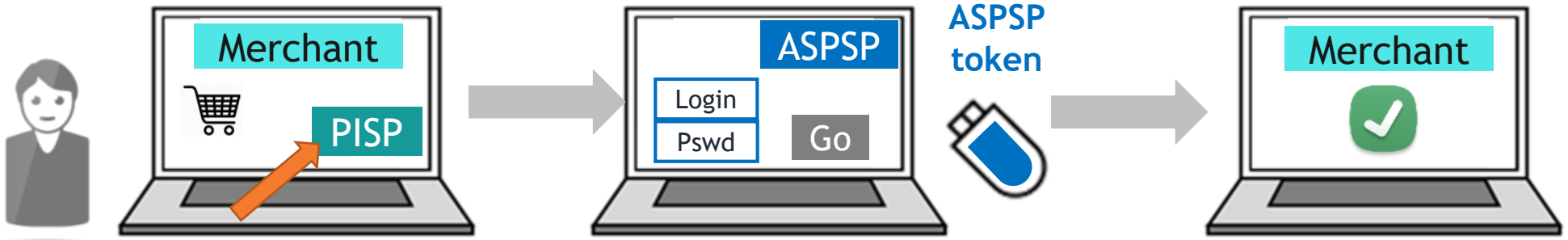


THE AUTHENTICATION MODELS AND HOW FIDO CAN HELP

THE “REDIRECTION” MODEL

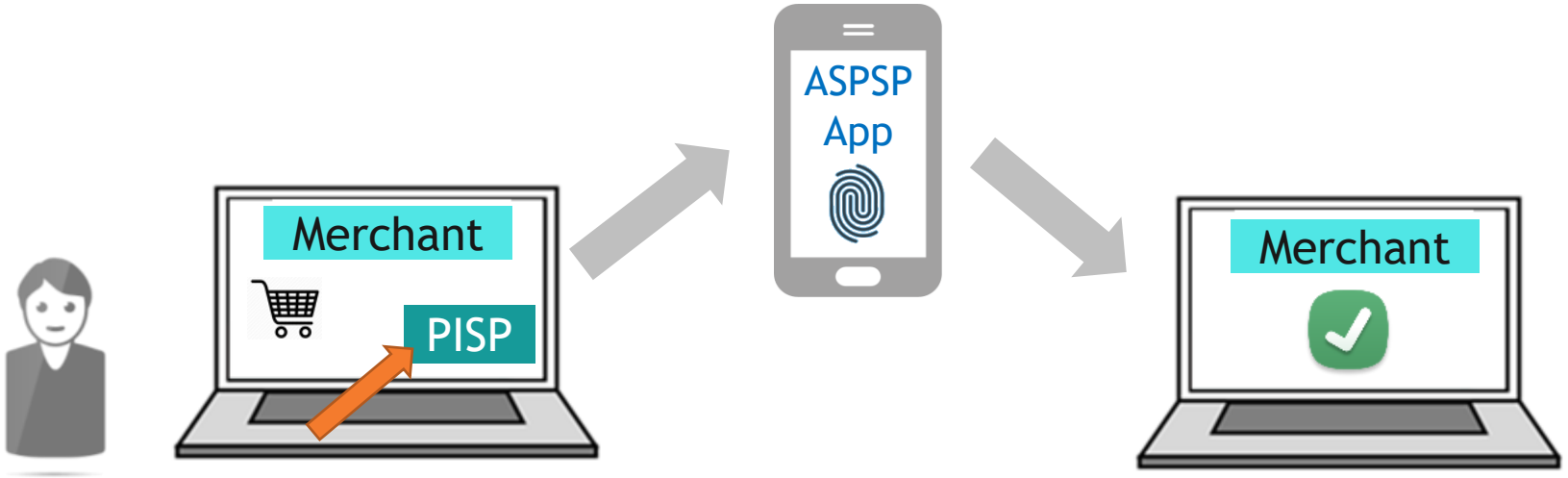


Example for account aggregation



Example for payment initiation

THE “DECOUPLED” MODEL



Example for payment initiation, from a browser

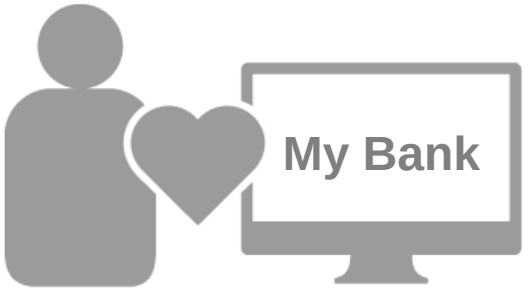
Example for account aggregation, on a smartphone

ADVANTAGES OF THE REDIRECTION/DECOUPLED MODEL

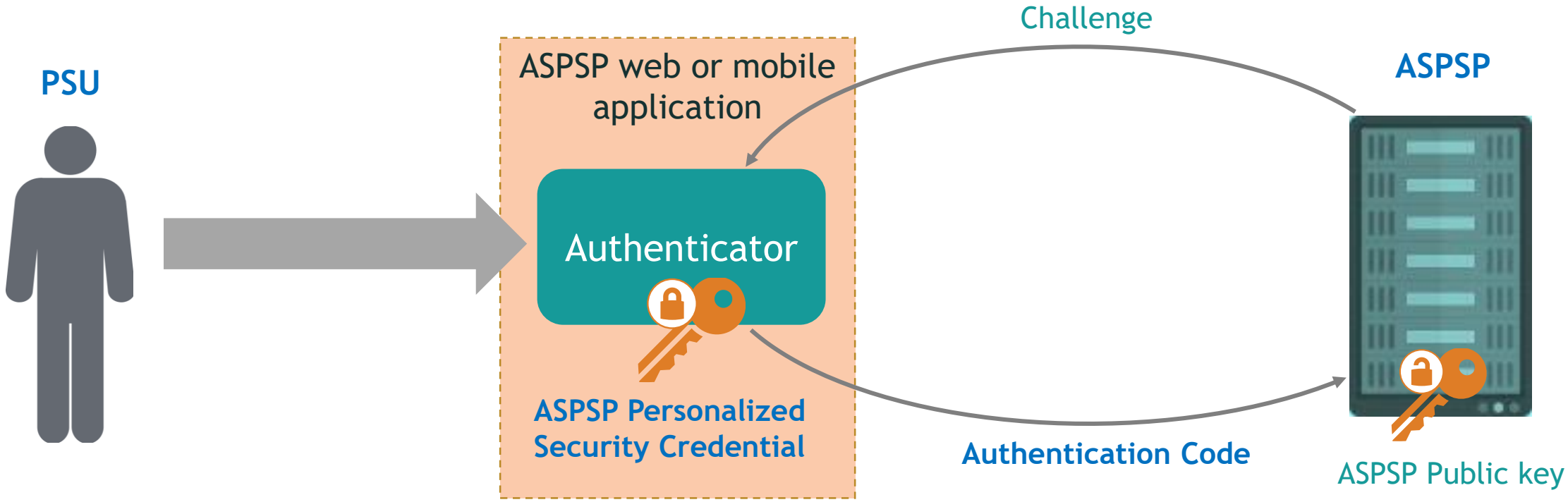
- Fastest way for a bank to implement SCA
  - Re-uses the authentication for bank's own services
  - In line with current practices
  - No dependence on other parties

- No impact on the Open APIs
  - There is no need for APIs to support authentication in these models

- A category of users will feel comfortable authenticating via the bank's interface
  - Trust
  - Familiarity

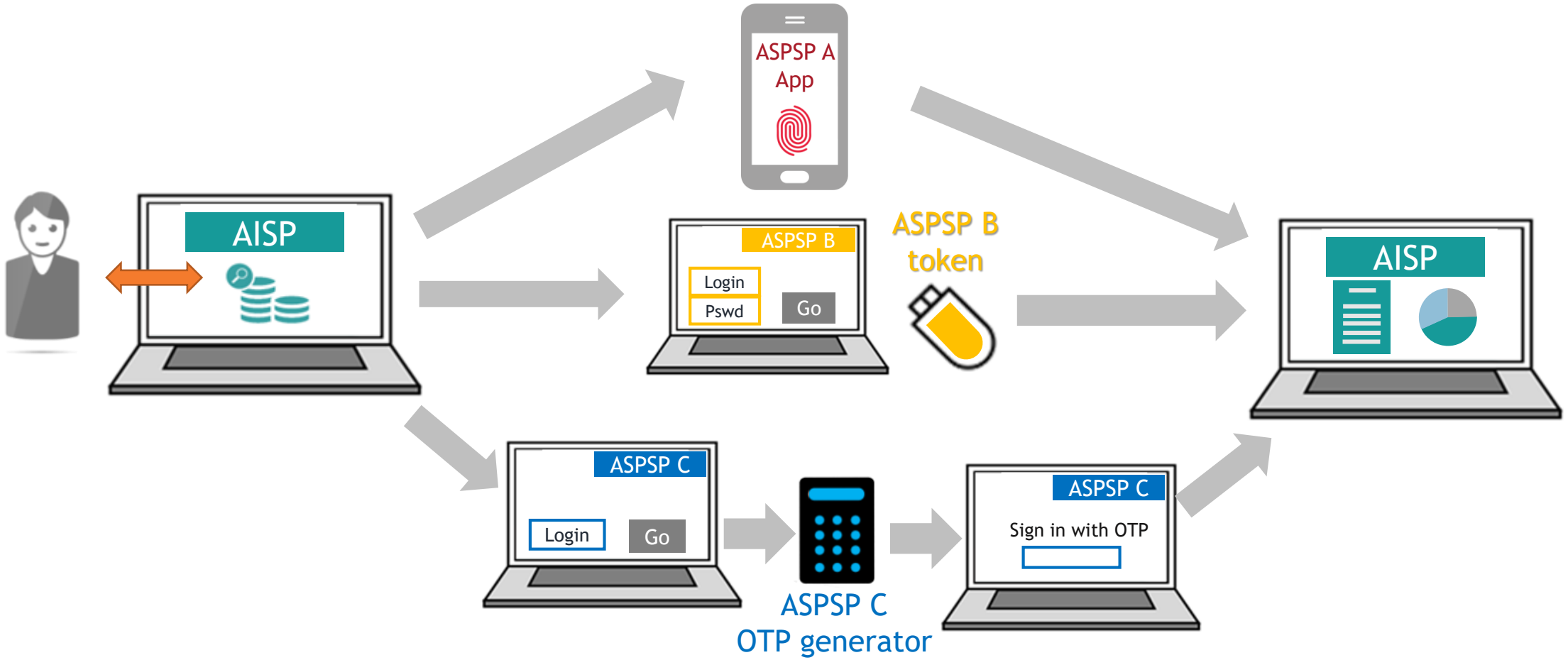


FIDO DESIGNED TO WORK IN THESE MODELS

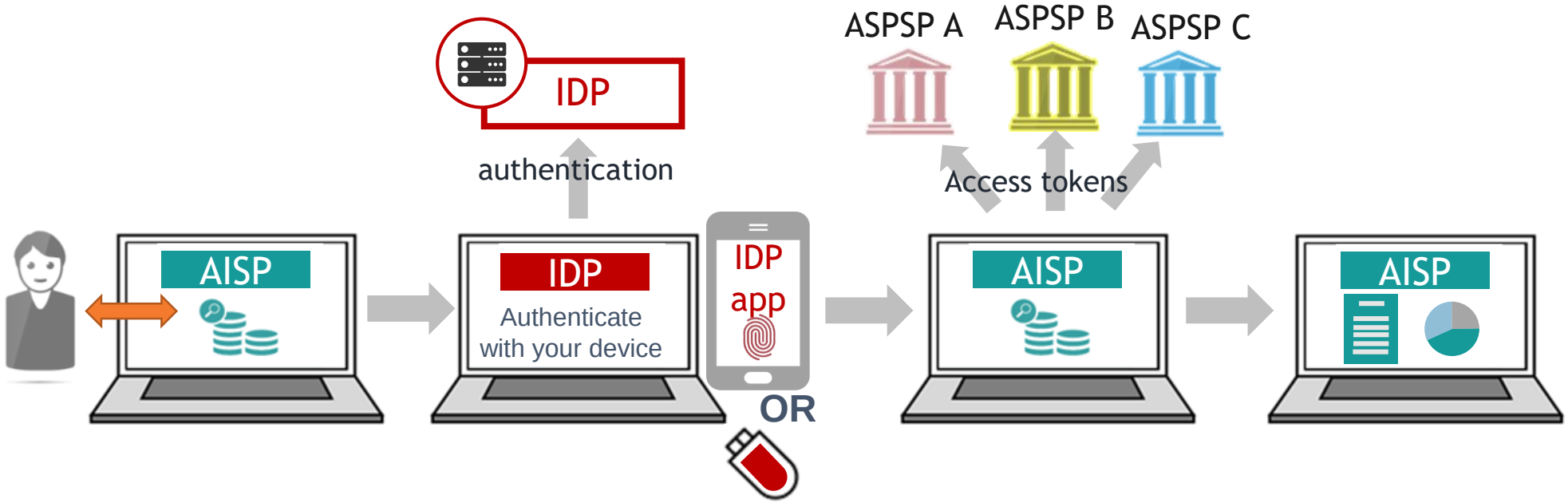


POTENTIAL POOR UX IN THE REDIRECTION/DECOUPLED MODEL

- In account aggregation use cases

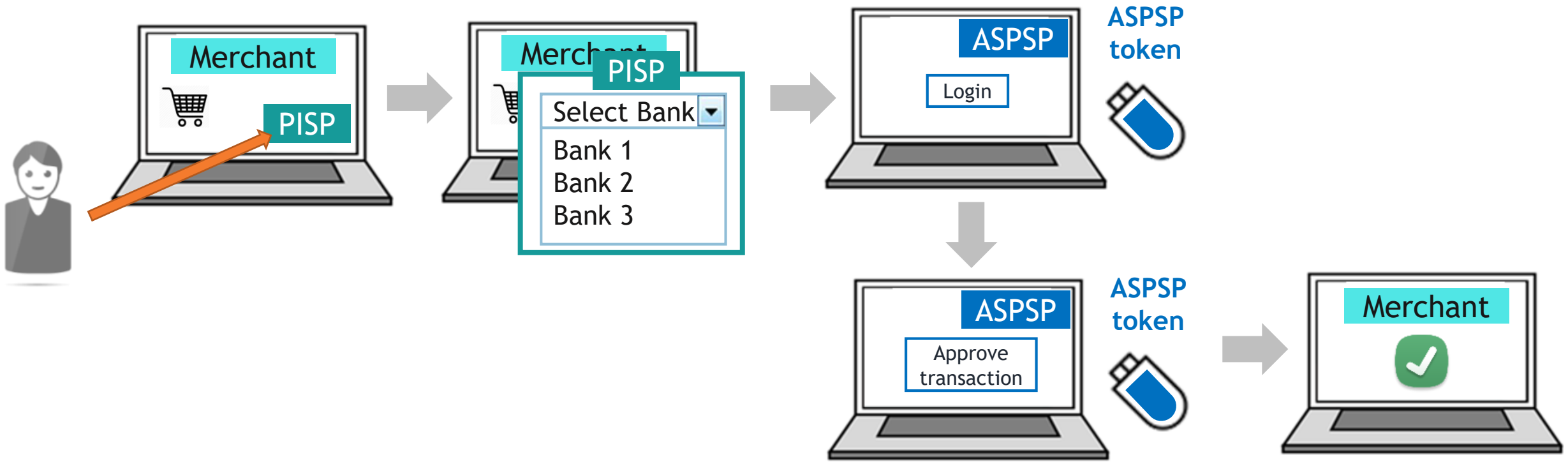


FEDERATED IDENTITY SYSTEM: ONLY ONE REDIRECTION



- FIDO standards fully functional in federated identity systems
- Can be combined with Authorisation frameworks
  - OAuth 2, Open ID Connect…

SOME FINTECHS MAY COMPLAIN ABOUT THE CUSTOMER JOURNEY

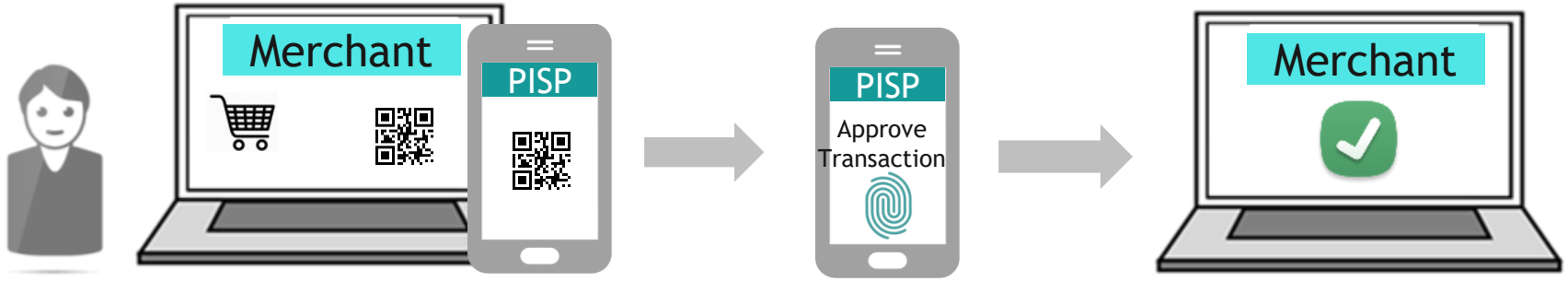


WHAT THE REGULATOR AND STAKEHOLDERS SAY

- The RTS (the law)
  - Article 32-3 on “obstacles” ➔ ASPSP may have to provide alternatives to Redirection if not properly implemented
- ERPB
  - Recommendations for Payment Initiation: The PSU should not be required to access an ASPSP webpage as a part of the authentication process if this limits the PISP in the innovative design of its customer interface
- EBA opinion paper
  - Redirection not an obstacle per se
- The Fintechs
  - Some happy with redirection
  - Some wanting to preserve the user experience they offer

THE “EMBEDDED” MODEL

Example for account aggregation



Example for payment initiation

TWO POSSIBILITIES

1. The user is registered with the TPP
   - The user makes use of the TPP app
   - Example for a PISP:

FIDO proposes a solution for this use case

2. The user is not registered with the TPP
   - The TPP only facilitates access to the account

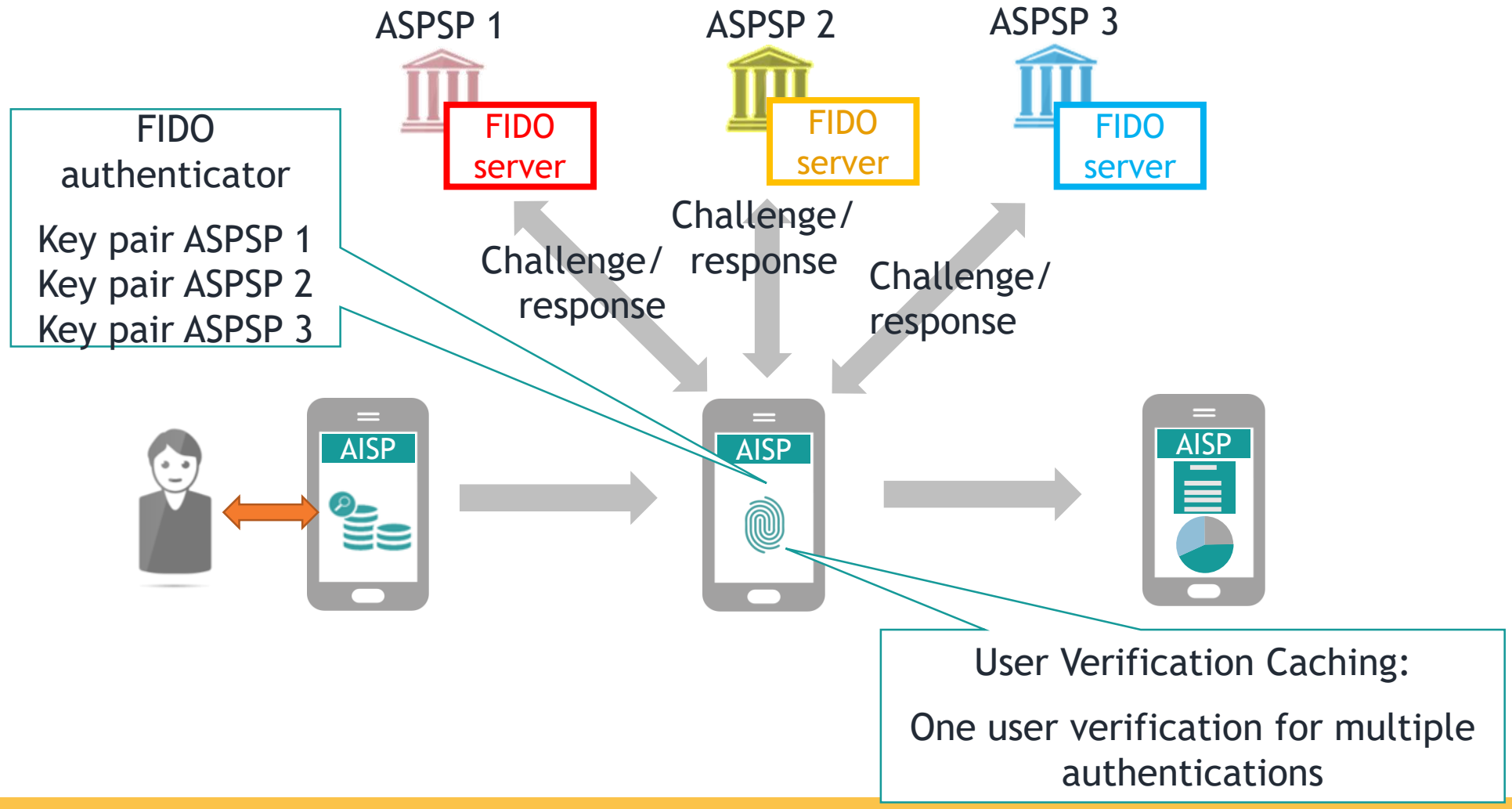
FIDO views the redirection or decoupled approach as suitable for this use case

USING FIDO IN THE EMBEDDED MODEL

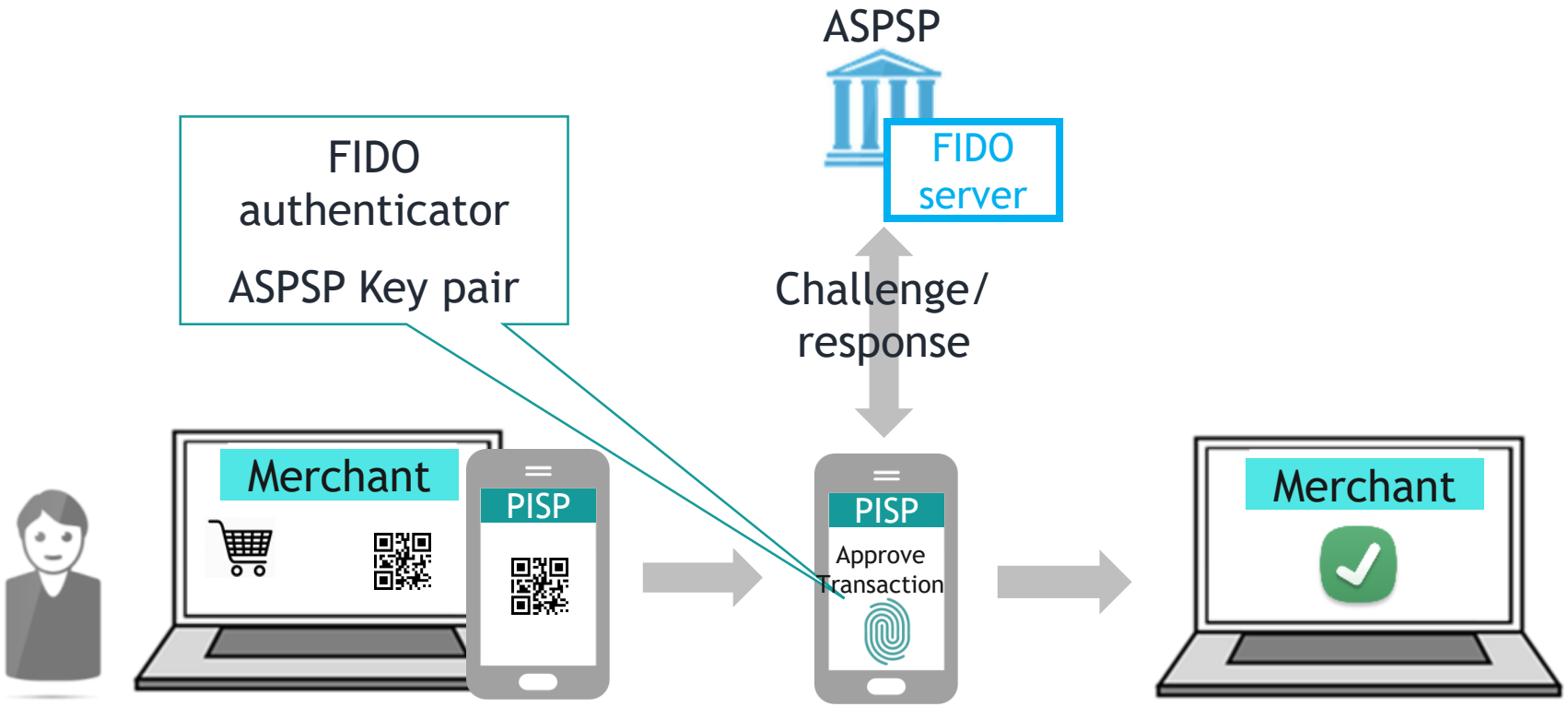
- The TPP handles the user interaction but the ASPSP verifies the user authentication
  - ASPSP security credentials are created in the authenticator
  - The TPP application calls the authenticator

- FIDO can be used in this model, with special care taken to ensure end user privacy
  - Made possible because PSD2 binds TPP and ASPSP under a common legal framework permitting the TPP to perform operations with the ASPSP on behalf of the user
  - De facto, the “Relying Party” role is partly executed by TPP, partly by ASPSP

FIDO FOR THE EMBEDDED MODEL – AISP EXAMPLE

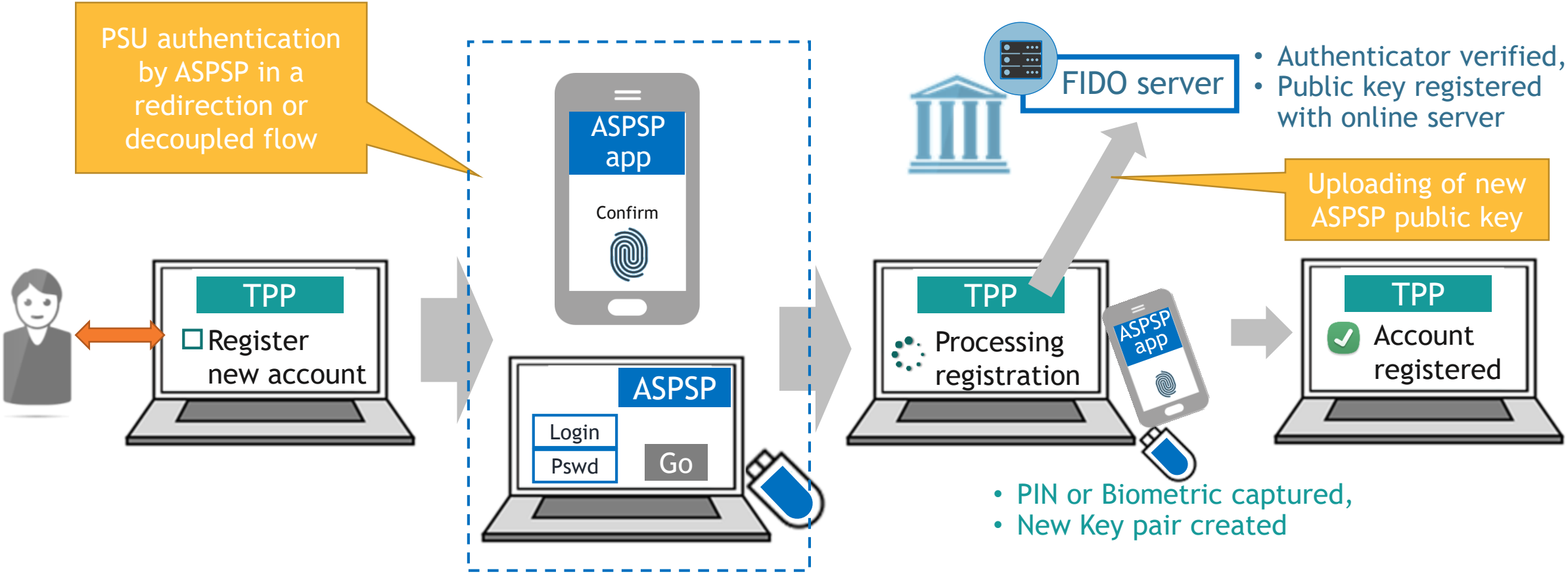


FIDO FOR THE EMBEDDED MODEL – PISP EXAMPLE



FIDO REGISTRATION IN THE EMBEDDED MODEL

- How do ASPSP keys get into the authenticator



PRE REQUISITES

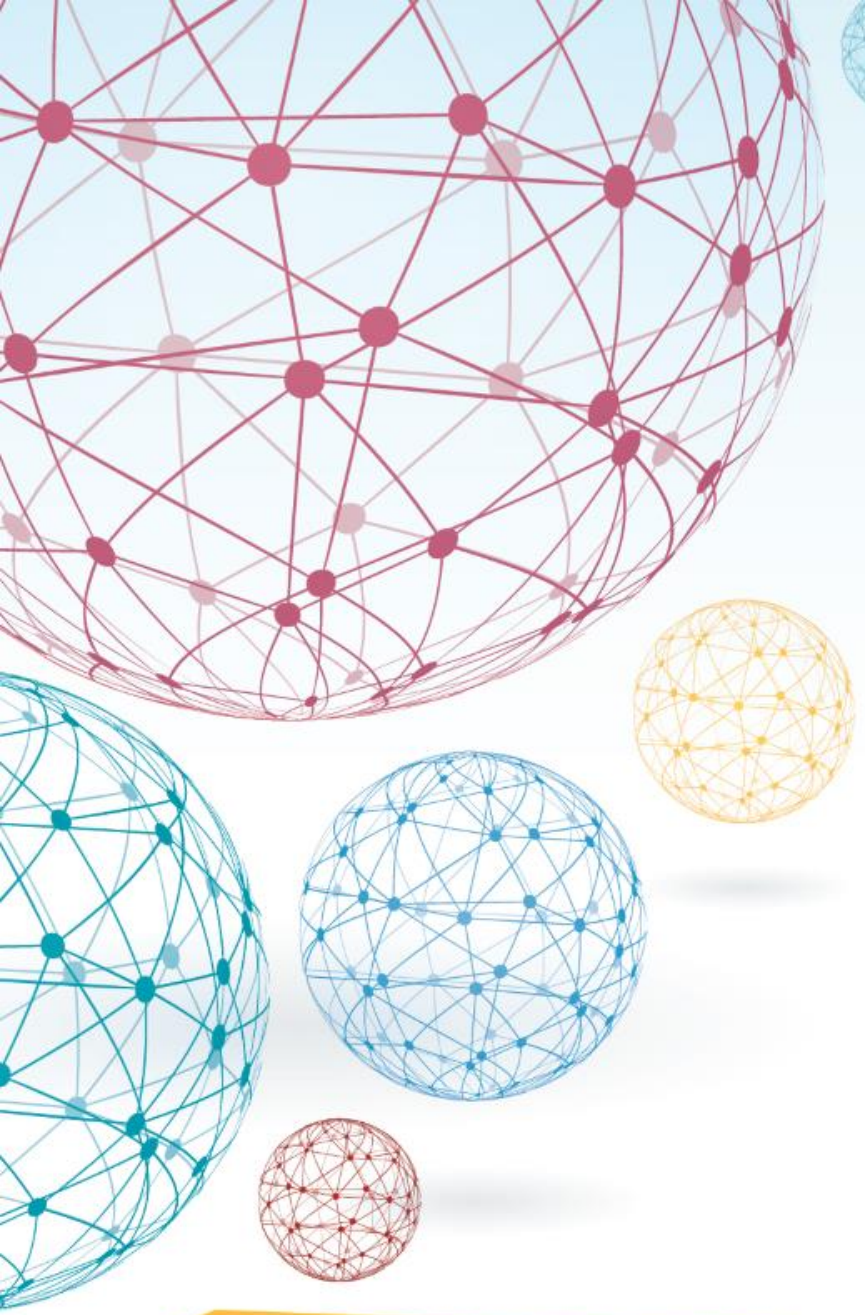
- The Open APIs must support challenge/response mechanisms and registration APIs
- TPP should ensure separate key created for each APSPSP to ensure end user privacy
- ASPSPs must automatically register TPP application ids in their FIDO server
- ASPSPs must agree to the user verification step being triggered by the TPP application
- Ideally, ASPSPs should use the same user verification method

KEY TAKE AWAYS

- FIDO standards: a user friendly solution to implement PSD2
  - Security and Privacy by design
  - Meet all the RTS requirements
  - Alignment with authorization frameworks

- FIDO standards maximize reach
  - They support a multiplicity 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



HTTPS://FIDOALLIANCE.ORG/