



eID Wallet Seminar

10 October 2024

Platinum Sponsor

THALES

Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany’s perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France’s perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform



Opening Keynote

Stéphanie El Rhomri
GlobalPlatform Board of Directors Chair

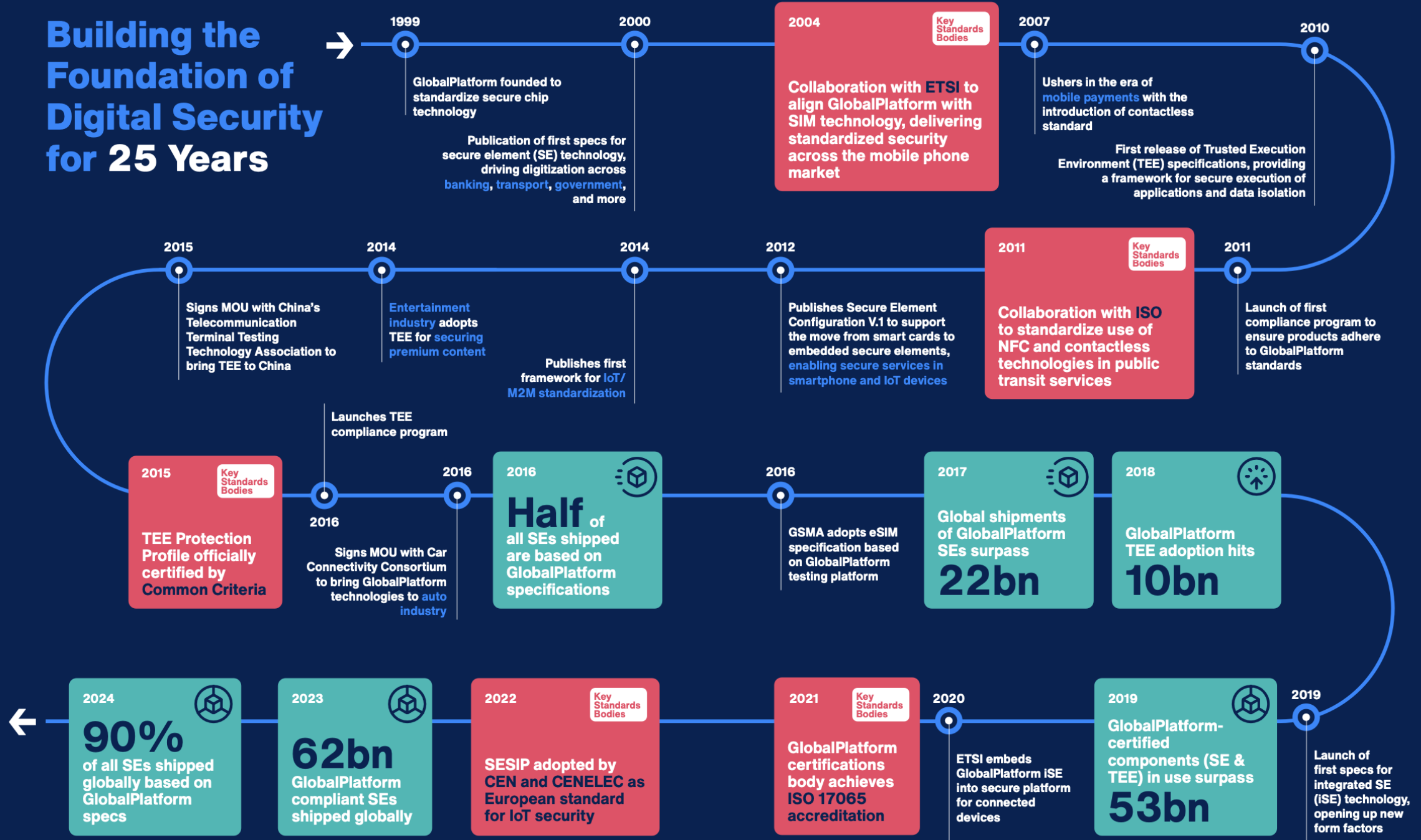
October 10th 2024

WELCOME TO BRUSSELS





Building the Foundation of Digital Security for 25 Years



Across different industries



Financial services



Consumer Electronics



Automotive



Identity



Healthcare



Utilities



Mobile



Smart City



Logistics

Our Members

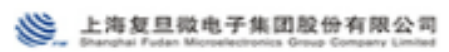
Full



Participant



Observer, Public Entity and Consultants



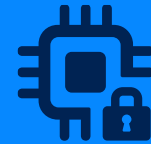
Standardizing Secure Component Technology

A Secure Component is a combination of **hardware, firmware and root of trust.**



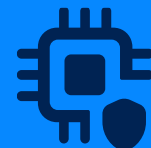
Secure Element (SE)

A tamper resistant execution environment, removable, embedded or integrated



Trusted Execution Environment (TEE)

An isolated execution environment in the main chip of the device



Isolated Technologies

New technologies that created isolated execution environments

GlobalPlatform Certification Program

Test and verify functionality of **SE** and **TEE** products

The program evaluates the functional behavior of SE and TEE products against the requirements outlined by GlobalPlatform configurations, to drive market interoperability and enable innovation. Independent testing confirms that a digital service will perform as intended in the field on any certified product, regardless of the product provider.

Verify the security of **SE** and **TEE** products

The program evaluates products in line with Common Criteria-recognized protection profiles. It ensures that secure components meet the required levels of security defined for a particular service, enabling service providers to confidently and effectively manage risk and comply with industry requirements.



Benefits

- Functional required by EMVCo, GSMA and other industry bodies
- Certification stamp gives products credibility
- Certification discounts and free test suites for members
- Network of test tool providers and labs around the world
- Processes in place are verified against international standards - ISO 17065 accredited (#5486.01)
- Certified products are listed in GlobalPlatform's website

Certification Benefits

The GlobalPlatform Certification Program confirms product adherence to functional requirements and market defined security thresholds.

Device Manufacturers can:

- Market products as meeting digital service provider needs with international recognition
 - Prove that their digital service management capabilities meet security and functional requirements
-

Service Providers have:

- Reassurance that certified products meet their needs

Simplifying security evaluation and conformance

What Is SESIP

A common and optimized approach for evaluating the security of connected products and meeting the specific compliance, security, privacy and scalability challenges of the evolving IoT ecosystem.

SESIP Provides

The framework for IoT stakeholders to adopt trusted components that have already been SESIP evaluated and to create new products without having to re-assess the security evaluation and certification.

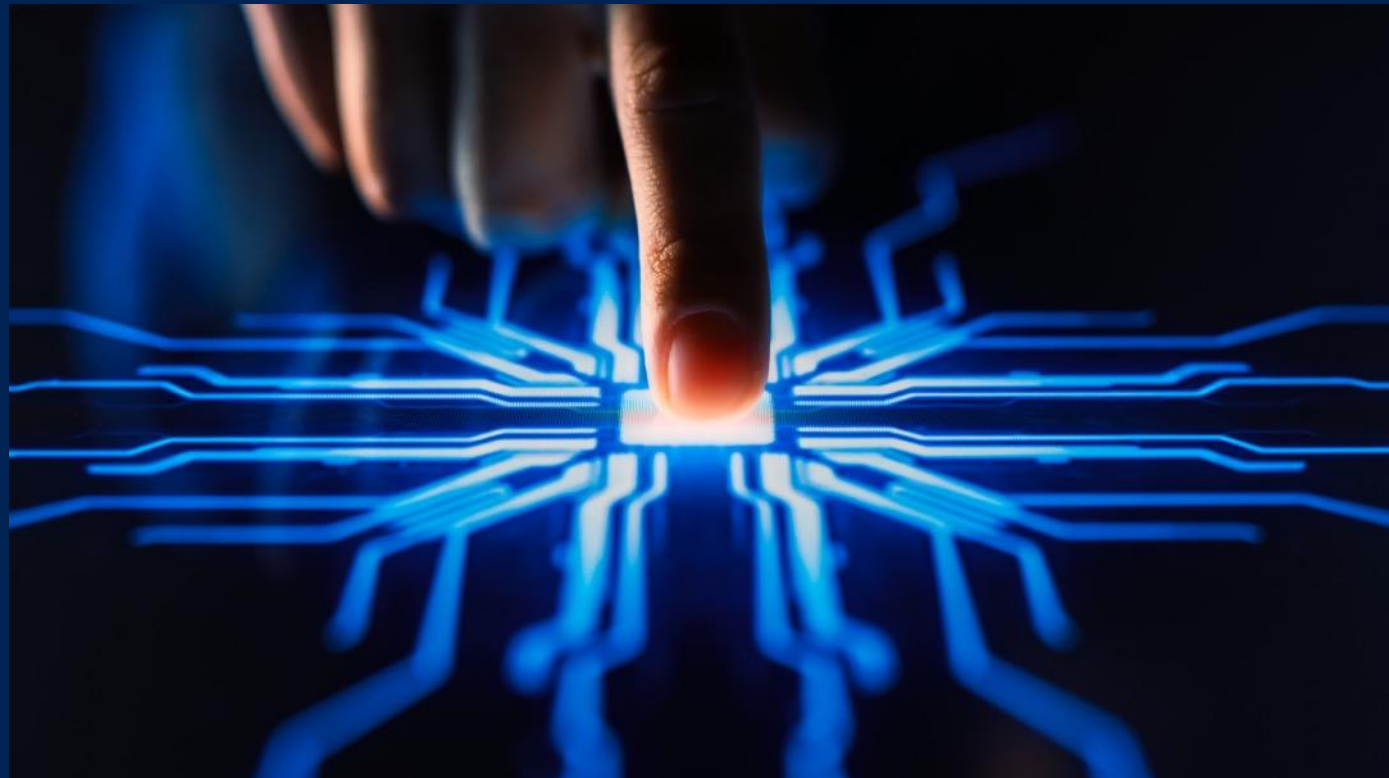
SESIP delivers greater efficiency and cost-savings, whilst ensuring defined assurance levels across a broad range of regulatory and security frameworks (including ETSI, ISO/IEC and NIST), as well as specific vertical regulations.

GlobalPlatform **continues to evolve this methodology** to map with additional regulations and standards requirements. It also creates specific security profiles to address new markets (e.g., Healthcare, Automotive).



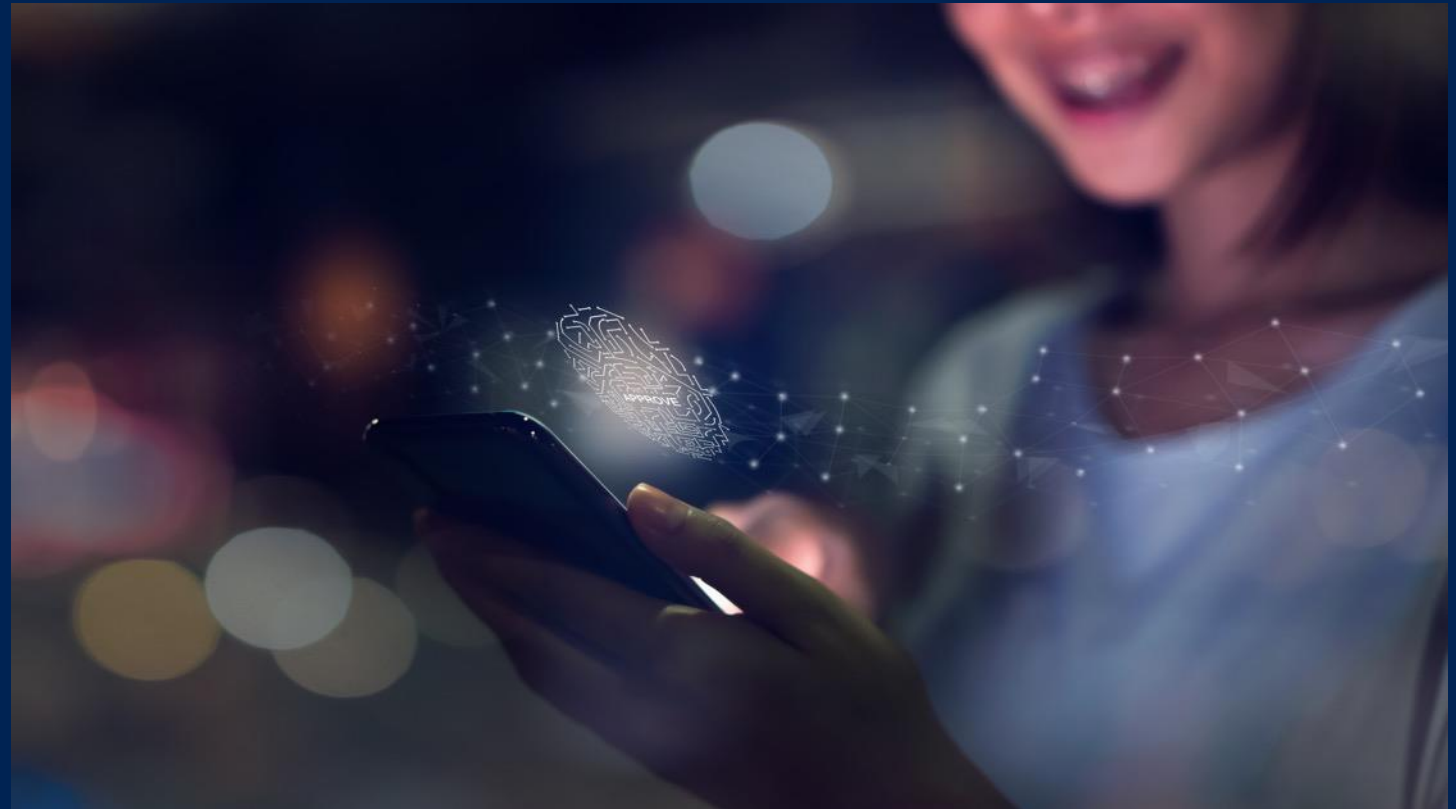
SESIP is now a CEN CENELEC standard EN 17927, GP supports implementation of IoT security schemes based on SESIP.

Digital Identity Wallets need to be secure, ensure privacy, be available to everyone and interoperable



A collaborative effort to deliver this vision for EUDI

Working with
different
stakeholders,
governments and
regulators to evolve
existing specs to be
ready for EUDI



eID Wallet Task Force

Objectives:

- Support the different digital identity deployments happening in Europe, US and rest of the world
- Analyze and support different possible solutions to enable high security for identity wallets deployment (e.g. eSE, eUICC, SAM)
- Identify requirements for the evolution of secure element technical specifications

Our members are helping to define the future industry requirements and solutions that will provide the secure foundation for eID Wallet services around the world.

GlobalPlatform technologies can support many different business models for eID deployments.



**Want to contribute to the
eID Wallet Task Force?**



Global Platform™

The standard for
secure digital services
and devices

THANK YOU!

Membership

membership@globalplatform.org

PR Contact

pressoffice@globalplatform.org

Questions

secretariat@globalplatform.org

→ globalplatform.org



Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany's perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France's perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform

Keynote: Unlocking the Future of Public Services - The Transformative Power of Digital Identity and Wallets

eID Wallet Seminar



Vedran Lalic

Independent Consultant

Formerly Head of MEPs Office, European Parliament



**Global
Platform™**

Brussels, Belgium
and Virtual

October 10th, 2024

Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany’s perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France’s perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform



**Global
Platform™**

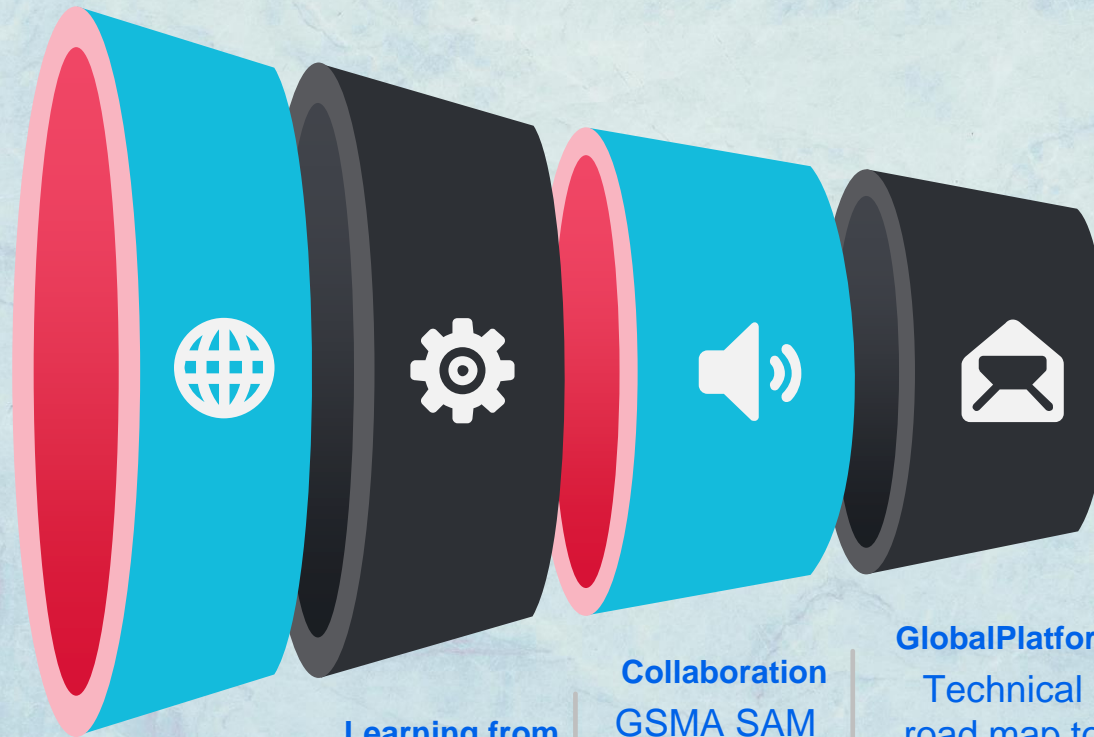
Easing Frictionless and Secure EU-DI Wallet Deployment

Gil Bernabeu, Chief Technology Officer

Current GlobalPlatform Road map for EU-DI



CENELEC

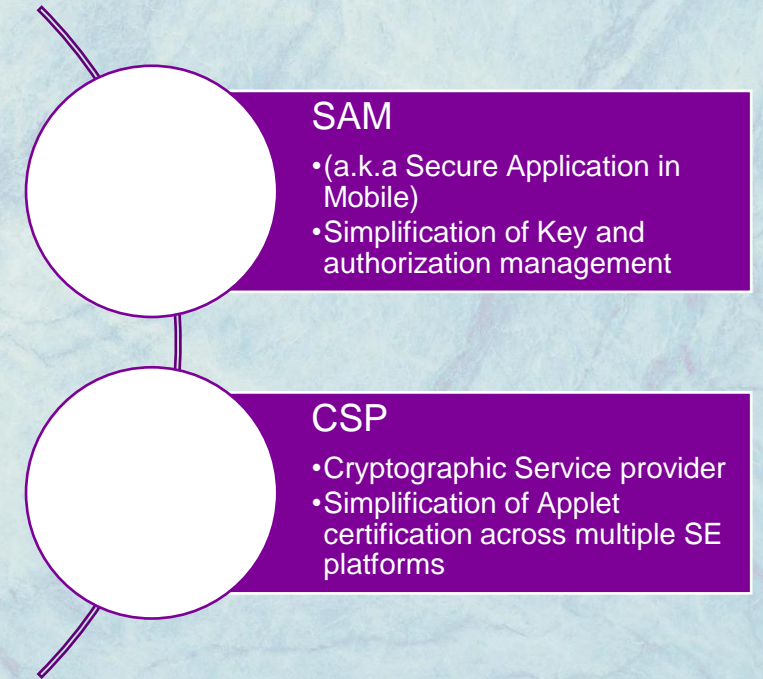


Workshops
And
seminars

Learning from
EU projects
and previous
deployment

Collaboration
GSMA SAM
ENISA 5G
scheme

GlobalPlatform
Technical
road map to
easy
deployment



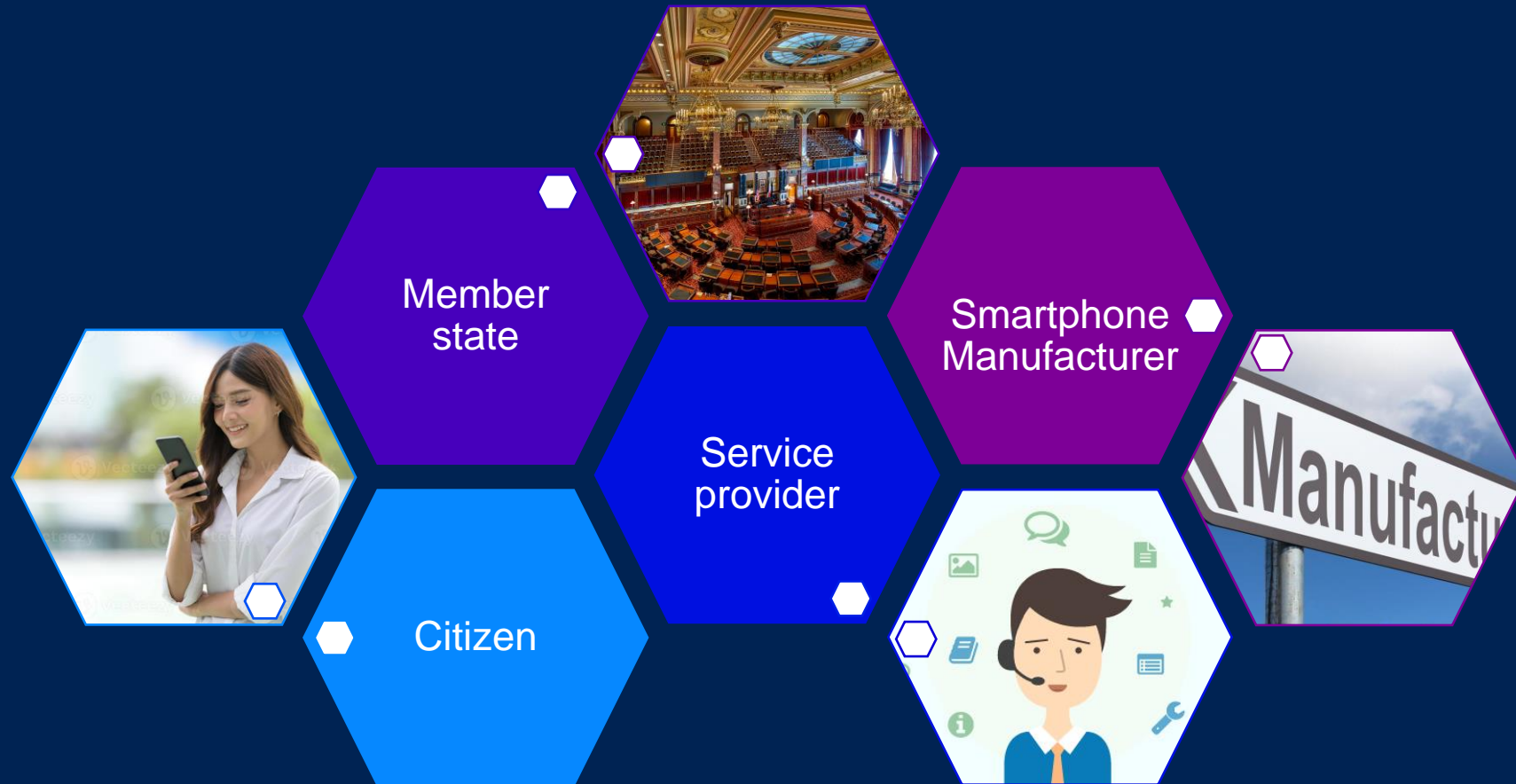
SAM

- (a.k.a Secure Application in Mobile)
- Simplification of Key and authorization management

CSP

- Cryptographic Service provider
- Simplification of Applet certification across multiple SE platforms

A Simplified Ecosystem



Member State



Smartphone



Citizen

27



TOP 10 SMARTPHONE COMPANIES IN 2023

RANK	BRAND	MARKET SHARE
1	Apple	20%
2	Samsung	19%
3	Xiaomi	13%
4	Oppo Group	9%
5	Transsion	8%
6	Vivo	8%
7	Honor	5%
8	Motorola	4%
9	Realme	4%
10	Huawei	3%

Note: Motorola is owned by Chinese tech firm Lenovo.
Source: Omdia Smartphone Shipment Preliminary Result 4Q23



A smartphone stays in the field around 7 years



Member State

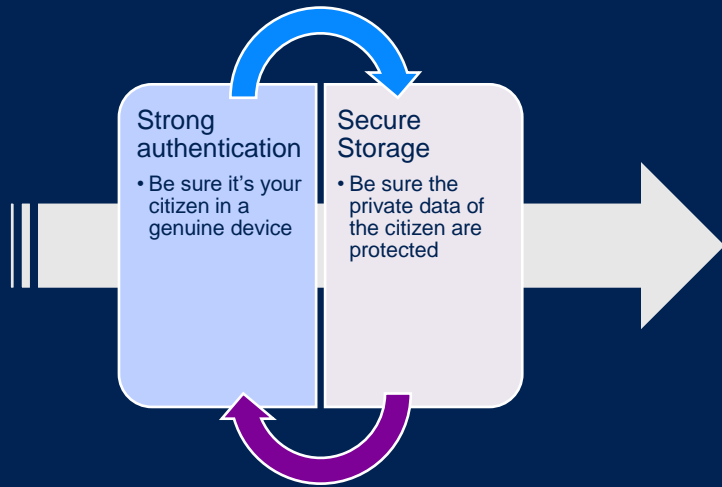


Smartphone



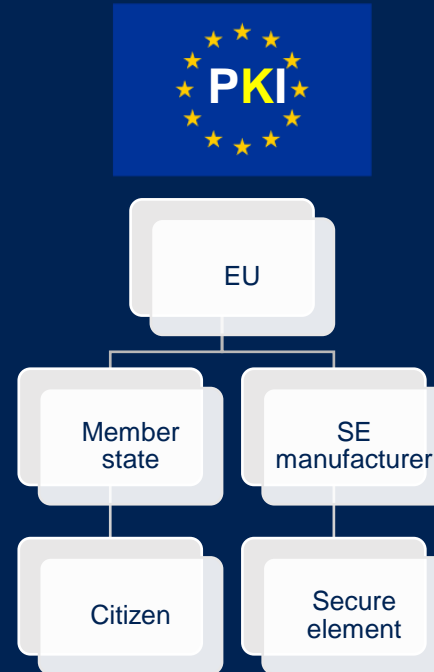
Citizen

27



SAM Technology Simplifies :

27



Smartphone manufacturer decision when selecting a eSIM/eSE

- Clear set of feature to offer

Member state analysis about level of secure feature available in the device

- Clear set of feature and associated certification

Key Management between 27 members states and dozens of smartphone manufacturers x 7 different models

- PKI based Key deployment

Clarifies deployment model for Member state

- Script based deployment – simple back end

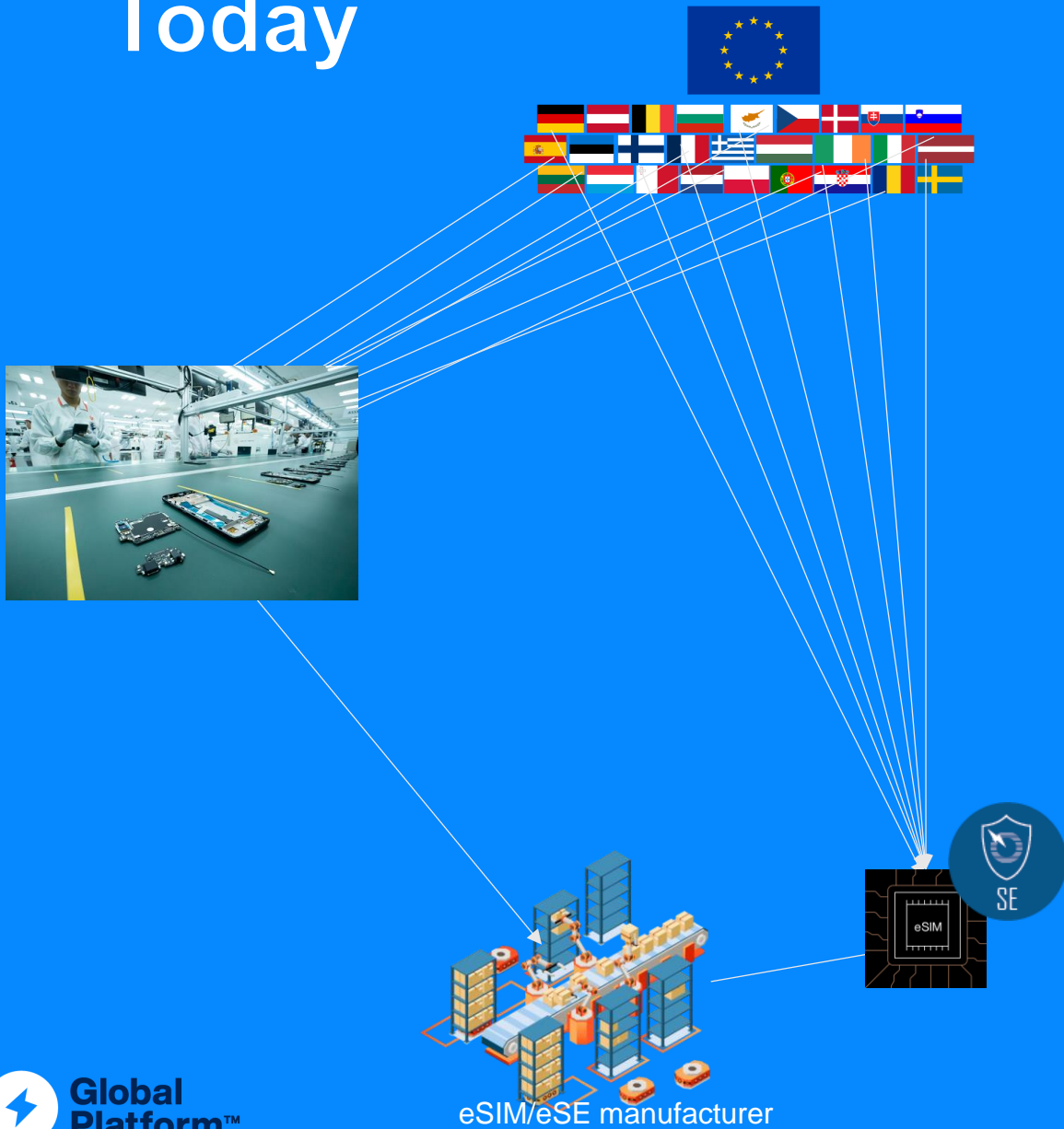
SAM : An Isolated Environment in eSIM or eSE



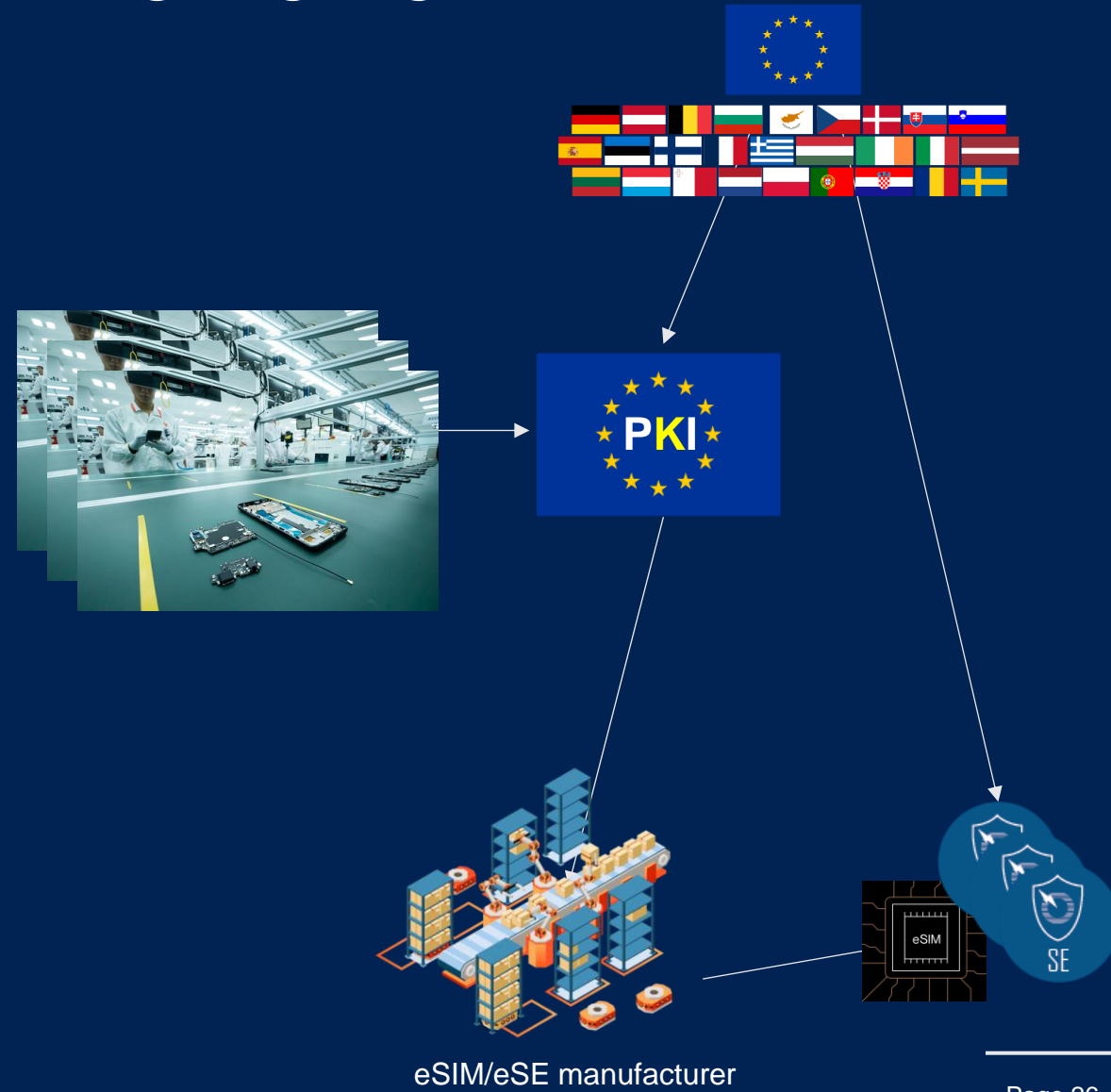
GlobalPlatform **SAM** extends the concept to eSE and allows an isolated area in an SE.

Along with certification and compliance, SAM offers a secure and standardized environment for member state to manage end user authentication , end 2 end security and secure storage

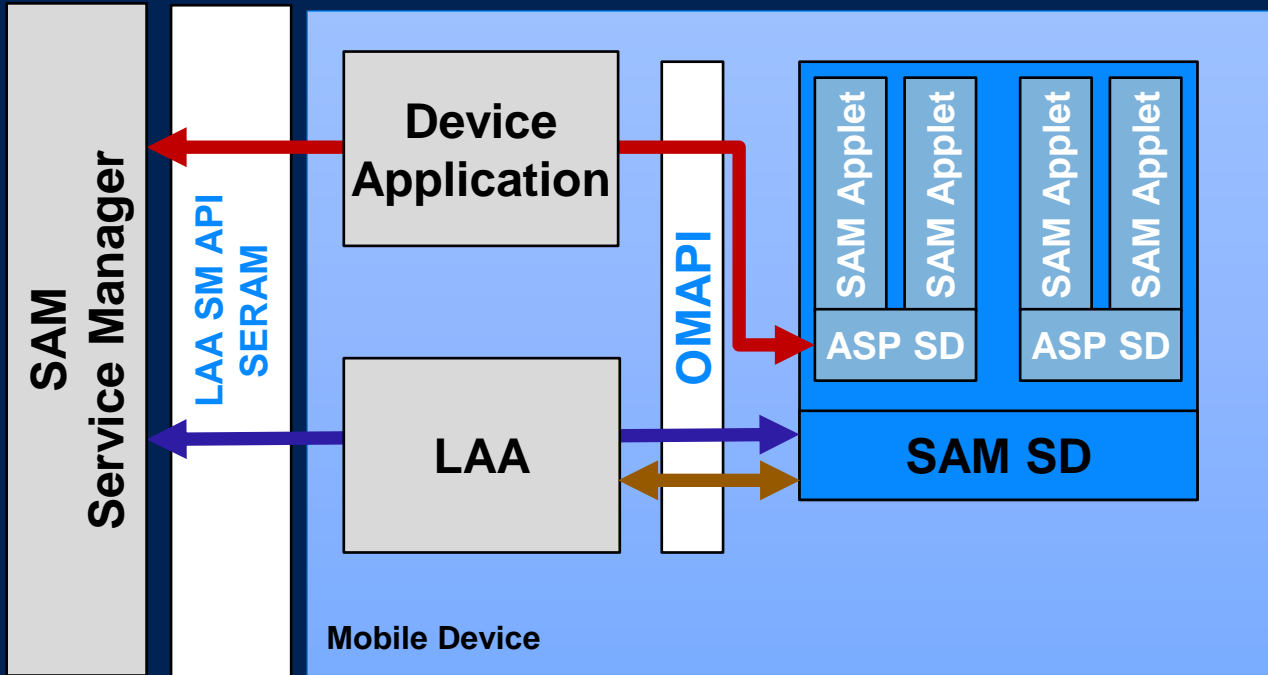
Today



Tomorrow



SAM – Device



- SAM SD (and its hierarchy) i.e. the “SAM Scope”
- Application Service Provider (ASP) SDs

- ↔ SAM05
APDU interface defined in SAM Config (secured via SCP11c/a)
- ↔ SAM08b
APDU interface defined in SAM Configuration (secured via SCP11c/a or SCP03)
- ↔ SAM01eu
APDU interface defined in SAM Configuration

GlobalPlatform Open Mobile API (OMAPI)

Protocols (GP Open-Source on GitHub):

LAA <-> SAM SM (Local Application Assistant <-> SAM Service Manager)

SERAM (SE Remote Application Management)

Today

Current SE products in smartphone support most of the features to implement the functional part of SAM.
It's not 100% but enough to deploy the member state processes

When ?

Note : SAM is a configuration (not a new specification). SE Configurations are implementation guideline for SE products

Tomorrow

SAM test suite availability will ensure interoperability and adherence with the SAM configuration
SE protection profile for SAM will ensure security interoperability for certification

What we need ?

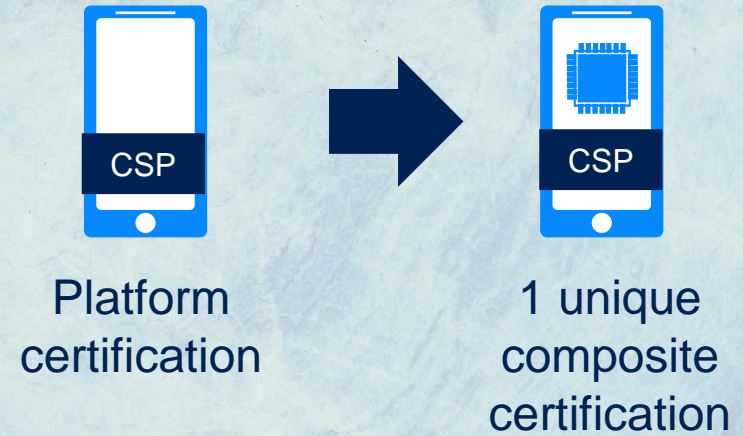
A



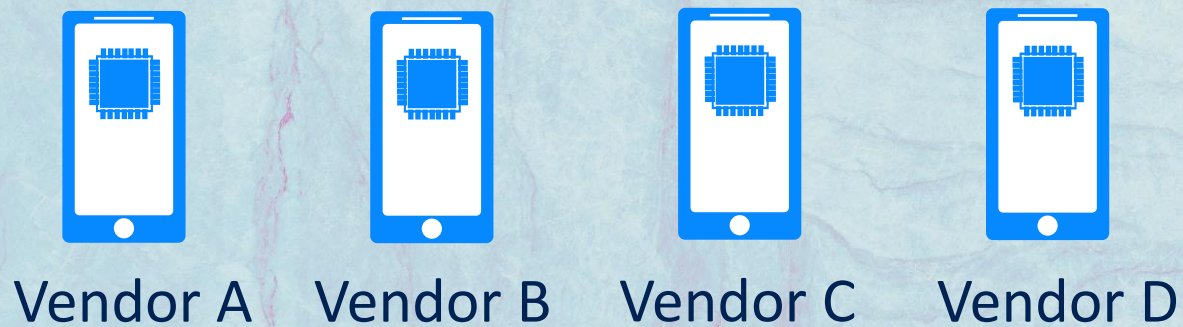
Composite certification (Applet with platform) is required for applet when targeting EAL_VAN.5 level of robustness



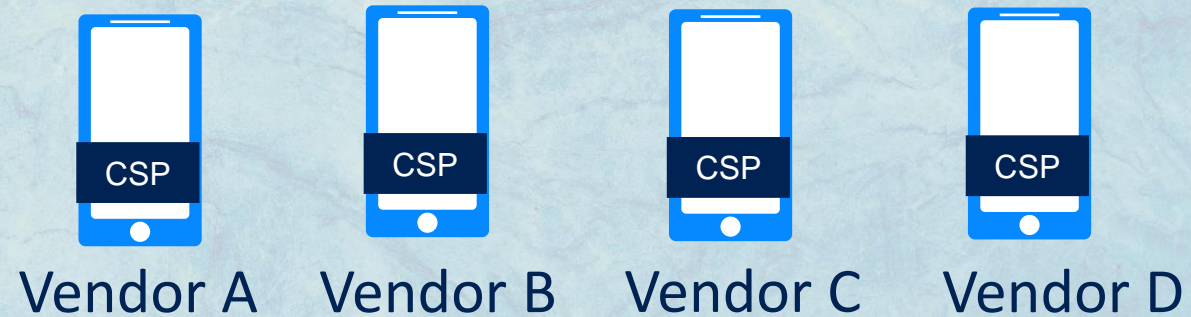
The Cryptographic Service Provider (CSP) is a self-contained component that includes software, firmware, and hardware of a CSP-enabled Secure Element.



Composite certifications do not scale in a multiple vendor deployment



Only one composite certification allows to be deployed in any CSP-enabled platform



SAM & CSP: Two EUDI Wallet Enablers

SAM (Secured Applications for Mobile)

Enables hosting 3rd party applications, such as the WSCA, on (e)SIMs independently of the GSMA or Mobile Network Operator

SAM Configuration, v1.0 (March 2024)

CSP (Crypto Service Provider)

Enables post-issuance installation of an EUDI Applet (WSCA) and yet meet EAL4+ without the need of composite certification

Card Specification – Amendment N (early 2025)



Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany’s perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France’s perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform

The path toward a secure European Digital Identity

Jean-Daniel Aussel,
Thales Digital Identity &
Security

www.thalesgroup.com





Wallet acceptance requires Trust
... and Trust requires Security

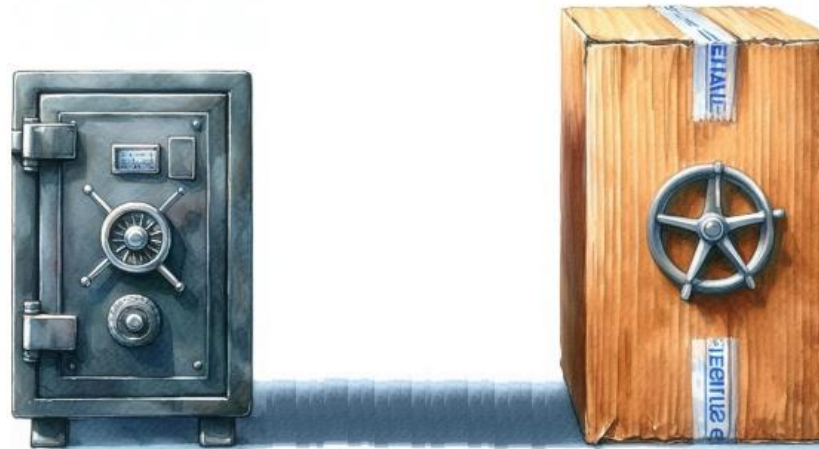
Should we have tamper-proof hardware for securing
the wallet? Or **Shall** we?

WALLET SECURITY



From High Level of Assurance certified tamper-proof solutions
(Regulation) ...

... to “an environment” that “needs to satisfy high standards of
certification” (draft Implementing Act on Certification)



WHAT HAPPENED?



- We have to deploy fast and do with what is readily available
- Secure hardware is not really much deployed
- Accessing secure hardware is not possible
- Our current solution is not hardware protected, nobody complained so far
- It's complicated ...

"Speed is useful only if you are running in the right direction." -Joel Barker



The risks and threats associated with the Wallet require that the Wallet security must be resistant to attackers with high attack potential



Low Security in the European Digital Identity Wallet:
An Unacceptable Risk for Citizens and Businesses

HOW TO COMPARE FAIRLY APPLE TO ORANGES



A fair and objective way of proving a high level of assurance in a system with 27+ national identity wallets and 27+ national certification scheme is to use the same rule.





Common Criteria methodology is the de-facto standard for certifying products with a high-level of assurance

Common Criteria certification EAL4+ AVA_VAN.5 is the minimum assurance level that certify products are resistant to attackers with high attack potential



The Wallet Cryptographic Secure Device (WSCD) **shall** be a hardware device certified with Common Criteria methodology at EAL4+ AVA_VAN.5 to provide the foundation for the wallet to have a high level of assurance



NOW CAN WE?



HARDWARE TAMPER-PROOF EAL4+4 AVA_VAN.5 CC CERTIFIED DEVICE OPTIONS FOR THE EUDI WALLET



External NFC ID Card



Remote Hardware Security Module (HSM)



Embedded Secure Element



Embedded or Removable SIM

These are not exclusive definitive choices, technologies can co-exist or replace each other over time, depending on use-cases, availability, convenience

BUT WHAT'S THE REACH?



448.4 million

Inhabitants in the
European Union ¹

Over 50%

Smartphones to
have embedded
hardware security
by 2025 ²

**Close to half a
billion** eSIM-

capable devices
were shipped in
2023 ³

Over 9 billion

eSIM-capable
devices to be
shipped by 2030 ⁴

Nearly 70%

proportion of
cellular devices
eSIM/-capable by
2030 ⁵

474.2 million

Projected eSIM
smartphone
shipments in
Europe in 2028 ⁶

Sources: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#)

BUT HOW DO I ACCESS SECURE ELEMENTS?



Where there is a will, there is a way.



WHO FOUND THE WAY SO FAR?

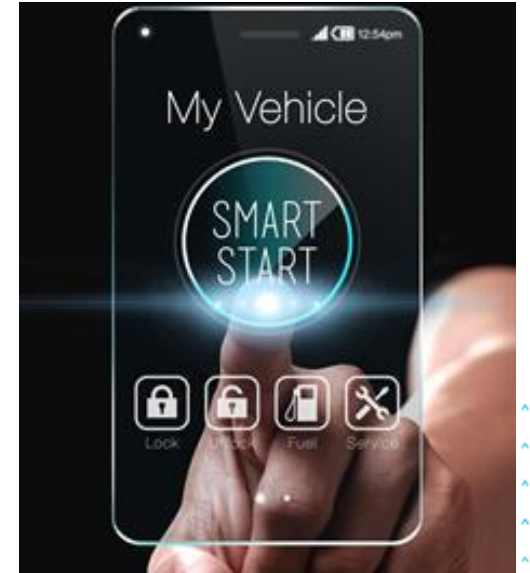


Mobile Network Operators

Banks and Payment Providers

Transports

Car Makers



GOVERNANCE OF SECURE ELEMENTS



> Embedded SE

- ▶ Owned by smartphone manufacturer
- ▶ eSE management controlled by smartphone manufacturer
- ▶ Secure provisioning addressed using Secure Element Issuer Trusted Service manager (SEI-TSM) server



> Embedded SIM

- ▶ Owned by smartphone manufacturer
- ▶ Root Certificate of GSMA pre-installed and profile download controlled by the GSMA
- ▶ Secure provisioning of wallet applet done with Subscription Manager Data Preparation (SM-DP) server



> Embedded SIM with SAM

- ▶ Owned by smartphone manufacturer
- ▶ Root Certificate of EU or Member State pre-installed
- ▶ Secure provisioning of wallet applet done with Secured Application for Mobile Service Manager (SAM-SM)

KEY TAKEAWAYS

The Wallet WSCD shall be a tamper-proof hardware, such as Secure Elements, HSM, or external NFC ID cards

The Wallet WSCD shall be certified with the Common Criteria Certification methodology at EAL4+ AVA_VAN.5

There are transition paths towards a secure wallet that do not sacrifice security for the go to market

If necessary, convenience for non high LoA use cases can use WSCD with lower level of assurance.

Using embedded Secure Elements inside the smartphone is a matter of business agreements and governance, not a technological issue

More info about Thales

Stay connected with Thales

www.thalesgroup.com

in

f

X

▶





Thank you

www.thalesgroup.com

Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany's perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France's perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform

GERMANY'S PERSPECTIVE ON THE EUDIW DEPLOYMENT

GlobalPlatform eID Wallet Seminar 2024, 10.10.2024, Brussels

THE GERMAN EUDIW PROJECT



Germany is developing the concept for a digital ecosystem for **secure, privacy-friendly and user-friendly EUDI Wallet(s)** in an **open architecture and consultation process**.



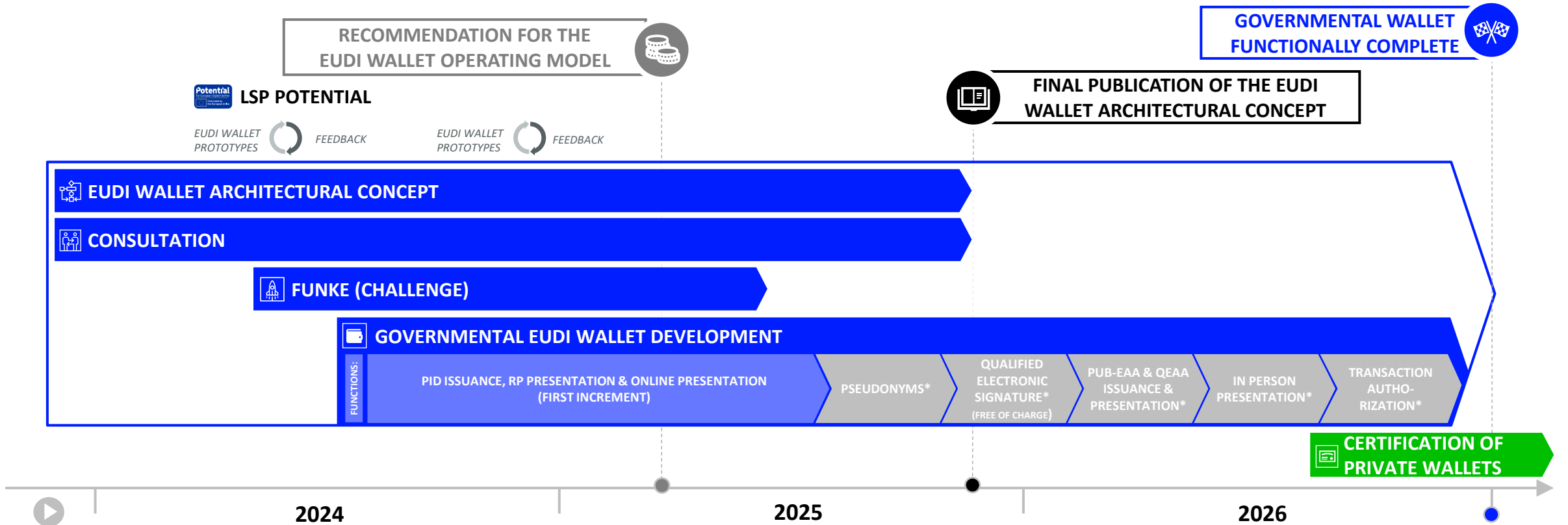
The associated project is being carried out by the Federal Agency for Disruptive Innovations (SPRIND GmbH) on behalf of the Federal Ministry of the Interior and Community with the Federal Office for Information Security and supported by Bundesdruckerei GmbH, Fraunhofer Institute for Applied and Integrated Security (Fraunhofer AISEC) and PricewaterhouseCoopers.



SPRIN-D



PROJECT OVERVIEW



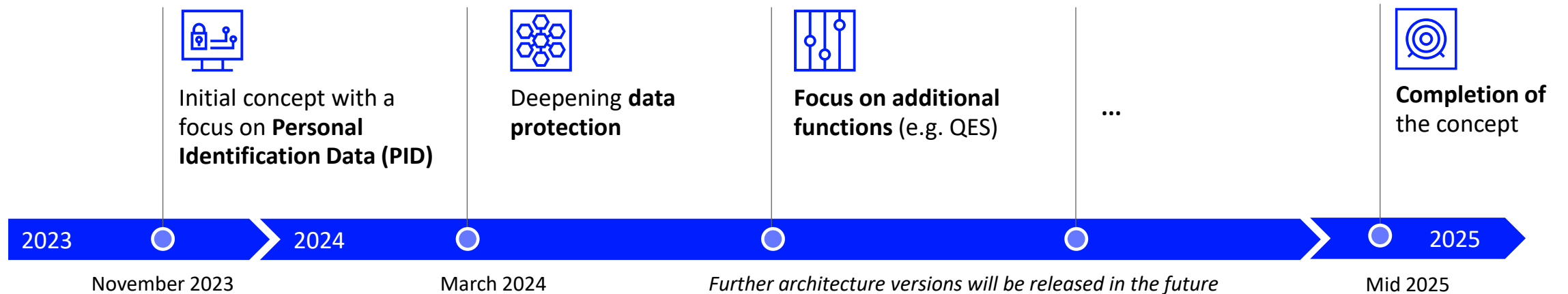
*The exact development periods have not yet been defined

IN THE ARCHITECTURE PROCESS, EXPERTS REGULARLY PUBLISH ITERATIONS WITH A DIFFERENT FOCUS

The **concept** for a **digital wallet ecosystem** is being developed by experts with **the ongoing involvement of the public**. The aim of this constant exchange is to ensure a **high level of user-friendliness and acceptance** of the wallet.




Roadmap of the architecture versions





THE CONSULTATION PROCESS ENSURES THE COMPREHENSIVE INVOLVEMENT OF RELEVANT STAKEHOLDERS AND THE PUBLIC

Consultation formats to accompany the architecture process





Workshops

- **Development of results** and feedback with stakeholders
- Workshops are offered **on new architecture versions**



Open Online Consultations

- **Low-threshold offer** for open questions on specific topics
- Consultation hours are held on **operating models**, for example



Interviews

- Determining the **needs of relevant stakeholder groups**
- Participation of **groups with special needs**

Would you like to participate in the consultation process?

- > All open consultation formats are announced and documented on **OpenCoDE**
- > **Comments and feedback** on the architectural concept and the consultation process can be submitted there



THE “EUDI WALLET PROTOTYPES” FUNKE - TESTS OF THE ARCHITECTURE CONCEPT AND NEW IDEAS FOR HARD CHALLENGES

Innovation competition Funke



6 teams took part in the **funded track**,
5 teams in the **non-funded track**



Jury comprised of **technical experts** and
representatives from **politics and civil society**



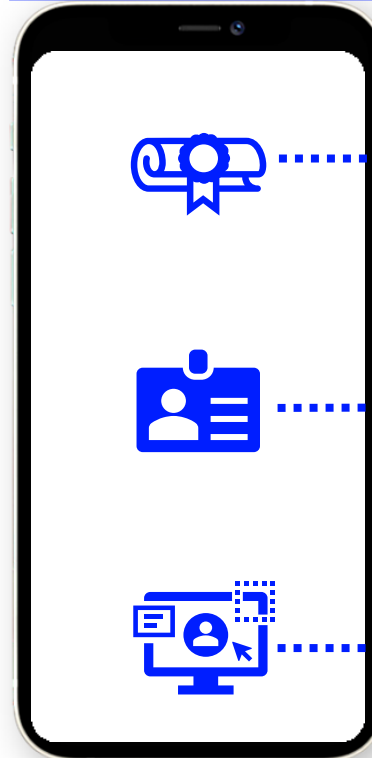
All PID implementation approaches of the
architecture concept are tested



Once stage 1 is complete, the prototypes will be
made available to the **pilot project POTENTIAL*** for
testing in six use cases.

**Within the framework of Potential, a consortium of 19 countries & 140 public and private partners is working to ensure the interoperability of EUDI wallets in six use cases.*

Core functions of the EUDI wallet prototype



Level 1

Issuing & presentation of **personal identification data (PID)**

Level 2

Issuing & presentation of **electronic certificates (EAs)**

Level 3

Pseudonymous login, qualified electronic signature (QES) & payment

GERMAN GOVERNMENT RECENTLY DECIDED IN FAVOR OF A HYBRID MODEL FOR WALLET PROVIDERS

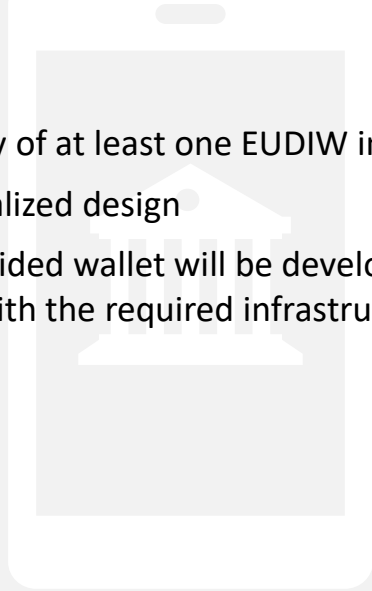
DE will build a Government-provided EUDIW

Ensures Sovereignty

Guarantees availability of at least one EUDIW in DE

Aims for fully decentralized design

The Government-provided wallet will be developed and rolled out incrementally along with the required infrastructure

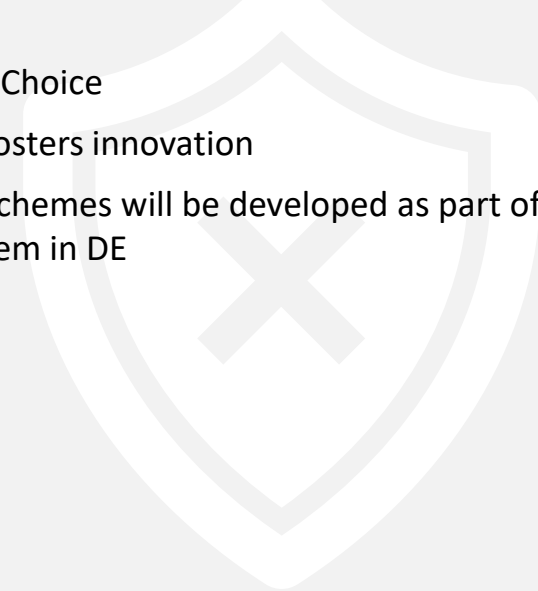


DE will be open to alternative Wallet Providers

Trust requires Choice

Competition fosters innovation

Certification Schemes will be developed as part of the establishment of the ecosystem in DE



THE FIRST ITERATION OF THE GOVERNMENT-PROVIDED EUDIW

Functions of the first iteration of the EUDI Wallet

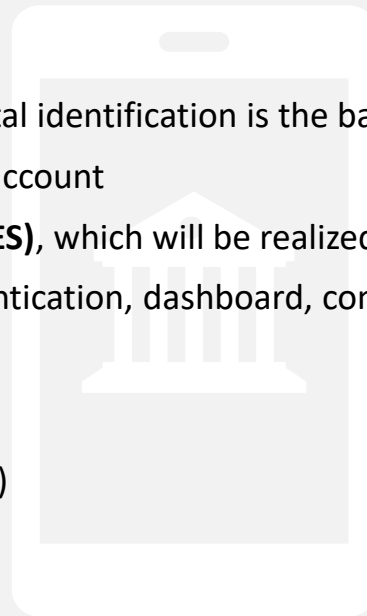
Focus on Identification (PID) on LOA High as secure and digital identification is the basic function of the EUDIW

- **Identification with Relying Parties**, e.g. opening of a bank account
- **Building block for further functions of the wallet (EAAs, QES)**, which will be realized in subsequent iterations.

Empowerment of Users is a further core objective (RP authentication, dashboard, complaints)

Technical Design

- PID data is stored (encrypted) on the phone
- Authentication keys managed in the cloud (security + reach)
- Signed data (interoperability)



WHY CLOUD HSM ?

Most phones these days **lack a security module** with the **required security level** we could utilize (either don't have it at all, or the user authentication is not sufficient or we cannot access it)

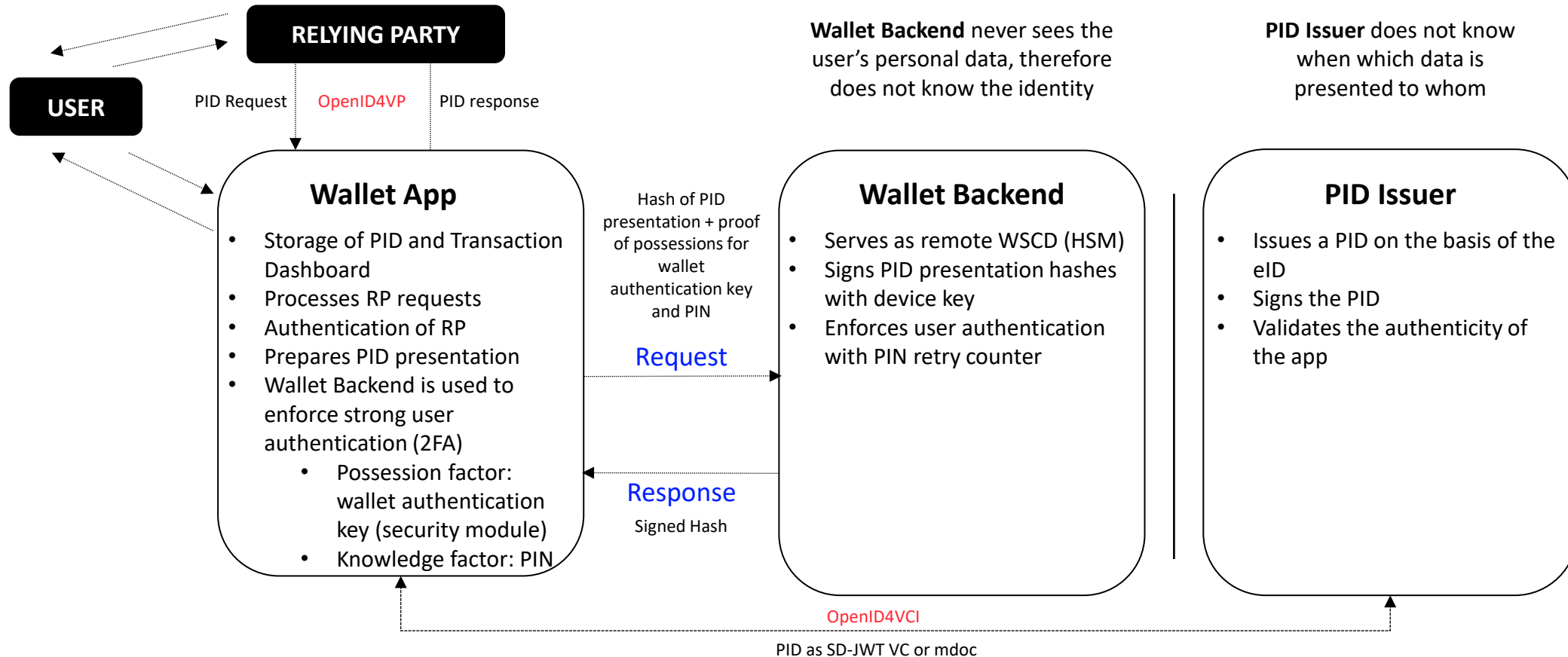
Interfaces of the wallet are **ARF compliant** and can be kept for the **subsequent increments**



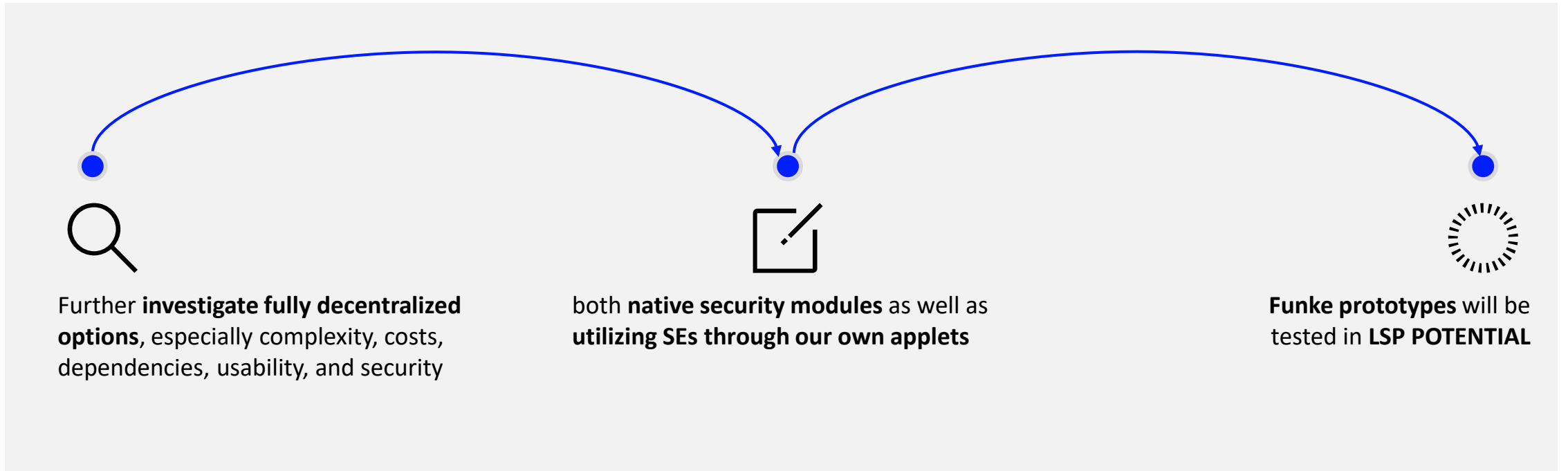
Prototypical experience with **eUICCs** indicate this approach **needs more work to become a viable solution** for large scale deployments

Design allows for **incremental migration to decentralized key management** (as suitable solutions become available and/or for lower assurance levels)

UNDER THE HOOD (FOCUS ON PRESENTATION)



WAY FORWARD (ON WSCDS)



FUTURE TOPIC: ZERO KNOWLEDGE PROOFS

EUDIW shall be privacy preserving

- Unlikability is hard to implement with traditional cryptography
- Requires ephemeral credentials and batch credential issuance
- Feasible but the issuance process is more complex and requires a secure, active „connection“ between wallet and issuer to fetch fresh credentials
- The federalistic organization of Germany would require to support this for 100k+ EAA providers (municipalities, schools, enterprises, ...)



Zero Knowledge Proofs could be an alternative

- Unlinkability can be implemented with single, long living credential
- Requires standardization, recognition, implementation, and **support in Secure Elements**

We are about to start looking into this topic as long term option

In case of questions, please contact us:

Via E-Mail:

DVI5@bmi.bund.de

konsultation-eudi@partner.sprind.org

On Open CoDE:



Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany's perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France's perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform

France's perspective on EUDI deployment



Anthony CARMOY

UC Implementation Lead of POTENTIAL Large Scale Pilot
Consultant for France Identité, ANTS

Potential
For European Digital Identity



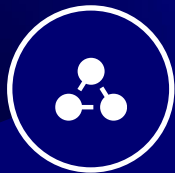
Co-funded by
the European Union



Addressing the initial problem: identity fraud

210k person / year

French population affected by identity fraud



\$3 million / year

Costs for companies victims of identity theft



\$7 to \$50 / month

Identity theft protection services



France Identité is based on a combination of multiple blocs to provide the PID

Reminder: Person Identification Data' (PID) means a set of data, issued in accordance with Union or national law, enabling the identity of a natural or legal person, or of a natural person representing a natural or legal person, to be established

Source: [Article 3 of Regulation \(EU\) No 910/2014 \(eIDAS\)](#)

Carte Nationale d'Identité électronique (CNIE)

« where the data comes from »



ICAO DataGroup
Enables cross-border travel within the EU

- contains biometric data

eID DataGroup
Contains the eIDAS minimum dataset

- readable only with the France Identité app (PIN + NFC scan)



France Identité app

« where the data can be read »



- Now available to **all French citizens** having a CNIE
- Also enables the **import of the mDL** (soon ISO/IEC 18013-5:2021 compliant)



eID Backend (SGIN)

« where the data is checked »



- Performs **integrity and authenticity checks** of the app and the card
- Checks whether the **card has been stolen / lost**, and that the **holder is alive**
- **No check in a registry**

How does the France Identité application work?

The new **identity card** contains
your identity details



An associated code

Allowing users to express their consent
to the use of their data.



France Identité: Achieving High Assurance and European Recognition

In February 2024, the French CAB, ANSSI, notified France Identité at the national level as compliant with the **High Level of Assurance** requirements.

Under the European eIDAS regulation on electronic identification and trust services, **the European Commission notified France Identité** on Monday, September 9, 2024, as compliant with the requirements for a **High Level of Assurance**.

This High LoA is achieved through **fingerprint comparison in city offices**.



France Identité's eID Uptake: A Surge in User Engagement and Digital Trust

Proximity presentation using gyroscopic cards



Soon to be experimented



Figures

1,2M+ eID

170k high eID

500k AuthN

Proxy assignment
for elections



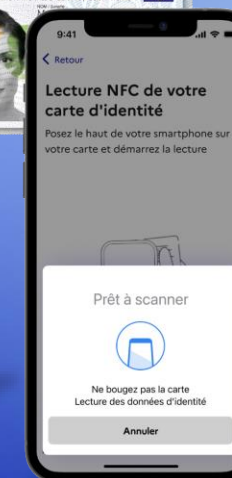
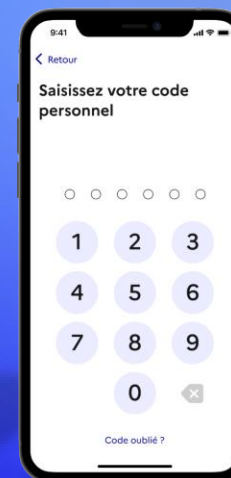
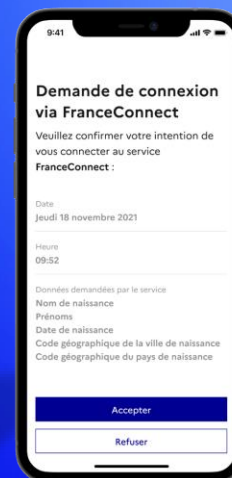
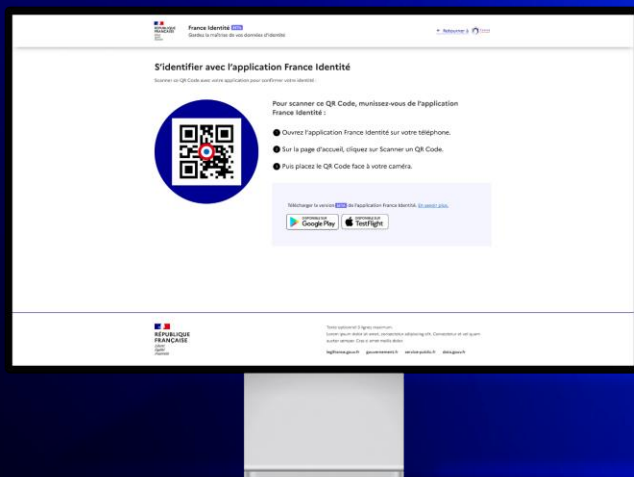
First real-life use case for LoA High

Step 1: enabling online authentication

- 1-click authentication with your personal code
- **Access sensitive services** with a second authentication factor on the application

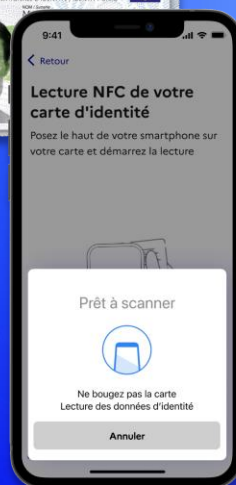
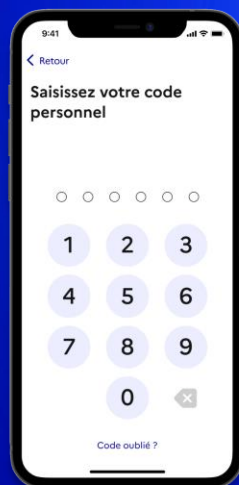


+ 1800 available services
via **FranceConnect**
OIDC protocol



Step 2: identity proofing for ID sharing

- Replace copies of identity cards
- Secure common administrative procedures
- Define a framework for use



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Justificatif d'identité à usage unique

N° Z6KZAAT76UI2TXC

CADRE D'UTILISATION	
DESTINÉ À 072c immo	MOTIF Location d'appartement
GENÉRE LE 06/09/2023	DATE LIMITE D'UTILISATION 11/12/2023

ÉMETTEUR

NOM
Martin

PRÉNOMS
Maëlys-Gaëlle, Marie

SEXE
F

NATIONALITE
FRA

DATE DE NAISSANCE
13/07/1990

LIEU DE NAISSANCE
Paris



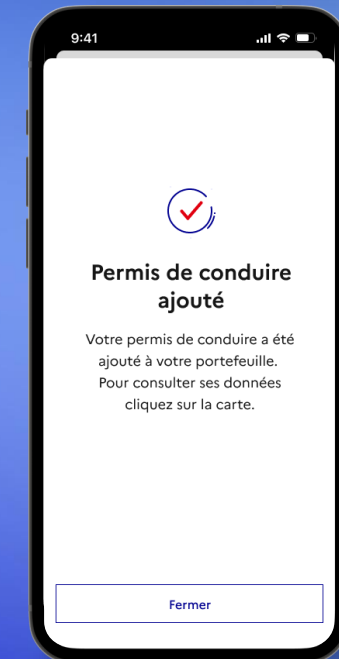
Vérifier ce justificatif sur france-identite.gouv.fr/justificatif

MINISTÈRE DE L'INTÉRIEUR - JUSTIFICATION
DÉPOSÉ PAR LE MINISTÈRE DE L'INTÉRIEUR - JUSTIFICATION

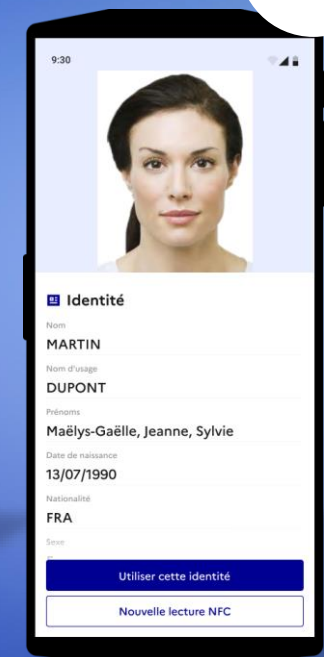
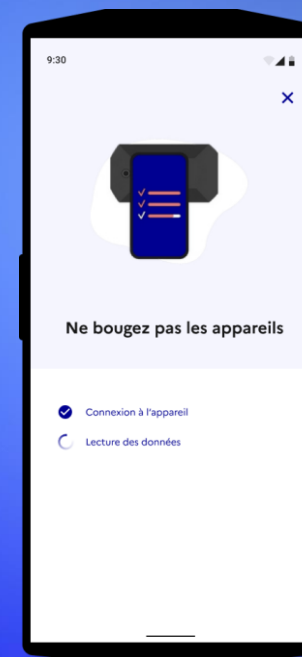
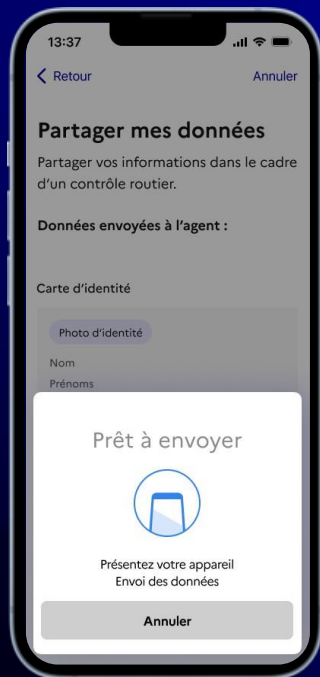
CESTE ATTESTATION ÉLECTRONIQUE D'IDENTITÉ A ÉTÉ GÉNÉRÉE À PARTIR DE DONNÉES ISSUES D'UNE CARTE D'IDENTITÉ VALABLE ET DE L'APPLICATION FRANCE IDENTITÉ, CONFORMÉMENT AU DÉCRET N°3023/18 DU 26 AVRIL 2022 AUTORISANT LA CRÉATION D'UN MOTIF D'IDENTIFICATION ÉLECTRONIQUE (MOTIF) ASSURANT LE SERVICE DE GARANTIE DE VOTRE NUMÉRIQUE (SIV) - CE MOTIF D'IDENTIFICATION EST GÉNÉRÉ ÉLECTRONIQUEMENT PAR LE MINISTÈRE DE L'INTÉRIEUR AFIN DE GARANTIR LA SÉCURITÉ ET L'INTEGRITÉ DES PRÉLÈVEMENTS DES DONNÉES D'IDENTITÉ DES CITIZENS FRANÇAIS ET DES ÉTRANGERS RÉSIDANT EN FRANCE - LE TRAITEMENT DES DONNÉES A CARACTÈRE PERSONNEL DE CE MOTIF D'IDENTIFICATION EST RÉGULÉ PAR LE DÉCRET N°3023/18 DU 26 AVRIL 2022 ET LE DÉCRET N°3023/18 DU 26 AVRIL 2022. LE MOTIF D'IDENTIFICATION EST GÉNÉRÉ ÉLECTRONIQUEMENT PAR LE MINISTÈRE DE L'INTÉRIEUR AFIN DE GARANTIR LA SÉCURITÉ ET L'INTEGRITÉ DES PRÉLÈVEMENTS DES DONNÉES D'IDENTITÉ DES CITIZENS FRANÇAIS ET DES ÉTRANGERS RÉSIDANT EN FRANCE - LE TRAITEMENT DES DONNÉES A CARACTÈRE PERSONNEL DE CE MOTIF D'IDENTIFICATION EST RÉGULÉ PAR LE DÉCRET N°3023/18 DU 26 AVRIL 2022 ET LE DÉCRET N°3023/18 DU 26 AVRIL 2022. LE MOTIF D'IDENTIFICATION EST GÉNÉRÉ ÉLECTRONIQUEMENT PAR LE MINISTÈRE DE L'INTÉRIEUR AFIN DE GARANTIR LA SÉCURITÉ ET L'INTEGRITÉ DES PRÉLÈVEMENTS DES DONNÉES D'IDENTITÉ DES CITIZENS FRANÇAIS ET DES ÉTRANGERS RÉSIDANT EN FRANCE - LE TRAITEMENT DES DONNÉES A CARACTÈRE PERSONNEL DE CE MOTIF D'IDENTIFICATION EST RÉGULÉ PAR LE DÉCRET N°3023/18 DU 26 AVRIL 2022 ET LE DÉCRET N°3023/18 DU 26 AVRIL 2022.

Step 3: driver's license with law enforcement

- QR code with proof of integrity
- Identity matching

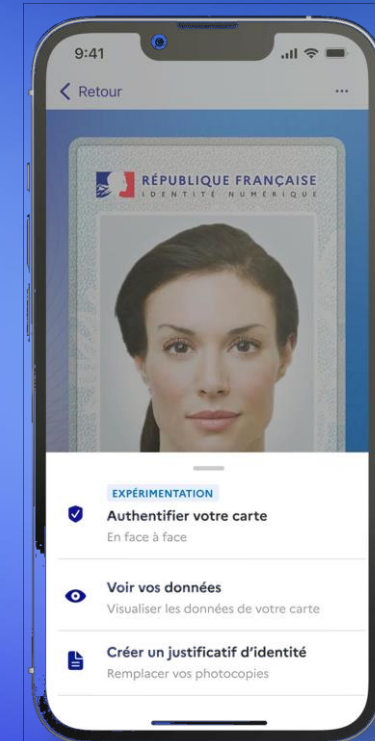
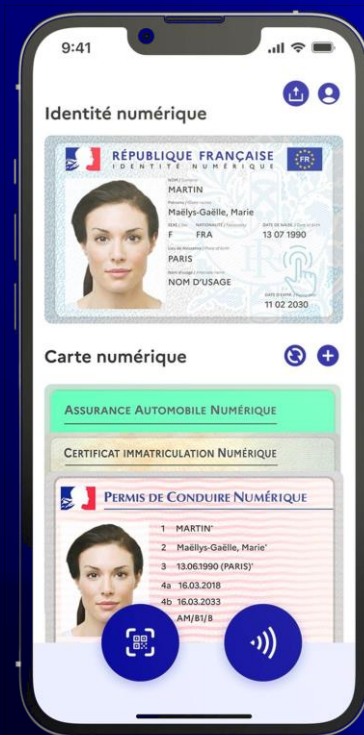


Step 3: driver's license with law enforcement (2/2)

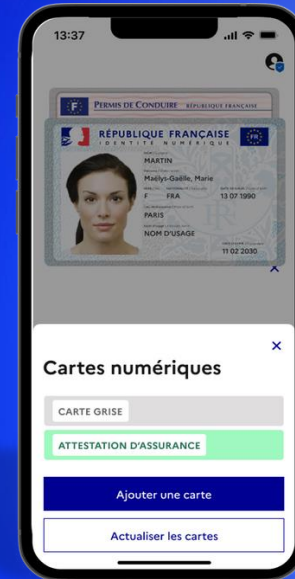


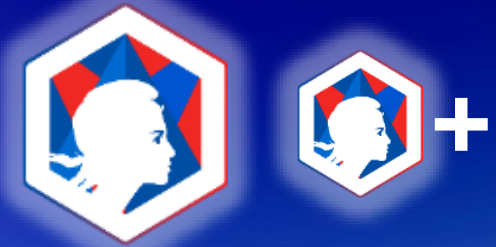
Step 4: Identity proof in day to day use

Digital cards can encapsulate various types of documents

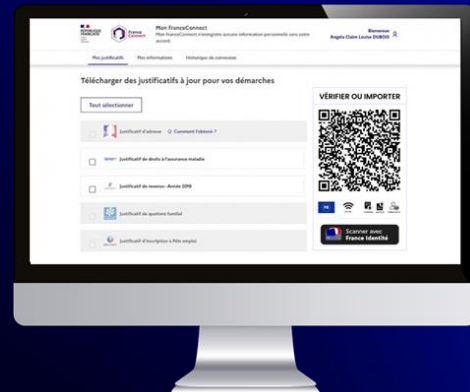


Expanding digital cards to various sectors

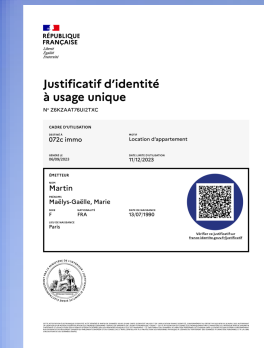
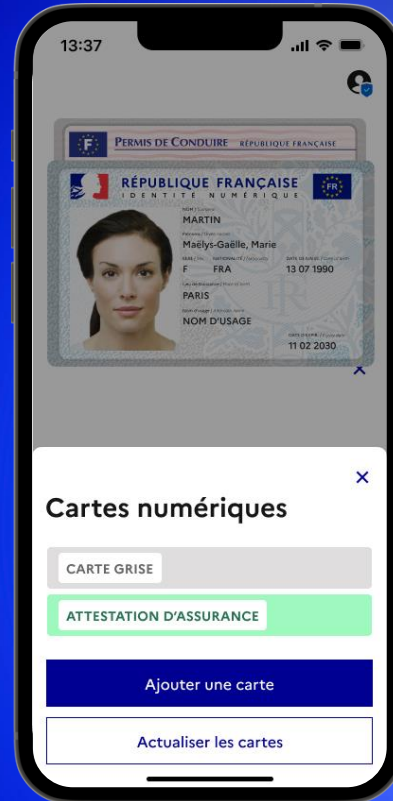




OID4VP



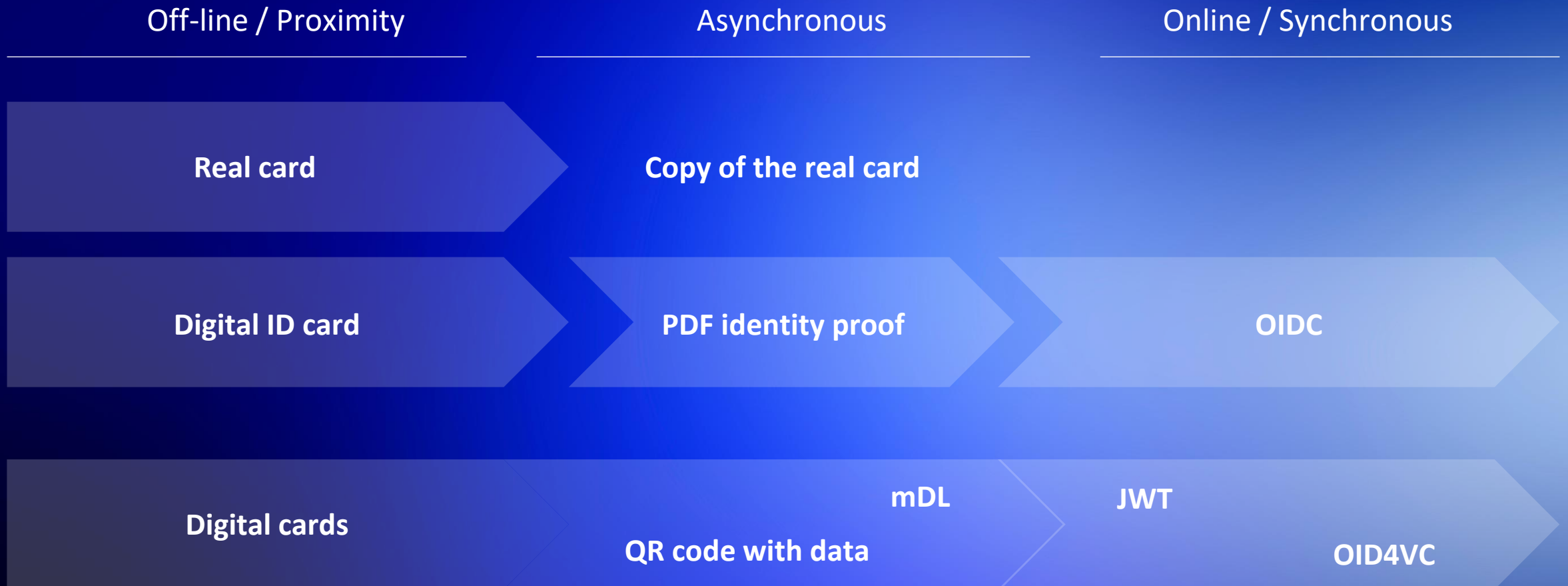
mDL
OID4VCI



mDL



A matrix overview of technology and timing use with France Identité



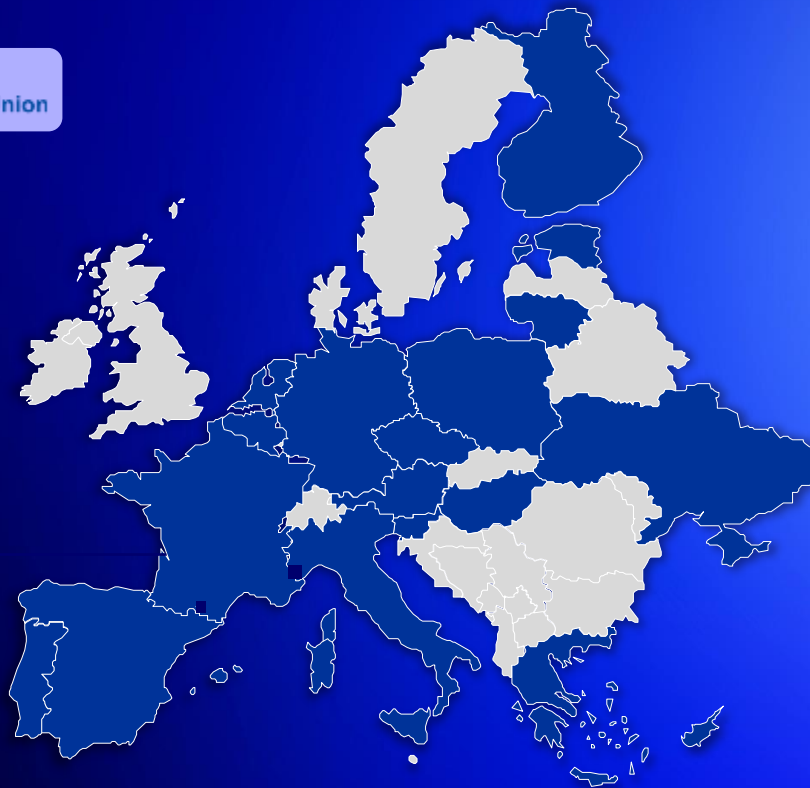
Potential, a Member States driven Consortium

EU Digital Decade Strategy for
2030

Revision of the eIDAS
regulation

Digital Europe Programme

4 LSP



19 Countries (18 EU
member-States + UA),
represented by a SPOC



155
Public and private
entities

Ministries, state operators, research centres, major companies and start-ups acting as wallet issuers, credential issuers, and relying parties



eGov Services

Simplification and full digitalization of identification and authentication. Enabling citizens to use eGov services, such as online administrative procedures, with their European Digital Identity Wallet.

Potential
For European Digital Identity
Co-funded by
the European Union

Enabled by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the Commission can be held responsible for any errors or for any consequences arising from the use of the information contained in this document.



Bank Account Opening

Convenient and secure account opening and management. Opening a current, savings, or custody account online and anytime gives citizens more freedom to manage their bank account.

Potential
For European Digital Identity
Co-funded by
the European Union

Enabled by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the Commission can be held responsible for any errors or for any consequences arising from the use of the information contained in this document.



SIM Card Registration

Simplification and full digitalization of SIM Card registration. Citizens register and activate their SIM Cards for plan and prepaid contracts digitally within the European Digital Identity Wallet.

Potential
For European Digital Identity
Co-funded by
the European Union

Enabled by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the Commission can be held responsible for any errors or for any consequences arising from the use of the information contained in this document.



Mobile Driving Licence

Driving Licence on citizens' personal devices. Equipping citizens with an eDriving Licence, commonly known as mobile Driving Licence (mDL), allowing identity verification and licence checking at car rental services or during police checks.

Potential
For European Digital Identity
Co-funded by
the European Union

Enabled by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the Commission can be held responsible for any errors or for any consequences arising from the use of the information contained in this document.

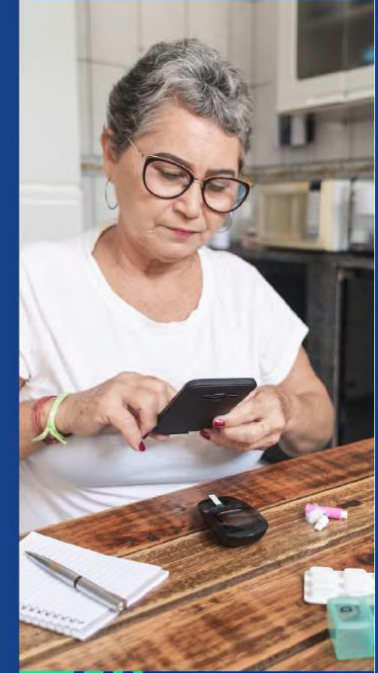


Qualified eSignature

Convenient digital Qualified eSignatures. Increasing eSignature usage integrating their functionality to create qualified eSignatures.

Potential
For European Digital Identity
Co-funded by
the European Union

Enabled by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the Commission can be held responsible for any errors or for any consequences arising from the use of the information contained in this document.



ePrescription

Paperless and convenient medical prescriptions. From the doctor's prescription to pharmacy pickup, the secure European Digital Identity Wallet gives citizens secure data control. This enables access to health information and users' control over who they wish to share their health data with and when, all over Europe.

Potential
For European Digital Identity
Co-funded by
the European Union

Enabled by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the Commission can be held responsible for any errors or for any consequences arising from the use of the information contained in this document.

PANEL: Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

eID Wallet Seminar



Moderator:
**Jean Daniel
Aussel**
Thales



**Torsten
Lodderstedt**
SPRIN-D



Iain Maxwell
FIME



Herbert Leitold
A-SIT



Eyles Lehtihet
ANSSI



**Global
Platform™**

Brussels, Belgium
and Virtual

October 10th, 2024



GP eID Seminar - One- Pager Topics

**Challenges and Opportunities in the deployment
of EUDI – Member States Wallet Issuers**

Date:

October 10, 2024

Presentation to:

Seminar Attendees

Panel Discussion: Challenges and Opportunities in the deployment of EUDI – Member States Wallet Issuers

1. **Fragmentation** - Many member states have different eID initiatives, most of them architecturally differ, so migration from these existing projects to effectively retrofit them into EUDI wallets will differ per member state/solution. Some use existing ID card and some take a cloud-based approach, some may launch an open ecosystem of multiple wallet providers (in the future), some have not yet decided. Several have a hybrid approach or apply a short-term and a long-term strategy, but they all need the WSCD (Wallet Secure Crypto Device) to guarantee attestation - wallets need to trust the SE. Some countries will be happy just to launch and offer a wallet to comply and replace current physical IDs. For others, it will be a catalyst to digitize the government.
2. **Certification**
 - a) EU has a lot of focus on security & privacy, which are key factors and preconditions for making the EUDI-wallet a success and GP has created the CSP to store sensitive data and perform crypto operations, however functional testing and certification to prove interoperability is key. Too many bad experiences for users when it simply “does not work”, will reflect poorly on the wallet, so the functional & interoperability must not be underappreciated
 - b) The EU is creating a certification scheme, but that will take too long because it is complex. Member states will have to certify their wallets before the EU scheme is available - how to do that is problematic!
3. **Immature Specifications** - But technologies that will deliver the WSCD such as GSMA SAM is far from complete (SAM.02) and requires dedicated Subscription Manager servers to issue, perso and manage the wallet applications, which along with the wallet client, the LAA and the SE needs to be tested and certified, so we need a fully operational functional certification process similar to the GSMA Consumer eSIM
4. **Interoperability** – Test specifications need to be written (ISO 18013-6 (in draft), ISO 18013-8 (not started), SAM (not started) etc.), test tools need to be qualified, certification processes need to be defined, but even with all of this we still need to test interoperability which means additional interoperability test events where member states test their implementations against other states readers and vice versa as the LSPs aren't properly addressing interoperability testing either. Therefore, testing budgets need to be approved and detailed planning and effort needs to be allocated to guarantee success



Thank you



Austrian eID & Wallet – Status and Plans

› Austria has mobile eID experience and a solid user base

- › Mobile eID (online) since 2005; currently ~5 mio. users in total, 3 mio. with "ID Austria" (notified at LoA high, attributes)
- › Wallet (proximity) since 2022; 600k mDL, 525 k car licences, 280k age-verification, 150k ID cards, ... further to come

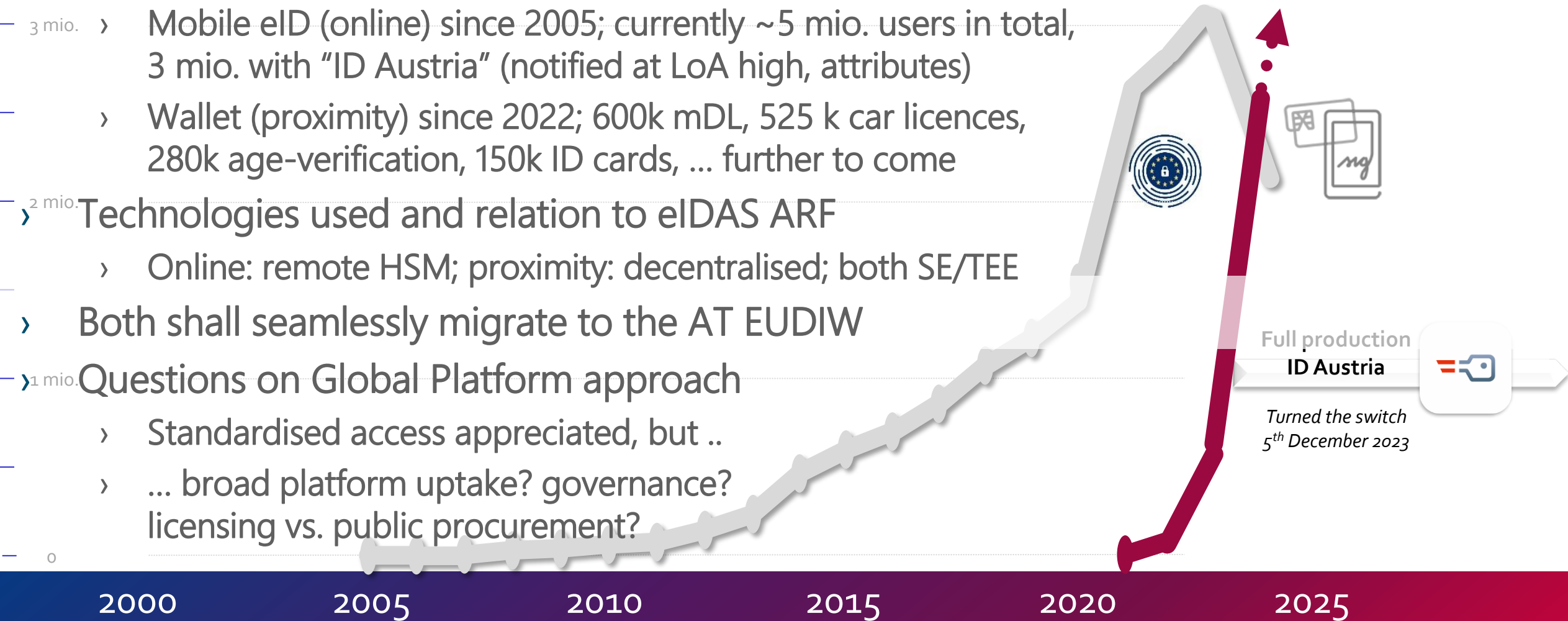
› Technologies used and relation to eIDAS ARF

- › Online: remote HSM; proximity: decentralised; both SE/TEE

› Both shall seamlessly migrate to the AT EUDIW

› Questions on Global Platform approach

- › Standardised access appreciated, but ..
- › ... broad platform uptake? governance? licensing vs. public procurement?



a-sit.at/

Herbert.Leitold@a-sit.at

CHALLENGES AND OPPORTUNITIES IN THE DEPLOYMENT OF EUDI – MEMBER STATES WALLET ISSUERS

Elyes LEHTIHET – ANSSI – FR



Certification of EUDI wallet

Conformance to CIR (EU) 2015/1502 for assurance level high for eID part

CC certification **EAL4+ AVA_VAN.5** for WSCD and if needed WSCA

Use of **tamper resistant device** WSCD

FitCEM (CEN EN 17640) like certification for more dynamic parts (wallet instance)



Resistance against a high attack potential

Avoid inconsistencies and a race to the bottom

- The WSCD must be included into the wallet certification scope
- The WSCD must be evaluated against the European Common Criteria Scheme (EUCS) for levels EAL4+ AVA_VAN.5 or higher
- The mention of “equivalent approaches” might lead to inequality in the level of security of the different EU wallets





THANK YOU!

French National Cyber Security Agency (ANSSI)
[CYBER.GOUV.FR](https://cyber.gouv.fr) | [X](#) | [LINKEDIN](#)

PANEL: Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

eID Wallet Seminar



Moderator:
**Jean Daniel
Aussel**
Thales



**Torsten
Lodderstedt**
SPRIN-D



Iain Maxwell
FIME



Herbert Leitold
A-SIT



Eyles Lehtihet
ANSSI



Brussels, Belgium
and Virtual

October 10th, 2024

Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany’s perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France’s perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform

Samsung EUDI Wallet

Smartphone manufacturer
perspective for EUDI deployment

Dawid Wróblewski

Digital Identity Product Manager, Samsung Wallet

Samsung Electronics

10th October 2024

Agenda

01

**Samsung Mobile
Security**

02

Samsung Wallet

03

**EUDI
challenge**

04

**What's
Next?**

01 | Samsung Mobile Security

Enabling developers to build a secure & private services

Over 35k
B2B
partners

Knox



eSE



Secure storage
(EAL6+
rating)

01 | Enhanced security with Samsung Knox

Security from the Chip-up

- Samsung manufactures everything from the chip up
- Security from design to manufacturing and quality assurance

Data Isolation

- Private data can be completely isolated in Secure Folder
- Work or personal apps can be separated on a fully-managed device



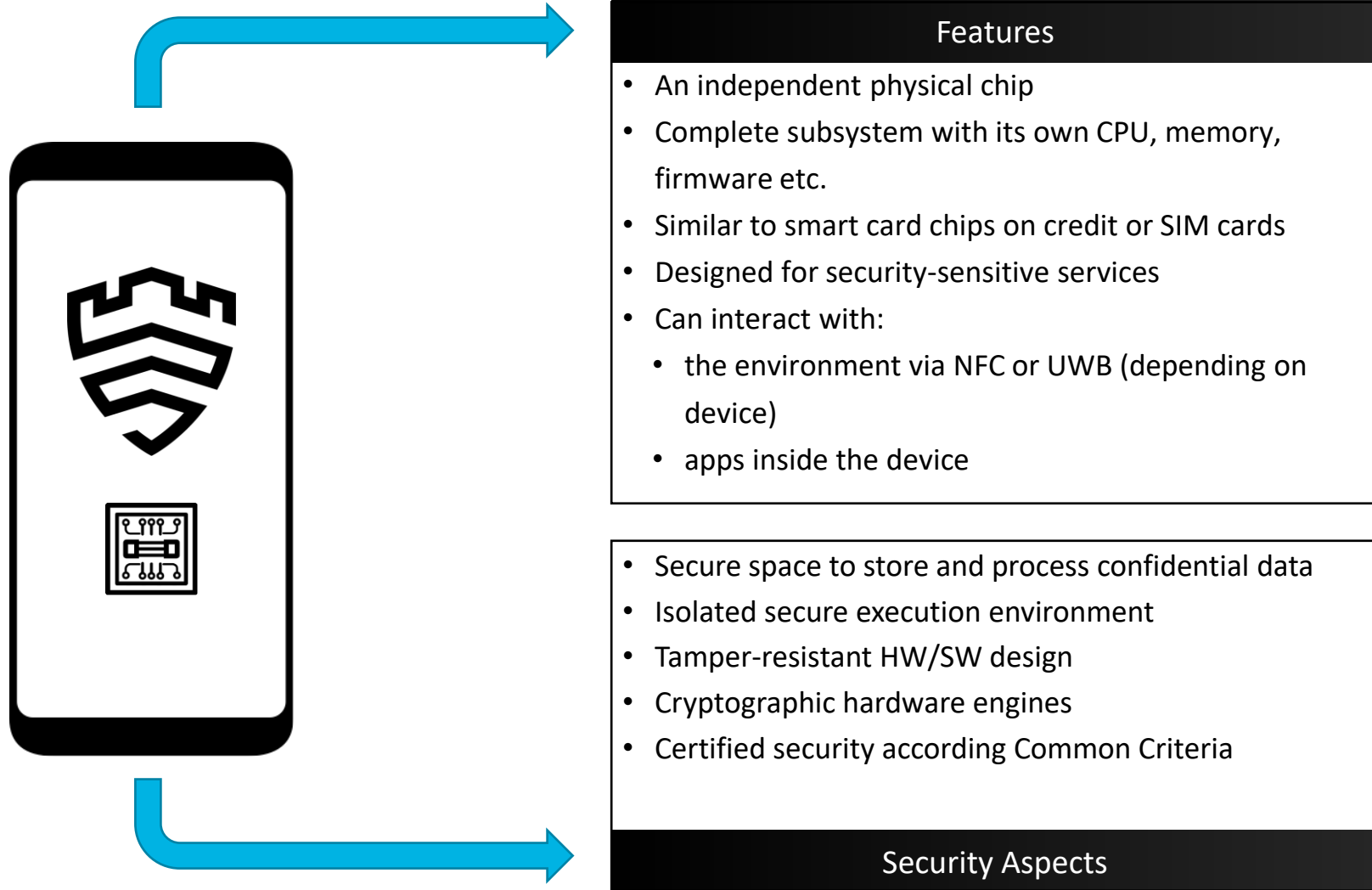
Data Encryption

- Dual-layered data-at-rest encryption for extra protection
- Sensitive data remains encrypted even after initial device unlock

Runtime Protection

- Samsung devices are always running in a safe state
- Unauthorized access to kernel is monitored and blocked

01 | embedded Secure Element (eSE)



Device = Wallet?

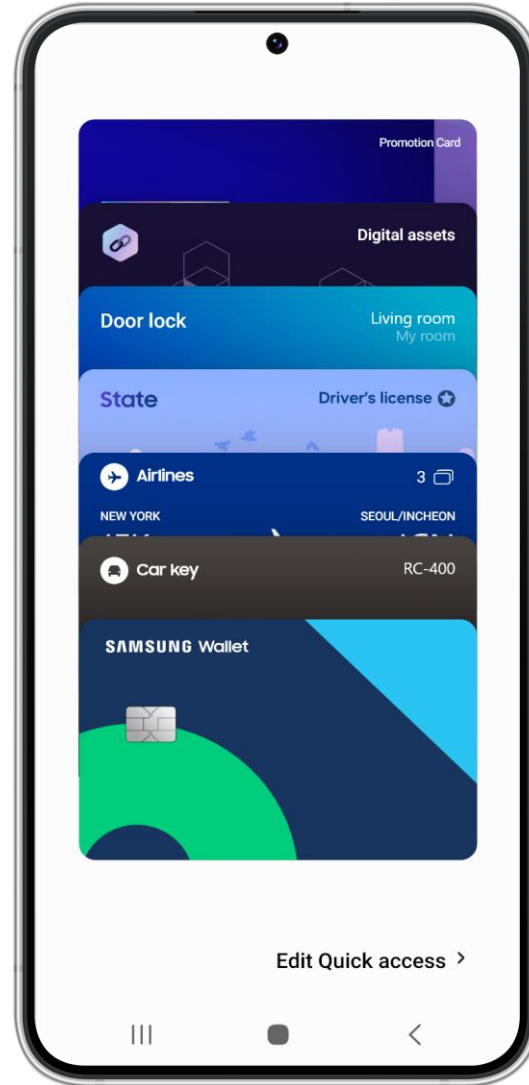



02 | Samsung Wallet

A smart wallet is already in your Galaxy.

Samsung Wallet is your go-everywhere, worry-free app for essentials — keys, credit cards, tickets and boarding passes. All in one spot, all accessible with one swipe. And you can secure it all behind a PIN number or personal biometric data, so only you can access it. So no more worries, hassle or jumping from app to app, even for your Password.

- 
Payment
- 
Boarding pass
- 
Digital Key
- 
Digital ID
- 
Samsung Pass (Autofill)
- 
Ticket Coupon Membership
- 
Digital asset



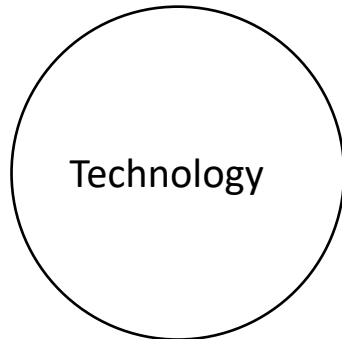
 **Fast. Safe. Samsung Pay.**

Samsung Pay allows you to tap to pay with your device, making in-store transactions quick and contactless. And it adds extra layers of digital security to protect your payments, whether you're online shopping or in-store browsing.

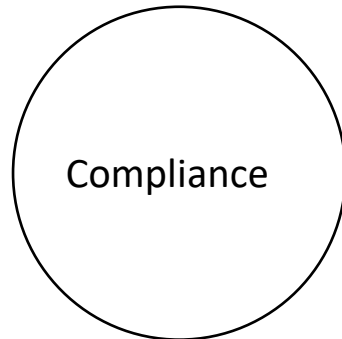
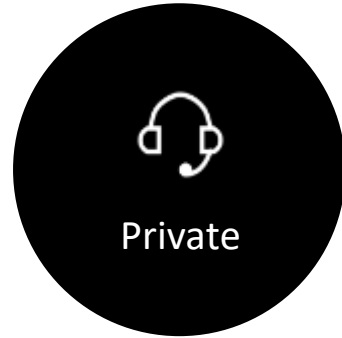
 **Your Wallet. Secured.**

Samsung Wallet is protected by Samsung's security platform, Samsung Knox, which includes fingerprint recognition and encryption to make sure important user data is protected. And it stores sensitive information in an isolated environment, which offers an extra layer of defence against potential hacking attempts.

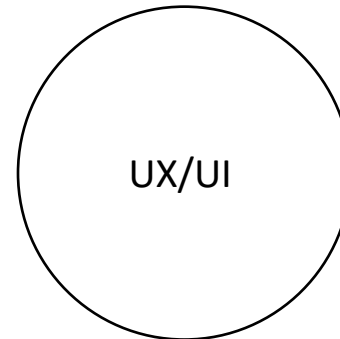
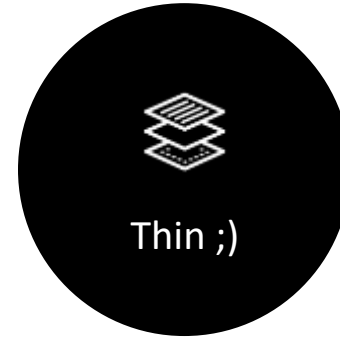
Delivering Wallet experience to Samsung Customers



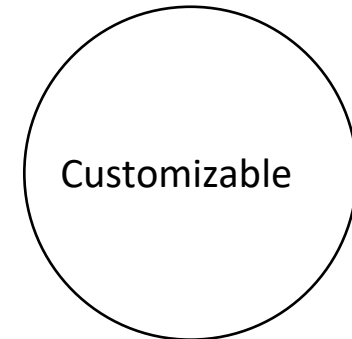
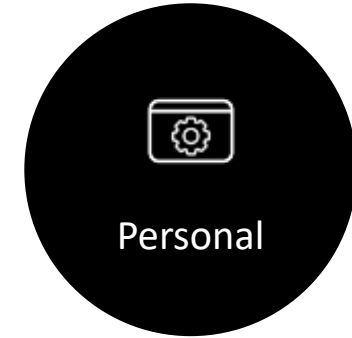
- Certified solutions (Knox)
- Root of trust (from factory to user)
 - Device security



- Privacy by design
- Regulatory compliance



- Quick Access to cards
- Optimized user flows
 - Card catalog



- Edit Quick Access
- Easy Card Enrolment

Standardization



EU Digital Identity
Wallet

Architecture and Reference
Framework

ARF – when it is considered as final?

eID Diversity



How to find a common ground for all EU
Member States?

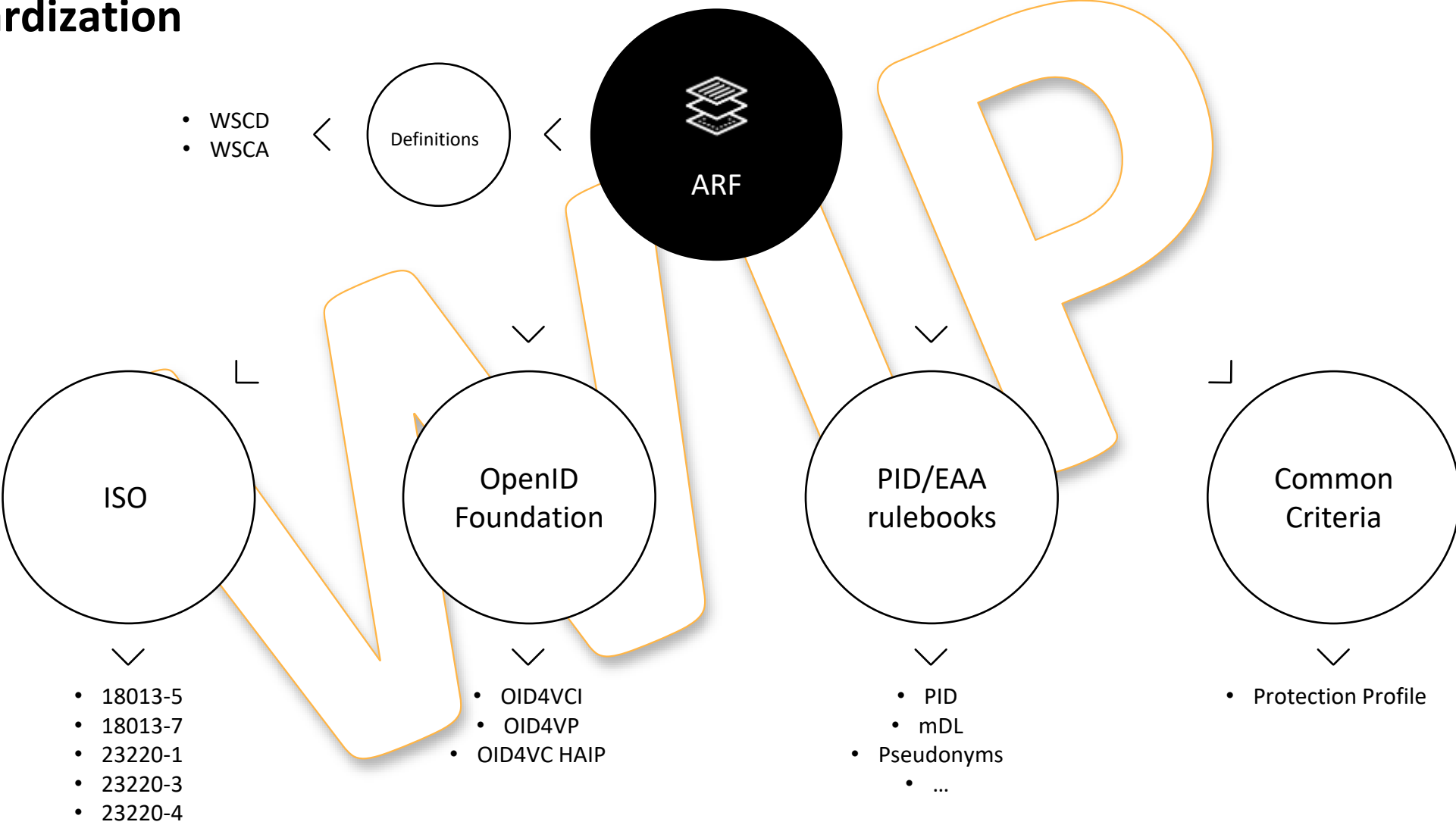
Governance & Operating Model



How to increase adaption?
What is the operating model for EUDI?

03 | EUDI challenge

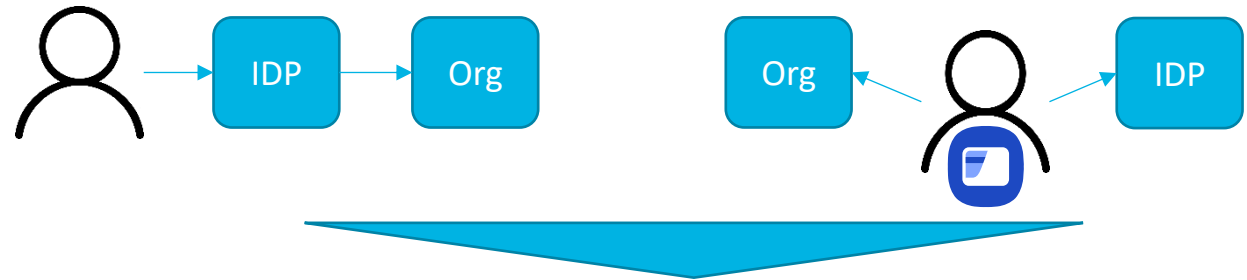
Standardization



03 | EUDI challenge

Governance & operating model

Digital ID operating model (r)evolution – from federated to SSI



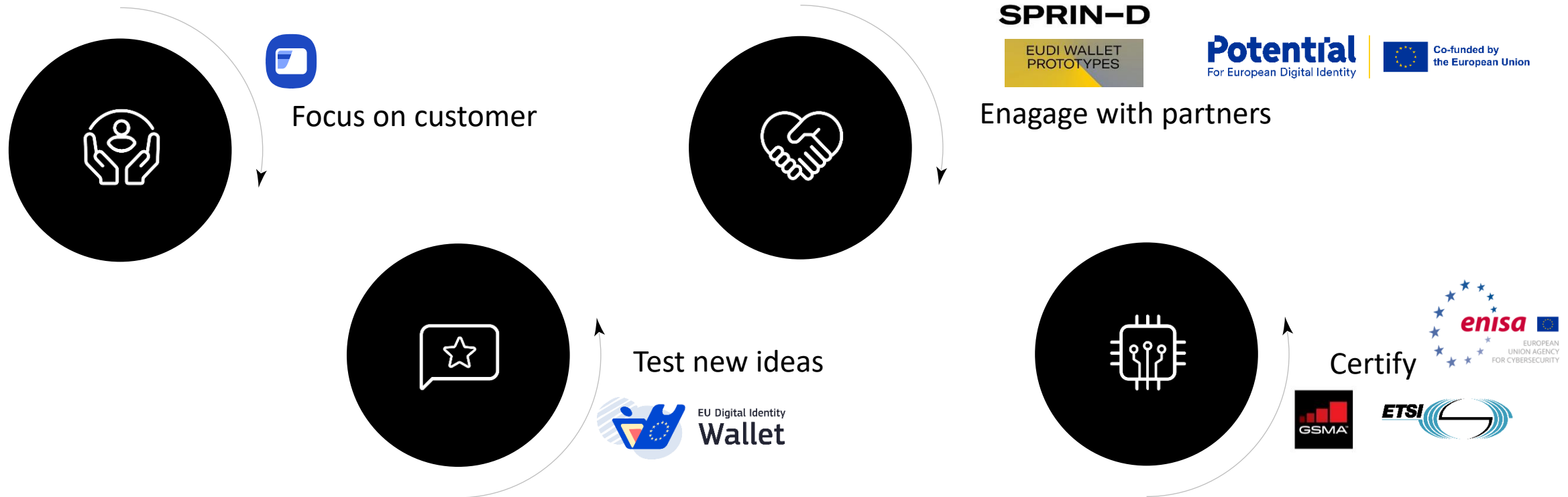
Rules & responsibilities



Business model



SAMSUNG



Backup

Samsung's Approach to Mobile Security

Multi-layer protection backed by strong hardware security

- To protect sensitive and critical information backed with hardware protection
- Root of Trust is protected with full hardware security.
- Secured by Knox (<https://www.samsungknox.com/de/about-knox#features-and-devices>)



Open platforms and open standards

- Security features are available for our partners as well as for our applications and services.
- Hardware-backed protection is offered for applications requiring stronger protection, including 3rd parties.







Lifecycle management of security

- During the development, we apply a secure development lifecycle management.
- Once the product is released, a lifecycle of vulnerability management processes is initiated such as vulnerability management, quality assurance and patch delivery to the product in the hands of customers.

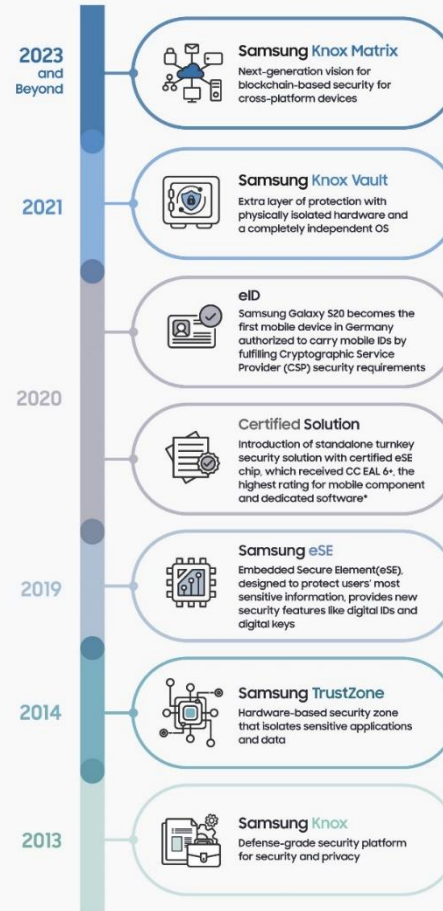
<https://news.samsung.com/global/samsung-raises-the-bar-for-mobile-experience-innovation-committing-to-three-generations-of-android-os-upgrades>

<https://news.samsung.com/us/samsung-galaxy-security-extending-updates-knox/>

00 | Certifications

Component	Certifications
Vendor application	Vendor eSE applet
Crypto-plugin	CSP (Cryptographic Service Provider) PP (EAL4+) PP 0104  
Platform (Javacard OS)	Vendor service e.g.) equivalent to <ul style="list-style-type: none">• PP QSCD - Part 2: Device with key generation• PP QSCD - Part 3: Device with key Import• PP QSCD - Part 6: Extension for device with key import and trusted communication with signature creation application Java Card System PP (EAL4+) PP 0099  
Chip (H/W)	Security IC Platform Protection Profile (EAL6+) PP 0084  


10 Years of Samsung Knox Security:
Key Highlights



*Applies as of the day of publication.

Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany’s perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France’s perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform

EUDI Large scale pilot learnings (Payments)

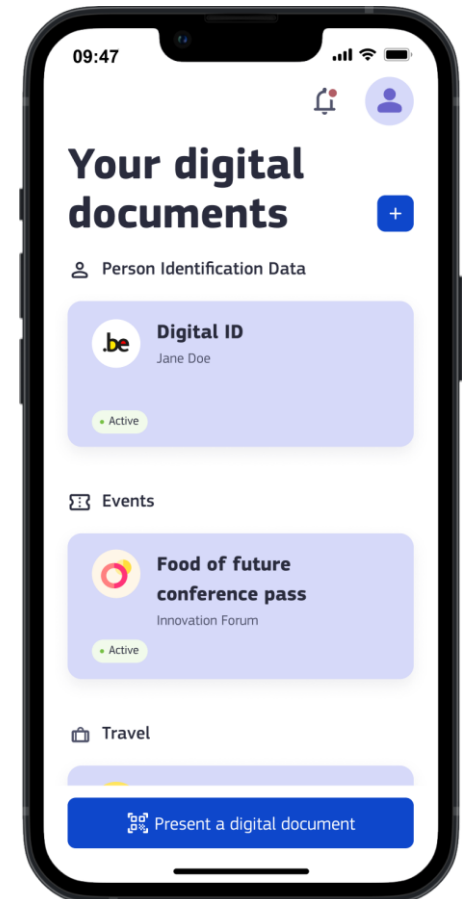
GlobalPlatform eID Wallet Seminar

October 10, 2024

Laurent Bailly – baillyl@visa.com

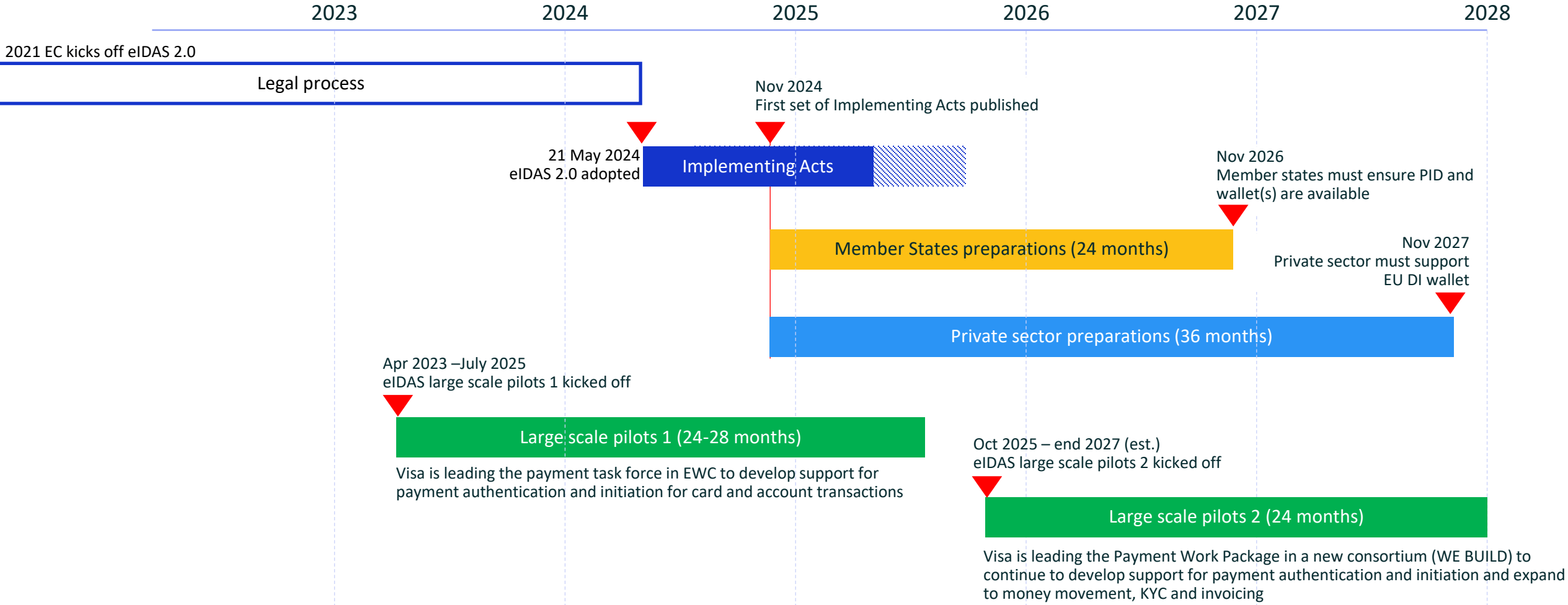
eIDAS 2.0 in a nutshell

- The **EU amended the regulation** for “electronic IDentification, Authentication and trust Services” (eIDAS 2.0) in May 2024.
- One of the provisions requires all EU member states to make available a **“European Digital Identity Wallet” (EUDIW) by 21 November 2026**.
- **Citizens will be able to store their ID**, driver’s license, education certificates and other types of attestations inside the EUDIW.
- **All regulated businesses including financial institutions** will be required to accept the EUDIW by **21 November 2027**.
- The European Commission has **awarded four consortia to carry out “Large Scale Pilots”** to test the EUDIW and underlying technology.
- **A new LSP call** has been launched in May 2024 **by the EC to select new consortia** that will further test the EUDIW for travel, business, payments & banking and age verification use cases

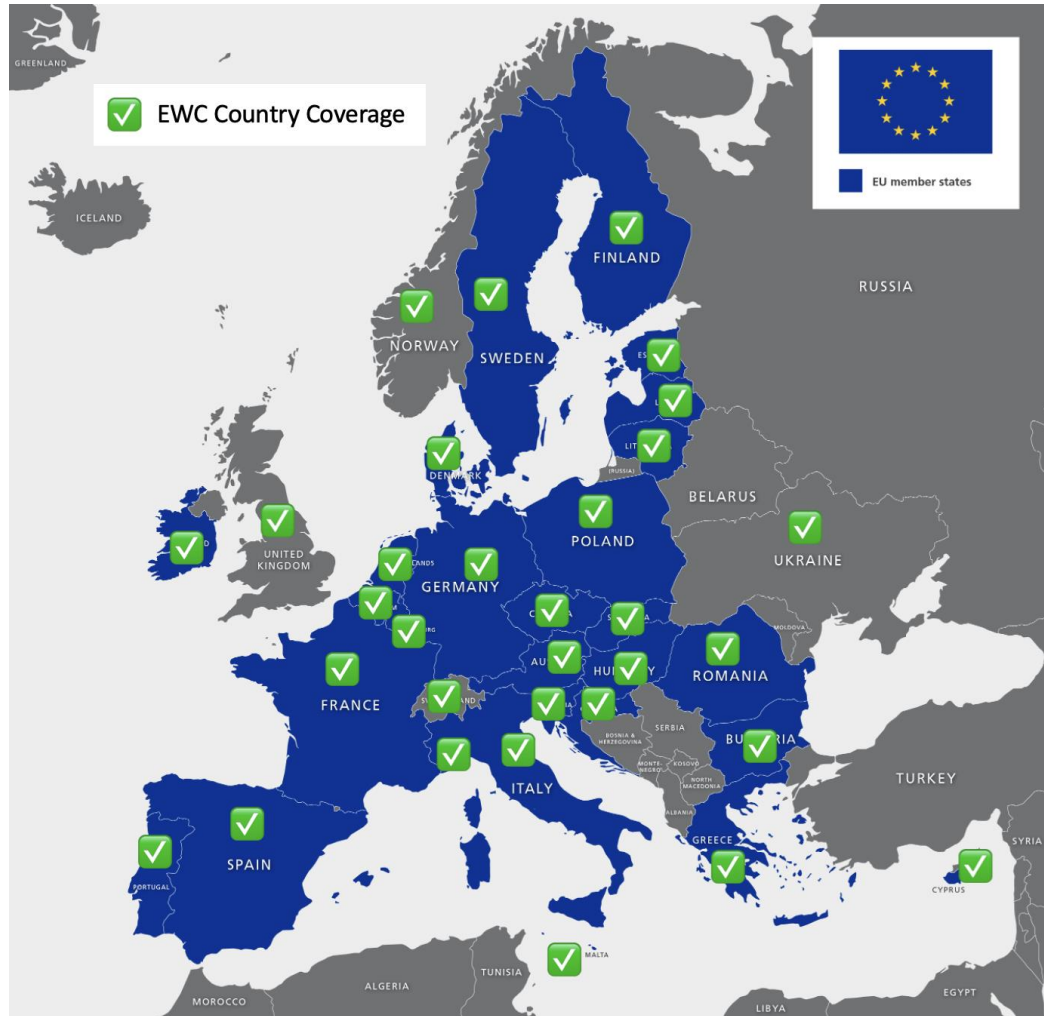


For illustration purpose only

eIDAS2 timelines



EWC large scale pilot



Focus on travel, organizational digital identity, and payments

Driven by the Member States but public-private to its core

Focus on remote and local user flows

Coordinators:

- Bolagsverket (Sweden)
- Ministry of Finance (Finland)

The EWC Payment Taskforce

- Explores **barriers and enablers** to scale adoption and acceptance of EUDIWs through payments
- Core **beliefs and principles**:
 - Payment is a **key use case**, covering both card and account-based transactions
 - Solutions should be based on and inform **open standards** for the benefit of the ecosystem
 - Strive for minimal impact on **existing infrastructure** in the field
 - Start with **authentication**, then progress with **payment initiation**
 - Innovate by **combining payment and identity**/other attestations



EWC Payment focus areas



Payment Authentication

EUDIW as an alternative SCA method for online payments

Satisfying regulatory obligations

- Linking a user's EUDI wallet with his payment account or card (**registration**)
- **SCA for card-based and account-based** online payments
- EUDI wallet **invoked by payer's bank** (card issuer or ASPSP) or authentication data **captured by the payee** (merchant)



Payment Initiation

EUDIW as a payment wallet, holding payment credentials

Beyond SCA, opportunities instore or online

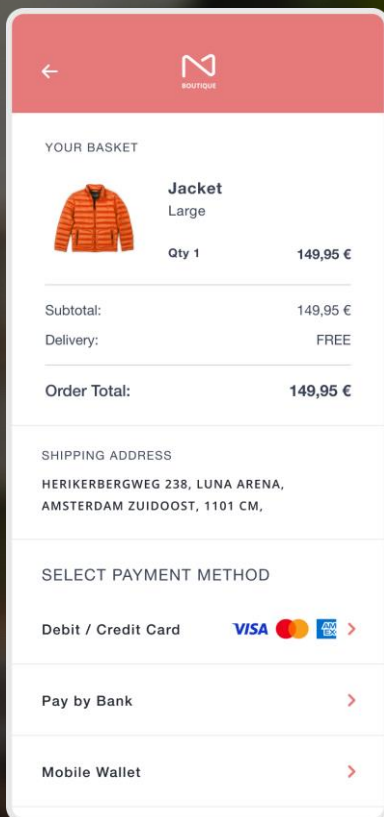
- EUDI Wallet to provision **card and account tokens** to initiate online or instore payments
- **Instore NFC card payment** with no impact on merchant acceptance – now available on both Android and iOS devices
- Push the **card or account token payload to an online merchant** for payment processing

Combining payment with identity attributes, enabling innovative payment flows and value for the market

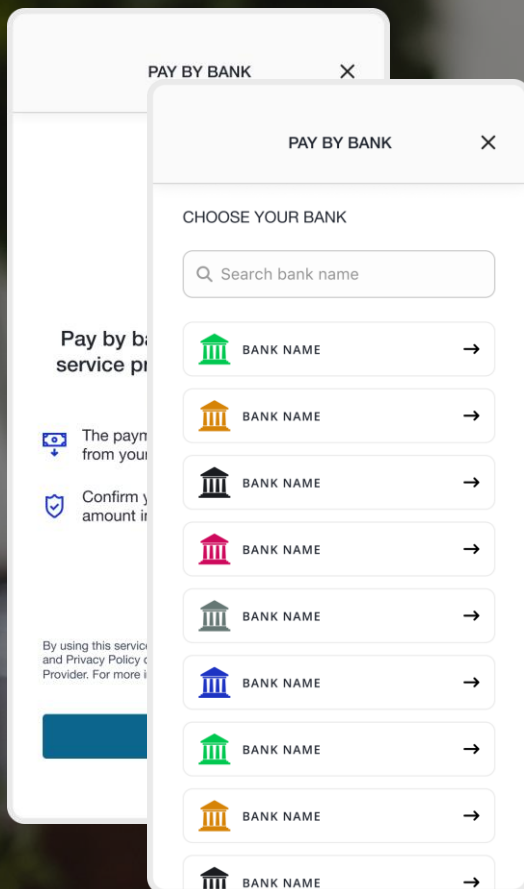
Payer's bank invokes EUDIW for SCA – Account-based payment case

- Prerequisite: User has registered his EUDI Wallet with his bank
- Merchant sends payment initiation request to its PISP
- Bank (ASPSP) proposes the EUDI Wallet option for SCA – source of funds selected in the EUDI Wallet

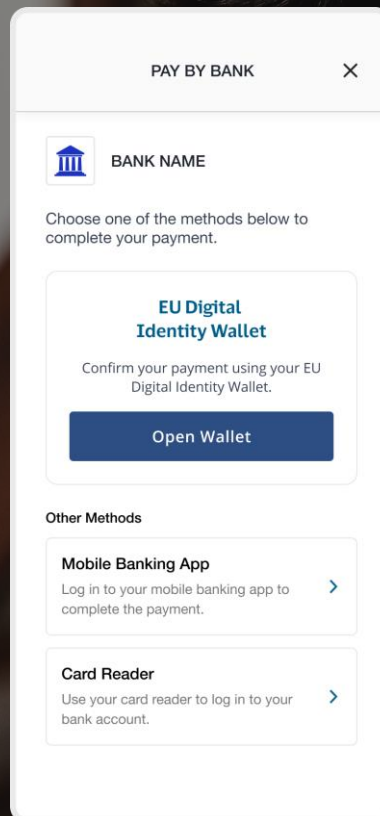
Payment method selection



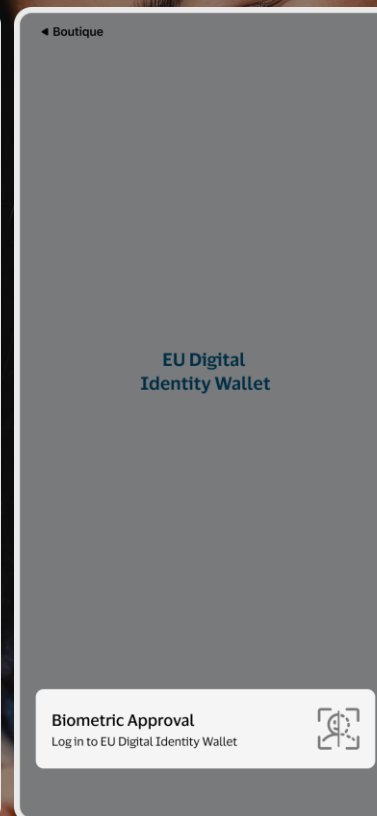
Consent capture and bank selection



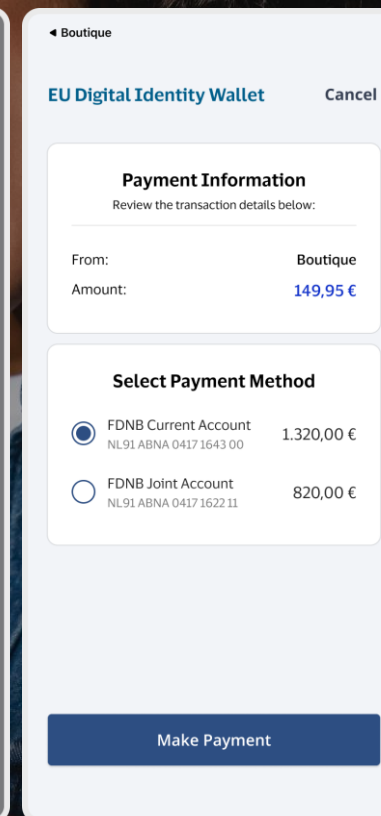
Bank authentication options



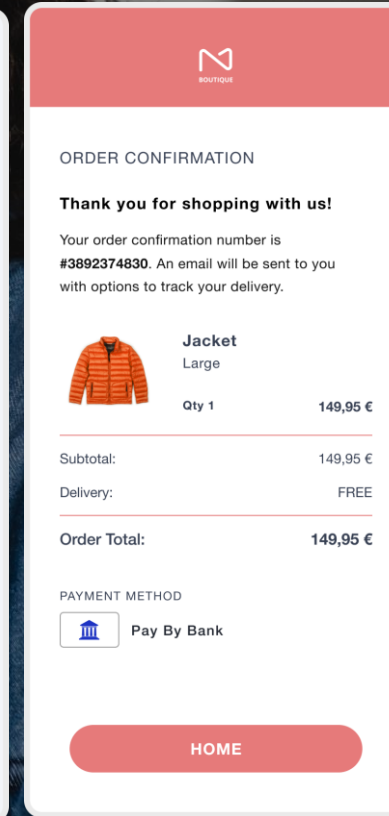
Log in to Wallet



Review and confirm payment



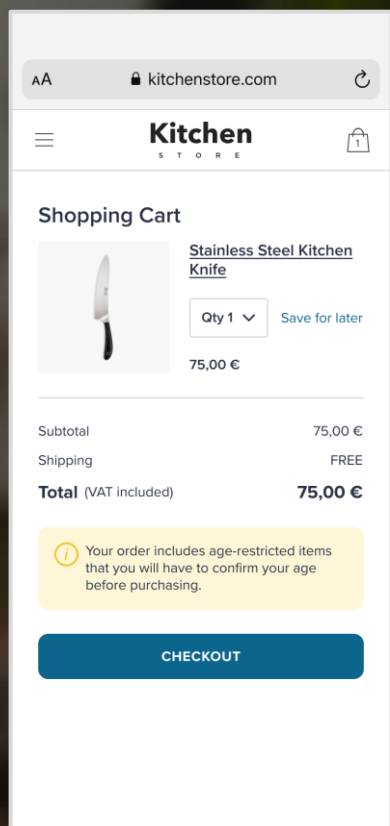
Order complete



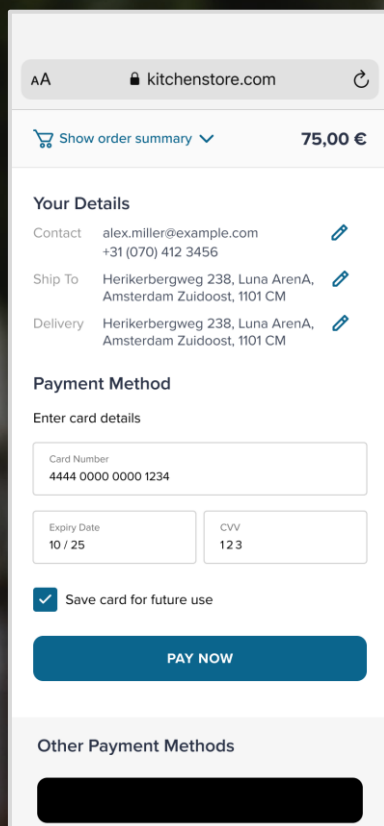
Merchant invokes the EUDIW for SCA – Card-based payment case

- Prerequisite: User has registered his EUDI Wallet with his bank
- One SCA for both payment authentication and age verification
- Merchant invokes the EUDI Wallet, captures authentication data and passes it back to the payer's bank

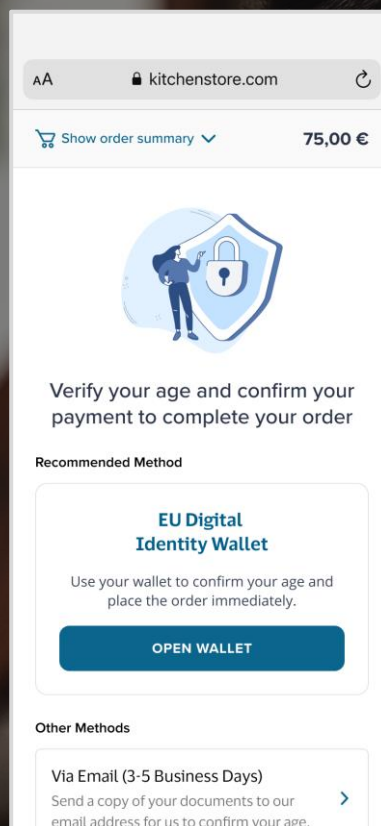
Shopping cart



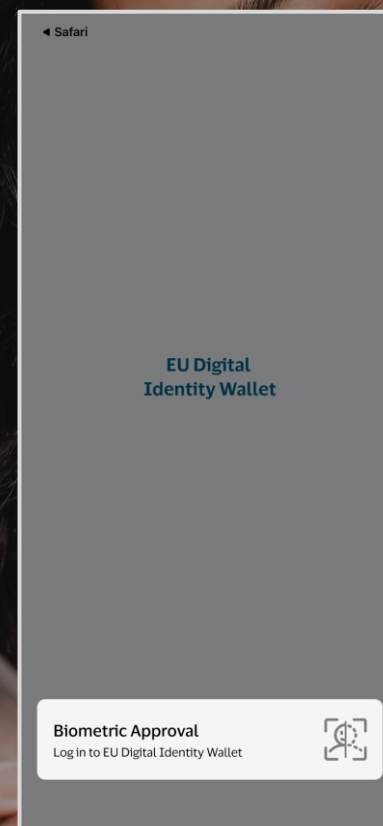
Checkout



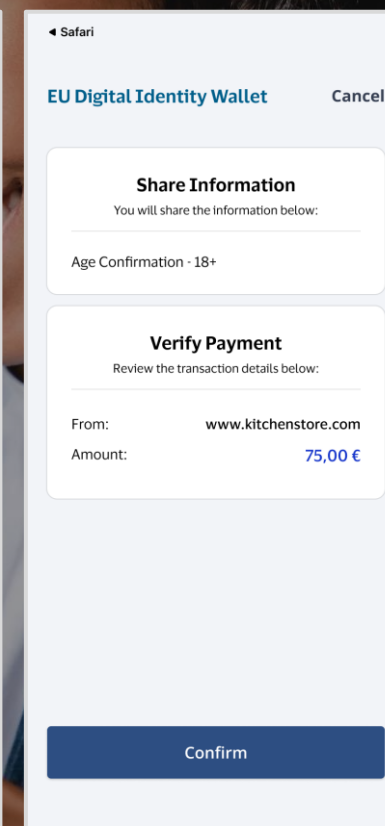
Payment & verification method selection



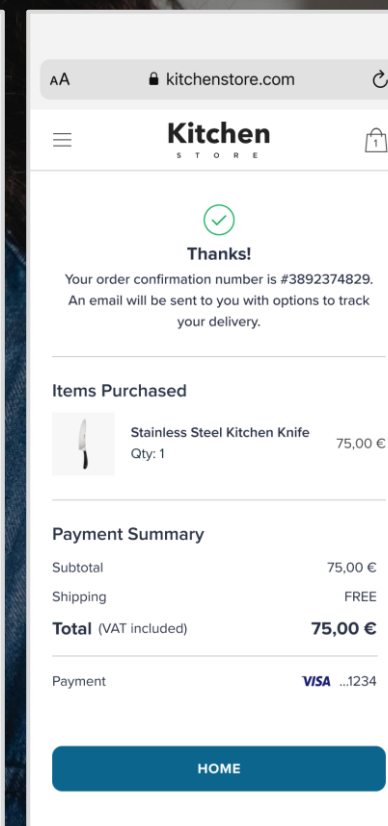
Log in to Wallet



Consent



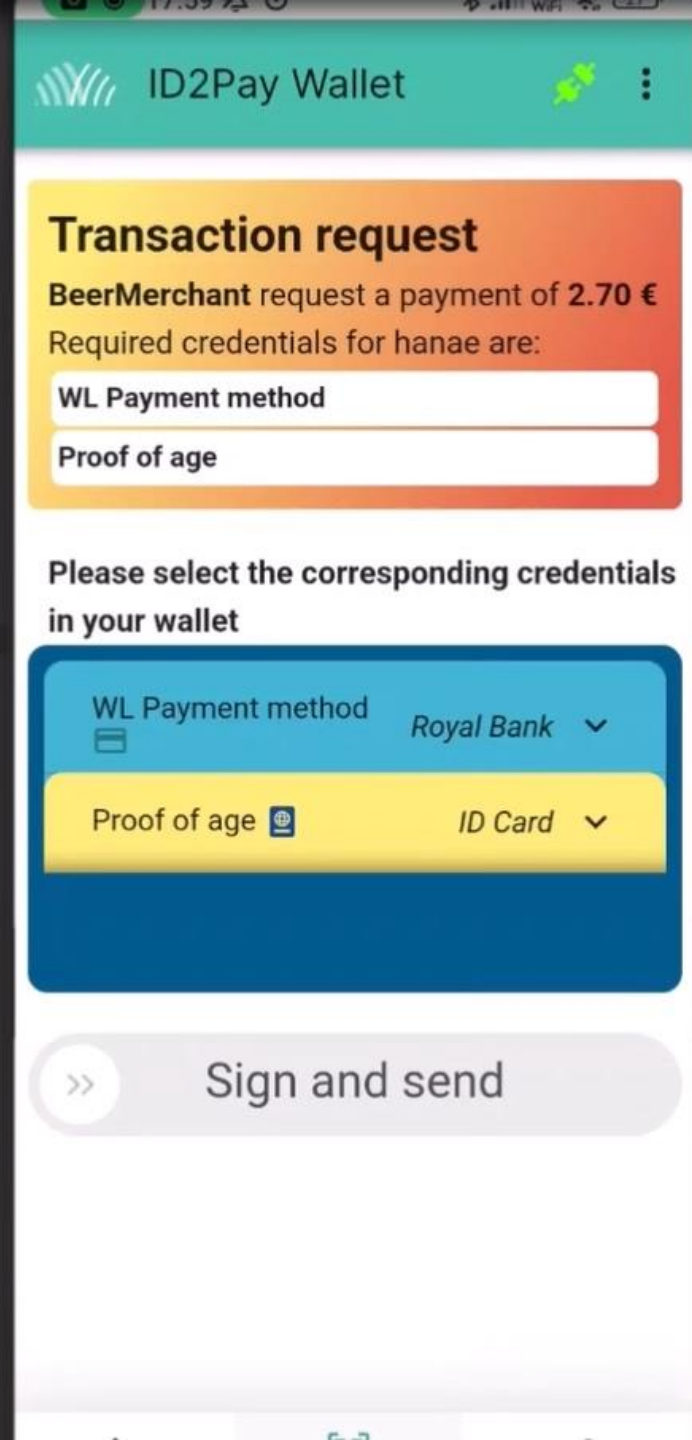
Order complete



Beyond SCA, what payment initiation with the EUDIW could look like



QR code vending machine with age verification example



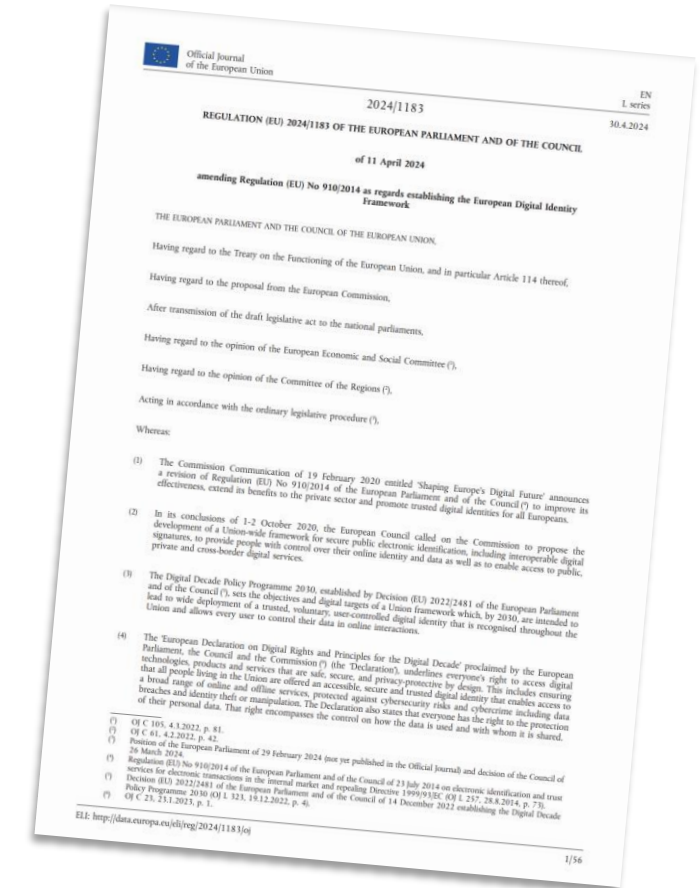
eIDAS 2.0 inclusion of payments

eIDAS 2.0, Article 5f(2):

- “Where (...) relying parties (...) are required by (...) law to use **strong user authentication** (...) including in the areas of (...) banking, financial services (...), those (...) relying parties shall (...) also **accept European Digital Identity Wallets** (...).”

eIDAS 2.0, Recital 62:

- “**Secure electronic identification and the provision of attestation of attributes should (...) support the fulfilment of strong customer authentication** requirements for online identification for the purposes of account login and of initiation of transactions in the field of payment services.”



Source: eIDAS 2.0, [Regulation \(EU\) 2024/1183](#) of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

What have we learnt so far?

Challenges:

- Need to get the technology standards right and completed – including industry specific standards and ability to leverage existing infrastructure – e.g OpenID4VP for transactions
- Risk of continued national fragmentation as build and certification are national responsibilities
- Commercial models still vague – but entities who own (information) assets are well positioned in principle
- Regulatory and legal alignment – e.g Liability and Outsourcing regime, unlinkeability (eIDAS2) vs tracability (PSR)

Opportunities:

- Significant installed base of interoperable and trusted EU DI wallets available to rely on – investments done by others
- EU DI wallet brings potential new use cases – wider choice of wallets for payment, flexibility in payment authentication (i.e. merchant-captured authentication), pay and confirm identity attributes, digital proofs such as proof of income or proof of IBAN
- Business opportunities across the eco-system created through eIDAS by lowering costs or introducing new revenue opportunities

eIDAS, EU DI wallet and the ARF are overcoming industry “commitment phobia”: Wallets and Verifiable Credentials are part of the future for digital transformation – the direction is set, let’s now focus on execution !



Thank you

Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany’s perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France’s perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform



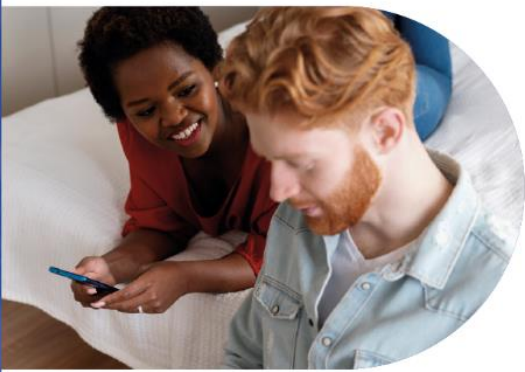
Implementing the EUDI Wallet

From fantasy to reality

EUDI Wallet or Discworld's Luggage ?

- Store anything
- No carrying: it follows its owner
- No instructions, works for anyone
- Handy in all situations
- Relentlessly defends its owner
- Eats anyone too curious





iDAKTO

iDAKTO makes digital identity easier to create, use and share.
As the leading technology provider for digital identity wallets, we help governments build their EUDI Wallet fast with best-in-class security.

#1

Citizen eID Platform

3

National digital ID programs

>50

80% R&D

People dedicated to digital ID

2019

Year of creation

They trust us:



France



Morocco



Egypt



Lebanon



Ivory Coast



ID Wallet Certified By ANSSI

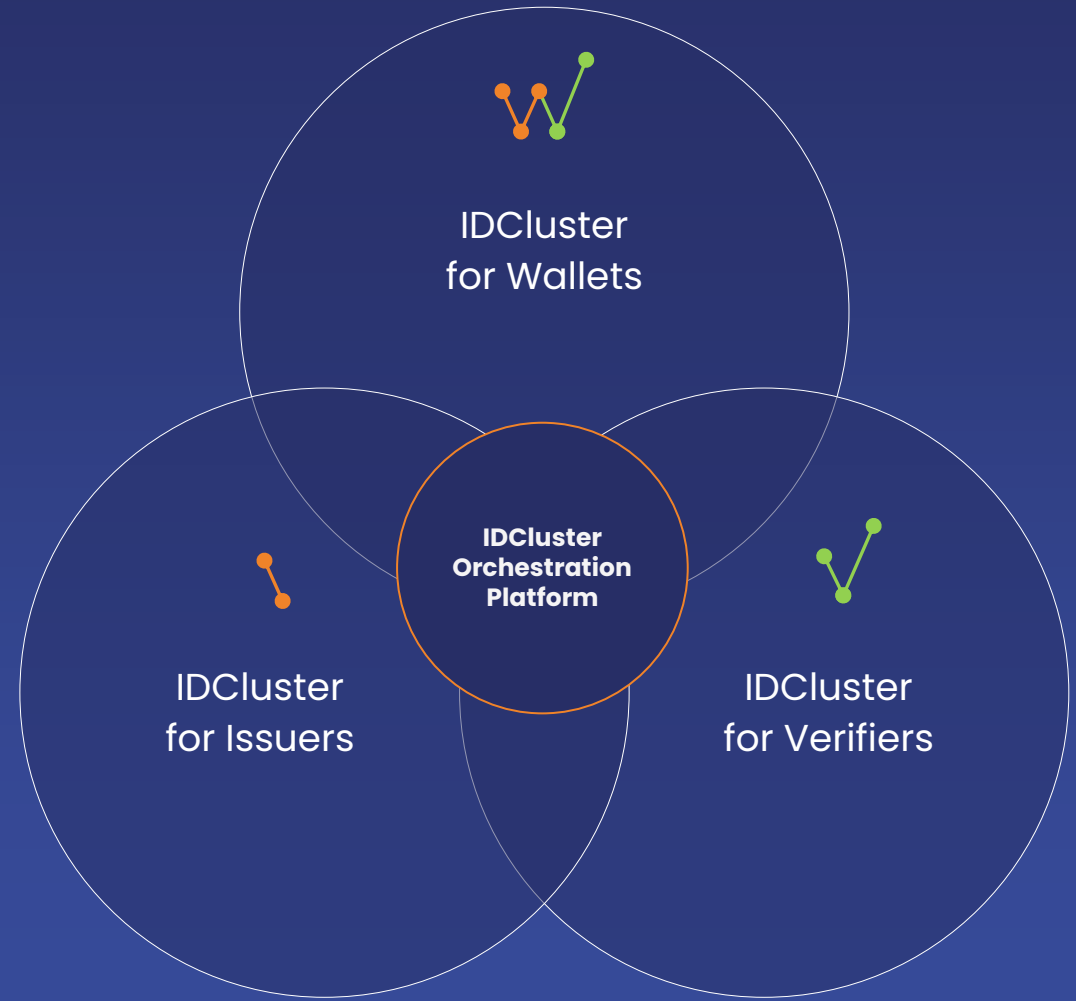
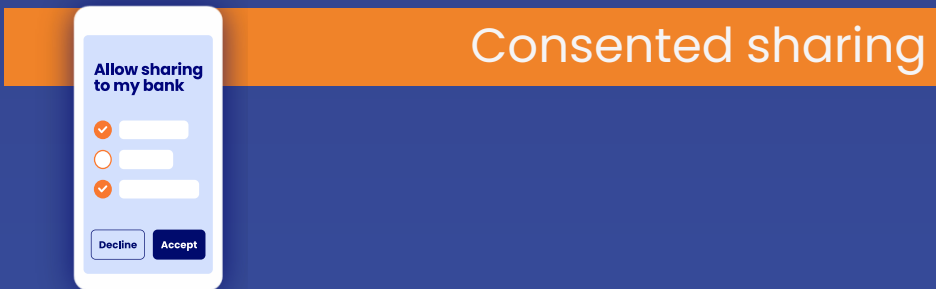


Innovation Award 2024



Label France Cybersecurity 2023 & 2024

iDAKTO Solutions for reusable identity



Do I actually need a DI wallet?

There is currently no foolproof solution to prevent fraud in high value use cases such as opening a bank account online.

- **We start with security and assurance level high**
- **We plan for adaptive UX to account for acceptance versus risk in other scenarios**



There are 4 situations to account for and secure



Managed by
government's civil
registry systems

Holder binding is the key

Many solutions assume PIN and mobile biometrics are sufficient.

- ! This does not achieve assurance level high
- ! Device biometrics are only a possession factor

In Europe, the eID card is **the ideal solution** for the **highest level**

IDCluster orchestrates numerous authentication factors to cover all use cases and assurance levels



Secure storage without Sapient Pearwood?

Relying only on phone security mechanisms is insufficient for level high

- ✓ **We leverage the CC Certified eID for level high**
- ✓ **We use smartphone secure storage for level low**
- ✓ **We implement remote storage using HSM and strong authentication**
- ✓ **Our certification does not care that a phone is rooted**



Winter is coming!

Security by design is a founding requirement of the EU digital identity wallet and of our IDCluster solution

- We look at security before all else
- We use existing certification schemes (FITSEM)
- We setup a dedicated security team
- We submit to a bug bounty program
- We provide regular updates



ID Wallet Certified
By ANSSI



Security, Privacy and UX Design

User training should not be forgotten

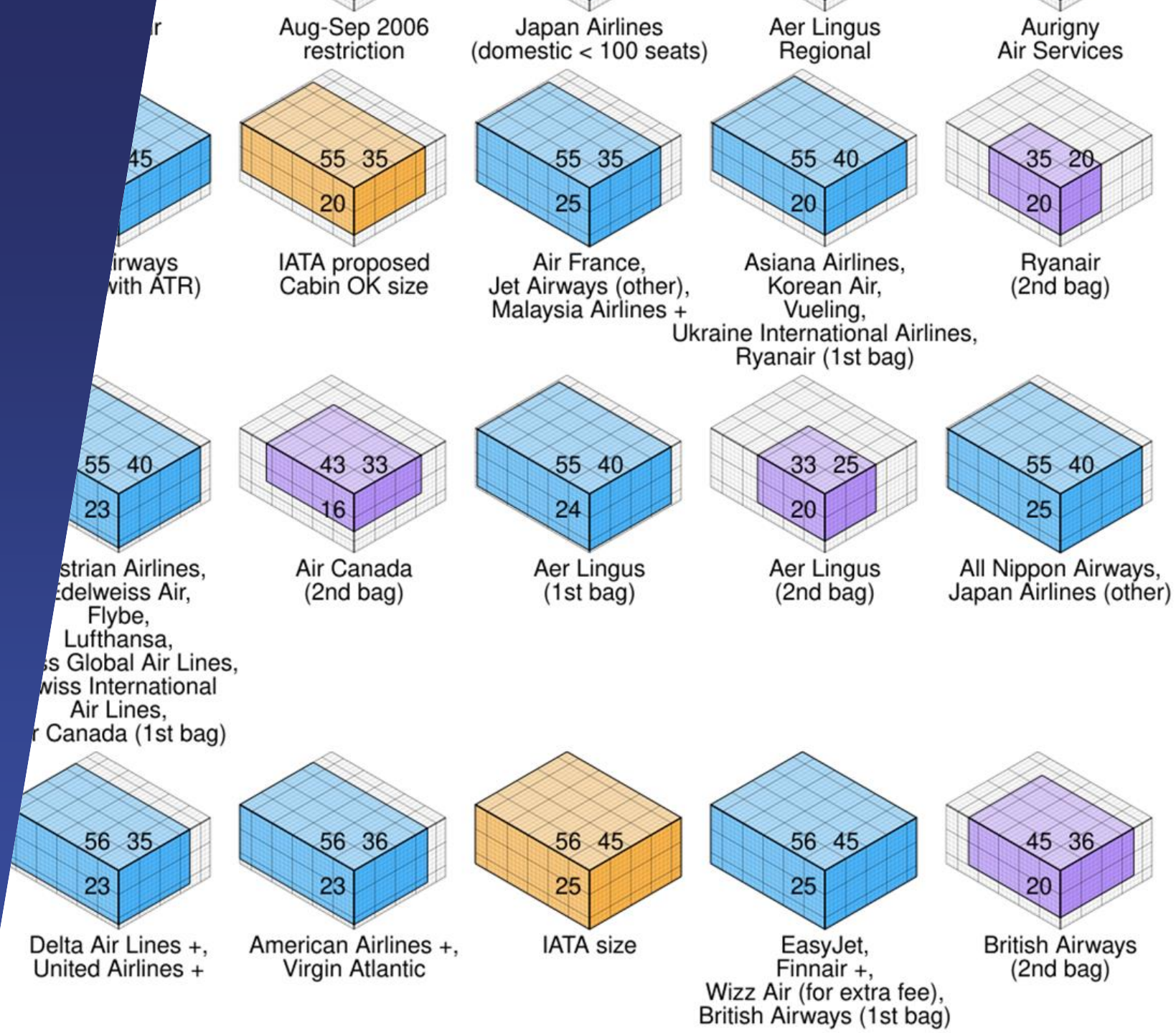
- Users should be a minimum aware of security risks and should care



Interoperability: One standard to rule them all?

Assume the wallet will be multi-standard and modular

- We participate in standards
- We implement and promote standards
- But we don't wait for standards



Weaving trust

The commission has yet to provide information on the EUDI trust framework.

However, there are existing frameworks that can be relied upon

! **For PID the existing ICAO PKI infrastructure is sufficient**



Patented innovations: Not magic, just never seen before

IDCluster is covered by 8 patents and counting, including:

- **Secure PIN capture**
- **Secure channel for device to server communications**
- **“Tap2Check” device to device presentation over NFC on IOS and Android**



A digital wallet or a digital suitcase?

Too many are rushing to throw everything in.

- Take what is essential for your destination
- Make sure you have the basics and get the rest locally if needed





Wallets should be something modular you build on over time



The French wallet is deployed and used with an assurance level high



It sets a live reference implementation on which to build interoperability



TRUST. CONNECT. EMPOWER.

iDAKTO provides innovative solutions to enhance identity systems, making digital identity easier to create, use and share. Our wide array of solutions is deployed globally across governments and corporate institutions leveraging technology to safeguard private data and elevate the user experience.

They already trust us for Digital ID



France Titres
(French Secure
documents Agency)



General Direction
of The National Security
(Morocco)



Central Bank of
Egypt



Independent
Electoral Commission
of Ivory Coast



Lebanese General
Security

PANEL: Readiness of the ecosystem to support EUDI

eID Wallet Seminar



Moderator:
Jean-Baptiste Milan
HID Global



Laurent Bailly
VISA



Dawid Wroblewski
SAMSUNG



Daniel Goldscheider
OPEN WALLET
FOUNDATION



Yann Bouan
IDAKTO



Brussels, Belgium
and Virtual

October 10th, 2024

Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany’s perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France’s perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

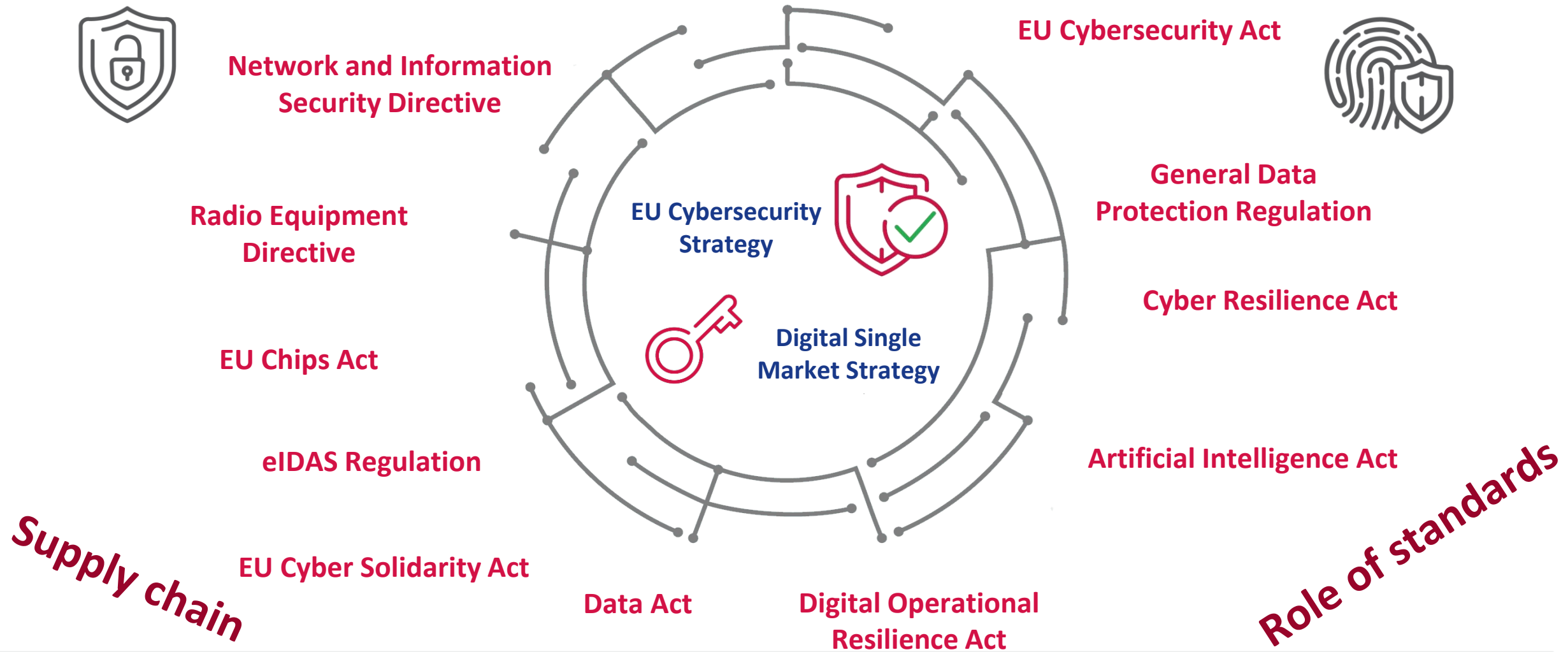
ENISA, EIDAS AND STANDARDISATION

Sławomir Górniak

Market, Certification and Standardisation Unit

10 | 10 | 2024

EU LEGISLATION – CYBERSECURITY LANDSCAPE



ENISA APPROACH TO STANDARDISATION

- **Influence stakeholders**

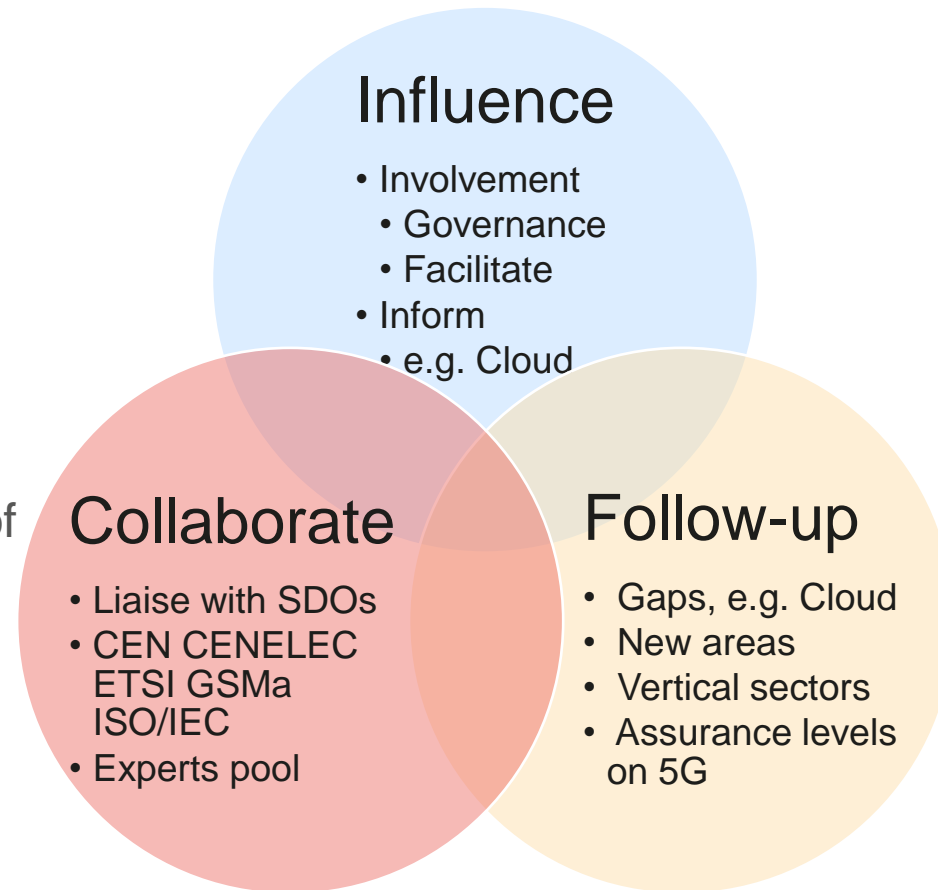
on key policy areas including cybersecurity certification

- **Collaborate with public interest and private stakeholders**

on the use and development of standards

- **Follow up**

On gaps and new content areas e.g. assurance level methodology



ENISA Work Programme:

Task 1: Developing the rapport with ESO/SDO/private initiatives:

Task 2: Analysis of standardisation requirements in support of cybersecurity policy

Task 3: Analysis of standardisation requirements in support of cybersecurity certification



EU CYBERSECURITY ACT – CERTIFICATION FRAMEWORK

- **EUCC: a horizontal ICT products scheme – published, additional documents under development**
 - Common Criteria, ISO/IEC 17065 & 17025
- **EUCS: a generic cloud services scheme – draft finalized at ENISA (commenting period ended)**
 - Defines a baseline of requirements that are applicable to all services and enables the same methodology
- **EU5G: combining product security evaluation and product lifecycle processes evaluation – reprioritized**
- **EUDI (?) – new priority for the EU**



ENISA ACTIONS IN EIDAS

- Proposing and validating with stakeholders guidelines and recommendations for the implementation of trust services;
- Mapping technical and regulatory requirements;
- Promoting the deployment of qualified trust services in Europe;
- Supporting relying parties and end users to secure their electronic transactions using trust services;
- Assessing the suitability of the newly published standards to use within the eIDAS ecosystem.



ENISA ACTIONS IN STANDARDISATION

- **Digital Identities Standards**
 - Update of the inventory of standards/standardisation activities related to digital identities
 - Specific considerations for the EUDI wallet (current state of standardisation activities)
 - Standards for certification of EUDI wallet (and considerations related to certification itself)
 - Standards for implementing acts of eIDASv2 (only trust services)
 - Cryptographic algorithms for EUDI wallet
- **Involvement in „Standardization Strategy for the EUDI Wallet”**
- **Further work on CRA**
- **Involvement in standardisation bodies**
 - ETSI TC CYBER, TC ESI
 - CEN-CENELEC JTC13, JTC21; CEN TC224, TC47X
 - ISO-IEC JTC1 SC27



EU DIGITAL WALLETS

- EC request to ENISA for support for the certification of EUDI Wallets
- ENISA supports the establishment of national schemes of EU Member States by providing harmonized certification requirements
- ENISA supports the EUDI Wallet toolbox process – security requirements
- First batch of implementing acts
 - *„laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the **certification** of European Digital Identity Wallets”*
 - Trust framework, Person Identification Data & Electronic Attestations of Attributes, Intergrity and core functionalities, Protocols and interfaces
- Second batch of implementing acts
 - Relying party registration, Wallet lists, Security breaches, Identity matching, Electronic attestation of attributes



EUDI WALLET CERTIFICATION

- **Functional requirements**

- Interfaces of the EUDI Wallet to relying parties and others
- Specifications to be defined in other epics and/or standards
- Conformity assessment to be based on interoperability test suites associated to standards/specs

- **Cybersecurity**

- Functions of the wallet (authentication)
- Coverage by the requirements

- **Privacy**

- **National schemes**

- The MS schemes will not cover functional certification, and it will arrive too late for the first generation
- The use of national schemes raises specific issues, in particular related to interoperability
- Work will continue in parallel on national and European schemes



DIGITAL WALLET STANDARDS

- **Major gaps in standardisation of EUDI Wallet**
- No standards for the cryptographic device interface (direct interface of the cryptographic component of the mobile device);
- Functional testing requirements missing for elements of the EUDI Wallet except:
 - PID/(Q)EAA mutual authentication protocols,
 - qualified electronic signatures
- No standards fulfilling the EUDI Wallet needs in 100%
- ISO/IEC 23220 series (published in 2023) designed to target the Digital Identity Wallet
- ETSI ESI and CEN TC224 efforts
- Definition of the “What” and not the “How”



REGULATORY SECURITY OBLIGATIONS

- Ex-Art.19
- Proposal of security requirements
- Incident reporting (CIRAS Tool)
- Complementary technical and practical guidance to the national authorities and TSPs

10TH ENISA TRUST SERVICES AND EID FORUM

<https://www.enisa.europa.eu/events/tsf-and-ca-day-2024/trust-services-eid-forum-ca-day-2024>

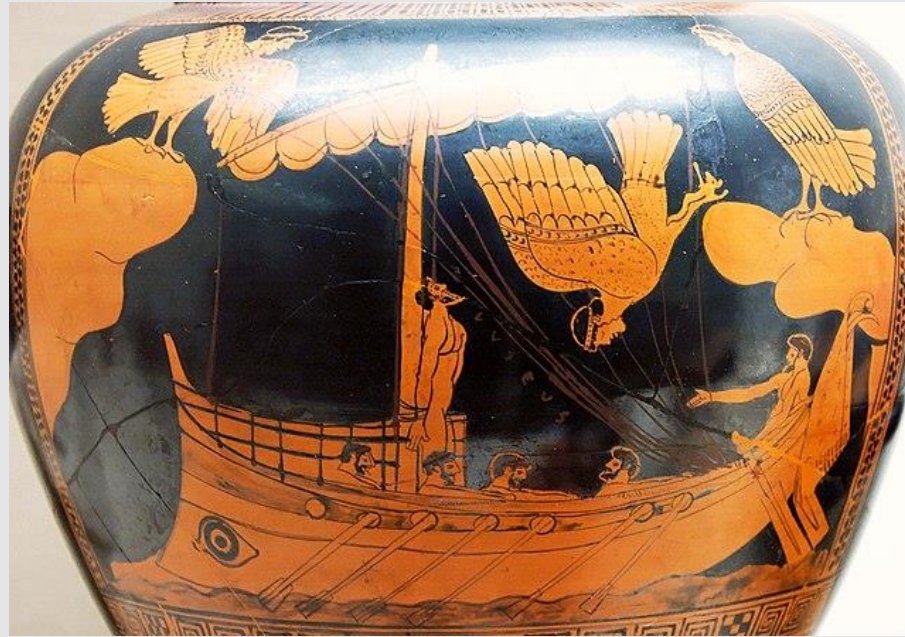


9TH ENISA-ESOS CYBERSECURITY STANDARDISATION CONFERENCE

20TH MARCH 2025 – SAVE THE DATE!



THANK YOU FOR YOUR ATTENTION



Sławomir Górniak

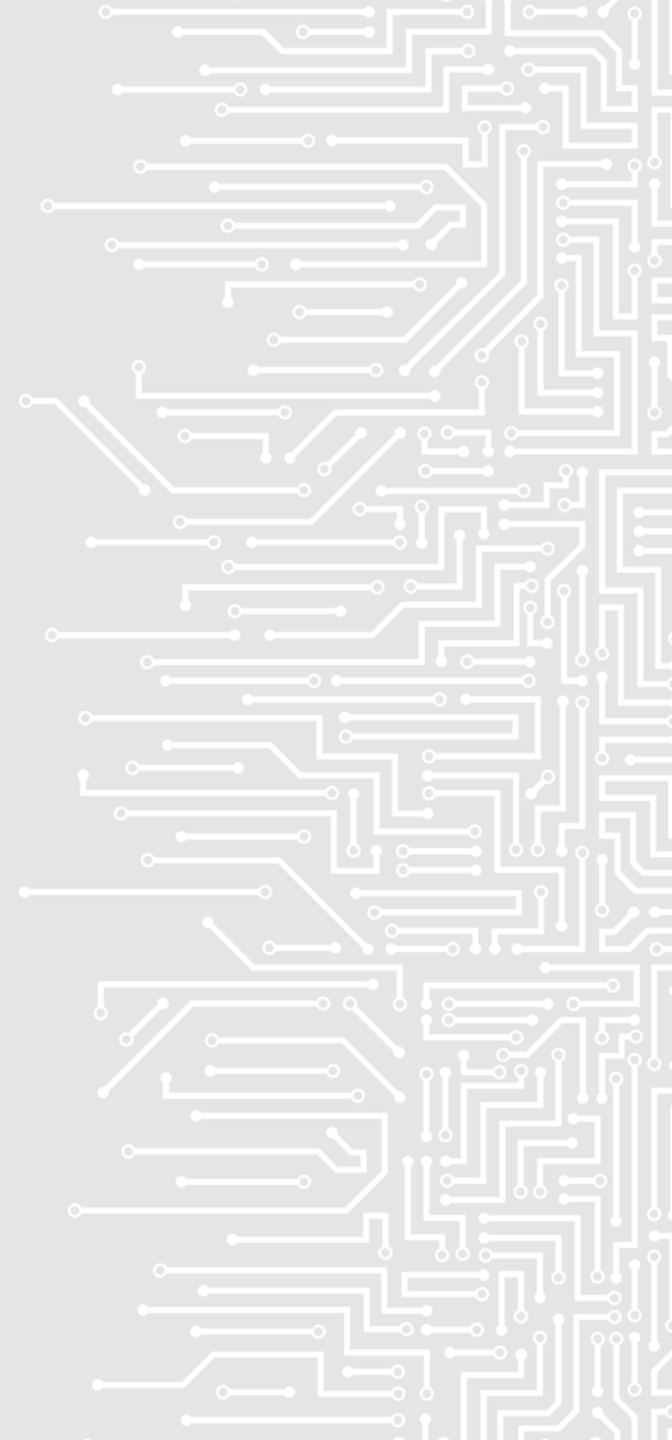
Market, Certification and Standardisation Unit

European Union Agency for Cybersecurity

 +30 697 00 151 63

 slawomir.gorniak@enisa.europa.eu

 www.enisa.europa.eu



PANEL: Pros and cons of possible wallet certification models

eID Wallet Seminar



Moderator:
Pierre-Jean
Verrando
EUROSMART



Slawomir Gorniak
ENISA



Johan Klykens
Centre for Cybersecurity
Belgium



Philippe Proust
Thales



Brussels, Belgium
and Virtual

October 10th, 2024



**Global
Platform™**

eID Wallet Seminar

Panel Discussion:

Pros and cons of different possible certification models for wallets

« La définition légale pourrait avoir au moins pour fonction et justification de dissiper l'équivoque et l'obscurité »

"The legal definition could at least have the function and justification of dispelling ambiguity and obscurity."

« Les définitions dans la loi » in MELANGES JEAN VINCENT, 1981, pp. 77-92, spéc. p. 78 §2.

Council Resolution of 7 May 1985

On a new approach to technical harmonization and standards

To address the length and technical complexity of community texts, EEC legislator decided to develop the so-called “*New Approach*” mandating the drafting of certain technical aspects of the necessary community legislation to European Standardization Organizations (ESOs).

Why the EUDI Wallet certification is necessary ?

3 good reasons

- To comply with the *'European Declaration on Digital Rights and Principles for the Digital Decade'* that underlines everyone's right to access digital technologies, products and services that are safe, secure, and privacy-protective by design;
- As required by Article 5c that lists *cybersecurity and functional requirements* – 5a(4), (5), (8), (14) + *privacy requirements* 5a;
- To facilitate the presumption of conformity with the *CRA essential requirements*. – recital 33.

Different types and means of certification applicable to the EUDI Wallet

Cybersecurity

EU CSA schemes

SOG-IS

National schemes

Privacy

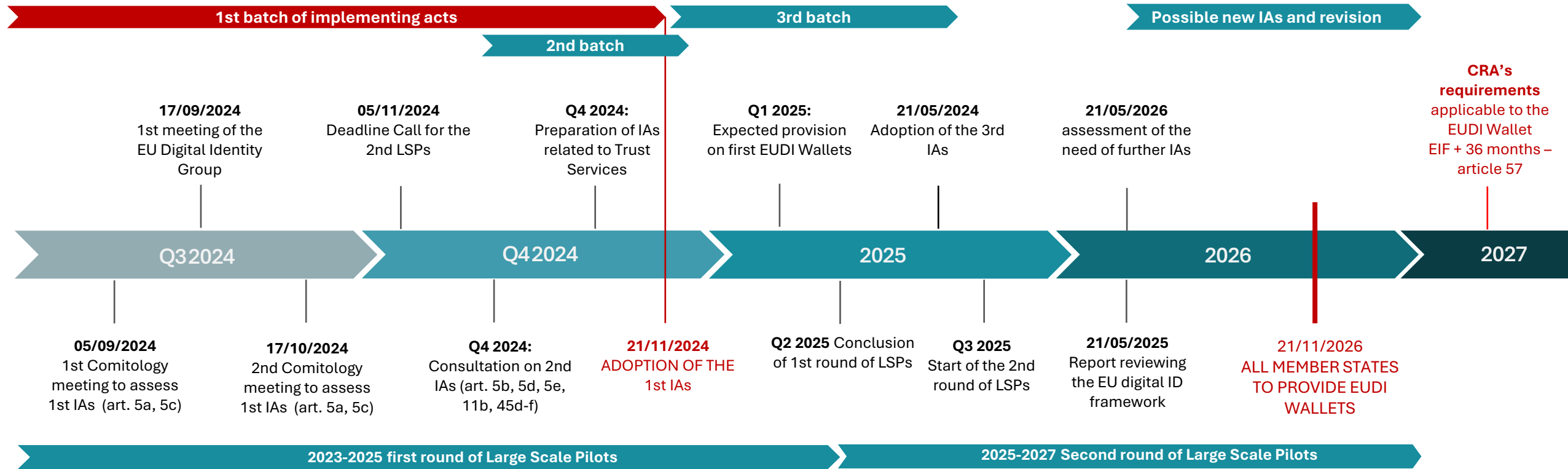
GDPR

Others (non-cyber)

Functional

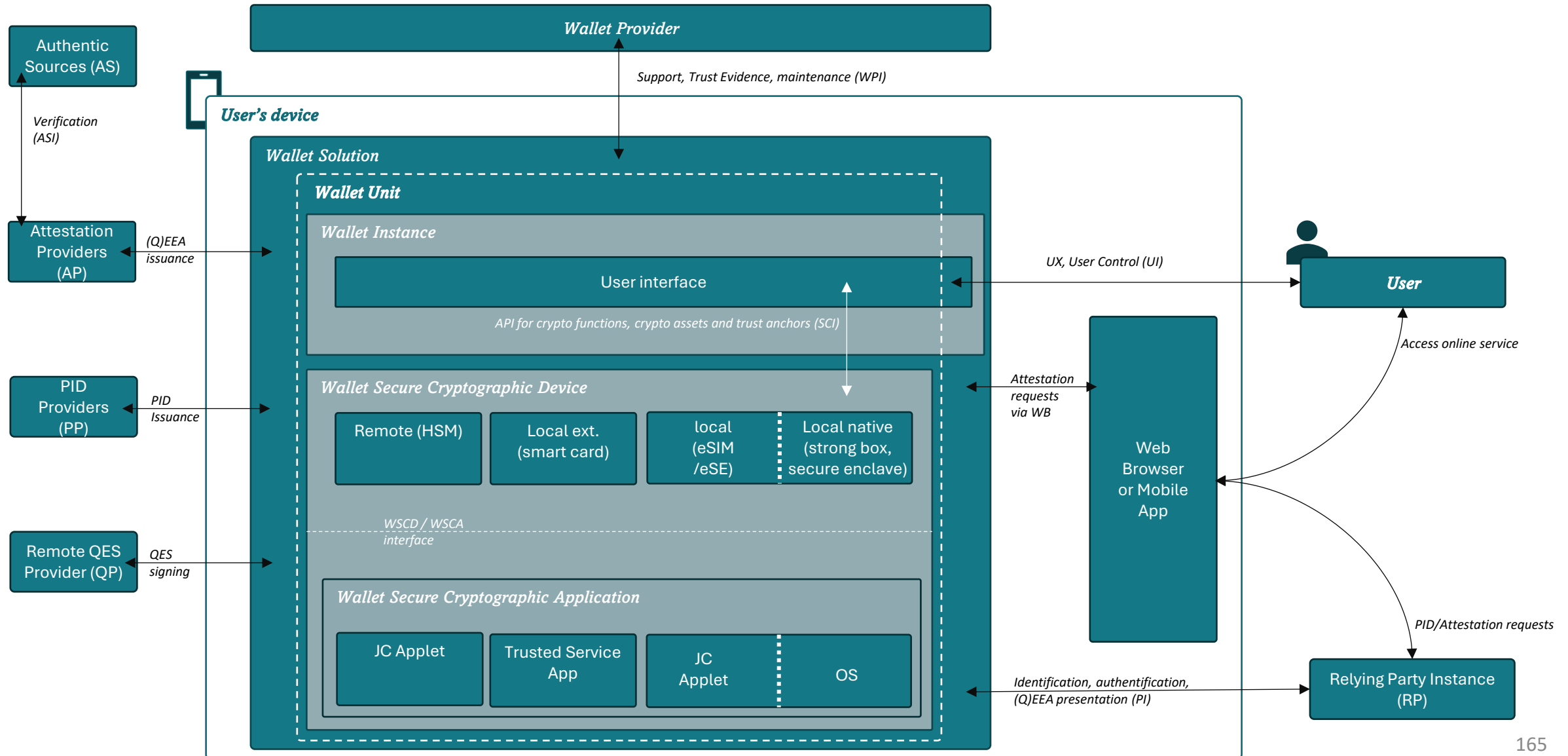
Interoperability

Provisional timeframe



What's the scope for certification?

ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



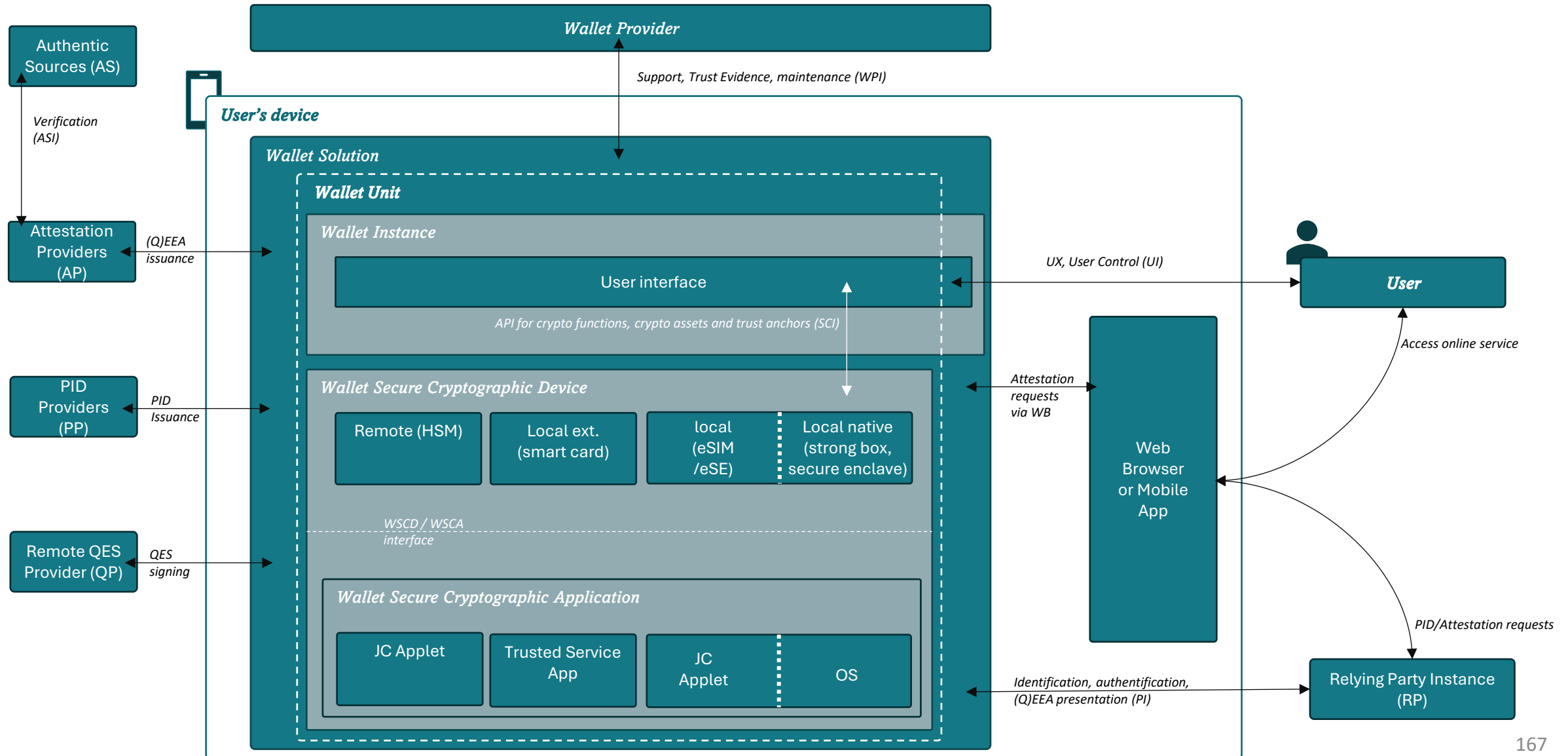
ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



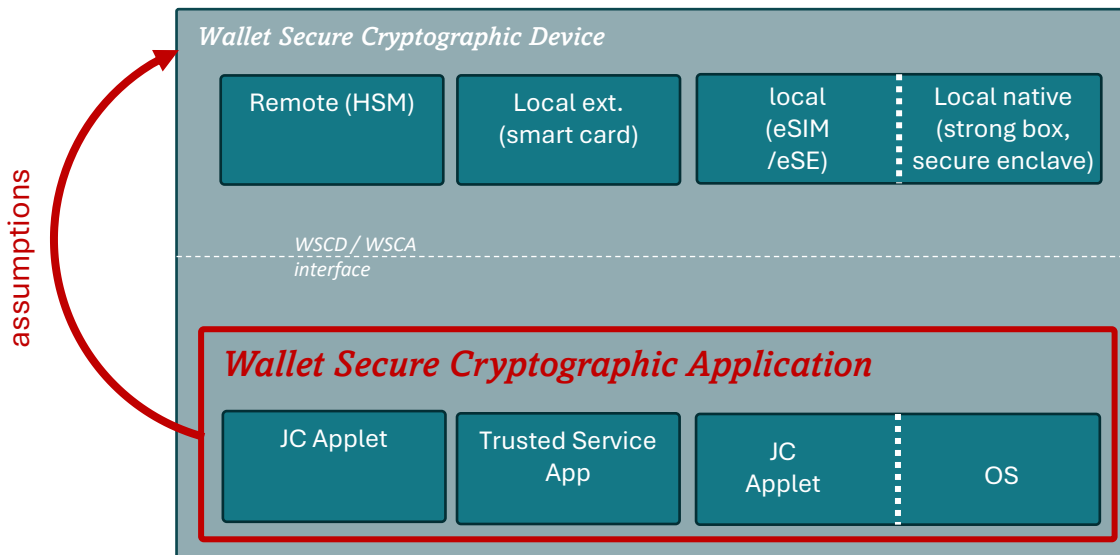
Wallet instance would be a very poor stand-alone candidate:

- doesn't include WSCD / WSCA
- Many variants
- In practice a « wallet front end instance »
- But will receive security update

ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



WSCA as requested by Draft implementing regulation for transitional national certification scheme

Shall formulate assumptions for the **WSCD** evaluation

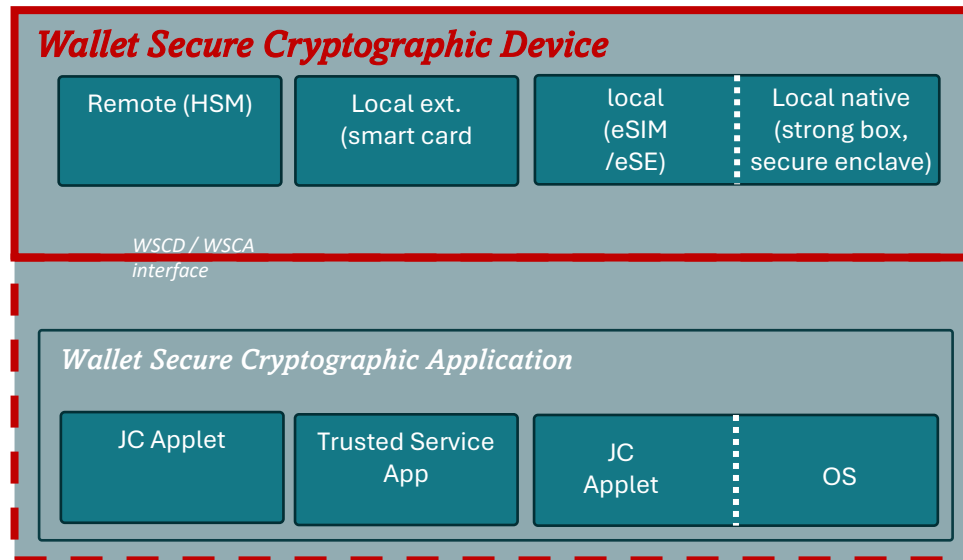
Applicable security certificates at level « high » according to Implementing Regulation (EU) 2015/1502

FITCEM

CSPN

BSZ

ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



WSCD means an environment that hosts the wallet secure cryptographic application and provides cryptographic functions;

If WSCA depends on a particular WSCD - it needs to be evaluated as a composite product ?

Applicable schemes for **WSCD**?

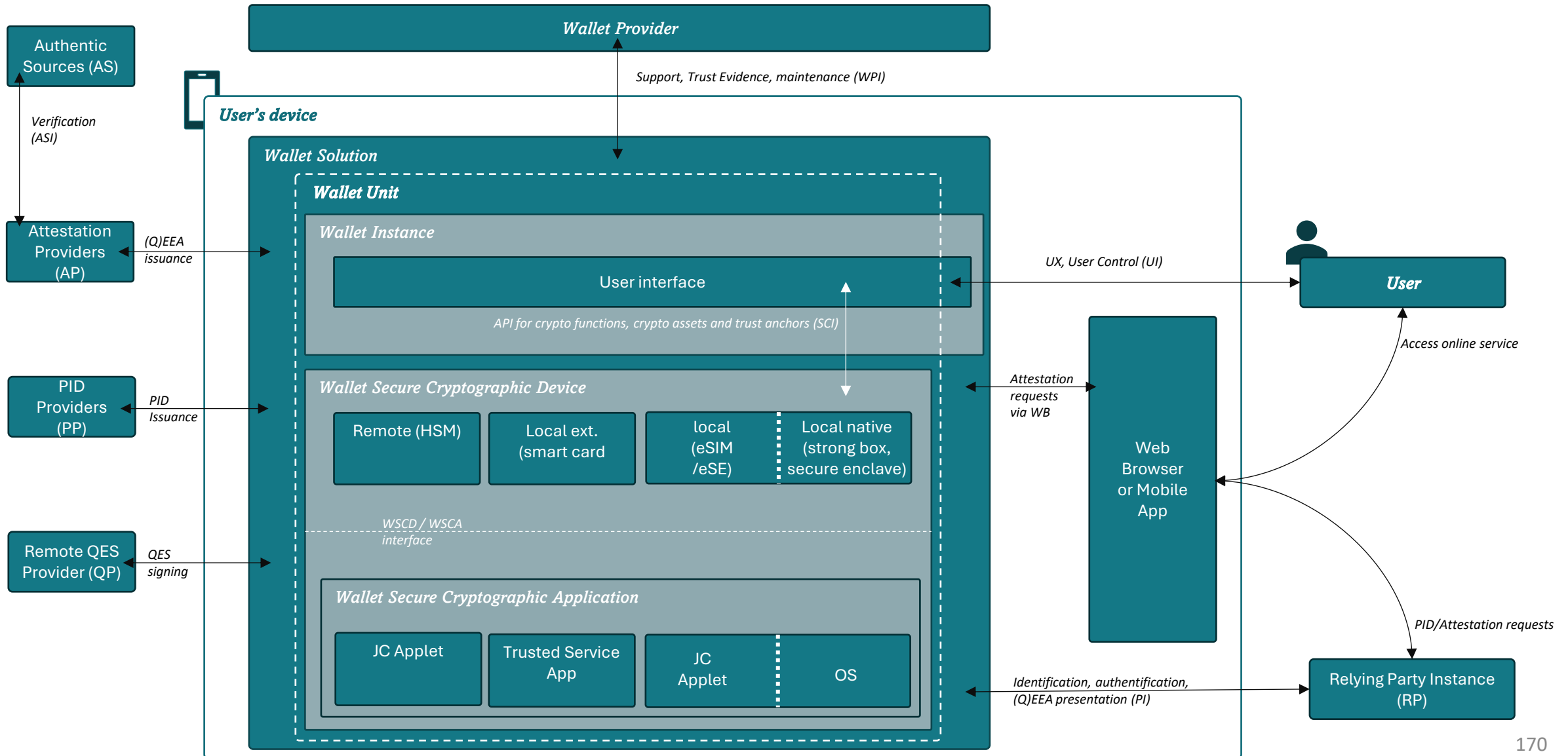
EUCC

SOG-IS

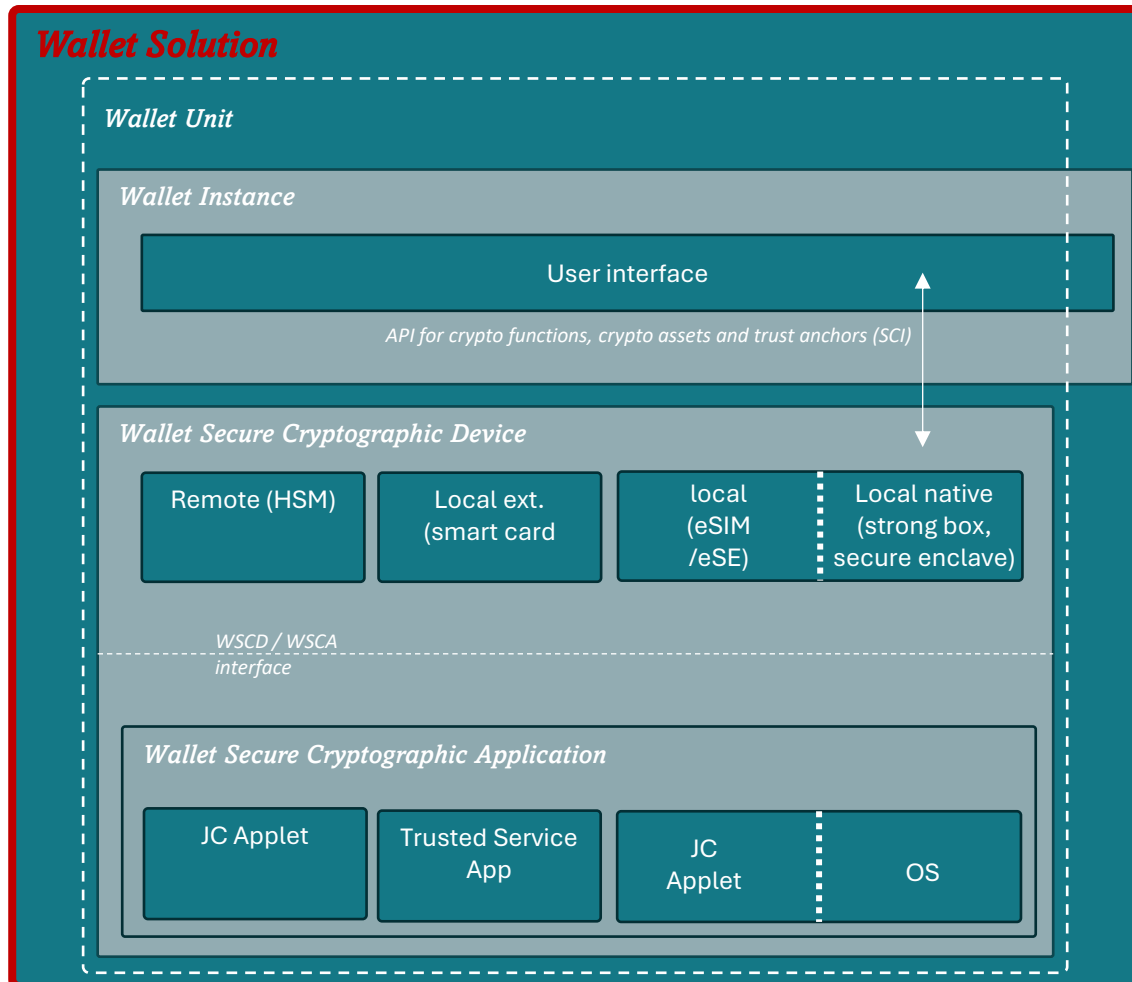
at level EAL4+ AVA_VAN.5

Are already available

ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



ARF's EUDI Wallet architecture vs Draft implementing regulation on certification

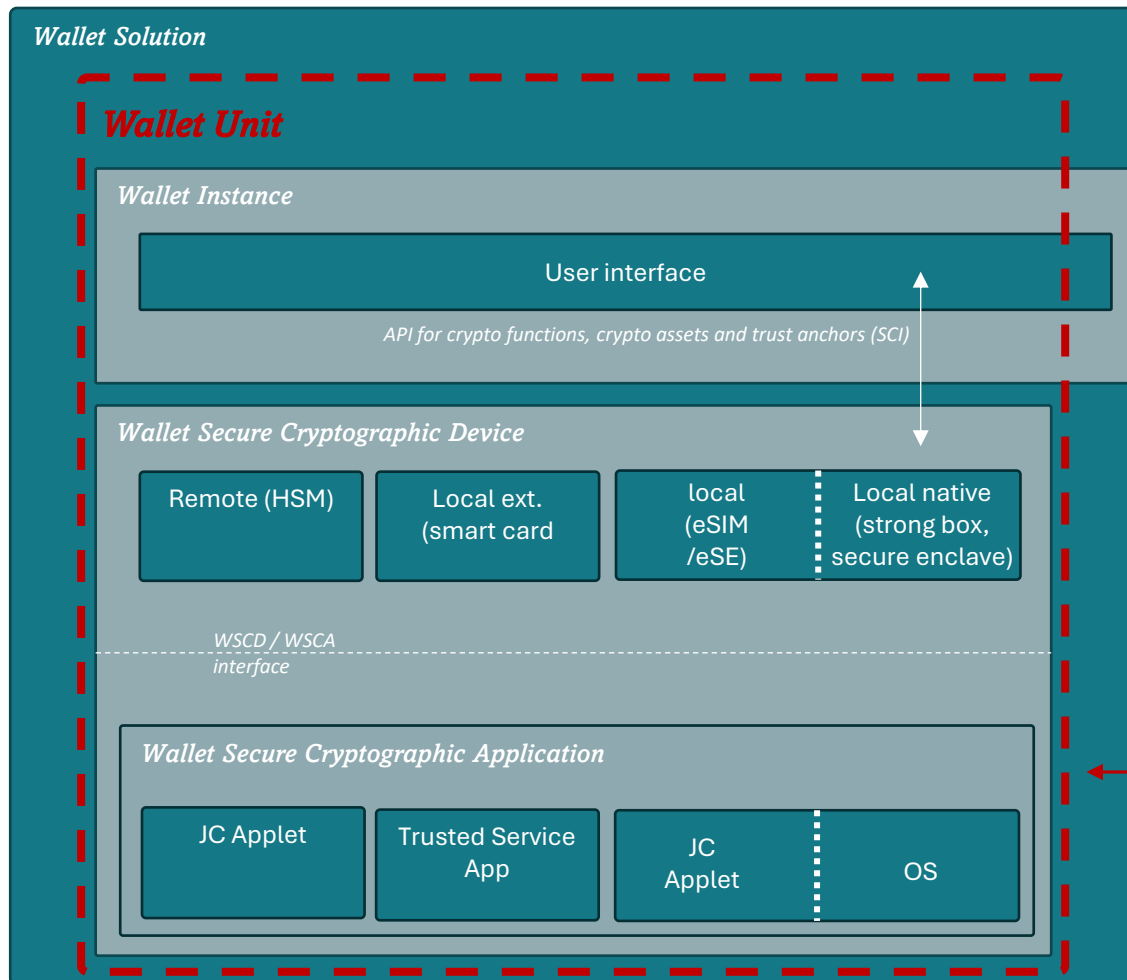


Wallet Solution:

A combination of software, hardware and platform, services, settings, and configurations.

Include the processes for provision and operation (including onboarding).

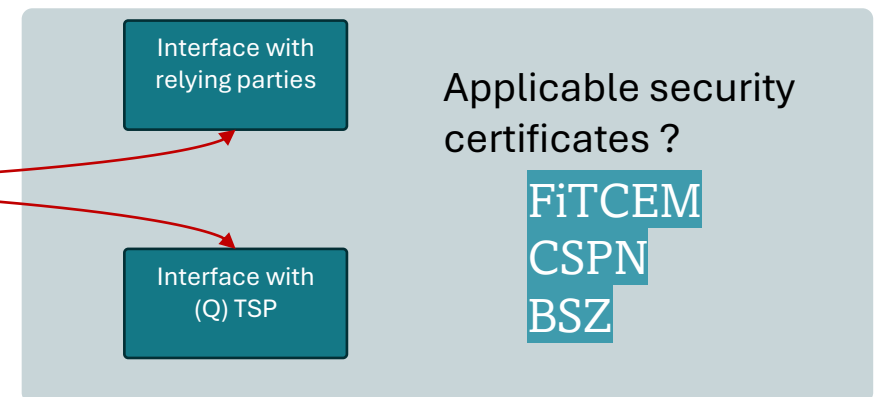
ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



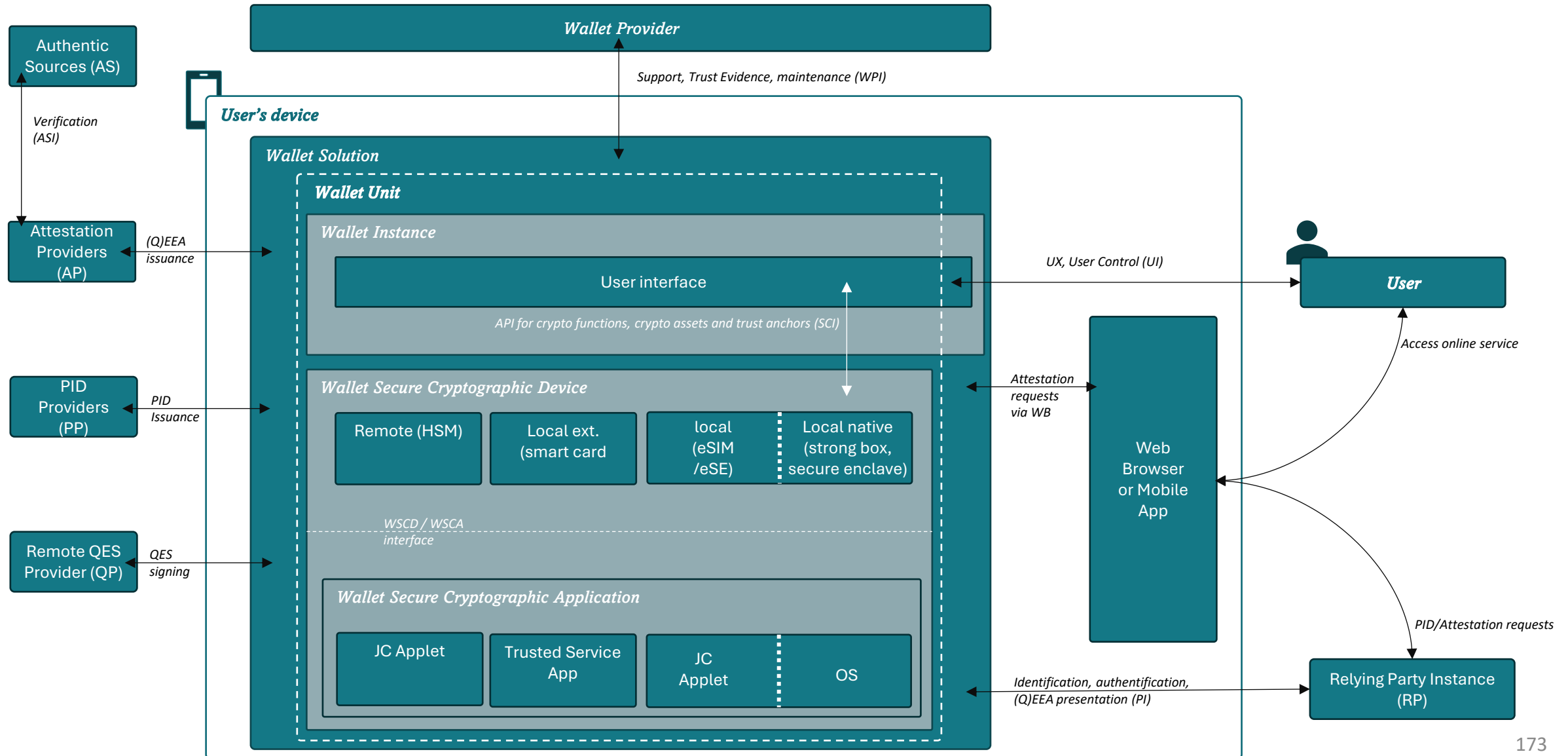
Wallet unit:

a unique configuration of a wallet solution that includes wallet instances, WSCA/D

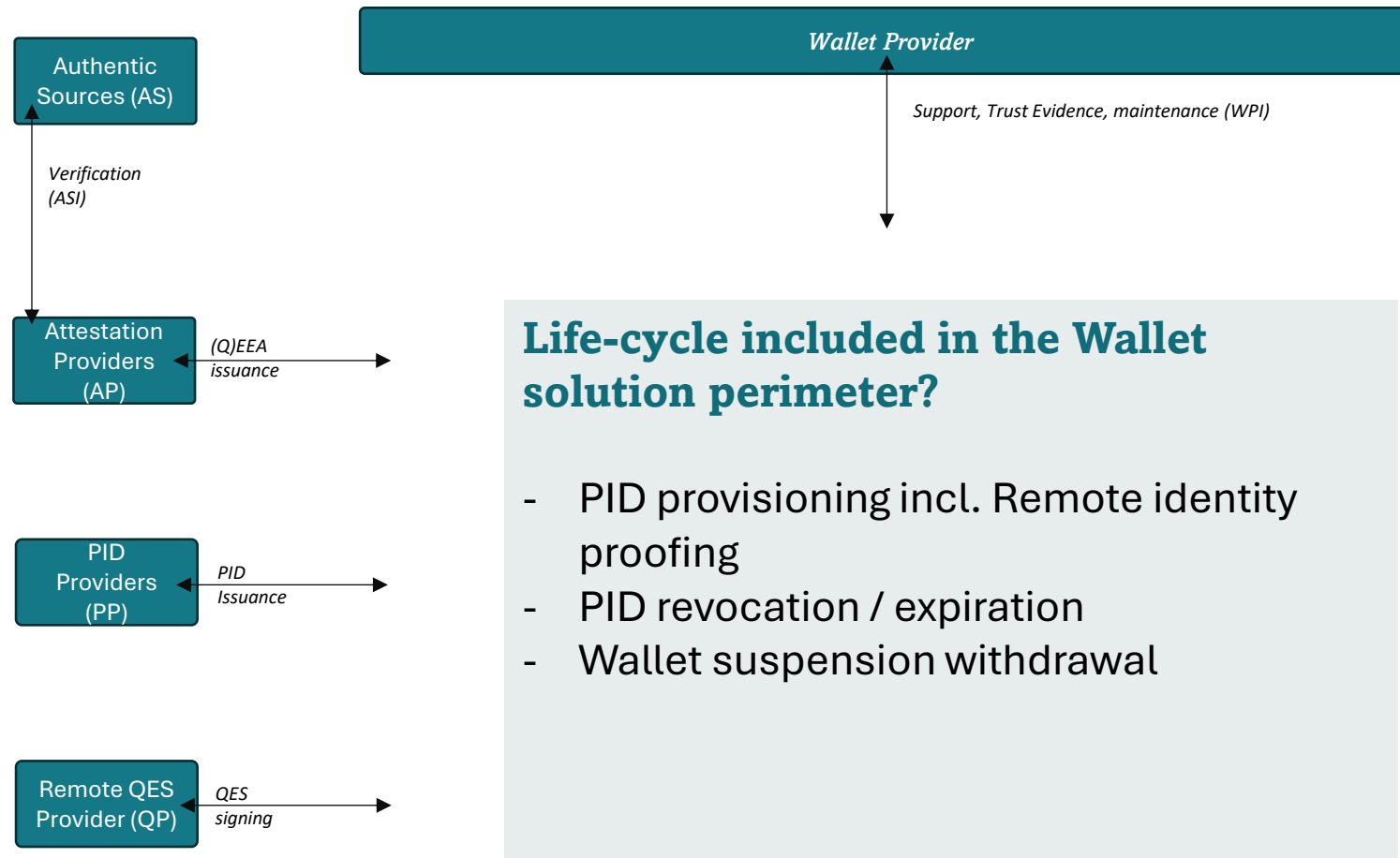
Including Application e.g.:



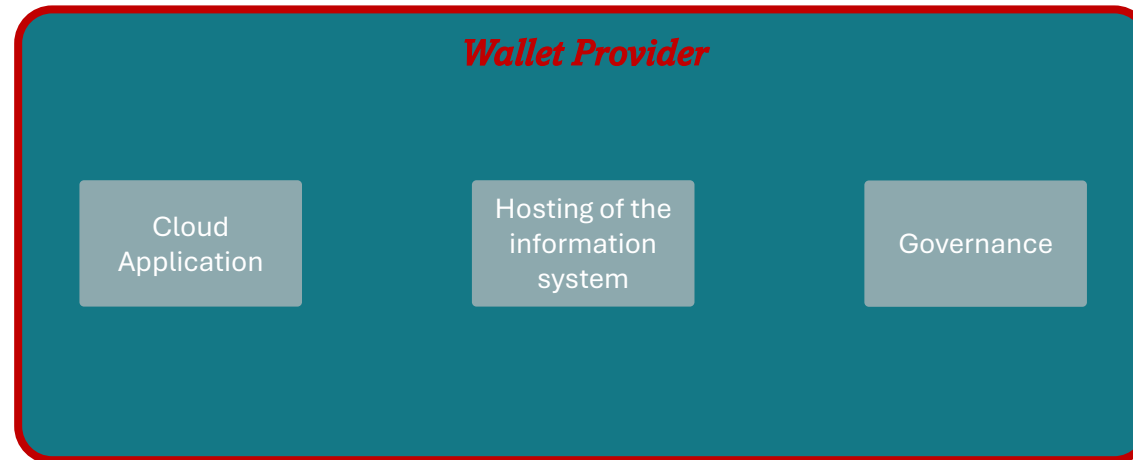
ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



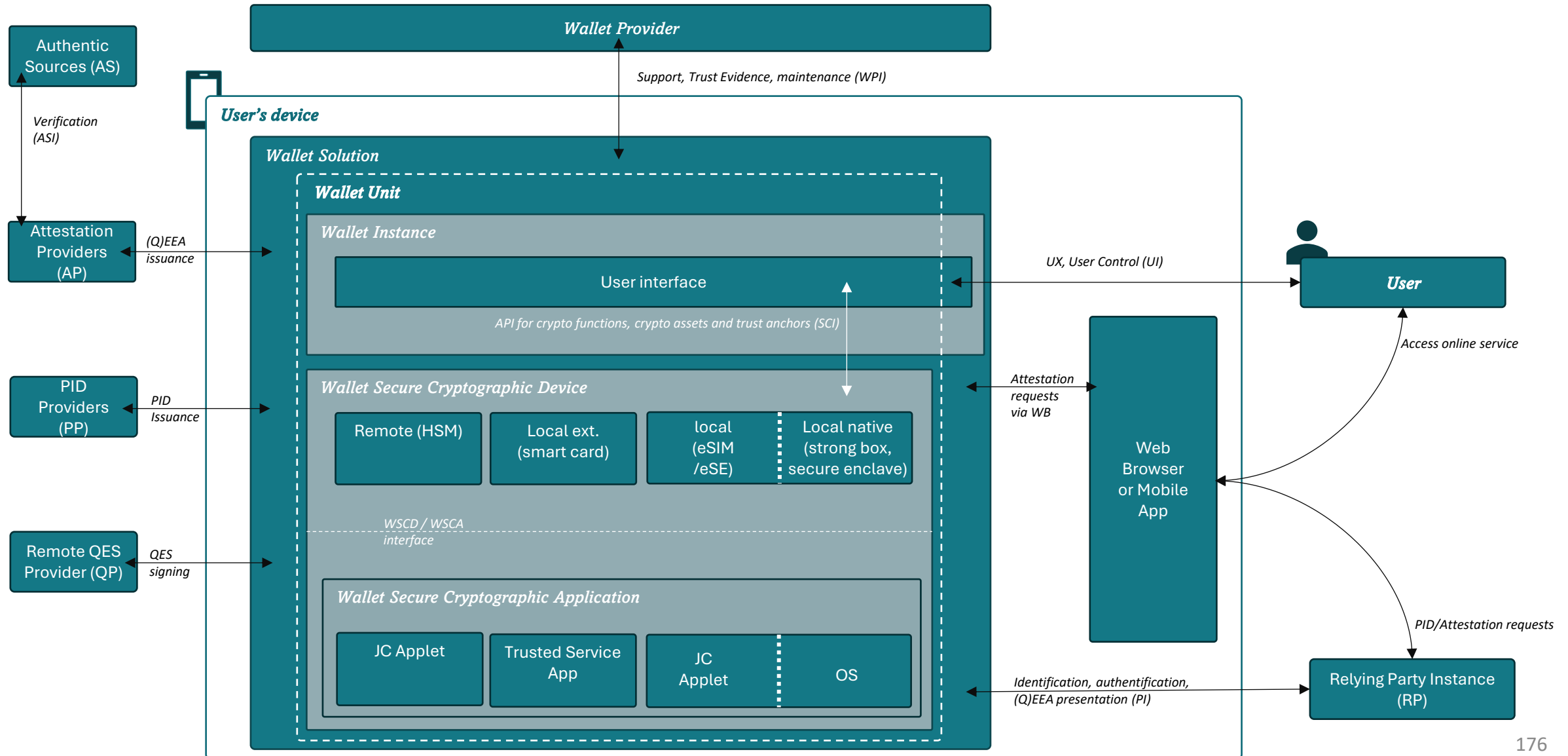
ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



ARF's EUDI Wallet architecture vs Draft implementing regulation on certification



Agenda

10.00 - Welcome and Introduction

Stephanie El Rhomri, Chair of the Board, GlobalPlatform

10.15 – Unlocking the Future of Public Services: The Transformative Power of Digital Identity and Wallets

Vedran Lalic, Independent Consultant

10.40 – GlobalPlatform – From Physical to Digital Identity

Gil Bernabeu, CTO, GlobalPlatform

11.00 – The path toward a secure European digital identity

Jean Daniel Aussel, Head of Standardization, Thales

BREAK: 11.25 – 11.40

11.40 – Germany’s perspective on EUDI deployment

Torsten Lodderstedt, Lead Architect (German EUDI wallet), SPRIN-D

12.00 – France’s perspective on EUDI deployment

Anthony Carmoy, ANTS

12.20 – Challenges and Opportunities in the deployment of EUDI – Member State Wallet Issuers

Moderator: Jean-Daniel Aussel (Thales) **Panelists:** Torsten Lodderstedt (SPRIN-D), Iain Maxwell (FIME), Herbert Leitold (A-SIT), Elyes Lehtihet (ANSSI)

13.05 – Smartphone manufacturer perspective for EUDI deployment

Dawid Wroblewski, Product Manager – Digital Identity, Samsung

LUNCH BREAK: 13.30 – 14.30

14.30 – EUDI large scale pilot learnings (Payments)

Laurent Bailly, Head of Product Strategy, VISA

14.55 – Developing EUDI Wallet Learnings and Opportunities

Yann Bouan, Chief Strategy Officer, iDAKTO

15.20 – Readiness of the Ecosystem to Support EUDI

Moderator: Jean-Baptiste Milan (HID Global) **Panelists:** Laurent Bailly (VISA), Dawid Wroblewski (Samsung), Daniel Goldscheider (Open Wallet Foundation), Yann Bouan (iDAKTO)

BREAK: 16.00 – 16.15

16.15 – EUDI Wallet Certification

Slawomir Gorniak, Senior Cybersecurity Expert, ENISA

16.45 – Pros and Cons of possible wallet certification models

Moderator: Pierre-Jean Verrando (EUROSMART) **Panelists:** Slawomir Gorniak (ENISA), Johan Klykens (Centre for Cybersecurity Belgium), Philippe Proust (Thales)

17.20 – Closing Remarks

Ana Tavares Lattibeaudiere – Executive Director, GlobalPlatform



Closing Remarks

Ana Tavares Lattibeaudiere
Executive Director, GlobalPlatform

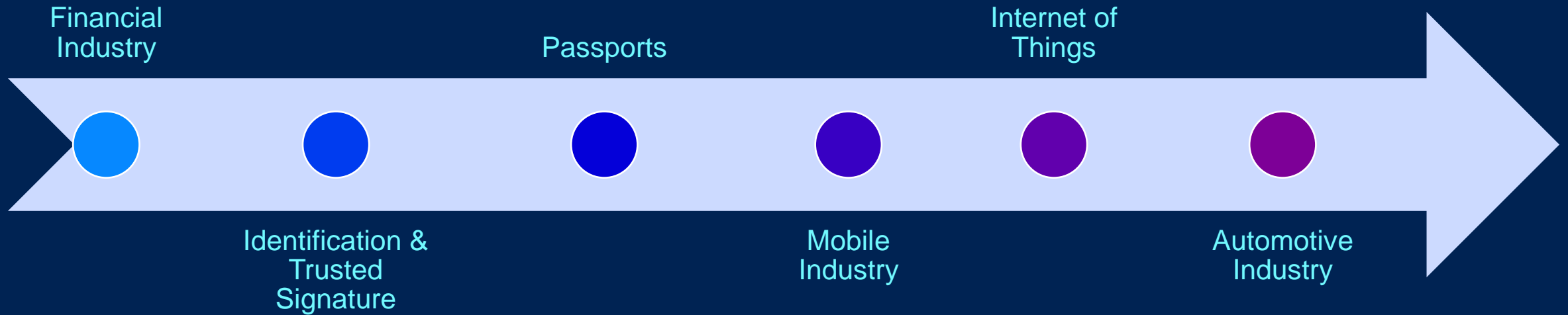
October 10th 2024

**Thank you to all our
speakers and sponsor**

GlobalPlatform

THE standard for managing applications on secure chip technology, with over 25 years of experience

- 70 billion+ Secure Elements shipped worldwide are based on GlobalPlatform specifications
- Over 17 billion GlobalPlatform-compliant Trusted Execution Environment in the market today



Members work together to evolve the standards that secure today and tomorrow's devices and services

FOLLOW US!



Follow on social media and YouTube channel



Subscribe to our newsletter and attend our events



Review our specification when they go to public review



Request GlobalPlatform functional certificates



Join the GlobalPlatform community of experts



Get your teams trained on secure element technologies



Global Platform™

The standard for
secure digital services
and devices

THANK YOU!

Membership

membership@globalplatform.org

PR Contact

pressoffice@globalplatform.org

Questions

secretariat@globalplatform.org

→ globalplatform.org



**THANK YOU FOR
JOINING US TODAY**

eID Wallet Seminar

Thank you to our Platinum Sponsor

THALES



**Brussels, Belgium
and Virtual**

October 10th, 2024