Ad Usque Fidelis
Cabinet Louis Reynaud

Trust Services Forum

Panel - eIDAS2: Certification and Standardisation in EU Digital Identities

Cabinet of expertise covering technologies, standards and European policies within the digital security and the Cyber security

&

CLR Labs
La Ciotat
Technology Evaluation Laboratory (Biometrics and Security)

Oct 27, 2022
ESMT Berlin Schlossplatz 1 10178 Berlin, Germany

Conclusion of my presentation at the last TSF - 2021vs current status at the current TSF-2022

2021	2022
• How to bridge existing standards from various sources?	Waiting for the ARF publication, but strong standardisation "agitations", but still no mandate to the ESO – need the EU legislation first!
• How to define the assets to be protected in the EU ID Wallet and its environment?	Waiting for the ARF publication, but does the issue is understood by the ARF Penholders?
• How to create security functions corresponding to the use case?	Waiting for the ARF publication, but does the issue is understood by the ARF Penholders?
• Do we need a specific security evaluation methodology?	Waiting for the ARF publication but does the issue is understood by the ARF Penholders?
• Do we need a specific Cybersecurity certification scheme ?	Waiting for the ARF publication but the first EU CSA Scheme is nearly available !
• How to guarantee firewalling between the applications aside the EU ID Wallet ?	Waiting for the ARF publication but does the issue is understood by the ARF Penholders?
• How to guarantee that the source of attributes are conform with the European values?	Waiting for the ARF publication but does the issue is understood by the ARF Penholders?

ARF Penholders are the DG Connect assisted by external consultants

EUDI Wallet : Data set

2022

Identification data

- Article 7.d: ‘person identification data’ means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

Identification means

- Depending of the LOA level, cryptographic challenge is mandatory for the high level -> at least some cryptographic keys

Attributes (annex VI)

- 1. Address;
- 2. Age;
- 3. Gender;
- 4. Civil status;
- 5. Family composition;
- 6. Nationality;
- 7. Educational qualifications, titles and licenses;
- 8. Professional qualifications, titles and licenses;
- 9. Public permits and licenses;
- 10. Financial and company data.

Credentials

- Article 3.A.I.42: ‘credential’ means a proof of a person’s abilities, experience, right or permission;

EUDI Wallet Data vs Functions

Functions

(on-line & off-line)

1) Identification means:
- Identification
- Authentication

2) Data storage:
- Attributes + EAA + QEAA
- ~~Credentials~~

Data storage access condition :
Identification data : not defined
Attribute : not defined
Credential : not defined
ARF

Data storage format :
Identification data : not defined
Attribute : not defined
Credential : not defined
ARF

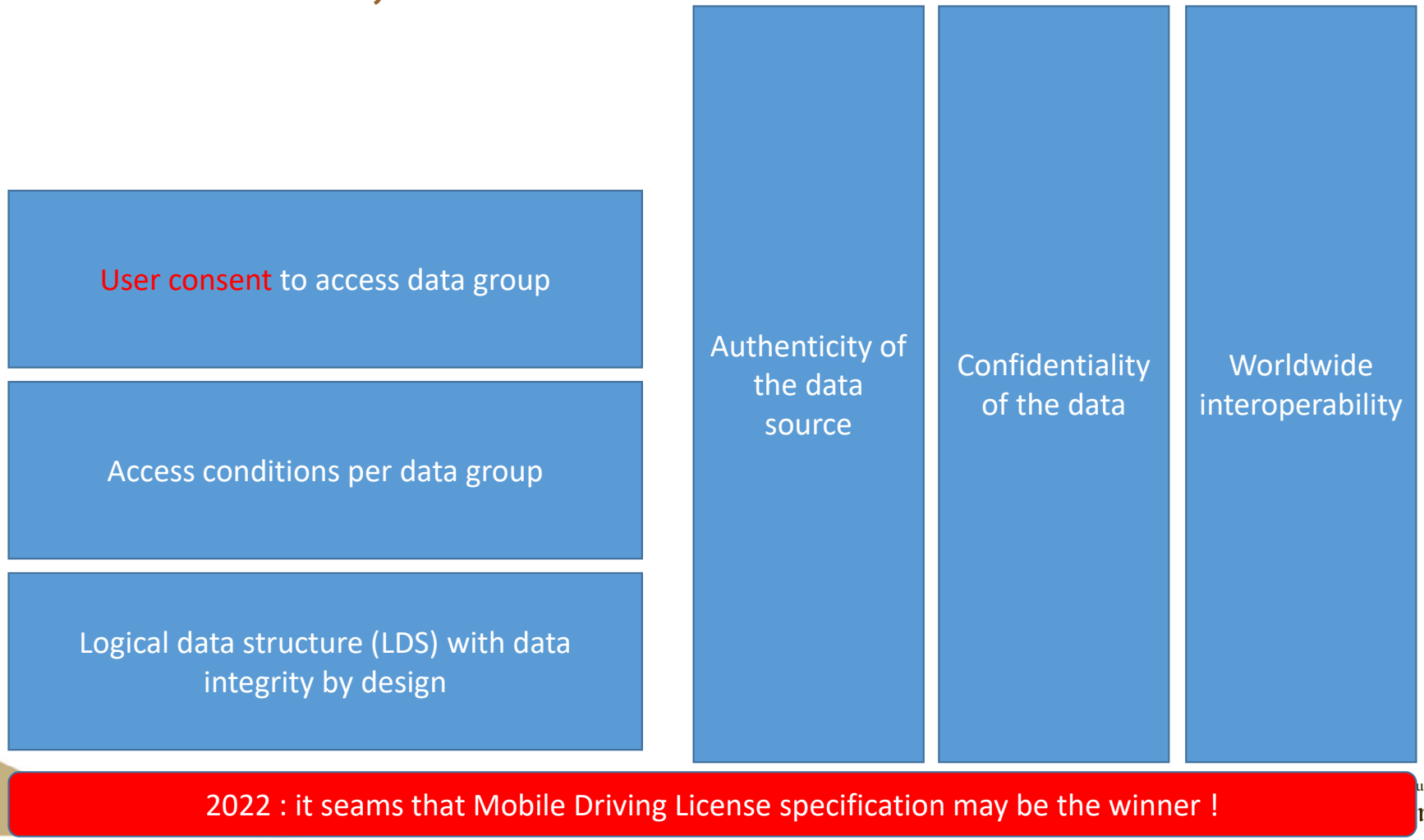
Data format :
Identification data : not defined
Attribute : not defined
Credential : not defined
ARF

Support :
Not defined but can be :
Official documents, USB Key, Mobile Applications, Smart Phones, Software running on PC, Cloud services
ARF

User consent :
Identification data : not defined
Attribute : not defined
~~Credential : not defined~~
ARF

Enrolment process :
not defined
ARF

EUDI Wallet, ICAO as model?



Attributes source?

1. Address; -> **Meta data, geolocation?**
2. Age; -> > **Human analysis or IA ?**
3. Gender; - > **Human analysis or IA ?**
4. Civil status; -> **Human analysis or IA ?**
5. Family composition; -> **Human analysis or IA ?**
6. Nationality; -> **Meta data, geolocation or IA?**
7. Educational qualifications, titles and licenses; **cross check with other pictures ?**
8. Professional qualifications, titles and licenses**; cross check with other pictures ?**
9. Public permits and licenses; -> **cross check with other pictures ?**
10. Financial and company data. -> **Data base crossing?**

Note this picture is free of rights

2022 : How are we sure that we are building a privacy by design EUDI Wallet?

Understand the complexity of what is behind certification(s): art 6 a - 2021

- **Art 6a3 it is corresponding to a mixture of functional, privacy and security requirements on the wallet :**
  - **Security requirement is based on the word : "Securely"**
  - **Privacy requirements are based on the words : "**in a manner that is transparent to and traceable by the user",
  - **Functional requirements are based on the rest of the text**

- **Art 6a4 it is corresponding to a mixture of functional, privacy and security requirements on the interfaces and eID Means of Wallet :**
  - **Security requirement is based on the words : "?"**
  - **Privacy requirements are based on the words : : "(b)** ensure that trust service providers of qualified attestations of attributes cannot receive any information about the use of these attributes**",**
  - **Functional requirements are based on the rest of the text**

- **Art 6a5 it is corresponding to a mixture of functional, privacy and security requirements on the Trust Model of wallet :**
  - **Security requirement is based on the word : "?"**
  - **Privacy requirements are based on the world : : "?",**
  - **Functional requirements are based on the rest of the text**

Functional		Privacy		Security	
Functional Requirements	**Functional testing Requirements**	**Privacy Requirements**	**Privacy testing Requirements**	**Security Requirements**	**Security testing Requirements**
• **ARF**	• **?**	• **ARF**	• **?**	• **ARF**	• **?**

Conclusion - 2022

- Does someone in the EU is understanding the complete impact on the choices taken today on the next 20 years on our digital society?
- Where are the risk analysis on :
  - the EU Citizen ?
  - the EU Member States ?
  - The EU Fundamental rights ?
  - The EU GDPR compliancy?
- Where is the ICT security risk analysis?

- How are we sure that we are really building a privacy by design EUDI Wallet?
- How are we sure we are really building a security by design EUDI Wallet?
- How are we sure we are really preparing the EU Industry to compete against the Gatekeepers?
- How are we sure that the public debate is taken place on the impact of the mandatory EUDI Wallet?

A bit of British Humor for the end!

Under the full control of the user

Under the full control of the user if the Smart Phone manufacturer and if the OS and if the Gatekeepers and if the application stores are considered as trusted environments....

"Being in a minority, even in a minority of one, did not make you mad. There was truth and there was untruth, and if you clung to the truth even against the whole world, you were not mad."
— George Orwell, 1984

"Chi va piano va sano e va lontano."
— Italian proverb

EU Standards

EU Certifications


Thanks for your attention!
stefane.mouille@cabinet-louis-reynaud.fr