eIDAS2.0とEUIDWにみるトラストの検討

2023/11/14@JNSA 電子署名WG/JT2A

株式会社コスモス・コーポレイション

副社長 濱口 総志

Trust of the Products and Services

First of All – "Trust" and Framework

- Technology
  - PKI, VC, DID, DLT
- Assessment
  - TTP、Self-declaration
- Standardization
  - ETSI, CEN, ISO, W3C, IETF, JIS,
- Legislation
  - Legal Certainty

eIDAS, a Framework for Trust services and eID

eIDAS regulation

- *Recitle (1) of eIDAS*

Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.
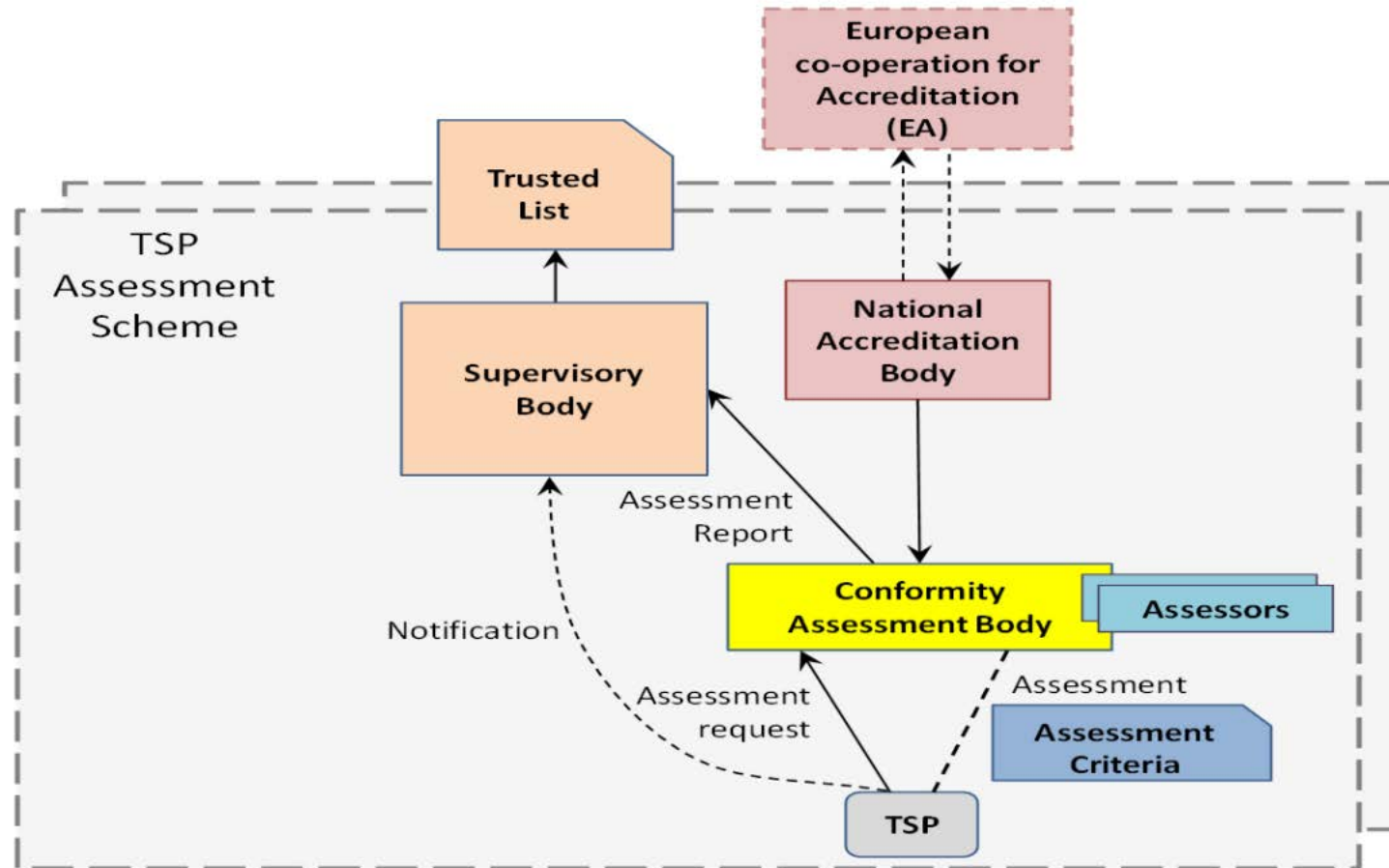
（和訳）

オンライン環境における信頼の構築は経済と社会の発展の鍵である。信頼の欠如、特に法的安定性の欠如が消費者、企業、公的機関に電子取引や新たなサービスの採用を躊躇させている。
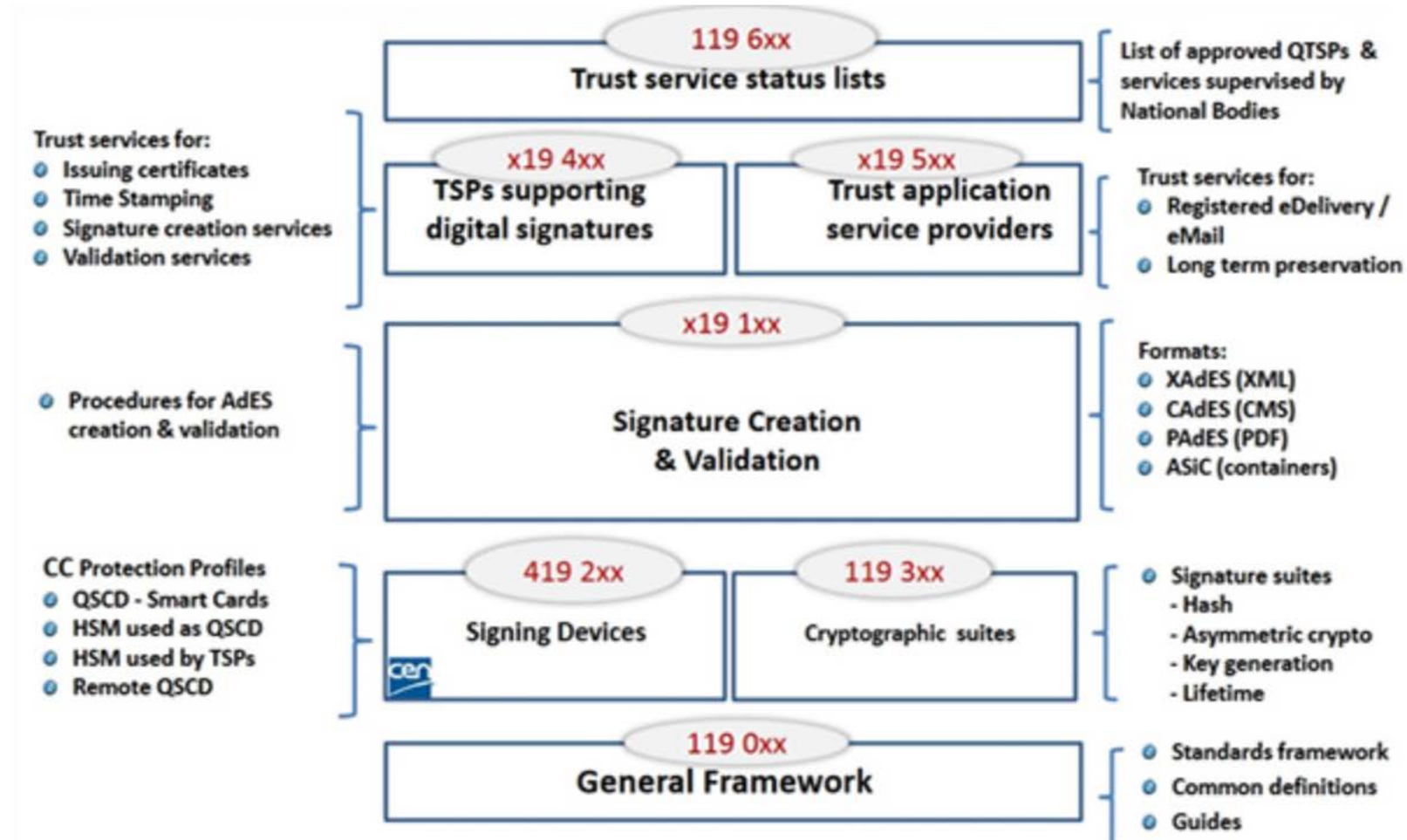
eSignature Directive - eIDAS

	eSignature Directive	eIDAS regulation
Scope	electronic Signature	Trust Services (eSig, eSeal, Timestamp, QWAC, eDelivery, Validation, Preservation) + eID
Defines	Simple, Advanced and Qualified	+ Uniform legal requirements and legal value for Trust services. + Three eID assurance levels and notification scheme.

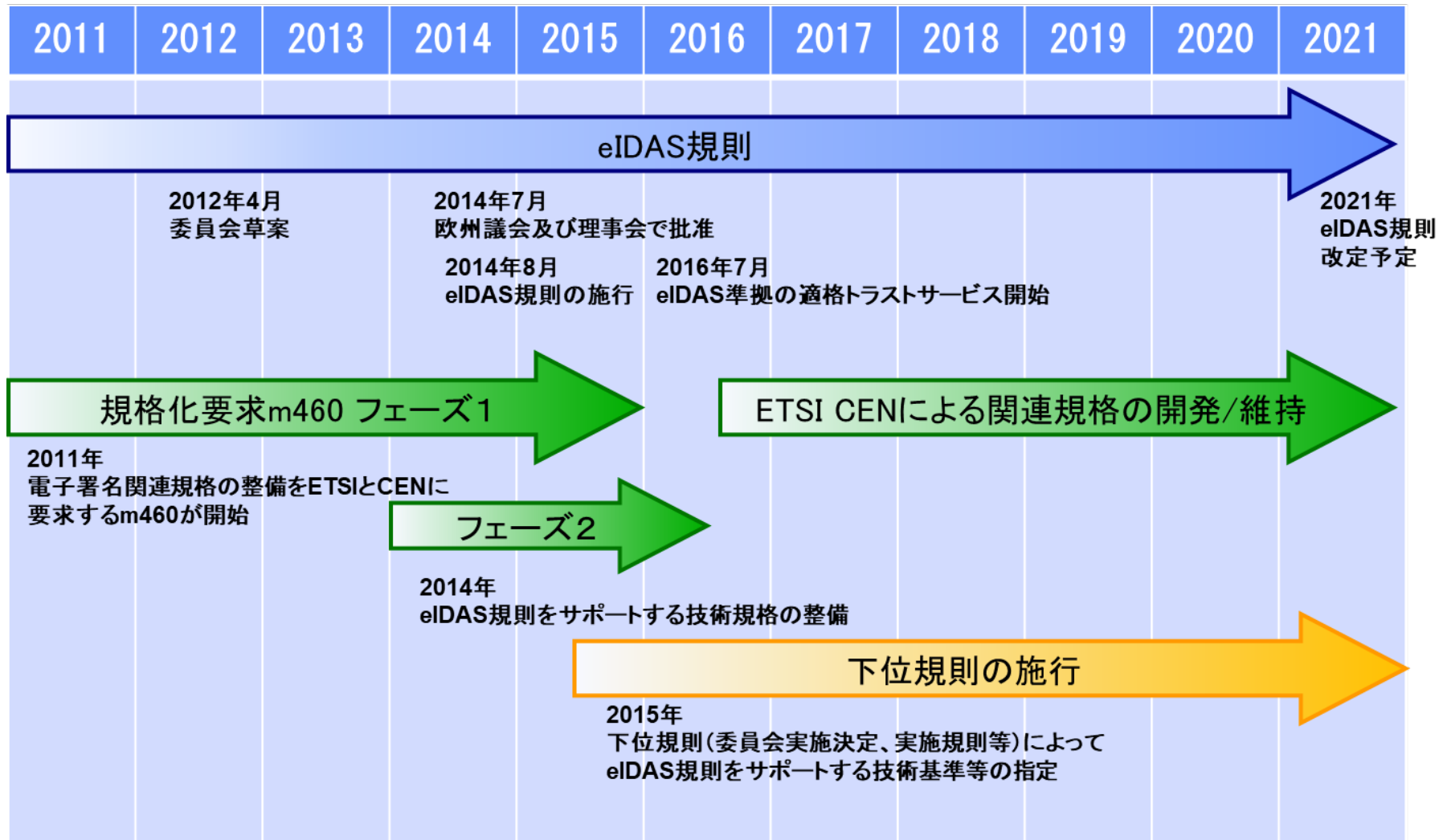# eIDAS Assessment framework

Source: ETSI(https://www.etsi.org/)

Standardization for eIDAS

Trust service status lists — 119 6xx
List of approved QTSPs & services supervised by National Bodies

Trust services for:
- Issuing certificates
- Time Stamping
- Signature creation services
- Validation services

TSPs supporting digital signatures — x19 4xx

Trust application service providers — x19 5xx

Trust services for:
- Registered eDelivery / eMail
- Long term preservation

Signature Creation & Validation — x19 1xx

Procedures for AdES creation & validation

Formats:
- XAdES (XML)
- CAdES (CMS)
- PAdES (PDF)
- ASiC (containers)

CC Protection Profiles
- QSCD - Smart Cards
- HSM used as QSCD
- HSM used by TSPs
- Remote QSCD

Signing Devices — 419 2xx

Cryptographic suites — 119 3xx

- Signature suites
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime

General Framework — 119 0xx

- Standards framework
- Common definitions
- Guides

Source: ETSI(https://www.etsi.org/)

Standardization for eIDAS

| 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |

From eIDAS to eIDAS2.0

eIDAS - eIDAS2.0

	eIDAS regulation	eIDAS 2.0
Scope	Trust Services (eSig, eSeal, Timestamp, QWAC, eDelivery, Validation, Preservation) + eID	Trust Services (+eLedger, eArchive, eAA, management of rQSCD) + eID and DIW
Defines	+ Uniform legal requirements and legal value for Trust services. + Three eID assurance levels and notification scheme.	+ Uniform Technical requirements. + Introduction of DIW. + requirements to Platform(Browsers and Mobile phone)

Perspective 1:Trust services in eIDAS and eIDAS2.0

New Trust Services

- Electronic Attestation of Attribute

- Electronic Archive

- Electronic Ledger

- Management of rQSCD

Is eIDAS successful?

Do we need legislation for these trust services too?

Perspective 2：EU and Platform

	Digital Service Act	Digital Market Act
Objective	To enable competition by making it easier for new platforms to enter the market	To enable transparency, user safety, and platform accountability

eIDAS2.0 and Platform

- Trust Anchor
  - QWAC, Root Store, Trusted List, VDR
- Identity Wallet
  - SE, TEE and Platform

Does it matter?

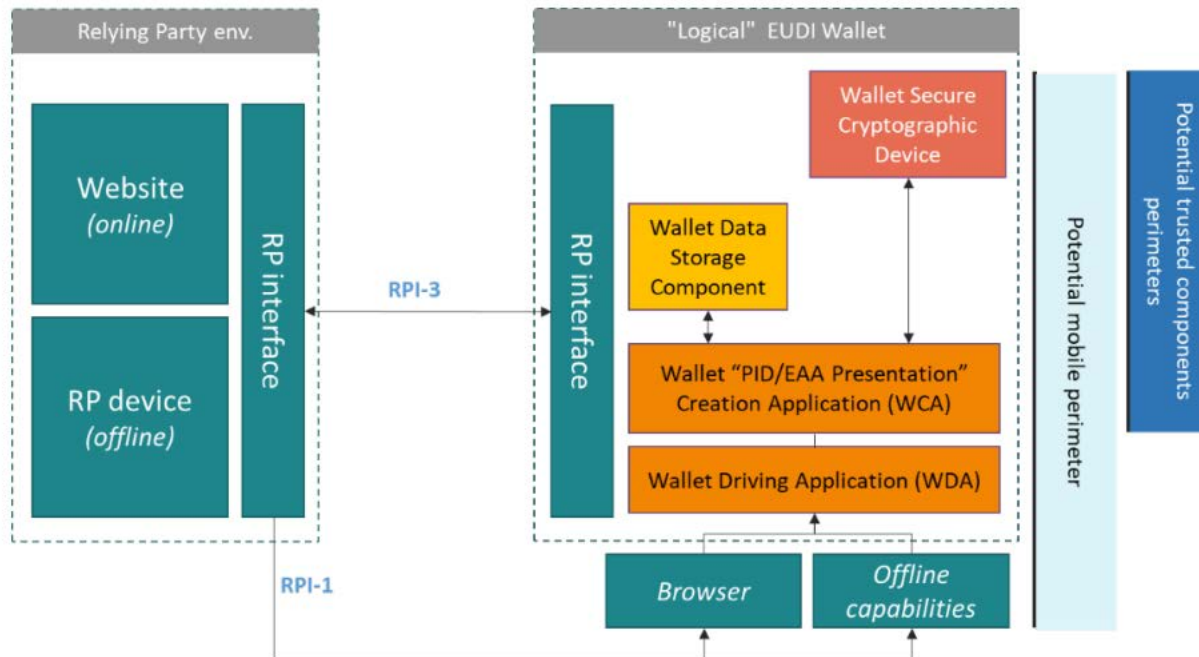- **[The Japan Times: Apple CEO Tim Cook conveyed concern over App Store curbs in meet with Kishida](#)**
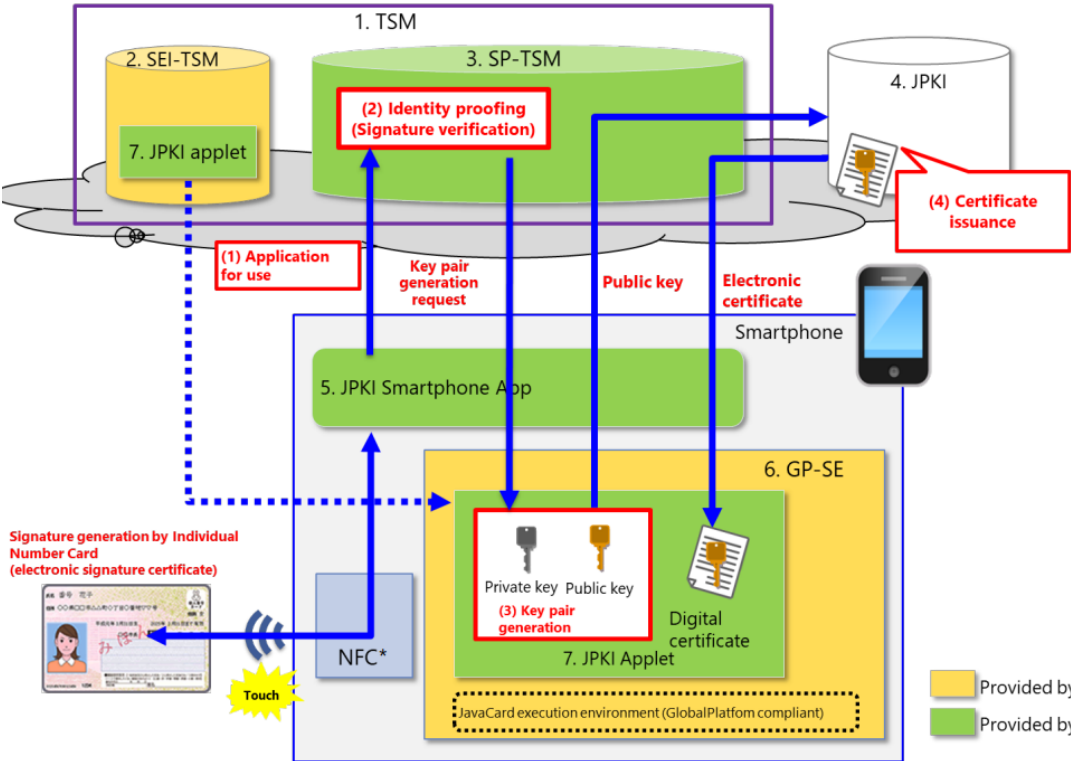
* Type B is used.

Source from MIC(https://www.soumu.go.jp/)

Source from X(https://twitter.com)

EUDIW?

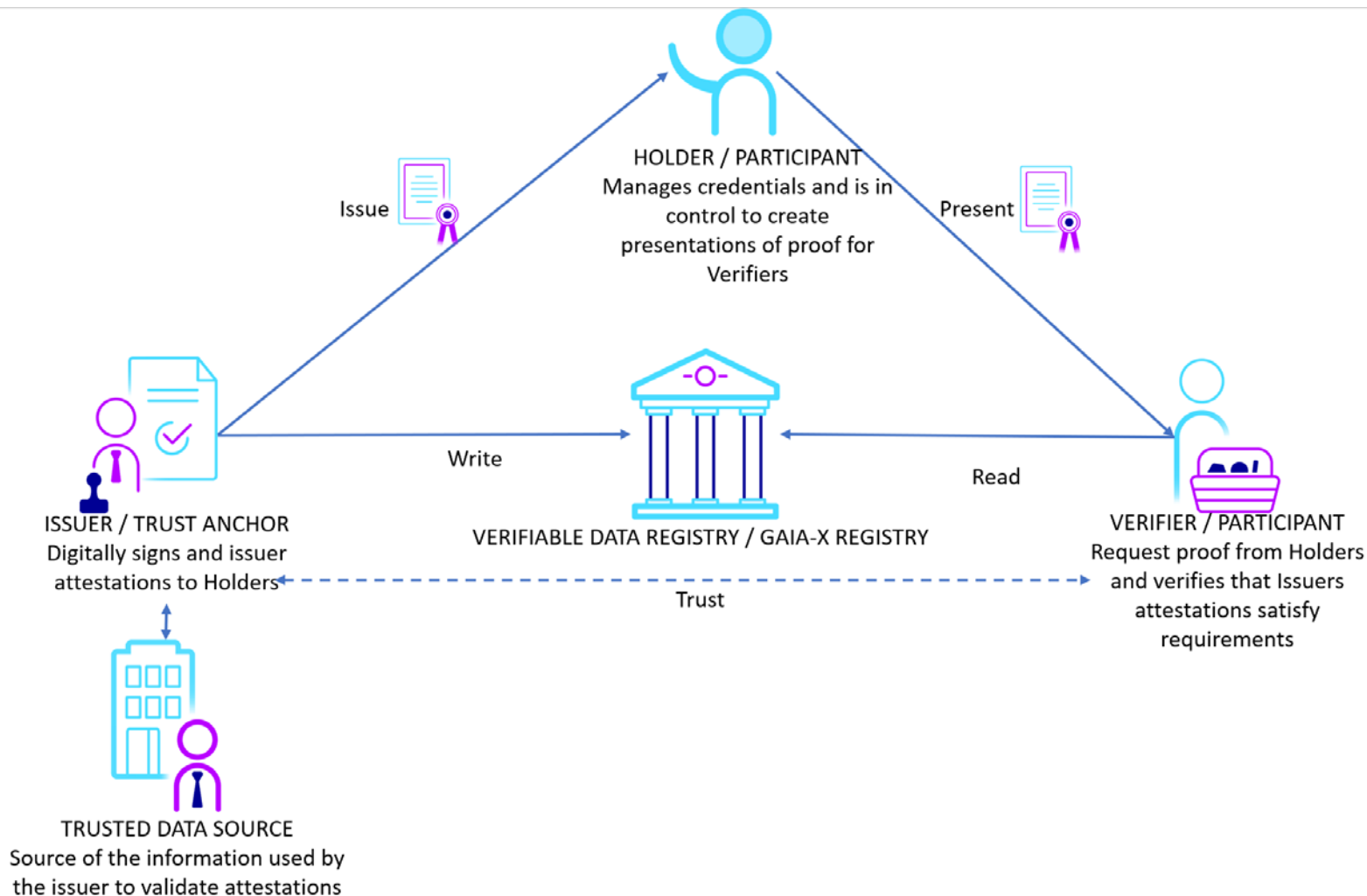

Cryptographic keys management system

Embedded Secure Element or Trusted Execution Environment

reliance on an external device (Secure Elements / Smart Cards), and

a backend (remote Hardware Security Module).

Source: ARF (https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/)

Perspective 3: VC and eIDAS

Name	Defined as
State	The Trust Service Providers (TSP) must be a state validated identity issuers or EV SSL issuers. - For participant, if the legalAddress.country is in EEA, valid state identity issuers are **eIDAS** ones. - **Gaia-X** Association may also be a valid TSP for Gaia-X Association members.
eIDAS	Issuers of Qualified Certificate for Electronic Signature as defined in eIDAS Regulation (EU) No 910/2014 (homepage: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home) (machine: https://ec.europa.eu/tools/lotl/eu-lotl.xml)
EV SSL	Extended Validation (EV) Secure Sockets Layer (SSL) certificate issuers are considered to be temporarily valid Trust Service Providers. (homepage: https://wiki.mozilla.org/CA/Included_Certificates) (machine: https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReportPEMCSV)
registration NumberIssuer	During the pilot phase, the Gaia-X Association nominated itself as a valid Trust Anchor under https://notary.gaia-x.eu

Sessions of the day

- Mr. Olivier Delos (S)
  - Expert & Consultant for Trust services, Mutual recognition
  - Legal aspect
- Mr. Nick Pope
  - Vice chair of ETSI ESI
  - Standardization
- Mr. Joerg Lenz
  - Head of Marketing of Namirial (QTSP)
  - Market view as QTSP
- Mr. Boris Goranov
  - CEO of Ubiqu (Solution provider of DIW and QSCD)
  - Secure implementation of DIW