

Solid Symposium Presentation:

Enhancing Access Control in EUDI Wallets with Solid Principles to Prevent Fraud







Jan Lindquist (Swedish Institute for Standards, StandICT fellow)

Harshvardhan J. Pandit (ADAPT Centre, Dublin City University, Ireland)



StandICT.eu

SOLID Principles alignment with EUDI Wallet

Solid Principle	EUDI Wallet Alignment
 Data Ownership & Control	EUDI Wallet aims to empower users to control access to their identity and credentials. Data is held in the wallet and shared only with informed consent .
 Fine-Grained Access Control	EUDI Wallet supports selective disclosure (e.g., Zero Knowledge Proofs), and WACE extends this with issuer/conduct-based policies and risk analysis .
 Interoperability via Linked Data	While EUDI Wallets don't (yet) require RDF/Linked Data, the idea of semantic, interoperable credentials aligns closely. Standardization (e.g. VC Data Model) helps.
 Separation of Data & Applications	EUDI Wallet separates data storage (in the wallet) from apps (Relying Parties). Wallet mediates access; RPs don't retain control. Similar to how Solid Apps work with Pods.
 Open Standards & Protocols	EUDI Wallet development is tied to open standards (e.g., W3C Verifiable Credentials, CEN, ETSI, eIDAS ARF). Similar ethos to Solid's W3C-based ecosystem.
 Decentralization	EUDI Wallet supports self-sovereign identity (SSI) models, especially where wallet users manage credentials from various issuers. WACE supports distributed trust validation .

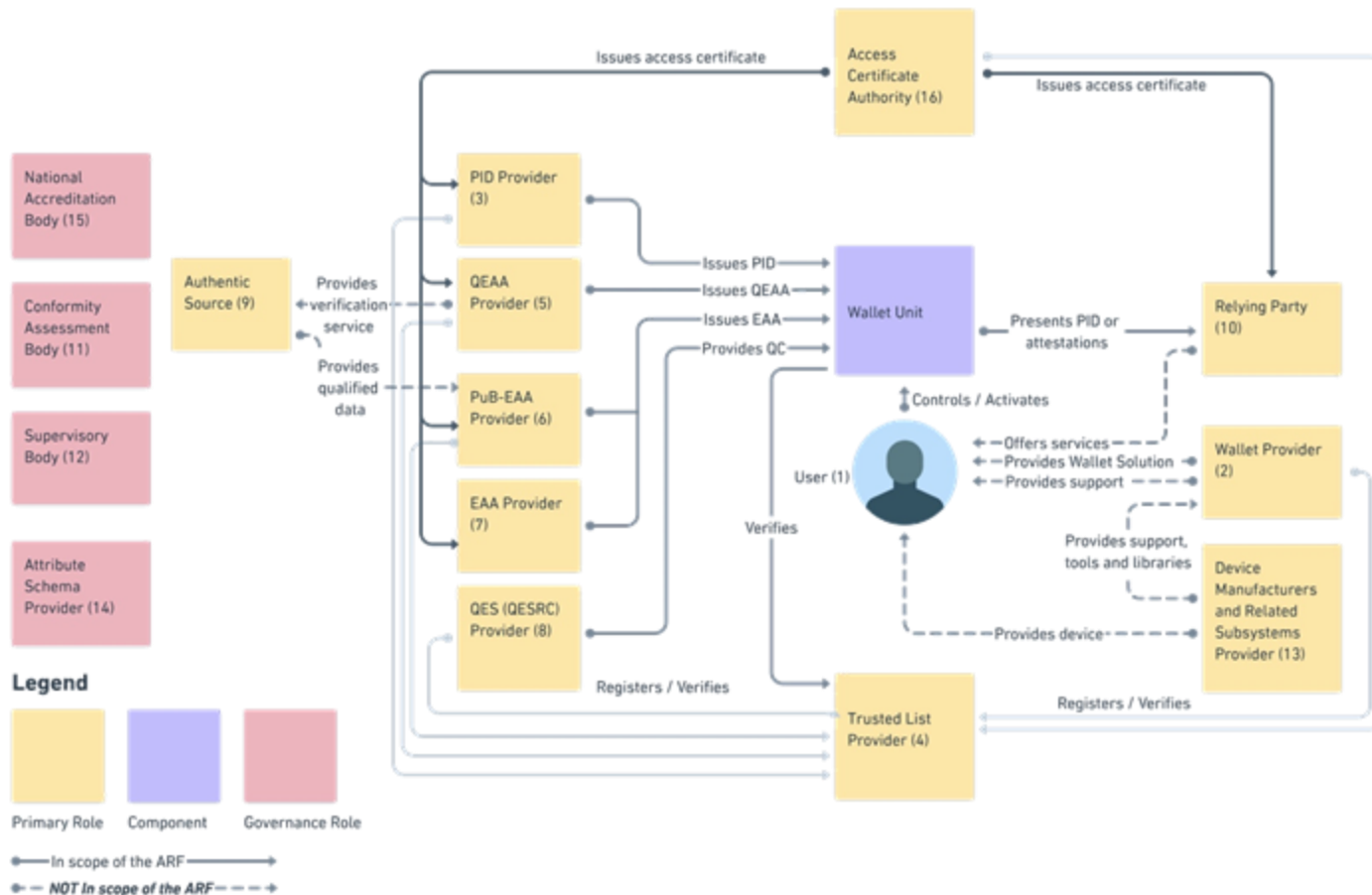
Annex 6: ENISA EUDI Wallets Certification

From clause 1.1 Scope

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to:

- (a) **securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user**, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible;
- (b) generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;
- (c) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;
- (d) **access a log of all transactions** carried out through the European Digital Identity Wallet via a common dashboard enabling the user to:
 - (i) **view an up-to-date list of relying parties** with which the user has established a connection and, where applicable, all data exchanged;
 - (ii) easily **request the erasure** by a relying party of personal data pursuant to Article 17 of the Regulation (EU) 2016/679;
 - (iii) easily **report a relying party** to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received;
- (e) sign by means of qualified electronic signatures or seal by means of qualified electronic seals;
- (f) **download, to the extent technically feasible, the user's data**, electronic attestation of attributes and configurations;
- (g) **exercise the user's rights to data portability**.

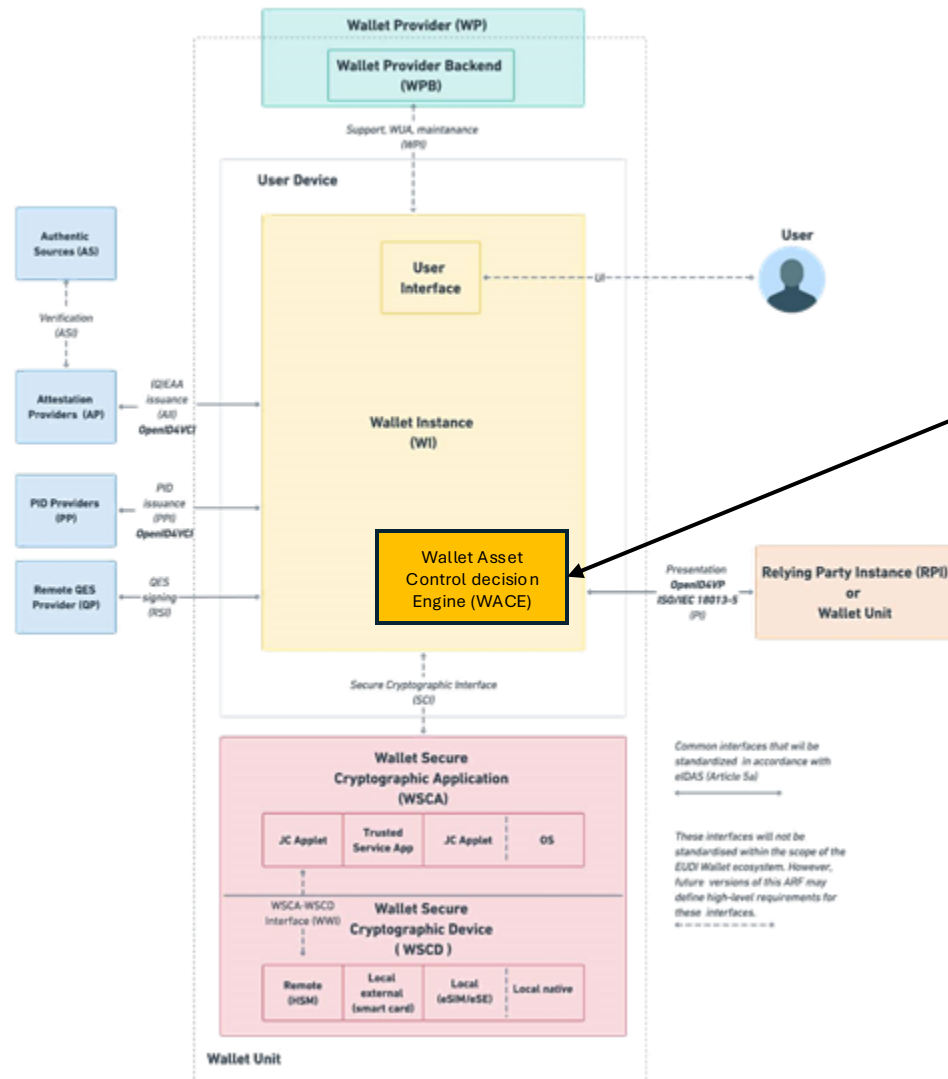
Overview of EUDI Wallet roles



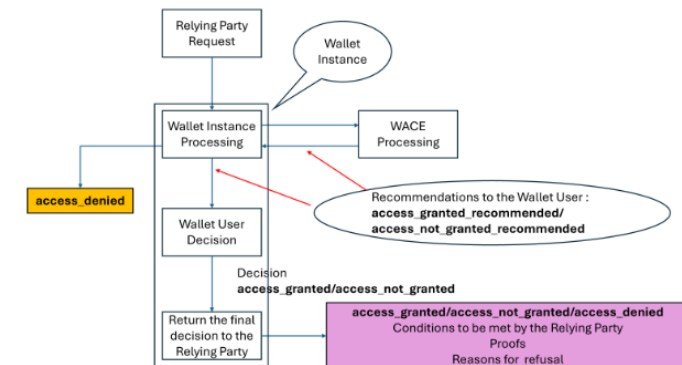
Use Cases

- **Identification and authentication** to access online services (user identification and authentication at LoA high)
- **Mobile Driving Licence** (request, store and present)
- **Health data** (patient summary, ePrescription)
- **Education** (educational credentials)
- **Digital finance** (retail payment and finance industry)
- **Digital Travel Credential** (smooth travel experience)
- **Social Security** (Electronic Health Insurance Card)

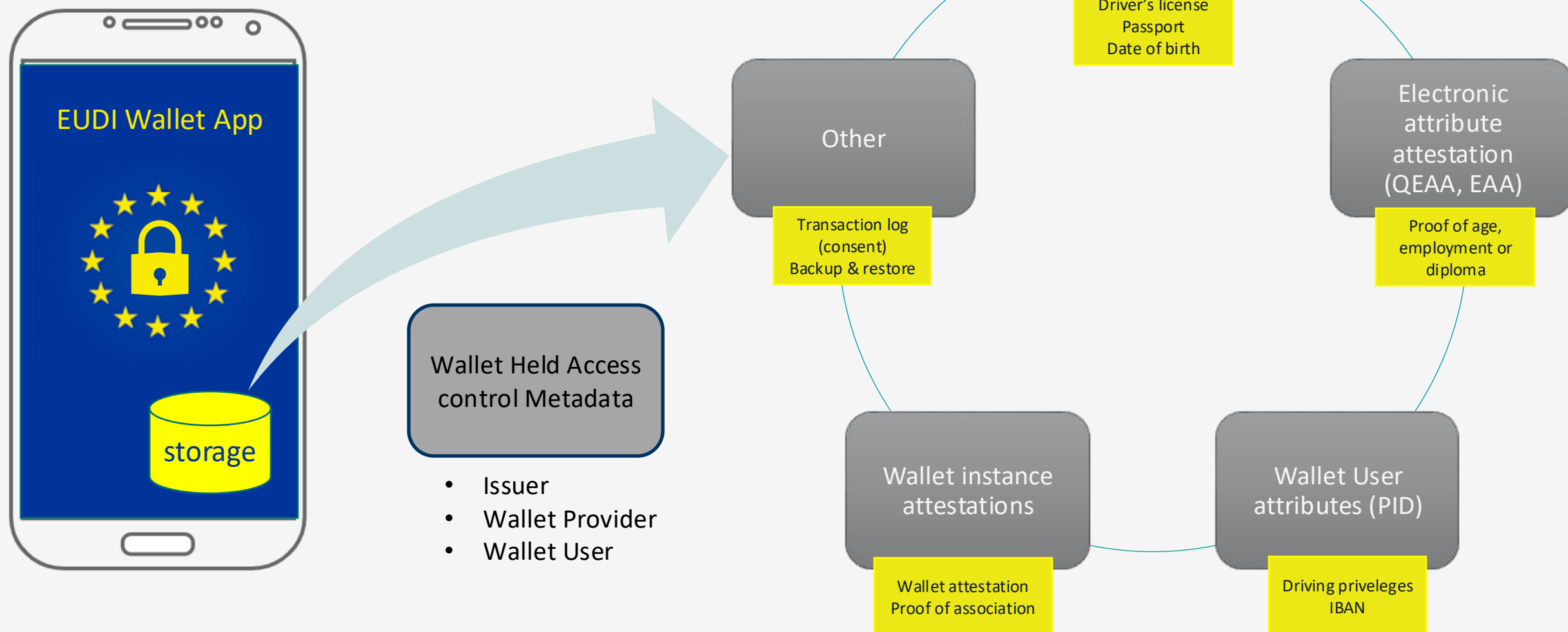
Wallet Unit Architecture



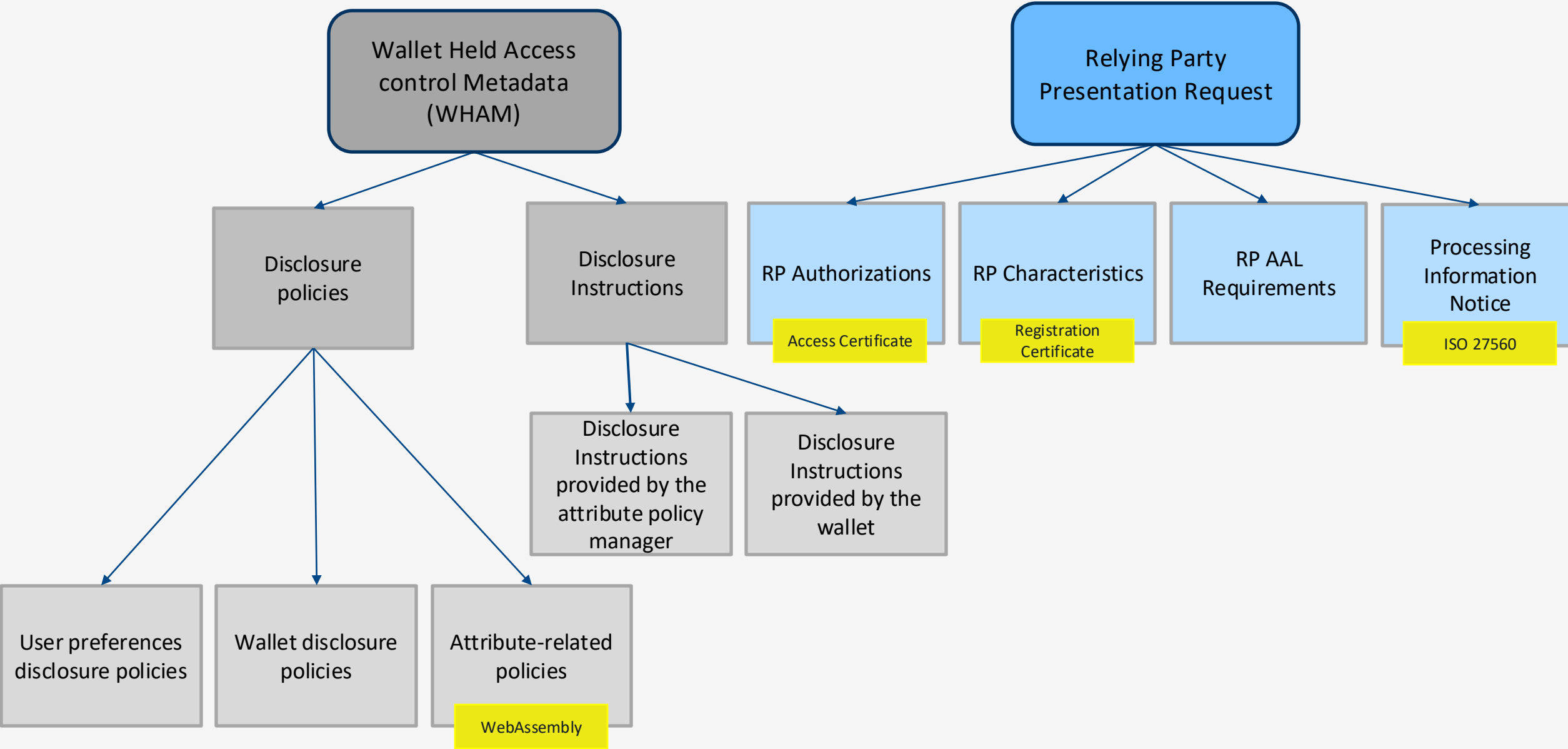
- Definition:
 - Component of the Wallet Instance in charge of processing the access control request to an operation on a WHA
- Operations include:
 - View, Share, Add, Update, Delete
- Input:
 - Wallet Held Access Control metadata
 - Relying Party Operation Request details
- Output:
 - Access_granted_recommended
 - Access_not_granted_recommended
 - Access_denied



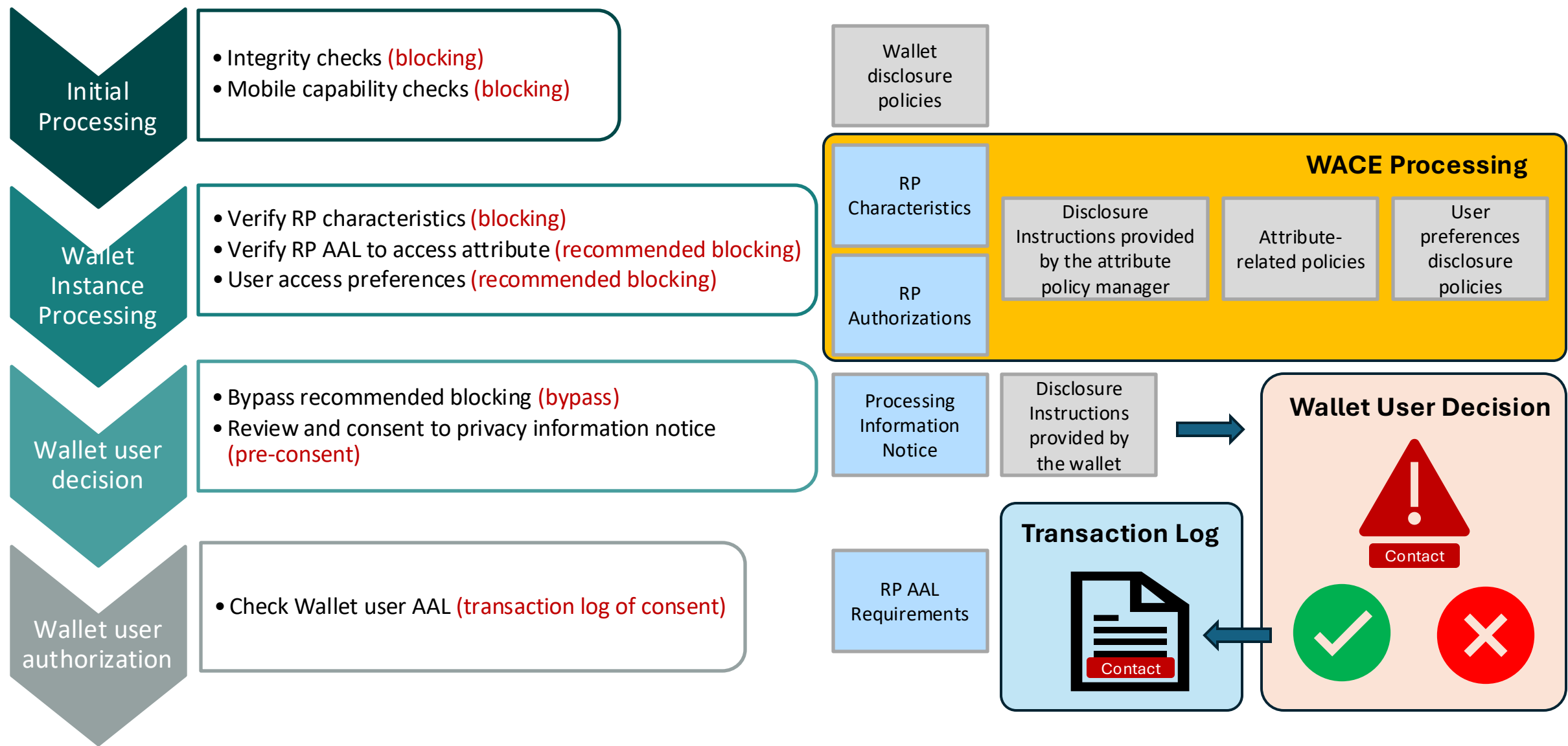
Wallet Held Assets (WHA)



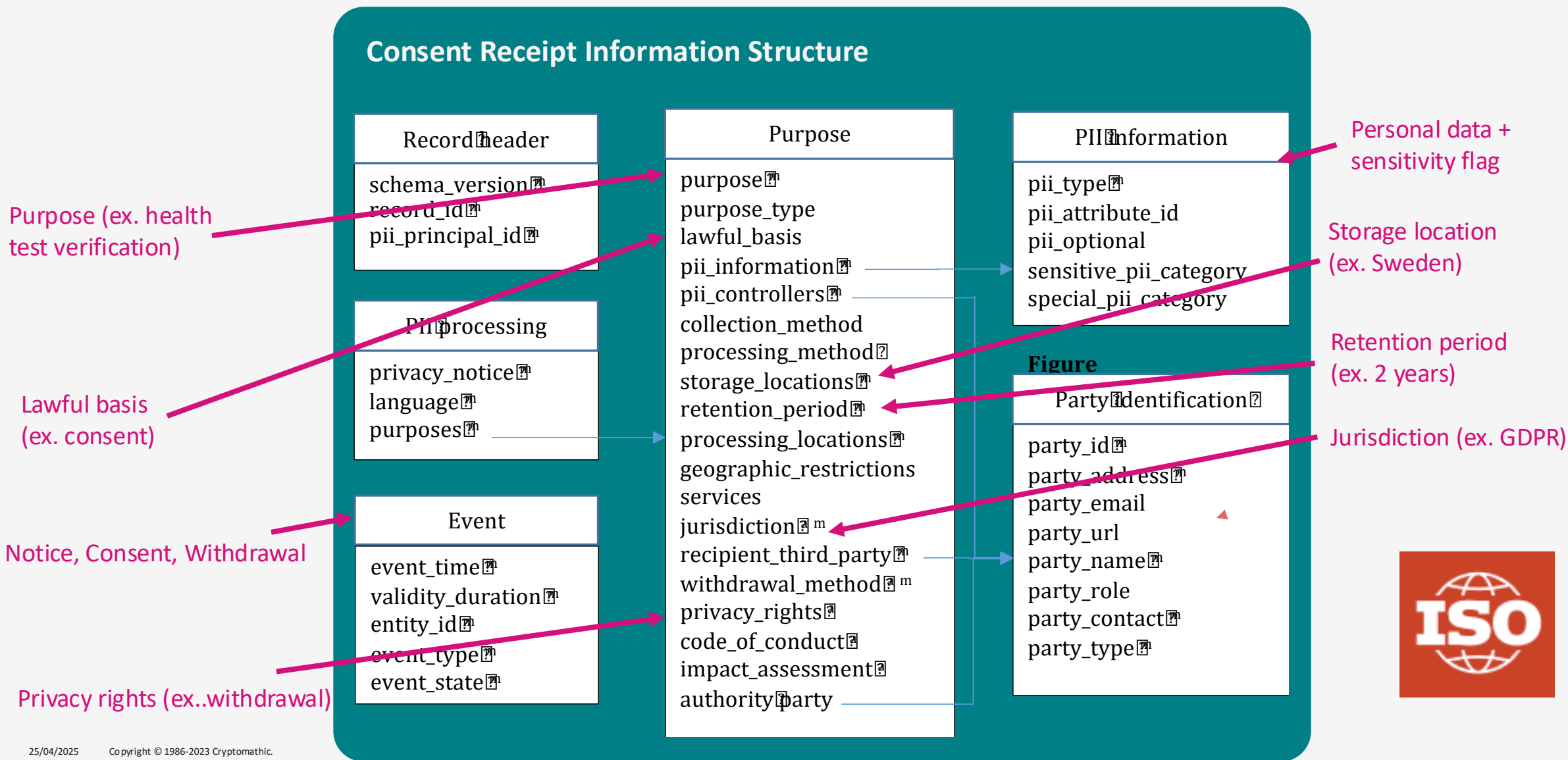
Access Control input



EUDIW Access Control Flow – RP Operation Request



ISO/IEC 27560 CONSENT RECORD AND RECEIPT STRUCTURE



Thank you!

Jan Lindquist - jan@linaltec.com

Harshvardhan J. Pandit - harshvardhan.pandit@adaptcentre.ie