Welcome to the World of Standards

ETSI

World Class Standards

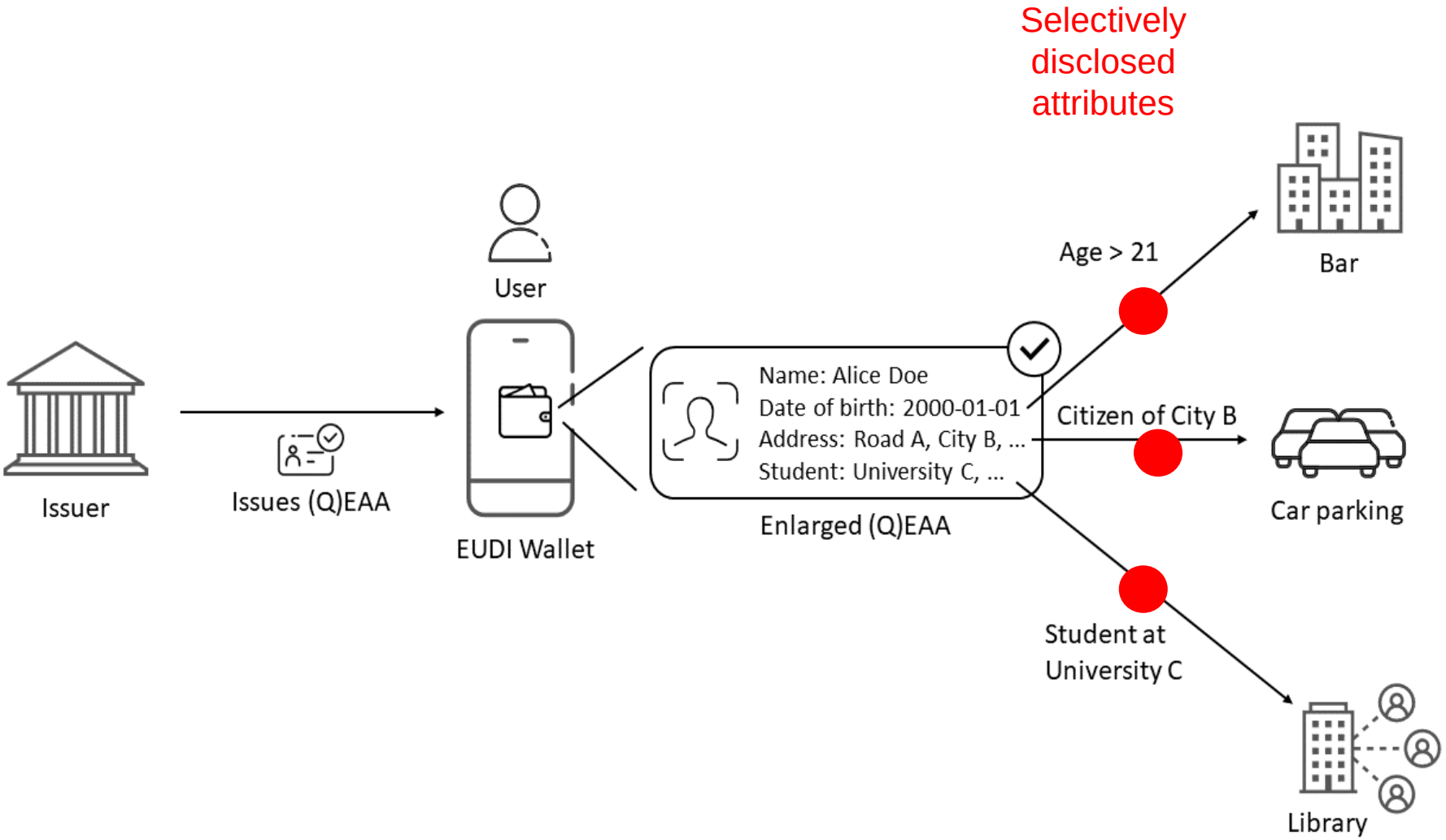
EIDAS 2.0 TOOLBOX: SELECTIVE DISCLOSURE FOR EAA

Sebastian Elfors, senior architect, IDnow

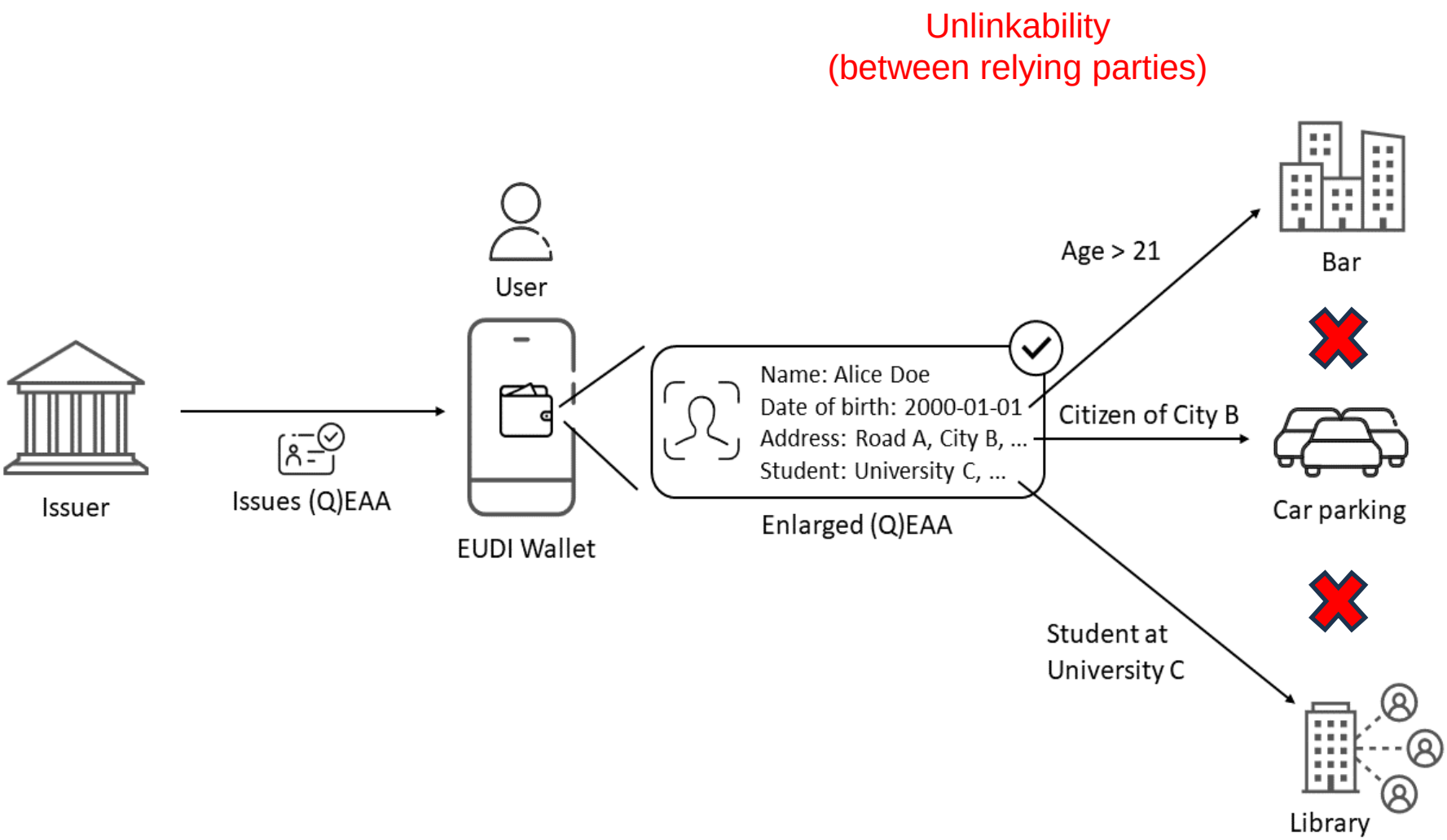
CA Day, Vienna, 2023-10-12

Introduction to selective disclosure

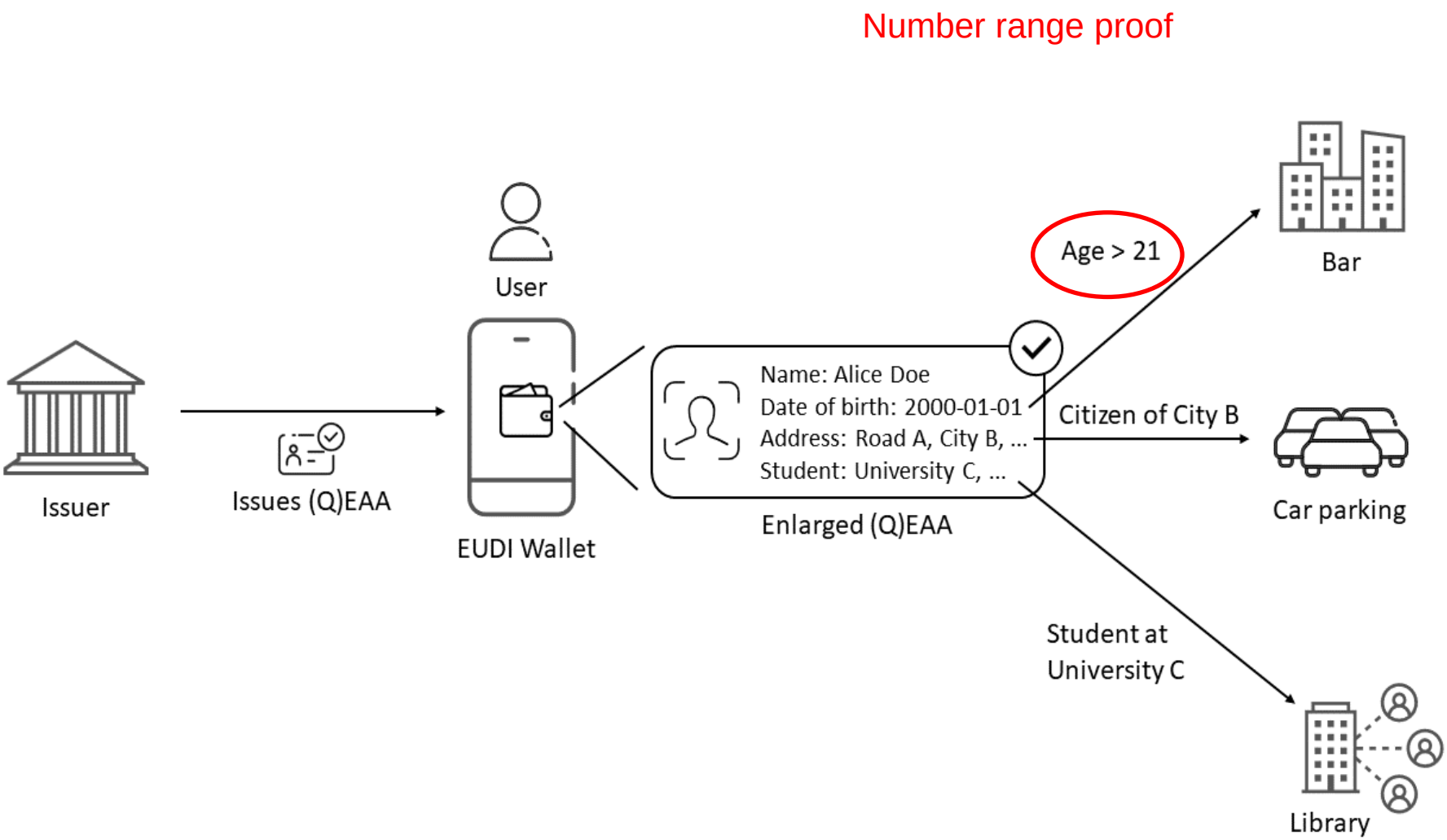
Selective disclosure



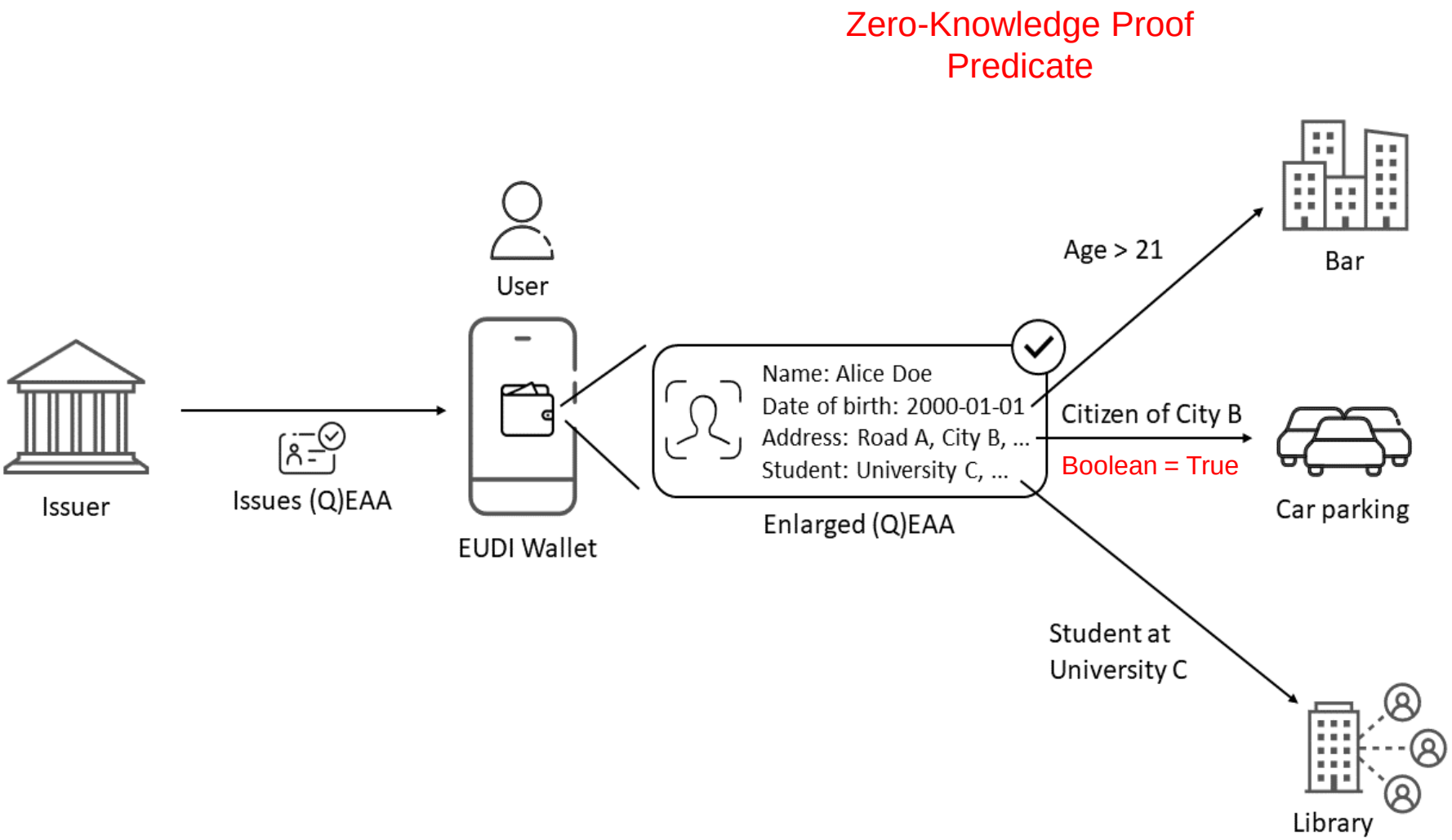
Unlinkability



Range proofs



Zero-Knowledge Proof predicate



EU regulations and standards

Legal definitions in eIDAS2 proposal

(29) Selective disclosure is a concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only information that is required, e.g. for a user to disclose only data to a relying party that is necessary for provision of a service requested by a user. The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. Such selectively disclosed attributes, including when originally parts of multiple distinct electronic attestations, may be subsequently combined and presented to relying parties. This feature should become a basic design feature thereby reinforcing convenience and the protection of personal data including data minimisation.

3. European Digital Identity Wallets are electronic identification means that shall enable the user in a manner that is transparent and traceable by the user to:

(a) securely request, select, combine, store, delete and present electronic attestation of attributes and person identification data to relying parties, including to authenticate online and, where appropriate, offline in order to use public and private services, while ensuring that selective disclosure of data is possible;

Technical definitions in ARF outline

The EUDI Wallet **shall** enforce privacy by design and selective disclosure of attributes.

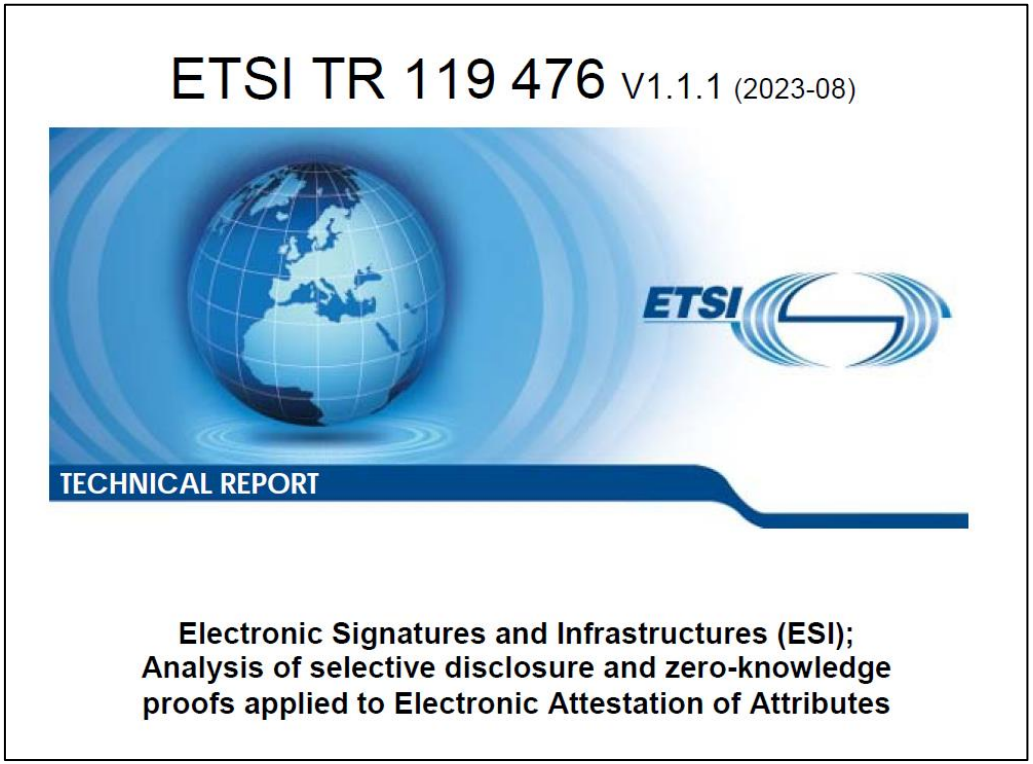
Selective disclosure and combination of attestations can be handled in two different ways:

- the EUDI Wallet may hold a very broad collection of attributes as PID, QEAA and EAA, and each time a specific attribute or the derivation of a specific attribute is required, a new PID or (Q)EAA has to be requested from providers.
- The EUDI Wallet may have the intrinsic capability, based on the obtained PID and (Q)EAA, to selectively disclose, derivate a specific attribute and aggregate several single attributes, without the need for new PID, (Q)EAA or interactions with the PID and (Q)EAA providers. For instance, specific fit for purpose signature schemes in PID and (Q)EAA could enable such capabilities.

The EUDI Wallet **shall** enable the user to share only the information they intend to share. The Wallet **shall** ensure an appropriate level of privacy, implementing policies about non-traceability and unlinkability of user's activities for third parties as appropriate considering:

- the applicable legal context for identity providers and attestation providers;
- the need to retain evidence for dispute resolution purpose;
- the right for the user to be informed of the use of their EUDI Wallet.

ETSI TR 119 476

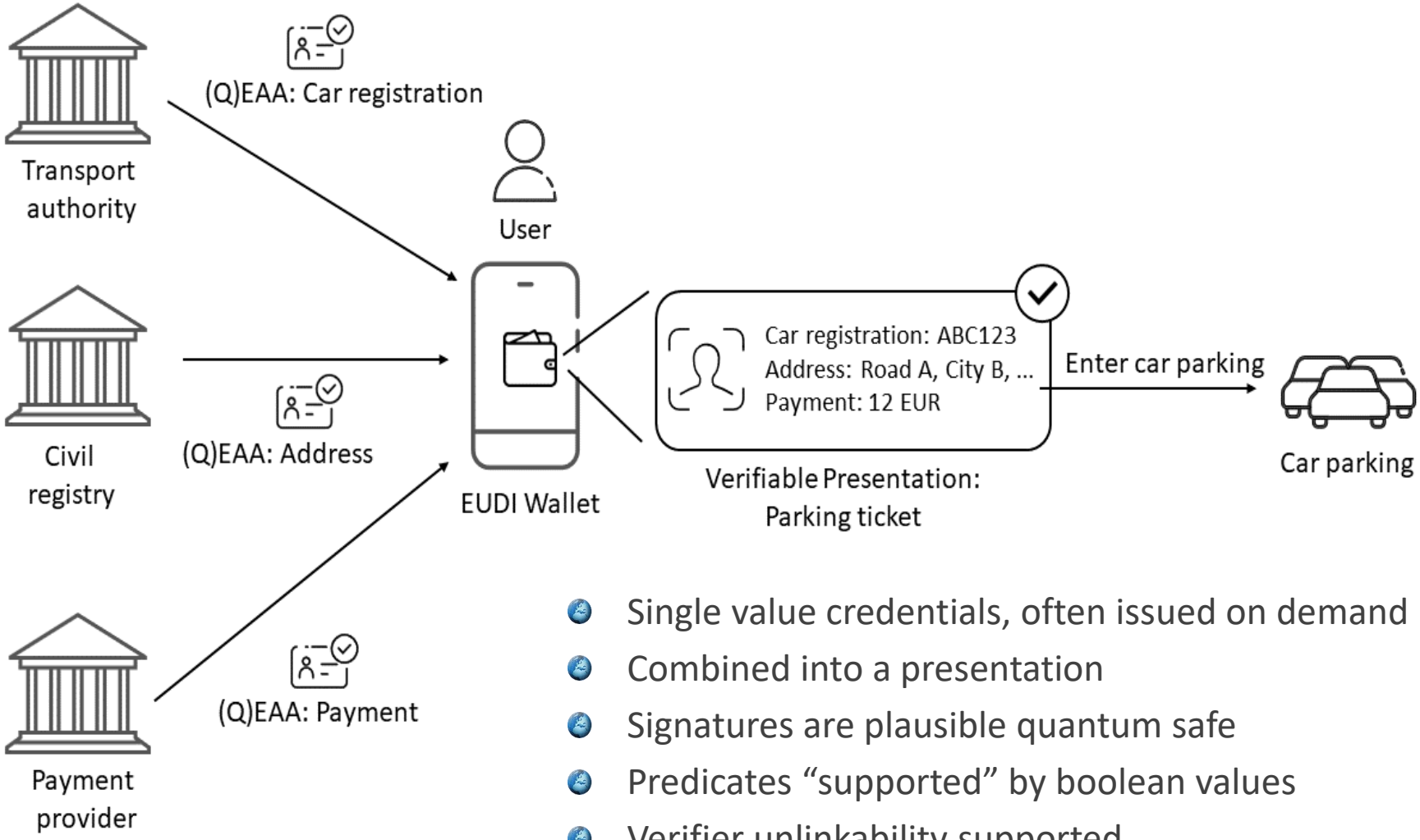


- ETSI ESI published the technical report ETSI TR 119 476 in August 2023
- Describes selective disclosure and Zero-Knowledge Proofs (ZKP)
- Analysis for eIDAS2 and Electronic Attestation of Attributes (EAA)

Selective disclosure schemes

- Atomic (Q)EAAs schemes
- Multi-message signature schemes
- Salted attribute hashes
- Proofs for arithmetic circuits

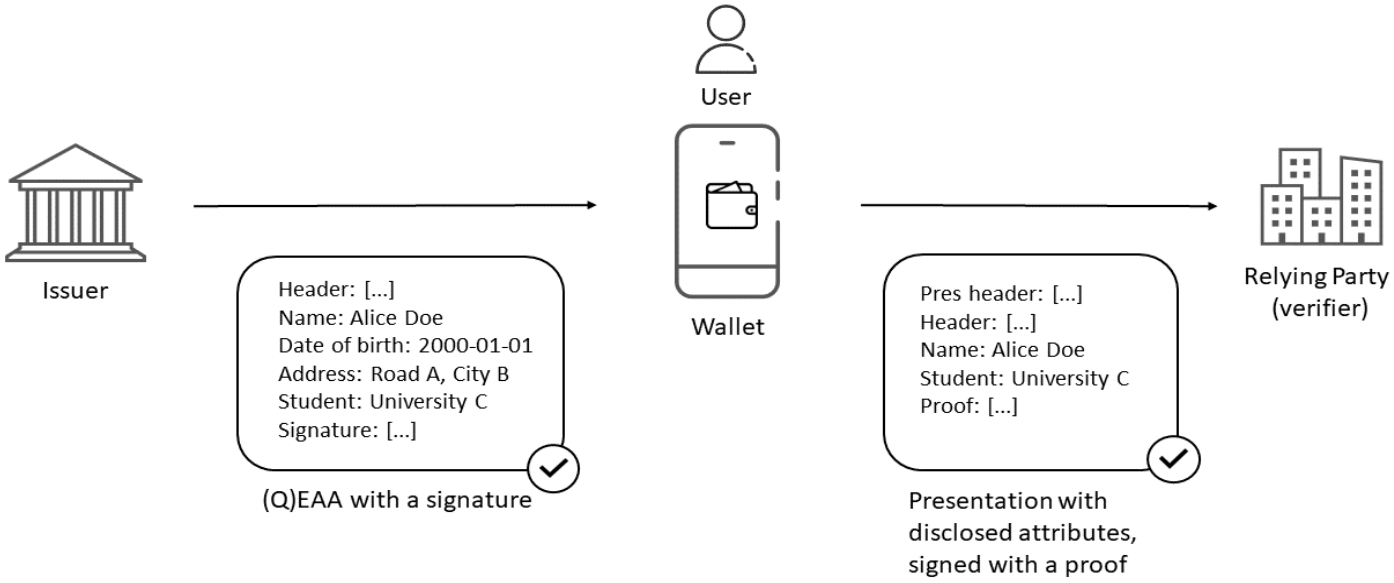
Atomic (Q)EAAs schemes



- Single value credentials, often issued on demand
- Combined into a presentation
- Signatures are plausible quantum safe
- Predicates “supported” by boolean values
- Verifier unlinkability supported

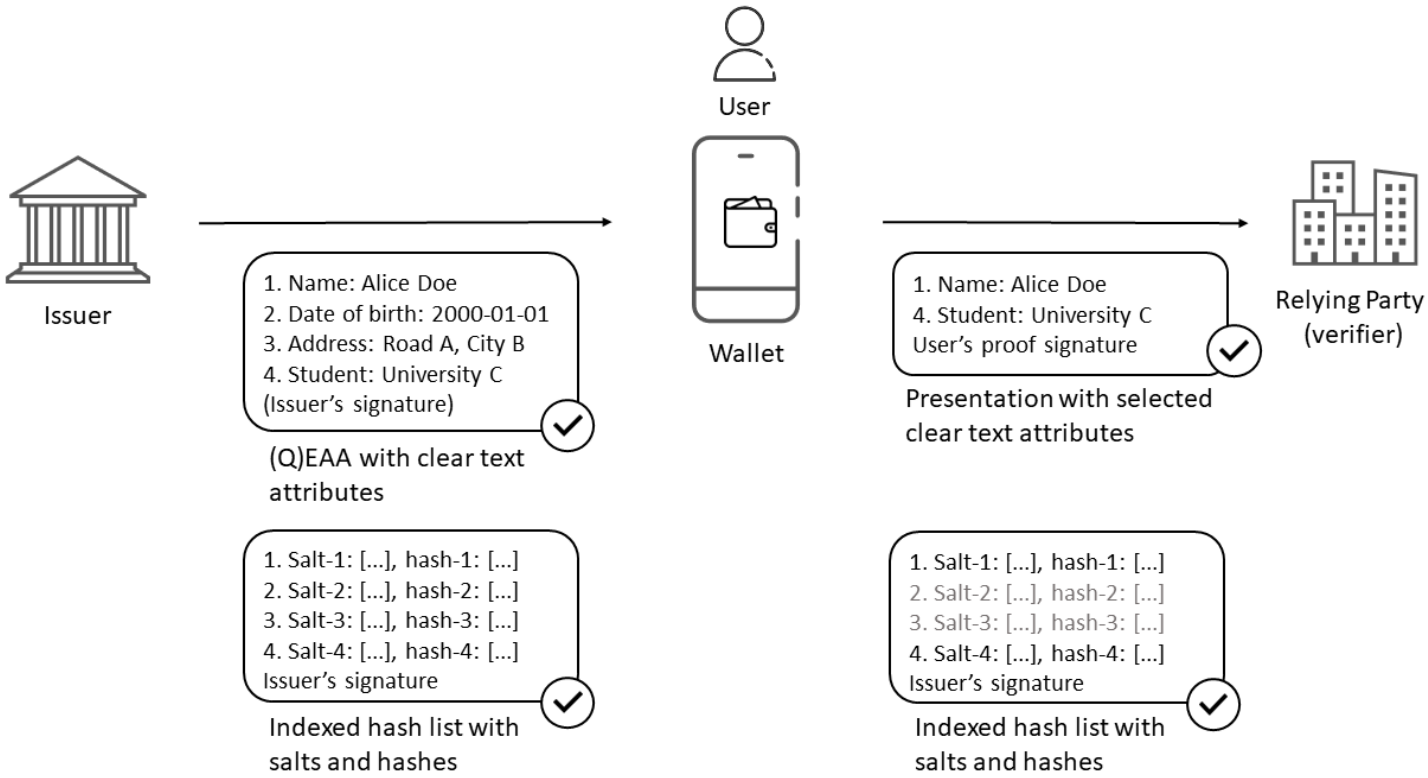
Multi-message signature schemes

- Generates multiple proofs over subsets of an originally signed message
- Multi-message signature schemes:
  - Boneh-Boyen-Shacham (BBS) signature scheme
  - Camenisch-Lysyanskaya (CL) signatures
  - Mercurial signatures
  - Pointcheval-Sanders Multi-Signatures (PS-MS)
- Unlinkability and predicates by design
- Not plausible quantum safe cryptography, not SOG-IS approved



Hashes of salted attributes

- Indexed list with hashes of salted attributes, signed by the issuer
- Plausible post quantum safe cryptographic algorithms
- No unlinkability by design, but batchwise issuance with random salts possible
- No predicates by design, but “supported” by boolean values



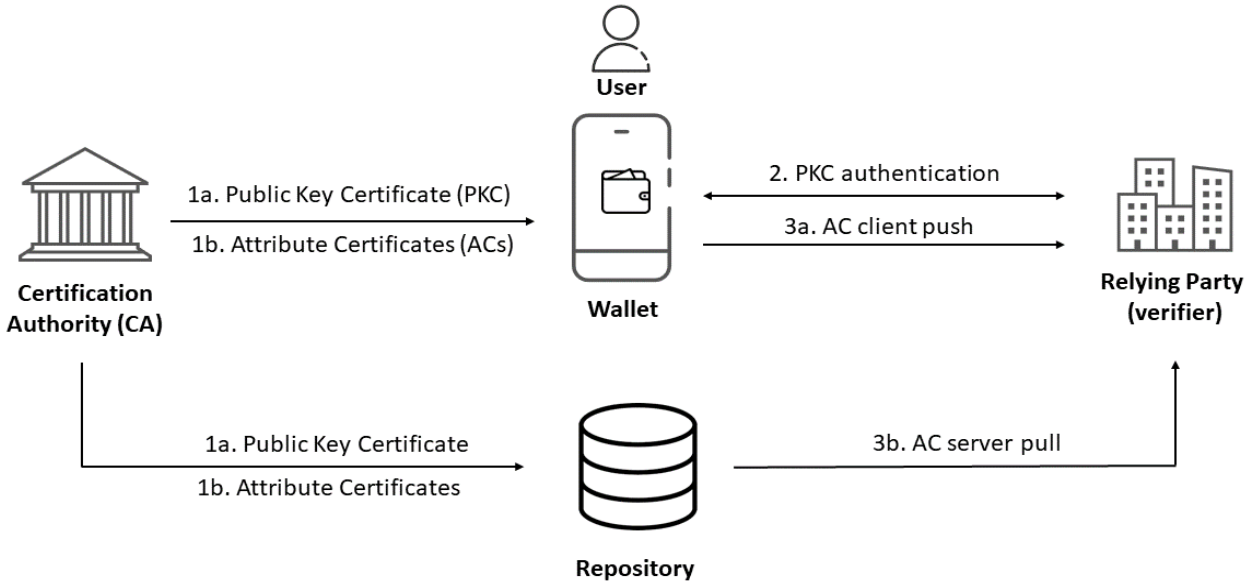
Proofs for arithmetic circuits

- Zero-knowledge proofs for proving correctness of short transactions
- Bulletproofs:
  - Based on Fiat-Shamir heuristics
  - Not plausible quantum safe
- HashWire:
  - Based on PayWord and Micromint
  - Plausible quantum safe, since it is hash based
- zk-SNARK:
  - Family of 18 protocols (and growing), in trusted or non-trusted setups
  - Some zk-SNARKs are plausible quantum safe, whilst others are not
- zk-STARK:
  - Family of two protocols (so far), always non-trusted setups based on hashes
  - Plausible quantum safe, since it is hash based
- Unlinkability by design
- Predicates are fully supported

Selective disclosure credential formats and solutions

Atomic attribute credentials

- Virtually “any” credential format can be atomic
- VC-FIDO solution:
  - FIDO (WebAuthn) used for retrieving atomic W3C Verifiable Credentials (VCs) from multiple issuers
  - Atomic W3C VCs combined into a verifiable presentation
- PKIX X.509 attribute certificates with single attributes



Multi-message signature solutions

- W3C Verifiable Credentials Data Model with section on ZKP
  - CL Signatures explicitly mentioned in the standard
  - Other implementations possible too, e.g. with BBS
- W3C Verifiable Credentials Data Integrity
  - BBS applied on W3C Verifiable Presentations
- Hyperledger AnonCreds
  - CL Signatures used as signature scheme
- Idemix (Identity Mixer) invented by IBM® Research in 2008
  - Based on ABC (Attribute Based Credentials) with CL Signatures
- U-Prove implemented by Microsoft® Research in 2013
  - Also based on ABC, according to Brand's research

Credentials with salted hashes

- IETF SD-JWT
  - Contains hash values of JSON attributes combined with random salts
  - Selected for selective disclosure of JSON credentials in ARF v1.0
- ISO Mobile Security Object (MSO)
  - Part of the ISO 18013-5 mDL standard
  - Contains hash values of ISO mDL attributes combined with random values (salts)
  - Selected for selective disclosure of ISO mDL in ARF v1.0

ISO mobile driving license (mDL)

- ISO 18013-5 device retrieval flow
  - Short proximity (“offline”) device connection to reader
  - MSO used for selective disclosure of mDL attributes
- ISO 18013-5 server retrieval flow
  - OpenID Connect used for selective disclosure of mDL attributes
- ISO 18013-7 unattended retrieval flow
  - Online access to web server with OpenID4VP and SIOP
  - MSO used for selective disclosure of mDL attributes

Selective disclosure for eIDAS2

Selective disclosure for eIDAS2

- ISO mDL and W3C VC are selected as PID formats in ARF v1.0 for EUDI Wallet Type 1 configurations
  - EU public sector requires SOG-IS approved cryptographic algorithms
- MSO used for selective disclosure for ISO mDL
  - Approved by SOG-IS and plausible quantum safe
- SD-JWT used for selective disclosure for JSON credentials
  - Approved by SOG-IS and plausible quantum safe
  - Compatibility of W3C Verifiable Credentials Data Model v1.1 and SD-JWT v0.5 is being analyzed
- To mitigate linkability for colluding verifiers:
  - Issue batchwise of MSOs or SD-JWTs with different random salts
  - Single use of MSO or SD-JWT per selective disclosure transaction
- EUDI Wallet Type 2 configurations allow for multi-message signature schemes and proofs for arithmetic circuits

Thanks!

Any questions?

Editors of ETSI TR 119 476:

Sebastian Elfors, sebastian.elfors@idnow.io

Peter Lee Altmann, peter.altmann@digg.se