ETSI TR 119 476 V1.2.1 (2024-07)

Electronic Signatures and Trust Infrastructures (ESI);
Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes

Reference
RTR/ESI-0019476v121

Keywords
identity, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The eIDAS2 regulation and the Architecture and Reference Framework (ARF) define regulatory requirements on selective disclosure and unlinkability for the EUDI Wallet. The present document provides a general yet comprehensive analysis of signature schemes, formats and protocols that cater for selective disclosure, unlinkability and predicates. More specifically, the present document includes an analysis of how certain selective disclosure techniques can be applied on eIDAS2 and the EUDI Wallet.

The term selective disclosure means that a user should be capable of presenting a subset of attributes from at least one, but potentially multiple, (Qualified) Electronic Attestations of Attributes ((Q)EAAs). For example, a user should be able to only present their birth date.

The term unlinkability means that different parties should not be able to connect the user's selectively disclosed attributes beyond what is disclosed. There are different categories and degrees of unlinkability, and the present report focuses both on verifier unlinkability and full unlinkability. Verifier unlinkable means that one or more verifiers cannot collude to determine if the selectively disclosed attributes describe the same identity subject, whilst fully unlinkable means that no party can collude to determine if the selectively disclosed attributes describe the same identity subject.

Predicate proofs are verifiable Boolean assertions (true or false) about attributes in a (Q)EAA without disclosing the attribute value itself. For example, a user could derive a proof that they are above the age of 20 from their birthdate and show only the proof as opposed to the birthdate itself. Predicate proofs are often employed in Zero-Knowledge Proof (ZKP) systems aimed at limiting information disclosure.

The selective disclosure signature schemes described in the present report are divided in the following categories:

- **Atomic (Q)EAA schemes**. An atomic electronic attribute attestation is a (Q)EAA with a single attribute claim, which can be issued by a (Q)TSP upon request or as part of a batch to an EUDI Wallet. The atomic (Q)EAAs can be selected by the user and be included in a verifiable presentation that is presented to a verifier.

- **Multi-message signature schemes**. The category of multi-message signature schemes has the capability of proving knowledge of a signature while selectively disclosing any subset of the signed messages. The following schemes in this category are described: BBS/BBS+, Camenisch-Lysyanskaya (CL) signatures, Mercurial signatures, and Pointcheval-Sanders Multi-Signatures (PS-MS). ISO/IEC have standardized parts of BBS and PS-MS in ISO/IEC 20008 [i.143], and have taken the initiative to standardize BBS+ and PS-MS in ISO/IEC PWI 24843 [i.144] and ISO/IEC CD 27565 [i.150]. Furthermore, there are cryptographic research projects, such as MoniPoly, where undisclosed attributes have no impact on the proof size.

- **Salted attribute hashes**. The general concept of this category is to combine each attribute with a salt, hash the combined values, and insert the resulting salted attribute hashes in a list that is signed. The user presents a selection of attributes to the verifier, which can validate them against the list of salted attribute hashes. The following schemes, based on salted attribute hashes, are described: HashWires, Authentic Chained Data Containers (ACDC), and Gordian Envelopes.

- **Proofs for arithmetic circuits (programmable ZKPs)**. This category of ZKP protocols enable the user to prove to the verifier that a certain statement is true, without revealing any additional information beyond the truth of the statement itself. The discussion of proofs for arithmetic circuits is focused on zk-SNARKs.

The present document also includes descriptions of (Q)EAA formats that can be used with selective disclosure. The (Q)EAA formats are divided in the following categories:

- **Atomic (Q)EAA formats**. These (Q)EAA formats are based on the category of atomic (Q)EAA formats. The following (Q)EAA formats in this category are described: PKIX X.509 attribute certificate with atomic attribute and W3C Verifiable Credential with atomic attribute.

- **Multi-message signature (Q)EAA formats**. This category of (Q)EAA formats is based on the multi-message signature schemes. Mainly W3C and Hyperledger have specified such formats to be used for privacy preserving features. The following (Q)EAA formats in this category are described: W3C VC Data Model with ZKP, W3C VC Data Integrity with BBS Cryptosuite, W3C Data Integrity ECDSA Cryptosuites v1.0, and Hyperledger AnonCreds (format).

- **(Q)EAAs with salted attribute hashes**. This category of (Q)EAA formats is based on the concept of salted attribute hashes. These (Q)EAA formats specify in detail how the attributes are combined with the random salts and hashed, inserted in a list, which is signed. The following (Q)EAA formats of this category are described: IETF SD-JWT and ISO/IEC 18013-5 [i.140] Mobile Security Object (MSO).

- **JSON container formats**. This category of generic JSON container formats allows for combining and presenting a mix of selective disclosure signature schemes. The following JSON container formats are described: IETF JSON WebProof (JWP) and W3C JSON Web Proofs For Binary Merkle Trees.

Furthermore, the present document describes systems and protocols with selective disclosure capabilities. The systems and protocols are divided in the following categories:

- **Atomic attribute (Q)EAA presentation protocols**. This category of protocols is designed to present the atomic attribute (Q)EAA formats. The atomic attribute (Q)EAAs may be issued on demand to the user, upon request by a verifier. The following protocols in this category are described: PKIX X.509 attribute certificates with single attributes and VC-FIDO for atomic (Q)EAAs.

- **Multi-message signature protocols and solutions**. This category of protocols is based on the multi-message signature schemes, such as BBS+ and CL-signatures, and are used to present selected attributes of the (Q)EAAs. The following protocols and solutions in this category are described: Hyperledger AnonCreds (protocols) and Direct Anonymous Attestation (DAA) used with Trusted Platform Modules (TPMs); the TPMs have been deployed in personal computers at a large scale.

- **Salted attribute hashes protocols**. These solutions and protocols are designed to present selectively disclosed attributes based on salted attribute hashes. The OpenAttestation solution of Singapore's Smart Nation is described in the present report. Furthermore, ISO mDL MSOs can be shared over the proximity protocols described in ISO/IEC 18013-5 [i.140] or over the Internet by using ISO/IEC 23220-4 [i.146]. The SD-JWTs can be presented with different protocols, such as OID4VP (OpenID for Verifiable Presentations), ISO 18013-7 [i.141] or ISO/IEC 23220-4 [i.146].

- **Solutions based on proofs for arithmetic circuits (programmable ZKPs)**. The solutions that are based on proofs for arithmetic circuits intend to use ZKP schemes such as zk-SNARK to facilitate data-minimizing verifiable presentations based on existing digital identity infrastructures. In particular, they can provide selective disclosure, unlinkability, and predicates. The projects Cinderella (zk-SNARKs used with X.509 certificates) and zk-creds (zk-SNARKs used with ICAO passports) are described in the present document.

- **Anonymous attribute based credentials systems**. These solutions are implementations of existing multi-message signature schemes such as CL-signatures or BBS+, with the purpose to present anonymous credentials ((Q)EAAs) to a verifier. The following solutions in this category are described: Idemix (Identity Mixer), U-Prove, ISO/IEC 18370 [i.142] (blind digital signatures), and Keyed-Verification Anonymous Credentials (KVAC).

- **ISO mobile driving license (ISO mDL)**. The ISO mDL standard specifies various flows for selective disclosure of attributes. In the present document, the following ISO mDL flows are described: ISO/IEC 18013-5 [i.140] (device retrieval flow), ISO/IEC 18013-5 [i.140] (server retrieval flows), ISO/IEC 18013-7 [i.141] (unattended flow) and ISO/IEC 23220-4 [i.146] (operational protocols).

The ARF proposes two protection mechanisms for the PID, which support selective disclosure but not unlinkability (unless batch issued):

- ISO/IEC 18013-5 [i.140] (ISO mDL). The ISO mDL mdoc contains all attributes of a user, whilst the ISO mDL MSO contains the corresponding hashed salted attributes.

- A JWT encoding of the W3C Verifiable Credentials Data Model v1.1 in conjunction with IETF SD-JWT. The JWT contains the user attributes, whilst the SD-JWT contains the corresponding hashed salted attributes.

The present document includes an extensive analysis of ISO mDL MSO and SD-JWT and how the formats comply with the eIDAS2 requirements on selective disclosure and unlinkability.

The ISO mDL MSO and the SD-JWT formats, and related presentation protocols, cater for selective disclosure based on the concept of salted attribute hashes. Furthermore, the MSO and SD-JWT formats support SOG-IS approved cryptographic algorithms and can also be used with quantum-safe cryptography for future use. The conclusion is thus that MSO and SD-JWT meet the eIDAS2 regulatory and technical requirements on selective disclosure.

As stated, ISO mDL MSO and SD-JWT are not fully unlinkable, although they can provide verifier unlinkability with certain operational measures. In order to achieve verifier unlinkability, batches of ISO mDL MSOs or SD-JWTs need to be issued to each EUDI Wallet. The random salts in the ISO mDL MSO and SD-JWT should be unique, meaning that refreshed MSOs and SD-JWTs are presented to a relying party. Furthermore, the user public keys used for holder binding, if present, need to be unique too.

There are many similarities between the ISO mDL issuers and the eIDAS2 compliant PID Providers (PIDPs) or QTSPs. The PIDPs/QTSPs can issue PIDs/(Q)EAAs to EUDI Wallets as follows to cater for selective disclosure:

- The PIDP/QTSP issues ISO mDL mdoc and/or JWT as PID/(Q)EAAs to the EUDI Wallet.

- The PIDP/QTSP issues ISO mDL MSOs and/or SD-JWTs batchwise to the EUDI Wallet. The ISO mDL MSOs are associated with the ISO mDL mdoc, and the SD-JWTs with the JWT. Random salts are used for the hashed salted attributes in each MSO or SD-JWT. This will cater for verifier unlinkability when the MSOs or SD-JWTs are presented to and validated by a relying party.

- The EUDI Wallet selectively discloses certain attribute(s) of an ISO mDL mdoc or JWT. One ISO mDL MSO or SD-JWT is selected from the batch in the EUDI Wallet, and is associated with the disclosed attribute(s).

- The relying party can use the eIDAS2 trust list (which is equivalent to an ISO mDL VICAL) to retrieve the QTSP/PIDP trust anchor (which is equivalent to the IACA trust anchor). The relying party validates the MSOs or SD-JWTs signatures by using the QTSP/PIDP trust anchor. The relying party also verifies that the presented selected attribute hash is present in the MSO or SD-JWT.

These recommendations could be considered for the upcoming ETSI TS 119 471 [i.80] and ETSI TS 119 472-1 [i.81] that will standardize the issuance policies and profiles of (Q)EAAs.

Multi-message signature schemes such as BBS+, Camenisch-Lysyanskaya (CL) signatures, Mercurial signatures, and Pointcheval-Sanders Multi-Signatures (PS-MS) cater for full unlinkability, although they are not yet fully standardized. Hence, ISO/IEC PWI 24843 intends to standardize BBS+ and PS-MS with blinded signatures, which may allow for a future standard that could be used in compliance with the EUDI Wallet requirements on selective disclosure and unlinkability in eIDAS2.

There are also systems based on programmable ZKPs in the form of zk-SNARKs, such as Cinderella and zk-creds, that can achieve both selective disclosure and unlinkability with existing digital identity infrastructures such as X.509 certificates or ICAO passports. Such systems can generate pseudo-certificates that share selected attributes from the (Q)EAAs and attest holder binding and non-revocation without exposing linkable cryptographic identifiers. In contrast to multi-signature schemes, anonymous credentials based on programmable ZKPs can be made compatible with deployed secure hardware and are easily extendable. However, these projects are still in the research phase. Still, they may be considered for the EUDI Wallet and eIDAS2 relying parties.

Furthermore, there are recommendations on how to store such (Q)EAA formats in the EUDI Wallet, and how to present selectively disclosed attributes to eIDAS2 relying parties. These recommendations can be considered for the upcoming ETSI TS 119 462 [i.79] on EUDI Wallet interfaces.

The present document also analyses the privacy aspects of revocation schemes and validity status checks. In order to achieve privacy preserving features for revocation and validity status checks it is recommended to use OCSP in Must-Staple mode, implement Revocation Lists or validity Status Lists with additional privacy techniques such as Private Information Retrieval or Private Set Intersection, and use cryptographic accumulators where possible given the associated complexity. If programmable ZKP schemes (such as zk-SNARKs) are combined with existing credentials (such as X.509), the status validity checks are performed at the EUDI Wallet, and only the relevant information (revocation state) without any linkable cryptographic identifiers is disclosed with the verifier.

The present document also includes an analysis of post-quantum computing attacks on cryptographic schemes with selective disclosure capabilities. More specifically, the hashed salted attributes formats, such as ISO mDL MSO and SD-JWT, can be signed with post-quantum safe cryptographic algorithms. Also the atomic (Q)EAA formats can be secured with post-quantum safe signatures. The multi-message signature schemes, such as BBS+ and CL-signatures, have the following characteristics in a post-quantum world: an attacker can use a quantum computer to reveal the signer's private key from the public key and thereafter forge proofs and signatures, but an attacker will not be able to break data confidentiality, meaning that undisclosed messages are safe in a post-quantum world, as are undisclosed signature values. As regards to the programmable ZKP schemes, it depends on the design of the arithmetic circuit proof if it is post-quantum safe or not, meaning that there are zk-SNARKs that are post-quantum safe whilst others are not.

Finally, there is an annex with research projects about innovative ZKP schemes. One such approach is to design cryptographic ZKP schemes based on quantum physics. Quantum Key Distribution (QKD), quantum physics applied to the graph 3-colouring ZKP scheme, and ZKP using the quantum Internet (based on Schnorr's algorithm) are described in the annex. The ZKP schemes based on quantum physics are still in the research phase, but may be considered for the future. There are also cryptographic research initiatives on post-quantum safe (lattice-based) anonymous credentials, which cater for privacy-preserving signature schemes. The most recent research in this field is related to efficient anonymous credentials that are post-quantum safe, yet with small signature sizes.

Introduction

A historical perspective

To facilitate an understanding of the concepts in the present document, the present clause begins with a brief account of the history of selective disclosure and Zero-Knowledge Proofs (ZKPs), the problems they were introduced to address, their applications, and their potential uses in electronic attestations of attributes. The present document also discusses related concepts where required.

Cryptographic schemes for selective disclosure, unlinkability, blinded signatures, Zero-Knowledge Proofs (ZKPs), predicates and range proofs have been researched and developed since the 1980s. The first ZKP scheme was published in a paper 1985 [i.97] by the researchers Shafi Goldwasser, Silvio Micali, and Charles Rakoff. The abstract of this paper defines ZKP as: "*Zero-Knowledge Proofs are defined as those proofs that convey no additional knowledge other than the correctness of the proposition to the question*".

The present document on selective disclosure can be linked to the broader work on signatures that allow for updates to the signed document. In their 1994 paper "Incremental Cryptography: The Case of Hashing and Signing" [i.14], Bellare, Goldreich, and Goldwasser investigate cryptographic transformations where the updates to the results are proportional to the amount of modification done. Using digital signatures as a case, the authors propose the idea of updating the signature upon modification of the underlying message in a way that is proportional to the amount of change in the message (as opposed to simply signing the new message). The authors called for future work to explore various operations, such as delete and update, that could be supported by incremental signatures.

It is important to note that ZKP is not a selective disclosure scheme in and of itself, but rather a property of a proof system. Goldwasser, Micali and Rakoff (1985) defined ZKP [i.97] as "*those proofs that convey no additional knowledge other than the correctness of the proposition to the question*". Thus, ZKP is not limited to selective disclosures or signatures proofs in the context of electronic attestations of attributes. On the contrary, Brassard et al. demonstrated in their paper "Minimum disclosure proofs of knowledge" [i.32] that everything that has a proof also has a ZKP version of that proof.

Put differently, every selective disclosure related proof has a ZKP version of that proof. But it is incorrect to state that every selective disclosure scheme is done using ZKP, or that every ZKP is used for selective disclosure. ZKPs matter because usually, in digital identification, holders share substantially more information than the verifier asks for, e.g. superfluous identity attributes, unique cryptographic information (signatures, public keys, revocation IDs). Using a ZKP, the holder only proves what the verifier wants to know (precisely the required identity attributes, i.e. selective disclosure; that the attributes are signed by the issuer without revealing the linkable digital signature (unlinkability), that an attribute has a required property without sharing it (predicates such as range proofs). As such, ZKPs can be considered as facilitating the perfect implementation of the data minimization principle.

Electronic attestations of attributes represent a context in which several features, such as selective disclosure or proofs about knowledge of states like a valid signature value, have been implemented with the ZKP property. Among the earliest work here was done by Feige, Fiat, and Shamir (1987) who demonstrated how ZKP can be used in identification schemes by a user demonstrating knowledge as opposed to prove the validity of assertions. Since then, ZKP has been widely deployed in many of the privacy focused selective disclosure capable electronic attestation of attribute solutions.

Another pioneer in the field of ZKP was the American cryptographer David Chaum who published the scientific paper Blind Signatures for Untraceable Payments [i.53] in 1982, which described anonymized digital money (DigiCash) for the first time. The concept of Blind Signatures was designed to ensure complete privacy of users who wanted to conduct online transactions.

In 2002, Steinfeld, Bull, and Zheng published their paper "Content Extraction Signatures" (CES) [i.190]. In it, the authors present a way to perform the delete operation without knowledge of the signer's private key. The authors argue that this would allow a user "to disclose only certain parts of a document" as opposed to "forcing the document holder to disclose all of its contents to a third party for the signature to be verifiable". The authors then go on to present the idea of context extraction, i.e. "the extraction of certain selected portions of a signed document" in cases where a user "does not wish to pass on the whole document to a third (verifying) party". Their method is based on signing digests of data subsets. Relatedly, Johnson et al. (2002) presented their work on redactable signatures, which are conceptually very similar to CES. In fact, the proposed schemes in the papers overlap, together detailing four different schemes for CES. Two of these rely on commitment vectors, and two on the homomorphic properties and batching of RSA respectively.

Brands (2002) directly applies these concepts to electronic attestations of attributes. In his 2002 paper "A Technical Overview of Digital Credentials" [i.30] Brands discusses the "selective disclosure properties of data fields" in digital credentials. In that paper, Brands presents the idea to "hash attributes [...] using a collision-intractable hash function; to disclose these attributes, Alice discloses the preimages of the corresponding [attributes]". Interestingly, Brands proposed design also relies on a proof of knowledge of the digital signature, which is among the first references to the use of ZKP for enhancing privacy when presenting electronic attestations of attributes. Brands' paper is also among the earliest work on the use of predicates in electronic attestations of attributes. In essence, Brands' work was based on commitment vectors and the algebraic manipulations (e.g. addition and multiplication) of these commitments, allowing proofs containing AND, OR, and NOT connectives between attributes and for a single attribute.

The above mentioned work laid the groundwork for the concept of selective disclosure and unlinkability. Ongoing work presented workarounds to discovered vulnerabilities in some of the proposed schemes, and introduced more advanced features that further improved privacy e.g. by enabling multi-show unlinkable selective disclosures (defined in clause 3.1 and for additional details see "Anonymous Credentials" [i.41] by Camenisch and Lysyanskaya in 2003). Notable early examples of implementations of this work focused on enhanced privacy include AnonCreds and Idemix (both based on Camenisch-Lysyanskaya signatures as detailed herein under clause 4), as well as U-Prove (based on Brands' work). A more recent example of a multi-message signature scheme capable of selective disclosure is the BBS+ signature scheme (detailed in clause 4.3 and is based on group signatures and the work of Boneh, Boyen, and Shacham, 2004). However, as noted in Camenisch et al. (2013) [i.41], real-world deployments of cryptographic primitives, schemes and protocols in electronic attestations of attributes have been slow due to them being hard to understand and "very difficult to use" as they often require advanced cryptography and the combination of several protocols to achieve the desired privacy goals. In a survey, Asghar (2011) [i.9] lists some of these often employed mechanisms, including blind signatures (Chaum, 1983), ZKPs (Goldwasser, Micali, and Rakoff, 1985), group signatures, commitment schemes (formalized in Brassard, Chaum, and Crépeau, 1988 [i.32]), and multi-message signing; which often need to be employed in tandem to reach privacy goals important for selective disclosure including multi-show unlinkability, blinding, and the ability to present a subset of the signed attestation.

In contrast to the focus on increasing privacy, others sought more performant schemes with lower but still acceptable levels of privacy. A notable example here is the early work of Bull, Stanski, and Squire (2003) [i.35], who presented a way to "enable selective disclosure of verifiable content" using a randomized salt to blind the attribute disclosures, using an identifier for each disclosable attribute, and the principle of signing the hash digests of attributes. To disclose the desired attributes, a user would simply present a subset of the attestation to the verifier, together with the attributes and salts to disclose. Variations of this salted hash digest based approach is used both in the ISO/IEC 18013-5:2001 [i.140] standard and in the IEFT SD-JWT specifications. Note that these techniques do not achieve the same levels of privacy as their more advanced counterparts (e.g. U-Prove, AnonCreds, Idemix, and BBS+) because they lack unlinkability and support for selected predicates, but they are easier to use and more performant.

The academic research of cryptographic schemes for selective disclosure, unlinkability, and predicates have continued from the mid 2010s until present day: Bulletproofs [i.36] and Pointcheval-Sanders Multi-Signatures [i.176] provide range proofs over committed values, whilst zk-SNARKs (clause 4.5.2) are advanced protocols for fully programmable ZKPs. More information about those cryptographic schemes is described in clause 4 of the present document.

The Internet standardization organizations Hyperledger, IETF and W3C® have followed the academic cryptographic research by creating Internet standards for selective disclosure, unlinkability, and predicates. Hyperledger has specified AnonCreds [i.104]. IETF has specified the BBS Signature Scheme [i.116], JSON WebProofs [i.120], PKIX attribute certificates [i.125], and SD-JWT [i.123]. W3C has specified BBS Cryptosuite and the Verifiable Credentials Data Model describes ZKPs [i.209]. Furthermore, ISO/IEC 18013-5 [i.140] specifies selective disclosure for the mobile driving license by introducing the Mobile Security Object (MSO) for the device retrieval use case. Clauses 5 and 6 in the present document describe the mentioned standards in more detail.

Overview and use cases

An overview of various use cases is provided in Figure 1 to illustrate the concepts of selective disclosure, unlinkability, and predicates.

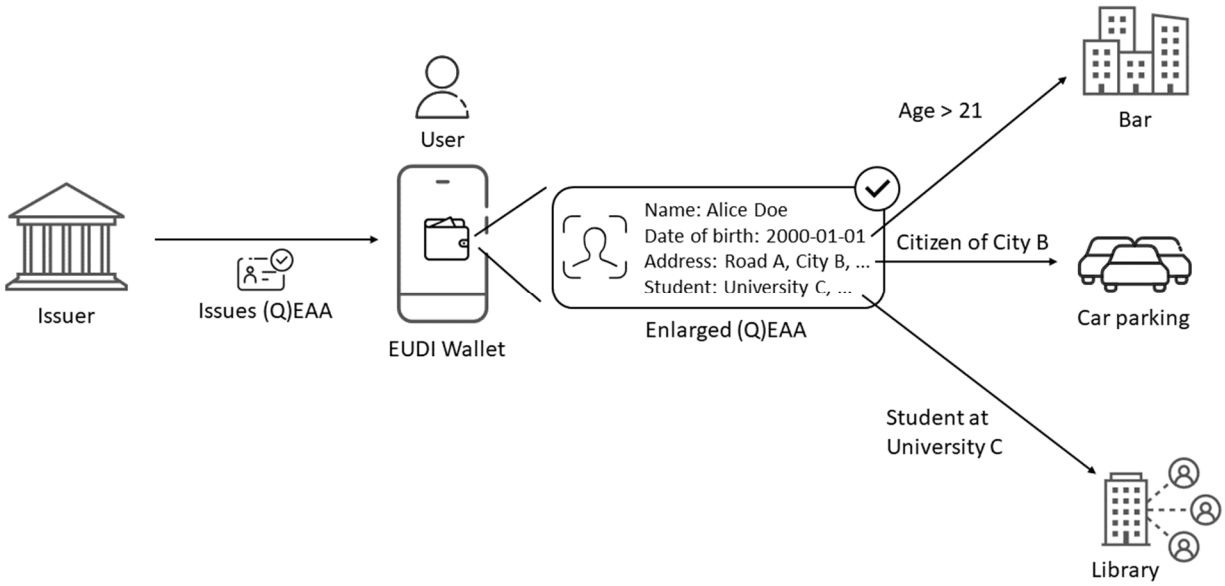

Figure 1: Overview of selective disclosure

First, an issuer creates and issues a (Qualified) Electronic Attestation of Attribute (EAA) (denoted as (Q)EAA) to a user, whereupon the (Q)EAA is stored in the user's EUDI Wallet.

EXAMPLE 1: The (Q)EAA contains the attributes name (first name and last name), date of birth, address (street, city, zip code, etc.), and student information (university, exams, course, etc.).

NOTE 1: The issuer may also issue a Person Identification Data (PID) with the same attributes, but a (Q)EAA is used for readability in this particular example.

The (Q)EAA that is stored in the user's EUDI Wallet is also associated with cryptographic keys that are necessary for the cryptographic scheme's selective disclosure capabilities. In order to access the private keys, the user needs to authenticate with PIN-code or biometrics. Clauses 6.3 and 6.5.3 in the Architecture and Reference Framework (ARF) [i.59] provide more information on the EUDI Wallet security architecture and the supported cryptographic keys management systems.

Now, the user can use its EUDI Wallet to present selected attributes of the (Q)EAA to various relying parties. A user may present multiple attributes to each verifier and is not limited to present only a single attribute claim. The user may also be able to create a presentation that includes claims from at least two (Q)EAAs even if these are issued by different issuers (herein referred to as combined presentation).

When going to a bar, for example, the user may only present a proof that she is over the age of 21 years.

NOTE 2: This is an example of a selective disclosure in combination with a predicate proof. The EUDI Wallet contains the user's actual date of birth (2000-01-01), but the EUDI Wallet only presents a proof that $21 \leq age$.

NOTE 3: This example can also be achieved using selective disclosure of a single attribute. The EUDI Wallet could contain an attestation with the key value pair `"age_over_21": "True"`. This is much simpler from a technical perspective but less flexible.

When parking the car in City B, the user may present a proof that she is a citizen of City B in order to get a discount when paying for the parking ticket. Unlinkability here helps prevent behavioural profiling and the user presents only a proof of knowledge of the undisclosed issuer's signature (the signature is linkable data).

NOTE 4: This can be achieved using a ZKP. The EUDI Wallet only presents a ZKP of knowledge of a valid signature without disclosing said signature. Analogously, a proof of holder binding without revealing the holder's linkable public key may be needed, which can also be given with a ZKP.

When borrowing a book at the university library, the user may only present that she is taking Course D at University C to prove that she is eligible to borrow the course literature.

NOTE 5: This is an example of selective disclosure of a single attribute. The EUDI Wallet contains detailed student information (university, degrees, courses, etc.), but the EUDI Wallet only presents the single claim that user studies at University C.

The concept of verifier unlinkability relates to the amount of additional information that colluding verifiers can discover about the user. High unlinkability means that the colluding verifiers learn little in addition to what the user disclosed to each verifier. Similarly, a single verifier cannot collect multiple selectively disclosed attributes and link them to the same user beyond what is possible solely based on the disclosed attribute values. This requires removing correlatable data (such as the signature) in the presentation to each verifier.

EXAMPLE 2: If presentations are unlinkable, then the bar (who knows that the user is over 21 years) cannot cooperate with the car parking (who knows that the user lives in City B) to link the user's age to the citizenship.

EXAMPLE 3: If presentations are unlinkable, then the user may visit the university library multiple times and present proofs of different courses (Course D, Course E, etc.) over time. The university library cannot link the different courses to the same user.

The concept of issuer unlinkability means that the issuer cannot collude with one or more verifiers to discover where the user is using the issued (Q)EAA. Most ZKP-based systems discussed in the present report provide full unlinkability, i.e. verifier unlinkability and issuer unlinkability.

Descriptions of selective disclosure and unlinkability

The preceding text introduced the terms 'selective disclosure' and 'unlinkability' without providing precise definitions. These terms often have varied interpretations, and these interpretations significantly influence the choice of an appropriate privacy preserving technique. Despite their apparent similarity, selective disclosure and unlinkability are distinct concepts, and their relationship to privacy is complex:

- Selective disclosure involves revealing specific attributes, or claims about these attributes, from a larger dataset. Selective disclosure, on its own, does not guarantee the highest privacy guarantees but may be a key part of a privacy preserving solution.
- Unlinkability relates to the difficulty or cost of linking multiple electronic attestation of attribute presentations. Unlinkability does not inherently ensure privacy but can be a vital element thereof.

Furthermore, the two concepts (selective disclosure and unlinkability) are not binary; they exist on a spectrum or scale, where various degrees or levels exist. And different privacy-preserving techniques are required at different degrees or levels. For selective disclosure, it is possible to understand these levels through a set of requirements:

1) The ability to selectively disclose a minimum of one attribute from a single (Q)EAA.
2) The ability to selectively disclose a minimum of two attributes from at least two distinct (Q)EAAs, with at least one attribute from each (Q)EAA. This ability is sometimes referred to as 'combined presentation'.
3) The user can disclose statements about an attribute rather than the attribute itself. This ability is sometimes referred to as predicate support.

Note that the attributes disclosed do not necessarily have to describe the identity subject. For instance, a disclosure can disclose the EAA type to reveal only that the user has a certain attestation (e.g. passport) without revealing any attribute about the identity subject. Furthermore, the above three requirements relate to other requirements to ensure important capabilities like holder binding (e.g. the verifier has to be assured that the: a) presented attributes cannot be combined in ways that make them appear to be part of another EAA than they originally were, b) presented attributes describe the same identity subject, and c) identity subject is the same entity as is presenting the attributes) and unlinkability.

Relatedly, unlinkability can be understood through a set of requirements. The general requirement relates to the ability to determine whether at least two EAA presentations describe the same identity subject. More precisely, presentations (p1, p2) are unlinkable if a set of entities cannot decide, with a non-negligible probability better than pure guessing based on the presentations and attributes received, whether the two presentations describe the same identity subject. The following cases are possible as unlinkability criteria:

1) The set is a single verifier who seeks to learn whether the attributes describe the same identity subject.