EUROSMART
The Voice of the Digital Security Industry

ETSI's draft technical specification on identity proofing

The objective of this paper is to make recommendations to ETSI's TC ESI for the draft technical specification TS 119 461 V005 "Security and policy requirements for trust service components providing identity proofing for trust services subjects".

Terminology and Intention of the Technical Specification

ETSI ESI's draft defines "identity proofing" as the process of verifying with the required degree of certainty that the identity of an applicant is correct. The scope of this specification is to prove the identity of applicants to qualified and non-qualified trust services. This specification can also be applicable in other areas such as issuing of electronic identity (eID[1]) and Know-Your-Customer (KYC) processes in various industries. This specification does not target identity proofing with low level of confidence[2]. The specification does not target either identity proofing at the level needed for issuing national identity documents.

Eurosmart believes that the overall intention of the technical specification should be clarified, especially when it comes to the applicable areas and possible use cases.

Identity can be defined as information that proves who a person/entity is, for instance a name or date of birth. In other words, it is a collection of characteristics that make a person/entity different from others and hence uniquely identifiable. Partial identity has been defined by ISO/IEC 24760-1[3]; it is a set of attributes related to an entity.

A digital identity is also comprised of characteristics or data attributes that can guarantee the unambiguous identification of a person in the online world and make it possible for this person to rightfully access services.

When it comes to identification, ISO/IEC 24760-1 defines identification as a process of recognizing an entity (3.1.1) in a particular domain (3.2.3) as distinct from other entities, whereby

- The process of identification applies verification to claimed or observed attributes
- Identification typically is part of the interactions between an entity and the services in a domain and to access resources. Identification can occur multiple times while the entity is known in the domain.

[1] Identity proofing used for eID and vice versa: Chicken & Egg problem if the eID root of trust is not defined.
[2] This terminology needs further precision, see corresponding Eurosmart's comments below.
[3] ISO/IEC 24760-1: IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts.

If the technical specification relied on already standardised definitions as the above[4], it would gain more transparency.

Rely on trustworthy identities

In the context of eIDAS and the Regulation on the security of identity cards[5] -introducing mandatory chip and biometrics-, national identity documents (identity cards and passports) and **notified** eIDs **(at least at level "Substantial")** under eIDAS should be the main roots of trust for identity proofing (see 8.1.3.3 "Use of existing eID"). In that respect, those shall always be accepted.

Eurosmart recommends amending the current version of the technical specification to take into account the following principles:

- Only notified eIDs (Art. 9 eIDAS) shall be used for identity proofing purposes. This ensures that the eID scheme underwent a peer review process among EU Member States.
- Only documents recognised as acceptable for identity proofing by applicable laws/regulations shall be accepted.

It is true that eIDAS minimum data set for natural and legal persons is still limited (see Annex A from Implementing Act 2015/1501). Therefore, it is all the more important for ETSI to have a clear scope for the technical specification. Could the data sets provided via eIDAS be sufficient for the envisaged use cases?

Additionally, Eurosmart strongly recommends ensuring consistency with the eIDAS Regulation[6], which is currently in the process of being revised. Consistency with eIDAS means, for instance, that there should be no discrepancies between the Levels of Assurance (LoA), as defined in eIDAS, and the Levels of Identity Proofing which are envisaged in the technical specification. Therefore, a respective mapping of the LoA requirements (basic, substantial, high) should be provided for clarification of the scope i.e. intention of the document.

Clarify the steps of identity proofing

Identity proofing is only one criterion and not the whole process of identification. This point is further developed in the last section of this paper. Moreover, identity proofing is itself comprised of several criteria that unfold as follows:

a. Identity Resolution: is this identity unique?
b. Evidence Validation: is the identity laid on a genuine evidence?
c. Identity Verification: does the evidence match a real person?
d. Relevance of the Issuer: is the issuer of such evidence an authoritative one, a reliable one, who is amenable for such identity delivery?
e. Explicit Reference: is the evidence an original one or a duplicated one, borrowed from another source and, if so, is the source referenced properly?

[4] Whereby additionally the types of data attributes to be covered should be added.

[5] REGULATION (EU) 2019/1157 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

[6] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

In the draft technical specification, the approach shortly described above is not adopted. Eurosmart recommends ETSI to be more precise on the granularity and methodology of identity proofing.

Once the above criteria are all checked (some of them may not necessarily be met), it is still not enough to talk of "identification" because it is mandatory to proceed with other aspects (see last section). Only an exhaustive approach across those aspects can lead to a reliable assessment of level of confidence/assurance that can be trusted by a verifier.

In addition, it is important to rely on **two-factor authentication** to provide a reliable identity proofing. For the binding of the holder, it is necessary to proceed with it separately from identity proofing and to consider additional authentication factors, for instance embedded chip, external physical document or biometrics.

Study the impacts of the use of Server Signing

The use of "Server Signing" is only implicit in the draft technical specification. Every service of the trust service provider may be linked to Identity Proofing if this meets the proprietary requirements of the trust service provider. This might involve server signing.

Centralised identification and signing are two completely independent services, and one cannot rely straightforwardly on the other. Identity proofing could be used in cases where identification is required, such as accessing a service, issuing a certificate or a registered letter.

In case identity proofing is based on the derivation of identity data from a signing certificate whose keys are centralised on a server ("on behalf"), the essential point in this case is the level of guarantee of the associated certificate, of the equipment which protects the keys (SCD), of the provider which hosts the service etc.

This means that server-signing level of assurance is contingent on the caution taken by issuers and trust services to provision or consume identity data and to bind it to a device/a holder, and to ensure holder authentication, and finally to prove data freshness and active status. Depending notably on how well the binding is performed, there may be a variety of levels of confidence/assurance and the signature on server does not necessarily offer a high level of confidence. Said otherwise, in the scale of binding strength, server-signing may be too light.

Server signing seems critical when used in the context of identity proofing, whereby "Identity Proofing", "Device/Holder binding to ID data" and "Holder Authentication" are not clearly separated in the draft technical specification. Therefore, its impact should be explicitly discussed in the technical specification.

Eurosmart recommends correct compliance with CEN (419 241) and ETSI (119 431) standards at the level consistent with the expected eID level. However, because the centralised signature service is itself based on an eID with a certain level (for example low), the derivation of the signature could not be used for creating a top-level eID.

Eurosmart recommends lowering a level when a derivation of identity is involved, from high we would go to substantial. In other words, server signing level high should become identity proofing level substantial.

Use of digital signature means with certificate: safeguards needed

First, in the draft technical specification, the use of Digital Signatures with Certificates will be claimed as identity proof on an equal term with eIDs. Thereby, certificates do not rely on freshness as a typical challenge – response protocol during an authentication process would provide. In Clause 8.1.3.4 "Use of existing digital signature means with certificate", a dynamic factor providing freshness is not required. This aspect should be improved in the technical specification.

Secondly, the possibility of using digital signatures with certificates is a valuable option IF the technical specification puts in place safeguards regarding the primary identity proofing used to deliver the signature certificate. Clause (8.1.3.4) -as it currently stands- is problematic. The use of digital signature means with certificate for identity proofing requires a previous identity proofing so that the applicant could be delivered a signature certificate. Allowing an applicant to use its signature certificate for identity proofing amounts to withdraw this previous identity proofing stage from the scope of the current technical specification.

Eurosmart believes that this Clause raises concerns in terms of Europe's sovereignty and effective control over identity proofing processes. The controls and procedures put in place for the primary identity proofing (to deliver the signature certificate) are ruled by the country where the TSP (providing the signature certificate) is located, not by the country where the identity proofing shall be performed. Concretely, this means that:

1) An applicant could get a signature certificate from a TSP certified/qualified in a non-EU State. Therefore, identity proofing would be ruled by this non-EU State and could be more permissive.

2) This very same applicant subsequently uses his/her signature certificate to prove his/her identity to meet EU legal provisions (e.g. for KYC purposes).

Therefore, Eurosmart recommends to explicitly include the primary identity proofing -required to get the signature certificate- within the scope of the technical specification. This means that this primary identity proofing shall comply with all the requirements set by the technical specification.

In addition, the primary identity proofing shall not rely itself on a signature certificate but only on one of the other methods described in the document – to avoid here again circumventing the requirements and endless recursive requirements.

Link with European and international work for confidence levels

ETSI TC Cyber has just confirmed a liaison with ETSI TC ESI, whereby ESI could use the Expertise of their Experts and vice versa. This is a positive development.

Liaison with other organisations is needed. This is the case of CEN-CENELEC, where a liaison with CEN-CENELEC JTC13 (Cybersecurity and data protection) and other relevant working groups should be envisaged.

In addition, ISO SC17 WG 4 currently works on building blocks for remote identification via mobile devices (working draft ISO/IEC WD4 23220-5). A final document is expected for Q1 2021. It is crucial for ETSI TC ESI to establish a liaison with this work in order to avoid duplication of efforts. ISO's work shows that ETSI draft technical specification -in their current shape- misses some aspects for a comprehensive identity proofing.

Confidence levels should be addressed from four standpoints to lead to a measurable appreciation:

-Identity Proofing: Confidence in the real-life identity of the holder based on the extent to which the issuer collects, validates, and verifies the evidence and attributes provided by the holder. This is about confirming a holder as legitimate Know Your Customer (KYC) target.

- Device-Credential binding: Confidence in the link between the device, the holder, and the holder data.

- Data Freshness and active status: Confidence based on how well the issuer maintains data freshness and its validity status.

- Holder Authentication: Confidence in the extent to which the issuer implements access control on the device such that the data is released under the control of the legitimate data holder. This also considers protection and integrity of the data on the device.

This approach would enable relying parties to comprehensively know how reliable the conveyed data is.

Conclusion

Eurosmart calls for consistency, clarity, and coherence to avoid misinterpretation of the technical specification. ETSI could improve the definition of the scope of the technical specification and clarify some crucial aspects, such as the use of server-signing.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **GS TAG**, **Huawei**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 35 | mail Contact@eurosmart.com