EUROSMART
The Voice of the Digital Security Industry

Too many security gaps in ETSI's document on identity proofing

Context

ETSI is currently drafting a technical specification named "Policy and security requirements for identity proofing of trust service subjects" (TS 119 461). Eurosmart had previously commented[1] version 0.5 of this draft technical specification. In this present document, Eurosmart gives comments on version 0.9 of ETSI's draft technical specification.

ETSI is finalising its work but Eurosmart still has many concerns. It these points are not addressed; the identity proofing process could be flawed and hence would not provide a reliable outcome.

Why does identity proofing matter so much?

Identity proofing is the process of verifying the claimed identity of an applicant. In other words, identity proofing enables an organisation to know whereas a person (applicant) claiming to be "Mr. A" is indeed "Mr. A". The applicant needs to provide evidence of identity, this might be a physical identity document (passport, identity card), an eID or other types of evidence. The level of assurance in the identity will depend on how secure and reliable the process is. The more secure every step of the process is (collection of evidence, validation, binding, issuance) the more reliable the outcome of the process will be.

In the context of ETSI's technical specification, identity proofing is performed for/by trust service providers. This might be, for instance, a trust service provider offering electronic signatures. In this example, the trust service provider needs to verify the identity of the person who wants to get the electronic signature. The trust service provider can verify the identity of the applicant itself or outsource this process to a specialised entity (an Identity Proofing Service Provider - IPSP).

It is therefore the confidence citizens can have in trust services which is at stake. Can I trust this electronic signature? This is nothing less than this question which is at stake.

The technical specification is also designed for other use cases, for instance remote Know-Your-Customer processes. This means that financial sector could apply this document to verify the identity of a person opening a bank account. Here again, it seems crucial to ensure a high level of confidence in the identity.

For these reasons, Eurosmart would like to point out flaws and gives recommendations on the current version of ETSI's technical specification. Identity proofing is too important, these flaws should be corrected before the final version of the document is released. Some comments were previously made

[1] Eurosmart, "ETSI's draft technical specification on identity proofing", published on 12 February 2021.

on the former version of the technical specification but are still relevant for the current version, hence they are reiterated in the present paper.

Clarify the link with eIDAS

The technical specification does not clearly refer to the eIDAS Regulation[2]. This creates confusion. The introduction does not mention eIDAS, and the "Scope" section only mentions eIDAS in a NOTE stating that "[s]pecifically, but not exclusively, the present document aims to support trust services as defined in Regulation (EU) No 910/2014". eIDAS is not mentioned among the references that are necessary for the application of the document, only among the references which are not necessary for its application.

However, the use of the terms "Trust Service Provider" and "Qualified Trust Service Provider" clearly stems from eIDAS. Further in the document, in the "General concepts" section, eIDAS is mentioned[3], confirming that it is the main reference for the definition of a trust service.

Therefore, the paradoxical ambition of the document is to provide technical specification for entities defined by eIDAS while not clearly stating it. It should explicitly state that this technical specification focuses exclusively on requirements for identity proofing of trust services subjects for **eIDAS trust service providers (TSP).** This technical specification could and should have the ambition to stay within the eIDAS framework. This is key for this technical specification to become a reference in the EU. This does not prevent the document from being a source of inspiration for other use cases or geographical contexts. In this case, use for EU/non-EU settings should be made clearer. A stronger link to eIDAS would bring undeniable advantages.

An essential contradiction in the technical specification?

One of the purposes of this technical specification is to harmonise remote identity proofing used for the issuance of qualified certificate as described in article 24(1)(d) of the eIDAS Regulation. The other sections of article 24 being self-explanatory and precise enough ((a), (b), (c)).

Again, it seems paradoxical to have a technical specification aiming at demonstrating compliance of trust service providers with the provision of eIDAS for issuance of qualified certificate pursuant to article 24(1)(d) of eIDAS, while ignoring key principles of the eIDAS Regulation and European laws, namely:

- The document makes no reference to **notified** eIDs pursuant to eIDAS as acceptable means to prove the applicant's identity, but instead introduce the following permissive and loose requirement: "The eID should conform to eIDAS substantial or high" (no mention of the notification mechanism defined in eIDAS);
- Only identity documents that are recognised as acceptable for identity proofing by applicable laws/regulations should be accepted for proving the applicant's identity. Instead, the technical specification introduces the following permissive and loose requirement "if physical identity documents are used as evidence, only passports, national identity cards **and other official**

[2] 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.

[3] "Regulation (EU) 910/2014 of the European parliament and of the council [i.1] (the eIDAS Regulation) does not define identity proofing as a trust service on its own, but identity proofing can be defined as a component of a trust service.", page 12.

identity documents that offer a comparable level of assurance in the identity should be accepted"

In Eurosmart's views, this is a major contradiction within this work, that deserves a clarification. Should this technical specification aim to support the implementation of Article 24(1)(d) of eIDAS, it shall also acknowledge and take into consideration all principles stemming from eIDAS, as well as the provisions of all other applicable European laws.

Prescribe the use of notified eIDs with minimum level of assurance "Substantial"

The technical specification foresees the use of existing eID as evidence (8.2.4). "The eID should conform to eIDAS substantial or high". eID level Basic has been discarded, this is a move that Eurosmart welcomes. However, conformity to level substantial or high should be a requirement, not a recommendation. Therefore, "shall" must replace "should" in this sentence.

In addition, the technical specification should prescribe the use of **notified** eID pursuant to eIDAS. The process of notification guarantees that the eID has undergone a peer review among the EU Member States. This means that other Member States evaluate the level of confidence and trust that can be granted to the eID at stake. Therefore, notification ensures trustworthiness. It is not acceptable to have a trust service provider operating in the EU and relying on non-notified eIDs, potentially level basic, for its identity proofing. There would be here a wide security gap.

Lack of clear mapping with levels defined in eIDAS

The technical specification defines two levels of assurance for identity proofing (LoIP): Baseline Level of Identity Proofing (Baseline LoIP) and Enhanced Level of Identity Proofing (Enhanced LoIP). These two levels are neither aligned with nor related to the eIDAS levels "Substantial" and "High" for digital identity, or with the requirements for the issuance of qualified certificate as defined in eIDAS.

Additionally, Eurosmart finds very odd to require an eID at level "Substantial" or "High" for both Baseline LoIP and Enhanced LoIP. With such an approach, it is hardly possible to add value to existing eIDs notified under eIDAS at level "High", as they do not bring supplemental benefits compared to the ones notified at level "Substantial".

The levels of assurance should be re-worked and aligned as follows: Baseline LoIP becomes "IP matching eIDAS substantial" and Enhanced LoIP becomes "IP matching eIDAS high".

Rely on recognised national identity documents

Passports and identity cards have well-defined and harmonised security features -especially since the adoption of the EU Regulation on the security of identity cards[4]. They are therefore ideal evidence for identity proofing. ETSI's technical specification also envisages the use of other physical identity documents as evidence. The document states that "[i]f physical identity documents are used as evidence, only passports, national identity cards and other official identity documents that offer a comparable level of assurance in the identity should be accepted" (8.2.3-04).

[4] REGULATION (EU) 2019/1157 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20June 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

This mention of identity documents "that offer a comparable level of assurance" is subjective and hence subject to interpretation. This should be replaced by the following requirement: only passport, national identity cards and other official identity documents that are recognised as acceptable for identity proofing by applicable laws/regulations **shall** be accepted.

Clear distinction between physical identity documents and digital identity documents

The distinction between physical identity documents and digital identity documents is unclear in the technical specification and may create substantial confusion. The proposed definition of a digital identity document reads "an identity document that is issued in machine-processable form and that is digitally signed by the issuer". As such, it is unclear whether the digital identity document contains the physical identity document (when applicable) or not. It is of the utmost importance to clearly define concepts, as many identity documents are both physical identity documents and digital identity documents (e.g. eMRTD – electronic passport - is both a digital identity document and a physical identity document), and may be used in both ways, depending on the choice/capacities of the IPSP/TSP. For instance, an IPSP/TSP that is only able to control physical identity document will see eMRTD as a physical identity document, while another one that is able to and needs to use the digital part will see it as a digital electronic document, and a third one able to use both parts (physical and digital) and for which the user only wants to use the physical part will see it as a physical identity document. Even if it is the same identity document, with the same characteristics, different features will be at stake depending on the situation.

According to the case, the requirements/considerations will not apply to the same part of the identity document. As such, Eurosmart calls for a clear definition of both concepts of physical identity document and digital identity document to distinctly identify which features of the identity document are covered by which requirements. Eurosmart proposes to see an identity document in a generic manner as being made up with a (1) a physical identity document (part) and (2) a digital identity document (part) that are mutually exclusive. Each of them being exploited in different manners in the course of remote identity proofing. Therefore, to avoid ambiguities in the implementation of requirements, there should not be any overlaps in the definitions of physical identity document and digital identity document, and they should be exclusive.

Eurosmart believes that a digital identity document should be defined as follows: "an identity document that is issued in machine processable form, that is digitally signed by the issuer, and that is in a purely digital format". A note should be added to state that a digital identity document may be contained in a physical identity document (e.g. eMRTD).

The definition of the physical identity document should also be refined to underline the fact that the main characteristic of a physical identity document is that it is issued in physical form.

Last but not least, it is also worth mentioning here that automated means and machine-learning technology are not applicable in any manner for digital identity documents. The technical specification states the following:

[CONDITIONAL] VAL-8.3.2-07: *If automated means and machine-learning technology are used for analysis of the photo obtained from a digital identity documents, the analysis should apply measures to detect morphed photos in identity documents.*

> *NOTE 6: A morphed photo is created by merging the face photos of two or more different persons into one photo. Since some countries allow persons to bring their own photo for the issuing of a passport or national identity card, there is a risk that documents are issued with morphed photos. With a morphed photo, there is a risk that both/all the persons can be recognized both by a human registration officer and by face biometrics with an assurance*

above the applied threshold, meaning more than one person can use the identity document containing the morphed photo.

The main difference between physical identity document and digital identity document is that the latter provides means to ensure the holder photo has not been tampered with after issuance thanks to cryptographic methods (e.g. digital photo is protected by a digital seal). Therefore, this requirement is not only useless for digital identity document but also not relevant and shall be removed.

Create safeguards when digital signature means are used as evidence

In this section, Eurosmart would like to reiterate previous comments.

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 8.2.5 "Use of existing digital signature means as evidence", 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 8.2.5 -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 withdrawing 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 trust service provider (providing the signature certificate) is located, not by the country where the identity proofing is performed. Concretely, this means that:

1) An applicant could get a signature certificate from a trust service provider 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.

Study the impacts of the use of server signing

In this section too, Eurosmart would like to reiterate previous comments.

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.

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.

Thus, 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 Baseline LoIP.

Correctly address the issue of morphing

The technical specification states the following regarding morphing:

[CONDITIONAL] VAL-8.3.3-19: *If automated means and machine-learning technology are used for analysis of physical identity documents, the analysis should apply measures to detect morphed photos in identity documents.*

> *NOTE 11: A morphed photo is created by merging the face photos of two or more different persons into one photo. Since some countries allow persons to bring their own photo for the issuing of a passport or national identity card, there is a risk that documents are issued with morphed photos. With a morphed photo, there is a risk that both/all the persons can be recognized both by a human registration officer and by face biometrics with an assurance above the applied threshold, meaning more than one person can use the identity document containing the morphed photo.*

While Eurosmart fully supports the concern of morphing, the requirement as such is incorrect and not relevant.

First of all, the morphing on the holder photo is a threat in the course of the issuance of the identity document where the applicant submits a photo combining his portrait but also others'. This is the reason why application procedure for identity documents requires applicant to show up at least once. After the identity document has been issued, there is no way to tell that the photo has been morphed by only looking at it. Eurosmart can only regret that there are no technical means to detect morphing. This is a regrettable fact but also an objective one. Therefore, when the technical specification recommends morphing detection, it is recommending something impossible. Eurosmart strongly advises to review this requirement to remove it.

By contrast, it is possible to detect if the photo printed on the identity document has been tampered with after the identity document has been issued. This is a classical forgery method consisting in slightly modifying the genuine photo (by adding or removing tiny bits of inks) so that it matches another person (the attacker). Eurosmart recommends updating the technical specification to

mandate detection on physical identity document of printed photo that has been tampered with (by adding or removing tiny bits of inks so that it matches another person).

Also, as discussed in the section "Clear distinction between physical identity documents and digital identity documents", and as discussed in this section, Eurosmart recommends deleting the following requirement dealing with morphing for digital identity document as it is useless and not relevant.

[CONDITIONAL] VAL-8.3.2-07: *If automated means and machine-learning technology are used for analysis of the photo obtained from a digital identity documents, the analysis should apply measures to detect morphed photos in identity documents.*

> *NOTE 6: A morphed photo is created by merging the face photos of two or more different persons into one photo. Since some countries allow persons to bring their own photo for the issuing of a passport or national identity card, there is a risk that documents are issued with morphed photos. With a morphed photo, there is a risk that both/all the persons can be recognized both by a human registration officer and by face biometrics with an assurance above the applied threshold, meaning more than one person can use the identity document containing the morphed photo.*

Nevertheless, whether a physical identity document or a digital identity document is used, it is possible to detect a morphed photo in the course of biometric authentication, where the photo and the face of the holder are compared (binding phase). In the case of morphed photo, the correlation between both will be lower. However, as for biometric comparison, the detection of morphed photo cannot be absolute (100%). It can only meet a given probability of detection. Eurosmart recommends introducing a requirement in the binding to applicant phase: morphed photos in identity documents (physical or digital) shall be detected with a probability of at least 95%.

Security of Presentation attack detection (PAD) for biometric capture

When the remote identity proofing involves the capture of biometry (e.g. capture of the face of the applicant to check it matches the one on the identity document), the technical specification provides for measures to ensure the biometric capture is protected against spoofing attacks. In that regards, the document requires the biometric device to support presentation attack detection (PAD) methods that are evaluated according to ISO/IEC 19989-3.

BIN-8.4.2-07*: The PAD should be evaluated according to ISO/IEC 19989-3.*

> *NOTE 6: ISO/IEC 19989-3 specifies security evaluation of PAD applying Common Criteria (ISO/IEC 15408).*

Eurosmart welcomes this proposal. However, it seems very strange to have such a precise security requirement covering capture of biometrics, while other aspects of the technical specification lacks basic security considerations (e.g. requirement on identity proofing for issuance of signature certificate used for remote identity proofing). Eurosmart considers that security considerations shall be homogenous throughout the entire document.

In addition, the requirement seems incomplete, and may rather allow for more fragmentation than harmonisation. The content, expertise and work at stake in an "evaluation" may be diverse and left up to the evaluation laboratories. This is the role of a certification authority (and thus a certification scheme) to ensure evaluations are properly carried out with the right level of expertise, skills and work,

and also to ensure homogeneity of evaluations across evaluation laboratories. For these reasons, Eurosmart believes this requirement shall not mandate a simple evaluation but a security certification.

Secondly, this security certification -which is based on common criteria as recalled in the note below this requirement- shall leverage on the Cybersecurity Act (Regulation 2019/881) and be performed in accordance with the EU CC scheme.

Towards more harmonisation or more fragmentation?

Eurosmart warmly welcomes this technical specification and considers that this document is of the utmost importance. Eurosmart believes that this technical specification shall foster harmonisation of remote identity proofing across Europe and eliminate diverging implementations. It should play a key role in the development of the Digital Single Market especially in the field of financial industry and trust services by providing harmonised procedure for remote Know Your Customer and qualified certificate issuance.

However, Eurosmart is concerned with the current content of the technical specification that globally undermines harmonisation in a substantial way. First of all, the requirements contained in the document shall define clear obligations that shall be applied to ensure harmonisation. Unfortunately, many of them make use of keywords such as “should” or “may”, which only imply a recommendation or a possibility, but not an obligation. Therefore, it would be possible for entities claiming compliance with this technical specification not to abide by these requirements. Secondly, the technical specification contains statements allowing alternate implementations of requirements without clearly defining them (“comparable” used 8 times). It constitutes loopholes that could be diverted to make nearly any implementation fit within the scope of the technical specification.

Eurosmart considers that all of these are major flaws, which will not only substantially undermine harmonisation, but seriously increase divergences of solutions across market, with indeed various levels of security. This is not something that Eurosmart would like to see.

Eurosmart calls for an editorial update of the technical specification so that it takes into consideration these two principles enacted above:

- Requirements written as obligations (without “should” or “may, but with “shall” instead);
- No wording that could constitute a loophole.

Last but not least, the issue highlighted in section “Create safeguards when digital signature means are used as evidence” also constitutes a major aspect substantially undermining the process of remote identity proofing, especially the trust that one can put in it.

Conclusion

Eurosmart strongly encourages ETSI TC ESI to correct the major security flaws that are found in the current version of the document. Eurosmart remains very supportive of the work currently carried out by ETSI TC ESI. ETSI can count on Eurosmart’s active contribution for this document.

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**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **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