ETSI TS 119 461 V2.1.1 (2025-02)

TECHNICAL SPECIFICATION

Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

Reference

RTS/ESI-0019461v211

Keywords

electronic signature, security, 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

Important notice

The present document can be downloaded from the ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

Introduction

Identity proofing is the process of verifying with the required degree of reliability that the purported identity of an applicant is correct. The scope of the present document is identity proofing of applicants to be enrolled as subjects or subscribers of a Trust Service Provider (TSP).

Identity proofing can be carried out by the TSP as an integral part of the trust service provisioning. It can also be the task of a specialized Identity Proofing Service Provider (IPSP) acting as a subcontractor to the TSP; such a separate IPSP can provide services to several TSPs. The present document applies to both of these scenarios.

The present document aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst others, applicable requirements from both the original eIDAS regulation published in 2014, Regulation (EU) No 910/2014 [i.1], and the amended eIDAS regulation [i.25] incorporating legal amendments approved in 2024 [i.34].

The present document poses policy and security requirements specific to identity proofing covering applicable technologies and use cases, resulting in identity proofing to either a Baseline or an Extended Level of Identity Proofing (LoIP) that are considered applicable to all relevant ETSI trust services standards.

Since neither the original eIDAS regulation [i.1] nor the amended eIDAS regulation [i.25] define identity proofing as a trust service on its own, a specialized IPSP is not a TSP per se, but acts under the responsibility of the TSP that has subcontracted the identity proofing. The IPSP will provide a component of the TSP's trust service, hence the name of the present document refers to policy and security requirements for identity proofing as a trust service component.

1 Scope

The present document specifies policy and security requirements for trust service components providing identity proofing of trust service subjects. Such a trust service component can be provided by the Trust Service Provider (TSP) itself as an integral part of the trust service or by a specialized Identity Proofing Service Provider (IPSP) acting as a subcontractor to the TSP. The term "trust service component" is used because identity proofing is not considered as a trust service on its own but as a component of the trust service for which the identity proofing is done.

The present document provides requirements for two Levels of Identity Proofing (LoIP), Baseline and Extended. These LoIPs aim to support identity proofing for ETSI trust services standards such as ETSI EN 319 411-1 [i.7], ETSI EN 319 411-2 [i.8] and ETSI EN 319 521 [i.12]. The present document also provides requirements to enhance an identity proofing from Baseline LoIP to Extended LoIP when the Baseline LoIP has been reached by use of electronic Identification means (eID) at Level of Assurance (LoA) 'substantial' according to the amended eIDAS regulation [i.25] or a similar LoA based on a comparable assurance level framework.

The present document aims at supporting identity proofing in European and other regulatory frameworks. Specifically, but not exclusively, the Baseline LoIP aims to support identity proofing for qualified certificates as defined in Regulation (EU) No 910/2014 [i.1] (the original eIDAS regulation) Article 24.1, while the Extended LoIP aims to support identity proofing for qualified certificates and qualified attestations of attributes as defined in Articles 24.1, 24.1a, and 24.1b of the amended eIDAS regulation [i.25]. The present document aims to meet the requirements of the original eIDAS regulation [i.1] by the requirements in clause C.2 and the requirements of the amended eIDAS regulation [i.25] by the requirements in clause C.3.

The present document is intended to be applicable for reference from an implementing act according to Article 24.1c of the amended eIDAS regulation [i.25], setting out minimum technical specifications, standards and procedures with respect to the verification of identity and attributes in accordance with Articles 24.1, 24.1a, and 24.1b of the amended eIDAS regulation [i.25].

The present document aims to meet the requirements of Article 44 of the aforementioned regulations on identity proofing for qualified electronic registered delivery services by the requirements in clause C.4. eIDAS has no specific requirements for identity proofing for other qualified trust services.

The present document can be used by Conformity Assessment Bodies (CAB) as the basis for confirming that an organization is trustworthy and reliable in its identity proofing process.

NOTE 1: See ETSI EN 319 403-1 [i.6] for guidance on the assessment of TSP processes and services.

NOTE 2: The present document has the potential to have wider applicability than the defined scope, but any application for other purposes than trust services is out of scope.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[2] ICAO Doc 9303 part 10: "Machine Readable Travel Document - Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)".

[3] ISO/IEC 30107-3: "Information technology — Biometric presentation attack detection — Part 3: Testing and reporting".

[4] ISO/IEC 19795-1: "Information technology — Biometric performance testing and reporting — Part 1: Principles and framework".

[5] TS 18099: "Biometric data injection attack detection", (produced by CEN).

[6] ISO/IEC 19989-3: "Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection".

[7] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) 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.

NOTE: The eIDAS regulation as published in 2014 and before amendments approved in 2024, sometimes called "eIDAS v1", shorthand notation "original eIDAS regulation".

[i.2] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

[i.3] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.4] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.5] ETSI EN 319 102-1: "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.6] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.7] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.8] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.9] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[i.10] Void.

[i.11] Void.

[i.12] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.13] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[i.14] Void.

NOTE: Moved to normative reference [7].

[i.15] ENISA: "Remote ID proofing - Analysis of methods to carry out identity proofing remotely", February 2021.

[i.16] ISO/IEC 30107-1: "Information technology — Biometric presentation attack detection — Part 1: Framework".

[i.17] Void.

NOTE: Moved to normative reference [4].

[i.18] Void.

NOTE: Moved to normative reference [6].

[i.19] ISO/IEC TS 29003: "Information technology — Security techniques — Identity proofing".

[i.20] Facial Identification Science Working Group (FISWG): "Facial Comparison Overview and Methodology Guidelines", Version 1.0, October 2019.

[i.21] Facial Identification Science Working Group (FISWG): "Facial Image Comparison Feature List for Morphological Analysis", Version 2.0, September 2018.

[i.22] Facial Identification Science Working Group (FISWG): "Minimum Training Criteria for Assessors Using Facial Recognition Systems", Version 1.0, July 2020.

[i.23] European Network of Forensic Science Institutes (ENFSI): "Best Practice Manual for Facial Image Comparison", ENFSI-BPM-DI-01, Version 01, January 2018.

[i.24] ISO/IEC 15408-1: "Information technology — Security techniques — Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.25] 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, consolidated version: 18/10/2024.

NOTE: The eIDAS regulation including the amendments of Regulation (EU) 2024/1183 [i.34], sometimes called "eIDAS v2", shorthand notation "amended eIDAS regulation".

[i.26] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.27] Public Register of Authentic Travel and Identity Documents Online (PRADO): "Glossary - Technical terms related to security features and to security documents in general".

[i.28] ENISA: "Methodology for Sectoral Cybersecurity Assessments", EU Cybersecurity Certification Framework, September 2021.

[i.29] ISO/IEC 19792: "Information technology — Security techniques — Security evaluation of biometrics".

[i.30] ISO/IEC 19989-1: "Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework".

[i.31] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services.

[i.32] ISO/IEC FDIS 29794-5: "Information technology — Biometric sample quality — Part 5: Face image data".

[i.33] ISO/IEC DIS 20059: "Information technology — Methodologies to evaluate the resistance of biometric recognition systems to morphing attacks".

[i.34] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.4], ETSI EN 319 401 [1] and the following apply:

amended eIDAS regulation: Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183 and Directive (EU) 2022/2555

NOTE: The combination of the original eIDAS regulation [i.1] published in 2014 and the identified amendments approved in 2024, sometimes called "eIDAS v2" - see **original eIDAS regulation** below.

applicant: person (legal or natural) whose identity is to be proven

attack potential: measure of the effort needed to exploit a vulnerability in a Target Of Evaluation (TOE)

NOTE: Source ISO/IEC 15408-1 [i.24], which has the following note to the definition: The effort is expressed as a function of properties related to the attacker (e.g. expertise, resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure).

Attack Presentation Classification Error Rate (APCER): proportion of attack presentations using the same presentation attack instrument species incorrectly classified as bona fide presentations in a specific scenario

NOTE: Source ISO/IEC 30107-3 [3]. Measure for rate of successful presentation attacks.

attended remote identity proofing: identity proofing process by remote use of identity document where the capture of the identity document (physical or digital document) and the face video of the applicant are performed in a session supervised by a registration officer

authentic source: repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognized as authentic in accordance with Union or national law, including administrative practice

NOTE: Source amended eIDAS regulation [i.25]. In the present document, the term "trusted register" is used as the general term while "authentic source" is used where the scope is explicitly the eIDAS legal context.

authoritative evidence: evidence that is presented by the applicant, holds identifying attribute(s) of the identity, and is trusted for the binding of these attributes to the applicant

NOTE: In the present document, authoritative evidence for a natural person is a physical or digital identity document, an eID used for authentication, and a certificate of a digital signature. For a legal person, documents and attestations are typically used as authoritative evidence.

authoritative source: any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity

NOTE: Source CIR (EU) 2015/1502 [i.3]. Authoritative evidence is an authoritative source, but also trusted register and other sources can be authoritative sources. Use can be to supply more attributes than those obtained from authoritative evidence, to validate attributes obtained from different sources, and to provide more updated attributes than those obtained from authoritative evidence.

(identity) attribute: characteristic, quality, right or permission of a natural or legal person or of an object

NOTE: Source amended eIDAS regulation [i.25].

Baseline LoIP: Level of Identity Proofing (LoIP) reaching a substantial level of confidence based on the fulfilment of good practice minimum requirements for the identity proofing process

NOTE: This level is considered suitable for identity proofing for the NCP policy level defined in ETSI EN 319 411-1 [i.7] and for issuing qualified certificates according to the original eIDAS regulation [i.1].

binding to applicant: part of an identity proofing process that verifies that the applicant is the person identified by the presented evidence

Bona fide Presentation Classification Error Rate (BPCER): proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

NOTE: Source ISO/IEC 30107-3 [3]. Measure of genuine presentations incorrectly classified as presentation attacks.

digital identity document: identity document that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form

NOTE 1: Machine-processable, in this case, does not include optical scanning and processing of a physical identity document.

NOTE 2: A digital identity document can be contained in a physical identity document, e.g. an eMRTD contained in a passport or national identity card.

NOTE 3: The eMRTD part of a passport or national identity card is sometimes called "electronic identity" or even "eID". In the present document, this part of a passport or national identity card is a digital identity document.

electronic attestation of attributes: attestation in electronic form that allows attributes to be authenticated

NOTE: Source amended eIDAS regulation [i.25]. In the present document, the term "attestation" is used as the general term while "(qualified) electronic attestation of attributes" is explicitly used in the eIDAS legal context.

electronic Identification means (eID means, eID): material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service

NOTE: Source amended eIDAS regulation [i.25].

eID scheme: governance model and technical specifications allowing interoperability between eID means from different eID providers

eIDAS certified eID: eID or eID scheme certified according to Article 12a of the amended eIDAS regulation

eIDAS high eID: eID or eID scheme fulfilling the requirements for assurance level high in Article 8 of the amended eIDAS regulation and CIR (EU) 2015/1502

eIDAS notified eID: eID or eID scheme notified according to Article 9 of the amended eIDAS regulation

eIDAS signature validation: validation of an electronic signature or electronic seal in compliance with the eIDAS regulation

NOTE: Requirements for validation of signatures and seal are set by Article 32 of the amended eIDAS regulation [i.25]. The text of Article 32 is the same in the original [i.1] and the amended eIDAS regulation [i.25].

eIDAS substantial eID: eID or eID scheme fulfilling the requirements for assurance level substantial in Article 8 of the amended eIDAS regulation and CIR (EU) 2015/1502

NOTE: The text of Article 8 and Article 9 is the same in the original [i.1] and the amended [i.25] eIDAS regulation. CIR (EU) 2015/1502 [i.3] has not changed with the amended eIDAS regulation [i.25].

(identity) evidence: information or documentation provided by the applicant or obtained from other sources, trusted to prove that claimed identity attributes are correct

extended LoIP: Level of Identity Proofing (LoIP) reaching a high level of confidence based on the fulfilment of good practice minimum requirements for the identity proofing process

NOTE: This level is considered suitable for identity proofing for issuing of qualified certificates and qualified electronic attestations of attributes according to the amended eIDAS regulation [i.25].

False Acceptance Rate (FAR): proportion of verification transactions with false biometric claims erroneously accepted

NOTE: Source ISO/IEC 19795-1 [4].

False Rejection Rate (FRR): proportion of verification transactions with true biometric claims erroneously rejected

NOTE: Source ISO/IEC 19795-1 [4].

freshness: time between time of issuance of an evidence and time of use/validation of the evidence

high attack potential: measure of the effort needed by a highly skilled adversary with significant resources and opportunity to exploit a vulnerability in a Target Of Evaluation (TOE)

NOTE: Based on ENISA: "Methodology for Sectoral Cybersecurity Assessments" [i.28].

identity: attribute or set of attributes that uniquely identify a person within a given context

identity document: physical or digital identity document issued by an authoritative source and attesting to the applicant's identity

identity proofing context: external requirements affecting the identity proofing process, given by the purpose of the identity proofing, the related regulatory requirements, and any resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself

identity proofing (process): process by which the identity, and possibly additional attributes, of an applicant is verified by the use of evidence attesting to the required identity attributes

identity proofing service policy: set of rules that indicates the applicability of an identity proofing service to a particular community and/or class of application with common security requirements

injection attack: attack consisting of injecting content controlled by the attacker into the data capture process

EXAMPLE: Bypassing the camera on the user device injecting a recorded or generated video stream purporting to come from the camera. A generated video stream can be a deep fake video of a face or of the visual appearance of a physical identity document.

Injection Attack Detection (IAD): automated determination of an injection attack

legitimate evidence holder: person for whom the evidence is issued

Level of Identity Proofing (LoIP): confidence achieved in the identity proofing

NOTE 1: Source ISO/IEC TS 29003 [i.19].

NOTE 2: In the present document, the term applies to the Baseline LoIP and the Extended LoIP.

liveness detection: measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture

NOTE: Source ISO/IEC 30107-1 [i.16]. Liveness detection is a subset of presentation attack detection.

moderate attack potential: measure of the effort needed by a skilled adversary with significant resources and opportunity to exploit a vulnerability in a Target Of Evaluation (TOE)

NOTE: Based on ENISA: "Methodology for Sectoral Cybersecurity Assessments" [i.28].

original eIDAS regulation: Regulation (EU) No 910/2014 as published in 2014 and without the amendments approved in 2024

NOTE: Sometimes called "eIDAS v1" - see **amended eIDAS regulation** above.

physical identity document: identity document issued in physical and human-readable form

EXAMPLE: The printed (non-digital) representation of passports and national identity cards.

physical presence: identity proofing where the applicant is required to be physically present at the location of the identity proofing

(IPSP) practice statement: statement of the practices that an IPSP employs in providing the identity proofing trust service component

NOTE: Source ETSI EN 319 401 [1].

presentation attack: presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

NOTE: Source ISO/IEC 30107-1 [i.16].

Presentation Attack Detection (PAD): automated determination of a presentation attack

NOTE: Source ISO/IEC 30107-1 [i.16].

proof of access: any source irrespective of its form that can be trusted for reliable data, information and/or evidence that can be used in an identity proofing process, provided that the applicant is able to demonstrate access to the source

EXAMPLE: Bank account, phone number, email or other resource owned by the applicant.

pseudonym: fictitious identity that a person assumes for a particular purpose, which differs from their original or true identity

NOTE: A pseudonym identity can, as opposed to an anonymous identity, be linked to the person's real identity.

qualified electronic seal: advanced electronic seal, which is created by a qualified electronic seal device, and that is based on a qualified certificate for electronic seal

NOTE: Source amended eIDAS regulation [i.25].

qualified electronic signature: advanced electronic signature, which is created by a qualified electronic signature device, and that is based on a qualified certificate for electronic signature

NOTE: Source amended eIDAS regulation [i.25].

registration officer: human being carrying out all or selected parts of an identity proofing process

remote identity proofing: identity proofing process where the applicant is physically distant from the location of the identity proofing

subject: legal or natural person that is enrolled to a trust service

subscriber: legal or natural person bound by an agreement with a trust service provider to any subscriber obligations