

Identity Validation Requirements for Certificate Issuance and Revocation by Registration Authorities

Version information		
Date	Version	Changes
23.09.2026	10.0	New version of Annex 2 that is restructured according to ETSI TS 119 461 V2.1.1.
06.12.2024	9.1	References updated.
19.01.2024	9.0	Main changes: • exceptions regarding national identity document validity defined; • explanations and requirement updated regarding re-use of existing evidence regarding national identity documents used in identity proofing process; • alternative controls regarding four-eye principle shall be approved by TSP; • some minor updates for clarification were added.
18.10.2021	8.0	Added: • references to normative requirement documents; • requirements related to physical document inspection and RA officer training; • requirements related to identity proofing and binding to applicant; • The back-office four-eye check was removed. • Document is restructured and removed requirement citations as for better understanding. • Source references updated.
19.08.2019	7.0	Added requirements related to non-qualified certificate issuance to non-residents and residents, which do possess the national identity document of Estonia, Latvia or Lithuania.
14.06.2019	6.0	This annex is applicable also to the non-qualified certificate issuance and revocation in RA office for policy +NCP.
26.11.2018	5.0	QES as one of the options for subscriber verification is added.
10.04.2018	4.1	References to the new versions of ETSI standards.
19.11.2017	4.0	Requirements for alternatives for four-eye control was added.
12.10.2017	3.0	Requirements for identity validation for revocation of certificates via Helpline was added.

23.02.2017	2.0	Requirements for identity validation for qualified certificate revocation was added (paragraph 2).
22.01.2017	1.1	Removed reference to Smart-ID.
15.11.2016	1.0	Initial draft.

Terms and Acronyms

Term	Definition
Certificate	Public Key, together with additional information, laid down in the Certificate Profile for Smart-ID, rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
eIDAS	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.
Legal Representative	A natural person who is authorised by law to represent minor.
Non-Qualified Smart-ID	Smart-ID which contains one pair of Certificates consisting of the Authentication Certificate and the non-qualified Electronic Signature Certificate, issued in accordance with the Certificate Policy for non-qualified Smart-ID, published at https://www.skidsolutions.eu/resources/certificate-policies/ .
Qualified Smart-ID	Smart-ID which contains one pair of Certificates consisting of the Authentication Certificate and the qualified Electronic Signature Certificate, issued in accordance with the Certificate Policy for qualified Smart-ID, published at https://www.skidsolutions.eu/resources/certificate-policies/ .
Registration Authority (RA)	Swedbank, an entity that is responsible for identification of the Smart-ID User and accepts Certificate applications, checks the applications and forwards the applications to the Certificate Authority.
SK	SK ID Solutions AS, Certification Service provider.
Smart-ID	Smart-ID is the electronic ID which provides the Smart-ID User with means for Electronic Authentication and (qualified and non-qualified) Electronic Signature.

Subscriber	An individual or entity that has established a relationship with the bank by opening an account or availing other financial services offered by the bank.
-------------------	---

References to Normative Requirements

1. eIDAS - 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;
2. 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, <https://eur-lex.europa.eu/eli/reg/2024/1183>;
3. EITSA - Electronic Identification and Trust Services for Electronic Transactions Act, <https://www.riigiteataja.ee/en/akt/530122025007>
4. 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, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002
5. ETSI EN 319 411-1 V1.5.1, Electronic Signatures and Trust Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.05.01_60/en_31941101v010501p.pdf
6. ETSI EN 319 411-2 V2.6.1, Electronic Signatures and Trust Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.06.01_60/en_31941102v020601p.pdf
7. ETSI EN 319 461 V2.1.1, (February 2025), Electronic Signatures and Trust Infrastructures; Policy and security requirements for trust service components providing identity proofing of trust service subjects https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/02.01.01_60/ts_119461v020101p.pdf

General Statements

The following controls define the identity proofing requirements applicable to the issuance and revocation of certificates, including:

- qualified certificates for electronic signatures under policy QCP-n-qscd/LoA High; and
- electronic signature certificates under policy NCP+/LoA Substantial;
- authentication certificates conformant to LoA High.

1. Identity Validation Requirements for Certificate Issuance

Number of controls	Name of controls	Controls for certificate issuance	Source
1.	Attribute and evidence collection	A subscriber (natural person) shall be verified: - by physical presence In case identity proofing by physical presence, attributes and evidence shall be collected using: - a national identity document; which - is a physical identity document; and - is presented in its original form; - contains a facial image; and - is recognized in EU (non-exhaustive list is available at: https://www.consilium.europa.eu/prado/en/prado-recognised-documents.html); - digital identity documents (e.g., LT printable digital residence permits) may be used as supplementary evidence in justified cases, but shall only be treated as supporting documentation and not as an authoritative identity evidence; - A legal representative shall be verified according to the above requirements and shall provide a Confirmation of Legal Representation as additional evidence. National identity documents that are driving licenses and documents with temporary or emergency nature shall not be accepted. The following attributes shall be collected: - family name(s), first name(s), which should be current names; - personal identity code (EE, LV, LT);	eIDAS regulation, article 24 clause 1a ETSI TS 119 461 9.2.1 USE-9.2.1.1-01, USE-9.2.1.1-02, USE-9.2.1.1-03, USE-9.2.1.1-05, USE-9.2.1.2-03X ETSI TS 119 461 8.2.2 COL-8.2.2.1-01X, COL-8.2.2.1-02, COL-8.2.2.1-03, COL-8.2.2.1-04 ETSI TS 119 461 8.2.3 COL-8.2.3-01X, COL-8.2.3-02X, COL-8.2.3-03X,

		- In case where personal identity code does not contain the date of birth (e.g., in case of new generation Latvian personal identity codes), date of birth shall be collected additionally; - If a person applies for a non-qualified Smart-ID and does not hold a personal identity code issued in either EE, or LV, or LT, then such attributes as date of birth and identity document number shall be collected. The personal data (person's name and personal identity code) from national identity document shall match 100% with the data on the application. If during the attribute collection, only one RA officer is physically present, then, for the purposes of the back-office four-eyes control (see Sect. 2 and 3), the RA officer shall record evidence of the subscriber's presence at the RA office (e.g., taking a photo of the subscriber that shows their presence at the RA office). The RA shall not collect additional identity attributes, unless such attributes are strictly necessary for the purposes of identity attribute validation and/or binding the applicant to the provided evidence.	COL-8.2.3-04X, COL-8.2.3-05X Risk assessment
2.	Attribute and evidence validation	In case of identity proofing by physical presence: a physical national identity document shall be used as identity evidence and it shall be checked in the following way: - validity of national identity document must be checked: - from the identity document; - from the Public Register of Authentic travel and identity Documents Online (PRADO) by identity document number (see: https://www.consilium.europa.eu/prado/en/check-document-numbers.html). If it is not possible, the certificate can be issued only according to non-qualified level certification policy and implementing additional controls minimising the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen,	ETSI TS 119 461 9.2.1 USE-9.2.1.2-04X, USE-9.2.1.1-04, USE-9.2.1.1-05, USE-9.2.1.2-01, USE-9.2.1.2-02 ETSI TS 119 461 8.3.1 VAL-8.3.1-01X, VAL-8.3.1-02, VAL- 8.3.1-03X, VAL- 8.3.1-04X, VAL-

		suspended, revoked or expired evidence (for example security measures that satisfy to anti-money laundering directive requirement etc.); - it shall be recognized in EU non-exhaustive list is available at: https://www.consilium.europa.eu/prado/en/prado-recognised-documents.html); - The RA officer may additionally check the person's attributes against the national population registry or other authoritative source as a part of the approved RA issuance process. The person's attributes shall match 100% with the data in the authoritative source and result of the check must be logged and retained according to requirements. The process shall verify that the physical identity document presented is: - visually equal to the expected visual appearance of the document type; - belongs to the applicant who is the legitimate evidence holder; - is a original, genuine, physical identity document that is not counterfeited or falsified/modified. Security elements used for inspection can be, for example, watermarks, optically variable devices (e.g., holograms, inks), printing techniques, visual patterns, see-through elements, and tactile elements. Special care shall be taken for inspecting integrity of security elements in the area of facial image and personal data. The RA will ensure that: - The RA officer shall guide the applicant and carry out the identity proofing process according to a defined process description. In case of deviations, the RA officer shall abort the identity proofing process and convey the information to the applicant; - The RA officer shall be allowed to spend sufficient time to examine the identity document and shall be provided with working conditions that do not impair the RA officer's judgement;	8.3.1-05, VAL-8.3.1-06X, VAL-8.3.1-07, VAL-8.3.1-08X, VAL-8.3.1-12 Commission implementing regulation (EU) 2015/1502 of 8 September, 2.1.2. Identity proofing and verification (natural person) - Level High Requirements ETSI TS 119 461 8.3.3 VAL-8.3.3-01, VAL-8.3.3-03, VAL-8.3.3-06, VAL-8.3.3-07X, VAL-8.3.3-07B, VAL-8.3.3-07C, VAL-8.3.3-08, VAL-8.3.3-09, VAL-8.3.3-10, VAL-8.3.3-14X, VAL-8.3.3-14A, VAL-
--	--	---	--

		• The RA shall ensure that validation of identity attributes and evidence, including verification of authenticity, integrity and validity, is performed within an environment controlled by the RA; • The RA shall verify a sufficient number of security features of the identity document to establish its authenticity. The selection of security features to be verified shall not be fixed and shall incorporate variability in order to reduce the risk of falsified elements. The procedures for verification of security features shall be defined, documented and maintained under the responsibility of the RA; • The RA officer shall have available tools to validate physical identity documents reliably (e.g., magnifying glass, UV-lamp, etc.); • The RA officer shall have access to authoritative sources of information on document appearance, e.g., Public Register of Authentic travel and identity Documents Online (PRADO) (see: https://www.consilium.europa.eu/prado/en/prado-start-page.html); • RA officers shall periodically pass appropriate training and internal instructions to verify authenticity of the specific document type and document, covering at least following: ○ fraud prevention and detection of forgery; ○ data protection; ○ communication with applicant; ○ training of software and equipment used; ○ training on verification of documents and their security elements; • The training of the RA officers shall be repeated or refreshed as required by threats intelligence, updates to procedure or tools, and at least annually. The four-eyes control principle: Applicable for the issuance of qualified certificates according to the policy QCP-n-qscd.	8.3.3-15X, VAL-8.3.3-16 Risk assessment
--	--	--	---

		In case of physical presence of subscriber, the four-eyes control of national identity document as evidence of identity and claimed identity of subscriber shall be conducted. During the four-eyes control, all controls described in subsections 2. and 3. shall be checked by the second RA officer. <i>Alternative</i> controls, in the case when the second RA officer cannot be physically present during the four-eyes control, can be implemented only by the approval of the TSP. For example, the four-eyes control can be replaced by a technical control, where the person's biometrical data or identity document data are matched with the person, or their identity document data from an authorized source (e.g., population registry, identity document registry, etc.) and the modification of the input and output data is technically restricted to the second employee. Additionally, as part of the subscriber's information checked by the second RA officer, there should be evidence collected about the presence of the subscriber in the RA office (e.g., a photo of the subscriber taken proving their presence in RA office). The result of such technical control must be logged and retained according to requirements.	
3.	Binding to applicant	The RA officer shall compare the face in the photo from the identity document presented by applicant with the applicant's physical appearance. • RA shall collect a photocopy/scanned copy of the national identity document's biodata page(s)/card and retain according to requirements as needed for binding to applicant and to evidence the identity proofing process; ○ If RA has previously already collected a photocopy/scanned copy of same the national identity document – this can be re-used as evidence for the next identity proofing only in the case and under following conditions: ▪ RA officer has checked and made sure that photocopy/scanned copy of the same document exists in the archive/information system; ▪ RA officer has collected in the information system additional data for evidence - the name and number of national identity document that was presented by applicant during present	ETSI TS 119 461 9.2.1 USE-9.2.1.2-05 ETSI TS 119 461 8.3.3 VAL-8.3.3-10 ETSI TS 119 461 8.4.1 BIN-8.4.1-01X, BIN-8.4.1-02X ETSI TS 119 461 8.4.4

		identity proofing process for the certificate issuance. This additional evidence shall be maintained under same requirements as photocopy/scanned copy of national identity document; • The RA officer shall be allowed to spend sufficient time to perform the face comparison of the applicant's face image against the identity document and shall apply a defined set of morphological features; • The RA officer shall have tools available to magnify images to view details; • The RA officer shall receive training before making any comparison that will be repeated or refreshed at least annually. The four-eyes control principle: Applicable for the issuance of qualified certificates according to the policy QCP-n-qscd. In case of physical presence of subscriber, the four-eyes control of national identity document as evidence of identity and claimed identity of subscriber shall be conducted. During the four-eyes control, all controls described in subsections 2. and 3. shall be checked by the second RA officer. <i>Alternative</i> controls, in the case when the second RA officer cannot be physically present during the four-eyes control, can be implemented only by the approval of the TSP. For example, the four-eyes control can be replaced by a technical control, where the person's biometrical data or identity document data are matched with the person, or their identity document data from an authorized source (e.g., population registry, identity document registry, etc.) and the modification of the input and output data is technically restricted to the second employee. Additionally, as part of the subscriber's information checked by the second RA officer, there should be evidence collected about the presence of the subscriber in the RA office (e.g., a photo of the subscriber taken proving their presence in RA office). The result of such technical control must be logged and retained according to requirements.	BIN-8.4.4-01X, BIN-8.4.4-02, BIN-8.4.4-03, BIN-8.4.4-04X, BIN-8.4.4-05 Risk assessment
--	--	--	--

4.	Issuing of identity proofing result	A successful identity proofing result shall be produced and securely communicated to the TSP, confirming that the applicant's identity has been established to the required Level of Identity Proofing (LoIP).	ETSI TS 119 461 8.5.1 ISS-8.5.1-01, ISS-8.5.1-02
Identity validation requirements for certificate issuance (<i>by a qualified electronic signature with its certificate (via RA's self-service)</i>)			
Number of controls	Name of controls	Controls for certificate issuance	Source
1.	Attribute collection	The subscriber (natural person) shall be verified: - by means of a qualified electronic signature certificate (that is issued by physical presence or ABIV). The qualified electronic signature shall be made under a guarantee of sole control by the signer when the signer is a natural person. The following attributes shall be collected: - family name(s), first name(s), which should be current names; - personal identity code (EE, LV, LT). The RA shall not collect additional identity attributes, unless such attributes are strictly necessary for the purposes of identity attribute validation and/or binding the applicant to the provided evidence.	eIDAS regulation, article 24 clause 1a ETSI TS 119 461 C3.3 QTS-C3.3-01, QTS-C3.3-02, QTS-C3.3-04 ETSI TS 119 461 9.2.5 USE-9.2.5-01, USE-9.2.5-02, USE-9.2.5-05 ETSI TS 119 461 8.2.2 COL-8.2.2.1-01X, COL-8.2.2.1-02, COL-8.2.2.1-03, COL-8.2.2.1-04

			ETSI TS 119 461 8.2.5 COL-8.2.5-01X, COL-8.2.5-03A, COL-8.2.5-06X
2.	Attribute validation	A qualified electronic signature shall be created as part of the identity proofing process. A qualified electronic signature shall be validated, and its certificate shall only be used as evidence for identity attributes if this signature is valid and is confirmed to have been created as part of the identity proofing process. Successful validation of the qualified electronic signature shall imply that the identity attributes conveyed from its signing certificate are validated and bound to the applicant. The identity attributes conveyed in the qualified electronic signature certificate must match the attributes presented in the application.	ETSI TS 119 461 9.2.5 USE-9.2.5-03 ETSI TS 119 461 8.3.5 VAL-8.3.5-00, VAL-8.3.5-01, VAL-8.3.5-02X Commission implementing regulation (EU) 2015/1502 of 8 September, 2.1.2. Identity proofing and verification (natural person) - Level High Requirements Risk assessment
3.	Binding to applicant	Binding to the applicant is completed based on: • successful validation of a qualified electronic signature;	ETSI TS 119 461 8.3.5 VAL-8.3.5-00

		- validation of identity attributes conveyed from the qualified electronic signature's certificate; - matching of attributes in the qualified electronic signature certificate with the attributes presented in the application.	
4.	Issuing of identity proofing result	A successful identity proofing result shall be produced and securely communicated to the TSP, confirming that the applicant's identity has been established to the required Level of Identity Proofing (LoIP).	ETSI TS 119 461 8.5.1 ISS-8.5.1-01, ISS-8.5.1-02

2. Identity Validation Requirements for Certificate Revocation

Number of controls	Name of controls	Controls for certificate revocation	Source
1.	Identity proofing and verification of a natural person	Verification of a person in case the person has a physical national identity document: - national identity document as evidence of identity and claimed identity shall be checked: - validity of national identity document; - authenticity of national identity document (inspect primary security features); - the subscriber is identified as the claimed identity through comparison of one or more physical characteristic of the person with national identity document, including verification that the document presented represents the claimed identity. Verification of a person in case the person has no national identity documents (lost, stolen, etc.):	ETSI 319 411-1, 6.2.4 REV-6.2.4-09

		- the person's identity is verified and claimed identity compared using historical data (in information system) about person's identity and physical characteristics. Verification of a person if the revocation is requested from the Helpline: - the person must present at least the following data: - Person's name (the current first and last name); - personal identity code (EE, LV, LT) or the date of birth; - The Helpline checks if presented contact information is known to RA (address, phone number or an e-mail address); - in the case of suspicion, the person's identity is verified and claimed identity compared using historical data (in information system) about the person's identity or his/her transactions that are known to RA. Verification of a person if the revocation is requested via RA's self-service: - the person has authenticated themselves to the RA self-service portal with authentication means that are subject to the prior agreement (e.g., eID means LoA High, authentication means provided by the banks, etc.).	
2.	Collection of evidence or attestation of subject's identity and attributes	In case of verification of person with national identity document: - RA shall collect copy of national identity document. In case of verification of person with historical identity data: - evidence that such check took place and by whom, that for verification and identity comparison historical data was used and reference to data set which was used to verify and comparison of identity. In case of verification of person's identity via Helpline: - RA shall maintain the call records according to the agreement.	ETSI 319 411-1, 6.2.2 REG-6.2.2-02B, REG-6.2.2-05, REG-6.2.2-18

		In case of verification of a person via RA self-service portal: • RA shall maintain the records of the request according to the agreement.	
--	--	---	--