Roksnet CA Policies: SIGN and AUTH

Document code: CP

Version: 1.0

Published: 4 November 2026

Effective date: 5 November 2026

Publisher: Roksnet Solutions OÜ

The second document accompanying the Roksnet CA model explanation. SIGN and AUTH are issued under Roksnet's own policy, developed on the basis of ETSI EN 319 411-1 V1.5.1 LCP. Conformance with LCP is not claimed.

In both policies, Roksnet does not establish the identity or verify the authority of natural persons on the Subscriber's side. This is a deliberate boundary of the service, not a gap to be closed: verification of persons does not return through registration, access recovery, renewal or revocation. Identification of the organisation and the issuance decision are performed by the CA.

How to read this document

Annex A maps the policy to the LCP requirements; its decisions describe SIGN. Decisions for AUTH that differ from SIGN are given in Annex A.1. The “Technical implementation” column is filled in from the documents listed in Annex D.

Statuses in Annex A:

- R — the LCP requirement is retained.
- P — the requirement is implemented through the procedure referred to in the “Decision” column.
- C — conditional applicability.
- N — not applicable; the reason is given.
- T — technical requirement; implementation in the “Technical implementation” column.
- O — open non-technical question.
- V — void item of the source edition.
- D — deviation from the LCP requirement; deviations for AUTH are set out in Annex A.1, other deviations in § 16.

The statuses describe design decisions, not audit results. A departure from a “should” recommendation is stated with a reason and is not treated as a replacement of the requirement. Annex B covers sections without their own identifiers; Annex C covers the referenced organisational areas.

1 Purpose and scope

1.1 The service

Roksnet CA issues specialised AUTH and SIGN certificates for use in the infrastructure provided by Roksnet. Trust Services operate under their own documentation. The use of Self-Service, the Member Code and the Security Server does not merge the CA and the Member Directory into a single service with a common identification procedure.

The Subscriber is always an organisation that is a Member: a legal person or a public-sector institution, including one without separate legal personality. In these policies the term “organisation” covers both categories. SIGN certificates are intended for the organisation's electronic seal; personal certificates of its employees are not part of this model. AUTH is used for authentication in the technical infrastructure provided.

This model does not claim the issuance of qualified certificates or publicly trusted website certificates. TSA services and remote management of Subscriber keys are outside the scope of this CA policy.

1.2 Roksnet policy

SIGN and AUTH certificates are issued under Roksnet's own policy, developed on the basis of ETSI EN 319 411-1 LCP. Conformance with LCP is not claimed and the LCP OID is not included in certificates. The mapping to the LCP requirements is given in Annex A. SIGN certificates contain the policy identifier (OID) 1.3.6.1.4.1.47435.1.2.1 and AUTH certificates 1.3.6.1.4.1.47435.1.2.2. CA certificates carry 1.3.6.1.4.1.47435.1.2. That policy authorises SIGN 1.3.6.1.4.1.47435.1.2.1 and AUTH 1.3.6.1.4.1.47435.1.2.2.

AUTH is issued in the same way as SIGN. For AUTH, conformance with the LCP requirements for device certificates is not claimed; the deviations are listed in Annex A.1.

1.3 Limits of the result

A certificate binds a public key to data formed under the approved profile and checked to the extent set out here. It is not a universal certification of the organisation's trustworthiness or of the lawfulness of its actions.

SIGN is designed for use in creating advanced electronic seals. In this version this is the intended use, not a promise that any operation with the certificate automatically acquires the corresponding legal status. Requirements for key use and for the result of an operation are considered separately from the procedure for admitting the Subscriber.

2 Participants and allocation of functions

2.1 Subscriber

Subscriber — as defined in the RTD: a legal entity that has accepted the Trust Services documentation. The account operator, the technical administrator and the Authorised Signatory do not become the Subscriber merely by performing these actions.

For SIGN, the organisation is both the Subscriber and the subject of the certificate. REG-6.2.2-19 and REG-6.2.2-20 do not apply. Basis: the definition of subscriber in EN 319 401 (clause 3.1) and the conditional nature of REG-6.2.2-19 and REG-6.2.2-20.

2.2 The organisation and its people

The organisation itself determines the persons who are allowed to use the account, submit applications, sign statements and manage certificates. The organisation ensures appropriate access management and promptly removes access from persons who have lost their authority. Roksnet does not establish the identity of the natural person operating the account and does not verify the corporate authority of the operator or of the Authorised Signatory.

The Authorised Signatory means the person whom the organisation must authorise to sign the statement. This designates a requirement on the Subscriber, not a status assigned or confirmed by the CA. The head of the organisation, a person acting in their place or any other person may act as the Authorised Signatory by decision of the organisation itself.

2.3 The CA and Self-Service

The CA identifies the organisation, checks the evidence and takes the issuance decision. Self-Service is not a registration authority of the CA: it authenticates the account and stores and transmits data. The CA does not receive Self-Service's conclusion on the identification of the organisation and does not rely on such a conclusion.

The Member Directory does not grant the Subscriber a right to a certificate and does not acquire any duty to identify the Subscriber for the CA as a result of technical integration. Issuing a certificate does not grant Directory Member status.

3 Admission to apply and acceptance of terms

3.1 Application channel

Applications for issuance or renewal are accepted only through Roksnet Self-Service with a valid Framework Membership. An application sent by any other route, for example by email to an administrator, is not accepted. Forwarding of the application from the account to the CA operator within Roksnet is part of this channel. Separate activation of the Member Directory is not required to submit an application.

Before first using Trust Services, the organisation goes through the step provided for accepting their documentation. The version of the terms, the date, the time and the account identifier are recorded. This record relates to the organisation's account; it is not declared to be an identification of a person.

3.2 Meaning of an authorised application

An authorised application is an application of the Subscriber submitted through its Self-Service account. The account is linked to the organisation at Identification: the Administrative Contact is designated by the organisation in the bank payment or in the Confirmation Message, and the account is set up with email verification, SMS verification of the phone and mandatory TOTP. Successful login alone is not sufficient. The CA treats an application as authorised if it is submitted through this Subscriber's account, the Member Code and the organisation's data in the account match the statement and the documents, the account is not flagged as compromised, and the statement is signed on behalf of the organisation. The CA decides whether an application is authorised under REG-6.3.2-01, REG-6.3.2-00B and REG-6.2.2-02AC. The identity and authority of the natural person are not verified.

The application identifier, the submission time, the Member Code and the link to the session or authentication event are recorded. The specific technical attributes are defined by the integration specification.

The CA does not treat every action performed with compromised account credentials as binding on the organisation regardless of the circumstances and the applicable law.

4 Documents for each application

4.1 Contents of the set

The Subscriber submits:

1. A scan of a new statement requesting issuance or renewal, signed by the Authorised Signatory.
2. A scan of a document on the registration, establishment or creation of the organisation by law, containing the necessary identification information.

One application may cover AUTH and SIGN for one Security Server. Each further order or renewal requires a new statement and a new submission of the document about the organisation. A registration document used before may be submitted again if the information in it remains current.

For an organisation created by law, an applicable official document or a confirmation from an official public list is provided for. The absence of an ordinary certificate of commercial registration does not by itself exclude such an organisation.

4.2 Contents of the statement

The statement contains, among other things:

- information about the organisation: full official name, registration number, registration body (register or official public list), country, registered address, Member Code and class;
- the organisation's declaration that this information and the attached document are current as at the date of the statement;
- the organisation's declaration that the Authorised Signatory may represent it and order certificates;
- information about the Authorised Signatory as declared by the Subscriber: name, position, date and place of signing.

The certificate order states the type of certificate, the Security Server and the seal designation declared by the Subscriber (§ 8.2).

REG-6.2.2-19 and REG-6.2.2-20 do not apply to SIGN (§ 2.1). The CA does not certify the scan of the statement as a genuine signature of a specific person.

The statement itself must express a request for a specific issuance. A general declaration by the organisation of responsibility for access does not replace the content of the order.

4.3 Form of documents

Mandatory notarisation, apostille, translation into English and a general requirement that the registration document be issued no more than three months earlier are not introduced. A document may be submitted in its original language. If the CA cannot extract or match the necessary information, the review is suspended until that information is clarified; this does not turn into a general requirement for a notarised translation.

5 Review of documents and identification information

5.1 Mandatory actions of the CA

The CA checks the evidence under REG-6.2.2-01, REG-6.2.2-02A and REG-6.2.2-02B: presence of the two documents, legibility, completion of the statement and presence of a signature; it matches the name and the official identifier between the documents and with the data recorded by Self-Service at Identification, and establishes the link to the account. The cross-check includes stored data obtained from third parties: from the bank in a SWIFT/SEPA payment, from the qualified seal provider in a Confirmation Message, or from another third party under country rules. The original confirmations are not checked again.

For a public-sector institution without separate legal personality, its affiliation with the state or another legal person is also established from the submitted documents where this is required to identify the subject of the certificate.

The rules for normalisation, transliteration, acceptable abbreviations and handling of differences are defined in writing. The Member Code and the national registration identifier are stored as separate values. A match of one of them must not automatically replace the check of the other.

The CA forms the certified data of the organisation in accordance with the result of the review and the approved profile. Arbitrary values from the CSR are not accepted without being matched against this result.

5.2 Excluded checks

The CA does not examine the authenticity of scans, original documents or the signature, does not establish the identity of the Authorised Signatory, does not verify the Authorised Signatory's position, the composition of management or the authority of persons, and does not promise an independent check of the organisation's current existence in an external register.

The CA's obligation is to carry out the established check and to transfer the reviewed identification data correctly into the certificate. The Subscriber is responsible for the accuracy of the submitted materials, the authority of the Authorised Signatory and the currency of the declared information.

5.3 Contradictions and decision

If an inconsistency is found, the CA records it and requests correction or clarification. If the submitted documents are not sufficient to verify the identity of the organisation, the CA may request additional documents about the organisation; the request does not concern the identity or authority of natural persons. If the data do not allow the required check to be carried out, the certificate is not issued.

Additional review of a specific contradiction does not create a general promise to carry out all possible external checks. At the same time, the limited scope of the check does not permit ignoring a discrepancy that is already known.

The decision record distinguishes between refusal, return for correction and successful completion of the check. Preparing the record of reasons must not require establishing the identity of the Subscriber's account operator.

6 Use of Self-Service data

6.1 Basis for trust in the channel

The CA uses the data that Self-Service recorded at Identification and stores, including third-party data. These data are checked by the CA under § 5.1. Self-Service authenticates the account and transmits data; it is not a registration authority of the CA. Self-Service's conclusion on the identification of the organisation is neither transmitted nor used. The original confirmations are not checked again.

The Self-Service routes are applied under its current documentation. SWIFT/SEPA, a qualified electronic seal and the confirmations provided for by separate country rules do not form a common mandatory package for every Subscriber.

6.2 Accompanying record

For each application, the following are transmitted and stored:

Field	Use in the CA
Member Code and account identifier	Link of the application to the Subscriber
Name, country, official identifier	Matching with the documents
Third-party data recorded at Identification: from the bank in SWIFT/SEPA, from the qualified seal provider, or from another third party under country rules	CA cross-check under § 5.1 to the extent needed
Framework Membership status and the time it was obtained	Check of admission to apply
Method and date of Identification	Context of trust in the channel
Application identifier and submission time	Link to the specific order
Version and event of acceptance of the Trust Services terms	Evidence of acceptance of the documentation
Identifiers of the original Self-Service records	Ability to trace the origin of the data

The transmitted package is protected against unnoticed modification and linked to the documents and the CSR. A snapshot at the time of the review is kept: a later change of the profile does not rewrite the issuance history.

6.3 Reuse and changes

Under REG-6.3.1-00D and REG-6.3.1-00E, each issuance and renewal requires a new CA check under § 5.1. An earlier CA identification decision does not replace this check. The Self-Service data and account are used with no calendar limit; the original confirmations are not checked again.

In case of account compromise, a change in the organisation's identity or contradictions, the CA considers their impact on the new application. If the channel is lost, issuance is suspended until it is restored under the Self-Service procedure; verification of a person is not used as a workaround. A change of the administrative contact is handled under the Self-Service procedure and does not by itself extend trust in the previously recorded details. Data from a Self-Service route excluded for security reasons are not used for the cross-check (REG-6.3.1-00C). Restoring the channel does not introduce verification of the identity or authority of natural persons.

6.3.1 Self-Service information on renewal

On renewal, the CA requests from Self-Service current data on the Framework Membership, account activity, account state and known changes affecting the link between the account and the organisation. The information received is linked to the new application and recorded as at the time of the review. If there is no response, the current status is not replaced by an assumption based on an old record. This is obtaining the current state, not a repeat check of the original payment, qualified seal or other confirmation.

Activity information is considered together with the application documents and the state of the channel. Its purpose is to strengthen the basis for trusting the continuity of the relationship with the same organisation. The absence of activity does not by itself cancel the CA check and does not create a calendar limit.

Recorded acceptance of invoices and regular payment for Member Directory services, where such events exist, are treated as additional indications of the organisation's continuing activity. Issuing or sending an invoice is not in itself its acceptance. Payment information is taken into account within the limits of the data actually known about the payer; a payment by a third party is not equated with a payment from the organisation's own account. These events do not prove that all attributes are unchanged, do not replace the two CA documents and do not certify the authority of persons. The absence of a Member Directory subscription, free-of-charge service or the absence of payments do not by themselves prevent renewal if the other CA conditions are met.

6.3.2 Recommendation on notifications between the services

It is recommended that Self-Service notify the CA of known material changes as soon as they are recorded, without waiting for the next renewal. Such events include a change of the organisation's name or identifier, of the Framework Membership status or of the account state, replacement of the administrative contact, access recovery and a known compromise of the account.

It is recommended that the notification be linked to the organisation and to the record of the change; it serves as a basis for assessing the impact of the event on pending applications and valid certificates under the CA procedures. A change of contact or another event does not mean an automatic revocation of all certificates. The status request at renewal complements the notifications, allowing the current state to be taken into account even if a notification was missed.

This is a recommendation for the interaction between independent services, not an approved delivery time for notifications, a new duty to monitor external registers or a verification of persons. The list of events, delivery, acknowledgement of receipt and error handling require a separate implementation.

6.4 Original history

The original materials may be kept in Self-Service with defined access and retention periods. The CA file distinguishes between a reference to a procedure performed earlier and an actual re-examination of the material. A check of a payment or seal must not be recorded as performed by a CA employee if they only cross-checked the stored Self-Service data.

7 Certificate application and keys

7.1 Key generation

The Subscriber's keys are generated on its side on the Security Server. The CA receives the public key in the CSR. The private AUTH and SIGN keys are not transferred to Roksnet CA and are not stored by it as part of this service.

Before issuance, the CA verifies the CSR signature, the acceptability of the algorithm and key parameters, conformance with the approved profile and the link between the CSR and a specific approved application. The certified information about the organisation is taken from the result of the CA check and is not accepted from the CSR without matching. The issued certificate contains the public key of the approved CSR. Successful verification of the CSR signature is not treated as proof of a person's identity, their authority or hardware storage of the key.

7.2 Protection of Subscriber keys

The Subscriber manages access to its keys and to the Security Server. Hardware storage is recommended in accordance with the adopted product model; this policy does not make it mandatory for every Subscriber. The CA does not claim to verify the storage location on the basis of a CSR alone.

7.3 SIGN profile

The SIGN profile is defined by the specialists under EN 319 412-3 in accordance with GEN-6.6.1-02. Certificate fields are not listed or described here.

SIGN profile: Roksnet End-Entity Sign Certificate Profile.

Algorithms, parameters and validity periods: SIGN keys are RSA of at least 2048 bits or ECDSA, AUTH keys are RSA of at least 2048 bits; certificates are signed with sha384WithRSAEncryption; validity is 1, 2 or 3 years.

8 Issuance and delivery

8.1 Conditions for issuance

Before issuance, the required checks of the documents, of the link with Self-Service and of the CSR must be completed. The certificate to be issued is matched against the approved application data. The decision, the person who performed it and the identifiers of the materials are recorded.

Implementation of issuance, CA configuration, approval system and technical roles: described in the CPS.

8.2 Issuance record

The record links the organisation and the Member Code, the Security Server, the application, the CSR or key identifier, the serial number, the validity period, the date of issuance and the purpose declared by the Subscriber. An internal designation of a unit or seal is kept as declared by the Subscriber and is not treated as independently verified.

If one application covers AUTH and SIGN, the decision on the organisation's documents may be common. For each certificate issued, its CSR, the profile and OID applied, the serial number, the result of the check of the finished certificate and the link to the common application are recorded separately.

8.3 Delivery and acceptance

The issued certificate is made available in the Member Account. Before using it, the Subscriber confirms in the account that the certificate data are correct or reports an error. Downloading alone is not confirmation. The confirmation is recorded with the date, time and account.

The Trust Services terms record the Subscriber's agreement to its obligations, the declared correctness of the data, the rules for keeping the file and the transfer of the necessary records if the CA ceases operation. Whether the certificate itself may be published to third parties is decided separately from the disclosure of the CP/CPS and of status information. If the certificate is published, the organisation's consent is recorded; this does not imply consent to publication of the scans.

The event of receipt or acceptance is linked to the organisation's account. It does not confirm the identity of the person who downloaded the certificate and is not the result of verifying their corporate authority.

9 Renewal and change of data

For each new order or renewal, the Subscriber submits the set established in section 4. The CA cross-checks the stored Self-Service data and carries out a new check under § 5.1 for each application.

The document about the organisation may be submitted again if the data are current; a new statement is required. The conditions for reusing a key or for mandatory generation of a new key are set in the technical profile. The terms renewal and re-key in the final CPS must correspond to the actual operation.

A change of the name or other certified attributes requires review of the updated information before a new issuance. What happens to a certificate issued earlier is determined by the rules on changes and revocation; a change in the account does not by itself change the content of an existing certificate.

Renewal, re-key and change of data do not introduce personal identification or verification of corporate authority. The responsibility model of section 2 applies in these procedures.

10 Revocation and incident reports

10.1 Requests by the Subscriber

Revocation uses the Subscriber's Member Account, with an unambiguous identification of the certificate. Suspension of the Member Account does not prevent a revocation request through it. The request is

recorded with the time of receipt and the result of processing. The conditions for reporting when the account is lost are set by a separate incident procedure.

The check of the Subscriber's revocation request concerns the established channel and the relevant certificate. Roksnet does not establish the corporate authority of the natural person making the request. If the channel is lost, pre-defined technical and organisational recovery measures or a CA decision on the incident apply, not an ad hoc verification of the person's power of attorney.

10.2 Other grounds

The CPS describes the handling of reports by third parties, a detected key compromise, an issuance error and material contradictions in the certified information. Receipt of a report must not automatically be treated as a confirmed instruction from the Subscriber. The CA records the basis of its own decision and the information used.

A revocation request submitted through the Member Account that identifies the certificate is acted on no later than 24 hours after receipt. Other reports of possible compromise are registered and acted on immediately upon receipt, under the incident procedure; by themselves they are not a confirmed revocation request. If a report cannot be confirmed as a request of the Subscriber within 24 hours, the CA records its actions and their basis; the procedure for such exceptions is described in the CPS.

10.3 Closure of the account and of individual services

Disabling the Member Directory and closure of the Member Account are considered separately. Cancelling the Member Directory service does not affect issued certificates. When the Member Account is closed, Roksnet revokes all certificates issued to the Subscriber. Until then, the Subscriber requests revocation through its Member Account.

11 Certificate status and use

The status of AUTH and SIGN certificates issued by Roksnet CA is available through OCSP 24/7; a single interruption of OCSP lasts no more than 4 hours. The CPS defines the methods of checking status, the addresses, and how interruptions are measured, monitored and remedied. Availability of the TSA and of the services of other providers is defined separately.

Persons relying on a certificate are provided with a clear description of its purpose and limitations. Validation of a certificate must take into account the chain of trust, the validity period, the status and the permitted use under the technical profile.

A Roksnet certificate may not be relied on as confirmation of the operator's identity, of the Authorised Signatory's position or of their right to perform a specific transaction. A party that needs such confirmation arranges it separately. The limitation of the check applies to all presentations of the result of the service, including the interface, the documentation and messages for the Subscriber.

12 Records and evidence

12.1 Issuance file

The issuance file includes both documents, the application identifier, the snapshot of Self-Service information, the result of the matching, the CSR, the issuance decision, the issued certificate and the delivery or acceptance events. The records must make it possible to explain which actions were actually performed and on which data the decision was based.

The record must not contain the marks “identity verified”, “authority confirmed” or “signature certified” if such actions are excluded by the policy. A mention of the Authorised Signatory in a scan and a verified personal identifier are different kinds of information.

12.2 Retention

For the archive, the benchmark of OVR-6.4.6-01 is retained: the minimum it sets applies to the categories designated there and is counted from the end of the validity of the certificate associated with the records.

This neither allows a single short period for all CA data nor requires every personal detail to be kept indefinitely.

The signed statements, the documents about the organisation and the records of acceptance, issuance, certificate confirmation and revocation are kept for ten years after the last related certificate ceases to be valid. This meets OVR-6.4.6-01. The periods for ordinary Self-Service logs are not automatically applied to the CA file.

The legal basis for processing is stated in the Roksnet Privacy Notice for Services. Technical logs are kept as set out in the CPS.

Storage location, means of protection, redundancy and access to the archive: described in the CPS.

Closure of Self-Service must not automatically destroy records that, under the approved schedule, are needed for certificates issued earlier. Access to the original evidence and a stored reference to it are different; for each category it is determined which option is used.

12.3 Integrity and confidentiality

The implementation design includes access restriction and logging of changes. Personal data in the documents are processed to the extent necessary. The retention rules are aligned with the privacy notice and the applicable obligations.

13 Technical sections

The adopted architectural facts are retained: Subscriber keys are generated on the Security Server side and are not transferred to the CA; HSM for the Subscriber is recommended but does not become a mandatory condition of this service. The “Roksnet implementation” column is filled in from the documents listed in Annex D; an empty cell means that the information has to be described in the CPS. The requirements for protecting the CA's own keys are not cancelled by this recommendation for the Subscriber.

Technical section	Roksnet implementation
CA hierarchy and root keys	Root CA — key offline, on premises; Intermediate CA (AUTH and SIGN) and TSA CA — keys in AWS CloudHSM; there is no OCSP CA, each CA issues its own OCSP responder certificates; OCSP responder keys — software keys in EJBCA; TSU keys — in AWS KMS (CPS V1.0, §§ 1, 3; CA certificates)
Algorithms and key parameters	CA keys — RSA 4096, signature sha384WithRSAEncryption (CA certificates); Subscriber certificates are signed with sha384WithRSAEncryption; Subscriber keys — RSA of at least 2048 bits; ECDSA for SIGN only (Procedure V1.4, § 5.3)
Certificate profiles and naming rules	Sign and Auth profiles; Procedure V1.4, §§ 4–5
Policy identifiers (OIDs) for SIGN and AUTH	SIGN 1.3.6.1.4.1.47435.1.2.1, AUTH 1.3.6.1.4.1.47435.1.2.2; CA certificates 1.3.6.1.4.1.47435.1.2; Timestamp Policy 1.3.6.1.4.1.47435.1.2.3 (CPS V1.0, § 2)
Generation and protection of CA keys	Root key — Root ceremonies V6.2; Intermediate CA and TSA CA keys — Intermediate ceremony V1.2, AWS CloudHSM; OCSP responder keys — software keys in EJBCA (CPS V1.0, § 3)
Issuance configuration and separation of duties	EJBCA; dual control — System Administrator and Security Officer; one protocol per certificate (Procedure V1.4, §§ 2, 7)
CSR check and protection of exchange between services	The CSR (PKCS#10) is submitted with the application through the Member Account (Procedure V1.4, § 6); its signature is verified, the subject data are checked against the result of the document check and the key fingerprint is recorded (Procedure V1.4, § 7.2). Protection of exchange between services is not described
Publication of CP/CPS and repository availability	https://www.roksnet.com/trustservices/cps and https://www.roksnet.com/resources; Root CA hash at https://www.roksnet.com/trustservices/rootca (Terms

Technical section	Roksnet implementation
	v1.2, § 17; CPS V1.0, § 8). 24/7 availability of the repository is not stated
CRL and OCSP	OCSP only: AUTH and SIGN — http://ocsp.roksnet.com/CA, TSU — http://ocsp.roksnet.com/TSA; available continuously, a single interruption lasts no more than 4 hours; no CRLs (Terms v1.2, § 8; CPS V1.0, § 7)
Revocation, technical deadlines and exceptions	Grounds — Terms v1.2, § 7; a request through the Member Account is acted on no later than 24 hours after receipt (Terms v1.2, § 7; CPS V1.0, § 6); the procedure for reports that cannot be confirmed is to be described in CPS V1.0, § 6
Physical protection and location	Root key material is held offline; Intermediate CA and TSA CA keys are in AWS CloudHSM; access to EJBCA and CloudHSM is restricted and logged (CPS V1.0, § 10). Physical security of the key ceremonies — Root ceremonies V6.2, § 2.1; Intermediate ceremony V1.2, §§ 2, 4.1
Networks, access, monitoring and updates	Issuance only from the registered workstation over the approved path to EJBCA and CloudHSM (Procedure V1.4, § 3); availability of OCSP and timestamping is monitored (CPS V1.0, § 7)
Logs and technical archive	One protocol per certificate and the EJBCA audit identifier, if available (Procedure V1.4, § 8); retention — § 12.2, Terms v1.2, § 12 and CPS V1.0, § 9
Technical actions in case of compromise	Revocation on key compromise and on compromise of the issuing CA key (Terms v1.2, § 7); reports of compromise are registered and investigated (CPS V1.0, § 6)
Testing and decommissioning	On cessation, the records required for status information are transferred or made available (Terms v1.2, § 15; CPS V1.0, § 11); the termination plan — CPS V1.0, § 11

14 Documentation and responsibility

In the final package, the CP defines the policy, the CPS defines the practice of implementing it, and the Trust Service Terms and Conditions define the contractual terms. They may be organised in an agreed set of documents without duplicating the same rules. The order of precedence of the documents and the amendment procedure are set out in the Trust Service Terms and Conditions (§§ 1, 17).

The Subscriber is responsible for the information submitted, the authority of its people, access and its own keys. Roksnet is responsible for carrying out the adopted scope of procedures and for its own systems. Excluding the verification of representation does not release Roksnet from carrying out the checks it has expressly promised.

The limits of contractual liability, the applicable law and the dispute procedure are set out in the Trust Service Terms and Conditions (§§ 14, 16).

Proposals to change the policy are assessed for compatibility with section 2.2. Introducing a function for verifying natural persons in the future requires a separate product decision; it cannot happen unnoticed by borrowing a CPS template.

14.1 Policy management

Roksnet management approves the CP/CPS and appoints the document owner and those responsible for changes. Issuance and revocation decisions are taken under the published procedure; commercial interest does not replace the required checks. Responsibility for applying the policy remains with Roksnet also when Self-Service or contractors are used.

Roksnet keeps a revision log and access to the applicable versions. Changes affecting the terms of use are brought to the Subscriber's attention before they apply, in the manner set by the service terms. Unpublished internal criteria are not presented as obligations already accepted by the Subscriber.

14.2 Risks of Roksnet's model

For the chosen architecture, the following are assessed separately: false information in documents, misuse of lawfully obtained access, account compromise, loss of currency of data and inconsistency between services. The assessment explicitly records the residual risk that an application has been made by a person without the necessary authority. Roksnet does not describe this risk as eliminated by verifying the person.

Management's acceptance of this risk justifies the level of verification based on LCP rather than NCP (EN 319 411-1, clause 4.2.2) and is accompanied by disclosure of the limits of the check. The risk assessment is reviewed when the model changes or when material information about incidents is received.

14.3 Subscriber obligations

The Subscriber provides correct information, keeps it current, protects keys and access, uses the certificate only for its intended purpose and reports an error or loss of control without undue delay. After a detected key compromise, the Subscriber stops using the key for new operations and initiates the incident handling provided for. Allocation of internal duties remains its own task.

These obligations do not turn the CA into a supervisor of the Subscriber's internal appointments. The absence of such supervision does not exclude refusing a specific application in case of a known contradiction or technical breach.

14.4 Termination of the service and notifications

Before launch, a CA termination plan is approved: informing the affected organisations, servicing previously issued certificates, keeping the necessary records and the person responsible for the remaining obligations. A transfer to another operator does not mean automatic consent to a new scope of identification. Technical actions on keys and statuses remain in section 13.

The Subscriber's withdrawal from the Member Directory is not the same as closure of the Member Account. The consequences of closing the account for certificates are set out in § 10.3.

14.5 Complaints and organisational safeguards

A complaint about the quality of the service is registered and considered separately from a certificate order. The result of the review and the means of further resolution are provided to the Subscriber. Complaints are submitted through the Member Account or to support@roksnet.com.

The exclusion of verification of the Subscriber's people does not apply to the CA's own staff. The authority, competence and access of Roksnet personnel must be managed by Roksnet itself. The boundary of section 2.2 does not extend to the CA's trusted roles.

14.6 Terms and disclosure of limitations

The Trust Service Terms and Conditions and the public description state the applicable SIGN or AUTH policy, the purpose of the certificates, the exact scope of the check, the Subscriber's obligations, the limitations of reliance, contacts, and the rules on acceptance, retention, complaints and termination. Statements about audits are given only if a corresponding result exists. Confidential technical information is not published together with the user terms.

The provisions on data processing are aligned with the RPN-Services. Confidentiality of the evidence is maintained regardless of whether the CA verifies a person's authority. Accessibility of the interface and documents is treated as a separate task, without introducing personal identification of the Subscriber's people.

15 Relationship with LCP

The policy is developed on the basis of ETSI EN 319 411-1 LCP; conformance is not claimed. The evidence check is performed under § 5.1, the allocation of roles under § 2.1, whether an application is authorised is

determined under § 3.2, and a new check at each issuance and renewal under § 6.3. The requirement-by-requirement mapping is in Annex A; the AUTH deviations are in Annex A.1, other deviations in § 16.

16 Departures from LCP

Recommendation REG-6.2.2-02AB is not applied in full. Roksnet uses the documentary check under §§ 4–6 of this policy: it reviews two documents, matches the information with the stored Self-Service data and establishes the link between the application and the organisation's account. This procedure does not provide for independent certification of the authenticity of the original documents under ETSI TS 119 461. The choice of procedure is justified by the limited scope of use of the certificates, the established application channel and the risk assessment under § 14.2. The other requirements of LCP, on which the policy is based, are retained.

Requirement REV-6.2.4-03A is not applied. A revocation request through the Member Account is acted on no later than 24 hours after receipt; the policy does not fix the time by which the certificate status changes.

17 Sources

- ETSI EN 319 411-1 V1.5.1, April 2025. Pages in Annex A are the PDF page numbers, which coincide with the printed ones.
- ETSI EN 319 401 V3.1.1, June 2024, for the referenced organisational areas.
- Roksnet documents: RTD, RPN-Services.
- “Roksnet CA Model Explanation”.

The full texts of the standards are not reproduced here. The annexes contain the identifiers and the decisions for Roksnet. Technical normative dependencies must be disclosed together with the completion of the technical part, and not marked as fulfilled on the basis of this policy.

Annex A Item-by-item map of EN 319 411-1

The map contains 388 items, including 57 Void. The “Technical implementation” column is filled in from the documents listed in Annex D. A combined status separates the normative decision from the technical implementation. O is an explicitly open non-technical parameter: it is not presented as technical and is not treated as decided.

References with a specific number lead to the definition of the item, not to its mention in another section. For mixed items, the status applies to the chosen LCP branch; NCP+ sub-items are not carried over automatically. The original force of shall/should/may is preserved: the presence of a row does not turn a recommendation into an obligation.

Items 5.1

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-5.1-01	18	V	—	
OVR-5.1-01A	18	N	Marking of another policy; not LCP	
OVR-5.1-02	18	V	—	
OVR-5.1-02A	18	N	Marking of another policy; not LCP	
OVR-5.1-03	18	T	§§ 7, 13	Profile rules for AUTH and SIGN — Procedure V1.4, §§ 4–5; Sign and Auth profiles

Items 5.2

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-5.2-01	18	P	§ 14; Annex C	
OVR-5.2-02	18	P	§ 14; Annex C	
OVR-5.2-03	18	V	—	
OVR-5.2-03A	18	T	§§ 7, 13	Profile rules for AUTH and SIGN — Procedure V1.4, §§ 4–5; Sign and Auth profiles
OVR-5.2-04	18	T	§§ 7, 13	CA keys — RSA 4096, signature sha384WithRSAEncryption (CA certificates). Subscriber certificates are signed with sha384WithRSAEncryption; Subscriber keys — RSA of at least 2048 bits; ECDSA for SIGN only (Procedure V1.4, § 5.3)
OVR-5.2-05	18	R/T	Publication retained; implementation in § 13	The CP, CPS, Timestamp Policy, Terms and profiles are published at https://www.roksnet.com/trustservices/cps and https://www.roksnet.com/resources (Terms v1.2, § 17; CPS V1.0, § 8). 24/7 availability of the repository is not stated
OVR-5.2-06	18	N	Marking of another policy; not LCP	
OVR-5.2-07	18	N	Marking of another policy; not LCP	
OVR-5.2-07A	18	N	Marking of another policy; not LCP	
OVR-5.2-07B	18	N	Public web PKI not chosen; outside the scope	
OVR-5.2-08	18	N	Marking of another policy; not LCP	
OVR-5.2-08A	18	N	Marking of another policy; not LCP	
OVR-5.2-08B	18	N	Public web PKI not chosen; outside the scope	
OVR-5.2-09	19	N	Marking of another policy; not LCP	
OVR-5.2-10	19	T	§§ 7, 13	Subscriber certificates are signed by the Intermediate CA, not the Root (Procedure V1.4, § 5.1); no CRLs are issued (Procedure V1.4, § 3). OCSP responses are signed by responders whose certificates are issued by the respective CA (CPS V1.0, § 1)
OVR-5.2-11	19	T	§§ 7, 13	

Items 5.3

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-5.3-01	19	P	§ 1.2; SIGN 1.3.6.1.4.1.47435.1.2.1, AUTH 1.3.6.1.4.1.47435.1.2.2; the OID changes if applicability changes	

Items 5.4

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-5.4.1-01	20	P	§§ 2.3, 6, 14.1	
OVR-5.4.1-02	20	T	§§ 7, 13	Root CA (Roksnet Trust Service Root CA 2026); subordinates — the Intermediate CA for Subscriber certificates (Roksnet Trust Service Intermediate CA 2026) and the TSA CA (Roksnet Trust Service TSA CA 2026); there is no OCSP CA (CPS V1.0, § 1; CA certificates)
OVR-5.4.1-03	20	T	§§ 7, 13	Both subordinate CAs are issued by the root CA to Roksnet Solutions OÜ (CA certificates)
OVR-5.4.3-01	21	P	§§ 2.3, 6, 14.1	

Items 6.1

Identifier	Page	Status	Decision for SIGN	Technical implementation
DIS-6.1-01	21	V	—	
DIS-6.1-01A	21	P	§ 8.3	
DIS-6.1-01B	21	C/P	If the certificate is published — § 8.3	
DIS-6.1-01C	21	N	The SIGN subject is an organisation, not a device or system; § 2.1	
DIS-6.1-02	21	V	—	
DIS-6.1-02A	21	P	§ 8.3	
DIS-6.1-03	21	V	—	
DIS-6.1-04	21	P	§§ 1.2, 11, 14.6	
DIS-6.1-05	21	P	§§ 1.2, 11, 14.6	
DIS-6.1-06	21	V	—	
DIS-6.1-06A	21	T	§ 13	The Subscriber downloads the certificate in the Member Account and confirms its data (Terms v1.2, § 5); the Terms, CP, CPS and the Root CA hash are published at https://www.roksnet.com/trustservices/cps and https://www.roksnet.com/resources (Terms v1.2, § 17)
DIS-6.1-07	22	V	—	
DIS-6.1-07A	22	N	Marking of another policy; not LCP	
DIS-6.1-08	22	P	§§ 1.2, 11, 14.6	
DIS-6.1-09	22	C/P	If public trust is claimed — § 14.6;	

Identifier	Page	Status	Decision for SIGN	Technical implementation
			it is not claimed now	
DIS-6.1-10	22	C/T	If cross-certification is introduced; § 13	
DIS-6.1-10A	22	N	Marking of another policy; not LCP	

Items 6.2

Identifier	Page	Status	Decision for SIGN	Technical implementation
REG-6.2.2-01	22	P	§§ 4–6; evidence check by the CA	
REG-6.2.2-02	22	V	—	
REG-6.2.2-02A	22	P	§ 5.1; evidence check by the CA	
REG-6.2.2-02AB	22	P	§ 16; departure from a should, with the reason stated	
REG-6.2.2-02AC	22	P	§ 3.2; the CA decides whether an application is authorised	
REG-6.2.2-02B	22	P	§ 5.1; cross-check of documents and stored data	
REG-6.2.2-03	22	V	—	
REG-6.2.2-03A	23	N	Marking of another policy; not LCP	
REG-6.2.2-04	23	V	—	
REG-6.2.2-05	23	N	Marking of another policy; not LCP	
REG-6.2.2-05A	23	N	Marking of another policy; not LCP	
REG-6.2.2-05B	23	N	Marking of another policy; not LCP	
REG-6.2.2-05C	23	N	Natural-person subjects are outside the service	
REG-6.2.2-06	23	N	Natural-person subjects are outside the service	
REG-6.2.2-07	23	N	Natural-person subjects are outside the service	
REG-6.2.2-08	23	N	Marking of another policy; not LCP	
REG-6.2.2-08A	23	N	Marking of another policy; not LCP	
REG-6.2.2-09	24	N	Natural-person subjects are outside the service	
REG-6.2.2-10	24	N	Marking of another policy; not LCP	
REG-6.2.2-10A	24	N	Marking of another	

Identifier	Page	Status	Decision for SIGN	Technical implementation
			policy; not LCP	
REG-6.2.2-11	24	V	—	
REG-6.2.2-12	24	P/C	§§ 2.1, 4–5; the organisation's name and, where applicable, its link to a legal person are established from the submitted documents	
REG-6.2.2-13	24	N	Marking of another policy; not LCP	
REG-6.2.2-13A	25	N	Marking of another policy; not LCP	
REG-6.2.2-14	25	V	—	
REG-6.2.2-14A	25	N	Marking of another policy; not LCP	
REG-6.2.2-14B	25	V	—	
REG-6.2.2-15	25	V	—	
REG-6.2.2-15A	25	N	The SIGN subject is an organisation, not a device or system	
REG-6.2.2-16	25	N	Marking of another policy; not LCP	
REG-6.2.2-16A	25	N	Marking of another policy; not LCP	
REG-6.2.2-16B	25	N	Marking of another policy; not LCP	
REG-6.2.2-17	25	V	—	
REG-6.2.2-17A	26	N	Natural-person subjects are outside the service	
REG-6.2.2-18	26	P	§ 12; record of the CA check	
REG-6.2.2-19	26	N	§ 2.1; the organisation is the Subscriber and the subject	
REG-6.2.2-20	26	N	§ 2.1; the organisation is the Subscriber and the subject	
REG-6.2.2-21	26	P	Organisation contacts in Self-Service; §§ 3, 6	
REG-6.2.2-22	26	P	§§ 12, 14.6; Annex C	
REG-6.2.2-23	26	P	§§ 1, 4–6, 14.2; adequacy of Roksnet's model	
REG-6.2.2-24	26	V	—	
REG-6.2.2-24A	26	V	—	
REG-6.2.2-25	26	C/P	If the CA is itself a Subscriber, the same procedure applies; §§ 3–8	
REG-6.2.2-26	26	N	Natural-person subjects are outside the service	

Identifier	Page	Status	Decision for SIGN	Technical implementation
REG-6.2.3-01	27	V	—	
REV-6.2.4-01	27	P/T	§ 10; technical parameters — § 13	Revocation grounds — Terms v1.2, § 7; requests through the Member Account; other reports of compromise are registered and investigated (Terms v1.2, § 7; CPS V1.0, § 6). The revocation procedure is outside the scope of Procedure V1.4 (§ 1.2); the procedure for reports that cannot be confirmed is to be described in CPS V1.0, § 6
REV-6.2.4-02	27	V	—	
REV-6.2.4-03	27	V	—	
REV-6.2.4-03A	27	D	§§ 10.2, 16	
REV-6.2.4-03B	27	V	—	
REV-6.2.4-03BA	27	T	§§ 10.2, 13; not replaced by Roksnet's own SLA	
REV-6.2.4-03BB	27	T	§§ 10.2, 13; not replaced by Roksnet's own SLA	
REV-6.2.4-03C	27	T	§ 13; not replaced by Roksnet's own SLA	
REV-6.2.4-04	27	V	—	
REV-6.2.4-05	27	V	—	
REV-6.2.4-05A	27	T	§ 13; not replaced by Roksnet's own SLA	
REV-6.2.4-06	27	V	—	
REV-6.2.4-06A	27	T	§ 13; not replaced by Roksnet's own SLA	
REV-6.2.4-07	28	T	§ 13; not replaced by Roksnet's own SLA	
REV-6.2.4-08	28	R/T	§ 10; implementation — § 13	
REV-6.2.4-09	28	P	§ 10.1; origin of the request, not the authority of a person	

Items 6.3

Identifier	Page	Status	Decision for SIGN	Technical implementation
REG-6.3.1-00A	28	P	§§ 4–6; identification is performed by the CA	
REG-6.3.1-00B	28	P	§§ 4.2, 6.3.1; currency is confirmed by the organisation's statement as at its date, the account status and known changes	

Identifier	Page	Status	Decision for SIGN	Technical implementation
REG-6.3.1-00C	28	P	§§ 5.1, 6.3; the current CA procedure applies; data from a route excluded for security reasons are not used	
REG-6.3.1-00D	28	P	§ 6.3; new CA check at each issuance and renewal	
REG-6.3.1-00E	28	P	§ 6.3; new CA check; data and account with no calendar limit	
REG-6.3.1-00F	28	N	The Subscriber and the subject of SIGN are the same organisation	
REG-6.3.1-01	28	T	§§ 7, 13	The CSR (PKCS#10) is generated on the Subscriber's Security Server and submitted with the application through the Member Account; its signature is verified and the public-key fingerprint is recorded (Procedure V1.4, §§ 6, 7.2)
REG-6.3.1-02	28	V	—	
GEN-6.3.2-00A	29	T	§§ 7, 13	One protocol per certificate: Member Code, Security Server, reference to the Self-Service registration, result of the document check, CSR signature check and public-key fingerprint (Procedure V1.4, § 7, Appendix A)
REG-6.3.2-00B	29	P	§ 3.2; the CA decides whether an application is authorised	
REG-6.3.2-01	29	P	§ 3.2; application after login to the Self-Service account	
REG-6.3.2-02	29	N	No external registration authorities; § 2.3	
GEN-6.3.3-01	29	T	§§ 7–8, 13	Dual control — System Administrator and Security Officer; the Intermediate CA key is in AWS CloudHSM; the certificate preview is checked against the protocol (Procedure V1.4, §§ 2, 3, 7.3–7.4)
GEN-6.3.3-02	29	T	§§ 7–8, 13	Dual control; the preview is checked against the protocol and the profile (Procedure V1.4, §§ 2, 7.4)
GEN-6.3.3-02A	29	N	Marking of another policy; not LCP	
GEN-6.3.3-03	29	N	The CA does not generate Subscriber keys	
GEN-6.3.3-04	29	V	—	
GEN-6.3.3-05	29	T	§§ 7–8, 13	Subscriber certificates — for 1, 2 or 3 years (Procedure V1.4, § 5.3; Terms v1.2, §

Identifier	Page	Status	Decision for SIGN	Technical implementation
				4); the Intermediate CA is valid until 12 September 2031 (CA certificates). Limiting certificate validity to the CA validity is not stated
GEN-6.3.3-06	29	T	§§ 7–8, 13	
GEN-6.3.3-07	29	N	The CA does not generate Subscriber keys	
GEN-6.3.3-08	29	N	The CA does not generate Subscriber keys	
SDP-6.3.3-09	29	V	—	
SDP-6.3.3-09A	29	N	Marking of another policy; not LCP	
GEN-6.3.3-10	30	T	§§ 7–8, 13	The Member Code is included in every certificate as serialNumber, together with the organisation's official identifier (Procedure V1.4, § 5.2)
GEN-6.3.3-11	30	N	No personal certificates	
GEN-6.3.3-12	30	P/T	§ 1.2; SIGN 1.3.6.1.4.1.47435.1.2.1, AUTH 1.3.6.1.4.1.47435.1.2.2; LCP OID not used	SIGN 1.3.6.1.4.1.47435.1.2.1, AUTH 1.3.6.1.4.1.47435.1.2.2 (Terms v1.2, § 1; Procedure V1.4, § 5.3; CPS V1.0, § 2); CA certificates contain 1.3.6.1.4.1.47435.1.2
OVR-6.3.4-01	31	P	§§ 3.1, 8.3, 14.6	
REG-6.3.4-02	31	P	§§ 3.1, 8.3, 14.6	
REG-6.3.4-03	31	N	No separate natural-person subject or other organisation	
OVR-6.3.4-04	31	P	§§ 3.1, 8.3, 14.6	
OVR-6.3.4-05	31	P	§§ 3.1, 8.3, 14.6	
OVR-6.3.4-06	31	P	§§ 3.1, 8.3, 14.6	
REG-6.3.4-07	31	P	§§ 3.1, 8.3, 14.6	
REG-6.3.4-08	31	P	§§ 3.1, 8.3, 14.6	
REG-6.3.4-09	31	N	No separate natural-person subject or other organisation	
REG-6.3.4-10	31	V	—	
REG-6.3.4-10A	31	C/P	Direct condition not chosen; content via -13 → § 8.3	
REG-6.3.4-11	31	V	—	
REG-6.3.4-11A	32	C/P	Direct condition not chosen; content via -13 → § 8.3	
REG-6.3.4-12	32	P	§§ 3.1, 8.3, 14.6	
REG-6.3.4-13	32	P	§§ 3.1, 8.3, 14.6	
REG-6.3.4-14	32	V	—	
REG-6.3.4-15	32	V	—	
REG-6.3.4-16	32	P	§§ 3.1, 8.3, 14.6	

Identifier	Page	Status	Decision for SIGN	Technical implementation
REG-6.3.4-17	32	P	§ 12.2; not all categories have a final period	
OVR-6.3.5-01	32	P/T	§§ 7.2, 14.3; NCP+ sub-items — N	Subscriber obligations — Terms v1.2, §§ 4, 6; accepted keys — RSA of at least 2048 bits; ECDSA for SIGN only (Procedure V1.4, § 5.3)
OVR-6.3.5-02	33	N	No separate natural-person subject or other organisation	
OVR-6.3.5-03	33	P	§§ 11, 14.6	
OVR-6.3.5-04	33	N	Marking of another policy; not LCP	
OVR-6.3.5-05	33	N	Marking of another policy; not LCP	
OVR-6.3.5-06	33	N	No Subscriber key management service	
REG-6.3.6-01	34	V	—	
REG-6.3.6-01A	34	P	§§ 6.3, 9; new CA check	
REG-6.3.6-02	34	C/T	If the previous certificate is used for authentication; § 13	
REG-6.3.6-03	34	V	—	
REG-6.3.6-04	34	V	—	
REG-6.3.6-05	34	V	—	
REG-6.3.6-06	34	N	Marking of another policy; not LCP	
REG-6.3.6-07	34	N	Marking of another policy; not LCP	
REG-6.3.6-08	34	P	§§ 3.1, 9, 14.1	
REG-6.3.6-09	34	V	—	
GEN-6.3.6-10	34	T	§§ 9, 13	Each application includes a CSR (Terms v1.2, § 4); each certificate has a new protocol (Procedure V1.4, § 7); for each renewal the full application set is submitted (§ 9). Reuse of the previous key is not described
REG-6.3.7-01	34	V	—	
REG-6.3.7-01A	34	P	§§ 6.3, 9; new CA check	
REG-6.3.7-01B	35	C/P	§§ 5.1, 9; check of changed data	
REG-6.3.7-02	35	V	—	
REG-6.3.7-02A	35	T	§§ 9, 13	Each application includes a CSR (Terms v1.2, § 4); each certificate has a new protocol (Procedure V1.4, § 7). Re-key is not described separately
REG-6.3.7-03	35	C/T	If the previous certificate is used for authentication; § 13	
REG-6.3.7-04	35	P	§§ 3.1, 9, 14.1	

Identifier	Page	Status	Decision for SIGN	Technical implementation
REG-6.3.7-05	35	N	Marking of another policy; not LCP	
REG-6.3.7-06	35	N	Marking of another policy; not LCP	
REG-6.3.8-01	35	V	—	
REG-6.3.8-01A	35	P	§§ 6.3, 9; new CA check	
REG-6.3.8-02	35	C/P	§§ 5.1, 9; check of changed data	
REV-6.3.9-01	35	P/T	§ 10; parameters — § 13	A revocation request through the Member Account is acted on no later than 24 hours after receipt (Terms v1.2, § 7; CPS V1.0, § 6); status information is published only by OCSP (CPS V1.0, § 6)
REV-6.3.9-02	35	R/T	§ 10.2; SIGN policy	Grounds: Subscriber request; closure of the Member Account; key compromise or misuse; inaccurate information or issuance not in accordance with the CA policy; cessation of the organisation; material breach of the Terms; compromise of the issuing CA key or cessation of the CA (Terms v1.2, § 7)
REV-6.3.9-03	35	P	§§ 10, 14.4; notification of the organisation	
REV-6.3.9-04	36	R	Not replaced; technical implementation — § 13	
CSS-6.3.9-05	36	T	§ 13	Not applicable: no CRLs are issued (Procedure V1.4, § 3; Terms v1.2, § 8)
CSS-6.3.9-06	36	T	§ 13	Not applicable: no CRLs are issued (Procedure V1.4, § 3; Terms v1.2, § 8)
CSS-6.3.9-07	36	T	§ 13	Not applicable: no CRLs are issued (Procedure V1.4, § 3; Terms v1.2, § 8)
CSS-6.3.9-08	36	T	§ 13	Not applicable: no CRLs are issued (Procedure V1.4, § 3; Terms v1.2, § 8)
CSS-6.3.9-09	36	V	—	
CSS-6.3.9-10	36	V	—	
CSS-6.3.9-11	36	V	—	
CSS-6.3.9-12	36	T	§ 13	CARL is not mentioned in the documents; the intermediate CA and TSA CA certificates refer only to OCSP (CA certificates)
CSS-6.3.9-13	36	T	§ 13	CARL is not mentioned in the documents; the intermediate CA and TSA CA certificates refer only to OCSP (CA certificates)
CSS-6.3.9-14	36	T	§ 13	

Identifier	Page	Status	Decision for SIGN	Technical implementation
REV-6.3.9-15	36	C/T	Short-term profile not chosen; its relaxations not applied	
REV-6.3.9-15A	36	C/T	Short-term profile not chosen; its relaxations not applied	
REV-6.3.9-16	36	C/T	Short-term profile not chosen; its relaxations not applied	
REV-6.3.9-17	37	C/T	Short-term profile not chosen; its relaxations not applied	
REV-6.3.9-18	37	C/T	Short-term profile not chosen; its relaxations not applied	
REV-6.3.9-19	37	C/T	Short-term profile not chosen; its relaxations not applied	
CSS-6.3.10-01	37	T	§ 13	OCSP for Subscriber certificates — http://ocsp.roksnet.com/CA (Procedure V1.4, § 3; Terms v1.2, § 8); for TSU certificates — http://ocsp.roksnet.com/TSA (CPS V1.0, § 7)
CSS-6.3.10-01A	37	T	§ 13	
CSS-6.3.10-01B	37	T	§ 13	
CSS-6.3.10-02	37	T	§§ 11, 13	OCSP is available continuously; a single interruption lasts no more than 4 hours (Terms v1.2, § 8; CPS V1.0, § 7)
CSS-6.3.10-03	37	T	§ 13	
CSS-6.3.10-04	37	T	§ 13	
CSS-6.3.10-05	37	T	§ 13	OCSP is supported (Procedure V1.4, § 3; Terms v1.2, § 8)
CSS-6.3.10-06	37	T	§ 13	OCSP is supported (Procedure V1.4, § 3; Terms v1.2, § 8)
CSS-6.3.10-07	37	V	—	
CSS-6.3.10-08	37	T	§ 13	Not applicable: only OCSP is used (Procedure V1.4, § 3)
CSS-6.3.10-09	38	T	§ 13	Not applicable: only OCSP is used (Procedure V1.4, § 3)
CSS-6.3.10-09A	38	T	§ 13	Not applicable: only OCSP is used (Procedure V1.4, § 3)
CSS-6.3.10-10	38	T	§ 13	OCSP is available at the public address http://ocsp.roksnet.com/CA (Terms v1.2, § 8)
SDP-6.3.12-01	38	C/T	If the Subscriber keeps copies of keys; § 13	Roksnet does not hold Subscriber private keys (Terms v1.2, § 4; CPS V1.0, § 3)
SDP-6.3.12-02	38	C/T	If the Subscriber keeps	Roksnet does not hold

Identifier	Page	Status	Decision for SIGN	Technical implementation
			copies of keys; § 13	Subscriber private keys (Terms v1.2, § 4; CPS V1.0, § 3)
SDP-6.3.12-03	38	P	§ 7.1; Subscriber keys are not transferred to the CA	
SDP-6.3.12-04	38	P	§ 7.1; Subscriber keys are not transferred to the CA	
SDP-6.3.12-05	38	N	No escrow or decryption service in the model	
SDP-6.3.12-06	38	N	No escrow or decryption service in the model	
SDP-6.3.12-07	38	N	No escrow or decryption service in the model	

Items 6.4

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-6.4.1-01	38	P/T	§ 14.2; technical parts — § 13; Annex C	
OVR-6.4.2-01	38	T	§ 13	
OVR-6.4.2-02	39	T	§ 13	Root CA key — offline, on premises (CPS V1.0, § 3); Intermediate CA and TSA CA keys — in AWS CloudHSM; OCSP responder keys — software keys in EJBCA (CPS V1.0, § 3; PKI Model V4.1). Physical security of the key ceremonies — Root ceremonies V6.2, § 2.1; Intermediate ceremony V1.2, §§ 2, 4.1
OVR-6.4.2-03	39	T	§ 13	
OVR-6.4.2-04	39	T	§ 13	
OVR-6.4.2-05	39	T	§ 13	
OVR-6.4.2-06	39	T	§ 13	
OVR-6.4.2-07	39	T	§ 13	
OVR-6.4.2-08	39	T	§ 13	
OVR-6.4.2-09	39	T	§ 13	
OVR-6.4.2-10	39	T	§ 13	
OVR-6.4.2-11	39	T	§ 13	Root CA key — offline, on premises (CPS V1.0, § 3); Subscriber certificates are signed by the Intermediate CA (Procedure V1.4, §

Identifier	Page	Status	Decision for SIGN	Technical implementation
				5.1)
OVR-6.4.3-01	39	V	—	
OVR-6.4.3-01A	39	T	§ 13	
GEN-6.4.3-02	39	T	§ 13	Root and Intermediate CA key ceremonies — Root ceremonies V6.2 and Intermediate ceremony V1.2
GEN-6.4.3-03	39	V	—	
OVR-6.4.4-01	39	R/T	§ 14.5; authority of CA staff is not excluded	Trusted roles — Ceremony Administrator, Security Officer and System Administrator (CPS V1.0, § 10); issuance roles — System Administrator and Security Officer (Procedure V1.4, § 2)
OVR-6.4.4-02	39	R/T	§ 14.5; authority of CA staff is not excluded	Registration and revocation roles are not named separately; trusted roles — CPS V1.0, § 10; issuance roles — Procedure V1.4, § 2
OVR-6.4.4-03	39	N	Marking of another policy; not LCP	
OVR-6.4.5-01	39	T	§ 13	
OVR-6.4.5-02	40	T	§ 13	
REG-6.4.5-03	40	P/T	§ 12; technical storage — § 13	One protocol per certificate; EJBCA audit identifier, if available (Procedure V1.4, § 8)
REG-6.4.5-04	40	P/T	§ 12; technical storage — § 13	The protocol records the name, official identifier, Member Code, Security Server, the reference to the Self-Service registration, the result of the document check, the CSR signature check and the operators (Procedure V1.4, Appendix A)
OVR-6.4.5-04A	40	P/T	§ 12; technical storage — § 13	The protocol is archived by the Security Officer together with the reference to the Self-Service registration (Procedure V1.4, § 7.5)
REG-6.4.5-05	40	P/T	§ 12; technical storage — § 13	Data processing — Terms v1.2, § 12
GEN-6.4.5-06	40	T	§ 13	

Identifier	Page	Status	Decision for SIGN	Technical implementation
GEN-6.4.5-07	40	V	—	
OVR-6.4.5-07A	40	T	§ 13	Issuance protocol and EJBCA audit identifier (Procedure V1.4, § 8). Recording of revocation events is not described
GEN-6.4.5-08	40	T	§ 13	
REV-6.4.5-09	40	P/T	§ 12; technical storage — § 13	
SDP-6.4.5-10	40	N	Marking of another policy; not LCP	
OVR-6.4.5-11	40	P	§ 12.2	
OVR-6.4.6-01	40	R/T	§ 12.2; technical archive — § 13	Signed statements, documents about the organisation and records of acceptance, issuance, certificate confirmation and revocation — ten years after the last related certificate ceases to be valid (§ 12.2; Terms v1.2, § 12; CPS V1.0, § 9); timestamping logs — at least 10 years (Timestamp Policy v1.0, § 6)
OVR-6.4.8-01	41	T	§ 13	
OVR-6.4.8-02	41	T	§ 13	
OVR-6.4.8-03	41	T	§ 13	
OVR-6.4.8-04	41	T	§ 13	
OVR-6.4.8-05	41	T	§ 13	
OVR-6.4.8-06	41	T	§ 13	
OVR-6.4.8-07	41	T	§ 13	
OVR-6.4.8-08	41	T	§ 13	When the private key of the issuing CA is compromised, Roksnet revokes the certificates (Terms v1.2, § 7)
OVR-6.4.8-09	41	T	§ 13	
OVR-6.4.8-10	41	T	§ 13	
OVR-6.4.8-11	41	R/T	§§ 10, 14.4; scenarios — § 13	
OVR-6.4.8-12	41	R/T	§§ 10, 14.4; scenarios — § 13	
OVR-6.4.8-13	41	R/T	§§ 10, 14.4; scenarios — § 13	
OVR-6.4.8-14	41	V	—	
OVR-6.4.8-14A	41	T	§ 13	Revocation of certificates on key compromise and on compromise of the issuing CA key (Terms v1.2, § 7)

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-6.4.8-15	41	R/T	§§ 10, 14.4; scenarios — § 13	
OVR-6.4.8-16	42	T	§ 13	
OVR-6.4.9-01	42	P/T	§§ 12, 14.4; Annex C	On cessation, the records required for status information are transferred or made available (Terms v1.2, § 15; CPS V1.0, § 11); the termination plan — CPS V1.0, § 11
OVR-6.4.9-02	42	P/T	§§ 12, 14.4; Annex C	
OVR-6.4.9-03	42	P/T	§§ 12, 14.4; Annex C	
OVR-6.4.9-04	42	C/T	In case of cross-certification; § 13	

Items 6.5

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-6.5.1-01	42	T	§ 13	
GEN-6.5.1-02	42	T	§ 13	Root key — offline, on premises (Root ceremonies V6.2); Intermediate CA and TSA CA keys — generated in AWS CloudHSM (Intermediate ceremony V1.2); OCSP responder keys — software keys in EJBCA (CPS V1.0, § 3)
GEN-6.5.1-03	42	T	§ 13	
GEN-6.5.1-04	42	T	§ 13	
GEN-6.5.1-05	42	T	§ 13	
GEN-6.5.1-06	42	T	§ 13	CA keys — RSA 4096, signature sha384WithRSAEncryption (CA certificates)
GEN-6.5.1-07	42	T	§ 13	CA keys — RSA 4096, signature sha384WithRSAEncryption (CA certificates)
GEN-6.5.1-08	43	T	§ 13	The root CA is valid until 10 September 2036, the intermediate CA and the TSA CA until 12 September 2031 (CA certificates). The CA certificate changeover procedure is not described
GEN-6.5.1-09	43	T	§ 13	
GEN-6.5.1-10	43	T	§ 13	
GEN-6.5.1-11	43	T	§ 13	Key ceremonies — Root ceremonies V6.2 and Intermediate ceremony V1.2
GEN-6.5.1-12	43	T	§ 13	
GEN-6.5.1-13	43	T	§ 13	
GEN-6.5.1-13A	43	T	§ 13	
GEN-6.5.1-13B	43	T	§ 13	
GEN-6.5.1-14	44	T	§ 13	
GEN-6.5.1-15	44	N	Marking of another policy; not LCP	
DIS-6.5.1-16	44	T	§ 13	The Root CA hash is published at https://www.roksnet.com/trustservices/rootca (CPS V1.0, § 8). Publication of the CA

Identifier	Page	Status	Decision for SIGN	Technical implementation
				certificates is not described
SDP-6.5.1-17	44	N	The CA does not supply Subscriber keys or devices	
SDP-6.5.1-18	44	N	The CA does not supply Subscriber keys or devices	
SDP-6.5.1-19	44	N	The CA does not supply Subscriber keys or devices	
SDP-6.5.1-20	44	N	The CA does not supply Subscriber keys or devices	
SDP-6.5.1-21	44	N	The CA does not supply Subscriber keys or devices	
SDP-6.5.1-22	44	N	The CA does not supply Subscriber keys or devices	
SDP-6.5.1-23	44	N	Marking of another policy; not LCP	
SDP-6.5.1-24	44	N	The CA does not supply Subscriber keys or devices	
SDP-6.5.1-25	45	N	The CA does not supply Subscriber keys or devices	
OVR-6.5.2-01	45	T	§ 13	Root CA key — generated in an HSM meeting FIPS 140-2 Level 3 or higher (Root ceremonies V6.2, § 2.3); Intermediate CA and TSA CA keys — in AWS CloudHSM; OCSP responder keys — software keys in EJBCA (CPS V1.0, § 3)
OVR-6.5.2-02	45	T	§ 13	
OVR-6.5.2-03	45	T	§ 13	
GEN-6.5.2-04	45	T	§ 13	The Intermediate CA key is used in AWS CloudHSM (Procedure V1.4, §§ 3, 7.3); Root CA key — offline, on premises (CPS V1.0, § 3)
GEN-6.5.2-05	45	T	§ 13	
GEN-6.5.2-06	45	T	§ 13	
GEN-6.5.2-07	45	T	§ 13	
GEN-6.5.2-08	45	T	§ 13	
GEN-6.5.2-09	45	T	§ 13	
OVR-6.5.2-10	45	T	§ 13	
OVR-6.5.2-11	45	T	§ 13	
OVR-6.5.2-12	45	T	§ 13	
GEN-6.5.2-13	45	T	§ 13	

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-6.5.3-01	45	T	§ 13	
OVR-6.5.3-02	46	T	§ 13	
GEN-6.5.3-03	46	T	§ 13	The Intermediate CA issues AUTH and SIGN certificates and its own OCSP responder certificates; the TSA CA issues TSU certificates and its own OCSP responder certificates; there is no OCSP CA (CPS V1.0, § 1)
GEN-6.5.3-04	46	T	§ 13	
GEN-6.5.3-05	46	T	§ 13	
GEN-6.5.3-06	46	T	§ 13	
GEN-6.5.3-07	46	T	§ 13	
GEN-6.5.4-01	46	T	§ 13	An EJBCA and CloudHSM session is opened by two people: the Security Officer provides the second factor (Procedure V1.4, § 7.3)
SDP-6.5.4-02	46	N	The CA does not supply Subscriber keys or devices	
SDP-6.5.4-03	46	N	The CA does not supply Subscriber keys or devices	
OVR-6.5.5-01	46	V	—	
OVR-6.5.5-01A	46	T	§ 13	
GEN-6.5.5-02	46	T	§ 13	
GEN-6.5.5-03	46	T	§ 13	
GEN-6.5.5-04	46	T	§ 13	Opening an EJBCA and CloudHSM session requires the Security Officer's second factor; issuance only from the registered workstation (Procedure V1.4, §§ 3, 7.3)
DIS-6.5.5-05	46	T	§ 13	
CSS-6.5.5-06	47	T	§ 13	
OVR-6.5.5-07	47	T	§ 13	
OVR-6.5.6-01	47	T	§ 13	
OVR-6.5.6-02	47	N	Marking of another policy; not LCP	
OVR-6.5.6-03	47	V	—	
OVR-6.5.7-01	47	T	§ 13	
OVR-6.5.7-02	47	T	§ 13	
OVR-6.5.7-03	47	T	§ 13	
OVR-6.5.7-04	47	T	§ 13	
OVR-6.5.7-05	47	T	§ 13	

Items 6.6

Identifier	Page	Status	Decision for SIGN	Technical implementation
GEN-6.6.1-01	47	T	§ 13	X.509 v3 certificates (Procedure V1.4, § 5.3)

Identifier	Page	Status	Decision for SIGN	Technical implementation
GEN-6.6.1-02	47	T	§§ 7.3, 13; SIGN profile under EN 319 412-3	AUTH and SIGN profiles — Sign and Auth profiles; Procedure V1.4, §§ 4–5
GEN-6.6.1-03	48	T	§ 13	
GEN-6.6.1-04	48	T	§ 13	
GEN-6.6.1-05	48	T	§ 13	
OVR-6.6.2-01	48	T	§ 13	Not applicable: no CRLs are issued (Procedure V1.4, § 3; Terms v1.2, § 8)
OVR-6.6.3-01	48	T	§ 13	
CSS-6.6.3-01A	48	T	§ 13	
CSS-6.6.3-01B	48	T	§ 13	
OVR-6.6.3-02	48	T	§ 13	
OVR-6.6.3-03	48	T	§ 13	

Items 6.8

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-6.8.2-01	49	O	Financial resources and liability insurance are not described in this policy; liability — Terms v1.2, § 14	
OVR-6.8.4-01	49	P/T	§§ 12, 14.6; protection — § 13	Data processing — Terms v1.2, § 12
OVR-6.8.4-02	49	P/T	§§ 12, 14.6; protection — § 13	Applications with the CSR are accepted only through the Member Account (Terms v1.2, § 4; Procedure V1.4, §§ 2, 6). Protection of data in transit is not described
OVR-6.8.4-03	49	P/T	§§ 12, 14.6; protection — § 13	Retention periods — § 12.2; Terms v1.2, § 12; CPS V1.0, § 9
OVR-6.8.6-01	49	V	—	
OVR-6.8.6-02	49	P	§ 14; CPS implementation	
OVR-6.8.6-03	49	V	—	
OVR-6.8.13-01	50	P/O	§ 14.5; contact and dispute procedure — Terms v1.2, §§ 13, 16; the time limit for handling complaints is open	
OVR-6.8.15-01	50	R	§ 14; the policy does not override the law	

Items 6.9

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-6.9.1-01	50	P	§§ 2.3, 14.1, 14.5; Annex C	
OVR-6.9.1-02	51	P	§§ 2.3, 14.1, 14.5; Annex C	
OVR-6.9.1-03	51	P	§§ 2.3, 14.1, 14.5; Annex C	
OVR-6.9.1-04	51	P	§§ 2.3, 14.1, 14.5; Annex C	
OVR-6.9.2-01	51	T	§ 13	
OVR-6.9.2-01A	51	T	§ 13	
OVR-6.9.2-01B	51	T	§ 13	
OVR-6.9.2-01C	51	T	§ 13	
OVR-6.9.2-02	51	V	—	
OVR-6.9.2-02A	51	V	—	
OVR-6.9.2-03	51	V	—	
OVR-6.9.2-04	51	V	—	
OVR-6.9.3-01	51	P/T	§ 14.6; interface — § 13	
OVR-6.9.4-01	51	P/O	§ 14.6; unfilled fields are disclosed separately	
OVR-6.9.4-02	51	P/O	§ 14.6; unfilled fields are disclosed separately	
OVR-6.9.4-03	52	N	Marking of another policy; not LCP	
OVR-6.9.4-04	52	V	—	

Items 7.1

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-7.1-01	52	P	§§ 14.1, 14.2	
OVR-7.1-02	52	P	§ 1.2; basis — LCP; mapping — Annexes A and A.1	
OVR-7.1-03	52	P	§ 14.1	
OVR-7.1-04	52	P	§ 14.2	
OVR-7.1-05	52	P	§ 14.1	
OVR-7.1-06	52	P	§ 14.1	
OVR-7.1-07	52	P	§ 14.6	
OVR-7.1-08	52	P	§§ 14.1, 14.6	
OVR-7.1-09	52	P	SIGN — Annex A; AUTH deviations — Annex A.1	
OVR-7.1-10	52	T	§§ 7.3, 13	AUTH and SIGN profiles — Procedure V1.4, §§ 4–5; Sign and Auth profiles
OVR-7.1-11	52	P/T	SIGN under EN 319 412-3 (§ 7.3); AUTH — Annex A.1	AUTH and SIGN profiles — Procedure V1.4, §§ 4–5; Sign and

Identifier	Page	Status	Decision for SIGN	Technical implementation
				Auth profiles
OVR-7.1-12	52	P/T	§ 1.2	SIGN 1.3.6.1.4.1.47435.1.2.1, AUTH 1.3.6.1.4.1.47435.1.2.2 (Terms v1.2, § 1; CPS V1.0, § 2); enterprise number 47435 in the IANA registry is registered to Roksnet

Items 7.2

Identifier	Page	Status	Decision for SIGN	Technical implementation
OVR-7.2-01	52	P	§ 14.6; Annexes A and A.1	

Annex A.1 Decisions for AUTH that differ from SIGN

The subject of the AUTH certificate is the Security Server operated by the organisation; the Subscriber is the organisation. The other decisions of Annex A apply to AUTH in the same way as to SIGN.

Identifier	Status	Decision for AUTH
DIS-6.1-01C	P	Consent to publication is given by the organisation operating the Security Server (§ 8.3)
REG-6.2.2-01	P	The identity of the Subscriber — the organisation — is checked under §§ 4–6; the subject — the Security Server — is determined under REG-6.2.2-15A
REG-6.2.2-12	N	The AUTH subject is the Security Server; information about the organisation — under REG-6.2.2-15A
REG-6.2.2-15A	P/D	b)–e) information about the organisation — under §§ 4–5; a) device identifier — the network name or IP address of the Security Server stated by the organisation in the order; the CA checks it against the CSR. In the certificate this is part of the name, not an address for connection: in X-Road operation the server is identified by its registration in the Member Directory. The CA does not verify that this name or address belongs to the organisation
REG-6.2.2-19	P	The organisation orders the certificate for its own Security Server through its account (§§ 3.2, 4.2)
REG-6.2.2-20	D	The authority of the organisation's representative is not verified (§ 2.2)
REG-6.3.1-00F	P	An order of a certificate for the organisation's own Security Server expresses the organisation's authorisation of issuance (§ 4.2)
REG-6.3.4-03	N	The subject is a device

Identifier	Status	Decision for AUTH
REG-6.3.4-07	P	The agreement is concluded with the organisation; the subject is a device (§§ 3.1, 8.3)
REG-6.3.4-09, REG-6.3.4-10A, REG-6.3.4-11A	N	The subject is a device; REG-6.3.4-12 and REG-6.3.4-13 apply
OVR-6.3.5-02	N	The subject is a device
GEN-6.6.1-02	D/T	AUTH profile — under the X-Road requirements for the Security Server authentication certificate; conformance with EN 319 412-4 is not claimed (§ 13)
OVR-7.1-09	D	As regards REG-6.2.2-15A a), REG-6.2.2-20 and GEN-6.6.1-02
OVR-7.1-11	D	Profile under the X-Road requirements

Annex B Sections without their own identifier

Section of the source document	Decision
1–4	Context and terminology; scope of the service — §§ 1–2 of this policy
5.1	Rule for reading markings and branches; Annex A
5.3	Roksnet's own OIDs; § 1.2
5.4.2	SIGN: the Subscriber and the subject are the organisation (§ 2.1). AUTH: the Subscriber is the organisation, the subject is its Security Server (Annex A.1)
5.5	Limited scope of use within Roksnet; § 1
6.2.1	Naming rules — Procedure V1.4, §§ 4–5; Sign and Auth profiles (§ 13)
6.2.3	Repeated operations are covered in § 9
6.3.11	Roksnet's termination procedure — §§ 10.3, 14.4
6.4.7	No requirements; CA key changeover is not described in the documents listed in Annex D
6.5.8	This document does not create a TSA policy
6.7	No audit statement is added; no result exists
6.8.1	Prices are governed separately in the Trust Services documentation
6.8.3	Confidentiality — §§ 12, 14.6
6.8.5	Separate contractual drafting of rights to materials, without changing identification
6.8.7–6.8.8	Boundaries of the service — §§ 1–6; liability amounts are not invented
6.8.9	Indemnification is not added automatically from a template
6.8.10–6.8.12	§§ 14.1, 14.4; they do not replace the special terms of the Trust Service Terms and Conditions
6.8.14	The applicable law is determined by the contract; no legal opinion is given
6.8.16	Additional obligations are not introduced automatically
ETSI Annex A	May serve as a disclosure form; Roksnet's disclosure — § 14.6
ETSI Annexes B–D and History	Reference material and history; not separate checks of the Subscriber

Annex C Referenced organisational areas

EN 319 401 is considered separately from the direct register in Annex A. The following map allocates its areas within this policy; the technical content is given from the documents listed in Annex D and has not been checked for implementation.

Area of EN 319 401 V3.1.1	Decision	Place in this policy
5	P: assessment of Roksnet's model and of the residual risk	14.2
6.1	P: document owner, approval, versions, external participants	14.1, 14.4, 14.6
6.2	P/O: the scope of disclosure is defined, the values of open parameters are visible	14.5–14.6
6.3	R/T: the internal security policy is not cancelled	13, 14.1
7.1.1	P/O: scope of access, complaints, resources	14.5
7.1.2	R/T: separation of duties within the CA	13, 14.1
7.2	R/T: the CA's own staff are not covered by the boundary of § 2.2	14.5; implementation — from the documents listed in Annex D
7.3	T	13
7.4	T	13
7.5	T	13
7.6	T	13
7.7	T	13
7.8	T	13
7.9	R/T: incident reports and actions	10, 13, 14.4
7.10	P/T: composition of evidence; implementation — from the documents listed in Annex D	12, 13
7.11	T	13
7.12	P/T: organisational termination plan; implementation — from the documents listed in Annex D	14.4, 13
7.13	R/P/T: law, accessibility and data are not excluded	12, 14.6
7.14	P/T: allocation of functions between providers; implementation — from the documents listed in Annex D	2.3, 6, 14.1

The direct non-technical references of EN 319 411-1 to REQ-7.1.1-04, REQ-7.1.1-06, REQ-7.13-01–05 and REQ-6.2-02(h) are covered in this map. For Self-Service and other components, the contractual boundary under REQ-7.14.3-01X–06X is also taken into account. The requirements for the CA's own staff keep their own meaning and are not weakened by the policy on managing the Subscriber's people.

Annex D Open fields and readiness boundary

The technical fields — the “Technical implementation” column of Annex A and section 13 — are filled in from the following documents: Roksnet Trust Service Terms and Conditions v1.2 (“Terms v1.2”), Roksnet Certification Practice Statement V1.0 (“CPS V1.0”), Roksnet PKI End-Entity Certificate Issuance Procedure V1.4 (“Procedure V1.4”), the End-Entity Sign and Auth Certificate Profiles (“Sign profile”, “Auth profile”), Roksnet Timestamp Policy v1.0 (“Timestamp Policy v1.0”), the Root Certificate Ceremonies V6.2 (“Root ceremonies V6.2”), the Intermediate CA Key and Certificate Generation Ceremony V1.2 (“Intermediate ceremony V1.2”), the PKI Model V4.1 diagram (“PKI Model V4.1”) and the certificates of the Root CA, the

Intermediate CA and the TSA CA (“CA certificates”). An empty cell means that these documents contain no information on the item; it has to be described in the CPS. This document is not a CA configuration manual.

The non-technical parameters still open are financial resources and liability insurance for Trust Services and the time limit for handling complaints. They are marked O. These values cannot reliably be derived from the standard in place of a Roksnet decision. The Self-Service data and account are used with no calendar limit; each issuance and renewal requires a new CA check under § 5.1.

Annex E Recommendations for implementing the advanced e-seal

Status: recommendations for design and later verification, added on 29 September 2026. They are not approved additional obligations of Roksnet or the Subscriber, not a completion of the technical fields of section 13 and not a report on tests performed. Once an implementation is chosen, the corresponding decisions may be moved into the working procedures and documentation of the applicable service. The recommendations relate to the implementation of the chosen SIGN policy.

E.1 Link between the account, the application, the CSR and the certificate

It is recommended that the CA side link the organisation's authenticated account, the approved application, the specific CSR and the result of issuance. It is proposed to keep the application identifier and the CSR fingerprint or an equivalent unambiguous reference to the unchanged request, to verify the CSR signature and key parameters, and to check that the certificate matches the approved data. It is recommended that the organisation's identity be formed from the approved data; values sent in the CSR must not make it possible to replace it with an arbitrary organisation. It is recommended that interface restrictions be backed by checks on the service side.

To verify the implementation, scenarios are proposed of substituting the Member Code or the name in the CSR, submitting a request from another organisation's account and replacing the CSR after the application has been approved. Expected result: issuance with an unconfirmed link is blocked; a correction requires the review of the changed data provided for.

Verification of the CSR signature confirms possession of the corresponding private key at the time the request was created. The link between the request and the organisation is established by the whole submission and review procedure. A CSR by itself does not prove the operator's identity, their authority, where the key is stored or continued control over the key after issuance.

E.2 Access recovery without losing the organisational link

It is recommended to define procedures for loss of TOTP, change of the administrative email and recovery of the account after compromise. The proposed options are a pre-established recovery method or a renewed confirmation through the organisational channel provided by Self-Service. This is a recommendation for recovery events, not a periodic re-identification and not a repeat check of the history at each issuance.

It is recommended not to allow replacement of the administrative email or disabling of the second factor solely on the basis of an ordinary email from a new address. In the chosen procedure, it is proposed to record the basis of the change, close compromised sessions and means of access, and notify the contacts provided for, taking into account the nature of the incident.

Verification of the implementation: a request from a person who controls only a new email does not give access to the organisation's account; the recovery method provided for works and leaves a record of the actions performed. No check of a passport, of the operator's identity or of their corporate authority is introduced.

E.3 Access to sending messages for signing

It is recommended to protect the connection of the Subscriber's information systems to the Security Server so that only systems admitted by the organisation can send messages for signing. One option is mutual TLS authentication with binding of the permitted client certificates to the corresponding systems. Any other solution is proposed to be assessed by the same result: an outside system cannot use the server to create the organisation's seal.

It is recommended to assess separately the HTTP and HTTPS modes without authentication of the Subscriber's system, taking into account network isolation and other access restrictions. TLS between

Security Servers does not replace protection of the entry point from a local information system. Keeping the private key secret is not sufficient by itself if an outsider can instruct the server to sign messages.

Verification of the implementation: requests from a non-admitted system, including those with a substituted identifier of the Subscriber or of a subsystem, are rejected before a seal is created; requests from an admitted system are processed in the established context of the organisation. Managing this access remains the Subscriber's task, not a check of its employees by the CA.

E.4 Protection of keys, administration and backups

It is recommended to specify, for the Security Server, the Subscriber's general obligations: restriction of administrative and system access, protection of the token PIN and other secrets, system updates, protection of backups and of the means to decrypt them, management of restored instances and response to compromise. For a software token, it is proposed to also take into account copies of the key material and access to the operating system; the fact that the server belongs to the organisation does not by itself describe these measures.

Verification of the implementation: a non-admitted user gets no access to the keys or to token management; the protection of backups and secrets matches the chosen scheme; recovery leaves no uncontrolled instances of the key. It is also recommended to provide for stopping the use of a compromised key and requesting revocation under the adopted procedure.

HSM remains a recommendation, not a mandatory condition for issuance. These proposals relate to operation on the Subscriber's side and create no obligation for the CA to inspect the Subscriber's infrastructure or to confirm the key storage method from the CSR. The checks may be carried out at acceptance of the solution, and also by the Subscriber itself in its own environment; they are not proposed as a new CA check before each issuance.

E.5 Basis and limits of the recommendations

The administrative email is transmitted through the organisational channel and the account is then set up with TOTP; the Subscriber is obliged to protect its systems and keys. The recommendations build on these existing mechanisms, without introducing a function of verifying natural persons.

Article 36 of eIDAS sets requirements for the link of the seal to its creator, the creator's identification, control over the use of the seal creation data and detection of changes to the sealed data. The recommendations aim to implement these properties; including them in the document does not by itself confirm the conformance of a particular seal. Source: eIDAS, Article 36.

X-Road provides software tokens and mechanisms for creating electronic seals; the mode of connecting information systems and the protection of backups require their own configuration. The capabilities of standard X-Road are not treated as confirmation of the settings of a specific Roksnet installation. Sources: X-Road Security Architecture, §§ 9 and 16; Security Server User Guide, §§ 9.1 and 13.4.