PROCERT Certificate Provider, C.A.
Certificate Policy (PC)

Date	August, 2025
Edition	1
Version	1
Prepared by	General Management August 2025
Approved	Senior Management August 2025
Description	Certificate Policy (PC)
In effect	Yes

1. Introduction.

The PSC PROCERT proceeds to the issuance and publication of this document of the electronic certificate policy, which includes all types of extended value certificates issued in favor of third parties and final part and which has the purpose of documenting, informing the senior management, personnel, suppliers, customers and interested party of the PSC PROCERT, about the authorized use and technical support of the electronic certificates issued by the PSC PROCERT. Customers, suppliers or interested parties who use the electronic certificates issued by the PSC PROCERT must comply with this certificate policy, in order to know the responsibilities and obligations of the PSC PROCERT, regarding the life cycle of the certificates, the process of management of electronic certificates. This policy is in accordance with the mandates imposed by the Decree Law on Data Messages and Electronic Signatures (LSMDFE), its Regulations and regulatory framework that regulates the matter within the Bolivarian Republic of Venezuela and the international standards of the CA Browser Forum and RFC 2026, RFC 2119, RFC 2560, RFC 3647, RFC 3779, RFC 5055, RFC 5736, RFC 6480, RFC 6481, RFC 6482, RFC 6484, RFC 6486, RFC 6487, RFC 6489, and RFC 6492. The keywords "MUST", "MUST NOT", "REQUIRED", "MUST", "MUST NOT", "MUST", "MUST NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this Certificate Policy document shall be interpreted as described in RFC 2119.

1.1. General Description.

The PSC PROCERT has a Public Key Infrastructure (PKI) which is a public key infrastructure that has been created and supports the issuance of electronic certificates and the means of validation of the status of their certificates and claims for the operation of these by the current owners of electronic certificates in their different configurations and under the Root of Certification of the Venezuelan State. The ability to verify the status of certificates and their status is essential to ensure the unambiguous distribution of these RFC 6480 e-certification resources. The structure of the PKI of the PSC PROCERT is consistent with the Internet's number resource allocation framework. And with those provided by the IANA through the Regional Internet Registries (RIRs) as established in RFC 5736. The RIRs, in turn, manage the allocation of number resources to end users of the electronic certificates issued by the PSC PROCERT.

The PCC CERT PKI covers several types of certificates as required by RFC 6487. These certificates are as follows:

- Electronic signature certificate for company employees.
- Electronic signature certificate for representatives of public companies.
- Electronic signature certificate for legal representative of private companies.
- Electronic signature certificate for qualified professionals.
- Electronic signature certificate for natural person.
- Electronic signature certificate for public official.
- Electronic certificate for transaction signature.
- Electronic certificate of electronic invoice.
- Electronic Certificate of electronic banking.
- Electronic Certificate for Electronic Justice Processes.
- Electronic Certificate for the capital market.
- Electronic Certificate for diplomatic personnel.
- Electronic Certificate for OCSP.

1.2. Name and identification of the document.

This document contains the Certificate Policy (PC) of the PSC PROCERT and that states, regulates and establishes the certificates that are issued by the PKI of the PSC PROCERT. For the purposes of its verification and validation, the following OID has been assigned to this PC:

- id-cp-ipAddr-asNumber OBJECT ID: = {iso (1)
- Organization-Identified (3) DOD (6) Internet (1)
- Security (5) Mechanisms (5) PKIX (7) CP (14) 2}

1.3. Participants of the PKI of the PSC PROCERT.

For the purposes of the P.S.C. P.P.I., the term subscriber shall be replaced by signatory for the purposes of complying with the Law on Data Messages and Electronic Signatures and the regulations of the Superintendence of Electronic Certification Services (SUSCERTE); and refers to a person or organization that is the subject of a certificate issued by the Certification Authority (CA) of the PSC PROCERT CA. The term is used this way throughout this document and without qualification. Also, please note that, for the purposes of simplifying this document, we will always refer to PSC PROCERT PKI signatory participants as organizations or entities, even if some of them are individuals.

1.3.1. Certification Authorities.

It refers to the CA within the PSC PROCERT PKI responsible for issuing certificates to end users and who are called signatories. There is a Root CA for the PFC CERT PKI, which is signed by each CA, for each type of certificate group issued, being distributed as follows:

- S/MIME: It is the Certificate Authority (CA) in charge of issuing email security certificates (S/MIME) in a multipurpose mode whose use includes the signing of documents (DS).

1.3.2. Registration Authority.

It is the internal organization within the PSC PROCERT in charge of validating and verifying the identification and data provided by the legal or natural persons who purchase electronic certificates and in order to be able to publicly attest that the customer who holds and uses an electronic certificate of the PKI of the PSC PROCERT, is the one who effectively claims to be or represent in the case of a legal person, thus guaranteeing the identity of the signatory and, consequently, the legality of the responsibilities and obligations arising from the use of electronic signatures under the assumptions of the Decree-Law on Data Messages and Electronic Signatures and its regulations. All those interested in obtaining an electronic certificate under the decree law on data messages and electronic signatures, its regulations and the regulations of SUSCERTE, must send a copy of the documentation supporting their data and attend the appointment set by the AR of the PSC PROCERT for the purpose of carrying out the verification. Face-to-face and documentary validation of the records, supports and other proofs that prove their identity and/or representation of the representatives of legal entities who opt for an electronic certificate.

If the interested party does not attend the interview scheduled by the AR of the PSC PROCERT, their application or request for registration will be cancelled and the withholding for penalty will be applied, consequently the interested party must proceed again to register the application for an electronic certificate on the PSC PROCERT website. The support documentation used to validate applications for electronic certificates will be stored by the PSC PROCERT for a period of ten (10) years from the validity of the certificate or any of its renewals.

1.3.3. Subscribers or Signatories

The term subscriber will be replaced by that of signatory for the purposes of complying with the Decree Law on Data Messages and Electronic Signatures (LSMDFE), its Regulations and regulatory framework that regulates the matter within the Bolivarian Republic of Venezuela. Signatories will be all persons who receive electronic certificates from the PSC PROCERT PKI.

1.3.4. Trusted Parties

It is any signatory or natural or legal person who, without being a signatory, trusts the electronic certificates generated by the PKI of the PSC PROCERT under the Certification Root of the Venezuelan State.

1.3.5. Other Participants

They are those entities related to the P.S.C. PROCERT PKI that assume a CA function under the aforementioned PKI and are responsible for maintaining the P.S.C. PROCERT PKI standard and publishing the repositories with the PKI certificates, CRLs, and signed objects that it issues. The PSC PROCERT does not have another participating entity within its PKI to date.

1.4. Using the Certificate

1.4.1. Appropriate Applications of the Certificate

Electronic certificates issued under the PCC PROCERT PKI have specific uses assigned by PSC PROCERT standard and internal norm. All electronic signing certificates assigned to signatories have the following uses:

S/MIME Certified Applications	Improved use of S/MIME certificates
Electronic signature, key encryption, non-repudiation, and data encryption.	Document Signing, Secure Mail

OCSP Certified Use	Improved OCSP Certificate Usage
Electronic signature.	OCSP Signing

Additionally, they are used for the following activities:

1.4.1.1. Electronic Signature Certificate for Company Employees: The assigned use for this type of certificate is as follows:

- Online transactions.
- Identify employees or workers of public or private companies online.
- Electronic communications without representation of public or private companies.
- It does not confer legal representation of public or private companies.

1.4.1.2. Electronic Signature Certificate for Representatives of Public Companies: The assigned use for this type of certificate is as follows:

- Certify a person as the legal representative of a public legal entity.
- Public or private online transactions, on behalf of companies or entities governed by public law.
- Private or public communications on behalf of companies or entities under public law.
- Electronic commerce on behalf of companies or entities under public law.
- Online declarations or procedures before the government on behalf of companies or entities under public law.

1.4.1.3. Electronic signature certificate for legal representative of private companies: The use assigned for this type of certificates is as follows:

- Certify a person as the legal representative of a private legal entity.
- Public or private online transactions, on behalf of a commercial company, civil society, or other corporate form.
- Private or public communications on behalf of a commercial company, civil society, or other corporate form.
- Electronic commerce on behalf of a commercial company, civil or other corporate form.
- Online declarations or procedures before the government on behalf of a commercial, civil, or other corporate form.

1.4.1.4. Electronic signature certificate for qualified professionals: The use assigned for this certificate is as follows:

- Online transactions associated with the exercise of a profession or trade with registration and legal recognition within the Bolivarian Republic of Venezuela.
- Private or public communications associated with the exercise of a profession or trade with registration and legal recognition within the Bolivarian Republic of Venezuela.

- Electronic commerce associated with the exercise of a profession or trade with registration and legal recognition within the Bolivarian Republic of Venezuela.
- Declarations or online procedures before the government associated with the exercise of a profession or trade with registration and legal recognition within the Bolivarian Republic of Venezuela.

1.4.1.5. Electronic signature certificate for natural person: The use assigned for this type of certificate is as follows:

- Private transactions, other than the provision of professional services.
- Private or public communications in a personal capacity.
- Electronic purchases for individuals.
- Online declarations or procedures before the government for natural persons.

1.4.1.6. Electronic signature certificate for public official: The use assigned for this type of certificate is as follows:

- Certify a person as a career public official, freely appointed, or removed or popularly elected and to which government entity he or she is attached or belongs.
- Public or private online transactions, representing centralized or decentralized government entities.
- Private or public communications on behalf of centralized or decentralized government entities.
- Electronic commerce on behalf of centralized or decentralized government entities.
- Online declarations or procedures before the government on behalf of centralized or decentralized government entities.
- Electronic signature of emails and electronic documents

1.4.1.7. Electronic certificate for transaction signature: The assigned use for this type of certificate is as follows:

- Online or offline transaction protection.
- Legal proof of transaction record.
- Integrity of Information.
- I do not repudiate.
- Electronic signature of electronic files and documents.

1.4.1.8. Electronic Certificate for Electronic Invoice Signature: The use assigned to the Electronic Invoice Electronic Certificate certificate is as follows:

- Online transaction protection.
- Legal proof of the electronic receipt.
- Integrity of Information.

- No repudiation
- Electronic signature of electronic documents.

1.4.1.9. Electronic Electronic Banking Certificate: The use assigned to the Electronic Electronic Banking Certificate is as follows:

- Electronic signature.
- Online transaction protection.
- Legal proof of the electronic receipt.
- Integrity of Information.
- I do not repudiate.

1.4.1.10. Electronic Signature Certificate for Electronic Justice Processes: The use assigned to the electronic signature certificate for virtual dispatch is as follows:

- Electronic signature of electronic documentation/communications related to those actions that are carried out in court and that are feasible to be signed electronically and in order to guarantee their integrity, authenticity and non-repudiation, and are authorized and endorsed in this way by the entity that regulates the matter.
- Proof of identity, Non-Repudiation and Authorship.
- Proof of information integrity.

1.4.1.11. Electronic certificate for capital markets: The use assigned to the electronic certificate for capital markets is as follows:

- Electronic signature.
- Online transaction protection.
- Legal proof of the electronic receipt.
- Integrity of Information.
- I do not repudiate.

1.4.1.12. Electronic Signature Certificate for Diplomatic Personnel: The use assigned to the Electronic Signature Certificate for Diplomatic Personnel is as follows:

- Certify that a person is accredited as a diplomatic representative or personnel duly accredited and recognized by the Bolivarian Republic of Venezuela.
- Public or private online transactions, on behalf of a republic, kingdom, protectorate, or country with which the Bolivarian Republic of Venezuela maintains diplomatic relations.
- Private or public communications on behalf of a republic, kingdom, protectorate, or country with which the Bolivarian Republic of Venezuela maintains diplomatic relations.
- Electronic commerce on behalf of a republic, kingdom, protectorate, or country with which the Bolivarian Republic of Venezuela maintains diplomatic relations.

- Online declarations or procedures before the Government of the Bolivarian Republic of Venezuela.
- Electronic Signature of Electronic Emails and Electronic Documents.

1.4.1.13. OCSP Electronic Certificate: The use assigned to the OCSP Electronic Certificate is as follows:

- Electronic signature.

1.4.2. Prohibited uses of the certificate

The signatories of electronic certificates generated by the PKI of the PSC PROCERT, are obliged to use them in accordance with the uses permitted and indicated in the previous section and those established by the Decree Law on Data Messages and Electronic Signatures (LSMDFE), its regulations and other sub-legal regulations in force or any regulatory text that replaces them and regulates the activity of electronic certification within the Bolivarian Republic of Venezuela. and for the use for which it was acquired, it being expressly indicated that any violation of the rules, uses and/or laws of the Bolivarian Republic of Venezuela is under the responsibility of the signatory, as well as the damages and losses that it causes, and in a whole the provisions that are contained in the law of computer crimes and supplementarily the Venezuelan Criminal Code and Criminal Procedure will be applicable. The electronic certificate whose signatory violates the authorized use will be revoked. In addition, the signatory customer assumes responsibility for indemnifying the PSC PROCERT for damages caused to third parties arising from claims, actions, effects of action, losses or damages (including legal fines) that are generated by the improper use of the contracted service.

1.5. Policy Management

1.5.1. Organization that administers the document.

This CP is administered by:
General Management
Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, Oficina B-132, Municipio Chacao, Caracas. 1010.
Bolivarian Republic of Venezuela.

1.5.2. Contact person.

The person in charge of administering the document and who should be contacted is the General Manager

Email: gerencia.general@procert.net.ve
Phone: +58 (0212) 2674880

1.5.3. CP approval procedures.

The processes associated with the review, approval, modification, or adjustment of the documentation of the PSC PROCERT will be regulated by the documentation and document management policy (AC-PO-0002). This PC will be modified, and the replacement DEB must be approved in case of modification in RFC 6484 or substitution of it and in the regulations of the Superintendence of Electronic Certification Services (SUSCERTE) of the Bolivarian Republic of Venezuela.

1.6. Definitions and Acronyms

CPS – Certificate Practice Statement. A CPS is a document that specifies the practices that a Certificate Authority (CA) of the PSC PROCERT employs in the issuance of certificates under its PKI.

IANA - Internet Assigned Numbers Authority. IANA is responsible for global coordination of the IP addressing system and AS numbers used to route Internet traffic. IANA distributes INR to Regional Internet Registries (RIRs).

INR - Internet Number Resources. INRs are numerical values for three sets of protocol parameters, namely:

- IP addresses version 4,
- Version 6 IP addresses, and
- Identifiers used in routing between Internet domains, currently Border Gateway Protocol-4 AS numbers.

ISP - Internet Service Provider. This is an organization that manages and provides internet services to other organizations.

LIR - Local Internet Registry. In some regions, this term is used to refer to what is called an-ISP in other regions.

NIR - National Internet Registry. This is an organization that manages the distribution of INR for a portion of the geopolitical area covered by a Regional Registry. NIR Form an optional second level in the tree schema used to manage INR.

RIR - Regional Internet Registry. This is an organization that manages the distribution of INR for a geopolitical area.

PKI-Signed Object: An RPKI-signed object is a digitally signed data file. object (other than a certificate or CRL) that is declared to be such by a Standards Track RFC, and that can be validated using certificates issued under this PKI. The content and format of these data constructs depend on the context in which the validation of claims from current INR holdings takes place. Examples of these objects are repository manifests [RFC6486] and Route Origin Authorizations (ROAs) [RFC6482].

Certification Authority (CA): It means an authority trusted by the signatories to create, issue and manage the life cycle of the certificates, which for the purposes of the Decree Law on Data Messages and Electronic Signatures must have the accreditation granted by the Superintendence of Electronic Certification Services (SUSCERTE).

Register Authority (RA): means the entity whose purpose is to provide local support to the PFC PROCT PKI. The RA performs a set of functions aimed at validating, verifying, and conforming the documentation provided, as well as the physical identity of a signatory who opts to purchase an electronic signature or certificate generated by the P.S.C. PROCT PKI.

Certificate chain: Means a chain of multiple certificates required to validate a certificate. Certificate chains are constructed by linking and verifying the electronic signature on a certificate with a public key that is located in a certificate issued by the PROCERT PKI (CA) CA, which is subordinated to and signed by the root certificate generated by SUSCERTE.

Certificate: Means a data structure that uses the CCITT ITU X.509 standard, which contains the public key of an entity together with associated information and presented as "unforgettable", by means of an electronic signature of the Certificate Authority that generated it.

Public Key Certificate: Means the electronic certificate that joins an entity's Public Key with the entity's distinctive identifier and indicates a specific validity period.

Encryption: It means the process by which the simple data of a text is transformed to hide its meaning. Encryption is a reversible process that is carried out through the use of a cryptographic algorithm and a key.

Electronic signature: Means the added data or a cryptographic transformation of a data unit that allows the recipient of the data unit to prove the source and integrity of the data and protect against forgery, for example, from the recipient.

Certification Revoke List (CRL): Means the list of certificates that have been revoked or suspended by the PSC PROCERT.

Online Certificate Status Protocol (OCSP) or Online Certificate Status Protocol: A protocol used to validate the status of a certificate in real time. The response to the requests includes three (3) statuses: valid, revoked, or unknown.

PSC: Stands for Certification Service Provider

Revocation: Means the change of status of a valid or suspended certificate to "revoked" as of a specific date forward.

Certificate Revocation: This means the process of changing the status of a certificate from valid to suspended or revoked. When a certificate has revoked status, this means that an entity should no longer be trusted for any purpose.

Certification Services: Means the services that can be provided in relation to the management of the certificate lifecycle at any level of the ICP hierarchy, including ancillary services such as OCPS services, time-sharing services, identity verification services, Revoked Certificate List (LCR) hosting, etc.

Signatory: Means the entity that has requested the issuance of a certificate within the PFC CERT PKI. The verification process varies according to the nature and, where applicable, the operational role within the PKI corresponding to the certificate that the entity is requesting.

2. Posting and Deposit Responsibilities.

2.1. Repositories.

RPKI-signed certificates, CRLs, and objects (intended for public consumption) MUST be available for download by all relying parties, to allow them to validate this data. This motivates the use of a robust distributed repository system. Each CA MUST maintain a publicly accessible online repository and publish all RPKI-signed objects (intended for public consumption) through this repository in a manner that fits a profile for the resource certificate repository structure.

2.2. Publication of Certification Information.

Each PSC PROCERT PKI CA must publish the certificates (intended for public consumption) that it issues through the repository system. Each PSC PROCERT PKI CA must publish the CRLs (intended for public consumption) that it issues through the repository system. Each PKI CA in the PSC PROCERT MUST publish its PKI signed objects (intended for public consumption) through the repository system.

Each PSC PROCERT PKI CA that issues certificates to entities outside its administrative domain MUST create and publish a CPS that complies with the requirements set forth in this CP; The PSC PROCERT does not maintain entities outside of your domain associated with your PKI to date. Publication means that entities to which the CA issues certificates MUST be able to acquire a copy of the CPS, and they MUST be able to determine when the CPS changes.

2.3. Time or frequency of publication.

The DPC of each PSC PROCERT PKI CA must specify the following information:

- The time period within which a certificate will be published after the CA issues the certificate.
- The time period within which a CA will issue a CRL with an entry for a revoked certificate after revoking that certificate.
- Expired and revoked certificates SHOULD be removed from the RPKI deposit system, upon expiration or revocation, respectively.
- Also, note that each CA MUST publish its CRL prior to the Next Update value in the scheduled CRL previously issued by the CA.

2.4. Access controls in repositories.

Each CA or repository operator MUST implement access controls to prevent unauthorized individuals from adding, modifying, or deleting entries from the repository. A CA or repository operator MUST NOT intentionally use technical means to limit read access to its CPS, certificates, CRLs, or PKI-signed objects. This data is intended to be accessible to the public.

3. Identification and authentication.

3.1. Denomination.

3.1.1. Types of names.

The distinguished name of each PFC PROCUR PKI CA and end-entity consists of a single CommonName (CN) attribute with a value generated by the certificate issuer. Optionally, the serialNumber attribute CAN be included together with the common name (to form a relative terminal set of distinguished names), to distinguish between successive instances of certificates associated with the same entity.

3.1.2. Need for names to be meaningful.
The subject name on each certificate MUST be "meaningful", i.e., the name must convey the identity of the signatory or subject, to the relying parties. The reason here is that certificates issued under the P.S.C. PROCERT PKI are used to identify individuals, grant authorship and non-repudiation, and offer legal proof.

3.1.3. Anonymity or Pseudonym of the Signatories.
Anonymity is not a function of this PKI; therefore, no explicit support is provided for this feature. Likewise, any anonymous request or request that does not allow the identity of the signatory to be established by the RA will not be processed.

3.1.4. Rules for interpreting various forms of names.
Not applicable. All names must be meaningful.

3.1.5. Uniqueness of names.
There is no guarantee that subject names will be globally unique in this PSC PROCERT PKI. Each CA certifies subject names that MUST be unique among the certificates it issues. While it is desirable that these subject names be unique across the PSC PROCERT PKI, the uniqueness of the names within the PSC PROCERT PKI cannot be guaranteed. However, subject names in certificates SHOULD be constructed in a way that minimizes the chances of two entities in the PKI being assigned the same name.

3.2. Initial identity validation.

3.2.1. Method for proving possession of the private key.
Each CA operating within the PSC PROCERT PKI must require each subject to demonstrate proof of possession (PoP) of the private key corresponding to the public key in the certificate, prior to issuing the certificate. Each P.C.I.P.I. PCI CA determines the means by which the PoP is achieved and MUST be declared in the CPS of each P.S.C. P.I. PKI CA declared.

3.2.2. Authentication of the organization's identity.
Each P.S.C. PROCERT PKI CA operating within the context of this PKI MUST employ procedures to ensure that each certificate it issues accurately reflects its records with respect to the organization from which the CA has requested the issuance of an electronic certificate. The specific procedures employed for this purpose MUST be described by the CPS for each PFC PROCT KKI CA.

Relying parties can expect each CA in P.S.C. PROCERT PKI to employ procedures proportionate to those it already uses as a record. This authentication is for the exclusive use of each P.S.C. PROCERT PKI CA in dealing with organizations to which it has issued electronic certificates and should be relied upon outside of this CA-signatory relationship.

3.2.3. Individual Identity Authentication.

Each P.S.C. PROCERT PKI CA operating within the context of this PKI MUST employ procedures to identify each individual in the case of certificates for natural persons or the representatives of each organization in the case of a legal entity. The specific means by which each CA authenticates individuals as representatives of an organization or themselves MUST be described by the CPS for each PFC CERT PKI CA for each PKI CA. Relying parties can expect each CA to employ procedures proportionate to those it already employs as a record to authenticate individuals.

3.2.4. Unverified subscriber information.

A CA MUST NOT include any unverified subscriber data in certificates issued under this certificate policy, except for Subject Information Access (SIA) extensions.

3.2.5. Validation of Authority.

Each CA operating within the context of the PSC PROCERT PKI must employ procedures to verify that a person claiming to represent an organization for which a certificate is issued is authorized to represent that organization in this context. The procedures MUST be described by the CPS for the CA in question. Relying parties can expect each CA to employ procedures proportionate to those it already employs as a registry, to authenticate individuals as representatives of INR holders.

3.2.6. Criteria for Interoperation.

This PKI is not intended or designed to interoperate with any other PKI.

3.3. Identification and authentication for key change requests.

3.3.1. Identification and authentication for routine key change.

Each CA operating within the context of the PSC PROCERT PKI must employ procedures to ensure that an organization requesting a new key is the rightful holder of the certificate to be regenerated and MUST request PoP of the private key corresponding to the new public key. The procedures used for these purposes MUST be described in the PFC PROCT PKI CA CRPD. With respect to owner authentication, relying parties can expect each CA to employ procedures proportionate to those it already employs as a record, in managing signatory data.

3.3.2. Identification and authentication for key renewal after revocation.

Each CA operating on the PSC PROCERT PKI must employ procedures to ensure that an organization requesting a new key after revocation is the same entity for which the revoked certificate was issued and is the rightful holder. The PSC PROCERT PKI CA must require PoPs of the private key corresponding to the new public key. The specific procedures employed for these purposes MUST be described by the CPS for the PFC PROCT PKI CA The specific procedures employed for these purposes MUST be described by the CPS for the P.C.I. PROCT PKI ac. With respect to holder authentication, relying parties can expect each CA to employ procedures proportionate to those it already employs as a registry, in handling signatory requests. Note that there MAY be different procedures for the case where the legitimate subject still possesses the original private key compared to the case where they no longer have access to that key.

3.4. Identification and Authentication for Revocation Request.

Each CA operating within the PSC PROCERT PKI must employ procedures to ensure that:

- An organization requesting revocation is the legitimate holder of the certificate to be revoked.
- Each certificate that you revoke accurately reflects your records regarding the organization to which the CA has distributed the certificate.
- An individual claiming to represent an organization for which a certificate is to be revoked is authorized to represent that organization in this context.

The specific procedures employed for these purposes MUST be described by the CPS for the PFC PROCT PKI CA The specific procedures employed for these purposes MUST be described by the CPS for the P.C.I. PROCT PKI ac. Relying parties can expect each CA to employ procedures proportionate to those it already uses as a registry, in managing certificates and assigning them to signatories.

4. Certificate lifecycle operational requirements.

4.1. Request for a certificate

4.1.1. Who can submit a certificate application?

Anyone interested in acquiring an electronic certificate must apply to the PKI of the PSC PROCERT and comply with the technical and legal requirements for each type of certificate. The request procedure MUST be described in the DPC of each PFC CERT PKI CA.

4.1.2. Enrollment Process and Responsibilities.

The CPS MUST describe the registration process and procedures for each PFC CERT PKI CA. An entity that wants one or more certificates must contact the CSP. PKI PROCERT provide all the technical and legal information that is required. The PKI of the PSC PROCERT is not obliged to handle requests for certificates that do not meet the technical and legal requirements.

4.2. Processing of certificate requests.

CAs SHOULD make use of existing standards for processing certificate requests. Section 6 of the Resource Certificate Profile [RFC 6487] defines the standard certificate request formats that MUST be supported. Each CA MUST define, through its CPS, the certificate request/response standards it employs.

4.2.1. Performing identification and authentication functions.

Existing practices are employed by registries and ISPs to identify and authenticate organizations that receive INR form the basis for issuing certificates to these subscribers. It's important to note that resource PKI MUST be used to authenticate an organization's identity, and to bind subscribers to the INR they have. The PSC PROCERT PKI must ensure the identity of signatories and verify that its procedures for handling certificate requests comply with proper validation of signatories' identity information and verify names of legal organizations, etc.

4.2.2. Approval or Rejection of Certificate Requests.

Certificate applications MUST be approved based on the PSC PROCERT PKI business, technical and legal practices. Each CA MUST follow the procedures specified in Section 3.2.1 to verify that the requestor possesses the private key corresponding to the public key that will be linked to the certificate that the CA issues to the requestor. The details of how certificate requests are approved MUST be described in the CPS of the CA in question.

4.2.3. Time to process certificate requests.

Any application for an electronic certificate must be accompanied by the RA of the PSC PROCT PKI, comply with the RA processes and comply with the payment of the certificate for the processing of the application. Once these steps have been completed, the period for issuing the certificate does not exceed six (6) hours. The processing and issuance of certificates is described in the CPS of the PSC PROCERT.

4.3. Issuance of certificates.

4.3.1. CA actions during certificate issuance.

If a CA determines that the request is acceptable, it MUST issue the appropriate certificate and publish it to the PSC PROCERT PKI Distributed Repository System by publishing the certificate at the CA's headquarters. The signatory must download their certificate and modify the access key to their user within the AR system of the P.S.C. PROCT PKI.

4.3.2. Notification to the Subscriber by the Certificate Issuance CA.

The CA MUST notify the signatory when the certificate is published. The means by which the signatory is notified is by email sent to the email address previously validated by the P.S.C. PROCT PKI RA. The certificate management notification process is defined in the PSC PROCERT CPS.

4.4. Acceptance of the certificate.

4.4.1. Conduct that constitutes acceptance of the certificate.

Within six (6) hours following the validation of all technical and legal requirements, the electronic certificate will be approved, which will be duly notified to the signatory. The download of the certificate and its use constitute the acceptance of the same by the signatory; this information is indicated in the CPS of the PSC PROCERT. Once the electronic certificate is approved by the CA, the certificate MUST be placed in the repository and the signatory notified. This MAY be done without the review and acceptance of the signatory. The deadlines for the publication of the certificate and notification to the subscriber are defined in the CPS of the PSC PROCERT.

4.4.2. Publication of the Certificate by the CA

Certificates MUST be published to the PKI distributed repository system by publishing the certificate to the publishing point of the CA repository according to the conduct described in Section 4.4.1. Procedures for publication MUST be defined by each CA in their CPS.

4.4.3. Notification of Issuance of Certificates by the CA to Other Entities.

The CPS of each CA MUST indicate whether other entities will be notified when a certificate is issued. The PKI of the PSC PROCERT does not maintain a relationship with other entities to date and therefore is not obliged to notify.

4.5. Key pair and use of certificates.

The following is an overview of the usage model for the PCC CERT PKI.

4.5.1. Use of the subscriber's certificate and private key.

Each holder of an INR is eligible to apply for an X.509 [X.509] CA certificate containing the appropriate RFC 3779 extensions. CA resource certificate holders CAN also issue EE certificates to enable verification of the RPKI-signed objects they generate.

4.5.2. Use of certificate and relying party public key.

Reliance on a certificate must be reasonable under the circumstances. If circumstances indicate the need for additional assurances, the relying party must obtain such assurances in order for such reliance to be considered reasonable. Prior to any act of trust, relying parties MUST (1) independently verify that the certificate will be used for a proper purpose that is not prohibited or restricted by this CP (see Section 1.4), and (2) assess the status of the certificate and all certificates in the chain (ending in a trust anchor (TA) accepted by the RP) that issued the certificates corresponding to the certificate in question.

If any of the certificates in the certificate chain have been revoked or have expired, the relying party is solely responsible for determining whether reliance on a digital signature to be verified by the certificate in question is acceptable. Any such reliance is made solely at the risk of the relying party. If a relying party determines that the use of the certificate is appropriate, the relying party must use the appropriate software and/or hardware to perform digital signature verification as a condition of trusting the certificate. In addition, the relying party MUST validate the certificate in a manner consistent with the RPKI certificate profile [RFC6487], which specifies the extended validation algorithm for PKI certificates.

4.6. Certificate renewal.

This section describes the procedures for certificate renewal. Certificate renewal is the issuance of a new certificate to replace a previous one before its expiration. Only the validity dates and serial number (the certificate field, not the DN attribute) are modified. The public key and all other information remain the same.

4.6.1. Circumstance for Certificate Renewal.

A certificate MUST be processed for renewal based on its expiration date or a renewal request from the signatory. Prior to the expiration of an existing signatory's certificate, it is the signatory's responsibility to renew the certificate to maintain continuity of use of the certificate. If the issuing CA initiates the renewal process based on the certificate expiration date, that CA MUST notify the holder prior to the renewal process.

The validity interval of the new (renewed) certificate SHOULD overlap that of the old certificate to ensure continuity of use of the certificate. It is RECOMMENDED that the renewed certificate be issued and published at least 1 week prior to the expiration of the certificate it replaces. The certificate renewal MUST incorporate the same public key as the previous certificate unless the private key has been reported to be compromised. If a new key pair is used, the provisions of Section 4.8 apply.

4.6.2. Who can apply for renewal?

Only the certificate signee or the issuing CA at the signer's request can initiate the renewal process. The certificate signatory MAY requests early renewal, for example, if they expect to be unavailable to support the renewal process during the normal expiration period. An issuing CA CAN initiate the renewal process based on the certificate's expiration date.

4.6.3. Processing of certificate renewal requests.

Renewal procedures MUST ensure that the person or organization seeking to renew a certificate is in fact the authorized signatory of the certificate and the rightful holder of the INR associated with the renewed certificate. The renewal process MUST verify that the certificate in question has not been revoked.

4.6.4. Notification of Issuance of New Certificate to Subscriber.

There are no additional provisions beyond those in Section 4.3.2.

4.6.5. Conduct that constitutes acceptance of a renewal certificate.

There are no additional provisions beyond those in Section 4.4.1.

4.6.6. Publication of the Renewal Certificate by the CA.

There are no additional provisions beyond those in Section 4.4.2.

4.6.7. Notification of Issuance of Certificates by the CA to Other Entities.

There are no additional provisions beyond those in Section 4.4.3.

4.7. Certificate Key Renewal.

This section describes the procedures for renewing the certificate key. Certificate key renewal is the issuance of a new certificate to replace the previous one because the key needs to be replaced. Unlike certificate reissuance, the public key is changed.

4.7.1. Circumstance for the renewal of the certificate key.

Rekeying a certificate MUST be done only, when necessary, based on:

- Knowledge or suspicion of compromise or loss of the associated private key, or
- The expiration of the cryptographic life of the associated key pair

A CA rekey operation has dramatic consequences because it requires the reissuance of all certificates issued by the entity to which the key was changed. Therefore, it should be performed only when necessary and in a manner that preserves the ability of the trusted parties to validate certificates whose validation path includes the entity with a new key.

CA Key Transfer MUST follow the procedures defined in "CA Key Transfer on the PKI" [RFC6489]. Note that if a certificate is revoked to replace RFC 3779 extensions, the replacement certificate MUST incorporate the same public key instead of a new key. This applies when adding INR (no revocation required) and when deleting INR (revocation required (see Section 4.8.1)). If the key renewal is based on a suspected compromise, then the old certificate MUST be revoked.

4.7.2. Who can request certification of a new public key?
The certificate holder can request a re-key. In addition, the CA that issued the certificate MAY choose to initiate a new key based on a verified compromise report.

4.7.3. Processing certificate key change requests.
The rekey process follows the general certificate generation procedures as defined in Section 4.3.

4.7.4. Notification of Issuance of New Certificate to Subscriber.
There are no additional provisions beyond those in Section 4.3.2.

4.7.5. Conduct that constitutes acceptance of a certificate with a new key.
There are no additional provisions beyond those in Section 4.4.1.

4.7.6. Publication of the Certificate Reissued by the CA.
There are no additional provisions beyond those in Section 4.4.2.

4.7.7. Notification of Issuance of Certificates by the CA to Other Entities.
There are no additional provisions beyond those in Section 4.4.3.

4.8. Certificate modification.

4.8.1. Circumstance for the modification of the certificate.
Modifying a certificate occurs to implement changes to the selected attribute values in a certificate. In the context of PKI, the only changes that accommodate the certificate modification are the changes to the INR holdings described by the RFC 3779 extensions and the changes to the SIA extension. When a certificate modification is approved, a new certificate is issued. If the INR holdings are not removed from the certificate, the new certificate MUST contain the same public key and expiration date as the original certificate, but with the SIA extension and/or the extended INR set.

In this case, the revocation of the previous certificate is not required. When previously distributed INRs are removed from a certificate, then the previous certificate MUST be revoked, and a new certificate MUST be issued that reflects the modified INR holdings. (The SIA extension on the new certificate will not change unless a new SIA value is provided by the affected INR holder.)

4.8.2. Who can request the modification of the certificate?

The certificate holder or issuer can initiate the certificate modification process.

4.8.3. Processing of certificate modification requests.

The CA MUST determine that the requested modification is appropriate and that the procedures for the issuance of a new certificate are followed (see Section 4.3).

4.8.4. Notification of Issuance of New Certificate to Subscriber.

There are no additional provisions beyond those in Section 4.3.2.

4.8.5. Conduct that constitutes acceptance of the modified certificate.

There are no additional provisions beyond those in Section 4.4.1.

4.8.6. Publication of the Certificate Modified by the CA.

There are no additional provisions beyond those in Section 4.4.2.

4.8.7. Notification of Issuance of Certificates by the CA to Other Entities.

There are no additional provisions beyond those in Section 4.4.3.

4.9. Revocation and Suspension of Certificates.

4.9.1. Circumstances for revocation.

A certificate MUST be revoked (and published on a CRL) if there is reason to believe that there has been a compromise of a subscriber's private key. A certificate CAN also be revoked to invalidate a data object signed by the private key associated with that certificate. Other circumstances that warrant revocation of a certificate MAY be specified in a CA's CPS. Note: If new INRs are added to an organization's existing distribution, you do not need to revoke the old certificate.

Instead, a new certificate CAN be issued with the old and novel resources and the old key. If the INRs are deleted or if there has been a key compromise, then the old certificate MUST be revoked (and a new key MUST be made in case of key compromise).

4.9.2. Who can request the revocation?

This MUST be defined in the CPS of the organization that issued the certificate.

4.9.3. Procedure for Request for Revocation.

A subscriber MAY submit a revocation request to the certificate issuer. This request MUST identify the certificate to be revoked and MUST be authenticated. The procedures for making the request MUST be described in the DPC of each CA. The RPKI provisioning document [RFC6492] describes a protocol that CAN be used to make revocation requests.

A certificate issuer MUST notify the subscriber when it revokes a certificate. The notification requirement is met by the publication of CRLs. A CA's CPS MUST indicate the means by which the CA will inform a subscriber of the certificate revocation.

4.9.4. Revocation Request Grace Period.

A subscriber MUST request revocation as soon as practicable after the need for revocation has been identified. There is no specified grace period for the subscriber in this process.

4.9.5. Time frame within which the CA must process the revocation request.

No stipulation. Each CA SHOULD specify its expected revocation processing time in its CPS.

4.9.6. Revocation verification requirement for relying parties.

A trusting party MUST acquire and verify the certificate issuer's most recent scheduled CRL, each time the relying party validates a certificate.

4.9.7. CRL emission frequency.

The frequency of CRL issuance MUST be determined by each CA and recorded in its CPS. Each CRL carries a nextScheduledUpdate value, and a new CRL MUST be published at or before that time. A CA MUST set the nextUpdate value when issuing a CRL to indicate when the next scheduled CRL will be issued.

4.9.8. Maximum latency for CRL.

The CPS for each CA MUST specify the maximum latency associated with publishing its CRL to the escrow system.

4.10. Certificate Status Services.

This PKI does not support the use of the Online Certificate Status Protocol (OCSP) [RFC2560] or the Server-Based Certificate Validation Protocol (SCVP) [RFC5055]. This is because it is anticipated that primary PRs (ISPs) will acquire and validate certificates for all participating resource holders. These protocols are not designed for large-scale bulk certificate health checking. PRs MUST check for new CRLs at least once a day. It is RECOMMENDED that PRs perform this check multiple times per day, but no more than 8 to 12 times per day (to avoid excessive access to the repository).

5. Controls of facilities, management, and operations.

5.1. Physical controls.

Each CA MUST maintain physical security controls for its operation that are commensurate with those employed by the organization in managing the distribution of INR. The physical controls employed for AC operation MUST be specified in your CPS. Below are the possible topics that will be covered at the CPS. (These sections are taken from [RFC3647].)

5.1.1. Site Location and Construction
5.1.2. Physical access
5.1.3. Electricity and Air Conditioning
5.1.4. Water exposures
5.1.5. Fire Prevention and Protection
5.1.6. Data Warehouse
5.1.7. Garbage Dump
5.1.8. Off-site backup

5.2. Procedural controls.

Each CA MUST maintain procedural security controls that are commensurate with those employed by the organization in managing the distribution of INR. The procedural safety controls employed for the operation of the AC MUST be specified in your DPC. Below are the possible topics that will be covered at the CPS. (These sections are taken from [RFC3647].)

5.2.1. Trusted Roles
5.2.2. Number of people required per task.
5.2.3. Identification and authentication for each role
5.2.4. Functions that require separation of duties

5.3. Personnel controls.

Each CA MUST maintain personnel security controls commensurate with those employed by the organization in managing the distribution of INR. The details of each CA MUST be specified in your CPS.

5.4. Audit Trail Procedures.

The details of how a CA implements the audit log described in Sections 5.4.1 through 5.4.8 MUST be addressed in its CPS.

5.4.1. Types of events logged.

Audit logs MUST be generated for the basic operations of the certificate authority's computer equipment. Audit logs MUST include the date, time, responsible user or process, and summary content data related to the event. Auditable events include:

- Access to CA IT equipment (e.g., login, logoff).
- Messages received requesting CA actions (for example, certificate requests, certificate revocation requests, commitment notifications).
- Actions for the creation, modification, revocation, or renewal of certificates.
- Publication of any material in a repository.
- Any attempt to change or delete audit data.
- Key generation.
- Software updates and/or AC configuration.
- Clock settings.

5.4.2. Audit trail protection.

The audit trail MUST be protected by current industry standards.

5.4.3. Audit log backup procedures.

The audit trial MUST be backed up to current industry standards.

5.4.4. Vulnerability assessments.

RPKI subsystems of a registry or ISP SHOULD participate in any vulnerability assessment that these organizations run as part of their normal business practice.

5.5. Change of password.

When a CA wants to change the keys, it MUST generate a new certificate containing its new public key. See [RFC6489] for a description of how the key change is affected in the RPKI.

5.6. AC or RA termination.

In the RPKI, each signatory acts as a CA for the specified INRs that were allocated to that entity. The procedures associated with terminating a CA MUST be outlined in the CPS for that CA. These procedures MUST include a provision to notify each entity that issued a certificate to the organization that is operating the CA that it is terminating. Since the RA function MUST be provided by the same entity operating as a CA (see Section 1.3.2), there are no separate stipulations for RAs.

6. Technical safety controls.

Organizations that distribute INR to network signatories have authority for these distributions. This PKI is designed to allow ISPs and network signatories to prove that they are the holders of the INR distributed to them. Consequently, the security controls used by CAs and signatories for this PKI need only be as secure as those that apply to the procedures for managing the distribution of INR data by existing organizations. The details of each CA's security controls MUST be outlined in the CPS issued by the CA.

6.1. Key pair generation and installation

6.1.1. Key pair generation

In most cases, the public key pairs will be generated by the subject, i.e., the organization that receives the INR distribution. However, some CAs MAY offer to generate key pairs on behalf of their subjects at the request of the subjects, for example, to accommodate subscribers who do not have the ability to securely perform key generation. (The CA must verify the quality of the keys only if it generates them; see Section 6.1.6.) Because the keys used in this PKI are not for non-repudiation purposes, the generation of key pairs by Cas does not inherently undermine the security of the PKI. Each CA MUST describe its key pair generation procedures in its CPS.

6.1.2. Delivery of private key to the subscriber.

If a CA provides subscriber key pair generation services, its CPS MUST describe the means by which private keys are delivered to subscribers securely.

6.1.3. Delivery of the public key to the certificate issuer.

When a public key is transferred to the issuing CA for certification, it MUST be delivered through a mechanism that ensures that the public key has not been altered during transit and that the subscriber possesses the private key corresponding to the transferred public key.

6.1.4. Delivery of CA public key to trusted third parties.

CA public keys for all entities (other than trust anchors) are contained in certificates issued by other CAs. These certificates MUST be published in RPKI's distributed repository system. Trusted parties download these certificates from repositories. Public key values and associated data for (assumed) trust anchors are distributed out-of-band and accepted by parties relying on the CSP PROCERT PKI based on locally defined criteria.

6.1.5. Key sizes.

The algorithms and key sizes used in RPKI are specified in "A Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure" [RFC6485].

6.1.6. Generation of public key parameters and quality control

The public key parameters used in the RPKI are specified in [RFC6485]. Each subscriber is responsible for performing quality checks on their key pair. A CA is not responsible for performing such checks for subscribers, except in the case that the CA generates the key pair on behalf of the subscriber.

6.1.7. Key usage purposes (based on the X.509 v3 key usage field)

The key usage extension bit values used in RPKI are specified in the RPKI certificate profile [RFC6487].

6.2. Private key protection and cryptographic module engineering controls.

6.2.1. Cryptographic module standards and controls.

The cryptographic module standards and controls employed by each CA MUST be described in the CPS issued by that CA.

6.2.2. Private Key (N of M) Control of Multiple Persons

CAs CAN employ multi-person controls to restrict access to their private keys, but this is not a requirement for all CAs in the PKI. The CPS for each CA MUST describe what, if any, multiple people controls it employs.

6.2.3. Custody of the private key.

Private key escrow procedures are not required for RPKI.

6.2.4. Private key backup.

Because of the adverse operational implications associated with losing the use of a CA private key in the PKI, each CA MUST employ a secure means to back up its private keys. Details of the procedures for backing up a CA's private key MUST be described in the CPS issued by the CA.

6.2.5. Private key file.

The details of the process and procedures used to archive the CA's private key MUST be described in the CPS issued by the CA.

6.2.6. Private key transfer to or from a cryptographic module.

The details of the process and procedures used to transfer the CA's private key to or from a cryptographic module MUST be described in the CPS issued by the CA.

6.2.7. Private key storage in cryptographic module.

The details of the process and procedures used to store the CA's private key in a cryptographic module and protect it from unauthorized use MUST be described in the CPS issued by the CA.

6.2.8. Method of activating a private key.

The details of the process and procedures used to activate the CA's private key MUST be described in the CPS issued by the CA.

6.2.9. Method of deactivating a private key.

The details of the process and procedures used to disable the CA's private key MUST be described in the CPS issued by the CA.

6.2.10. Method of destroying a private key.

The details of the process and procedures used to destroy the CA's private key MUST be described in the CPS issued by the CA.

6.2.11. Qualification of the cryptographic module.

The security rating of the cryptographic module MUST be described in the CPS issued by the CA.

6.3. Other aspects of key pair management.

6.3.1. Public key file.

Because this PKI does not support non-repudiation, there is no need to archive the public keys.

6.3.2. Certificate Operating Periods and Key Pair Usage Periods

The INRs held by a CA may change periodically when it receives new allocations. To minimize disruption, the CA key pair should NOT change when INR is added to your certificate. If the ISP and subscriber certificates in the network are tied to the duration of the service agreements, these certificates must have validity periods proportional to the duration of these agreements. In any case, the validity period of the certificates MUST be chosen by the issuing CA and described in its CPS.

6.4. Activation data.

Each CA MUST document in their CPS how they will generate, install, and protect their activation data.

6.5. Computer security controls.

Each CA MUST document in its CPS the technical security requirements that it uses for the computer operation of the CA.

6.6. Technical controls of the life cycle.

6.6.1. System development controls.

The CPS for each CA MUST document any system development controls required by that CA, if applicable.

6.6.2. Security management controls.

Each CA's CPS MUST document the security controls applied to the software and equipment used for this PKI. These controls MUST be proportionate to those used for systems used by CAs for INR management.

6.6.3. Lifecycle security controls.

Each CA's CPS MUST document how the equipment (hardware and software) used for this PKI will be acquired, installed, maintained, and updated. This MUST be done in a manner consistent with the way the equipment is handled for INR management and distribution.

6.7. Network security controls.

Each CA's CPS MUST document the network security controls employed for the operation of the AC. These MUST be commensurate with the protection you employ for computers used to manage the distribution of INR.

6.8. Marking the time.

The RPKI does not make use of time stamps.

7. Certificate and CRL profiles.

See the RPKI Certificate and CRL Profile [RFC6487].

8. Compliance Audit and Other Assessments.

The certificate policy for a typical PKI defines the criteria against which potential CAs are evaluated and sets out the requirements they must meet. In this PKI, CAs already have authority for INR management, and PKI simply supports verifying the distribution of these resources to network subscribers. Consequently, any audits and other assessments already used to ensure the security of INR management are sufficient for this PKI. The CPS for each CA MUST describe what audits and other assessments are used.

9. Other business and legal matters.

As outlined throughout this certification policy, organizations that manage the distribution of INR have authority in their roles as stewards of this data. They MUST operate this PKI to allow INR holders to generate digitally signed data that certifies these allocations. Therefore, the way the organizations in question manage their legal and business affairs for this PKI MUST be proportionate to the way they already handle legal and business matters in their existing roles.

Since there is no single set of responses to this section that would apply to all organizations, the topics listed in Sections 4.9.1 through 4.9.11 and 4.9.13 through 4.9.17 of RFC 3647 SHOULD be covered in the CPS issued by each organization. CAs, although not all CAs may choose to address all of these issues.

9.1. Amendments.

9.1.1. Amendment procedure.

The procedure to modify this CP is through a written notification from the IESG in the form of a new (BCP) RFC that updates or makes this document obsolete.

9.1.2. Mechanism and deadline for notification.

Successive versions of the CP will be published with the following mention:

This COP enters into force on 01/08/2025.

9.1.3. Circumstances in which the OID should be changed.

If the IESG judges that the changes in the CP do not materially reduce the acceptability of certificates issued for RPKI purposes, there will be no changes in the CP OID. If the IESG judges that the changes in the CP materially modify the acceptability of the certificates for RPKI purposes, then there MUST be a new CP OID and revision of this CP.

10. Security considerations.

According to X.509, a certificate policy (CP) is "a set of named rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements." A trusting party can use a CP to help decide whether a certificate and the binding it contains are sufficiently reliable and appropriate for a particular application.

This document describes the CP for Resource Public Key Infrastructure (RPKI). There are separate documents (CPS) that cover the factors that determine the degree to which a relying party can trust the embedded link in a certificate. The degree to which such a link can be relied upon depends on several factors, for example, the practices followed by the CA in authenticating the subject; the CA's security operational policy, procedures, and technical controls, including the scope of the subscriber's responsibilities (e.g., in private key protection), and the CA's stated responsibilities and terms and conditions of liability (e.g., warranties, disclaimers of warranties, and limitations of liability).

Because name exclusivity cannot be guaranteed within the RPKI, there is a risk that two or more RPKI CAs will issue certificates and CRLs with the same issuer name. Route validation implementations that conform to the Resource Certification Path Validation algorithm (see [RFC6487]) verify that the same key was used to sign both the target (the resource certificate) and the corresponding CRL.

Therefore, a name collision will not change the outcome. Using the basic X.509 path validation algorithm, which assumes name exclusivity, could result in a revoked certificate being accepted as valid or a valid certificate being rejected as revoked. Relying parties should ensure that the software they use to validate certificates issued under this policy verifies that the same key was used to sign both the certificate and the corresponding CRL, as specified in [RFC6487].

11. Version Control

Version	Reason for Change	Publication	Validity
Issue 1	Emission	1/08/2025	Yes