REUNA Certificate Authority

Certificate Policy And Certification Practice Statement

Version 1.2-0

September 1st, 2025

OID: 1.2.840.113612.5.4.2.2.1.1.1.2

1. Introduction

1.1. Overview

REUNA, Red Universitaria Nacional, is the Chilean National Research and Education Network was founded at 1992 as a not for profit organization, Today it consists of 50 institutions, including universities, consortiums like AURA (Association of Universities for Research in Astronomy) and ANID (Agencia Nacional de Investigación y Desarrollo) and other institutions related to education and research in Chile.

The mission of the REUNA Consortium is to provide its community, with services in Information and Communications Technologies, supported by a highly qualified and committed team, and to promote the inter-university collaboration through its advanced research and education network infrastructure, connecting member institutions with international counterparts. This aims to enhance the quality of their offerings and leverage opportunities that arise through international collaboration.

REUNA CA will issue certificates to members of the REUNA consortium, but if any external research/ education organization in the country wants a certificate issued by the REUNA CA, then the REUNA CA will study the possibility to issue certificates to that organization/unit. The primary qualifier for external organizations requesting credentials is that they must be for research/ education.

This document is a draft of the Certificate Policy and the Certificate Practice Statement. It describes the set of procedure followed by REUNA CA and is structured according to RFC 3647.

1.2. Document name and Identification

Document Title

REUNA CA Certificate Policy and Certification Practice Statement

Document Version

Version 1.2

Document Date

April 8th, 2025

OID assigned

1.2.840.113612.5.4.2.2.1.1.1.2

OID descriptionIso (1) member-body (2) us (840) esnet (l 13612) igtf (5) members (4) issuing-authorities (2) REUNA(2) REUNA CA(1) REUNA CA CP/CPS (1) Version (1.2)

1.2.1. Type of Certificate

The OIDs utilized for the REUNA IGTF PKI are iso (1) member-body (2) us (840) esnet (l 13612) igtf (5) members (4) issuing-authorities (2) REUNA (2) REUNA CA (1) identifiers. REUNA organizes its OID arcs for the various applicable IGTF Certificates described in the applicable CP/CPSes as follows:

Named Object	Policy Identifier
REUNA Certificate Type	1.2.840.113612.5.4.2.2.1.2
Grid Host - Classic	1.2.840.113612.5.4.2.2.1.2.1
Grid Client - Classic	1.2.840.113612.5.4.2.2.1.2.2
Grid Robot - Classic	1.2.840.113612.5.4.2.2.1.2.3
IGTF Classic AP	1.2.840.113612.5.2.2.1

This CP/CPS applies to any entity asserting one or more of the Object IDentifiers (OIDs) identified within this document. When a CA issues a Certificate containing one of the here-specified policy identifiers, it asserts that the Certificate was issued and is managed in accordance with the requirements applicable to that respective policy.

Subsequent revisions to this CP/CPS may be amended with new Certificate and Object Types with corresponding new OIDs.

1.3. PKI Participants

1.3.1. Certificate Authority

REUNA CA provides PKI services for the users of the Chilean Research and Education community (mainly universities) that are involved in Grid activities, it does not issue certificates to subordinate Certification Authorities.

The REUNA CA operations are contracted via the eMudhra IGTF PKI Service which has been Accredited by the IGTF through the APGridPMA. eMudhra IGTF PKI Services are governed by the *emSign Certificate Policy/Certification Practices Statement for IGTF PKI Services* document identified by OID: 1.3.6.1.4.1.50977.1.0.3.1. The REUNA CA is governed by both this REUNA CP/CPS and the emSign CP/CPS for IGTF PKI Services.

1.3.2. Registration Authorities

REUNA CA does not perform the role of a Registration Authority (RA). RAs will be setup as needed to support the target community's activities in the respective institutions. Such trusted intermediaries are formally assigned by REUNA and their identities and contact details are published in an on-line accessible repository.

RAs must sign an agreement with REUNA CA, stating their adherence to the procedures described in this document.

1.3.3. Subscribers

REUNA CA issues certificates to persons, researchers, students (user certificate), computers (host certificate) and services (host application). The entities that are eligible for certification by REUNA CA are all those entities related to the Chilean research and education community.

The certificates issued by REUNA Certificate Authority may not be used for financial transactions and for any commercial usage. The ownership of a certificate from REUNA CA does not imply automatic access to any kind of computing resources.

1.3.4. Relying parties

Relying parties are individuals or organizations using the certificates to verify the identity of subscribers and to secure communication with this subscriber. Relying parties may or may not be subscribers within this CA.

1.3.5. Other participants

No stipulation.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

Certificates issued within the scope of this CP may be used by subscribers for purposes of authentication, digital signature and data encryption.

1.4.2. Prohibited certificate uses

Certificates issued by the REUNA CA must not be used for purposes that violate Chilean law or the law of the country in which the target end entity (i.e. application or host, addressee of an e-mail) is located. Certificates are only valid in the context of academic research and educational activities, any other usage including financial transactions is strictly forbidden.

1.5. Policy administration

1.5.1. Organization administering the document

REUNA - Red Universitaria Nacional
Jose Domingo Canas 2819,
7750268, Nunoa
Santiago, Chile
Tel: +56 2 2337 0340
https://www.reuna.cl

1.5.2. Contact person

The contact person is published on the repository (See 2.1).

1.5.3. Person determining CPS suitability for the policy

The manager of the REUNA CA (see Section 1.5.2) 1s responsible for determining the CPS suitability for the policy.

1.5.4. CPS approval procedures

This CP / CPS document requires the approval of The Americas Grid Policy Management Authority (http:/ /www.tagpma.org) under the classic CA profile of the Interoperable Grid Trust Federation (https://www.igtf.net).

1.6. Definitions and acronyms

Certificate	Equivalent to Public Key Certificate.
Certification Authority (CA)	An entity trusted by one or more users to create and assign public key certificates and be responsible for them during their whole lifetime.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Practice Statement (CPS)	A statement of the practices which CA employs in issuing certificates.
Certificate Revocation List (CRL)	A time-stamped data file, digitally-signed by the issuing CA, containing the list of certificates revoked by that CA.
Certificate Signing Request (CSR)	A standard data file (IETF RFCs 4211, 9045) used to request a digital certificate, digitally signed using the private key for the End Entity requesting the certificate.
Public Key Certificate	A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.
End Entity (EE)	The person, host or service for which a digital credential may be issued, and identified in the credential distinguished name or subject.
Policy Management Authority (PMA)	An entity establishing requirements and best practices for Public Key Infrastructures.
Registration Authority (RA)	An entity that is responsible for identification of the end entity, but that does not sign or issue certificates (i.e. an RA is delegated certain tasks on behalf of a CA).
IGTF	The Interoperable Global Trust Federation establishes and enforces standards for digital authentication for the research and education community worldwide, and maintains a repository of trust anchors for accredited authentication providers. IGTF is managed by three regional policy management authorities, APGridPMA, EUGridPMA, and TAGPMA, which accredit member authentication providers in their respective regions for authentication services according to IGTF authentication profiles.
TAPGMA	The Americas Grid Policy Management Authority represents IGTF members in countries of North, Central and South America and the Caribbean.

EUGridPGMA	The European Grid Policy Management Authority represents IGTF members in countries of Europe, Africa and the Middle East.
APGridPGMA	The Asia Pacific Grid Policy Management Authority represents IGTF members in countries in Asia and the Pacific region.

2. Publication and repository responsibilities

2.1. Repositories

The online repository (website) or information from the REUNA CA is accessible at the URL: https://reuna-ca.reuna.cl/.

2.2. Publication of certification information

REUNA CA website contains:

- The REUNA CA's certificate,
- A link to the CA Portal where certificate information is published,The CRL (Certificate Revocation List),
- All past and current official versions of the CP / CPS.
- Information about the existing RAs,
- Other relevant information about the REUNA CA service.
- A link to the TAGPMA trust anchor repository where the CA root of trust has been previously published.

The REUNA CA will publish the trust anchor in the repository specified by the TAGPMA for this effect, using the method specified in the policy of the trust anchor repository.

2.3. Time or frequency of publication

- In the repository will always be the latest official version of CP / CPS.
- The CRL shall have a lifetime of 30 days at most, the REUNA CA must issue a new CRL at least 7 days before the expiration date or as soon as practically possible after having a revocation. A new CRL must be published as soon as practically possible after its issuance.

2.4. Access controls on repositories

The online repository is maintained on a best effort basis and is available substantially 24 hours per day, 7 days per week.

The CRL, Root certificate and the CP/CPS of the REUNA CA are available without restrictions on downloading and redistribution at the online repository: https://reuna-ca.reuna.cl/

Modification of the CP/CPS is only allowed by the REUNA CA manager.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

The subject name is an X.500 name type, a Distinguished Name. The generic format for a service subject is as follows:

C=CL, O=REUNACA, O=RA, OU=Organization or Department-Unit, CN=service/FQDN The DN

of the subject takes one of the following forms:

For a person:
C=CL, O=REUNACA, O=RA, OU=Organization or Department-Unit, CN = Full username

For a server:
C=CL, O=REUNACA, O=RA, OU=Organization or Department-Unit, CN = host/FQDN

For a service:
C=CL, O=REUNACA, O=RA, OU=Organization or Department-Unit, CN = service/FQDN

Where:
RA is the Register Authority where the end entity requested the certificate.
OU is optional, in case is present represent the Organization or the Department Unit of the end entity.

3.1.2. Name Meanings

The Common Name in a certificate must have a reasonable association with the end entities. For person certificates, the CN must contain the full family name. For host certificates, the CN must be stated as the fully qualified domain name (FQDN).

3.1.3. Anonymity or pseudonym of subscribers

Subscribers cannot be anonymous or pseudonymous. The REUNA RA validates the identity of subscribers.

3.1.4. Rules for interpreting various name forms

The CN component of the subject name in a certificate for a natural person must contain the full family name as it appears in the authentication document proving the name of the subscriber. In addition the character'.' (period) and the character'/' (slash) are allowed in host

and service certificates. The period must be used to separate the DNS host name components and the slash must be used to separate the service name or the keyword "host" from the DNS host name.

Many names have special characters that are not supported by the ASCII character set used to define the subject in the certificate. To work around this problem local substitution rules can be used:

In general national characters are represented by their ASCII equivalent. E.g é, è, à, ç are represented by e, e, a, c. The German "umlaut" characters may receive special treatment: ä, ö, ü are represented by either ae, oe, ue or a, o, u.

3.1.5. Uniqueness of names

The Distinguished Name (DN, a.k.a. Subject) of each certificate issued by REUNA CA is unique among all REUNA CA issued certificates. No other CAs are authorized to issue certificates with DNs of the types described in Section 3.1.1 above

3.1.6. Recognition, authentication, and role of trademarks

No stipulation.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

The RA confirms possession of the private key by verification of CSR (Certificate Signing Request) signature.

3.2.2. Authentication of organization identity

The RA shall verify that the requesting party's organization or a unit of an organization is entitled to get a certificate from the REUNA CA. The organization should be members of the REUNA consortium, if it is not, REUNA CA will study the possibility to issue certificates to that organization/ unit.

The relationship between the subscriber and the organization must be proved through an organization identity card, a legally acceptable document or an official document stamped and signed by an official representative of that organization (i.e. Dean).

The first time an organization/unit wants to get a certificate for a natural person, a server or a service, it has to announce this officially to the appropriate RA and the RA has to ascertain that the organization or organizational unit exists and is entitled to request a REUNA CA certificate. But if an organization wants to establish an RA it must contact the REUNA CA and the REUNA CA must do the checking process.

3.2.3. Authentication of individual identity

Certificate for a user:

- The RA must meet the user in person and authenticate his identity by checking a document accepted by the Chilean law (Chilean national identity card or passport, the document must have a photo-id). During the meeting the individual must present the proof of their current relationship with the organization
- In exceptional cases, for example due to subscriber's geographical remote location, this presentation may be help by video conference. In this situation, an **authenticated** photocopy of all documentation (identity and proof of relationship) with the subscriber's **notarized** signature must be sent by mail/courier to the RA manager (or the CA Manager in the case of setting up an RA) prior to the meeting. The **"authenticated"** and **"notarized"** refer to the verifications made by a legally appointed (under Chilean law) notary public.

Certificate for a host:

- The requestor must be the person responsible for the host.
- The RA must meet the person responsible for the host in person and authenticate his identity by checking a document accepted by the Chilean law (Chilean national identity card or passport, the document must have a photo-id).
- The individual must present the proof of their current relationship with the organization

3.2.4. Non-verified subscriber information

No stipulation.

3.2.5. Validation of authority

Any organization or unit willing to apply for certificates from REUNA CA shall appoint one more representatives who are entitled to answer all the questions related to user certificate requests.

3.2.6. Criteria for interoperation

No stipulation.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

Expiration warnings are sent to subscribers before re-key time. Re-key after expiration uses completely the same authentication procedure as new certificate.

3.3.2. Identification and authentication for re-key after revocation

Re-key of revoked certificates is not performed.

3.4. Identification and authentication for revocation request

The revocation request can be made by the user of the certificate, the RA or the CA when a key compromise has occurred. Such a request from the user must be made by the RA in a signed transfer to the CA. Before revoking a certificate the REUNA CA must properly authenticate the source of the request.

The revocation request can also be performed by anyone with proof that the private key was compromised.

4. Certificate life-cycle operational requirements

4.1. Certificate Application

4.1.1. Who can submit a certificate application

The REUNA CA issues certificates for:

- Natural person,
- Host administered by the requesting organization,
- Services provided on a host that is administered by an eligible organization.

4.1.2. Enrollment process and responsibilities

The requesting party generates the key pair with at least 2048 bits on their system. After storing the private key in a safe place the requesting party must send the request through the RA to the CA.

Subscriber must read and agree to the conditions of the REUNA Subscriber Agreement as outline in section 9.6.3 of this document.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

Users must present an application form to the appropriate RA by email or on paper. The RA may use the REUNA CA administration module to identify all pending CSRs. The RA must meet the user face to face and authenticate the identity by checking a document accepted by the Chilean law (Chilean national identity card or passport, the document must have a photo-id). If the application is approved, then the RA will inform the REUNA CA that the request has been approved. A secure transmission is used for the notification from the RA to the REUNA CA.

In case of a server or service the request can only be submitted by the administrator responsible for the particular host.

The RA must record and archive requests and confirmations.

4.2.2. Approval or rejection of certificate applications

A Certificate request is only allowed for users who do not already have a valid certificate assigned, otherwise renewal or revocation will be proposed. If the user wants more than one certificate, a clear justification must be provided to support this request. If the authentication information proves to be inaccurate or if a request fails to meet the authentication requirements within 7 days after the request has been received by the RA, the request shall be rejected. If the requesting party insists on getting a certificate it has to initiate a new request.

4.2.3. Time to process certificate applications

Certificate issuing and processing is done as soon as practically possible: since identity verifications have been made previously.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

Issuance is completed using the appropriate CA Certificate after fulfilling the requirements of the associated agreements and CP. After issuance is complete, the certificate is stored in a database and notice is sent to the Subscriber.

4.3.2. Notification to subscriber by the CA of issuance of certificate

The CA shall send to the subscriber by email the URL to download the issued certificate, and it shall also send an acknowledgement of the issuance to the appropriate RA.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

The requesting party shall notify the REUNA CA and the appropriate RA of the acceptance of the issued certificate. If there is no acceptance of the certificate in the space of time of 10 days, the RA will request the certificate to be revoked.

Until a Digital Certificate is accepted, it is not published in any Repository or otherwise made publicly available. Without limitation to the generality of the foregoing, the use of a Digital Certificate or the reliance upon a Digital Certificate signifies acceptance by that person, of the terms and conditions of this CP/CPS and the corresponding Subscriber Agreement by which they irrevocably agree to be bound.

4.4.2. Publication of the certificate by the CA

REUNA CA publishes end-entity certificates by delivering them to the Subscriber and through the methods described in section 2.1.

4.4.3. Notification of certificate issuance by the CA to other entities

RAs may receive notification of a certificate's issuance if the RA was involved in the issuance process. The applicable community is notified when a CA Certificate is issued for that community.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

By accepting the certificate the subscriber assures to all participants of the REUNA CA and all parties relying that

- the private key will be maintained in a safe and secure manner,
- no unauthorized person has or will ever have access to the private key of a host or services
- the certificate will solely and exclusively be put to such uses as are in accordance with this Certificate Policy,
- Immediate action will be undertaken by subscriber to revoke the certificate if the data in the certificate is no longer valid or the private key is compromised.
- The suscriber should do a revocation request when they no longer need the certificate.
- Private keys pertaining to host and service certificate may be stored without a passphrase, but must be adequately protected by system methods if stored without passphrase.
- When using software tokens, the private key must be protected with a strong pass phrase, following current best practice in choosing high-quality passwords.

4.5.2. Relying party public key and certificate usage

A relying party must:

Verify the validity of the certificate before using it by

- Checking that the CA that issued the certificate is trustworthy
- Checking that the certificate hasn't expired
- Consult the latest available CRL from REUNA CA

4.6. Certificate renewal

Renewal of certification involves the issuance of a new certificate to the subscriber by the REUNA CA without changing the old key pair. The information contained in the certificate must be without change or modification, and there must be no suspicion of compromise to the private key. The renewal process must be done before the certificate expires, so the new certificate and the old certificate will have an overlap time.

The frequency and total lifetime of renewed certificates are limited to the maximum allowable under the IGTF Assurance Profile for Classic CAs[1]

4.6.1. Circumstance for certificate renewal

Application for certificate renewal can only be made when the term of a certificate nears expiration. The request must be made no more than one month before the certificates expires. The

[1] https://www.eugridpma.org/guidelines/authn-assurance/

REUNA CA may decide to reject such renewal for security reason to avoid issues arising from long exposure of the private key.
Certificates are NOT renewed for EEs with private keys managed in a software-based token. EEs with private keys managed in a software-based token must re-key and request new certificates accordingly (See 4.7).

4.6.2. Who may request renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's certificates.

4.6.3. Processing certificate renewal requests

Upon receipt of the request endorsed to the appropriate RA and after the RA verifies the authenticity of the subscriber and his relationship with the organization (a face to face meeting is necessary), the REUNA CA shall process the renewal as it processes an initial certification request.

Users must present an application form to the appropriate RA by email or on paper. The RA may use the REUNA CA administration module to identify all pending CSRs. The RA must authenticate thr suscriber identity by checking a document accepted by the Chilean law (Chilean national identity card or passport). If the application is approved, then the RA will inform the REUNA CA that the request has been approved. A secure transmission is used for the notification from the RA to the REUNA CA. In case of a server or service the request can only be submitted by the administrator responsible for the particular host.

4.6.4. Notification of new certificate issuance to subscriber

The REUNA CA shall notify the subscriber as described in 4.3.2.

4.6.5. Conduct constituting acceptance of a renewal certificate

The same procedure shall be followed as described in 4.4.1.

4.6.6. Publication of the renewal certificate by the CA

See 4.4.2.

4.6.7. Notification of certificate issuance by the CA to other entities

See 4.4.3.

4.7. Certificate re-key

Basically, the provisions of section 4.6 apply here. However, in the case of a re-key a new key pair will be used.

4.7.1. Circumstance for certificate re-key

When the private key for the EE is changed, or when the private key associated with an issued certificate is managed in a software-based token.

4.7.2. Who may request certification of a new public key

The subscriber who owns a valid certificate may request the certification of a new public key in a CSR also signed with his/her still valid key. If the certificate has already expired, the certificate request procedure as described for initial certification request must be followed.

4.7.3. Processing certificate re-keying requests

Users must generate the new key pair of at least 2048 bits on their system. After storing the private key in a safe place the requesting party must send the request through the RA to the CA, the subscriber must still provide the RA with a proof of relationship with the organization mentioned in the certificate subject name. The re-key process does not require the physical presence of the subject, the proof of relationship could be perform through paper documents sent to the RA by signed email or another secure way.

Re-key requests for expired certificates are not accepted. In this case, the procedure for obtaining a new certificate must be followed.

4.7.4. Notification of new certificate issuance to subscriber

See 4.3.2.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

See 4.4.1.

4.7.6. Publication of the re-keyed certificate by the CA

See 4.4.2.

4.7.7. Notification of certificate issuance by the CA to other entities

See 4.4.3.

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

Certificates must not be modified. All changes are processed as new certificate requests, and replaced certificates must be revoked.

4.8.2. Who may request certificate modification

Not applicable.

4.8.3. Processing certificate modification requests

Not applicable.

4.8.4. Notification of new certificate issuance to subscriber

Not applicable.

4.8.5. Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6. Publication of the modified certificate by the CA

Not applicable.

4.8.7. Notification of certificate issuance by the CA to other entities

Not applicable.

4.9. Certificate revocation and suspension

This section explains the circumstances under which a certificate should be revoked.

4.9.1. Circumstances for revocation

Subscribers must request revocation as soon as possible, but within one working day after detection of loss or compromise of the private key pertaining to the certificate, or if the data in the certificate is no longer valid.

The certificate must be revoked if:

- The certificate contains data that is no longer valid.
- The private key of the subscriber has been changed, lost, stolen or compromised.
- The certificate is no longer needed.
- The RA does not comply with the terms and conditions of the CP/CPS document.
- The subscriber does not comply with the terms and conditions of the REUNA Subscriber Agreement.

4.9.2. Who can request revocation

A certificate revocation can be requested by:

- The subscriber who owns the certificate.
- The REUNA CA or any RA that has proof of a private key compromise.
- The RA which authenticates the subscriber who owns the certificate.

- Any person presenting proof of knowledge that the subscriber's private key has been compromise or the subscriber's data have changed.

4.9.3. Procedure for revocation request

Unless the REUNA CA acts on its own, a revocation request must be made:

- By the subscriber who owns the certificate, properly authenticated, using the online revocation facilities. In case of emergency, the subscriber who owns the certificate must go to the RA as soon as possible.
- The RA must contact the REUNA CA by signed email, or other secure way, and request the revocation of the certificate for one of the reasons in 4.9.1
- By the RA using a signed email or a secure web interface.
- If the CA, RA or a relying party receive a proof from any person that the subscriber's private key has been compromise or the subscriber's data have been changed, the revocation request must be made as soon as practically possible.

4.9.4. Revocation request grace period

No grace period is defined for revocation request. The REUNA CA shall process the authenticated request with priority and publish the revocation (CRL) as soon as possible. The REUNA CA will as soon as practically possible issue the CRL after a revocation.

4.9.5. Time within which CA must process the revocation request

The REUNA CA must process the request for revocation as soon as practically possible.

4.9.6. Revocation checking requirement for relying parties

Before using a certificate the relying parties should check the most recently published CRL in the REUNA CA repository.

4.9.7. CRL issuance frequency (if applicable)

See 2.3.

4.9.8. Maximum latency for CRLs (if applicable)

CRLs for certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation or per requirements in legal agreements and CP, usually within minutes of generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9. On-line revocation/status checking availability

REUNA CA provides an on-line repository where the latest CRL is made available.

4.9.10. On-line revocation checking requirements

Before using any certificate the relying parties should check the CRL. No access control shall limit the possibility to check the CRL.

4.9.11. Other forms of revocation advertisements available

Currently no other forms of revocation advertisements are available.

4.9.12. Special requirements re key compromise

No stipulation.

4.9.13. Circumstances for suspension

Suspension of certificates is not supported.

4.9.14. Who can request suspension

Not applicable.

4.9.15. Procedure for suspension request

Not applicable.

4.9.16. Limits on suspension period

Not applicable.

4.10. Certificate status services

Certificate status services are not supported by the REUNA CA.

4.10.1. Operational characteristics

Not applicable.

4.10.2. Service availability

Not applicable.

4.10.3. Optional features

Not applicable.

4.11. End of subscription

The subscription ends when the certificate expires and is not renewed or the subscriber requests a revocation of his certificate.

4.12. Key escrow and recovery

The REUNA CA does not support key escrow and recovery.

4.12.1. Key escrow and recovery policy and practices

Not applicable.

4.12.2. Session key encapsulation and recovery policy and practices

Not applicable.

5. Facility, management and operational controls

5.1. Physical controls

5.1.1. Site location and construction

The REUNA CA is hosted from secure and diverse data centers operated by eMudhra. The data centers are equipped with logical and physical controls that make REUNA CA operations inaccessible to non-trusted personnel as described in section 5.1.2. The REUNA CA operates under a security policy designed to detect, deter, and prevent unauthorized access to the REUNA CA's operations .

5.1.2. Physical access

The REUNA CA's contractor (eMudhra), protects its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering. The secure parts of REUNA CA hosting facilities are protected using physical access controls making them accessible only to appropriately authorized individuals in layers of security as described here. Access to secure areas of the buildings requires the use of an "access" or "pass" card. The buildings are equipped with motion detecting sensors, and the exterior and internal passageways of the buildings are under constant video surveillance in each subsequent area. REUNA CA securely stores all removable media and paper containing sensitive plain-text information related to its CA operations in secure containers in accordance with its Data Classification Policy.

Access to the data centers housing the CA platforms requires two-factor authentication—the individual must have an authorized access card and pass biometric access control authenticators. These biometric authentication access systems log each use of the access card that specify which layers of security they have access to based on their trusted role status and designated responsibilities described in section 5.2.1.

REUNA CA deactivates and securely stores its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer REUNA CA's private keys. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

REUNA CA personnel perform periodic security checks of the data center to verify that:

1. REUNA CA's equipment is in a state appropriate to the current mode of operation,
2. Any security containers are properly secured,
3. Physical security systems (e.g., door locks) are functioning properly, and
4. The area is secured against unauthorized access.

REUNA CA's administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

5.1.3. Power and air conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and diesel generators provide redundant

backup power. REUNA CA monitors capacity demands and makes projections about future capacity requirements to ensure that adequate processing power and storage are available. REUNA CA's data center facilities use multiple load- balanced HVAC systems for heating, cooling, and air ventilation through perforated-tile raised flooring to prevent overheating and to maintain a suitable humidity level for sensitive computer systems.

5.1.4. Water exposures

The cabinets housing REUNA CA's systems are located on raised flooring, and the data centers are equipped with monitoring systems to detect excess moisture.

5.1.5. Fire prevention and protection

The data centers are equipped with fire suppression mechanisms.

5.1.6. Media storage

REUNA CA protects its media from accidental damage and unauthorized physical access. Backup files are created on a regular basis. REUNA CA's backup files are maintained at locations separate from REUNA CA's primary data operations facility.

5.1.7. Waste disposal

CA media and documentation that are no longer needed for operations are destroyed in a secure manner. All unnecessary copies of printed sensitive information are shredded on-site before disposal.

5.1.8. Off-site backup

REUNA CA maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure. Backup copies of CA Private Keys and activation data are stored for disaster recovery purposes off-site in safe deposit boxes that are accessible only by trusted personnel.

5.2. Procedural controls

5.2.1. Trusted roles

Trusted roles are created in the REUNA CA PKI system in order to ensure that one person acting alone cannot circumvent security safeguards implemented in the CA system. To ensure this the responsibilities are shared by multiple roles and individuals. This is accomplished by creating separate roles and accounts on various components of the CA system, and each role has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles.

The trusted roles within the REUNA CA PKI system defined includes various roles like Admin Officer, Audit Officer, Registration Officer, Security Officer, Systems Officer, etc. These are defined in detail along with their responsibilities as part of internal policy documents, and may be confidential in nature.

The RA role is:

- The RA must be the chief of the department or the host administrator and a paid employee of the specific organization and must be appointed by an Authority responsible for a department or faculty of that organization. The Authority will make a declaration to the CA Manager in writing on the organization's headed note paper, saying that the RA is a person to trust and that he can do the job. The complete information that must be contained in this letter is defined by the CA Manager and is available in the repository.
- The RA is responsible to authenticate and to collect all the information about the End Entity and the organization. (Photo-id, address, phone numbers, email, etc.)
- Archive all the data of the End Entity and also the CSR, confirmation and revocation request.
- Must use signed email or other secure way to communicate with CA and End Entity.

5.2.2. Number of persons required per task

REUNA CA requires that at least two people acting in a trusted role (one the CA Administrator and the other not an Internal Auditor) take action requiring a trusted role, such as activating REUNA CA's Private Keys, generating a CA key pair, or backing up a REUNA CA private key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access.

5.2.3. Identification and authentication for each role

All personnel are required to authenticate themselves to CA and RA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4. Roles requiring separation of duties

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing backups, recording, and record keeping functions;
3. Those performing audit, review, oversight, or reconciliation functions; and
4. Those performing duties related to CA key management or CA administration.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

The associated Policy Authority is responsible and accountable for REUNA CA's PKI operations and ensures compliance with this and any other applicable CP/CPS. REUNA CA's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

5.3.2. Background check procedures

Background check procedures include but are not limited to checks and confirmation of:

- **Previous employment**
- **Professional references**
- **Educational qualifications**
- **Identity Verification**
- **Other relevant government records (e.g. national identifiers, etc.)**

Where the checks and confirmations cannot be obtained due to a prohibition or limitation of law or other circumstances, All Issuing CAs of REUNA CA PKI will utilize available substitute investigation techniques that provide similar information, including background checks performed by applicable Government and/or Private agencies.

For RA's:

- The RA Manager must be a paid employee of the Organization hosting that Registration Authority and must be appointed by an Authority responsible for a Department within that organization.

- The RA Manager must be a member of that Department. The Authority will make a declaration to the CA Manager in writing on the organization's headed note paper, saying that the RA is a person to trust and that he can do the job. The complete information that must be contained in this letter is defines by the CA Manager and is available in the repository.

- The RA Manager will make a declaration to the CA Manager in writing on the organization's headed note paper. The information that must be contained in this letter is defined by the CA Manager also available in the repository.

5.3.3. Training requirements

REUNA CA provides skills training to all employees involved in REUNA CA's PKI operations. The training relates to the person's job functions and covers:

1. Basic Public Key Infrastructure (PKI) knowledge,
2. Software versions used by REUNA CA,
3. Authentication and verification policies and procedures,
4. REUNA CA security principals and mechanisms,
5. Disaster recovery and business continuity procedures,
6. Common threats to the validation process, including phishing and other social engineering tactics, and
7. Applicable industry and government guidelines.

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

REUNA CA maintains records of who received training and what level of training was completed. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. Where competence is demonstrated in lieu of training, REUNA CA maintains supporting documentation.

Internal training is given to the REUNA RA operators.

5.3.4. Retraining frequency and requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. REUNA CA makes all employees acting in trusted roles aware of any changes to REUNA CA's operations. If REUNA CA's operations change, REUNA CA will provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

Retraining of the RAs shall be mandatory when new software or features, as well as new organizational procedures are introduced.

5.3.5. Job rotation frequency and sequence

There is no stipulation about job rotation frequency, but the REUNA CA should maintain updated a list of CA and RA personnel.

5.3.6. Sanctions for unauthorized actions

REUNA CA employees and agents failing to comply with this CP/CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7. Independent contractor requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6. Otherwise, independent contractors and consultants are escorted and directly supervised by Trusted Persons when they are given access to REUNA CA and any of its secure facilities.

5.3.8. Documentation supplied to personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4. Audit logging procedures

5.4.1. Types of events recorded

REUNA CA's systems require identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

REUNA CA enables all essential event auditing capabilities of its CA applications in order to record the events listed below. If REUNA CA's applications cannot automatically record an event, REUNA CA or an RA implements manual procedures to satisfy the requirements. For each event, REUNA CA records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. Event records are available to auditors as proof of REUNA CA's or RA practices.

In generally, REUNA CA audits all activities related to the CA, including security events, authentication to systems, data entry, key generation, private key storage, etc. The systems audited are dependent on platform as well as requirements specified by the community of interest. Anomalies in the system are investigated and tracked.

The following events at a minimum shall be recorded from the RA:

- All the requests and certificates authorized.
- All the revocation requests.

5.4.2. Frequency of processing log

When checking logs, the administrator may perform the checks using automated tools. During these checks, the administrator (1) checks whether anyone has tampered with the log, (2) scans for anomalies or specific conditions, including any evidence of malicious activity, and (3) prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to REUNA CA's operations management committee and are made available to REUNA CA's auditors upon request. REUNA CA documents any actions taken as a result of a review.

5.4.3. Retention period for audit log

Logs are kept on a removable medium for at least 3 years.

5.4.4. Protection of audit log

CA audit log information is retained on equipment until after it is copied by a system administrator. REUNA CA's systems are configured to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. REUNA CA's off-site storage location is a safe and secure location that is separate from the location where the data was generated.

5.4.5. Audit log backup procedures

Every archive log file is backed up on a removable medium every 2 weeks.

5.4.6. Audit collection system (internal vs. external)

Automatic audit processes begin on system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, REUNA CA's Administrators, External Program PMAs, and the correponding Policy Authority (PA) shall be notified and the PA will consider suspending the CA's or RA's operations until the problem is remedied.

5.4.7. Notification to event-causing subject

No stipulation.

5.4.8. Vulnerability assessments

REUNA CA performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. REUNA CA also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that REUNA CA has in place to control such risks. REUNA CA's Internal Auditors review the security audit data checks for continuity. REUNA CA's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5. Records archival

5.5.1. Types of records archived

REUNA CA retain the following information in its archives (as such information pertains to REUNA CA's operations in the CP and legal agreements):

1. Accreditations of REUNA CA,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA,
4. System and equipment configurations, modifications, and updates,
5. Rejection or acceptance of a certificate request,
6. Certificate issuance, re-key, renewal, and revocation requests,
7. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes,
8. Any documentation related to the receipt or acceptance of a certificate or token,
9. Subscriber Agreements,
10. Issued certificates,
11. A record of certificate re-keys,
12. Certificate Revocation List (CRL),

13. Data or applications necessary to verify an archive's contents,
14. Compliance auditor reports,
15. Changes to REUNA CA's audit parameters,
16. Any attempt to delete or modify audit logs,
17. Key generation, destruction, storage, backup, and recovery,
18. Access to Private Keys for key recovery purposes,
19. Export of Private Keys,
20. Approval or rejection of a certificate status change request,
21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,
24. Remedial action taken as a result of violations of physical security, and
25. Violations of the CP/CPS.

5.5.2. Retention period for archive

The minimum retention period is 3 years.

5.5.3. Protection of archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the EPA or as required by law. REUNA CA maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If REUNA CA needs to transfer any media to a different archive site or equipment, REUNA CA will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4. Archive backup procedures

Archive shall be backed up on a removable medium periodically and shall be stored with restricted access.

5.5.5. Requirements for time-stamping of records

REUNA CA automatically time-stamps archived records with system time (non-cryptographic method) as they are created. REUNA CA synchronizes its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

5.5.6. Archive collection system (internal or external)

Archive information is collected internally by REUNA CA. External information from RAs is the responsibility of the RA as per their agreement.

5.5.7. Procedures to obtain and verify archive information

Details concerning the creation and storage of archive information are found in section 5.5.4. After receiving a request made for a proper purpose by a customer, its agent, or a party involved in a dispute over a transaction involving the PKI, REUNA CA may elect to retrieve the information from archival. REUNA CA may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

5.6. Key changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, REUNA CA ceases using the expiring CA Private Key to sign certificates and uses the old Private Key only to sign CRLs, OCSP responses, and OCSP responder certificates. A new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration.

In case of a changeover of the REUNA CA's key pair, an overlap of the old and new keys will exist. While the new key will be used for signing certificates, the older but still valid certificate must be available to verify old signatures - and the private key to sign CRLs - until all certificates signed using the associated private key have also expired. The overlap of the old and new key must therefore be at least as long as the validity of an end entity certificate.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

REUNA CA maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. REUNA CA reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

If the private key of the subscriber is compromised or suspected to be compromised, the appropriate RA has to be informed as soon as practically possible in order to start the certificate revocation process.

If the private key of the CA is compromised or suspected to be compromised the CA manager must inform the RAs of the incident. The RAs must inform to all the subscribers of the incident. Also the CA must revoke all the certificates issued with that private key.

5.7.2. Computing resources, software, and/or data are corrupted

REUNA CA makes regular system backups on at least a weekly basis and maintains backup copies of its Private Keys, which are stored in a secure, off-site location. If REUNA CA discovers that any of its computing resources, software, or data operations have been compromised, REUNA CA assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If REUNA CA determines that a continued operation could pose a significant risk to

Relying Parties or Subscribers, REUNA CA suspends such operation until it determines that the risk is mitigated.

5.7.3. Entity private key compromise procedures

In the case the key of an end entity or an RA is compromised, the corresponding certificate must be revoked. The subscriber who owns the key must inform to all relying parties whom accept this certificate that the private key is compromised. The **RP** can verify the reliability of a credential by contacting the CA.

5.7.4. Business continuity capabilities after a disaster

To maintain the integrity of its services, REUNA CA implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving REUNA CA's primary facility and that REUNA CA be capable of maintaining other services or resuming them as quickly as possible following a disaster. REUNA CA reviews, tests, and updates the BCMP and supporting procedures at least annually.

REUNA CA's systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes REUNA CA's primary CA operations to become inoperative, REUNA CA will re-initiate its operations at its secondary location giving priority to the provision of certificate status information and time stamping capabilities, if affected.

5.8. CA or RA termination

Before terminating its CA activities, REUNA CA will:

- Provide notice and information about the termination by sending notice by email to its customers; and
- Transfer all responsibilities to a qualified successor entity. If a qualified successor entity does not exist, REUNA CA will:

    - transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
    - revoke all certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
    - destroy all Private Keys; and
    - make other necessary arrangements that are in accordance with this CP/CPS

6. Technical security controls

6.1. Key pair generation and installation

6.1.1. Key pair generation

CA key pairs are generated by trusted roles and using a cryptographic hardware device. Typically, the cryptographic hardware is evaluated to FIPS 140-1 Level 3 and EAL 4+. Community requirements may specify a lower version of control. REUNA CA creates auditable evidence during the key generation process to prove that the CP/CPS was followed and role separation was enforced during the key generation process.

The REUNA CA does not generate private keys for subjects. The key pairs for end entities (personal certificates), host or service certificates are generated by the requesting parties themselves on their own system. Under no circumstances should the private key be in the possession of someone other than the owner.

6.1.2. Private key delivery to subscriber

Since each subscriber must generate their own key pair using their own trustworthy software on their personal computer. REUNA CA does not generate and know the subscriber private key.

6.1.3. Public key delivery to certificate issuer

The subscriber will send its public key included in the CSR at time of certificate enrollment.

6.1.4. CA public key delivery to relying parties

The CA certificate, contain its public key, can be obtain by the relying party by downloading from the REUNA CA repository.

6.1.5. Key sizes

The REUNA CA key must be at least of 2048 bits long. For subscribers the key must also be at least 2048 bits long.

6.1.6. Public key parameters generation and quality checking

REUNA CA uses a cryptomodule that conforms to FIPS140-2 and provides random number generation and on- board generation of up to 4096-bit RSA Public Keys and a wide range of ECC curves.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

REUNA CA's certificates may include key usage extension fields that specify the intended use of the certificate and technically limit the certificate’s functionality in X.509v3 compliant software. The use of a specific key is determined by the key usage extension in the X.509 certificate and by the requirements

specified by the relevant legal agreements, CP, and technical specification documents. Subscriber certificates assert key usages based on the intended application of the key pair. In particular certificates to be used for digital signatures (including authentication) set the digitalSignature and/or nonRepudiation bits. Certificates to be used for key or data encryption shall set the keyEncipherment and/or dataEncipherment bits. Certificates to be used for key agreement shall set the keyAgreement bit.

Key usage bits and extended key usages are specified in the certificate profile for each type of certificate as set forth in relevant profiled document.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

End entities shall use their own software to generate their own key pair with strong a passphrase only known the suscriber.

CA Private keys and generally protected using FIPS 140-2 Level 3 systems. External Program communities may elect a different standard for key protection, in which case that standard prevails. Private key holders must take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with the relevant CP and contractual obligations specified in the appropriate legal agreements.

RAs with cryptographic modules will protect the Private Keys at the level specified in the relevant CP, legal agreements, this CP/CPS, and technical specification documents.

6.2.2. Private key (n out of m) multi-person control

REUNA CA's authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons. Backups of CA Private Keys are securely stored off-site and require two- person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations.

6.2.3. Private key escrow

End entity private keys must not be escrowed.

6.2.4. Private key backup

The encrypted private key backup of the REUNA CA is kept offline on a removable media inside a safe where the access is restricted.

6.2.5. Private Key archival

No stipulation.

6.2.6. Private Key transfer into or from a cryptographic module

CA private keys are transferred from one cryptographic module to another to perform CA key backup procedures in section 6.3.4.

All other keys are generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key is encrypted during transport; private keys never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport are protected from disclosure.

Entry of a private key into cryptographic modules use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

When REUNA CA generates CA or RA private keys on one hardware cryptographic module and transfers them into another device, REUNA CA securely transfers such private keys into the second cryptographic module in a manner that prevents loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens.

If REUNA CA pre-generates private keys and transfers them into a hardware token, REUNA CA will securely transfer such private keys into the token in a manner that prevents the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7. Private key storage on cryptographic module

No stipulation beyond that specified in FIPS 140-2.

6.2.8. Method of activating private key

REUNA CA's Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data passphrases for CA private keys comply with recommendations specified in IGTF PKI Technology Guidelines[2].

REUNA CA protects the activation data for their private keys against loss, theft, modification, disclosure, or unauthorized use.

CA administrators are authenticated to the cryptographic token before the activation of the associated private key(s). Entry of activation data is protected from disclosure (i.e., the data is not be displayed while it is entered).

Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their private keys.

[2] https://www.eugridpma.org/guidelines/pkitech/

6.2.9. Method of deactivating private key

REUNA CA's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. REUNA CA never leaves its HSM devices in an active unlocked or unattended state. Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10. Method of destroying private key

REUNA CA/RA personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding certificate is revoked or expired or if the Private Key is no longer needed. REUNA CA may destroy a Private Key by deleting it from all known storage partitions. REUNA CA also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros.

CA keys associated with an External Program will be destroyed according to the requirements in the relevant legal agreements, CPs, technical specification documents, requirement(s), and this CP/CPS.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other aspects of key pair management

6.3.1. Public key archival

The REUNA CA archives copies of Public Keys in accordance with Section 5.5 and per the associated CP requirements or other program documentation.

6.3.2. Certificate operational periods and key pair usage periods

The certificate validity period (i.e., certificate operational period and key pair usage period) are set to the time limits set forth in the relevant certificate profile.

6.4. Activation data

6.4.1. Activation data generation and installation

REUNA CA activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. All REUNA CA personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. REUNA CA employees are required to create non-dictionary, alphanumeric passwords with a minimum length. If REUNA CA uses passwords as

activation data for a signing key, REUNA CA will change the activation data change upon re-key of the CA Certificate.

6.4.2. Activation data protection

REUNA CA protects data used to unlock private keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All REUNA CA personnel are instructed to memorize and not to write down their password or share it with another individual. REUNA CA locks accounts used to access secure CA processes if a certain number of failed password attempts occur. REUNA CA protects the activation data for its private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. These details are maintained in the disaster recovery procedures. REUNA CA maintains an audit trail of Secret Shares, and Shareholders participate in the maintenance of an audit trail.

6.4.3. Other aspects of activation data

Not defined.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

Computer security controls are required to ensure CA operations are performed as specified in the relevant contract agreements, CPs, and technical specification documents.

REUNA CA secures its CA systems and authenticates and protects communications between its systems and trusted roles. REUNA CA's servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices.

6.5.2. Computer security rating

Not stipulation.

6.6. Life cycle technical controls

6.6.1. System development controls

REUNA CA has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. REUNA CA only installs software on CA systems if the software is part of the CA’s operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose

for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by REUNA CA are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the- shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to REUNA CA's operations is scanned for malicious code on first use and periodically thereafter.

6.6.2. Security management controls

REUNA CA has mechanisms in place to control and monitor the security-related configurations of its CA systems. When loading software onto a CA system, REUNA CA verifies that the software is the correct version and is supplied by the vendor free of any modifications. REUNA CA verifies the integrity of software used with its CA processes at least once a week.

6.6.3. Life cycle security controls

No stipulation.

6.7. Network security controls

REUNA CA documents and controls the configuration of its systems, including any upgrades or modifications made. REUNA CA's system is connected to one internal network and is protected by firewalls and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). REUNA CA's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs, OCSP responses (if applicable), OCSP Responder Certificates (if applicable), or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. REUNA CA's security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. REUNA CA's network configuration is available for review on- site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8. Time-stamping

When required, CP, technical specification requirements documents, Certificates, CRLs, and other revocation database entries contain time and date information. Such time information need not be

cryptographic-based. Asserted times are accurate to within three minutes from a trusted and synchronized time source. Electronic or manual procedures may be used to maintain system time.

7. Certificate, CRL, and OCSP profiles

7.1. Certificate profile

All the certificates issued by the REUNA CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280.

7.1.1. Version number(s)

The REUNA CA issues X.509 version 3 certificates only.

7.1.2. Certificate extensions

The extensions to the X.509 v3 certificate that shall be present in the REUNA CA certificates are:

1. For subscriber certificates:

Basic Contraints	Critical, CA: false
Subject Key identifier	Unique identifier of the subject key (composed of 160bits SHA1 hash of the value of the certified public key)
Authority Key Identifier	Keyid (the unique identifier of the issuing CA composed of 160bits SHA1 hash of the value of the REUNA CA public key)
Key Usage	critical, digitalSignature, KeyEncipherment, dataEncipherment
Extended Key Usage	clientAuth, emailProtection, codeSigning, timeStamping
X509v3 CRL Distribution Points	URI of the CRL
Certificate Policy Identifier	The OID of the REUNA CA CP/CPS

2. For server/ services certificates:

Basic Contraints	Critical, CA: false
Subject Key identifier	Unique identifier of the subject **(HASH)**
Authority Key Identifier	Keyid
Key Usage	critical, digitalSignature, KeyEncipherment, dataEncipherment
Extended Key Usage	ServerAuth, clientAuth, emailProtection, codeSigning, timeStamping

XS09v3 CRL Distribution Points	URI of the CRL
Certificate Policy Identifier	The OID of the REUNA CA CP/CPS

3. For the REUNA CA certificate:

Basic Contraints	Critical, CA: true
Subject Key identifier	Unique identifier of the subject key **(HASH)**
Authority Key Identifier	Keyid
Key Usage	critical, keyCertSign, cRLSign
X509v3 CRL Distribution Points	URI of the CRL
Certificate Policy Identifier	The OID of the REUNA CA CP/CPS

7.1.3. Algorithm object identifiers

Algorithm object identifiers are specified in the relevant certificate profile document or requirements document(s). eMudhra strongly recommends the following:

sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
ecdsa-with-sha384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3]

7.1.4. Name forms

Each entity has a unique and unambiguous Distinguished Name (DN) in all certificates issued by the REUNA CA. Depending on the type of the entity the DN has the form defined in section 3.1.1.

7.1.5. Name constraints

There are no other name constraints than those that are to be derived from the stipulations in sections: 7.1.4, 3.1.2 and 3.1.1.

7.1.6. Certificate policy object identifier

The OID of this CP/CPS is: 1.2.840.113612.S.4.2.2.1.1.1.2

7.1.7. Usage of Policy Constraints extension

No stipulation.

7.1.8. Policy qualifiers syntax and semantics

No stipulation.

7.1.9. Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2. CRL profile

7.2.1. Version number(s)

The REUNA CA creates and publish X.509 version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
Issuer Distinguished Name	[As appropriate]
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2. CRL and CRL entry extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3. OCSP profile

Not yet used.

7.3.1. Version number(s)

Not applicable.

7.3.2. OCSP extensions

Not applicable.

8. Compliance audit and other assessments

8.1. Frequency or circumstances of assessment

The CA shall at least once a year assess the compliance of the procedures of each RA with the CP / CPS document in effect.

The frequency of internal operational audits of the CA/RA staff, besides list of CA/RA personnel, which must be performed at least once a year.

8.2. Identity/ qualifications of assessor

Qualified assessors may include peer IGTF Authentication Provider members and institutional auditors in Chile for digital authentication services

8.3. Assessor's relationship to assessed entity

The assessments shall be made by personnel of the REUNA CA or by agreed qualified independent external auditors.

8.4. Topics covered by assessment

The audit will verify that the services provided by the CA and RAs comply with the latest approved version of the CP/ CPS.

Operational records retained by the REUNA CA will be made available to external auditors, subject to the Chilean regulations.

8.5. Actions taken as a result of deficiency

If an audit reports a material noncompliance with applicable law, this CP/CPS, or any other contractual obligations related to REUNA CA's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify REUNA CA, and (3) REUNA CA will develop a plan to cure the noncompliance.

If the assessment reveals a conflict between the provisions of the CP / CPS document and actual practice, the CA must improve the actual practice and, potentially, this also may result in a new version of the CP / CPS document.

If the deficiency has direct consequences on the reliability of the certification process, the certificates (suspected of being) issued under the influence of this problem shall be revoked as soon as practically possible.

8.6. Communication of results

The CA Manager will make the results of an assessment publicly available on the CA web site with as many details of any deficiencies as (s)he considers necessary.

8.7. Self-Audits

The REUNA CA shall carry out at least once a year a self-assessment to check compliance of the operation with the CP/ CPS document in effect.

9. Other business and legal matters

9.1. Fees

No fees will be charged for the certification service provided by the REUNA CA to the community.

9.1.1. Certificate issuance or renewal fees

See 9.1

9.1.2. Certificate access fees

See 9.1

9.1.3. Revocation or status information access fees

See 9.1

9.1.4. Fees for other services

No fees will be charged for access to CP and CPS or other CA status information.

9.1.5. Refund policy

See 9.1

9.2. Financial responsibility

No financial responsibility or liability is accepted for certificates issued under this policy.

9.2.1. Insurance coverage

No stipulation

9.2.2. Other assets

No stipulation

9.2.3. Insurance or warranty coverage for end-entities

No stipulation

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

No stipulation

9.3.2. Information not within the scope of confidential information

No stipulation

9.3.3. Responsibility to protect confidential information

No stipulation

9.4. Privacy of personal information

The RE UNA CA and RAs are responsible for recording, at the time of validation, sufficient information (name, works telephone number, work address, email address) regarding the subscribers to identify the subscriber. Information included in issued certificates and CRLs is public and not considered confidential.

Under no circumstances will the REUNA CA have access to the private keys of any subscriber to whom it issues a certificate.

9.4.1. Privacy plan

No stipulation

9.4.2. Information treated as private

The personal information provided by the subscriber to verify his/her identity will also be kept confidential.

9.4.3. Information not deemed private

Information included in issued certificates and CRLs are not considered confidential. RA contact information is not considered confidential since this information is generally available from the web pages of the RA's employer. Statistics regarding certificates issuance and revocation contain no personal information and is not considered confidential.

9.4.4. Responsibility to protect private information

The responsibility to protect private personal information rests with the REUNA CA and all of its accredited RAs.

9.4.5. Notice and consent to use private information

In the case that the REUNA CA or any of its accredited RAs want to use private information, it must obtain written consent from the subscriber. The subscriber shall not be be construed as having an obligation to provide consent.

9.4.6. Disclosure pursuant to judicial or administrative process

The REUNA CA will not disclose confidential information to any third party unless it 1s authorized to do so by the subscriber or when required by law enforcement officials who present the appropriate judicial documentation.

9.4.7. Other information disclosure circumstances

A subscriber is entitled to request disclosure of all information held by the REUNA CA related to that subscriber only. This information must be released to the subscriber if the CA has received a signed email from the subscriber requesting such information. The CA must recognize requests for the release of personal information from a subscriber properly authenticated.

9.5. Intellectual property rights

The REUNA CA does not claim any intellectual property rights on certificates that has issued. Parts of this document is based on the RFC 3647, RFC 2527 and this document have been inspired and even copied from other CP/CPS: ArmeSFo, IUCC, EstonianGrid, pkIRISGrid, LIP CA, CERN, EELA-LA CA.

Anyone may freely copy from any part of the REUNA CA's Certificate Policy and Certification Practices Statement provided an acknowledgment of the source is made.

9.6. Representations and warranties

9.6.1. CA representations and warranties

REUNA CA does not offer any warranty with regard to its operational procedures, nor does it take responsibility for problems arising from its operation or the use made of the certificates it provides and nor does it give any guarantees about the security or suitability of the service. The REUNA CA only guarantees to verify subscriber's identities according to procedures described in this document. The REUNA CA does not accept any liability for financial loss, or loss arising from incidental damage or impairment, resulting from its operation. No other liability, implicit or explicit, is accepted.

REUNA CA is responsible for issuance and management of certificates referencing this document. REUNA CA shall:

Handle certificate requests and issue new certificates.

- Accept and confirm certification request for acceptable subjects identified by request received from RAs via secure means.
- Issue certificates based on requests from authenticated entities
- Make issued certificates publicly available

Handle certificate revocation requests and certificate revocation:

- Accept and confirm revocation request from acceptable entitles entities or the RAs which approved the subscriber's request, or if the CA has itself reasonable proof that circumstances merit revocation,
- Authenticate revocation before performing revocation,
- Issue a Certificate Revocation List (CRL) according with the rules described in this document,
- Publish the CRL issued,
- Follow the policies and procedures described in this document.

9.6.2. RA representations and warranties

All accredited RAs shall perform their task of identification of requesting parties as described in 3.2.3 and 3.2.2 to the best knowledge. No other warranties are accepted.

It is the RA's responsibility to request revocation of a certificate if the RA is aware that the circumstances for revocation are satisfied.

9.6.3. Subscriber representations and warranties

By requesting a REUNA CA certificate, a subscriber agrees to the following obligations know as the REUNA Subscriber Agreement:

- Read and adhere to the procedures described in this agreement;
- Provide true and accurate information to REUNA CA and/or its delegated
- Registration Authorities and only such information as the suscriber is entitled to submit for the purpose of the REUNA CP/CPS;
- Use the certificate exclusively for authorized and legal purposes, consistent with this document;
- Generate a key pair using a trustworthy method;
- Take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:
- Selecting a strong pass phrase of a minimum recommended 12 characters;
- Protecting the pass phrase from others;
- Always using the pass phrase to encrypt the stored private key; and
- Never sharing the private key with other users;
- Provide correct personal information;

- Notify the REUNA CA as soon as practically possible in case of private key loss or compromise;
- Requesting revocation if the subscriber is no longer entitled to a certificate, or if the information in the certificate becomes wrong or inaccurate.
- Use the certificates for the permitted uses only.

Any breach of stipulations of the REUNA Subscriber Agreement or obligations to which that the subscriber agreed to by requesting a REUNA CA certificate will cause that the certificate will be revoked as soon as practically possible.

9.6.4. Relying party representations and warranties

A relying party should accept the subscriber's certificate for authentication purposes if:

- It is familiar with the REUNA CA's CP/CPS that generated the certificate before drawing any conclusion on the trust of the subscriber's certificate,
- It has verified the authenticity of the REUNA CA root certificate,
- The certificate is being used for the permitted uses only,
- Validate the certificate by verifying it is not on the REUNA CRL.
- It has checked the status of the certificate to their own satisfaction prior to reliance.

9.6.5. Representations and warranties of other participants

No stipulation.

9.7. Disclaimers of warranties

The REUNA CA uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP / CPS document. However, it declines to offer any warranties as to their full correctness.

Also, the REUNA CA cannot be held responsible for any misuse of its certificate by a subscriber or any other party who managed to acquire possession of the corresponding private key, nor of any unchecked acceptance of any of its certificates by a relying party.

Any relying party that accepts a certificate for any usage for which it was not issued does so completely at its own risk and responsibility.

9.8. Limitations of liability

The REUNA CA declines any liability for damages incurred by a relying party accepting one of its certificates or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party. It can also decline any liability for

damages arising from the non-issuance of a request certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting m conformance with this CP/CPS.

9.9. Indemnities

The REUNA CA declines to make any payment of indemnities for damages arrising from the use or rejection of certificates it issues. End entities shall be held responsible and shall indemnify and hold harmless the REUNA CA, and all appropriate RAs operating under this CP/CPS, against all claims and settlements resulting from fraudulent information provided with the certificate application. Relying parties shall be held responsible and shall indemnify and hold harmless the REUNA CA under this CP/CPS against all claims and settlements resulting from the use and acceptance of a certificate that violates the provisions of this CP / CPS document.

9.10. Term and termination

9.10.1. Term

This document comes into effective after its publication on the web site of the REUNA CA and the starting date announced there. No term is set for its expiration.

9.10.2. Termination

This CP/ CPS remains effective until it is superseded by a newer version.

9.10.3. Effect of termination and survival

The text shall remain available for at least 2 years after the last certificate issued under this CP/ CPS expires or is revoked.

9.11. Individual notices and communications with participants

All communications between the CA and its accredited RAs must be via a secure channel. All communications between the CA or an RA and a subscriber must be in a secure way in order to have the value of a proof. All requests for any action must be made by a secure way.

9.12. Amendments

9.12.1. Procedure for amendment

Amendments to this CP /CPS must undergo the same procedures as for the initial approval (see section 1.5.4). Rephrasing provisions to improve their understandability as well as pure spelling corrections are however not considered amendments.

9.12.2. Notification mechanism and period

The amended CP/CPS document shall be published on the REUNA CA web pages at least 2 weeks before it becomes effective.

9.12.3. Circumstances under which 01D must be changed

Substantial changes shall cause the OID to be changed. The decision is made by the CA manager of the REUNA CA and submitted to the TAGPMA for approval.

9.13. Dispute resolution provisions

Disputes arising out of the CP/ CPS shall be resolved by the Manager of the REUNA CA.

9.14. Governing law

The REUNA CA and its operation are subject to the laws of India and management processes to Chilean law. All legal disputes arising from the content of this CP /CPS document, the management of the REUNA CA and their accredited RAs, the use of their services, the acceptance and use of any certificate issued by the REUNA CA shall be resolved according to Chilean law.

9.15. Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of an REUNA CA certificate must comply with the Chilean law. Activities initiated from or destined for another country other than Chile must also comply with that country's law.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

This CP / CPS document supersedes any prior agreements, written or oral, between the parties covered by this present document.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

Should a clause of the present CP / CPS document become void because it is conflicting with the governing law (see section 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, this clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5. Force Majeure

Events that are outside the control of the REUNA CA will be dealt with immediately by the TAGPMA.

9.17. Other provisions

No stipulation