Reuna
Red
Universitaria
Nacional

REUNA Certificate Authority

Certificate Policy
And
Certification Practice Statement

Version 1.0

April 2nd, 2007

1. INTRODUCTION

1.1 Overview

REUNA, Red Universitaria Nacional (National University Network - Chile), is a non-profit private corporation initially formed by 14 Chilean universities and the National Commission for Scientific and Technological Research (CONICYT). It is an initiative of university collaboration that only counts on the technological infrastructure of advanced networks of an academic nature, dedicated to research and development in Chile.

REUNA provides their community with services in matters regarding information and communication technologies, and is supported by a highly qualified and committed work team. The objective of REUNA is to promote inter-university work through the use of its infrastructure of advanced networks and education network, connecting its member institutions with their international peers, in order to increase the quality of their supply and take advantage in a collaborative way of the opportunities that the internationalization gives.

REUNA CA will issue certificates to members of the REUNA consortium, but if any external research/education organization in the country want 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, network requirements, etc.

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 1.0
Document Date
April 2, 2007
OID assigned
1.2.840.113612.5.4.2.2.1.1.1.0
OID description

1.2.840.113612.5.4.2	IGTF
	iso(1) member-body(2) us(840) esnet(113612)
	igtf(5) members(4) issuing-authorities(2)

2	REUNA
1	REUNA CA

1	REUNA CA Certification Policy and CPS
1.0	Version of this CP/CPS

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.

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
Canadá 239,
750-0782, Providencia
Santiago, Chile
Tel: +56 2 3370340
Fax: +56 2 2040865
http://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) is 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 International Grid Trust Federation (http://www.gridpma.org).

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 a certification authority employs in issuing certificates.
Certificate Revocation List (CRL)	A time stamped list identifying revoked certificates
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.
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).

2 Publication and repository responsibilities

2.1 Repositories

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

2.2 Publication of certification information

REUNA CA website contains:

- The REUNA CA's certificate,
- All publicly accessible certificates issued by this CA,
- The CRL (Certificate Revocation List),
- All past and current officials versions of the CP/CPS.
- Information about the existents 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, issued certificates and the CP/CPS of the REUNA CA are available without restrictions on downloading and redistribution at the online repository: http://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**=Organization, **OU**=Department-Unit, **CN**=service/FQDN

The DN of the subject takes one of the following forms:
For a person:
C=CL, O=REUNACA, O = Organization, OU = Department-Unit, CN = Full username

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

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

Some examples of certificate subjects that obey to the REUNA CA subject-naming scheme are as follows:

C=CL, O=REUNACA, **O**=UCHILE, **OU**=DIM-CMM, **CN**= Juan Carlos Maureira Bravo
C=CL, O=REUNACA, **O**=UCHILE, **OU**= DIM-CMM, **CN**=uhira.dim.uchile.cl
C=CL, O=REUNACA, **O**=UCHILE, **OU**= DIM-CMM, **CN**=ldap/uhira.dim.uchile.cl

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 must be unique for all certificates issued by the REUNA CA.

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).
- The individual must present the proof of their current relationship with the organization

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 1024 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 in person and authenticate his/her 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 transmition 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, he/she must specify the reason why he/she should have more than one certificate. 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

The CSR shall be transferred to the off-line computer which holds the private key of the REUNA CA. On this computer is where the certificate is signed. The signed certificate shall be transferred back to the online REUNA CA server.

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 certificate will be revoked.

4.4.2 Publication of the certificate by the CA

REUNA CA will publish on its web server the certificates as soon as they are issued.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

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.
- He should do a revocation request if the user no longer needs the certificate.

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.

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 REUNA CA may decide to reject such renewal for security reason to avoid issues arising from long exposure of the private key.

4.6.2 Who may request renewal

Renewal of a certificate must always be requested by the subscriber.

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 no 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 his/her 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 transmition 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 parameters of the certificate are changed or when the old certificate is about to expire.

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 1024 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

The certificate must not be modified, it must be revoked if the data in the certificate is no longer valid, and a new key pair must be generated and a new certificate must be requested.

4.8.2 Who may request certificate modification

The subscriber who owns the original certificate may submit a request for re-key and revocation of the original certificate.

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

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)

The new CRL shall be copied to a removable device as soon as practically possible after creation at the off-line CA computer and transferred without delay to the on-line repository.

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 offline in a secure environment in the REUNA Computer Center locate at the following address:

Canadá 239, Providencia
750-0782, Santiago
Chile

5.1.2 Physical access

The REUNA CA operates in a controlled environment, where the access is restricted to authorized people. The private key is kept in a safe deposit with restricted access.

5.1.3 Power and air conditioning

All the servers in the REUNA computer center are connected to uninterrupted power supply units, and air conditioners are used to moderate temperature.

5.1.4 Water exposures

The REUNA computer center is on a fourth floor so no floods are expected.

5.1.5 Fire prevention and protection

There are fire extinguishers (chemical powder) with appropriate contents for computer environment, also the structure of the computer center, floor, walls, etc., are made of non combustion material.

5.1.6 Media storage

The REUNA CA key is stored on several removable storage media. Backup copies of CA related information are kept in a fireproof safe with restricted access.

5.1.7 Waste disposal

Waste containing important data (cryptographically important data like: private key, pass phrase or personal data) must be shredded. Electronic media must be physically/mechanically destroyed before disposal.

5.1.8 Off-site backup

No off-site backups are currently performed.

5.2 Procedural controls

5.2.1 Trusted roles

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

There is one REUNA CA manager, however it is important to remark that REUNA CA is inside the Technical Management Area of REUNA, which is composed of a Technical Manager, Network Engineers (CA Manager) and the Network Operation Center Staff (A NOC Chief plus network operators). Mainly, the activities related with high level decisions will be made by the CA manager and the operational procedures also will be shared with the network operation staff, taking into account all the security issues mentioned in this document.

5.2.3 Identification and authentication for each role

No stipulation.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All REUNA CA personnel shall have system administrator or analyst experience and be familiar with the importance of a PKI, and they must be technically and professionally competent.

5.3.2 Background check procedures

- 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 defined 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

Internal training is given to the REUNA CA and RA operators.

5.3.4 Retraining frequency and requirements

Retraining of the RA and CA 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

In the event of unauthorized actions, abuse of authority or unauthorized use of the entities systems by the CA or RA operators, the CA manager must revoke the privileges concerned.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

Personnel have access to a restricted part of REUNA CA website where all operational procedures can be found.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following events shall be recorded from the REUNA CA signing computer:

- All the requests and certificates issued.
- All the revocation requests.
- All the CRL issued.
- The login/logout information of the CA computer.

The following events shall be recorded from the RA:

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

5.4.2 Frequency of processing log

The log file shall be analyzed once a month, or after a potential security breach is suspected.

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

Audit logs are only accessible to the administrators of REUNA CA and to external authorized audit personnel.

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)

Internal.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

See 5.4.1.

5.5.2 Retention period for archive

The minimum retention period is 3 years.

5.5.3 Protection of archive

The archive shall be accessible to the administrators of REUNA CA and to authorized personnel.

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

Archive records are time-stamped. For online systems the clock is synchronized through NTP (ntp.shoa.cl). For offline systems the clock is manually set and periodically verified.

5.5.6 Archive collection system (internal or external)

Internal.

5.5.7 Procedures to obtain and verify archive information

No stipulation

5.6 Key changeover

As the key generation is done by the end entities for their own use, no provision is made for a key changeover.

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

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

If the CA staff detects that hardware, software or data are corrupted or damaged, it must as soon as practically possible recover the system by using the backed up data.

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

Not stipulation.

5.8 CA or RA termination

In case of CA termination, the CA must:

- Inform the Registration Authorities, all subscribers, and relying parties with which the CA has agreements.
- The CA must notify at least 60 days in advance before termination of the CA.
- Make publicly available information of its termination.
- Revoke all certificates.
- Stop issuing certificates.
- Publish the last CRL.
- Destroy private keys and all copies.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pair generation for the REUNA CA is generated by authorized CA staff on a computer not connected to the network. The key is generated using trustworthy software.

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 subscriber the key must be at least of 1024 bits long.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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

Private Key for end entity is used for digital signature, non repudiation, proxy creation, message integrity, key encryption, and data encryption.

The CA private key is used to sign certificates and CRLs.

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 pass phrase at least 12 characters long and only known to him/her.

The REUNA CA private key is generated using trustworthy software with a strong pass phrase at least 15 characters long. This encrypted private key shall be stored on an offline computer used to issue the certificates and on a removable media stored in a safe.

The private CA key shall not be on a permanent disc of any online computer.

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

No stipulation.

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

The CA private key is protected with strong a pass phrase of at least 15 characters. The pass phrase is known only to specified REUNA CA personnel.

6.2.7 Private key storage on cryptographic module

The CA private key is activated by a pass phrase which is kept in a safe. The safe which contains the pass phrase does no contain any copy of the private key.

6.2.8 Method of activating private key

The activation of the CA private key is performed by providing the pass phrase.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

After termination of the CA, all media that contain the CA private key must be securely and permanently destroyed according to the best current practice.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The REUNA CA shall archive all issued certificates on removable media and stored off-line in a secure place.

6.3.2 Certificate operational periods and key pair usage periods

There is no stipulation about the validity period of the key pair. But the certificates issued by the REUNA CA to end entities have a validity period of one year and one month (the overlapping period, see 4.6) or less if the affiliation of the requesting party to one of the organization members of REUNA is less than one year.

The REUNA CA certificate has a validity period of 10 years.

6.4 Activation data

6.4.1 Activation data generation and installation

The private key of the REUNA CA is protected by a strong pass phrase of at least 15 characters long (see 6.2.1) and known only to specified REUNA CA personnel. The private key of the subscriber must be protected by a strong pass phrase of at least 12 characters long.

6.4.2 Activation data protection

The pass phrase must only be known by the owner of the private key. In case of the REUNA CA pass phrase is known by the REUNA CA manager and operator and a backup of the pass phrase is kept in a safe.

6.4.3 Other aspects of activation data

Not defined.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The CA signing machine is a Linux based system with all reasonable security features, and it is kept off-line all the time. The server hosting the CA on-line system is on a dedicated machine, Linux based, with all reasonable security features and protected also by a firewall and no other unnecessary services are running.

The server will receive occasional patches and other adjustments if the security risk warrants, in the judgment of REUNA CA staff.

6.5.2 Computer security rating

Not stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

The Certificate Authority's signing machine will never be connected to a computer network under any circumstances. It is also located in a secure environment and managed by trained personnel.

The server which is the REUNA CA online repository is protected by a suitably configured firewall.

6.8 Time-stamping

All time stamping entries created on the online servers at the REUNA CA is based on the network time provide by the time server of SHOA (Servicio Hidrográfico y Oceanográfico de la Armada de Chile).

The hardware clock of the offline system for the certificate and CRL signing, which determines the time stamping of the certificates and CRLs, will be synchronized by the operator whenever the computer starts.

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, nonRepudiation, KeyEncipherment, dataEncipherment
Extended Key Usage	clientAuth, emailProtection, codeSigning, timeStamping
Netscape Cert Type	SSL Client, S/MIME, Object Signing
Netscape Comment	CP/CPS version and CA name
Issuer Alternative Name	REUNA CA email address
X509v3 CRL Distribution Points	URI (http://reuna-ca.reuna.cl) of the CRL, noReasonFlags shall be set
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, nonRepudiation, KeyEncipherment, dataEncipherment
Extended Key Usage	ServerAuth, clientAuth, emailProtection, codeSigning, timeStamping

Netscape Cert Type	SSL Client, SSL Server, S/MIME, Object Signing
Netscape Comment	CP/CPS version and CA name
Issuer Alternative Name	REUNA CA email address
X509v3 CRL Distribution Points	URI (http://reuna-ca.reuna.cl) of the CRL, noReasonFlags shall be set
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, digitalSignature, nonRepudiation, keyCertSign, cRLSign
Netscape Cert Type	SSL CA, Email Certificate Authority, Object Signing
Netscape Comment	STRING
X509v3 CRL Distribution Points	URI of the CRL, noReasonFlags shall be set
Certificate Policy Identifier	The OID of the REUNA CA CP/CPS

7.1.3 Algorithm object identifiers

The OIDs for algorithms used for signatures of certificates issued by the REUNA CA are according to:

▪ hash function:	id-sha1	1.3.14.3.2.26
▪ encryption:	rsaEncryption	1.2.840.113549.1.1.1
▪ signature:	sha1WithRSAEncryption	1.2.840.113549.1.1.5

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: 1.2.840.113612.5.4.2.2.1.1.1.0

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.

7.2.2 CRL and CRL entry extensions

The REUNA CA shall issue complete CRLs for all certificates issued by itself independently of the reason for the revocation. The reason for the revocation shall not be included in the individual CRL entries.

The CRL shall include the date by which the next CRL should be issued. A new CRL shall be issued before this date or if new revocations are issued (for more details see section 4.9.7).

The CRL extensions that shall be included are:

- The Authority Key Identifier
- The CRL Number

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 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.
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

Not defined

8.3 Assessor's relationship to assessed entity

The assessments shall be made by personnel of the REUNA CA. Any governmental organization or academic institution with the appropriate jurisdiction can perform an external audit. If other trusted CAs or relying parties request an external assessment, the requesting party must pay for the costs of the assessment.

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.

8.5 Actions taken as a result of deficiency

In case of a deficiency, the REUNA CA manager shall take immediate action by announcing the steps to follow to remedy the deficiency, this announcement shall include a timetable.

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.

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 REUNA 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 under the impression that he/she has an obligation to agree.

9.4.6 Disclosure pursuant to judicial or administrative process

The REUNA CA will not disclose confidential information to any third party unless it is 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 he/she 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 in conformance with this CP/CPS.

9.9 Indemnities

The REUNA CA declines to make any payment of indemnities for damages arising 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 OID 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 Chilean law. All legal disputes arising from the content of this CP/CPS document, the operation 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.