Instituto Brasileiro para o Desenvolvimento do Silício

Fundação de Amparo à Pesquisa do Estado de São Paulo

The Academic Network at São Paulo Grid Certification Authority

Certificate Policy and Certification Practice Statement

Version 2.0 -- 06 Sep 2018

CONTENTS

1. INTRODUCTION

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the document (either the CP or the CPS being written) is targeted.

This document is a combined certification policy and certificate practice statement. It describes the set of procedures followed by the **Academic Network at São Paulo Grid Certification Authority** (that operates as a traditional X.509 Public Key Certification Authority which issues long-term credentials to end-entities) as well as outlining the responsibilities of the involved parties.

This document follows the framework and structure outlined in the Internet Engineering Task Force's RFC 3647 [Chokani03] (extracts of which have been included in this document in a blue courier font to assist the reader in understanding the certificate policies and certification practice statements). Compliance of this document with the current minimum requirements of the International Grid Trust Federation (IGTF) Classic CA profile [CCA06], maintained by the EUGridPMA, is highlighted in Section 10.

This document is based on (and is in fact almost identical to) the TAGPMA approved CP/CPS (OID: 1.3.6.1.4.1.24839.2.1.10.2.1.1.0) of the UFF Latin American Catch-all Grid CA (UFF LACGrid CA).

1.1 OVERVIEW

This subcomponent provides a general introduction to the document being written. This subcomponent can also be used to provide a synopsis of the PKI to which the CP or CPS applies. For example, it may set out different levels of assurance provided by certificates within the PKI. Depending on the complexity and scope of the particular PKI, a diagrammatic representation of the PKI might be useful here.

The *Instituto Brasileiro para o Desenvolvimento do Silício* (Brazilian Institute for the Development of Silicon - IBDF) is a nonprofit entity qualified as *Organização da Sociedade Civil de Interesse Público* (Organization of Civil Society of Public Interest - OSCIP) that holds the Academic Network at São Paulo (ANSP) research program, created to organize and maintain many projects related with Internet and sponsored by *Fundação de Amparo à Pesquisa do Estado de São Paulo* (Foundation for Research Support of the State of São Paulo, or FAPESP). FAPESP is a public foundation located in São Paulo, Brazil, with the aim of providing grants, funds and programs to support research, education and innovation of private and public institutions and companies in the state of São Paulo. ANSP implemented and manages a WAN connecting the most relevant universities and research centers in the State of São Paulo and is also responsible for the maintenance and operation of the **Academic Network at São Paulo Grid Certification Authority** (hereinafter known as the **ANSPGrid CA**). The main objective of the ANSPGrid CA is to issue certificates to support academic

research activities in the e-Science and Grid computing domains in all Brazilian territory.

This Certificate Policy and Certification Practice Statement (CP/CPS) document describes the:

a) Applicability of certificates signed by the ANSPGrid CA;
b) Operational practices employed by the ANSPGrid CA.

This and any subsequently approved CP/CPS document can be found on the ANSPGrid CA web site http://gridca.ansp.br/. Currently, the operation of the Academic Network at São Paulo Grid Certification Authority is funded by research grant from FAPESP.

1.2 DOCUMENT NAME AND IDENTIFICATION

This subcomponent provides any applicable names or other identifiers, including ASN.1 object identifiers, for the document. An example of such a document name would be the US Federal Government Policy for Secure E-mail.

Title:	Academic Network at São Paulo Grid CA Certificate Policy and Certification Practice Statement.
Version:	Version 2.0.
Date:	06 Sep 2018.
Approved:	At the Monthly TAGPMA Conference Call in April 18th 2012
Expiration:	This document is a valid until further notice.

ASN.1 OID: The following unique Object Identifier (OID) identifies this CP/CPS

1.3.6.1.4.1.19550.3.1.2

The next paragraph describes the meaning of the OID: iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Academic Network at Sao Paulo (ANSP) (19550) ANSPGrid CA (3) CP/CPS (1) Version (2).

1.3 PKI PARTICIPANTS

This subcomponent describes the identity or types of entities that fill the roles of participants within a PKI.

The ANSPGrid CA issues certificates to members of academic and research communities **in Brazil**, for e-Science and Grid computing related activities.

1.3.1 Certification authorities

The entities that issue certificates. A CA is the issuing CA with respect to the certificates it issues and is the subject CA with respect to the CA certificate issued to it. CAs may be organized in a hierarchy in which an organization's CA issues certificates to CAs operated by

subordinate organizations, such as a branch, division, or department within a larger organization.

All certificates will only be issued under TAGPMA approved versions of the CP/CPS and must be signed by the ANSPGrid CA. The ANSPGrid CA does not issue certificates to subordinate Certification Authorities.

1.3.2 Registration authorities

The entities that establish enrollment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA. Subordinate organizations within a larger organization can act as RAs for the CA serving the entire organization, but RAs may also be external to the CA.

The RA at ANSP will be the principal (catch-all) Registration Authority for the ANSPGrid CA. End entity authentication is delegated to RAs which will be setup as needed to support the target community's activities in the respective institutions under the laws of the country in which that organization resides. A list of currently active RAs for the ANSPGrid CA is available from the CA's website http://gridca.ansp.br/.

Registration authorities must be operated by organizations related with the academic community in Brazil. RAs must sign an agreement contract with the ANSPGrid CA where they assume the obligation of following the procedures imposed by this CP/CPS and the ANSPGrid CA for their operation and authentication of certificate requests. The RAs should be operated by full time members of staff of their respective organization.

1.3.3 Subscribers (End Entities)

Examples of subscribers who receive certificates from a CA include employees of an organization with its own CA, banking or brokerage customers, organizations hosting e-commerce sites, organizations participating in a business-to-business exchange, and members of the public receiving certificates from a CA issuing certificates to the public at large.

The ANSPGrid CA issues certificates for e-Science activities performed within the Grid computing community in Brazil. The CA will issue personal, server and service certificates for entities related with the following organizations:

a) academic organizations (e.g. public and private universities and educational institutes);
b) academic research centres (either public or private, non-profit ones); and,
c) other organizations with research and development (R&D) affiliations with one of the above classes of organization.

The subject entities for certificates are of the following types:

a) employees, researchers and students related with the above organizations; or,
b) computer systems and services related with the above organizations;

All subjects will be uniquely identified for the entire lifetime of the ANSPGrid CA, not just the period of validity of the certificate.

1.3.4 Relying parties

Examples of relying parties include employees of an organization having its own CA who receive digitally signed e-mails from other employees, persons buying goods and services from e-commerce sites, organizations participating in a business-to-business exchange who receive bids or orders from other participating organizations, and individuals and organizations doing business with subscribers who have received their certificates from a CA issuing certificates to the public. Relying parties may or may not also be subscribers within a given PKI.

Relying parties may be:

a) natural persons receiving signed e-mails, or accessing hosts or services
b) hosts to which certificate owners login or send processes or jobs
c) services called on by owners of a certificate

1.3.5 Other participants

Such as certificate manufacturing authorities, providers of repository services, and other entities providing PKI-related services.

No stipulation.

1.4 Certificate Usage

This subcomponent contains:

* A list or the types of applications for which the issued certificates are suitable, such as electronic mail, retail transactions, contracts, and a travel order, and/or
* A list or the types of applications for which use of the issued certificates is prohibited.

In the case of a CP or CPS describing different levels of assurance, this subcomponent can describe applications or types of applications that are appropriate or inappropriate for the different levels of assurance.

1.4.1 Appropriate certificate uses

CA certificates may only be used to issue certificates and for checking certificates that claim to be issued by the ANSPGrid CA. RA certificates may only be used by the RA Manager for RA related activities, not for other activities of that natural person; these must be undertaken using an end-entity certificate. The end-entity certificate may be used for any application that is suitable for X.509 certificates such as integrity and non-repudiation (see Section 6.1.7), in particular:

a) authentication of users, hosts and services;

b) authentication and encryption of communications;
c) authentication of signed e-mails;
d) authentication of signed objects.

Certificates may only be used or accepted for actions authorized by the certificate keys.

1.4.2 Prohibited certificate uses

Certificates issued by the ANSPGrid CA must not be used for purposes that violate Brazilian 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.

Certificates issued by the ANSPGrid CA do not claim legal value, nor does the ownership of a certificate issue by the ANSPGrid CA imply automatic access to any kind of computing resources.

1.5 Policy Administration

This subcomponent includes the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of this CP or CPS. It also includes the name, electronic mail address, telephone number, and fax number of a contact person. As an alternative to naming an actual person, the document may name a title or role, an e-mail alias, and other generalized contact information. In some cases, the organization may state that its contact person, alone or in combination with others, is available to answer questions about the document.

Moreover, when a formal or informal policy authority is responsible for determining whether a CA should be allowed to operate within or interoperate with a PKI, it may wish to approve the CPS of the CA as being suitable for the policy authority's CP. If so, this subcomponent can include the name or title, electronic mail address (or alias), telephone number, fax number, and other generalized information of the entity in charge of making such a determination. Finally, in this case, this subcomponent also includes the procedures by which this determination is made.

1.5.1 Organization administering the document

The ANSPGrid Certification Authority is responsible for the registration, maintenance, and interpretation of this CP/CPS. This CA is managed by the Academic Network at São Paulo, located in São Paulo (Brazil). The full ANSPGrid CA postal address for operational issues is:

ANSPGrid Certification Authority,
Academic Network at São Paulo,
Rua Dr. Ovídio Pires de Campos, 215 – 2º andar

Cerqueira César,
CEP 05403-010 São Paulo, SP, Brazil.

E-mail: gridca@ansp.br
ANSPGrid CA web server URL: http://gridca.ansp.br/

1.5.2 Contact Person

The contact person for questions related with this document or any other issues related to the ANSPGrid CA is the current CA manager:

Angelo de Souza Santos,
Academic Network at São Paulo,
Rua Dr. Ovídio Pires de Campos, 215 – 2º andar
Cerqueira César,
CEP 05403-010 São Paulo, SP, Brazil.

Mobile: (+ 55 11) 99579 3353
Skype Name: angelift
E-mail: angelo.santos@unesp.br

1.5.3 Person determining CPS suitability for the policy

The manager of the ANSPGrid 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 has been approved by The Americas Grid Policy Management Authority (http://www.tagpma.org) under the classic CA profile of the International Grid Trust Federation (http://www.igtf.net).

1.6. Definitions and Acronyms

This subcomponent contains a list of definitions for defined terms used within the document, as well as a list of acronyms in the document and their meanings.

1.6.1 Definitions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [Brader97].

Activation data

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g.,a PIN, or a passphrase).

Authentication

The process used to establish the authenticity of an individual, organization, computer system, service or software component. Authentication is used to ensure that the subject is really who or what it claims to be. In the public key infrastructure (PKI) there are two different authentications. The first occurs after a request for a certificate is made and has the objective of verifying that the certificate will be issued to the correct subject (also known as *identification*). The second is a security service that provides assurances that the individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization, or that the data sent electronically originated from the specific individual, organization, or device that claims to have sent it. Thus, it is said in the case of the latter, that a digital signature of a message authenticates the message's sender.

Certification Authority

A certification authority (CA) is a trusted authority that issues and manages public key certificates as part of a public key infrastructure (PKI).

Public-key Certificate (or just "certificate")

Electronic document binds a public key held by an entity (such as person, organization, account, device, or site) to a set of information that identifies the entity associated with use of the corresponding private key.

CA-certificate

A certificate for given CA's public key issued by another CA or, in the case of a selfsigned CA-certificate, issued by the same CA.

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. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification Practice Statement (CPS)

A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

CPS Summary (or CPS Abstract)

A subset of the provisions of a complete CPS that is made public by a CA.

Certificate Revocation List

A time stamped list containing the index number of the revoked certificates, which is signed by a CA and made available in the CA’s public repository.

Digital Signature

Refers to the use of the owner’s private key to sign an electronic document, for example a digitally signed email. The recipient(s) can use the owner’s public key (from the owner’s corresponding valid certificate) to verify that the owner was indeed the author of the document (see Authentication).

Identification

The process of establishing the identity of an individual or organization.

Issuing certification authority (issuing CA)

In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also subject certification authority).

Participant

An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS)

An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.

Personal Certificate

A certificate used for authentication to establish the identity an individual person.

Policy qualifier

Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.

Registration authority (RA)

An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants; the approval or rejection of certificate applications; initiating certificate revocations or suspensions under certain circumstances; processing subscriber requests to revoke or suspend their certificates; and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). Note that the term *Local Registration Authority* (LRA) is sometimes used in other documents for the same concept.

Relying party

A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying party agreement (RPA)

An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Repository

The on-line storage area where the CA stores issued certificates, CRLs, the root certificate etc.

Set of provisions

A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework.

Signed e-mail

An e-mail message that has been check summed and signed by a valid certificate.

Strong passphrase

A characteristic of a password. The password used to protect the private key must be strong. That means difficult to guess.

Subject Identification
The process of establishing the identity of a person.

Subject certification authority (subject CA)
In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority).

Subscriber
A subject of a certificate to whom a certificate is issued.

Subscriber Agreement
An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

Validation
The process of identifying and verifying certificate applicants. *Validation* is a subset of *identification* and refers to identification in the context of establishing the identity of certificate applicants.

1.6.2 Acronyms

C	Country
CA	Certification Authority
CN	Common Name
CDROM	Compact Disc Read Only Memory
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguish name
EUgridPMA	The European Grid Authentication Policy Management Authority in e-Science, http://www.eugridpma.org/
ANSP	Academic Network at São Paulo
LDAP	Lightweight Directory Access Protocol
MIME	Multi-purpose Internet Mail Extensions
NTP	Network Time Protocol
O	Organization
OID	Object Identifier
OU	Organizational Unit
PKI	Public Key Infrastructure
RA	Registration Authority
SSL	Secure Sockets Layer
TAGPMA	The Americas Grid Authentication Policy Management Authority, http://www.tagpma.org/
ANSPGrid CA	Academic Network at São Paulo Grid Certification Authority
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier
URL	Universal Resource Locator

2. Publication and Repository Responsibilities

2.1 Repositories

An identification of the entity or entities that operate repositories within the PKI, such as a CA, certificate manufacturing authority, or independent repository service provider.

An online repository of information relating to the ANSPGrid CA is accessible through the WWW URL http://gridca.ansp.br/.

2.2 Publication of certification information

The responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status of such certificates, which may include the responsibilities of making the CP or CPS publicly available using various mechanisms and of identifying components, subcomponents, and elements of such documents that exist but are not made publicly available, for instance, security controls, clearance procedures, or trade secret information due to their sensitivity.

The ANSPGrid CA will operate a secure online repository that contains:

a) the ANSPGrid CA's root certificate, in the appropriate formats, and all previous ones necessary to check existing valid certificates;
b) certificates issued by the ANSPGrid CA;
c) a list of revoked ANSPGrid CA certificates (Certificate Revocation List);
d) a copy of this document (CP/CPS);
e) a contact email address for inquires and fault and incident reporting;
f) a postal contact address;
g) as well as any other information deemed relevant to the ANSPGrid CA service.

As an accredited CA member of the TAGPMA, the ANSPGrid CA grants the IGTF and its PMAs the right of unlimited re-distribution of this information.

2.3 Time or frequency of publication

When information must be published and the frequency of publication.

All information published shall be up-to-date. Certificates will be published in the ANSPGrid CA repository as soon as they have been issued i.e., even before being checked and accepted by the subscriber (see Sections 4.4.1 and 4.4.2).

The certificate revocation list (CRL) shall have a lifetime of at most 30 days. The ANSPGrid CA must issue a new CRL at least 7 days before expiration or immediately

after having successfully processed a revocation, whichever comes first. A new CRL must be published immediately after its issuance.

The OID of this document will be changed to reflect updates that have been made to this CP/CPS. The modified CP/CPS will be published at least two weeks before changes come into effect. In the case of major changes, implementation will only occur the new CP/CPS has been approved by the TAGPMA.

2.4 Access controls on repositories

Access control on published information objects including CPs, CPS, certificates, certificate status, and CRLs.

Public information on the ANSPGrid CA web site is accessible without any restriction. The ANSPGrid CA does not impose any access control on its CP/CPS, its certificate, issued certificates or CRLs. However, if misuse of the data is evident, access controls may be enacted in order to protect the owners of certificates.

The online repository is maintained on a best effort basis and is available on a 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance. Outside the period 09:00-17:00 (local time) Monday-Friday it may run unattended.

3. Identification and Authentication

This component describes the procedures used to authenticate the identity and/or other attributes of an end-user certificate applicant to a CA or RA prior to certificate issuance. In addition, the component sets forth the procedures for authenticating the identity and the criteria for accepting applicants of entities seeking to become CAs, RAs, or other entities operating in or interoperating with a PKI. It also describes how parties requesting re-key or revocation are authenticated. This component also addresses naming practices, including the recognition of trademark rights in certain names.

3.1 Naming

This subcomponent includes the following elements regarding naming and identification of the subscribers.

3.1.1 Types of names

Types of names assigned to the subject, such as X.500 distinguished names; RFC-822 names; and X.400 names.

The certificate subject names used as unique certificate identifiers obey the X.501 standard. Subject names have a fixed and a variable component. The certificate subject names start with the fixed component to which a variable component is appended to make it unique.

The fixed component is common to all certificates issued by the ANSPGrid CA and is used to identify the namespace that can be signed by the CA. The fixed component is as follows:

/C=BR/O=ANSP/OU=ANSPGrid CA

A common name (CN) that uniquely identifies the subject name within the CA namespace must follow the previously mentioned components. The common name must be obtainable from the subject's real name as stated in section 3.1.2. For computer systems or services, the common name is the DNS full-qualified domain name (FQDN) of the system (in lower case) and in the case of certificates for the Globus Toolkit prefixed with the qualifier "host/" for a system, or the service name initials followed by a slash. IP addresses are not acceptable.

The generic format for a person subject is as follows:

/C=BR/O=ANSP/OU=ANSPGrid CA/OU=People/CN=*subject-name*

The generic format for a system (e.g. web server) subject is as follows:

/C=BR/O=ANSP/OU=ANSPGrid CA/OU=Services/CN=*host-dns-name*

The generic format for a globus host (system) subject is however as follows:

/C=BR/O=ANSP/OU=ANSPGrid CA/OU=Services/CN=host/*host-dns-name*

The generic format for a globus service subject is as follows:

/C=BR/O=ANSP/OU=ANSPGrid CA/OU=Services/CN=*service/host-dns-name*

Some examples of certificate subjects that obey to the ANSPGrid CA subjectnaming scheme are as follows:

/C=BR/O=ANSP/OU=ANSPGrid CA/OU=People/CN=John Smith
/C=BR/O=ANSP/OU=ANSPGrid CA/OU=Services/CN=www.ncc.unesp.br

For globus certificates:

/C=BR/O=ANSP/OU=ANSPGrid CA/OU=Services/CN=host/www.ncc.unesp.br

The common names must be encoded as Printable Strings according with RFC1778 and RFC2252. National characters must be represented by their ASCII equivalent, e.g., é, õ, à, ç, â, and ü shall be represented by e, o, a, c, a, u, respectively. The characters allowed in the common names of personal certificates are as follows:

a) **‘ ’** (space), **‘(’**, **‘)’** and **‘-’**;
b) **‘0’** – **‘9’**;
c) **‘a’** – **‘z’** and **‘A’** – **‘Z’**.

In addition, the characters ‘**.**’ (period) and ‘*/*’ (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 in the case of globus certificates.

3.1.2 Need for names to be meaningful

Whether names have to be meaningful or not.

The information specified in the common name, in the organization name and in the organizational unit must be meaningful. The names must be related to (and express a

reasonable association with) the authenticated subscriber’s real name and organization.

For personal certificates, the common name must be obtainable from the legal person name as presented in an official governmental identity document such as a passport or identity card. Subscribers must choose a representation of their names in the permitted character set (see 3.1.1). The name must not refer to a role. Subscribers can be neither anonymous nor pseudonymous.

For server (machine) or service certificates, the common name must be the fully qualified DNS host name.

3.1.3 Anonymity or pseudonymity of subscribers

Whether or not subscribers can be anonymous or pseudonymous, and if they can, what names are assigned to or can be used by anonymous subscribers.

No personal certificates shall be issued for roles or functions; certificates must only be issued to identified and authenticated named persons.

3.1.4 Rules for interpreting various name forms

Rules for interpreting various name forms, such as the X.500 standard and RFC-822;

Refer to sections 3.1.1 and 3.1.2.

3.1.5 Uniqueness of names

Whether names have to be unique.

The Distinguished Name (DN) in each certificate issued by the ANSPGrid CA must be unique. Under this CP/CPS policy, two names are considered identical if they differ only in case, punctuation or whitespace; in other words, case, punctuation or whitespaces must not be used to differentiate names.

Since person names are usually quite long it is not required that a subject name contains all of the person real names. However, for persons with three or more names, at least three should be specified in the common name in order to avoid clashes. In cases where the person name is not sufficient to differentiate two certificates then numbers will be added to the end of the common name.

Certificates must apply to unique individuals or resources. Every subject distinguished name must be linked to one and only one end entity throughout the entire life time of the ANSPGrid CA. Subscribers must not share certificates.

3.1.6 Recognition, authentication, and role of trademarks

The ANSPGrid CA does not guarantee that the subject names of the certificates issued will contain the requested trademarks.

3.2 Initial Identity Validation

This subcomponent contains the following elements for the identification and authentication procedures for the initial registration for each subject type (CA, RA, subscriber, or other participant).

3.2.1 Method to prove possession of private key

If and how the subject must prove possession of the companion private key for the public key being registered, for example, a digital signature in the certificate request message.

The possession of the private key by the requestor is considered proven when the digital signature of the certificate signing request (CSR) can be verified using the public key present in the request.

3.2.2 Authentication of organization identity

Identification and authentication requirements for organizational identity of subscriber or participant (CA; RA; subscriber (in the case of certificates issued to organizations or devices controlled by an organization), or other participant), for example, consulting the database of a service that identifies organizations or inspecting an organization's articles of incorporation.

If an organization or unit intends to requests a number of certificates, it is encouraged to make a formal request to the ANSPGrid CA to setup a ANSPGrid CA Registration Authority (RA) for that organization or unit. The CA must then ascertain whether or not that the organization or organizational unit exists and is entitled to request ANSPGrid certificates. It must also obtain competent information on who is entitled to sign documents on behalf of the institution.

The first time an organization or organizational unit requests a certificate for a person, a server or a service from an RA (that is not directly related to that organization or organizational unit), that RA must first ascertain if it is indeed the most appropriate of the existing ANSPGrid CA RAs fulfill the request. The responsible RA shall verify that the requesting party's organization or a unit of an organization is entitled (see Section 1.3.3) to get a certificate from the ANSPGrid CA. The RA will inform the ANSPGrid CA that it is now responsible for this organization or unit.

The relationship between the subscriber and the organization or unit mentioned in the subject name must be proved through an organization identity card, a legally acceptable document or an official organization (letter-headed) document stamped and signed by an official representative of that organization. In case of doubt, the RA may take any required steps to inquire about the relationship of the subscriber with the organization. The request may optionally be authorized electronically through the digital signature of an official representative of the organization in possession of a valid ANSPGrid CA issued certificate.

In special cases, the organization can provide the RA with access to official databases that can be used to verify the relation of the requesters with the organizations. In this case, the RA must produce and keep a written document where it declares that the relationship of the requester with the organization was performed according with the data in the database provided by the organization. The accuracy of the database contents is the responsibility of the organization. The access to the database information must be performed in a secure way.

3.2.3 Authentication of individual identity

Identification and authentication requirements for an individual subscriber or a person acting on behalf of an organizational subscriber or participant (CA, RA, in the case of certificates issued to

organizations or devices controlled by an organization, the subscriber, or other participant), including:

a) Type of documentation and/or number of identification credentials required;
b) How a CA or RA authenticates the identity of the organization or individual based on the documentation or credentials provided;
c) If the individual must personally present to the authenticating CA or RA;
d) How an individual as an organizational person is authenticated, such as by reference to duly signed authorization documents or a corporate identification badge.

Individuals are authenticated through the presentation of a valid identity document (officially recognized under the Law in which the subscriber resides) such as a valid passport or identity card containing a photograph. The individual should present himself ***in person*** to a ANSPGrid CA Registration Authority (RA) for their identity to be verified. At that moment, the individual must also present the proof of their current relationship with the organization(s) to be specified in the certificate subject distinguished name. A photocopy of all documentation (identity and proof of relationship) must be given to the RA. In exceptional cases, for example due to the subscriber's geographical remote location, this presentation may be held 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. In either case, the RA is responsible for convening this meeting. Note that ***"authenticated"*** and ***"notarized"*** refer to verifications made by a legally appointed notary public. The association of the subscriber to the Certificate Signing Request (CSR) is proved by the subscriber providing the RA with matching PIN (entered when the certificate request was made).

For each authentication, the RA will record and archive:

a) The type, identification number and name in the identification document presented by the subject to be authenticated;
b) The document(s) used as proof of relationship with the organization or organizational unit;
c) The E-mail, phone number and address of the requester;
d) The identification of the person that has performed the authentication;
e) The date, time and place of the authentication;
f) Whether the authentication was successful or not and why.

For host or service certificates, the requests must be signed with a ANSPGrid CA issued personal certificate corresponding to the system administrator or person responsible of the resource. The RA corresponding to the organisation mentioned in the certificate request distinguish name will verify whether the requester has the right to request a certificate for the intended host or service and that the FQDN has been registered in the Internet's DNS.

If a requesting party fails to meet the authentication requirements within 10 working days after the RA received the request, the request is void, and a new one has to be submitted.

The RA shall send via a secure communication channel (using the SSL protected pages of the ANSPGrid CA web server that require bi-directional authentication) or in a

signed e-mail to the ANSPGrid CA, an electronic copy of the recorded authentication documentation and the certificate request. The information will be stored in a secure database at the CA site and shall be considered private and confidential (see Section 9.4).

3.2.4 Non-verified subscriber information

List of subscriber information that is not verified (called "nonverified subscriber information") during the initial registration.

The contact e-mail, phone number and address of the requester.

3.2.5 Validation of authority

Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate.

In a statement, preferably written and signed by an individual authorized by the organization to sign on behalf that organization or unit and for which the CA or appropriate RA has ascertained the right of authority, the organization shall nominate one or more representatives (known as RA Local Representatives or Agents) who are entitled to request server or service/application certificates and answer all questions related to personal certificate requests.

These persons shall be the first in their organization/unit to request individual certificates according to the provisions outlined in Section 3.2.3. The digital signatures of these individuals with the private key associated with the certified public key shall be sufficient for all future information exchanges with or requests from that organization/unit. When the organization/unit rescinds an individual's authorization, it must inform its RA and the ANSPGrid CA of this fact in the same way as the authorization was made known.

3.2.6 Criteria for interoperation

In the case of applications by a CA wishing to operate within, or interoperate with, a PKI, this subcomponent contains the criteria by which a PKI, CA, or policy authority determines whether or not the CA is suitable for such operations or interoperation. Such interoperation may include cross-certification, unilateral certification, or other forms of interoperation.

No stipulation.

3.3. Identification and Authentication for Re-key Requests

This subcomponent addresses the following elements for the identification and authentication procedures for re-key for each subject type (CA, RA, subscriber, and other participants).

3.3.1 Identification and authentication for routine re-key

Identification and authentication requirements for routine re-key, such as a re-key request that contains the new key and is signed using the current valid key.

Re-key before the certificate expires can be done either using a secure web interface or by sending a re-key request based on a new public key in an e-mail signed with the old private key to the appropriate RA of the ANSPGrid CA. However if the certificate subject is a person it must still provide the RA with a proof of relationship with the organization(s) mentioned in the certificate subject name (see Section 3.2.2). Although a proof of relationship is required, the re-key process does not require the identity verification by the RA and therefore does not require the physical presence of the subject. If the proof of relationship is performed through paper documents, they can be sent to the RA by surface mail, by fax or scanned and sent by email. Credentials cannot be re-keyed more than five years in succession without identity verification. Re-key requests for expired certificates are not accepted. In this case, the procedure for obtaining a new certificate must be followed.

3.3.2 Identification and authentication for re-key after revocation

Identification and authentication requirements for re-key after certificate revocation. One example is the use of the same process as the initial identity validation.

The ANSPGrid CA does not perform re-key of a certificate after its revocation. After revocation of a key, no re-key is possible. A new certificate must be requested and the procedure for obtaining a new certificate must be followed.

3.4 Identification and Authentication for Revocation Requests

This subcomponent describes the identification and authentication procedures for a revocation request by each subject type (CA, RA, subscriber, and other participant). Examples include a revocation request digitally signed with the private key whose companion public key needs to be revoked, and a digitally signed request by the RA.

Every revocation request (independent of the source) must be verified and the requesting party authenticated. Such a request coming from an RA must be made via ANSPGrid CA secure web interface or in a signed e-mail sent to the CA. The e-mail message must be signed with a valid non-expired certificate.

Before revoking a certificate the ANSPGrid CA has to authenticate the source of the request as it does for a certificate request. Such a revocation request must be made by:

a) the owner of the certificate in an e-mail signed with the private key associated with the non-expired certificate;
b) the owner, in person, at the appropriate RA who must authenticate the requestor following the same procedure for a certificate request (see Section 3.2.3);
c) on behalf of the owner who has lost his/her private key in an e-mail signed by an authorized person of the organization/unit that consented to the certificate;
d) on behalf of the organization/unit that consented to the certificate in an email signed by an authorized person (see 3.2.2); or
e) the appropriate RA that has knowledge of a key compromise.

The ANSPGrid CA can revoke certificates without authentication upon proof of key compromise or violation of the CP/CPS rules and user obligations by the certificate holder. In case of emergency if no such e-mail can be sent, the revocation can be initiated via oral communication with the appropriate RA or the ANSPGrid CA.

4. Certificate Life-Cycle Operational Requirements

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, subscribers, or other participants with respect to the life-cycle of a certificate.

Within each subcomponent, separate consideration may need to be given to subject CAs, RAs, subscribers, and other participants.

4.1 Certificate Application

This subcomponent is used to address the following requirements regarding subject certificate application: Who can submit a certificate application, such as a certificate subject or the RA; and Enrollment process used by subjects to submit certificate applications and responsibilities in connection with this process.

An example of this process is where the subject generates the key pair and sends a certificate request to the RA. The RA validates and signs the request and sends it to the CA. A CA or RA may have the responsibility of establishing an enrollment process in order to receive certificate applications. Likewise, certificate applicants may have the responsibility of providing accurate information on their certificate applications.

4.1.1 Who can submit a certificate application

The ANSPGrid CA issues certificates for entities related with the following organizations in Brazil, without IGTF accredited CAs:

a) academic organizations (e.g. public and private universities and educational institutes);
b) academic research centers (either public or private non-profit ones); and,
c) other organizations with research and development (R&D) affiliations with one of the above class of organizations.

The subject entities for certificates are of the following types:

a) employees, researchers and students affiliated with the above organizations;
b) computer systems (hosts) related with, and administered by, the above organizations; and
c) services provided by a host administered by an organization above.

4.1.2 Enrollment process and responsibilities

The requesting party must generate a key pair with a size of at least 1024 bits on their system through the form provided at the ANSPGrid CA web site. After this form has been completed, the encrypted private key will be stored on the system where the browser runs in a file only accessible to the requestor (if the operating system allows such a restriction), and the Certificate Signing Request (CSR) will be sent to the

appropriate RA of the ANSPGrid CA. If using the browser for this purpose is not appropriate (e.g. when a secure hardware device generates the key pair), the CSR in PKCS #10 format [Nystrom00] can be generated using appropriate software (e.g. OpenSSL) and uploaded to the secure web interface sent to the appropriate RA. In this case, the subscriber must contact the RA beforehand to get the correct DN to be included in the request.

User certificate applications must be acknowledged by the sponsoring organization that appears in the certificate. For host or service certificates the CSR or the e-mail containing the CSR must also be signed by the nominated representative (see 3.2.5) of the organization or unit with his/her personal private key.

By submitting an application, subscribers are confirming that they have read and will adhere to the procedures published in this document. In summary they must:

a) Generate a key pair using a trustworthy method;
b) Use the certificate for the authorized purposes only;
c) Authorize the processing and conservation of the personal data required for the request verification process.

In particular, subscribers must take every precaution to prevent any loss, disclosure or unauthorized access to or use of the private key associated with the certificate, including:

a) Selecting a strong passphrase with a minimum of 12 characters; and
b) protecting the passphrase from others, in the case of user certificates.

Subscribers must request revocation by notifying their RA, the ANSPGrid CA and any relying parties immediately (at most one working day):

a) if the private key is lost, destroyed or compromised;
b) if the subscriber is no longer entitled to a certificate, or;
c) if the information in the certificate is no longer correct or is inaccurate.

4.2 Certificate Application Processing

This subcomponent is used to describe the procedure for processing certificate applications. For example, the issuing CA and RA may perform identification and authentication procedures to validate the certificate application. Following such steps, the CA or RA will either approve or reject the certificate application, perhaps upon the application of certain criteria. Finally, this subcomponent sets a time limit during which a CA and/or RA must act on and process a certificate application.

4.2.1 Performing identification and authentication functions

An RA operator may use the ANSPGrid CA administration module to identify all pending CSRs. Each RA is obliged follow the procedures described in this CP/CPS document (and the *RA Obligations, Responsibilities and Operations Manual*) to verify the compliance of such pending CSRs to the policies set out in this CP/CPS document. In particular, as set out in Section 3.2, request validation obligations for certificate issuance (and revocation) include:

a) Verify whether requests obey the requirements expressed in the CP/CPS document;
b) Authenticate the subjects according with the procedures described in the CP/CPS document and the RA operations manual;
c) Verify that the requesters are in the possession of the private key corresponding to the certificate request;

d) Notify the ANSPGrid CA about the result of each request validation using a secure and reliable mechanism in accordance with this CP/CPS document;

If the certification request is received by email, the RA must check the digital signature of the CSR. In the case of a server or service request, it must also check that the message has been digitally signed by a representative (see Section 3.2.5) of the organization or unit responsible for the host.

4.2.2 Approval or rejection of certificate applications

Upon successful authentication, an electronic copy (signed by the RA) of the requesting party's identification documents and the certification request shall be sent to the ANSPGrid CA. Alternatively, a secure transmission to the ANSPGrid CA may be used, if it is at least as secure as a signed e-mail. If the authentication information proves to be inaccurate or if a requesting party fails to meet the authentication requirements within 10 working days after the RA received the request, the request shall be rejected. If the requesting party insists on getting a certificate, a new request must be initiated.

4.2.3 Time to process certificate applications

The turn-around time from request to issuance depends mostly on the authentication process, and should not be more than 10 working days.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

Describes the actions performed by the CA during the issuance of the certificate, for example a procedure whereby the CA validates the RA signature and RA authority and generates a certificate

The CSR shall be transferred manually to the signing computer running only the services necessary for the CA operations. On this system, the certificate will be created and signed with the private key of ANSPGrid CA. The signed certificate shall then be transferred manually back to the ANSPGrid CA online web server.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Describes the notification mechanisms, if any, used by the CA to notify the subscriber of the issuance of the certificate; an example is a procedure under which the CA e-mails the certificate to the subscriber or the RA or e-mails information permitting the subscriber to download the certificate from a web site.

The ANSPGrid CA shall then send either the certificate or the URL of the certificate download page to the requesting party in an e-mail signed by the CA agent's certified private key. An acknowledgement of the issuance will also be sent to the corresponding RA. A certificate will be valid for one year from the date of issuance or less than one year in specific cases (e.g. if the applicant's affiliation to the organization/unit is known to be less than one year).

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The conduct of an applicant that will be deemed to constitute acceptance of the certificate. Such conduct may include affirmative steps to indicate acceptance, actions implying acceptance, or a failure to object to the certificate or its content. For instance, acceptance may be deemed to occur if the CA does not receive any notice from the subscriber within a certain time period; a subscriber may send a signed message accepting the certificate; or a subscriber may send a signed message rejecting the certificate where the message includes the reason for rejection and identifies the fields in the certificate that are incorrect or incomplete.

The requesting party shall first, upon receipt of the e-mail with the certificate or the URL or the certificate download page, check the digital signature of the e-mail. The usability of the certificate should be verified in conjunction with the private key in requesting party's possession by, for example, signing an arbitrary file with his/her private key and checking the digital signature with the certificate and/or encrypting a file using the public key of the certificate and decrypting it with the private key. If the result of this check is successful and there are no objections to other aspects of the certificate, the subscriber must inform the ANSPGrid CA and the appropriate RA that he/she accepts the certificate. If the certificate is rejected, the requesting party must inform the CA and the RA of the rejection and explain the reasons. The ANSPGrid CA shall revoke any certificate whose acceptance has not been confirmed within 10 working days.

4.4.2 Publication of the certificate by the CA

Publication of the certificate by the CA. For example, the CA may post the certificate to an X.500 or LDAP repository.

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other entities

Notification of certificate issuance by the CA to other entities. As an example, the CA may send the certificate to the RA.

The ANSPGrid CA shall inform the appropriate RA of the issuance of a certificate.

4.5. Key Pair and Certificate Usage

This subcomponent is used to describe the responsibilities relating to the use of keys and certificates.

4.5.1 Subscriber private key and certificate usage

Subscriber responsibilities relating to use of the subscriber's private key and certificate. For example, the subscriber may be required to use a private key and certificate only for appropriate applications as set forth in the CP and in consistency with applicable certificate content (e.g., key usage field). Use of a private key and certificate are subject to the terms of the subscriber agreement, the use of a private key is permitted only after the subscriber has accepted the corresponding certificate, or the subscriber must discontinue use of the private key following the expiration or revocation of the certificate.

Certificates issued by the ANSPGrid CA and their associated private keys must only be used according to the permitted conditions set out in Section 1.4. All other uses are strictly prohibited. Certificates shall only be used according to the key usage fields of the certificate. When a certificate is revoked or has expired, the associated private key should no longer be used.

4.5.2 Relying party public key and certificate usage

Relying party responsibilities relating to the use of a subscriber's public key and certificate. For instance, a relying party may be obligated to rely on certificates only for appropriate applications as set forth in the CP and in consistency with applicable certificate content (e.g., key usage field), successfully perform public key operations as a condition of relying on a certificate, assume responsibility to check the status of a certificate using one of the required or permitted mechanisms set forth in the CP/CPS (see Section 4.9 below), and assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

A relying party should, upon being presented with a certificate issued by the ANSPGrid CA, check

* its validity by:
    a) checking that it trusts the CA that issued the certificate;
    b) checking that the certificate hasn't expired;
    c) consulting the ANSPGrid CA CRL in effect at the time of use of the certificate; and

* the appropriate usage as outlined in the CP pointed to by the certificate and the usage keys included in the certificate.

4.6 Certificate Renewal

This subcomponent is used to describe the following elements related to certificate renewal. Certificate renewal means the issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate.

4.6.1 Circumstance for certificate renewal

Circumstances under which certificate renewal takes place, such as where the certificate life has expired, but the policy permits the same key pair to be reused;

Due to the danger of exposure of keys that are used for too long, ANSPGrid CA encourages subscribers not to renew certificates for the same key pair when they are about to expire. Only when the appropriate RA can ascertain the protection of the private key (for example, credentials based on hardware tokens), shall the CA accept and process a renewal request. Nevertheless, hardware token based credentials of key lengths equivalent to 2048 and to 1024 bits may only be renewed annually for 5 and 3 years respectively. The ANSPGrid CA may decide to reject such a renewal for security reasons, to avoid risks derived from long exposures of private keys. In any case, credentials cannot be renewed more than five years in succession without identity verification.

4.6.2 Who may request renewal

Who may request certificate renewal, for instance, the subscriber, RA, or the CA may automatically renew an end-user subscriber certificate;

The owner of a certificate may request the renewal of a certificate before it expires using a secure web interface or by sending to the appropriate RA, an e-mail signed with the private key associated with the certificate for which renewal is requested.

4.6.3 Processing certificate renewal requests

A CA or RA's procedures to process renewal requests to issue the new certificate, for example, the use of a token, such as a password, to re-authenticate the subscriber, or procedures that are the same as the initial certificate issuance;

If the certificate subject is a person, the subscriber must still provide the RA with a proof of relationship with the organization(s) mentioned in the certificate subject name (see Section 3.2.2). Although a proof of relationship is required, the renewal process does not require the identity verification by the RA and therefore does not require the physical presence of the subject. However, certificates cannot be renewed more than

five years in succession without identity verification. If the proof of relationship is performed through paper documents, they can be sent to the RA by surface mail, fax or scanned and sent by signed email.

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

Upon receipt of the request endorsed by the appropriate RA, the ANSPGrid CA shall process the renewal as it processes an initial certification request.

4.6.4 Notification of new certificate issuance to subscriber

The ANSPGrid CA shall notify the subscriber of the issuance as described for the initial certificate issuance in Section 4.3.2.

4.6.5 Conduct constituting acceptance of the renewal certificate

The same procedure described in Section 4.4.1 shall be followed.

4.6.6 Publication of the renewal certificate by the CA

See Section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.7 Certificate Re-key

This subcomponent is used to describe the following elements related to a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key.

4.7.1 Circumstance for certificate re-key

Circumstances under which certificate re-key can or must take place, such as after a certificate is revoked for reasons of key compromise or after a certificate has expired and the usage period of the key pair has also expired.

For security reasons, the certificate re-key is the preferred method for issuing a new certificate to a subscriber whose certificate is about to expire or who require a change in the certificate's parameters.

The ANSPGrid CA does not perform a re-key of a certificate after its revocation. A new certificate must be requested and the procedure for obtaining a new certificate must be followed.

4.7.2 Who may request certification of a new public key

Who may request certificate re-key, for example, the subscriber.

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

4.7.3 Processing certificate re-keying requests

A CA or RA's procedures to process re-keying requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance.

Users can use the ANSPGrid CA web interface to request a certificate re-key. If the certificate subject is a person, the subscriber must still provide the RA with a proof of relationship with the organization(s) mentioned in the certificate subject name (see Section 3.2.2). Although a proof of relationship is required, the re-key process does not require the identity verification by the RA and therefore does not require the physical presence of the subject. However, certificates cannot be re-keyed more than five years in succession without identity verification. If the proof of relationship is performed through paper documents, they can be sent to the RA by surface mail, fax or scanned and sent by signed email.

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

Upon receipt of the request endorsed by the appropriate RA, the ANSPGrid CA shall process the re-key as it processes an initial certification request.

4.7.4 Notification of new certificate issuance to subscriber

The ANSPGrid CA shall notify the subscriber of the issuance as described for the initial certificate issuance in Section 4.3.2.

4.7.5 Conduct constituting acceptance of the re-keyed certificate

The same procedure described in Section 4.4.1 shall be followed.

4.7.6 Publication of the re-keyed certificate by the CA

See Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.8 Certificate Modification

This subcomponent is used to describe the following elements related to the issuance of a new certificate due to changes in the information in the certificate other than the subscriber public key.

4.8.1 Circumstance for certificate modification

Circumstances under which certificate modification can take place, such as name change, role change, reorganization resulting in a change in the DN.

Certificates must not be modified. The old certificate must be revoked, a new key pair must be generated and a request for the modified certificate contents submitted with the new public key. The revocation may be conditional on the issuance and acceptance of the new certificate, and thus the old certificate will only be revoked after the new one is accepted.

4.8.2 Who may request certificate modification

Who may request certificate modification, for instance, subscribers, human resources personnel, or the RA.

Not applicable. The owner of the original certificate may submit the requests for re-key and revocation as per Sections 4.7.2 and 4.9.3 respectively.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

A CA or RA's procedures to process modification requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance.

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

4.9.1 Circumstances for revocation

Circumstances under which a certificate may be suspended and circumstances under which it must be revoked, for instance, in cases of subscriber employment termination, loss of cryptographic token, or suspected compromise of the private key.

A certificate must be revoked when the information it contains or the implied assertions it carries are known, or suspected, to be incorrect or compromised. This includes situations where:

a) the subscriber has ceased to be a member of or associated with his/her organization (or if said organization/unit withdraws its consent);
b) the subject does not want the certificate any more;
c) the subscriber's private key has been lost, suspected to have been compromised, or it is no longer needed;
d) the information in the subscriber' s certificate is (or suspected of being) wrong or inaccurate;
e) the subject has failed to comply with the rules in this policy document; or
f) the system (host or service) for which the certificate was issued has been retired.

Should the private key of the ANSPGrid CA be compromised or lost all certificates signed with it shall be revoked.

4.9.2 Who can request revocation

Who can request the revocation of the participant's certificate, for example, the subscriber, RA, or CA in the case of an end-user subscriber certificate.

In addition to the subscriber, who must request revocation as soon as possible if any of the circumstances outlines in Section 4.9.1 arise, revocation can be requested by:

a) the ANSPGrid CA or any RA that has proof of a compromise;
b) the organization that wants to revoke its consent to its inclusion in the certificate;
c) the Registration Authority which authenticated the holder of the certificate;
d) any entity presenting proof of knowledge that the subscriber's private key has been compromised or that the subscriber' s data have changed.
e) any entity presenting proof of responsibility for a certified machine or service; or
f) any entity presenting proof of the certificate misuse;

4.9.3 Procedure for revocation request

Procedures used for certificate revocation request, such as a digitally signed message from the RA, a digitally signed message from the subscriber, or a phone call from the RA.

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

a) by the owner of the certificate, properly authenticated, using the online revocation facilities or in an e-mail signed with the private key associated with the (still not expired) certificate;
b) by the owner going in person as soon as possible to the appropriate RA to request revocation;
c) on behalf of the owner in an e-mail signed by an authorized person of the organization/unit that consented to the certificate (see Section 3.2.2),
d) by the RA administrator using a secure web interface or signed email.

In case of emergency, revocation can be initiated via oral communication with the appropriate RA or the ANSPGrid CA.

Before revoking a certificate, the ANSPGrid CA shall authenticate the source of the request according procedures as used for the initial registration. The ANSPGrid CA will always try to notify the certificate subscriber before revoking the certificate.

The ANSPGrid CA can revoke certificates without authentication upon proof of key compromise or violation of the CP/CPS rules and user obligations by the certificate holder.

4.9.4 Revocation request grace period

The grace period available to the subscriber, within which the subscriber must make a revocation request;

No grace period shall be defined for a revocation request. The ANSPGrid CA shall process the authenticated request with the highest priority and publish the revocation as fast as possible.

4.9.5 Time within which CA must process the revocation request

The ANSPGrid CA will act promptly to revocation requests in at most one working day, which means however that implementation may be delayed by weekends or public holidays.

4.9.6 Revocation checking requirement for relying parties

The mechanisms, if any, that a relying party may use or must use in order to check the status of certificates on which they wish to rely;

Before using a certificate, the relying party must validate it against the most recently published CRL in the ANSPGrid CA repository.

4.9.7 CRL issuance frequency (if applicable)

If a CRL mechanism is used, the issuance frequency;

A new CRL is published in the ANSPGrid CA repository after every certificate revocation and at least 7 days before the expiration of the current CRL.

4.9.8 Maximum latency for CRLs (if applicable)

If a CRL mechanism is used, maximum latency between the generation of CRLs and posting of the CRLs to the repository (in other words, the maximum amount of processing- and communication-related delays in posting CRLs to the repository after the CRLs are generated);

The CRL shall be copied from the computer that manages the HSM device to the on-line repository over a dedicated network that will be enabled for this purpose and will be only activated during this operation.

4.9.9 On-line revocation/status checking availability

On-line revocation/status checking availability, for instance, OCSP and a web site to which status inquiries can be submitted;

The latest CRL is always available from the ANSPGrid CA web site. No other on-line checking is available, although the possibility of setting up of an OCSP facility will be investigated.

4.9.10 On-line revocation checking requirements

Requirements on relying parties to perform on-line revocation/status checks;

Relying parties should check the CRL before they use and trust a certificate. No access control shall limit the possibility to check the CRL.

4.9.11 Other forms of revocation advertisements available

Except for informing the owner of a newly revoked certificate and the appropriate RA of the issued revocation, no advertisement of a new CRL other than its publication in the ANSPGrid CA repository will be made.

4.9.12 Special requirements re-key compromise

Any variations of the above stipulations for which suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation).

No stipulation.

4.9.13 Circumstances for suspension

Circumstances under which a certificate may be suspended.

The ANSPGrid CA does not suspend certificates.

4.9.14 Who can request suspension

Who can request the suspension of a certificate, for example, the subscriber, human resources personnel, a supervisor of the subscriber, or the RA in the case of an end-user subscriber certificate.

The ANSPGrid CA does not suspend certificates.

4.9.15 Procedure for suspension request

Procedures to request certificate suspension, such as a digitally signed message from the subscriber or RA, or a phone call from the RA.

The ANSPGrid CA does not suspend certificates.

4.9.16 Limits on suspension period

How long the suspension may last.

The ANSPGrid CA does not suspend certificates.

4.10 Certificate Status Services

This subcomponent addresses the certificate status checking services available to the relying parties.

4.10.1 Operational characteristics

The operational characteristics of certificate status checking services.

The ANSPGrid CA shall store in its public repository and make available via its web site:

a) the ANSPGrid CA certificate (and any parent CA certificate);
b) valid certificates; and
c) the most up-to-date CRL.

4.10.2 Service availability

The availability of such services, and any applicable policies on unavailability.

The ANSPGrid CA shall run this service continuously, except for unavoidable maintenance activities. Due to the nature of the Internet, this service cannot be guaranteed to be accessible always.

4.10.3 Optional features

Any optional features of such services.

Currently, none are being planned.

4.11 End of Subscription

This subcomponent addresses procedures used by the subscriber to end subscription to the CA services, including the revocation of certificates at the end of subscription (which may differ, depending on whether the end of subscription was due to the expiration of the certificate or termination of the service).

The subscription ends with the expiry of the certificate if it is not renewed before the expiration date. A subscription may end earlier if the subscriber requests a revocation of the certificate (see Section 4.9.3).

4.12 Key Escrow and Recovery

This subcomponent contains the following elements to identify the policies and practices relating to the escrowing, and/or recovery of private keys where private key escrow services are available (through the CA or other trusted third parties).

4.12.1 Key escrow and recovery policy and practices

Identification of the document containing private key escrow and recovery policies and practices or a listing of such policies and practices.

No key escrow or recovery services are provided. The key owner must take all reasonable steps to prevent loss of his/her private key.

4.12.2 Session key encapsulation and recovery policy and practices

Identification of the document containing session key encapsulation and recovery policies and practices or a listing of such policies and practices.

See Section 4.12.1.

5. Management, Operational, and Physical Controls

This component describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving.

This component can also be used to define non-technical security controls on repositories, subject CAs, RAs, subscribers, and other participants. The non-technical security controls for the subject CAs, RAs, subscribers, and other participants could be the same, similar, or very different.

These non-technical security controls are critical to trusting the certificates since lack of security may compromise CA operations resulting for example, in the creation of certificates or CRLs with erroneous information or compromising the CA private key.

Within each subcomponent, separate consideration will, in general, need to be given to each entity type, that is, the issuing CA, repository, subject CAs, RAs, subscribers, and other participants.

5.1 Physical Security Controls

In this subcomponent, the physical controls on the facility housing the entity systems are described.

The ANSPGrid CA equipment is located within the datacenter of the Núcleo de Computação Científica (NCC) da Unesp at the Unesp Barra Funda Campus in São Paulo, SP, Brazil. NCC maintains an access control system to its datacenter. All accesses to the CA server are limited to ANSPGrid CA personnel and system administrators. The ANSPGrid CA machine is equipped with a Hardware Security Module and may be kept online for backup and updates of the on-line repository with connectivity established through a highly protected and monitored network.

5.1.1 Site location and construction

Site location and construction, such as the construction requirements for high-security zones and the use of locked rooms, cages, safes, and cabinets;

The ANSPGrid CA office is located at the address of the organization administering this document (see Section 1.5.1).

The hardware is located at the following address:
Núcleo de Computação Científica da Unesp
Rua Dr. Bento Teobaldo Ferraz, 271 – Bloco II - Térreo
CEP 01140-070
São Paulo – SP – Brazil

The backup equipment (HSM and removable media) will be located ate the ANSPGrid CA office (see Section 1.5.1). The equipment is powered (standby) and is kept inside a locked rack with access restricted to ANSPGrid-CA´s staff.

5.1.2 Physical access

Physical access, i.e., mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room monitored by guards or security alarms and requiring movement from zone to zone to be accomplished using a token, biometric readers, and/or access control lists.

The CA operates in a controlled environment, where access is restricted to authorized ANSPGrid CA personnel and logged. The machine hosting the CA (also known as the signing machine) and its HSM device are kept locked in a safe. Access to the grounds and premises is controlled (and protected) by security guards and cameras.

5.1.3 Power and air conditioning

The ANSPGrid CA computing resources are protected by uninterruptible power supplies that provide sufficient energy to overcome power outages. This online machine operates in an air-conditioned environment and is not rebooted or taken offline except for essential maintenance. Environment temperature in the room housing the CA server is maintained at appropriate levels by the air conditioning systems at the NCC datacenter. The total capacity consists of three units of Stulz precision air conditioning system, each one with a 30 TR capacity.

5.1.4 Water exposures

Due to the location of the NCC facilities, floods are not expected. The ANSPGrid CA computing resources are kept away from windows, so no water exposure is expected to occur.

5.1.5 Fire prevention and protection

The NCC datacenter is equipped an air-sampling smoke detector to prevent fire. Fire extinguishants are composed by HFC-227ea clean agent system, a waterless fire supression.

5.1.6 Media storage

Media storage, for example, requiring the storage of backup media in a separate location that is physically secure and protected from fire and water damage.

All media, used for:

a) the ANSPGrid CA's private key, extracted from the operational HSM in an encrypted file that is accessible only by the backup HSM device, is kept in several removable storage media; and
b) backup copies of CA related information, kept on DVD or CD; are stored in a safe place to which only authorized personnel have access.

5.1.7 Waste disposal

Waste containing potential confidential information or data to be protected (cryptographically relevant data like private keys or passphrases, or personal data) shall be disposed off in a way to guarantee that the information may not be obtained or re-used.

5.1.8 Off-site backup

Off-site backups will be performed at reasonable intervals.

5.2. Procedural Controls

In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role. Examples of trusted roles include system administrators, security officers, and system auditors.

5.2.1 Trusted roles

The following roles are defined within the ANSPGrid CA:
a) the CA Manager is the overall responsible for the administration of the CA covering all administrative and technical aspects of the CA activities;
b) the CA System Administrator(s) is responsible for the maintenance and security of the CA systems;
c) the CA Operator(s) issues certificates and CRLs, revokes certificates and performs backups;
d) the RA Manager authenticates identities and signs CSRs;
e) the RA Local Representative or Agent verifies the requester's identity and eligibility and informs the RA manager via signed e-mail; and
f) the Auditor verifies log files and ensures the proper compliance of the CA operation with the CP/CPS and operation documents.

5.2.2 Number of persons required per task

For each task identified, the number of individuals required to perform the task (n out m rule) should be stated for each role. Identification and authentication requirements for each role may also be defined.

All administrative tasks require the presence of at least two out of six people. All operational tasks require the presence of a single operator.

5.2.3 Identification and authorization for each role

This component also includes the separation of duties in terms of the roles that cannot be performed by the same individuals.

No stipulation.

5.3 Personnel Security Controls

All personnel will be required to sign an agreement with the ANSPGrid CA stating awareness and agreement to adhere to the current version of the ANSPGrid CA CP/CPS document.

5.3.1 Qualifications, experience, and clearance requirements

Qualifications, experience, and clearances that personnel must have as a condition of filling trusted roles or other important roles. Examples include credentials, job experiences, and official government clearances that candidates for these positions must have before being hired.

The ANSPGrid CA management and system administration personnel shall have system administrator or analyst experience.

5.3.2 Background check procedures

Background checks and clearance procedures that are required in connection with the hiring of personnel filling trusted roles or perhaps other important roles; such roles may require a check of their criminal records, references, and additional clearances that a participant undertakes after a decision has been made to hire a particular person;

All access to the servers and applications that comprise the ANSPGrid service is limited to ANSP technical support staff. No external persons are authorized to access the CA facilities without the physical presence of CA personnel.

The RA Manager should preferably be a paid employee of the organization hosting that Registration Authority, but must:

a) be member of the department or unit hosting that Registration Authority; and
b) be appointed by an authority responsible for the department or unit of the organization.

The ANSPGrid CA can only recognize the appointment of an RA Manager with receipt of a written declaration to said effect from the appropriate authority on the organization's headed paper. The information that must be contained in this letter is

defined in the *Registration Authority Obligations, Responsibilities and Operations Manual*.

The recruitment of other RA personnel (RA Local Representatives) is the responsibility of the RA Manager. The RA Manager may appoint any number of RA Local Representatives including himself/herself. All RA personnel must have personal certificates and must adhere to both the subscriber and RA obligations as set out in the current version of the ANSPGrid CA CP/CPS.

5.3.3 Training requirements

Training requirements and training procedures for each role following the hiring of personnel.

All personnel acting as CA operators and RA managers shall be trained on the job by the team responsible the development and maintenance of the CA management software. Internal training covering Public Key Encryption (PKI) principles, security and the CA operation procedures will be available to all CA personnel.

5.3.4 Retraining frequency and requirements

Any retraining period and retraining procedures for each role after completion of initial training.

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

5.3.5 Job rotation frequency and sequence

Frequency and sequence for job rotation among various roles.

Job rotation is not performed.

5.3.6 Sanctions for unauthorized actions

Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity systems for the purpose of imposing accountability on a participant's personnel.

In the event of unauthorized actions, abuse of authority or unauthorized use of entity systems by CA or RA personnel, the CA manager may revoke the privileges of those concerned. The ANSPGrid CA also reserves the right to prosecute unauthorized actions to the fullest extent under the legal provisions of the appropriate organization and the local national law.

5.3.7 Independent contractor requirements

Controls on personnel that are independent contractors rather than employees of the entity; examples include: Bonding requirements on contract personnel; Contractual requirements including indemnification for damages due to the actions of the contractor personnel; Auditing and monitoring of contractor personnel; and other controls on contracting personnel.

No stipulation.

5.3.8 Documentation supplied to personnel

Documentation to be supplied to personnel during initial training, retraining, or otherwise.

All ANSPGrid CA personnel shall be provided with up to date documentation to help perform their tasks successfully.
The following documentation is provided to the ANSPGrid CA personnel:

a) A copy of the current CP/CPS document;
b) ANSPGrid CA *Obligations, Responsibilities and Operations Manual*.

Each RA Manager and Local Representative will receive the following documentation:

a) A copy of the current CP/CPS document;
b) *Registration Authority Obligations, Responsibilities and Operations Manual*.

5.4 Audit Logging Procedures

This subcomponent is used to describe event logging and audit systems, implemented for the purpose of maintaining a secure environment.

5.4.1 Types of events recorded

Types of events recorded, such as certificate lifecycle operations, attempts to access the system, and requests made to the system.

The following types of events associated the ANSPGrid CA signing machine shall be recorded:

a) reboot / login / logout;
b) issued signed certificates;
c) revoked certificates
d) re-keyed certificates;
e) issued CRLs;
f) audit log events;

The following events on the ANSPGrid CA Web server shall be recorded together with supporting documentation, where applicable:

a) reboot / login / logout;

b) certification requests;
c) revocation requests;
d) certificate re-key requests;
e) issue and import of certificate to repository;
f) certificate revocation;
g) issued CRLs; and
h) implemented versions of the CP/CPS documents.

Event records are time-stamped. For online systems, the clock is synchronized through NTP. For offline systems the clock is manually set and periodically verified.

5.4.2 Frequency of processing log

Frequency with which audit logs are processed or archived, for example, weekly, following an alarm or anomalous event, or when ever the audit log is n% full.

The log files shall be processed and archived once a month, or after a potential security breach is suspected or known, whichever comes first.

5.4.3 Retention period for audit log

Period for which audit logs are kept.

The minimal retention period for the audit logs is 3 years for both log files and repository data. Information relating to subscriber certificates must be kept for at least for two years after the expiry of the last certificate issued to that end entity.

5.4.4 Protection of audit log

Who can view audit logs, for example only the audit administrator. Protection against modification of audit logs, for instance a requirement that no one may modify or delete the audit records or that only an audit administrator may delete an audit file as part of rotating the audit file; and protection against deletion of audit logs.

While in the system, the audit logs are protected by the operational HSM device and shall only be accessible to the ANSPGrid CA Manager, Auditor and system administrators. When processed, the archives are copied to a read only off-line medium in encrypted form and stored in a safe place. The protection shall be state-of-the-art best effort.

5.4.5 Audit log backup procedures

The audit logs are copied monthly to an off-line medium in encrypted format and stored in a safe place. Paper documents are kept in a locked place with restricted access.

5.4.6 Audit collection system (internal vs. external)

Whether the audit log accumulation system is internal or external to the entity.

The audit collection system is internal to the ANSPGrid CA.

5.4.7 Notification to event-causing subject

Whether the subject who caused an audit event to occur is notified of the audit action.

Not defined.

5.4.8 Vulnerability assessments

Vulnerability assessments, for example, where audit data is run through a tool that identifies potential attempts to breach the security of the system.

Audit data on the ANSPGrid CA web server will be analyzed daily for potential breaches of system security automatically using the appropriate tools available (e.g. logwatch). Furthermore, if considered necessary, tools will be employed to allow the ANSPGrid CA server to protect itself from, for example, denial of service attacks.

5.5 Records Archival

This subcomponent is used to describe general records archival (or records retention) policies.

5.5.1 Types of records archived

Types of records that are archived, for example, all audit data, certificate application information, and documentation supporting certificate applications.

See Section 5.4.1.

5.5.2 Retention period for archive

The minimum retention period is 3 years. Information relating to subscriber certificates must be kept for at least for two years after the expiry of the last certificate issued to that end entity.

5.5.3 Protection of archive

Who can view the archive, for example, a requirement that only the audit administrator may view the archive; Protection against modification of the archive, such as securely storing the data on a write once medium; Protection against deletion of the archive; Protection against the deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media; and protection against obsolescence of hardware, operating systems, and other software, by, for example, retaining as part of the archive the hardware, operating systems, and/or other software in order to permit access to and use of archived records over time.

The archive held on read-only media shall only be accessible to authorized external auditors (see Section 8.3) and the ANSPGrid CA personnel.

5.5.4 Archive backup procedures

The archives are copied monthly to an off-line medium in encrypted format and stored together with any paper documents in a locked place with restricted access.

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

Whether the archive collection system is internal or external.

The archive collection system is internal to the ANSPGrid CA. Information considered confidential is not made available to be public. Information considered nonconfidential maybe made available to the public only if the information is kept on-line.

5.5.7 Procedures to obtain and verify archive information

Procedures to obtain and verify archive information, such as a requirement that two separate copies of the archive data be kept under the control of two persons, and that the two copies be compared in order to ensure that the archive information is accurate.

Not defined.

5.6 Key Changeover

This subcomponent describes the procedures to provide a new public key to a CA's users following a re-key by the CA. These procedures may be the same as the procedure for providing the current key. Also, the new key may be certified in a certificate signed using the old key.

As the key generation is carried out by each end entity (subscriber) by, for example, using a web browser, no provision is made by the ANSPGrid CA for a key changeover.

In the case of a changeover of the ANSPGrid CA's key pair, an overlap of the old and new keys will exist. While the new key will be used for signing certificate, the older but still valid certificate must be available to verify old digital signatures – and the private key to sign CRLs – until all the 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 (see Section 4.3.2).

5.7 Compromise and Disaster Recovery

This subcomponent describes requirements relating to notification and recovery procedures in the event of compromise or disaster. Each of the following may need to be addressed separately.

5.7.1 Incident and compromise handling procedures

Identification or listing of the applicable incident and compromise reporting and handling procedures.

If the private key of an end entity is lost or compromised due to corruption, the end entity must inform their RA immediately in order to request the revocation of their certificate. All relying parties known to accept the key should be informed by the owner of the key.

If the private key of the ANSPGrid CA is (or suspected of being) compromised, the CA Manager must:

a) make every reasonable effort to notify subscribers and RAs;
b) terminate the issuing and distribution of certificates and CRLs;
c) request revocation of the compromised certificate;
d) generate a new CA key pair and certificate and publish the certificate in the repository;
e) revoke all of the valid certificates that have been previously signed by the compromised key;
f) publish the new CRL on the ANSPGrid CA repository;
g) Notify relevant security contacts; and
h) Notify relying parties and cross-certifying CAs, of which the CA is aware, as widely as possible.

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

The recovery procedures used if computing resources, software, and/or data are corrupted or suspected to be corrupted. These procedures describe how a secure environment is re-established, which certificates are revoked, whether the entity key is revoked, how the new entity public key is provided to the users, and how the subjects are re-certified.

The ANSPGrid CA will take best effort precautions to enable a quick recovery. In case of corruption, the CA systems are either repaired or rebuilt from the last good backup. If a good backup cannot be identified, the systems will be reinstalled from scratch. In order to be able to resume operation as soon as possible after corruption, the following steps shall be performed:

a) all CA software shall be backed-up on a removable medium after a new release or modifications to any of its components have been installed;

b) all data files of the offline CA shall be backed-up on a removable medium after each change, before the session is closed.

If the ANSPGrid CA private key has not been comprised and even all but one of the encrypted copies of the private key been destroyed or lost, CA operations shall be reestablished as soon as possible without need to revoke all issued certificates. In the case of a major disaster where critical CA information is completely lost, the CA will suspend operations as in the case of CA private key compromise.

If public certificates stored in the repository are lost or corrupted, certificates will be revoked.

5.7.3 Entity private key compromise procedures

The recovery procedures used if the entity key is compromised. These procedures describe how a secure environment is re-established, how the new entity public key is provided to the users, and how the subjects are re-certified.

If an end entity's or RA's private key is compromised, the corresponding public key and certificate must be revoked following the procedure in Section 4.9. All relying parties known to accept the certificate should be informed by the owner of the compromised key. After revocation, the user should request a certificate for a new key pair.

5.7.4 Business continuity capabilities after a disaster

The entity's capabilities to ensure business continuity following a natural or other disaster. Such capabilities may include the availability of a remote hot-site at which operations may be recovered. They may also include procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is re-established, either at the original site or at a remote site. For example, procedures to protect against theft of sensitive materials from an earthquake-damaged site.

The ANSPGrid CA will make its best efforts to keep the CA systems and materials secure in case of disaster. The recovery plan will be activated as soon as possible using the off-site system backup, which includes a second HSM device used for backup purposes, located inside the ANSP CA office (see section 5.1.1).

5.8 CA or RA Termination

This subcomponent describes requirements relating to procedures for termination and termination notification of a CA or RA, including the identity of the custodian of CA and RA archival records.

Prior to termination, the ANSPGrid CA will:

a) Notify the ANSPGrid CA subordinate RAs;
b) Notify subscribers and rely parties;
c) Make information of its termination widely available;
d) Terminate the issuance and distribution of certificates;
e) Revoke all certificates;
f) Issue and publish CRLs; and
g) Notify relevant security contacts.

Notifications will be sent prior to the termination and as early as possible. An advance notice of no less than 60 days will be given in the case of normal (scheduled) termination. The CA Manager may decide to let the CA only issue CRLs during the last year (i.e. the maximum lifetime of a subscriber certificate) before the actual termination. This will allow subscribers' certificates to be used until they expire. In that case, notice of termination is given no less than one year and 60 days prior to the actual termination, i.e. no less than 60 days before the CA ceases to issue new certificates.

Upon termination, all copies of its private key will be destroyed. The CA Manager at the time of termination shall be responsible for the subsequent archival of all records as required in Section 5.5.2. The CA records will remain, if possible, under the custody of the Academic Network at São Paulo.

6. Technical Security Controls

This component is used to define the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). This component may also be used to impose constraints on repositories, subject CAs, subscribers, and other participants to protect their private keys, activation data for their private keys, and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, and archiving. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

This component can also be used to define other technical security controls on repositories, subject CAs, RAs, subscribers, and other participants.

6.1 Key Pair Generation and Installation

Key pair generation and installation need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers.

6.1.1 Key pair generation

Who generates the entity public, private key pair? Possibilities include the subscriber, RA, or CA. Also, how is the key generation performed? Is the key generation performed by hardware or software?

The key pair for the ANSPGrid CA is generated by the operational HSM.

The ANSPGrid 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.

6.1.2 Private key delivery to subscriber

How is the private key provided securely to the entity? Possibilities include a situation where the entity has generated it and therefore already has it, handing the entity the private key physically, mailing a token containing the private key securely, or delivering it in an SSL session.

The ANSPGrid CA does not generate private keys for its subscribers, hence does not deliver private keys. Each subscriber must generate his/her own key pair using a trustworthy method. The ANSPGrid CA will provide web interface to guide subscribers.

6.1.3 Public key delivery to certificate issuer

How is the entity's public key provided securely to the certification authority? Some possibilities are in an online SSL session or in a message signed by the RA.

The authenticating RA can either transmit the certification request containing the public key to the ANSPGrid CA in an e-mail signed by the RA Manager or in person by the RA Manager on floppy disk, CDROM or pendrive. However, it is preferable that the request be uploaded to the CA's secure web server via a SSL connection via the interface provided.

6.1.4 CA public key delivery to relying parties

In the case of issuing CAs, how is the CA's public key provided securely to potential relying parties? Possibilities include handing the public key to the relying party securely in person, physically mailing a copy securely to the relying party, or delivering it in a SSL session.

The CA certificate (containing its public key) can be downloaded from the ANSPGrid repository on the ANSPGrid CA web server (see Section 2.1). Alternatively, the certificate can also be obtained from the IGTF's TAGPMA repository (see Section 1.3.5) to which a copy of certificate will be securely transferred once accreditation of the ANSPGrid CA has been approved by the TAGPMA.

6.1.5 Key sizes

What are the key sizes? Examples include a 1,024 bit RSA modulus and a 1,024 bit DSA large prime.

The minimum key length for a personnel or server certificate is 1024 bits (RSA modulus). Keys of length less than 1024 bits will not be accepted.

For the ANSPGrid CA, the key shall be an RSA key with a modulus of 2048 bits.

6.1.6 Public key parameters generation and quality checking

Who generates the public key parameters, and is the quality of the parameters checked during key generation?

There is no stipulation as to the validity and quality of the generated key pair. Only the validity of the certificate issued by the ANSPGrid CA is defined by this CP/CPS document.

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

For what purposes may the key be used, or for what purposes should usage of the key be restricted? For X.509 certificates, these purposes should map to the key usage flags in X.509 Version 3 certificates.

The ANSPGrid CA issues X.509 v3 certificates which are valid if they have been signed by the ANSPGrid CA's private key and have not been revoked, i.e. do not appear in the currently valid CRL.

The keys may be used according to the type of certificate. The CA's private key is the only key that can be used for signing certificates and CRLs. An RA certificate may only be used for activities required for the work of an RA. Uses for an end-entity certificate may include:

a) Authentication;
b) non-repudiation;
c) data and key encipherment;
d) object integrity (especially messages);
e) session establishment; and
f) proxy creation and signing.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Requirements for private key protection and cryptographic modules need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers.

6.2.1 Cryptographic module standards and controls

What standards, if any, are required for the cryptographic module used to generate the keys? A cryptographic module can be composed of hardware, software, firmware, or any combination of them. For example, are the keys certified by the infrastructure required to be generated using modules compliant with the US FIPS 140-1? If so, what is the required FIPS 140-1 level of the module? Are there any other engineering or other controls relating to a cryptographic module, such as the identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests.

The ANSPGrid CA operates using two Hardware Security Modules (HSM) devices, one for operational and the other for backup purposes.
The HSM device chosen is provided a brazilian security company called Kryptus (http://kryptus.com) and the model is the ASI-HSM AHX2, which is compliant with the FIPS140-2 level 4. It also features advanced physical protection.

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

Is the private key under n out of m multi-person control? If yes, provide n and m (two person control is a special case of n out of m, where n = m = 2)?

The private key is kept inside the operational HSM and can be restored only by the backup HSM via upload of an encrypted file generated by the operational HSM. The administrative role of the HSM´s requires two out of six smart cards. The operational role of the HSM´s requires one out of six smart cards.

6.2.3 Private key escrow

Is the private key escrowed? If so, who is the escrow agent, what form is the key escrowed in (examples include plaintext, encrypted, split key), and what are the security controls on the escrow system?

Private keys must not be escrowed.

6.2.4 Private key backup

Is the private key backed up? If so, who is the backup agent, what form is the key backed up in (examples include plaintext, encrypted, split key), and what are the security controls on the backup system?

See 6.2.2.

6.2.5 Private key archival

Is the private key archived? If so, who is the archival agent, what form is the key archived in (examples include plaintext, encrypted, split key), and what are the security controls on the archival system?

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

Under what circumstances, if any, can a private key be transferred into or from a cryptographic module? Who is permitted to perform such a transfer operation? In what form is the private key during the transfer (i.e., plaintext, encrypted, or split key)?

The CA private key is transferred off the HSM only for backups in a encrypted form using HSM backup asymmetric key.

6.2.7 Private key storage on cryptographic module

How is the private key stored in the module (i.e., plaintext, encrypted, or split key)?

The CA private key is kept encrypted inside the operational HSM and is activated by smartcards with pin. Once activated, the key is available in the HSM RAM memory, however, as the device has an advanced physical security protection, the key cannot be stolen.

6.2.8 Method of activating private key

Who can activate (use) the private key? What actions must be performed to activate the private key (e.g., login, power on, supply PIN, insert token/key, automatic, etc.)? Once the key is activated, is the key active for an indefinite period, active for one time, or active for a defined time period?

See 6.2.7.

6.2.9 Method of deactivating private key

Who can deactivate the private key and how? Examples of methods of deactivating private keys include logging out, turning the power off, removing the token/key, automatic deactivation, and time expiration.

The operators can deactivate the private key via the HSM interface, but the key should be automatically deactivated after the requested number of operations informed during the activation process. Also the HSM automatically deactivated the private key after a time out.

6.2.10 Method of destroying private key

Who can destroy the private key and how? Examples of methods of destroying private keys include token surrender, token destruction, and overwriting the key.

Only the administrators of the HSM (two out of six) can perform this operation.

6.2.11 Cryptographic Module Rating

Provide the capabilities of the cryptographic module in the following areas: identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests. Capability may be expressed through reference to compliance with a standard such as U.S. FIPS 140-1, associated level, and rating.

The HSM device model is the ASI-HSM AHX2, which is compliant with the FIPS140-2 level 4. It also features advanced physical protection.

6.3 Other Aspects of Key Pair Management

Other aspects of key management need to be considered for the issuing CA, repositories, subject CAs, RAs, subscribers, and other participants.

6.3.1 Public key archival

Is the public key archived? If so, who is the archival agent and what are the security controls on the archival system? Also, what software and hardware need to be preserved as part of the archive to permit use of the public key over time? Note: this subcomponent is not limited to requiring or describing the use of digital signatures with archival data, but rather can address integrity controls other than digital signatures when an archive requires tamper protection. Digital signatures do not provide tamper protection or protect the integrity of data; they merely verify data integrity. Moreover, the archival period may be greater than the cryptanalysis period for the public key needed to verify any digital signature applied to archival data.

The ANSPGrid CA shall archive all certificates it issues on removable media to be stored off-line in a secure place. This information will be maintained after the CA has been deactivated for the period stated in Section 5.5.2.

6.3.2 Certificate operational periods and key pair usage periods

What is the operational period of the certificates issued to the subscriber. What are the usage periods, or active lifetimes, for the subscriber's key pair?

Subscribers' certificates have a validity period of at most one year (as outlined in Section 4.3.2). The CA certificate has a validity of 10 years.

6.4 Activation Data

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorized use of the private key, and potentially needs to be considered for the issuing CA, subject CAs, RAs, and subscribers. Such consideration potentially needs to address the entire life-cycle of the activation data from generation through archival and destruction. For each of the entity types (issuing CA, repository, subject CA, RA, subscriber, and other participants), all of the questions listed in 6.1 through 6.3 potentially need to be answered with respect to activation data rather than with respect to keys.

6.4.1 Activation data generation and installation

The ANSPGrid CA private key is protected by the HSM.

6.4.2 Activation data protection

Not defined.

6.4.3 Other aspects of activation data

Not defined.

6.5 Computer Security Controls

This subcomponent is used to describe computer security controls such as: use of the trusted computing base concept, discretionary access control, labels, mandatory access controls, object re-use, audit, identification and authentication, trusted path, security testing, and penetration testing. Product assurance may also be addressed.

A computer security rating for computer systems may be required. The rating could be based, for example, on the Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), or the Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408:1999. This subcomponent can also address requirements for product evaluation analysis, testing, profiling, product certification, and/or product accreditation related activity undertaken.

6.5.1 Specific computer security technical requirements

No stipulation.

6.5.2 Computer security rating

Not defined.

6.6 Life Cycle Security Controls

This subcomponent addresses system development controls and security management controls.

System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design

and implementation techniques (e.g., defensive programming) and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEICMM).

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

This subcomponent addresses network security related controls, including firewalls.

The Certificate Authority's signing machine will be equipped with a HSM module and will be kept online protected by a suitably configured firewall. The signing machine is located in a secure environment and is managed by suitably trained personnel. The signing machine is a dedicated resource; only the services necessary for the secure operation of the signing machine are enabled.

The online web server is protected by a suitably configured firewall.

6.8 Time-stamping

This subcomponent addresses requirements or practices relating to the use of timestamps on various data. It may also discuss whether or not the time-stamping application must use a trusted time source.

All time stamping of entries created on the online servers at the ANSPGrid CA is based on the network time obtained from the www.ntp.br supported by NIC.Br.

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

7. Certificate, CRL and OCSP Profiles

This component is used to specify the certificate format and, if CRLs and/or OCSP are used, the CRL and/or OCSP format. This includes information on profiles, versions, and extensions used.

7.1 Certificate Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 3280):

All certificates issued by the ANSPGrid CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280 [Housley02].

7.1.1 Version number(s)

The ANSPGrid 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 ANSPGrid CA certificates for personal certificates are the following:

a) Basic Constraints: **critical, ca: false**
b) Subject Key Identifier: ***unique identifier of the subject key*** (composed of the 160-bit SHA-1 hash of the value of the certified public key).
c) Authority Key Identifier: ***keyid*** (the unique identifier of the issuing CA composed of the 160-bit SHA-1 hash of the value of the public key of the ANSPGrid CA)
d) Key Usage: **critical, digitalSignature, keyEncipherment, dataEncipherment**
e) Extended Key Usage: **TLS Web Server Authentication, TLS Web Client Authentication**
f) X509v3 CRL Distribution Points: **http://gridca.ansp.br/media/ca/anspca.crl**
g) Subject alternative name: **User E-mail address**.

For server/services certificates:

a) Basic Constraints: **critical, ca: false**
b) Subject Key Identifier: ***unique identifier of the subject key*** **(hash)**.
c) Authority Key Identifier: ***keyid*** **(the unique identifier of the issuing ANSPGrid CA)**
d) Key Usage: **critical, digitalSignature, keyEncipherment, dataEncipherment**
e) Extended Key Usage: **TLS Web Server Authentication, TLS Web Client Authentication**
f) X509v3 CRL Distribution Points: **http://gridca.ansp.br/media/ca/anspca.crl**
g) Subject alternative name: ***Server DNS FQDN host name***

In the case of the ANSPGrid CA certificate:

a) Basic Constraints: **critical, ca: true**
b) Subject Key Identifier: **hash**
c) Authority Key Identifier: **keyid**
d) Key Usage: **critical, Certificate Sign, CRLSign**

7.1.3 Algorithm object identifiers

The OIDs for the respective algorithms used for digital signatures of certificates issued by the ANSPGrid CA are, according to [Polk02], as follows:

a) hash function: id-sha1 1.3.14.3.2.26
b) encryption: rsaEncryption 1.2.840.113549.1.1.1
c) signature: sha1WithRSAEncryption 1.2.840.113549.1.1.5

7.1.4 Name forms

Each entity will be given a unique and unambiguous Distinguished Name (DN) by the ANSPGrid CA. Depending on the type of entity, the DN will be of 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

Each ANSPGrid certificate policy has a unique associated object identifier (OID). The OID for this policy is given in Section 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

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 3280).

7.2.1 Version number(s)

The ANSPGrid CA creates and publishes X.509 version 2 CRLs that conform to the Internet PKI profile (PKIX) for X.509 Certificate Revocation Lists as defined by RFC 3280 [Housley02].

7.2.2 CRL and CRL entry extensions

CRL and CRL entry extensions populated and their criticality.

The ANSPGrid CA shall issue complete CRLs for all certificates issued by it independently of the reason for the revocation. The CRL shall include the date by which the next CRL should be issued. A new CRL shall be issued before this date if new revocations are issued.

The CRL extensions that shall be included are:

a) the Authority Key Identifier (equal to the issuer's key identifier); and
b) the CRL Number (a monotonically increasing sequence number).

Each entry will be identified by the certificates serial number and a corresponding Revocation Date. The following CRL entry extension may also be included:

a) CRL Reason Code

Stale entries (certificates which would have expired if not revoked) will not be removed from the CRLs.

7.3. OCSP Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the IETF RFC 2560 profile).

Not yet used.

7.3.1 Version number(s)

Version of OCSP that is being used as the basis for establishing an OCSP system.

Not yet defined.

7.3.2 OCSP extensions

OCSP extensions populated and their criticality.

Not yet defined.

8. Compliance Audit and Other Assessment

The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment; examples include WebTrust for CAs and SAS 70.

8.1 Frequency or circumstances of assessment

Frequency of compliance audit or other assessment for each entity that must be assessed pursuant to a CP or CPS, or the circumstances that will trigger an assessment; possibilities include an annual audit, pre-operational assessment as a condition of allowing an entity to be operational, or investigation following a possible or actual compromise of security.

The ANSPGrid CA shall carry out, at least once a year, a self-assessment to check the 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 and the RA operations manual in effect.

The auditor, as his/her discretion, may ask to carry out an audit at anytime, in particular, in the event of (or suspicion of) malpractice by CA or RA personnel, security flaws or complaints from subscribers or relying parties.

8.2 Identity/qualifications of assessor

The identity and/or qualifications of the personnel performing the audit or other assessment.

Not defined.

8.3 Assessor's relationship to assessed entity

The relationship between the assessor and the entity being assessed, including the degree of independence of the assessor.

The Auditor of the ANSPGrid CA or a duly appointed member(s) of the IC-UFF are free to make assessments of the CA operations at anytime. Member organizations of the TAGPMA may also undertake assessments if previously approved by the TAGPMA. Any Brazilian governmental organization or academic institution 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

Actions taken as a result of deficiencies found during the assessment; examples include a temporary suspension of operations until deficiencies are corrected, revocation of certificates issued to the assessed entity, changes in personnel, triggering special investigations or more frequent subsequent compliance assessments, and claims for damages against the assessed entity.

The ANSPGrid CA shall take immediate action if the assessment reveals a conflict between the provisions of the CP/CPS document and actual practice. This may result in improving the practice of the CA and, potentially, reflecting the change in a new version of the CP/CPS document, or if the practice seems adequate the policy and CP/CPS document shall be reviewed.

In case of a deficiency, the ANSPGrid CA Manager will announce the steps that will be taken to remedy the deficiency and an estimated timetable. If a discovered 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 immediately.

8.6 Communication of results

Who is entitled to see results of an assessment (e.g., assessed entity, other participants, the general public), who provides them (e.g., the assessor or the assessed entity), and how they are communicated.

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

This component covers general business and legal matters. Sections 9.1 and 9.2 of the framework discuss the business issues of fees to be charged for various services and the financial responsibility of participants to maintain resources for ongoing operations and for paying judgments or settlements in response to claims asserted against them. The remaining sections are generally concerned with legal topics.

Starting with Section 9.3 of the framework, the ordering of topics is the same as or similar to the ordering of topics in a typical software licensing agreement or other technology agreement. Consequently, this framework may not only be used for CPs and CPSs, but also associated PKI-related agreements, especially subscriber agreements, and relying party agreements. This ordering is intended help lawyers review CPs, CPSs, and other documents adhering to this framework.

With respect to many of the legal subcomponents within this component, a CP or CPS drafter may choose to include in the document terms and conditions that apply directly to subscribers or relying parties. For instance, a CP or CPS may set forth limitations of liability that apply to subscribers and relying parties. The inclusion of terms and conditions is likely to be appropriate where the CP or CPS is itself a contract or part of a contract.

In other cases, however, the CP or CPS is not a contract or part of a contract; instead, it is configured so that its terms and conditions are applied to the parties by separate documents, which may include associated agreements, such as subscriber or relying party agreements. In that event, a CP drafter may write a CP so as to require that certain legal terms and conditions appear (or not appear) in such associated agreements. For example, a CP might include a subcomponent stating that a certain limitation of liability term must appear in a CA's subscriber and relying party agreements. Another example is a CP that contains a subcomponent prohibiting the use of a subscriber or relying party agreement containing a limitation upon CA liability inconsistent with the provisions of the CP. A CPS drafter may use legal subcomponents to disclose that certain terms and conditions appear in associated subscriber, relying party, or other agreements in use by the CA. A CPS might explain, for instance, that the CA writing it uses an associated subscriber or relying party agreement that applies a particular provision for limiting liability.

9.1 Fees

This subcomponent contains any applicable provisions regarding fees charged by CAs, repositories, or RAs.

No fees will be charged for the certification service provided by the ANSPGrid CA to the community defined in Section 1.3.3.

9.1.1 Certificate issuance or renewal fees

Not applicable, see Section 9.1.

9.1.2 Certificate access fees

Not applicable, see Section 9.1.

9.1.3 Revocation or status information access fees

Not applicable, see Section 9.1.

9.1.4 Fees for other services

Fees for other services such as providing access to the relevant CP or CPS.

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

9.1.5 Refund policy

Not applicable, see Section 9.1.

9.2 Financial Responsibility

This subcomponent contains requirements or disclosures relating to the resources available to CAs, RAs, and other participants providing certification services to support performance of their operational PKI responsibilities, and to remain solvent and pay damages in the event they are liable to pay a judgment or settlement in connection with a claim arising out of such operations.

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

9.2.1 Insurance coverage

A statement that the participant maintains a certain amount of insurance coverage for its liabilities to other participants.

No stipulation.

9.2.2 Other assets

A statement that a participant has access to other resources to support operations and pay damages for potential liability, which may be couched in terms of a minimum level of assets necessary to operate and cover contingencies that might occur within a PKI, where examples include assets on the balance sheet of an organization, a surety bond, a letter of credit, and a right under an agreement to an indemnity under certain circumstances.

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

A statement that a participant has a program that offers first-party insurance or warranty protection to other participants in connection with their use of the PKI.

No stipulation.

9.3 Confidentiality of Business Information

This subcomponent contains provisions relating to the treatment of confidential business information that participants may communicate to each other, such as business plans, sales information, trade secrets, and information received from a third party under a nondisclosure agreement.

9.3.1 Scope of confidential information

The scope of what is considered confidential information.

No stipulation.

9.3.2 Information not within the scope of confidential information

The types of information that are considered to be outside the scope of confidential information.

No stipulation.

9.3.3 Responsibility to protect confidential information

The responsibilities of participants that receive confidential information to secure it from compromise, and refrain from using it or disclosing it to third parties.

No stipulation.

9.4 Privacy of Personal Information

This subcomponent relates to the protection that participants, particularly CAs, RAs, and repositories, may be required to afford to personally identifiable private information of certificate applicants, subscribers, and other participants. Specifically, this subcomponent addresses the following, to the extent pertinent under applicable law.

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

The ANSPGrid CA service collects information about its subscribers for administrative and operational purposes only. Information included in issued certificates and CRLs is public and not considered confidential. All other information that is not included in the certificates and CRL shall be considered confidential and shall not be released outside the ANSPGrid CA and the RA performing the registration. Additionally, the ANSPGrid CA also keeps contact information of CA Operators, RA Managers and RA Local Representatives for restricted internal use only.

9.4.1 Privacy plan

The designation and disclosure of the applicable privacy plan that applies to a participant's activities, if required by applicable law or policy.

No stipulation.

9.4.2 Information treated as private

Information that is considered private within the PKI.

All personal information provided by the subscriber to verify his/her identity will be kept confidential except for that which is included in their certificate.

9.4.3 Information not deemed private

Information that is not considered private within the PKI.

Information included in the certificates and the CRL issued by the ANSPGrid CA shall not be considered private. By requesting a certificate from the ANSPGrid CA, the subscriber consents to the inclusion of this information as part of the certificate publication. 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

Any responsibility of participants that receive private information to secure it, and refrain from using it and from disclosing it to third parties.

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

9.4.5 Notice and consent to use private information

Any requirements as to notices to, or consent from individuals regarding use or disclosure of private information.

In the case that the ANSPGrid CA or any of its accredited RAs want to use private information, it must obtain written consent from the subscriber. The subscriber is under no obligation to agree to the request and his/her decision has no effect what so ever on the service provided to that subscriber.

9.4.6 Disclosure pursuant to judicial or administrative process

Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

The CA will not disclose confidential information to any third party unless authorized to do so by the subscriber or when required to 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 ANSPGrid CA related to that subscriber only. This information will be released to the subscriber if the CA has received a signed e-mail from the subscriber requesting such information. The CA will recognize requests in writing for the release of personal information from a subscriber provided the subscriber can be properly authenticated.

9.5 Intellectual Property Rights

This subcomponent addresses the intellectual property rights, such as copyright, patent, trademarks, or trade secrets, that certain participants may have or claim in a CP, CPS, certificates, names, and keys, or are the subject of a license to or from participants.

The ANSPGrid CA does not claim any intellectual property rights on certificates that it has issued. This document is based on the following sources:

a) RFC 3647 [Chokani03] and RFC 2527 [Chokani99] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
b) RFC 1778 The String Representation of Standard Attribute Syntaxes;
c) RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions;
d) RFC 882 Standard for the format of ARPA Internet text messages;
e) Profile for Traditional X.509 Public Key Certification Authorities with secured infrastructure (Classic CA minimum requirements of the IGTF) Version 4.0 [CCA05];

Parts if this document have been inspired by and even copied from other CP/CPS (in no particular order):

f) UFF LACGrid CA Certificate Policy and Certificate Practice Statement (Brazil), Version 1.0, December 2006. https://lacgridca.ic.uff.br//index.php?option=com_docman&task=cat_view&gid=3&Itemid=13 ;
g) UFF BrGrid CA Certificate Policy and Certificate Practice Statement (Brazil),

Version 1.0, July 2006. http://brgridca.ic.uff.br/policy/cp-cps-1.0.pdf ;
h) pkIRISGrid Certificate Policy and Certificate Practice Statement (Spain), Version 1.1.0, January 2006. http://www.irisgrid.es/pki/cps/cps-1.2.pdf ;
i) AUSTRIANGRID CA Certificate Policy and Certification Practice Statement (Austria) Version 1.0.0, March 2005. https://ca.austriangridca.at/CP_CPS/AustrianGridCA_CP_CPS_1_0_0.pdf ;
j) LIP CA Certificate Policy and Certificate Practice Statement (Portugal), Version 4.0, May 2005. http://ca.lip.pt/docs/cps4.0.pdf ;
k) CNRS Grid-Fr Certification Authority Certificate Policy and Certification Practice Statement (France), Version 1.0, May 2005. https://igc.services.cnrs.fr/grid-fr/grid-fr_cp-cps.pdf ;
l) UK e-Science Certification Authority Certificate Policy and Certification Practice Statement (United Kingdom), Version 1.2, May 2005. http://www.grid-support.ac.uk/ca/cps/cps-1.2.pdf ;
and indirectly from the documents which they draw from.

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

9.6 Representations and Warranties

This subcomponent can include representations and warranties of various entities that are being made pursuant to the CP or CPS. For example, a CPS that serves as a contract might contain a CA's warranty that information contained in the certificate is accurate. Alternatively, a CPS might contain a less extensive warranty to the effect that the information in the certificate is true to the best of the CA's knowledge after performing certain identity authentication procedures with due diligence. This subcomponent can also include requirements that representations and warranties appear in certain agreements, such as subscriber or relying party agreements. For instance, a CP may contain a requirement that all CAs utilize a subscriber agreement, and that a subscriber agreement must contain a warranty by the CA that information in the certificate is accurate. Participants that may make representations and warranties include CAs, RAs, subscribers, relying parties, and other participants.

9.6.1 CA representations and warranties

The ANSPGrid 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. However, the ANSPGrid CA must fulfill the obligations described below.

Certificate issuance guarantees:

a) Accept certification requests for acceptable subjects identified by requests received from RAs via secure means (see Section 4.2.2);

b) Authenticate subjects according with the procedures described in the CP/CPS document with the assistance of the recognized RAs (see Sections 3.2.2 and 3.2.3);
c) Issue certificates based on the requests after successful request validation by the recognized RAs;
d) Notify the subscriber about the certificate issuance;
e) Publish the issued certificates.

Certificate revocation guarantees:

a) Accept revocation requests from acceptable persons or the RA which approved the subscriber's request, or if the CA has itself reasonable proof that circumstances merit revocation;
b) Authenticate revocation requests before performing revocations;
c) Issue and publish a Certificate Revocation List (CRL) immediately after a revocation.

CRL issuance guarantees:

a) Issue CRLs and publish them according with the regulations described in the CP/CPS document;

Compliance guarantees:

a) Publish the policies and procedures in a CP/CPS document.
b) Follow the policies and procedures described in the CP/CPS document.

Archive obligations:

a) Keep a record of all operations performed;

Repository obligations:

a) Publish on its web server the ANSPGrid CA root certificate including URL of the PEM-formatted CA certificate;
b) Publish on its web server the CRLs as soon as issued;
c) Maintain a repository with the issued certificates.

Data privacy:

a) Collect only the personal data required to perform its function;
b) b) Protect confidential data against unauthorized access.

Private key protection and use:

a) The CA has the obligation of taking all appropriate measures to protect the integrity and confidentiality of the CA private key;
b) The CA private key can only be used to sign certificates, CRLs and information required for the proper CA operation.

The information published in the certificates, CRLs and on the CA web server respectively is accurate to the best of the ANSPGrid CA's knowledge. The 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.

9.6.2 RA representations and warranties

All accredited RAs shall perform the task of identification and authentication of the requesting parties as described in Sections 3.2.2 and 3.2.3 to the best of their knowledge. It is the RA's responsibility to request revocation of a certificate if the RA is aware that circumstances for revocation are satisfied. No other warranties are offered other than the obligations outlined below.

Compliance obligations:

a) Read and accept the policies and procedures published in the CP/CPS document;

b) Agree with the CA on a set of operation rules and guidelines that will govern the day-to-day operations of the RA, namely considerations with respect to the validation of requests (for certificates and revocations). These rules and guidelines must be compatible with the CP/CPS;

c) Establish, with the CA, the community of subjects for which certificate requests can be authenticated.

Request validation obligations for certificate issuance and revocation:

e) Follow the procedures described in the CP/CPS document and RA operation rules while validating requests;

f) Verify whether the requesters and subjects obey to requirements expressed in the CP/CPS document and to the RA operations manual;

g) Verify whether the requests obey to requirements expressed in the CP/CPS document and to the RA operations manual;

h) Authenticate the subjects according with the procedures described in the CP/CPS document and with the RA operations manual;

i) Verify that the requesters are in the possession of the private key corresponding to the certificate request; Notify the CA about the result of each request validation using a secure and reliable mechanism according with this CP/CPS document;

Archive obligations:

a) Keep a record of all request validation operations performed;

b) Allow the CA to access the logs and documents related with the performed validations;

Data privacy:

a) Collect only the personal data required to perform its function;

b) Protect confidential data against unauthorized access.

Other obligations:

a) Choosing their own staff and providing appropriate conditions for the staff to operate the RA following the rules established in this CP/CPS;

An RA can conclude, with the approval of the ANSPGrid CA, a more stringent agreement with its subscribers, but this shall never commit the ANSPGrid CA or any of its other accredited RAs.

9.6.3 Subscriber representations and warranties

By requesting a ANSPGrid CA certificate, a subscriber agrees to the following obligations (i.e. **must**):

a) Read and accept the policies and procedures published in the CP/CPS document;
b) Generate a key pair using a trustworthy method;
c) Keep the private key safe and protected. The subscribers are fully responsible for the private key confidentiality and integrity;
d) Use a strong pass-phrase with a minimum of 12 characters to protect the private key of personal certificates;
e) Use the certificate only for the purposes authorized by the CP/CPS document;
f) Request revocation and notify any relying parties in case of loss or possible private key compromise;
g) Notify the CA or RA in case of key destruction and loss;
h) Request revocation when the certificate is no longer required or when the information in the certificate becomes wrong or inaccurate;
i) Authorize the processing and conservation of their personal data submitted during the request verification process.

Any breach of stipulations of the CP/CPS document or obligations to which that the subscriber agreed to by requesting a ANSPGrid CA certificate will cause that certificate to be revoked immediately.

9.6.4 Relying party representations and warranties

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

a) it is familiar with the ANSPGrid CA' s CP and the CPS that generated the certificate before drawing any conclusion on the trust of the subscriber' s certificate;
b) it has verified the certificate's validity, revocation or suspension while performing the certificate authentication;
c) it has verified the authenticity of the ANSPGrid CA root certificate;
d) the certificate is being used for permitted purposes only; and
e) it has checked the status of the certificate to their own satisfaction prior to reliance.

When a relying party issues a proxy based on a certificate issued by the ANSPGrid CA, it should take all possible measures to limit the effects caused by a proxy outliving the validity of the certificate on which it is based directly or through one or more intervening proxies ([Tuecke04]).

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

This subcomponent can include disclaimers of express warranties that may otherwise be deemed to exist in an agreement, and disclaimers of implied warranties that may otherwise be imposed by applicable law, such as warranties of merchantability or fitness for a particular purpose. The CP or CPS may directly impose such disclaimers, or the CP or CPS may contain a requirement that disclaimers appear in associated agreements, such as subscriber or relying party agreements.

The ANSPGrid 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.

In addition, the ANSPGrid 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

This subcomponent can include limitations of liability in a CP or CPS or limitations that appear or must appear in an agreement associated with the CP or CPS, such as a subscriber or relying party agreement. These limitations may fall into one of two categories: limitations on the elements of damages recoverable and limitations on the amount of damages recoverable, also known as liability caps. Often, contracts contain clauses preventing the recovery of elements of damages such as incidental and consequential damages, and sometimes punitive damages. Frequently, contracts contain clauses that limit the possible recovery of one party or the other to an amount certain or to an amount corresponding to a benchmark, such as the amount a vendor was paid under the contract.

The ANSPGrid CA cannot be held liable 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 also cannot be held liable for damages arising from the non-issuance of a requested 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

This subcomponent includes provisions by which one party makes a second party whole for losses or damage incurred by the second party, typically arising out of the first party's conduct. They may appear in a CP, CPS, or agreement. For example, a CP may require that subscriber agreements

contain a term under which a subscriber is responsible for indemnifying a CA for losses the CA sustains arising out of a subscriber's fraudulent misrepresentations on the certificate application under which the CA issued the subscriber an inaccurate certificate. Similarly, a CPS may say that a CA uses a relying party agreement, under which relying parties are responsible for indemnifying a CA for losses the CA sustains arising out of use of a certificate without properly checking revocation information or use of a certificate for purposes beyond what the CA permits.

The ANSPGrid 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 ANSPGrid 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 ANSPGrid 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

This subcomponent can include the time period in which a CP or a CPS remains in force and the circumstances under which the document, portions of the document, or its applicability to a particular participant can be terminated. In addition or alternatively, the CP or CPS may include requirements that certain term and termination clauses appear in agreements, such as subscriber or relying party agreements.

9.10.1 Term

The term of a document or agreement, that is, when the document becomes effective and when it expires if it is not terminated earlier.

This document comes into effective after its publication on the web site of the ANSPGrid CA and the starting date announced there. Major revisions require the prior approval of the TAGPMA. No term is set for its expiration.

9.10.2 Termination

Termination provisions stating circumstances under which the document, certain portions of it, or its application to a particular participant ceases to remain in effect.

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

9.10.3 Effect of termination and survival

Any consequences of termination of the document. For example, certain provisions of an agreement may survive its termination and remain in

force. Examples include acknowledgements of intellectual property rights and confidentiality provisions. Also, termination may trigger a responsibility of parties to return confidential information to the party that disclosed it.

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

This subcomponent discusses the way in which one participant can or must communicate with another participant on a one-to-one basis in order for such communications to be legally effective. For example, an RA may wish to inform the CA that it wishes to terminate its agreement with the CA. This subcomponent is different from publication and repository functions, because unlike individual communications described in this subcomponent, publication and posting to a repository are for the purpose of communicating to a wide audience of recipients, such as all relying parties. This subcomponent may establish mechanisms for communication and indicate the contact information to be used to route such communications, such as digitally signed e-mail notices to a specified address, followed by a signed email acknowledgement of receipt.

All e-mail communications between the CA and its accredited RAs must be signed with a certified key. All e-mail communications between the CA or an RA and a subscriber must be signed with a certified key in order to have the value of a proof. All requests for any action must be signed.

9.12 Amendments

It will occasionally be necessary to amend a CP or CPS. Some of these changes will not materially reduce the assurance that a CP or its implementation provides, and will be judged by the policy administrator to have an insignificant effect on the acceptability of certificates. Such changes to a CP or CPS need not require a change in the CP OID or the CPS pointer (URL). On the other hand, some changes to a specification will materially change the acceptability of certificates for specific purposes, and these changes may require corresponding changes to the CP OID or CPS pointer qualifier (URL).

9.12.1 Procedure for amendment

The procedures by which the CP or CPS and/or other documents must, may be, or are amended.

Amendments to this CP/CPS must undergo the same procedures as for the initial approval (see Sections 1.5.4 and 9.10.1). Rephrasing provisions to improve their understandability as well as pure spelling corrections are however not considered amendments.

9.12.2 Notification mechanism and period

In the case of CP or CPS amendments, change procedures may include a notification mechanism to provide notice of proposed amendments to affected parties, such as subscribers and relying parties, a comment period, a mechanism by which comments are received, reviewed and incorporated into the document, and a mechanism by which amendments become final and effective.

The amended CP/CPS document shall be published on the ANSPGrid CA web pages at least 2 weeks before it becomes effective. The ANSPGrid CA will inform its subscribers and all relying parties it knows of by means of e-mail.

9.12.3 Circumstances under which OID must be changed

The circumstances under which amendments to the CP or CPS would require a change in CP OID or CPS pointer (URL).

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

9.13 Dispute Resolution Procedures

This subcomponent discusses procedures utilized to resolve disputes arising out of the CP, CPS, and/or agreements. Examples of such procedures include requirements that disputes be resolved in a certain forum or by alternative dispute resolution mechanisms.

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

9.14 Governing Law

This subcomponent sets forth a statement that the law of a certain jurisdiction governs the interpretation and enforcement of the subject CP or CPS or agreements.

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

9.15 Compliance with Applicable Law

This subcomponent relates to stated requirements that participants comply with applicable law, for example, laws relating to cryptographic

hardware and software that may be subject to the export control laws of a given jurisdiction. The CP or CPS could purport to impose such requirements or may require that such provisions appear in other agreements.

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

9.16 Miscellaneous Provisions

This subcomponent contains miscellaneous provisions, sometimes called "boilerplate provisions," in contracts. The clauses covered in this subcomponent may appear in a CP, CPS, or agreements.

9.16.1 Entire agreement

An entire agreement clause, which typically identifies the document or documents comprising the entire agreement between the parties and states that such agreements supersede all prior and contemporaneous written or oral understandings relating to the same subject matter.

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

9.16.2 Assignment

An assignment clause, which may act to limit the ability of a party in an agreement, assigning its rights under the agreement to another party (such as the right to receive a stream of payments in the future) or limiting the ability of a party to delegate its obligations under the agreement.

No provisions.

9.16.3 Severability

A severability clause, which sets forth the intentions of the parties in the event that a court or other tribunal determines that a clause within an agreement is, for some reason, invalid or unenforceable, and whose purpose is frequently to prevent the unenforceability of one clause from causing the whole agreement to be unenforceable.

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)

An enforcement clause, which may state that a party prevailing in any dispute arising out of an agreement is entitled to attorneys' fees as part of its recovery, or may state that a party's waiver of one breach of contract does not constitute a continuing waiver or a future waiver of other breaches of contract.

No stipulation.

9.16.5 Force Majeure

A force majeure clause, commonly used to excuse the performance of one or more parties to an agreement due to an event outside the reasonable control of the affected party or parties. Typically, the duration of the excused performance is commensurate with the duration of the delay caused by the event. The clause may also provide for the termination of the agreement under specified circumstances and conditions. Events considered to constitute a "force majeure" may include so-called "Acts of God," wars, terrorism, strikes, natural disasters, failures of suppliers or vendors to perform, or failures of the Internet or other infrastructure. Force majeure clauses should be drafted so as to be consistent with other portions of the framework and applicable service level agreements. For instance, responsibilities and capabilities for business continuity and disaster recovery may place some events within the reasonable control of the parties, such as an obligation to maintain backup electrical power in the face of power outages.

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

9.17 Other Provisions

This subcomponent is a "catchall" location where additional responsibilities and terms can be imposed on PKI participants that do not neatly fit within one of the other components or subcomponents of the framework. CP and CPS writers can place any provision within this subcomponent that is not covered by another subcomponent.

No stipulation.

10. References

[Brader97] S. Brader, Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, March 1997;
http://www.ietf.org/rfc/rfc2119.txt

[CCA06] D. Groep, editor, Profile for Traditional X.509 Public Key Certification Authorities with secured infrastructure (Classic CA minimum requirements of the IGTF) Version 4.1, December 2006;
http://www.eugridpma.org/guidelines/IGTF-AP-classic-4-1.pdf

[CCA08] D.,Groep, editor, Profile for Traditional X.509 Public Key Certification Authorities with secured infrastructure (Classic CA minimum requirements of the IGTF) Version 4.2, October 2008;
http://www.eugridpma.org/guidelines/IGTF-AP-classic-4-2.pdf

[Chokani03] S. Chokani, W. Ford, R. Sabett and S.Wu, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647, November 2003.
http://www.ietf.org/rfc/rfc3647.txt

[Chokani99] S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999.
http://www.ietf.org/rfc/rfc2527.txt

[Groep06] D. Groep and M. Helm, Grid Certificate Profile, CAOPS-WG, Global Grid Forum, (Draft version 0.15), November 2006.
https://forge.gridforum.org/sf/go/doc13741

[Housley02] R. Housley, W. Polk, W. Ford and D. Solo, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, April 2002.
http://www.ietf.org/rfc/rfc3280.txt

[Nystrom00] M. Nystrom and B. Kaliski, PKCS #10: Certification Request Syntax Specification Version 1.7., RFC 2986, November 2000.
http://www.ietf.org/rfc/rfc2986.txt

[Polk02] W. Polk, R. Housley and L. Bassham, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.
http://www.ietf.org/rfc/rfc3279.txt

[Tuecke04] S. Tuecke, V. Welch, D. Engert, L. Pearlman and M. Thompson, Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile, RFC 3820, June 2004.
http://www.ietf.org/rfc/rfc3820.txt

11. List of Changes

Version 0.5 (15 August 2008) major rewrite for review. This version is very closely based on theTAGPMA approved version of the UFF LACGrid CA´s CP/CPS (OID 1.3.6.1.4.1.24839.2.1.10.2.1.1.0)

Version 0.7 (20 January 2010) major rewrite for review. This version was written after comments from Vinod Rebello and purchase of HSM devices.

Version 0.8 (08 March 2010) major rewrite for review. This version was written after comments from James Marsteller and Jens Jensen.

Version 0.9 (14 March 2011) major review for operational review:

Version 0.95 (13 October 2011) major review for operational review. This version was written after comments from Derek Simmel

Version 0.97 (16 March 2012) minor review for operational review. This version was written after comments from James Marsteller

Version 0.98 (03 April 2012) minor review for operational review. Meaning of OID updated

Version 1.0 (18 April 2012) Final version after accreditation process completed

Version 2.0 (28 May 2018) minor rewrite expanding ANSPGrid CA scope to whole Brazil and inclusion of Angelo Santos as new contact person