SISP – SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTO

SISP Certification Practice Statement

- CPS of SISP Root Certification Authority -

Code:	PCRL001.05
Version:	5.0
Version Date:	June 30, 2019
Created by:	SISP
Approved by:	Board of Directors
Level of Confidentiality:	Public

Change Control Log

Date	Version	Created by	Description of the Amendment
January 2018	1.0	SISP	Document creation. Established.
March 2018	2.0	SISP	Document updated
April 13, 2018	3.0	SISP	Updating of the document model
July 31, 2018	4.0	SISP	Change to the PKI hierarchical structure
June 30, 2019	5.0	SISP	Web Authentication (SSL) certificate

Related Documents

Certificate Policy of SISPRoot CA

Jair Elísio Andrade Ferreira Silva

Digitally signed by Jair Elísio Andrade Ferreira Silva
DN: email=jsilva@sisp.cv, cn=Jair Elísio Andrade Ferreira Silva, serialNumber=CV-4874, givenName=Jair Elísio, sn=Andrade Ferreira Silva, title=Diretor-Geral, ou=Direção SISP, ou=Certificado para pessoa singular - Assinatura Qualificada, o=Sociedade Interbancária e Sistemas de Pagamentos S.A., l=Praia, st=Santiago, c=CV
Date: 2020.03.10 10:10:39 -01'00'

Table of Contents

1. INTRODUCTION

1.1. OBJECTIVES

This document aims at defining the practices and procedures used by the SISP Root Certification Authority (SISPRoot CA) to support its digital certification business.

1.2. TARGET AUDIENCE

This is a public document and is intended for all those who relate with the SISP Root Certification Authority, notably SISP Auditors and Partners.

1.3. DOCUMENT LAYOUT

This document complies with the layout defined and proposed by the PKIX task force of the IETF in document RFC 3647[1], as well as the “MINIMUM DRAFTING REQUIREMENTS FOR CERTIFICATION PRACTICE STATEMENTS (CPS) OF THE PKI-CV”.

Paragraph 2 provides a few relevant acronyms and definitions used in the document. The following paragraphs focus on the most important procedures and practices followed within the scope of digital certification of SISP Root Certification Authority. The thirteenth section is devoted to legal matters.

2. ACRONYMS AND DEFINITIONS

[1] Cf. RFC 3647, 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework

2.1. ACRONYMS

Acronym	
ANSI	American National Standards Institute
CA	Certification Authority (the same as for CE)
CE	Certification Entity
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DL	Decree-Law
DN	Distinguished Name
ICP-CV	Public Key Infrastructure of Cabo Verde
MAC	Message Authentication Codes
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
SHA	Secure Hash Algorithm
SISPRoot CA	SISP Root Certification Authority
SSCD	Secure Signature Creation Device
URI	Uniform Resource Identifier

2.2. DEFINITIONS

Digital signature, as provided for in DL no. 33/2007, of September 24	Advanced electronic signature modality based on an asymmetric cryptographic system made up by an algorithm or series of algorithms with which is generated an exclusive and interdependent key pair, one of which is private and another public, and which allows the titleholder to use the private key to declare authorship of the electronic document to which the signature has been added and agreement with its content, and the recipient to use the public key to check if the signature has been created with the corresponding private key and if the electronic document was changed after the signature was added.
Electronic signature, as provided for in DL no. 33/2007, of September 24	Data in electronic form which are attached to or logically associated with a data message and which serve as a method of authentication.
Advanced electronic signature as set forth in DL no. 33/2007, of September 24	An electronic signature that meets the following requirements: i) It is uniquely linked to the signatory; ii) Affixing it to the document depends solely on the willingness of the signatory; iii) It is created using means that the signatory can maintain under his sole control; iv) It relates in such a manner with the document that any subsequent change of the data is detectable.
Qualified electronic signature as provided for in DL no. 33/2007, of September 24	Digital signature or other advanced electronic signature that meets safety demands identical to those of digital signature, based on a qualified certificate and created through a security device for signature creation.
Accreditation authority, as set forth in DL no. 33/2007, of September 24	Entity responsible for accrediting and supervising the Certification Entities.
Certificate, as anticipated in DL no. 33/2007, of September 24	Digital record that links signature-verification data to the signatory and confirms the identity of that person.
Qualified certificate, as set forth in DL no. 33/2007, of September 24	Certificate that includes all the elements referred to in Article 67 of the DL 33/2007 [6]and is issued by a certification authority that complies with the requirements defined in Article 45 of DL 33/2007.
Private key, as provided for in DL no. 33/2007, of September 24	An element of the pair of asymmetric keys that is kept secret by its holder, and that is used to affix the digital signature to the electronic

	document or to decrypt electronic records previously encrypted with the corresponding Public Key.
Public Key, as set forth in DL no. 33/2007, of September 24	The key of a key pair that may be publicly disclosed and that is used to verify digital signatures created by the holder of the asymmetric keys or to encrypt messages to be sent to the holder of the said key pair.
Accreditation, as set forth in DL no. 33/2007, of September 24	The act whereby upon request an entity that performs the role of certification entity is acknowledged to fulfil the requirements defined in the DL no. 33/2007, of September 24, for the purposes anticipated therein.
Signature-creation data, as provided for in DL no. 33/2007, of September 24	Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.
Signature-verification data, as set forth in DL no. 33/2007, of September 24	A set of data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.
Signature-creation device, as anticipated in DL no. 33/2007, of September 24	Configured software or hardware used to implement the signature-creation data.
Secure signature-creation device, as set forth in DL no. 33/2007, of September 24	A signature-creation device that ensures, by appropriate technical and procedural means, that: i) Data required for the creation of a signature, used for signature generation, can occur only once and their secrecy is fully guaranteed; ii) Data required for the creation of a signature, used for signature generation, cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology; iii) Data required for the creation of a signature, used for signature generation, can be reliably protected by the holder against the illegitimate use by third-parties; iv) Data to be signed cannot be altered and may be submitted to the holder prior to the signature process.
Electronic document, as laid down in DL no. 33/2007, dated September 24	Document prepared by electronic data processing.
Electronicaddress, as laid down in DL no. 33/2007, dated September 24	Identification of appropriate computer equipment to receive and store electronic documents.

3. GENERAL CONTEXT

3.1. OBJECTIVE

The present document is a Certification Practice Statement (CPS) and aims to define a set of practices required to issue and validate certificates and safeguard the reliability of such certificates. It is not meant to list legal rules or obligations but rather inform the parties involved. Therefore, this document is intended to be clear, straightforward, and understood by a larger audience, including those who do not hold any technical or legal knowledge.

This document describes the overall practices observed by SISPRoot Certification Authority (SISPRoot CA) in certificate issuance and management, explains what a certificate means and also specifies the procedures that must be followed by Relying Parties and any other relevant person in order to rely on the Certificates issued by SISPRoot CA.

This document may be subject to regular updating.

Any certificate issued by SISPRoot CA shall include a reference to the present CPS, Document Code no. PCRL001.03, to enable the Relying Parties and other relevant persons to obtain information on the certificate and the issuing entity.

3.2. FRAMEWORK

The practices associated with certificate creation, signature and issuance, as well as certificate revocation, whose validity period has expired or otherwise upon request of the titleholder, carried out by a CE are key issues to ensure the reliability of a Public Key Infrastructure.

This CPS applies to SISPRoot CA, in accordance with the structure in use under ICP-CV, based on the following standards:

a) RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practice Framework;
b) RFC 5280 – Internet X.509 Public Key Infrastructure – Certificate and CRL Profile.

and further specifies the way to implement the procedures and controls used at SISPRoot CA and how SISPRoot CA should attain the requirements laid down in ICP-CV standards.

3.3. DOCUMENT IDENTIFICATION

This document is formally referred to as a CPS and is represented on a certificate through a single number named as “Object Identifier” (OID). The OID associated with this CPS is 2.16.132.1.1.2.3.

This document shall be identified through data contained in the following table:

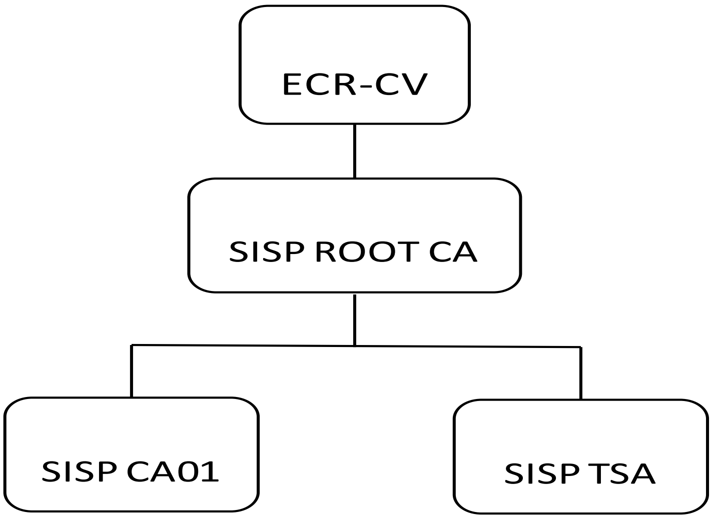
3.4. PARTICIPANTS IN THE PUBLIC KEY INFRASTRUCTURE

As the Managing Body of the PKI, SISP complies with all the provisions set forth in the applicable laws and regulations, and makes full use of the powers and responsibilities described therein. Accordingly, SISP is responsible for providing services and ensuring the procedures required to guarantee the functionalities below:

1. Generating the key pairs associated with each one of the Certification Authorities;
2. Receiving and validating the requests for certificate issuance made by Subordinate Certification Authorities (CA), as well as other subscribers;
3. Issuing certificates related with requests that comply with the format required by SISP Certification Authorities;
4. Receiving and validating requests for certificate suspension and revocation;
5. Publishing the certificates (when, where, and if deemed appropriate) and disclosing information on their status;
6. Ensuring continuous availability of public information to all its users.

SISP PKI comprises the following CE:

- Root Certification Entity of Cabo Verde (RCE-CV)
- SISP Root Certification Authority (SISPRoot CA)
- SISP Certification Authority (SISPCA01)
- SISP Time-Stamping Certification Authority (SISP TSA)



3.4.1. SISP ROOT CERTIFICATION AUTHORITY (SISPROOT CA)

SISPRoot CA rests upon the hierarchy of trust of the ICP-CV, thus representing a second level certification entity signed by the Root Certification Authority of Cabo Verde (ECR-CV). It is empowered only to issue certificates intended to sign the certificates of CAs at the hierarchal level immediately prior in the certification chain, in conformity with the list released in http://pki.sisp.cv.

3.4.2. SISPCA01CERTIFICATION AUTHORITY (SISP CA01)

The Subordinate Certification Entity SISP CA01 stands out as an Issuing Certification Authority accredited by ARME – National Agency of Communications, in light of the Cabo-Verdean legislation. It is legally authorized to issue any type of certificate, including qualified certificates, those of a higher degree of security, as anticipated by law.

It is included in the hierarchy of trust of the Public Key Infrastructure of Cabo Verde.

SISPCA01 may issue certificates of:

- Qualified signature for private individuals;
- Qualified signature in representation of a legal entity;
- Qualified signature of professional associations;
- Authentication for private individuals and legal entities;
- Electronic stamp:
- Web Authentication (SSL)

as well as OCSP Online Validation.

3.4.3. SISP TSA CERTIFICATION ENTITY FOR CHRONOLOGICAL VALIDATION OR TIMESTAMP

SISP TSA – Certification Entity for Chronological Validation issues digital certificates within the hierarchy of trust of SISP and may equally issue timestamps for other purposes whenever proof of legal time is deemed necessary.

The legal time used in chronological validation is obtained by using equipment including atomic clock covering 12 satellites and network imprecision level ranging between 1-10 milliseconds and GPS lower than 1 microsecond with reference to UTC.

3.4.4. ENTITIES OR REGISTRATION UNITS

Registration Units or Entities refer to the entities to which the CAs delegate the provision of services in the field of identification and registration of certificate users, as well as management of requests for certificate renewal and revocation. SISP may act as a Registration Unit and/or establish agreements with third-parties in order to play this role. The list of Registration Entities comprised in the PKI of SISP is available on http://pki.sisp.cv.

3.4.5. CERTIFICATE HOLDERS

a) For the purposes of this document and whereas it concerns the CPS of SISPRoot CA, certificate holders shall be the legal entities under human responsibility who accept the certificate and are responsible for its proper use, as well as for the protection and safeguarding of its private key. Preferably, the legal representative of the legal entity or one of his legal representatives will be held accountable for the certificate.

b) The holder of SISPRoot CA certificate is SISP.

c) The holders of CAs that have a certificate signed by SISPROOT CA are the entities responsible for them, or a legal representative appointed in this regard.

3.4.6. SPONSOR

Nothing to remark.

3.4.7. RELYING PARTIES

a) Relying parties or recipients are private individuals, entities or equipment that rely on the validity of the mechanisms and procedures used throughout the process of associating the holder name with its public key, i.e. they trust that the certificate corresponds, in reality, to whomever it claims to belong to.

b) In this CPS, a relying party is the one that relies on the contents, validity, and applicability of the certificate issued in the hierarchy of trust of the ICP-CV, and may or may not hold certificates of the ICP-CV community.

3.4.8. OTHER PARTICIPANTS

3.4.8.1. ACCREDITATION AUTHORITY

The Accreditation Authority takes on the role of a body that provides compliance audit/inspection services in order to assess whether the processes used by the CAs in the certification activities meet the minimum requirements set out in the laws and regulations in force.

Therefore, the following are some of its most important duties:

a) Accredit the certification entities;
b) Control and monitor the certification entities;
c) Charge fees for accreditation services;
d) Ensure that the certification entities are held liable for any damage caused to any entity, either private individuals or legal entities, who reasonably relies on the certificates;
e) Audit the certification entities;
f) Ensure that the security devices supporting the creation of electronic signatures comply with the conditions anticipated in article 28 of the Decree-Law no. 33/2007, of September 24;
g) Promote mutual recognition agreements with accreditation authorities of foreign countries, subject to prior authorization granted by the governmental department in charge of communications;
h) Maintain information on the internet regarding the list of certification entities and the suspension or revocation of digital certificates, as well as on other relevant aspects associated with the certification process;
i) Define the technical requirements that determine the adequacy of any activity developed by the certification entities;
j) Assess the activities undertaken by authorized certification entities in light of the technical requirements defined under the terms of the preceding paragraph;
k) Ensure adequate operation and effective service provision of the certification entities, in conformity with the related legal and regulatory provisions;
l) Any other business as may be determined by law.

3.4.8.2. SECURITY AUDITOR

The security auditor is independent from the sphere of influence of the Certification Authority and is required by the Accreditation Authority. He is endowed with the task of auditing the infrastructure of the Certification Authority in what respects equipment, human resources, processes, policies and rules, being bound to submit an annual report to the Accreditation Authority. A list of Security Auditors of Certification Authorities accredited by the Accreditation Authority can be found at http://www.pki.ecrcv.cv/.

3.5. CERTIFICATE USE

3.5.1. CERTIFICATES ISSUED

The certificates issued by SISPRoot CA are exclusively meant for the signature of digital certificates of the Certification Entities of the next higher level, the List of Revoked Certificates (CRL), and SISP TSA, with the objective of guaranteeing the following services:

- Access control
- Confidentiality
- Integrity
- Authentication, and
- Non-repudiation.

These services are provided with resort to the use of public key cryptography, by using it in the trust structure made available by the PKI of SISP. Furthermore, the identification, authentication, integrity, and non-repudiation services are offered by using digital signatures. Secrecy or confidentiality is guaranteed through recourse to encipherment algorithms, along with mechanisms to establish and distribute keys managed by certified cryptographic equipment.

3.5.2. PROPER USE

The requirements and rules defined in this document apply to all certificates issued by SISPRoot CA.

The certificates issued by SISP Root SA are used by the relying parties to verify the chain of trust of a certificate issued under ICP-CV, and also to ensure the authenticity and identity of the issuer of a digital signature generated by the private key corresponding to the public key contained in a certificate signed by the PKI of SISP.

The certificates issued by SISPRoot CA must be used in accordance with the capacity and purpose established in this document, the related Certificate Policies, and the legislation in force.

3.5.3. UNAUTHORIZED USE

The certificates may be used in other contexts only to the extent of what is permitted by the rules of ICP-CV and the applicable legislation.

The certificates issued by the PKI of SISP cannot be used in any other capacity out of the scope of the previously described use.

The certification services offered by the PKI of SISP have not been designed. On the other hand, no authorization has been granted for their use in high risk activities or others that require an activity exempt from failures, such as hospital and nuclear operations, air traffic control, railway traffic control or any other activity where a failure can lead to death, personal injury or serious damages to the environment.

3.6. POLICY ADMINISTRATION

The Security Working Group is responsible for administering this CPS and may be contacted through the address and telephone numbers listed below:

Name:	Security Working Group
Address:	SISP, SA Conjunto Habitacional Novo Horizonte Rua de Funchal Achada Santo António – Praia Cabo Verde
e-mail:	pki@sisp.cv
Site:	www.sisp.cv
Telephone:	+238 260 6310 / +238 262 6317

The Security Working Group provides for the suitability and application of this CPS (and/or respective CPs) at internal level, and subsequently submits it to the Management Working Group for approval purposes.

Validation of this CPS (and/or respective CPs) and subsequent amendments shall be carried out by the Security Working Group. Any corrections or amendments should be released as new versions of this CPS (and/or respective CPs), thus replacing any previously adopted CPS (and/or respective CPs).

The Security Working Group shall also determine the time when amendments to the CPS (and/or respective CPs) will lead to alterations in object identifiers (OID) of the CPS (and/or respective CPs).

Following completion of the validation phase, the CPS (and/or respective CPs) is submitted to the Management Working Group, which is the entity responsible for approving and authorizing any corrections or amendments to this type of document.

All certification policies, rules, and practices implemented within the scope of this CPS may be found in the repository available at http://pki.sisp.cv.

4. LEGAL PROVISIONS

4.1. DUTIES AND OBLIGATIONS

4.1.1. DUTIES AND OBLIGATIONS OF THE CERTIFICATION ENTITIES

The PKI of SISP is bound to:

- Carry out its operations in accordance with this Policy;
- Clearly state all its Certification Practices in the appropriate document;
- Protect its private keys;
- Issue certificates in accordance with Standard X.509;
- Issue certificates that are in conformity with the information known at the time they are issued and free from data input errors;
- Ensure confidentiality in generating signature-creation-data and its secure delivery to the holder;
- Use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the certification processes;
- Use trustworthy systems to store certificates under conditions necessary to establish their authenticity and prevent unauthorized persons to modify those data;
- Archive, unaltered, the certificates issued;
- Guarantee that the date and time on which a given certificate was issued or cancelled or suspended can be precisely determined;
- Employ personnel who possess the expert knowledge, experience, and qualifications necessary for the certification services provided;
- Revoke certificates under the terms set forth in section 7.7 of this document and publish the revoked certificates in the CRL of the SISPRoot CA repository with the frequency stipulated in section 7.7.10;
- Publish its CPS and the applicable Certificate Policies in its repository, so ensuring access both to the current and previous versions of those documents;
- Promptly notify, by e-mail, the certificate holders in case the CA revokes or suspends their certificates, together with the reasons for such action;
- Cooperate with the audits led by the Accreditation Authority in order to validate their own keys;
- Operate in accordance with the applicable legislation;
- Safeguard, where they exist, the keys under custody;
- Guarantee CRL's availability in light of the provisions of section 7.7.10;
- In the event of ceasing its activity, inform all holders of certificates issued, as well as the Accreditation Authority, at least three months in advance;
- Comply with all specifications included in the standard on Personal Data Protection;
- Store and keep all records and documents related with an acknowledged certificate and the Certificate Practice Statement in force at all times and for a period of twenty years as from the moment of issuance; and
- Make available the certificates of SISPRoot CA.

4.1.2. DUTIES AND OBLIGATIONS OF REGISTRATION ENTITIES

Nothing to report.

4.1.3. DUTIES AND OBLIGATIONS OF CERTIFICATE HOLDERS

The duties and obligations of holders of issued certificates include:

- Restrict and tailor the use of certificates in accordance with the use foreseen in the Certificate Policies;
- Take every caution and measures deemed necessary to ensure possession of their private key;
- Apply immediately for the revocation of a certificate where there is knowledge or suspicion that the private key can be computed from the public key contained in the certificate, as per section 7.7.5.;
- Abstain from using a digital certificate that has lost its efficiency either due to revocation or suspension, or because its validity period expired;
- Submit to the Certification (or Registration) Entity full, accurate information as regards data requested by the former to conclude the registration process. Any changes in such information should be reported at once to the CA;
- Abstain from monitoring, manipulating or executing “reverse engineering” techniques on the infrastructure (software and hardware) of the certification services without previous written authorization of the PKI of SISP.

4.1.4. DUTIES AND OBLIGATIONS OF RELYING PARTIES

The parties who rely on the certificates issued by the PKI of SISP are bound to:

- Restrict the reliability of the certificates to the uses permitted under the corresponding Certificate Policy;
- Check the status of the certificates before a transaction based on them takes place;
- Assume the responsibility for the accurate verification of the digital signatures;
- Assume the responsibility for proof of validity, revocation, or suspension of the certificates relied upon;
- Be fully aware of the guarantees and responsibilities applicable in certificate acceptance and use, and agree to be subject to them.

4.1.5. DUTIES AND OBLIGATIONS OF OTHER PARTICIPANTS

No stipulation.

4.2. PUBLICATION AND STORAGE RESPONSIBILITIES

SISP reserves the right to publish information regarding the digital certificates issued in a repository available online, as well as publish information on the certificate status in third-party repositories.

SISP maintains a document repository online through which information on its practices, procedures, and contents of certain policies, including the CPS, are released. All parties associated with the issuance, use or management of SISP certificates are herein notified that SISP can publish, upon request, in its publicly accessible repository, information on the status of the digital certificate.

SISP abstains from publicly releasing confidential information, namely those related with security controls, procedures, internal security policies, among other.

4.2.1. REPOSITORIES

SISP, S.A. is responsible for the repository functions of SISPRoot CA, by publishing, *inter alia*, information related with the practices adopted and the status of the certificates issued (CRL).

Access to the information made available by the repository is facilitated through the HTTPS and HTTP protocol, and the following security mechanisms have been implemented:

- Both the CRL and the CPS can only be modified through duly defined processes and procedures;
- The technological platform for the repository is duly protected with state-of-the-art techniques of physical and logical security;
- The human resources who manage and administer the said platform hold the educational skills and training deemed adequate for the service at stake.

4.2.2. PUBLICATION OF INFORMATION ON CERTIFICATION

SISP maintains a repository on a Web environment that enables the Relying Parties to carry out online research regarding revocation and other information on the status of the certificates, 24 (twenty-four) hours a day, 7 (seven) days a week.

SISP always releases the following public information at URL http://pki.sisp.cv:

- Its own certificate;
- An updated electronic copy of this CPS;
- An updated electronic copy of the CP;
- A list of the Certification Entities linked to SISPRoot CA;
- A list of Revoked Certificates of Certification Entities (CRL);
- A list of the Registration Entities and addresses of the respective technical facilities;
- Application form for certificate issuance;
- Application form for certificate revocation.

In addition, all previous versions of the CPS of SISPRoot CA will be kept and made available upon request (to be reasoned). However, they will remain outside the free public access repository.

4.2.3. TIME OR FREQUENCY OF PUBLICATION

SISP guarantees that all updates to the present CPS and respective policies will be published whenever an alteration is deemed necessary.

A new CRL of SISPRoot CA will be published whenever a revocation takes place. Even if no revocation is made, SISPRoot CA shall make available a new CRL every 90 (ninety) days.

In what concerns the certificates of issuing CAs and the certificates they issue, publication of the policies and standards will comply with the provisions contained in the respective CPS.

4.2.4. ACCESS CONTROL

The information published by SISP will be available on the internet, remaining subject to access control mechanisms (read-only access). SISP has implemented logical and physical security measures intended to prevent unauthorized people to add, erase or modify records included in the repository.

4.3. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

A regular audit on compliance with this CPS and other rules, procedures, and processes will be undertaken by the members of the Audit Working Group of the PKI of SISP.

Other than compliance audits, SISP will carry out additional surveillance and investigations to ensure conformity of the Certification Entities with the national legislation, as well as with the applicable international standards. The execution of these internal audits, surveillance, and investigations may be delegated to an external audit entity.

In the case of the Certification Entities embraced by the PKI of SISP but operated by other entities, SISP may, whenever deemed appropriate, perform internal audits to the former. These entities are also required to submit an annual audit report, or a compliance statement, to SISP, made by an independent recognized security audit firm.

4.3.1. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

SISPRoot CA complies with the requirements defined by ICP-CV.

The audit is executed by auditors duly certified by ARME.

4.3.2. FREQUENCY OR REASON FOR THE AUDIT

SISP certification practices are subject to regular audits at minimum intervals determined by law, *id est*, at least once a year, with the issuance of a report as at March 31 of the financial year at stake. This audit shall be carried out by an Auditor certified by the ARME, based on the existing standards. The results are henceforth reported to the accreditation authority, which is entitled to publish the outcome of the entire process.

In order to fulfil these duties, SISP keeps records of all operations related with the life-cycle of certificates and all correspondence exchanged with recognized registration/certification entities. Likewise, SISP requires these entities to keep records of the subscription applications received and processed, in which it has been involved.

Such records must be maintained in a data repository created for that purpose and confirmed by analyzing the mail records (e-mail or other) exchanged with the certification entity.

To verify compliance with these provisions, SISP will conduct periodical audits to the registration/certification entities as a means to determine the adequacy of the operating procedures and levels of technological security to the Certificate Policies in place. Non-compliance with the contractual conditions and terms may lead to the suspension and/or revocation of the issued certificate(s).

5. IDENTIFICATION AND AUTHENTICATION

5.1. NAMING

This section describes the procedures used to authenticate the certified entities prior to certificate issuance, as well as name related disputes.

5.1.1. TYPES OF NAMES

Naming is based on the methodology determined by ICP-CV. SISP guarantees the issuance of certificates including a X.509 Distinguished Name (DN), defined as RFC5280, and issues certificates for applicants that submit documents containing a verifiable name.

SISP shall ensure, within its reliable infrastructure, the absence of certificates which, even containing the same DN, may identify separate entities.

5.1.2. NEED FOR NAMES TO BE MEANINGFUL

SISP will ensure that the names used in the certificates it issues identify, in a significant way, its users. In other words, SISP will ensure that the DN used is appropriate for the user in question, and that the component “Common name of DN” represents the user in a readily comprehensible manner. Nevertheless, SISP may issue pseudonymous certificates provided that they are identified as such.

5.1.3. RULES FOR INTERPRETING VARIOUS NAME FORMS

The rules used by SISP to interpret name format conform with those stipulated in the RFC 5280, thus ensuring that all *DirectoryString*features of the *issuer* and *subject* fields of the certificate are codified in a *UTF8String*, with the exception of the *country* and *serial number*features, which are codified in a *PrintableString*.

5.1.4. UNIQUENESS OF NAMES

SISP will control the existing subject names in such a way as to ensure that a certificate includes an unambiguous and unique DN related to a sole entity.

5.1.5. NAME CLAIM DISPUTE RESOLUTION PROCEDURE

SISP will be responsible for granting and approving the DNs. It will also be responsible for settling any disputes that are likely to arise in this field.

5.1.6. RECOGNITION, AUTHENTICATION, AND ROLES OF TRADEMARKS

The subject names issued by SISP will conform, to the maximum possible extent, with registered trademark holders. SISP will not deliberately permit the use of registered names whose ownership may not be proved by the applicant. However, SISP may reject the issuance of certificates with names of registered trademarks if it considers another identification as more suitable.

5.1.7. METHOD TO PROVE POSSESSION OF PRIVATE KEY

In the cases where SISP is not responsible for generating the cryptographic keys to be allocated to the user, it will ensure that the user possess a private key corresponding to the public key included in the certificate application, prior to issuing it.

The proof method will necessarily be even more complex and precise depending on the importance of the certificate type requested. This method is laid down in the Certificate Policy of the certificate in question.

5.2. INITIAL IDENTITY VALIDATION

SISP is responsible for authenticating the identity of the entities that apply for a certificate.

SISP should also store all documents used to verify the identity of the certification entity, ensuring the verification of the identity of its legal representatives by legally recognized means, and guaranteeing, where those representatives are not present at the certificate issuance ceremony, that the representative appointed by the entity holds enough powers for the said issuance ceremony.

The process of authenticating the identity of a legal entity must mandatorily guarantee that the legal entity for whom the certificate is to be issued is truly whom it claims to be, and that the creation of signature through a signature-creation-device requires the intervention of natural persons who, statutorily, represent such legal entity.

The document supporting the issuance of a CE certificate includes, among others, the following items:

a) Documents for the purposes of identifying the CE and its legal name;
b) Tax identification number, headquarters, corporate object, names of the members of the corporate bodies and other persons who have the power to bind the CE;
c) Full name, identification card number or any other document that enables the unique identification of the natural persons who, legally or statutorily, represent the CE;
d) Address and other contact details;

e) Indication that the certificate is issued for the entity, as a CE under the supervision of the CRE-CV, in the hierarchy structure of ICP-CV, in conformity with the present CPS;
f) Distinguished name (DN) to be allocated to the CE certificate;
g) Information, if required, related with the identification and powers of the representatives appointed by the CE to participate in the certificate issuance ceremony;
h) Additional information concerning the certificate request to be submitted during the CE's certificate issuance ceremony.

5.2.1. AGREEMENT WITH THE SUBSCRIBER

SISP shall keep record of the agreement signed with the subscriber, including:

1. Agreement with the subscriber on the terms and conditions. In case the certificate subscriber is different from the subject, the latter will also be informed on the terms and conditions;
2. Consent concerning the keeping of records by SISP with the information used in the registration process and information on subsequent events related with the agreement and its purpose;
3. Permission to pass on this information to third-parties under given conditions;
4. Permission to pass on information on the status of the issued certificates, under the agreement, to unspecified third-parties.

5.2.2. CERTIFICATE APPLICATION

SISP shall:

1. Require that the entity applying for a certificate prepare and submit appropriate data as specified in this CPS;
2. Whenever necessary, require the final petitioner to submit its public key for certification in a digitally signed message, by using the private key corresponding to the public key included in the application, in order to:
   i. Enable error detection in the certification process;
   ii. Prove possession of the private key related with the public key to be certified.
3. Use the public key contained in the CSR, hereinafter called Certificate Signing Request, to verify the signature of the petitioner in the Certificate Application submitted;
4. Verify the authenticity of the request by the RE in accordance with this CPS;
5. Verify the signature of the RE included in the Certificate Signing Request;
6. Verify the Certificate Signing Request to check if it contains any errors or omissions in conformity with this CPS.
7. Verify the uniqueness of the petitioner's DN within its infrastructure;
8. Accept the Certificate Signing Request submitted by the petitioner whose identity has been validated;
9. Reject the Certificate Signing Request when repeated public keys have been detected.

5.3. FACE-TO-FACE AUTHENTICATION OF SEPARATE ENTITIES

Face-to-face authentication of the authorized representative of the organizations applying to a certificate shall be based in at least two types of identification issued by the government (identification document with a photo, such as a passport or an identification card). The person's capacity to act on behalf of an applicant organization shall also be authenticated upon the presentation of paper documents stating that fact.

The above described information has to be validated by SISP when returning the fully completed forms. SISP or the Registration Entity it designates will be responsible for personally verifying the identity of the representatives.

5.4. IDENTIFICATION AND AUTHENTICATION FOR KEY RENEWAL REQUESTS

5.4.1. IDENTIFICATION AND AUTHENTICATION FOR KEY ROUTINE RENEWAL

A number of PKI implementations enable the issuance, automatic or facilitated, of updated certificates for a subscriber, before the end of the validity period of the existing certificate. This action is acknowledged as a routine renewal and is made possible due to the fact that a relationship of trust already exists with the subscriber.

However, depending on the certificate at stake, itmay become necessary to guarantee that the original conditions required to obtain the certificate are set to remain, that is to say:

- The individual/organization still exists and has authorized the issuance of the certificate;
- The individual/organization continues to comply with the subscription requirements;
- The individual/organization possesses the private key corresponding to the new public key dispatched for certification;
- SISP accepts the continuity of the individual/organization within its hierarchy.

Renewal may only be repeated a maximum of 3 times without the need to repeat a new registration of the user. Nevertheless, the Certificate Policy of the Certificate to be renewed may expressly specify other renewal conditions, even those opposing this one.

5.4.2. RENEWAL AFTER REVOCATION

If a certificate is revoked, the individual/organization will be subject to the entire registration process in order to obtain a new certificate.

5.5. REVOCATION REQUEST

The revocation request must obey to the conditions described in detail in section 6.7.

6. OPERATIONAL REQUISITES FOR THE LIFECYCLES OF THE CERTIFICATES

6.1. CERTIFICATE REQUEST

The certificate request must be made by completing the appropriate form available in the repository of the PKI of SISP in http://pki.sisp.cv.

6.2. CERTIFICATE ISSUANCE

6.2.1. PROCEDURES FOR CERTIFICATE ISSUANCE

Issuance of the certificate is made in a ceremony that takes place at the high security zone of the PKI of SISP, with the presence of:

- The legal representatives of the subordinate applicant entity or representatives appointed for this ceremony;
- At least 3 members of the Working Groups;
- An Auditor of ARME in charge of generating the key pair of SISPRoot CA, and SISP Auditor, in case of Subordinate CAs;
- Any observers simultaneously accepted by the members of the Working Group and the representatives of the subordinate applicant entity.

The certificate issuance ceremony comprises the following steps:

- Identification and authentication of all individuals present in the ceremony to ensure that the representant(s) and the members of the Working Group hold the powers required for the acts to be performed;
- The members of the Working Group start processing the certificate and issue the Certificate Signature Request (CSR) (corresponding to PKCS#10 generated in the HSM), which is saved and filed in a technological support (non-rewritable);
- The certificate issued and signed by the higher-ranking Certification Entityis imported into the corresponding CE;
- The first CRL is then generated;
- The issuance ceremony is completed with the execution of the last processing procedure of the certificate by the members of the Working Group.

The certificate comes into force at the moment it is issued.

6.2.2. TITLEHOLDER NOTIFICATION AS TO THE ISSUANCE OF A CERTIFICATE

The issuance of the certificate occurs face-to-face, under the terms of the previous section.

6.3. CERTIFICATE ACCEPTANCE

6.3.1. PROCEDURE FOR CERTIFICATE ACCEPTANCE

The certificate is deemed to have been accepted after the certificate issuance and acceptance form is signed by the representative(s) of the subordinate entity, in accordance with the issuance ceremony (as per section 6.2.1.).

Emphasis is put on the fact that, before the certificate is made available to the titleholders, and consequently all functionalities for use of the private key and certificate are also made available, it should be guaranteed that:

- The titleholder is duly aware of his rights and responsibilities;
- The titleholder becomes familiar with the certificate functionalities and contents;
- The certificate and its usage conditions are formally accepted and, accordingly, the Certificate Delivery Form is signed.

6.3.2. PUBLICATION OF THE CERTIFICATE

SISPRoot CA does not publish the issued certificates. They are fully made available to the representatives under the terms set forth in paragraph 6.3.1.

6.3.3. NOTIFICATION OF CERTIFICATE ISSUANCE TO OTHER ENTITIES

No stipulation.

6.3.4. USAGE OF PRIVATE KEY AND CERTIFICATE BY SUBSCRIBER

Certificate titleholders (representatives) shall use their private keys only for the purpose for which these are meant (as set forth in the certificate “key usage” field) and always for legal purposes.

Their use is only allowed:

- To anyone assigned in the “Subject” field of the certificate;
- In conformity with the conditions defined under section 3.5.;
- As long as the certificate is valid and is not in the CRL of SISPRoot CA.

Additionally:

- The certificate of the subordinate CE may be used to sign certificates and respective CRL, as well as any certificates deemed necessary for the operation and services of a subordinate CE;
- The online certificate validation must be used in OCSP servers.

6.3.5. KEY AND CERTIFICATE USAGE BY RELYING PARTIES

In using the certificate and the public key, Relying Parties may only rely on the certificates taking into account what is laid down in this CPS and the respective Certificate Policy. To that end, relying parties should, *inter alia*, ensure compliance with the following conditions:

- Hold knowledge of, and understand the usage and functionalities provided by public key cryptography and certificates;
- Be responsible for their correct use;
- Read and understand the terms and conditions described in the Certification Policies and Practices;
- Responsibly verify the certificates (validation of chains of trust) and CRL, with particular attention to the extensions marked as critical and to key purpose;
- Trust the certificates, using them while they are valid.

6.4. CERTIFICATE RENEWAL

This practice is not supported by the PKI of SISP.

Certificate renewal is a process in which previous data of the certificate is used for the issuance of a new certificate, without modifying the keys or any other information, except for the validity period of the certificate.

6.4.1. CIRCUMSTANCE FOR CERTIFICATE RENEWAL

No stipulation.

6.4.2. WHO MAY REQUEST CERTIFICATE RENEWAL

No stipulation.

6.4.3. PROCESSING CERTIFICATE RENEWAL REQUESTS

No stipulation.

6.4.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

No stipulation.

6.4.5. PROCEDURES FOR CERTIFICATE ACCEPTANCE

No stipulation.

6.4.6. PUBLICATION OF CERTIFICATE FOLLOWING RENEWAL

No stipulation.

6.4.7. NOTIFICATION OF CERTIFICATE ISSUANCE TO OTHER ENTITIES

No stipulation.

6.5. CERTIFICATE RENEWAL WITH THE CREATION OF A NEW KEY PAIR

Certificate keys renewal (certificate re-key) is a process where a titleholder generates a new key pair and submits a request for the issuance of a new certificate which certifies the new public key. This process, within the scope of the PKI of SISP, is named as certificate renewal with the creation of a new key pair.

Certificate renewal with the creation of a new key pair is accomplished in accordance with the provisions of section 6.2.

6.5.1. CIRCUMSTANCES FOR CERTIFICATE RENEWAL WITH THE CREATION OF A NEW KEY PAIR

Certificate renewal with the creation of a new key pair will be acceptable whenever the following circumstances occur:

- The certificate is about to expire;
- The key pair has reached the anticipated usage period;
- The information that originated the certificate has changed.

6.5.2. WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

As set out in section 6.1.

6.5.3. PROCESSING CERTIFICATE RENEWAL REQUEST WITH THE CREATION OF A NEW KEY PAIR

As set out in section 6.2.

6.5.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

As set out in section 6.2.2.

6.5.5. CONDUCT CONSTITUTING ACCEPTANCE OF THE CERTIFICATE RENEWED WITH THE CREATION OF A NEW KEY PAIR

As set out in section 6.3.1.

6.5.6. PUBLICATION OF THE CERTIFICATE RENEWED WITH THE CREATION OF A NEW KEY PAIR

As set out in section 6.3.2.

6.5.7. NOTIFICATION OF RENEWED CERTIFICATE ISSUANCE TO OTHER ENTITIES

As set out in section 6.3.3.

6.6. CERTIFICATE MODIFICATION

This practice is not supported by the PKI of SISP.

Certificate modification is a process in which a certificate is issued to a titleholder and the respective keys are maintained. Changes occur only in the information contained in the certificate.

6.6.1. CIRCUMSTANCES FOR CERTIFICATE MODIFICATION

No stipulation.

6.6.2. WHO MAY REQUEST CERTIFICATE MODIFICATION

No stipulation.

6.6.3. PROCESSING CERTIFICATE MODIFICATION REQUESTS

No stipulation.

6.6.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

No stipulation.

6.6.5. CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

No stipulation.

6.6.6. PUBLICATION OF THE MODIFIED CERTIFICATE

No stipulation.

6.6.7. NOTIFICATION OF THE MODIFIED CERTIFICATE TO OTHER ENTITIES

No stipulation.

6.7. CERTIFICATE SUSPENSION AND REVOCATION

6.7.1. CIRCUMSTANCES FOR SUSPENSION

Suspensions are not executed by SISPRoot CA.

6.7.2. WHO CAN REQUEST SUSPENSION

No stipulation.

6.7.3. PROCEDURE FOR SUSPENSION REQUEST

No stipulation.

6.7.4. LIMITS ON THE SUSPENSION PERIOD

No stipulation.

6.7.5. REASONS FOR REVOCATION

Certificate revocation takes place when the certificate becomes invalid before the end of its validity period, thus losing its operability.

After revocation, certificates cease to be valid.

A certificate may be revoked if one or more of the following circumstances occur:

- Private key is compromised (SISPRoot CA or subordinate CE);
- Private key has been lost;
- Information in the certificate is inaccurate;
- Loss, destruction, or damage of the device supporting the private key (for example, cryptographic support/token);
- Password of access to the private key is compromised (e.g. PIN number);
- Certificate has been misused;
- Risk of compromised key (for example, due to weakness in the algorithm or key size);
- By court order or, provided it is reasonably substantiated, by the entities comprised in the PKI-CV, namely:
    - Managing Board of ICP-CV
    - Accreditation Authority
    - ECR-CV (Root Certification Entity of Cabo Verde).
- Termination of service.

The certificate is revoked within a maximum period of 24 hours.

6.7.6. WHO CAN REQUEST REVOCATION

The following entities are entitled to request a certificate revocation if one or more of the circumstances described in 6.7.5. occur that suggest reasonable cause to revoke the certificate:

- The legal representatives of the Subordinate Certification Entity;
- SISP, S.A.;
- A relying party, whenever it can demonstrate that the certificate was used for purposes other than those for which they were intended.

SISPRoot CA should store all information and documents used to verify the identity and authenticity of the entity requesting the revocation, guarantee verification of the identity of its legal representatives by legally recognized means, and not accept powers of representation for any revocation request of a certificate of SISPRoot CA or Subordinate Certification Entities.

6.7.7. PROCEDURE FOR REVOCATION REQUEST

All revocation requests must be addressed to SISP, S.A. in writing or by digitally signed e-mail, through a specific revocation request form, provided that the following is observed:

- Identification and authentication of the entity that made the revocation request;
- Record and archive the revocation request form;
- Analysis of the revocation request by the Authentication Working Group of the PKI of SISP, which shall propose, to the Management Working Group, the approval or rejection of the revocation request;
- In consideration of the opinion issued by the Authentication Working Group of the PKI of SISP, the Management Working Group shall decide on the approval or rejection of the certificate revocation request;
- Whenever a certificate is revoked, the revocation is published in the respective CRL.

In any case, a detailed description of the entire decision-making process is archived, including the following:

- Date of the revocation request;
- Name of the certificate titleholder;
- Detailed description of the reasons behind the revocation request;
- Name and duties of the person requesting the revocation;
- Signature of the person requesting the revocation.

6.7.8. PROCESSING THE REVOCATION REQUEST

The revocation request must be handled at once and, therefore, shall not take more than 24 hours.

6.7.9. REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

Prior to using a certificate, the relying parties shall verify the status of all certificates through the CRLs or via the online certificate status protocol (OCSP).

6.7.10. CRL ISSUANCE FREQUENCY (IF APPLICABLE)

SISPRoot CA shall publish a new CRL in the repository as soon a revocation request is fulfilled. Where there are no changes in the validity status of the certificates, that is, if no revocation is produced, SISPRoot CA shall make available a new CRL every 3 months.

Maximum time period between issuance and publishing of the CRL should not exceed 3 hours.

All CRLs issued by SISP are digitally signed by SISP.

6.7.11. VERIFICATION REQUIREMENTS OF THE CRLs

The most updated information on a certificate revocation status will be made available through Servers with status verification services provided by SISP. All relevant parties must use those servers to check the current status of a certificate.

6.7.12. OTHER FORMS AVAILABLE FOR DIVULGING THE REVOCATION

No stipulation.

7. MANAGEMENT, OPERATIONAL, AND PHYSICAL SECURITY MEASURES

SISP has developed and implemented a number of rules and policies on the physical, human, and procedural controlsthat support the security requirements included in this CPS.

These rules and policies comply with the good practices recommended by the main international standards related with information security, namely ISO 27001.

7.1. PHYSICAL SECURITY CONTROLS

7.1.1. SITE LOCATION AND CONSTRUCTION TYPE

The operations of the PKI of SISP are conducted within physically protected environments designed to control and audit access to the certification systems, and prevent unauthorized use, damage, or interference. Its architecture uses the concept of in-depth defense, that is, independent levels of protection, so guaranteeing that access to a higher security level is only possible when one has previously reached the immediately prior level.

7.1.2. PHYSICAL ACCESS

The PKI systems of SISP are protected by a minimum of 4 (four) hierarchical security levels which ensure that access to a higher security level is only possible when one has previously reached the immediate prior level.

Sensitive operational activities of the CEs, creation and storage of cryptographic material, any activities within the lifecycle of the certification process like authentication, verification, and issuance, occur within the limits of the most restricted security areas. Physical access is automatically entered and recorded for auditing purposes.

7.1.3. POWER AND AIR CONDITIONING

The secure facilities of the PKI of SISP are equipped with redundant power and climate control systems to ensure continuous and uninterrupted operation of the systems 24 hours a day, 7 days a week, for:

- Uninterrupted feeding systems with enough power to maintain an autonomous electrical network during periods when power is off and to protect the equipment in case of electrical surges that may damage them (redundant equipment consists of batteries for uninterrupted power supply and diesel electricity generators);
- Refrigeration/ventilation/air conditioning that control the temperature and humidity levels and guarantee adequate conditions for the proper functioning of all electronic and mechanical equipment present within the environment.

7.1.4. WATER EXPOSURES

No stipulation.

7.1.5. FIRE PREVENTION AND PROTECTION

Reasonable fire prevention and protection measures are in place at the secure facilities of the PKI of SISP to detect and extinguish fires and prevent damage from exposure to flames or smoke. These mechanisms comply with the existing regulations:

- Fire detection and fire alarm systems are installed at the various physical security levels;
- Fixed and mobile fire-extinguishing appliances are available and placed at easily accessible and strategic locations so that they can be rapidly used when a fire outbreaks to successfully extinguish it;
- Well defined emergency procedures, in case of fire.

7.1.6. MEDIA STORAGE

All sensitive computer media are stored in safety vaults and lockers within the high security area, as well as in a different environment outside the building, with appropriate physical and logical access controls that restrict access only to authorized members of the Working Groups.

7.1.7. WASTE DISPOSAL

Documents and paper material that contain sensitive information shall be shredded before secure disposal.

No information can be retrieved from the media support used to store or transmit sensitive information before they are securely disposed of. Cryptographic devices or logical access keys shall be physically destroyed in accordance with the manufacturer’s waste disposal guidelines, before disposal.

Other storage equipment, namely hard disks and tapes, shall be duly erased so that no information whatsoever can be retrieved.

7.1.8. OFF-SITE BACKUP

Alternate facilities have been established with physical security and environmental controls comparable to those of the primary facility.

7.2. PROCEDURAL CONTROLS/TRUSTED ROLES

The activity of a Certification Entity (hereinafter called CE) depends on the coordinated and complementary action of a wide range of human resources, namely because:

- Given the security requirements inherent in the operation of a CE, it becomes vital to guarantee an adequate separation of duties aimed at minimizing the individual importance of each one of the team members;
- It becomes necessary to guarantee that the CE may only be subject to denial-of-service attacks when a significant number of intervening parties act in collusion;
- Whenever the same entity holds various CEs with different security or hierarchical levels, it may be often desirable that the human resources associated with a CE do not accumulate duties (at least the same) in a different CE.

Due to the above, this section describes the requirements needed to recognize trusted roles and responsibilities linked to each duty. This section also includes the separation of duties as to the roles that cannot be executed by the same individuals.

7.2.1. WORKING GROUPS

Trusted roles consist of employees, suppliers, and consultants that require access to or control over cryptographic or authentication operations.

The PKI of SISP has established that trusted roles be grouped in six different categories (which correspond to five separate Working Groups) in order to ensure that sensitive operations are carried out by different authorized persons that eventually belong to distinct Working Groups, each comprising two members.

7.2.1.1. AUDIT WORKING GROUP

It is responsible for performing internal audits to all actions deemed relevant and necessary to ensure the operational readiness of the CE.

This group is endowed with the following tasks:

- Audit the execution and confirm the accuracy of the CE's processes and ceremonies;
- Record all sensitive operations;
- Investigate suspected cases of procedural frauds;
- Periodically verify the functionality of the security controls (alarm devices, access controls, fire sensors, etc.) present in the various environments;
- Periodically verify the integrity of the Safekeeping Environments, by ensuring that they have the respective apparatus and are duly identified;
- Save all procedures likely to be subject to audit;
- Record the results of all actions undertaken;
- Assume and play the role of Systems Auditor;
- Validate the fact that all resources used are safe.

7.2.1.2. SECURITY WORKING GROUP

The Security Administration Working Group is responsible for proposing, managing, and implementing all policies that are up-to-date, and ensure that all information needed for the functioning and audit of a CE is available over time. This Working Group also exercises the duty of HSM Operation.

Duties of this Working Group:

- Manage the Security Administration Environment;
- Define and manage all policies of the CE and guarantee that they are updated and adjusted to their reality;
- Ensure the implementation of the policies defined;
- Ensure that the CPs of the CEs are supported by the CPS of the CE;

- Ensure that all relevant documents, directly or indirectly related with the operation of the CE and existing in paper form are duly stored in the Information Environment;
- Manage and control the physical security systems, including accesses, in the production environment;
- Explain all security mechanisms to the employees who must know them and raise awareness on security issues, so leading them to enforce the security rules and policies in place;
- Schedule ceremonies for tests, training activities, and audits to the information systems;
- Configure the accesses to the CE application (groups, rules, logs);
- Set up profiles of the certificates on the CE application;
- Activate the interface for the operation of the CE;
- Activate the keys for its use;
- Authorize key generation for the application. This operation is required during the key generation ceremony for the CE;
- Start-up SISPROOT CA configuration interface.

On the other hand, the role of HSM administration/operation entails the following duties:

- Recovery of the functionality of cryptographic hardware in case of failure of an HSM;
- Key recovery in case they have been accidentally erased;
- Replacement of a set of manager cards. This operation is required only if the number of manager cards is to be expanded or reduced;
- Replacement of a set of operator cards. This operation is required only when the number of operator cards is to be expanded or reduced, or for the purpose of replacing any damaged card;
- Expansion of the number of HSM integrated in the infrastructure;
- Taking into account that the system operates in a FIPS140-2 level 3 mode, authorization is required for generating sets of operator cards and keys. This operation is needed only during the key generating ceremony of the CE;
- Key activation. This means that each time the CE starts up, it becomes necessary to insert the operator cards associated to the keys;
- Authorization for generating keysfor the application. This operation is required during the key generation ceremony for the CE;
- Start-up of the configuration interface of the CE and the remaining entities that are part of the PKI.

7.2.1.3. SYSTEMS ADMINISTRATION GROUP

The Systems Administration Working Group is responsible for installing, setting up, and maintaining (hardware and software) the CE, without affecting the application security.

Its duties are detailed below:

- Maintain an updated inventory of all products related with the CE;

- Install, interconnect, and configure the CE's hardware;
- Install and set up the CE'S basic software;
- Manage and update the installed products;
- Prepare in-house news releases about the initial keywords;
- Prepare in-house news releases on the Hash of the installation CDs used;

On the other hand, the Group must:

- Daily operate the systems, making security copies, and restore information as needed;
- Execute routine tasks of the CE, including backup copies of its systems;
- Manage the Operation Environment.

7.2.1.4. REGISTRATION GROUP

The Registry Administration Working Group is responsible for executing the routine tasks needed for the smooth operation of the CE, as well as all incidents that take place. This Group is also in charge of operating the CE in what concerns certificate issuance, suspension, and revocation.

The duties of this Group include certificate issuance, suspension, and revocation.

7.2.1.5. MANAGEMENT GROUP

The Management Group is responsible for appointing the members of the remaining groups and taking critical level decisions. This group must comprise a minimum of 4 (four) members.

The duties of this group are detailed below:

- Review and approve the policies proposed by the Security Administration Working Group;
- Request policy approval to the Managing Board of the ICP-CV;
- Appoint the members of the remaining working groups;
- Make available the identification details of all individuals who are part of the various Working Groups in one or more access points that are easily accessible by the authorized persons.

7.2.2. NUMBER OF INDIVIDUALS REQUIRED PER TASK

There are a number of strict control procedures that require the separation of duties based on the specificities of each Working Group, so as to ensure that sensitive tasks may only be executed by a manifold set of certified persons.

Internal control procedures have been prepared in such a way as to guarantee a minimum of 2 trusted individuals to have physical or logical access to the security devices. Access to the cryptographic hardware of the CE follows rigorous procedures involving multiple authorized individuals to have access during its lifetime, from reception and inspection to the physical and/or logical damage of the hardware. Following activation of a module with operational keys, additional access controls are used to ensure that the physical and logical accesses to the hardware are only possible with 2 or more authorized individuals. The individuals holding physical access to the modules do not hold the activation keys and vice-versa.

7.2.3. ROLES REQUIRING SEPARATION OF DUTIES

The following matrix defines the incompatibilities (indicated by an X) between membership of a group/subgroup identified in the left column and membership of the group/subgroup identified in the first line, within the context of this CE:

Working Group	**Inconsistent with**				
	(a)	(b)	(c)	(d)	(e)
Security Administration (a)		X	X	X	
Systems Administration (b)	X		X	X	
Registry Administration (c)	X	X		X	
Audit (d)	X	X	X		X
Management (e)				X	

7.3. STAFF CONTROL MEASURES

7.3.1. REQUIREMENTS RELATED WITH QUALIFICATIONS, EXPERIENCE, BACKGROUND AND CERTIFICATION

All personnel occupying a trusted role in the PKI of the SISP must comply with the following requirements:

- Be formally appointed for the position to be performed;
- Present evidence of the background, qualifications and experience needed for the tasks related with his position;
- Hold adequate training for the performance of the respective duties;
- Guarantee secrecy as to the sensitive information on the CE or identification details of titleholders;
- Guarantee knowledge of the terms and conditions for the position to be performed; and
- Guarantee that he/she does not perform any other duties that may conflict with his/her responsibilities at the CE.

7.3.2. BACKGROUND CHECK PROCEDURES

Background check procedures derives from the accreditation process of the individuals appointed for assignments in any trusted role position. Background check includes:

- Confirmation of identification, using documents issued by reliable sources; and
- Investigation of criminal records.

7.3.3. TRAINING REQUIREMENTS AND PROCEDURES

The members of the Working Groups receive adequate training so that they may perform their duties in a satisfactory and efficient way.

In addition, they are subject to a training plan embracing the following topics:

- Digital certificate and Public Key Infrastructures;
- General concepts on information security;
- Specific training for his/her role within the Working Group;
- Operation of the software and/or hardware used in the PKI of SISP;
- Certificate Policy and Certification Practice Statement;
- Recovery in case of disaster;
- Business continuity procedures, and
- Basic legal aspects related with the provision of certification services.

7.3.4. RETRAINING FREQUENCY AND REQUIREMENTS

Whenever required, additional training will be provided to the members of the Working Groups in order to guarantee the intended level of professionalism for the satisfactory execution of their duties. In particular,

- In the event of any technological change, introduction of new tools or changes in the procedures, adequate training is organized for all staff members working at the PKI of SISP;
- Where there are alterations in the Certificate Policy or Certification Practice Statement, retraining sessions for the PKI staff will also be organized.

7.3.5. JOB ROTATION FREQUENCY AND SEQUENCY

No stipulation.

7.3.6. SANCTIONS FOR UNAUTHORIZED ACTIONS

Unauthorized actions are regarded as any actions that fail to respect the Certification Practice Statement and the Certification Policies, whether arising from negligence or being deliberate.

In accordance with the rules and regulations of the PKI of SISP and the national security legislation, appropriate disciplinary actions shall be taken for unauthorized actions or unauthorized use of the systems.

7.3.7. SERVICE PROVIDERS' CONTROLS

Consultants or independent service providers are allowed access to the high security area provided that they are always accompanied and directly supervised by the members of the Working Group and that their access is entered in the Guest Book.

7.3.8. DOCUMENTATION SUPPLIED TO PERSONNEL

The Working Groups are provided with all adequate information so that they may carry out their tasks in a competent and satisfactory fashion.

7.4. AUDIT LOGGING PROCEDURES

7.4.1. TYPE OF EVENTS RECORDED

Significant events generate auditable records. These include at least the following:

- Access attempts (successful or unsuccessful) to request, generate, sign, issue, or revoke certificate keys;
- Access attempts (successful or unsuccessful) to create, modify, or delete information on certificate titleholders;
- Access attempts (successful or unsuccessful) and security profile changes in the operating system;
- Issuance and publication of the CRLs;
- Application start-up and shut down;
- Access attempts (successful or unsuccessful) for login and logout;
- Access attempts (successful or unsuccessful) to create, modify, and delete user accounts in the system;
- Backup copies, data retrieving or filing;
- Software and hardware changes or updates;
- System maintenance;
- Operations executed by members of the Working Groups;
- Changes in Human Resources;
- Access attempts (successful or unsuccessful) to the premises on the part of authorized or unauthorized personnel;
- The key generation ceremony and systems involved therein, such as applicational servers, databases, and operating system.

7.4.2. FREQUENCY FOR PROCESSING AUDIT LOGS

Audit logs are reviewed on a daily basis and in an automated form, sending alerts to the Audit Working Group whenever there are suspicions or unusual activities, or threats of some kind. The actions taken, based on the information included in the logs, are also documented.

7.4.3. RETENTION PERIOD FOR AUDIT LOGS

Audit logs shall be available online during the validity period of the certification after which they are archived under the terms described in section 8.5.

7.4.4. PROTECTION OF AUDIT LOGS

Audit logs are exclusively reviewed by members of the Audit Working Group and reported to the Management Working Group.

Audit logs are protected by auditable electronic mechanisms enabling to detect and prevent the occurrence of modification attempts, removal, or other unauthorized data manipulation schemes.

Audit logs of the PKI of SISP are backed up and stored at a secure location and in vaults complying with the Standard EN 1143.

The destruction of an audit log shall only take place with the authorization of the Management Group and executed in the presence of at least two employees (a security element and an audit element). This act should be recorded in an audit log.

7.4.5. AUDIT LOG BACKUP PROCEDURES

Audit logs are backed up on a regular basis in high capacity storage systems, namely tape and in storage.

7.4.6. AUDIT LOG ACCUMULATION SYSTEM (INTERNAL / EXTERNAL)

The audit log handling and collection process comprises a combination of automatic and manual processes executed on the operating systems by the applications of PKI of SISP and the personnel that operate them. All audit logs are stored in the internal systems of the PKI of SISP.

7.4.7. NOTIFICATION TO EVENT-CAUSING SUBJECT

Auditable events are recorded in the audit system and kept in a safe way without notification to the event-causing subject.

7.4.8. VULNERABILITY ASSESSMENTS

Auditable logs are regularly analyzed in order to minimize and eliminate potential attempts to compromise system security. Four intrusion tests are performed yearly with the objective of detecting and assessing vulnerabilities. The result of the analysis is then reported to the Management Group of the PKI of SISP to review and approve an implementation and correction plan for the vulnerabilities detected.

7.5. RECORDS ARCHIVAL

7.5.1. TYPES OF RECORDS ARCHIVED

All auditable data are archived (as indicated in section 8.4.1), as well as information on certificate requests and documents supporting the lifecycle of the various operations.

The information and events that are recorded and archived include:

- Audit data, as specified in Section 8.4.1. of this CPS;
- Backups of the applications and systems comprised in the PKI of SISP;
- All documents related to the lifecycle of the certificates, namely:
  - Certificate issuance and revocation procedures;
  - Certificate issuance and acceptance forms;
- Confidentiality agreements;
- Protocols established with Subscribers;
- Contracts signed between the PKI of SISP and other entities – only made available upon request, after previous analysis and approval of the request;
- Authorizations of access to the information systems;
- Access to the apparatus found in the custodies.

7.5.2. RETENTION PERIOD FOR ARCHIVE

Data subject to archive are retained for the period defined in the national legislation.

7.5.3. ARCHIVE DATA PROTECTION

Archives are protected so that:

- Only authorized members of the Working Groups may view and have access to the archives;
- Archives are protected against any modification or attempt to remove them;
- Archives are protected against damage of the media where they are kept, by means of periodical migration to a new media;
- Archives are protected against obsolescence of the hardware, operating systems, and other software, by maintaining the hardware, operating systems, and other software which become part of the archive itself, in order to enable access and use of the records kept in a timeless way;
- Archives are kept in a secure manner, in safe, external environments, in accordance with the Policy of Data Retention. The backups of the PKI of SISP are maintained in safe locations, in vaults that comply with the standard EN 1143.

7.5.4. ARCHIVE BACKUP PROCEDURES

Backup copies are fully made and kept in WORM (Write Once Read Many) devices.

7.5.5. REQUIREMENTS FOR TIME-STAMPING OF RECORDS

A few database entries shall contain time and date information which is provided by an accurate, time reference service.

7.5.6. ARCHIVE COLLECTION SYSTEM (INTERNAL / EXTERNAL)

The systems for the collection and maintenance of archived records are internal.

7.5.7. PROCEDURES TO OBTAIN AND VERIFY ARCHIVED INFORMATION

Only authorized members of the Working Groups shall have access to archives in order to verify their integrity.

Integrity checks to the electronic archives (backup copies) shall be automatically carried out at the time of their creation. In the event of errors or unforeseen practices, new archives will be created.

7.6. KEY CHANGEOVER

Only subordinate certification entities of the PKI of SISP with valid certificates may request renewal of the respective key pair, provided that the generation of a new key pair is in conformity with section 7.7.

7.7. COMPROMISE AND DISASTER RECOVERY

This section describes the requirements linked to the notification and recovery procedures in case of disaster or compromise.

7.7.1. INCIDENT AND COMPROMISE HANDLING PROCEDURES

Backup copies of private keys of SISPRoot CA (generated and maintained in light of section 8.2.3.1) and data archived (section 7.5.1) are stored in safe external environments and made available in the event of a disaster. In case of compromise of the private key of SISPRoot CA, the latter should take the following actions:

- Proceed to its immediate revocation;
- Revoke all dependent certificates contained therein;
- Inform all titleholders of certificates and known third-parties;
- Inform all Entities comprised in the PKI of SISP.

7.7.2. RECOVERY PROCEDURES IF COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

In case the computing resources, software, and/or data are corrupted or should there exist suspicion of corruption, backup copies of the private key of the CE and data archived may be obtained to enable verification of the integrity of the original data.

Where there is confirmation that the computing resources, software, and/or data are corrupted, appropriate measures should be taken to address the incident. Incident response may include recovery of the corrupted equipment/data by using similar equipment and/or recovering backup copies and data archived. Until such time as safe conditions are restored, SISPCA01Root will suspend its services and notify all Entities involved. In cases where it is found that this situation has affected the issued certificates, titleholders will be notified accordingly and the respective certificates revoked.

7.7.3. RECOVERY PROCEDURES AFTER PRIVATE KEY COMPROMISE

Where the private key of SISPRoot CA is compromised or there is suspicion of its compromise, appropriate measures must be taken for incident response, which may include:

- Informing the National Accreditation Authority and the Managing Board of the ICP-CV;
- Notifying subordinate CAs, all holders of certificates issued within the trust hierarchy of SISPRoot CA;
- Revoking the certificate of SISPRoot CA and all other certificates issued within the trust hierarchy of SISPRoot CA;
- Generating a new key pair for SISPRoot CA and including them in the various systems/browsers;
- Renewing all certificates issued within the trust hierarchy of SISPRoot CA.

7.7.4. BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

The PKI of SISP has established the computing resources, software, backup copies, and archived data in its secondary facilities, deemed necessary to resume or recover key operations (certificate issuance and revocation with the publication of information on revocation) based on the procedures defined in the Contingency Plan, after a natural disaster or any other type of disaster.

7.8. PROCEDURES IN CASE OF TERMINATION OF THE CE OR RE

In case of termination of its activities as a Certification services provider, SISP shall execute the procedures anticipated in the Business Cessation Plan, as per article 36 of DL no. 33/2007.

If any modifications occur in the organization/structure responsible for managing the CA, the latter shall report such fact to the National Accreditation Authority and the Managing Board of the ICP-CV.

8. TECHNICAL SECURITY CONTROLS

This section defines the security controls implemented by the PKI of SISP for SISPRoot CA with the objective of protecting the cryptographic keys generated by the latter, and the respective activation data. The security level allocated to key maintenance must be the maximum so that private keys and secure keys, as well as activation data, are protected at all times and can be accessed by duly authorized persons.

8.1. KEY PAIR GENERATION AND INSTALLATION

Generation of SISPRoot CA key pairs is processed in conformity with the requirements and algorithms defined in this policy.

Generation of cryptographic keys of SISPRoot CA is performed by a Working Group including members so authorized in a ceremony planned and audited in accordance with written procedures on the operations to be executed. All key generation ceremonies are recorded, dated, and signed by the members of the Working Group.

The cryptographic hardware used for generating the keys of SISPRoot CA complies with the requirements FIPS 140-2 level 3, and/or Common Criteria EAL 4+, and carries out key maintenance, retrieval, and all operations involving cryptographic keys by exclusively using the hardware. Access to critical keys is protected by security policies, role division between the Working Groups, as well as through restricted access rules for users. The backup copies of cryptographic keys are only made using hardware, enabling these copies to be duly audited and facilitating total, secure key recovery in the event of loss of data.

Generation of SISPRoot CA key pair is performed by authorized members of the Working Groups in a cryptographic hardware that meets the requirements set forth in FIPS 140-2 level 3, and/or Common Criteria EAL 4+.

SISPRoot CA works in offline mode and the certificate is signed by ECR-CV.

8.1.2. PRIVATE KEY DELIVERY TO THE SUBORDINATE CE

SISPRoot CA does not generate the private key associated with the certificates it issues.

8.1.3. PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

The public key is delivered to SISPRoot CA in accordance with the procedures defined under section 6.2.2.

8.1.4. PUBLIC KEY DELIVERY TO THE RELYING PARTIES

The public key of SISPRoot CA will be made available through the certificate of SISPRoot CA, as per section 6.3.2.

8.1.5. KEY SIZES

The length of the key pairs must be long enough so as to prevent possible cryptanalysis attacks that may unveil the private key corresponding to the key pair in its lifecycle. Key sizes are the following:

- 4096 bits RSA for the SISPRoot CA key.

8.1.6. PUBLIC KEY PARAMETER GENERATION AND QUALITY CHECKING

Generation of public key parameters and quality checking shall always be based on the standard that defines the algorithm.

The CE's keys should be generated based on the use of random or pseudo-random processes described in ANSI X9.17 (Annex C), as stipulated in the standards ISO 9564.1 and 11568-5, respectively.

8.1.7. KEY USAGE PURPOSES (FIELD X.509 V3)

When used in accordance with the recommendations of RFC 5280, the field "KeyUsage" of the certificates includes the following uses:

- Key Certificate Signature
- CRL Signature

8.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE CHARACTERISTICS

This section considers the requirements for private key protection and the cryptographic modules of SISPRoot CA. The PKI of SISP has implemented a combination of duly documented physical and logical controls and procedures meant to ensure the secrecy and integrity of the private keys of SISPRoot CA.

8.2.1. CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

In order to generate the key pairs of SISPRoot CA, as well as for private key storage, the PKI of SISP uses a cryptographic module in hardware that meets the following standards:

- Physical Security
    - Common Criteria EAL 4+ and/or
    - FIPS 140-2, level 3
- Authentication
    - Two-factor authentication.

8.2.2. PRIVATE KEY (N out of M) MULTI-PERSON CONTROL

Multi-person control is only used for CA's keys whereas the private key of the certificates is under the exclusive control of its titleholder.

The PKI of SISP has implemented a series of mechanisms and techniques that require the participation of various members of the Working Groups to perform sensitive cryptographic operations in the CA.

All operations are executed with a minimum of two persons in trusted roles positions of the entity, with distinct duties.

In practice, at least two persons (N=2) among the entire workforce of the entity (M=staff) are used in the different duties.

The private keys of the PKI of SISP are held by more than one member. They are activated by starting the CA's software through a combination of operators of SISPRoot CA and HSM administrators. This is the only method of activating the private key.

8.2.3. PRIVATE KEY RETENTION (KEY ESCROW)

SISPRoot CA only retains its private key.

8.2.3.1. KEY RECOVERY POLICIES AND PRACTICES

The private key of SISPRoot CA is stored in an HSM and a backup copy is made by using a direct connection from hardware to hardware with the two-factor authentication, executed by representatives of different Working Groups.

The backup hardware, along with the backup copy of the private key of SISPRoot CA, is placed in a secure vault in secure secondary facilities, accessible only to authorized members of the Working Groups.

The backup copy of the private key of SISPRoot CA may be recovered in case of malfunction of the original key. The key recovery ceremony uses the same two-factor authentication mechanisms with multiple persons who participated in the backup copy ceremony.

8.2.3.2. POLICIES AND PRACTICES FOR ENCAPSULATION AND RECOVERY OF SESSION KEYS

No stipulations.

8.2.4. PRIVATE KEY BACKUP

The private key of SISPRoot CA has at least one backup with the same security level as the original key.

All keys that have been subject to backups are archived for a minimum of 20 years following the end of its validity period.

8.2.5. PRIVATE KEY ARCHIVAL

The private keys of SISPRoot CA, subject to backups, are archived as referred to in section 8.2.3.

8.2.6. PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

The private keys of SISPRoot CA are not retrievable from the cryptographic token FIPS 140-2 level 3.

If a backup of the private keys of SISPRoot CA is copied into another cryptographic token, then such copy is directly made, from hardware to hardware, so ensuring transport of the keys between modules in an encrypted transmission.

8.2.7. PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The private keys of SISPRoot CA are stored in a ciphered form in the cryptographic hardware modules.

8.2.8. ACTIVATING PRIVATE KEYS

The key is activated when the system/application of SISPRoot CA is connected. This activation becomes effective when authentication has been carried out by the HSM administrators in the cryptographic module, being compulsory the use of two-factor authentication. In order to activate the private key, at least two individuals are required to be authenticated. Once the key is activated, it will remain so until the deactivation process is executed.

8.2.9. DEACTIVATING PRIVATE KEYS

The private key of SISPRoot CA is deactivated when the CA system is disconnected. Once deactivated, it will remain inactive until the activation process is executed.

8.2.10. DESTROYING PRIVATE KEYS

The private keys of SISPRoot CA (including the backup copies) shall be deleted/destroyed through a duly identified procedure, audited within a minimum of 30 days following its validity term (or otherwise if revoked before that period).

The PKI of SISP shall destroy the private keys and guarantee that there are no residues that can enable their reconstruction. To that end, it makes use of the formatting function (boot value zero) made available by the cryptographic hardware or other appropriate means, to ensure destruction of the CA's private keys.

8.2.11. CRYPTOGRAPHIC MODULE ASSESSMENT / LEVEL

See section 8.2.1.

8.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

8.3.1. PUBLIC KEY ARCHIVAL

A backup copy of all public keys of SISPRoot CA is executed by the members of the Working Group and remains in storage after the expiration of the corresponding certificates for verification of the signatures generated during their validity period.

8.3.2. CERTIFICATE AND KEY PAIR VALIDITY PERIODS

The usage period of keys is determined by the certificate validity period and, therefore, after expiration of the certificate the keys cannot be used, giving way to permanent cessation of their operability and usage.

Given the above, the validity of the various types of certificates and the period in which they must be renewed is as follows:

- The certificate of SISPRoot CA shall be valid for 12 years and be used to sign certificates during its first 6 years and be reissued prior to reaching 6 years and 6 months of validity;
- The certificate of subordinate CEs is valid for 6 years, being used to sign certificates during its first 3 years and reissued after 3 years of validity;
- The OCSP (Online Certificate Status Protocol) certificates are valid for 5 years and 4 months. They are used during their initial four years and reissued following the fourth month of validity.

8.4. ACTIVATION DATA

8.4.1. ACTIVATION DATA GENERATION AND INSTALLATION

Activation data needed to use the private key of SISPRoot CA are divided into various parts (saved in PED keys – small digital identification tokens in a smartcard format – distinguishing the different roles in accessing the HSM), and remain under the responsibility of different members of the Working Group. The different parts are generated in accordance with the rules defined in the key generation process/ceremony and obey to the requirements specified in the standard FIPS 140-2 level 3.

8.4.2. ACTIVATION DATA PROTECTION

Activation data (in separate parts and/or password) are memorized and/or saved in tokens that highlight violation attempts and/or are stored in envelopes and kept in secure vaults.

The private keys of SISPRoot CA are kept, in a ciphered form, in cryptographic tokens.

8.4.3. OTHER ASPECTS OF ACTIVATION DATA

If it becomes necessary to transmit the activation data of private keys, this transmission will be protected against information losses, theft, data alteration, and unauthorized disclosure.

Activation data are destroyed (by means of formatting and/or physical destruction) when the related private key is destroyed.

8.5. COMPUTER SECURITY CONTROLS

8.5.1. SPECIFIC TECHNICAL REQUIREMENTS

Access to SISPRoot CA servers is restricted to the members of the Working Groups who present a valid reason for that access. SISPRoot CA can operate offline, being disconnected at the end of each certificate issuance or any other technical intervention, and complies with the requirements for identification, authentication, access controls, administration, audits, reusage, responsibility, and recovery of services and information exchange.

8.5.2. ASSESSMENT/COMPUTER SECURITY RATING

The various systems and products used by SISPRoot CA are reliable and protected against modifications. The cryptographic module on Hardware of SISPRoot CA conforms with the standard EAL 4+ Common Criteria for Information Technology Security Evaluation and/or FIPS 140-2 level 3.

8.6. LIFECYCLE OF TECHNICAL CONTROLS

8.6.1. SYSTEM DEVELOPMENT CONTROLS

Applications are developed and implemented by third-parties, in light of their regulations regarding system development and change management.

Auditable methodology is made available which enables to verify that SISPRoot CA software has not been modified before its first use. The entire configuration and software changes are executed and audited by members of the Working Groups of the PKI of SISP.

8.6.2. SECURITY MANAGEMENT CONTROLS

The PKI of SISP has mechanisms and/or Working Groups that control and monitor the configuration of the CE's systems. Whenever used for the first time, the SISPRoot CA system is verified in order to guarantee that the software used is reliable and legal, and has not been modified after being installed.

8.6.3. LIFECYCLE OF SECURITY CONTROLS

The updating and maintenance operations of SISPRoot CA systems and products follow the same controls as the original equipment and are installed by members of the Working Group holding adequate knowledge and training in that field, who follow the procedures defined for that purpose.

8.7. NETWORK SECURITY CONTROLS

SISPRoot CA is viewed as an offline CE and is connected to no specific network.

8.8. TIME-STAMPING

Certificates, CRLs, and other revocation database entries shall always contain time and date information. The chronological information is not based on a dedicated time source. The maximum deviation is of 60 seconds. All operations are performed at SISPRoot CA and, in its capacity as an offline CA, they start upon verification of the system's date/time.

9. CERTIFICATE AND CRL PROFILES

9.1. CERTIFICATE PROFILE

The users of a public key must trust that the associated private key is held by the right remote titleholder (person or system) with whom they will use encipherment mechanisms or digital signature. Trust is obtained through the use of X.509 v.3 digital certificates, which are a data structure that establishes connection between the public key and its holder. This connection is asserted through the digital signature of each certificate by a trusted CA. The CA may base this assertion upon technical means (for instance, proof of possession of private key by means of a challenge-solution protocol), presentation of the private key, or the registration made by the titleholder.

A certificate has a limited validity period, which is indicated in its contents and signed by the CA. Considering that the signature on the certificate and its validity may be separately verified by any software that uses certificates, the latter may be distributed throughout communication lines and public systems, and also be kept in any type of storage unit.

The user of a security service who needs to know the public key of the user normally has to obtain and validate the certificate containing that key. If the service does not have a reliable copy of the public key belonging to the CA that signed the certificate, as well as the name of the CE and related information (such as the validity period), then it may need an additional certificate in order to obtain the public key of the CA and validate the user's public key. As a rule, validation of a user's public key may require a chain of multiple certificates, including the user's public key certificate signed by a CA and zero or more additional certificates of CAs signed by other CAs.

The profile of the certificates issued by SISPRoot CA is in conformity with the:

- Recommendation ITU.T X.509;
- RFC 5280;
- National applicable laws and regulations.

9.2. PROFILE OF THE CERTIFICATE REVOCATION LIST (CRL)

When a certificate is issued, it is expected to be used during its entire validity period. However, various circumstances may lead a certificate to become invalid before its validity period expires. Such circumstances include name change, change of association between the holder and certificate data (e.g. an employee who leaves the company), compromise or suspected compromise of the corresponding private key. Under those circumstances, the CA has to revoke the certificate.

The protocol X.509 defines a certificate revocation method involving the periodical issuance, by the CA, of a signed data structure which is called Certificate Revocation List (CRL).

The CRL is a list including the temporary identification of revoked certificates, signed by the CA and freely made available in a public repository. Each revoked certificate is identified in the CRL by its series number. When an application makes use of a certificate (for example, to verify the digital signature of a remote user), the application verifies the certificate's signature and validity and simultaneously obtains the most recent CRL to check if the series number of the certificate is not contained therein. It should be noted that every CE shall issue a new CRL on a regular and periodic basis.

The CRL is in accordance with the:

- Recommendation ITU.T X.509;
- RFC 5280; and
- National applicable legislation.

The profiles of the CRLs may be viewed in the Certification Policies related to this CPS in what concerns SISPRoot CA.

10.POLICY MANAGEMENT

10.1. SPECIFICATION CHANGE PROCEDURES

10.1.1. PROCEDURES FOR AMENDING THE CPS

10.1.1.1. LIST OF CHANGES

Any changes to be introduced in the CPS of SISPRoot CA will result in a change proposal document.

10.1.1.2. NOTIFICATION MECHANISMS

Changes in the policies will be made available in a repository and forwarded to the Registration Entities.

10.1.1.3. PARTICIPANTS' CONTRIBUTIONS

The relying parties of the services provided by SISPRoot CA (subscribers and registration, validity, and time-stamping entities, or even certification entities with which mutual trust-based relations have been established) may provide insights and comments, and issue opinions to SISP or the Registration Entities via e-mail pki@sisp.cv.

10.1.1.4. MECHANISMS TO HANDLE CONTRIBUTIONS

Once completed, a formal change proposal including the inputs collected will be submitted to the Management Working Group of the PKI of SISP. The Management Working Group shall be bound to request the opinion of the Accreditation Authority on the impact of those changes upon the accreditation of SISPRoot CA.

Once in possession of all that information, the Management Group and the Security Working Group shall discuss and deliberate on the proposed changes to the CPS and notify all interested parties on the decisions taken. The subscribers will then be entitled to a maximum period of 30 days to request termination of the agreement with SISPRoot CA, without which the new provisions shall be deemed to have been accepted.

10.1.1.5. PERIOD IN WHICH CHANGES ENTER INTO FORCE

Following conclusion of this process, the approved changes will be implemented after validation of all related controls. In addition, procedures will be adopted in order to ensure that all changes to the CPs and the CPS are tracked and strict version control tools are adopted.

10.2. PUBLICATION AND NOTIFICATION POLICIES

10.2.1. REQUEST FOR PUBLICATION AND NOTIFICATION

All items contained in SISPRoot CA's CPs and CPS shall be subject to publication and notification.

Any material to be published or notified will be so made through SISP site https://pki.sisp.cv/index.html, unless such publication or notification has major impact on SISP and titleholders/relying parties.

SISPRoot CA must digitally sign each publication or notification before it is placed in the respective repository.

SISP will make available, publish, or notify titleholders on matters concerning:

- Adequate protection forms of private keys;
- Risks associated to the use of any certificate issued by SISPRoot CA, whose technology has been discontinued;
- Security rules and practices for the use of the services made available.

10.2.2. PUBLICATION OF CPS UPDATES

The duly updated CPS document remains permanently available on the URL https://pki.sisp.cv/.

10.2.3. CPS APPROVAL PROCEDURES

Validation of this CPS (and/or respective CPs) and any corrections (or updates) thereof must be carried out by the Security Working Group. Any corrections (or updates) must be published by way of new versions of this CPS (and/or respective CPs), thus replacing any previously defined CPS (and/or respective CPs). The Security Working Group shall also determine the time when changes to the CPS (and/or respective CPs) will lead to a change in the object identifiers (OID) of the CPS (and/or respective CPs).

After the validation phase, CPS (and/or respective CPs) will be submitted to the Management Group, which is the entity responsible for the approval and authorization of any changes introduced in this type of document.

11.OTHER BUSINESS AND LEGAL MATTERS

This section regulates business aspects and legal matters.

11.1. FEES

11.1.1. CERTIFICATE ISSUANCE OR RENEWAL FEES

Fees will be made available on the company’s site www.sisp.cv.

11.1.2. CERTIFICATE ACCESS FEES

No stipulation.

11.1.3. REVOCATION OR STATUS INFORMATION ACCESS FEES

Free of charge and open access is provided for information on certificate revocation or status information.

11.1.4. FEES FOR OTHER SERVICES

The fees for time-stamping and online validation (OCSP) services will be identified in a formal proposal to be made by SISP.

11.1.5. REFUND POLICY

No stipulation.

11.2. FINANCIAL RESPONSIBILITY

11.2.1. INSURANCE COVERAGE

SISP maintains a civil liability insurance or self-insures in accordance with article 45 of the Decree-Law no. 33/2007, dated September 24.

11.2.2. OTHER ASSETS

No stipulation.

11.2.3. INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

SISP maintains a civil liability insurance or self-insures in accordance with article 45 of the Decree-Law no. 33/2007, dated September 24.

11.3. CONFIDENTIALITY OF BUSINESS INFORMATION

11.3.1. SCOPE OF CONFIDENTIAL INFORMATION

It is herein expressly declared as confidential any information that cannot be disclosed to third-parties without explicit authorization. This information is taken into custody and only duly authorized Working Groups may be allowed access to it.

11.3.2. INFORMATION BEYOND THE SCOPE OF CONFIDENTIAL INFORMATION

The following information may be disclosed to the public:

- Certificate Policy;
- Certification Practice Statement;
- CRL, and

Any information categorized as "public" (information not expressly considered as "public" is deemed to be confidential).

SISP permits access to non-confidential information without prejudice of any security controls required to protect the authenticity and integrity of such information.

11.3.3. RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

The members of the Working Groups or other entities receiving private information shall be responsible for ensuring that it is not copied, reproduced, stored, translated or disclosed to third-parties by any means whatsoever, before obtaining SISP's written consent.

The coordination of this responsibility is undertaken by the CISO (Chief Information Security Officer). In case of breach of trust, the CISO should be contacted by e-mail ciso@sisp.cv.

11.4. PRIVACY OF PERSONAL INFORMATION

11.4.1. PRIVACY SAFEGUARD MEASURES

The Certificate Lifecycle Management System (CLMS) is responsible for the implementation of measures guaranteeing the privacy of personal information in accordance with the Cabo-Verdean legislation.

11.4.2. INFORMATION TREATED AS PRIVATE

Any information provided by the certificate holder that is not available through the content of the holder's digital certificate is treated as private.

11.4.3. INFORMATION NOT DEEMED PRIVATE

Any information provided by the holder, on which the latter indicates a processing option shall not be deemed private.

11.4.4. RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

In accordance with the Cabo-Verdean legislation.

11.4.5. NOTICE AND CONSENT TO USE PRIVATE INFORMATION

In accordance with the Cabo-Verdean legislation.

11.4.6. DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

No stipulation.

11.4.7. OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

No stipulation.

11.5. INTELLECTUAL PROPERTY RIGHTS

All intellectual property rights, including those related with certificates, CRL, OID, CPS, and CP, as well as any other document belonging to the PKI of SISP, are property of SISP, S.A.

Private keys and public keys are the titleholder’s property, regardless of the physical means used for their storage.

The titleholder retains all intellectual property rights on the trademarks, products, or commercial name contained in the certificate.

11.6. DISCLAIMERS OF WARRANTIES

Except for express warranties stated in this CPS, the PKI of SISP disclaims all other warrantees.

11.7. LIMITATIONS OF LIABILITY

SISPRoot CA:

- Shall be responsible for any losses and damages that it may cause to any person while performing its business activities, as provided for in Article 62 of the Decree-Law no. 33/2007, of September 24;

- Shall be liable for any damages that it may cause to the titleholders or third-parties due to failure or delay in including certificate revocation or suspension in the consulting service on certificate validity whenever it is aware of such failure or delay;
- Shall undertake total responsibility towards third-parties for the performance of the holders of the positions required for the provision of certification services;
- The responsibility of SISPRoot CA administration/management rests upon an objective basis and covers every risk that private parties are likely to suffer as a consequence of the normal or abnormal operation of its services;
- Shall only be responsible for losses and damages caused by the improper use of a recognized certificate whenever the certificate does not state, in a clear way duly acknowledged by third-parties, the limit as to its possible use;
- Shall not be liable when the titleholder overcomes the limits imposed in the certificate as to its possible uses, in accordance with the conditions established and notified to the titleholder;
- Shall not assume any responsibility in case of loss or damage:
    - Arising from the services provided, in case of war, natural disasters, or any other force majeure cases;
    - Caused by certificate use when the limits established in the Certificate Policy and corresponding CPS are exceeded;
    - Caused by improper or fraudulent use of the certificates or CRLs issued by SISPRoot CA.

11.8. INDEMNITIES

In conformity with the legislation in force.

11.9. TERM AND TERMINATION

11.9.1. TERM

The documents related with the PKI of SISP (including this CPS) become effective upon being approved by the Management Working Group and are only amended or cancelled by order of that working group.

This CPS enters into force upon its publication in the SISPRoot CA repository.

This CPS shall remain into force until it is expressly revoked by being replaced by a new version or through the renewal of SISPRoot CA keys, in which case a new version will be compulsorily drafted.

11.9.2. CPS REPLACEMENT AND REVOCATION

The Management Working Group may decide in favor of the elimination or amendment of a document related with the PKI of SISP (including this CPS) whenever:

- Its contents are considered incomplete, inaccurate or wrong;

- Its contents have been compromised.

In that case, the eliminated document shall be replaced by a new version.

This CPS shall be replaced by a new version with autonomy of transcendence of the changes herein made and, therefore, it is to be implemented at all times as a whole.

Once the CPS is revoked, it shall be withdrawn from the repository, being however retained for a period of 20 years.

11.10. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

All participants must use reasonable methods to communicate with each other. These methods may include digitally signed electronic mail, facsimile, signed forms or other, depending on the communication criticality and subject.

11.11. AMENDMENTS

11.11.1. PROCEDURE FOR AMENDMENT

For the purposes of amending this document or any certificate policies, a formal request must be submitted to the Security Working Group, including (at least):

- The identification of the person who submitted the amendment request;
- The reasons underlying the request;
- The changes requested.

The Security Working Group will review the request and, if it is found relevant, it will proceed to the introduction of the required changes, which will result in a new draft version. The new draft version is then made available to all members of the Working Group and the parties affected (if any), to enable its scrutiny. Commencing from the date on which the document became available, the parties involved will submit their comments within a period of 15 working days. Once that period has expired, the Security Working Group will be entitled to an additional 15 working days to assess all comments received and, if relevant, incorporate them in a document. Thereafter, the document is approved and made available to the Management Working Group for validation, approval, and publication. At this stage, the amendments made become final and effective.

11.11.2. NOTIFICATION MECHANISM AND PERIOD

Should the Management Working Group consider that the amendments to the specification may affect the acceptability of the certificates for specific purposes, the users of the corresponding certificates will be notified of the changes and advised to view the new CPS in the defined repository.

11.11.3. CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

The Security Working Group must determine if the changes to the CPS require changes in the OID of the Certificate Policy or the URL indicated for the CPS.

In such situations where, in the view of the Security Working Group, the changes in the CPS do not affect the acceptability of the certificates, an increase in the lower version number of the document and the last Object Identifier (OID) number that represents it will take place, keeping the highest version number of the document, as well as the rest of its associated OID. It is not deemed necessary to notify this type of amendments to certificate users.

In case the Security Working Group considers that the changes to the specification may affect the acceptability of the certificates for specific purposes, the highest version number of the document shall be increased and its lower number shall be placed at zero. The two last numbers of the Object Identifier (OID) that represent it will also be modified. This type of modifications will be notified to the certificate users according to the provisions of paragraph 11.11.2.

11.12. DISPUTE RESOLUTION PROVISIONS

All disputes between users and the PKI of SISP must be reported by the aggrieved party to the Accreditation Authority for the purposes of resolution between the parties involved.

For the resolution of any dispute that may arise in relation to this CPS, the parties, expressly waiving any other jurisdiction that may apply to them, submit to the jurisdiction of Administrative Litigation.

11.13. GOVERNING LAWS

The following specific laws govern the activity of the certifying entities or certification authorities:

a) Decree-Law no. 33/2007, of September 24;
b) Decree-Law no. 44/2009, of November 9;
c) Ordinance no. 2/2008, of January 28;
d) Joint Ordinance no. 4/2008, of February 2008;
e) Regulatory Decree no. 18/2007, of December 24.

11.14. COMPLIANCE WITH APPLICABLE LAWS

This CPS is subject to all applicable national laws, rules, regulations, ordinances, decrees, and orders, including but not limited to, restrictions on the export or import of software, hardware, or technical information.

The Accreditation Authority is bound to ensure compliance with the applicable legislation listed in section 11.13.

11.15. MISCELLANEOUS PROVISIONS

11.15.1. ENTIRE AGREEMENT

All relying parties assume, in its entirety, the contents of the latest version of this CPS.

11.15.2. ASSIGNMENT

In case one or more provisions of this document are, or tend to be, invalid, null, or unclaimable, in legal terms, they should be considered as ineffective.

The situation referred to above shall only be valid in cases where such provisions are not deemed essential. It is the responsibility of the Accreditation Authority to assess their importance and relevance.

11.15.3. SEVERABILITY

No stipulation.

11.15.4. ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

No stipulation.

11.15.5. FORCE MAJEURE

No stipulation.

11.16. **OTHER PROVISIONS**

No stipulation.

BIBLIOGRAPHICAL REFERENCES

1) ARME, Certification Practice Statement of the Root CE of Cabo Verde;
2) ARME, Certificate Policies of the ICP-CV and Minimum-Security Requirements;
3) Ordinance no. 2/2008, of January 28;
4) Decree-Law no. 44/2009, of November 9;
5) Regulatory Decree no. 18/2007, of December 24;
6) Decree-Law no. 33/2007, of September 24;
7) Joint Ordinance no. 4/2008, of February 2008;
8) FIPS 140-2. 1994, Security Requirements for Cryptographic Modules;
9) ISO/IEC 3166. 1997, Codes for the representation of names and countries and their subdivisions;
10) ITU-T Recommendation X.509. 1997 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework;
11) NIST FIPS PUB 180-1. 1995. The Secure Hash Algorithm (SHA-1). National Institute of Standards and Technology. “Secure Hash Standard”, U.S. Department of Commerce;
12) RFC 1421. 1993. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures;
13) RFC 1422. 1993, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management;
14) RFC 1423. 1993, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers;
15) RFC 1424. 1993, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services;
16) RFC 2252. 1997. Lightweight Directory Access Protocol (v3);
17) RFC 2560. 1999. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
18) RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7;
19) RFC 3161. 2001, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP);
20) RFC 3279. 2002, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
21) RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
22) RFC 3647. 2003, Internet X. 509 Public Key Infrastructure Certificate Policy and Certification Practice Framework;
23) RFC 4210. 2005, Internet X. 509 Public Key Infrastructure Certificate Management Protocol (CMP);
24) Certificate Policy of the Root CE of Cabo Verde (ECR-CV).
25) CABForum Baseline Requirements
26) CABForum-EV-Guidelines –v1.7.0