SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTOS

SISP ROOT CA02 - CPS

Certification Practices Statement

Code:	PLRC011
Version:	01
Version Date:	06/14/2022
Created by:	SISP
Approved by:	Director-General - Jair Silva
Level of Confidentiality:	Public

Change Control Log

Date	Version	Created by	Description of Amendment
06/14/2022	01	Ruben Veiga	Document Creation

Table of Contents

TABLE INDEX

1. Introduction

- **Scope**

The present document is a Certification Practices Statement and aims to disseminate the general certificate issuance and management practices followed by SISPROOTCA02 Root Certification Entity, as a qualified trust service provider under the CAB Forum "*Baseline for Issuance and Management of Publicly-Trusted Certificates*" and *eIDAS Regulation* No. 910/2014, in support of its digital certification activity.

This document may be subject to regular updates.

- **Target Audience**

This is a public document and is intended for all those who deal with the SISPROOTCA02 Root Certification Entities, hereinafter referred to as SISPROOTCA02.

Certificates issued by SISPROOTCA02 contain a reference to the present CPS, Document Code No. PLRC00X.01, in order to allow relying parties and other interested persons to find information about the certificate and the entity that issued it.

- **Document Layout**

This document follows the structure defined and proposed by the PKIX working group of the IETF, in the RFC 3647 document. It is assumed that the reader is already familiar with the concepts of cryptography, public key infrastructure and electronic signatures. If this is not the case, we recommend that you study these topics beforehand to better understand the content. The document is structured in 9 chapters, the first 7 of which are reserved for certification procedures and practices used by the PKI of SISP, while the remaining two are dedicated to Audit/Compliance and legal issues, respectively.

1.1. General Context

This CPS specifies the security requirements, policies and practices used by SISPROOTCA02 in its digital certification activity and is in accordance with the following standards:

a) RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework;
b) RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile;
c) eIDAS Regulation No.910/2014;
d) CA –Browser-Forum Baseline Requirements 1.8.4;
e) ETSI TS 119 312 - Electronic Signatures and Infrastructures (ESI): Cryptographic Suites.

1.2. Document Title and Identification

This document is formally referred to as a CPS and is represented on a certificate through a unique number named as “Object Identifier” (OID). The OID value associated with this CPS is 1.3.6.1.4.1.4146.1.60.

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

Table 1: Document Information

DOCUMENT INFORMATION	
Document Title	SISPROOTCA02 Certification Practices Statement
Document Version	Version 1.0
Document Status	Approved
OID	1.3.6.1.4.1.4146.1.60
Date of Issue	06/14/2022
Validity	06/13/2023
Location	http://pki.sisp.cv/

Updates shall be made to the document whenever applicable.

1.2.1. Reviews

Version	Creation	Approval	Reason for Review
1.0	06/14/2022	06/15/22	Creation
	Security Administrator	Management Group	
	Ruben Veiga	Jair Silva	

1.2.2. Document Background

Table 2: Document Background

Date	Version	Created by	Description of the Amendment
06/14/2022	1.0	Ruben Veiga	Document Creation

1.3. 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 cryptographic key pairs associated with each one of the Certification Entities;
2. Receiving and validating the requests for certificate issuance made by Subordinate Certification Entities (CE), as well as other subscribers;
3. Issuing certificates related with requests that comply with the format required by SISP Certification Entities;
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.

The PKI of SISP comprises the following CEs:

- SISP *Root Certification Authority 02 (SISP Root CA02)*
- SISP QWAC Certification Authority (SISP QWAC)

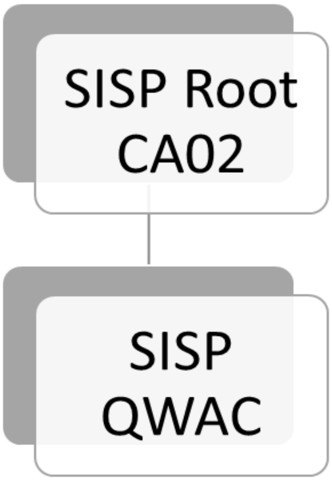

Illustration 1: Structure of the PKI of SISP

1.3.1. Certification Entities

➢ SISP Root Certification Authority 02 (SISP Root CA02)

It is a self-signed root certifying entity, being qualified to issue certificates for the signature of subordinate certifying entities that may issue qualified and non-qualified TLS/SSL Web authentication and code sign certificates.

Table 3: Certificate Information (SISP Root CA02)

CERTIFICATE INFORMATION	
Distinguished Name	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Root Certification Entity of SISP 02
Signature Algorithm	sha512WithRSAEncryption
Serial Number	6f1566a98112c3fffd6a7b9c0c9bc9d062cf2293
Validity	June 28, 2034 06:45:00
Thumbprint	9C:D8:8D:03:09:AB:9F:63:60:73:A3:AA:28:E6:4E:F8:94:CC:A3:E6:D9:37:08:74:BA:ED:C7:1F:C9:3A:2D:1E:DB:80:B3:C8:80:9E:0A:D5:B8:F9:47:2A:A0:51:6C:9B:1E:78:AF:D8:F7:74:97:E9:D7:64:2E:5E:C2:0A:02:62
Issuer	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Root Certification Entity of SISP 02

- **SISP QWAC Certification Authority**

It is a subordinate certification entity, signed by *SISP Root CA 02*, being qualified to issue certificates to end users in conformity with the CA/Browser Forum "*Baseline for Issuance and Management of Publicly-Trusted Certificates*" and *eIDAS Regulation* No. 910/2014.

SISP QWAC issues qualified *TLS/SSL Extended Validation (EV)* Web Authentication certificates in conformity with the *CA/Browser Forum Guidelines for the issuance and management of Extended Validation Certificates*.

Table 4: Certificate Information (SISP QWAC *Certification Authority*)

CERTIFICATE INFORMATION	
Distinguished Name	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN= SISP QWAC
Signature Algorithm	sha512WithRSAEncryption
Serial Number	77a5aacfb1eb23c603e9f429b724826dbc78add6
Validity	June 29, 2028 07:22:55
Thumbprint	9C:D8:8D:03:09:AB:9F:63:60:73:A3:AA:28:E6:4E:F8:94:CC:A3:E6:D9:37:08:74:BA:ED:C7:1F:C9:3A:2D:1E:DB:80:B3:C8:80:9E:0A:D5:B8:F9:47:2A:A0:51:6C:9B:1E:78:AF:D8:F7:74:97:E9:D7:64:2E:5E:C2:0A:02:62
Issuer	C = CV, O = SISP, OU = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Root Certification Entity of SISP 02

1.3.2. Registration Entities or Units

Registration Entities or Units refer to the entities to which the CEs delegate the provision of services in the field of identification and registration of certificate users, as well as the management of requests for certificate renewal and revocation. SISP may act as a Registration Unit and/or establish agreements with third-parties for them to play this role.

- **Internal Registration Entity**

Within the scope of the SISPROOTCA02 Certification Authority, the registration entity is materialized by the internal services of the PKI of SISP that proceed to the registration and validation of the necessary data, as explained in the Certificate Policy of each type of certificate issued.

- **External Registration Entity**

The hierarchy of trust of SISPROOTCA02 includes no external registrars.

1.3.3. Certificate Holders

In the context of this document the term subscriber/holder applies to all end users to whom certificates have been assigned by the PKI of SISP.

The titleholders of certificates issued by the PKI of SISP are considered to be those whose name is inscribed in the certificate's "*Subject*" field and use the certificate and respective private key in accordance with the provisions of the various certificate policies described in this document, with certificates being issued for the following titleholder categories:

- Natural person;
- Legal person (Organizations);
- Services (computers, servers, domains, etc.)
- Members of the working groups.

In some cases, certificates are issued directly to individuals or legal entities for personal use; however, there are situations in which the applicant is different from the certificate titleholder, for example, an organization may request certificates for its employees to represent the organization in electronic transactions. In these situations the entity requesting the issuance of the certificate is different from the certificate titleholder.

1.3.4. Relying Parties

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.

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 PKI of SISP.

1.3.5. Other Participants

- **Supervisory Authority**

The Supervisory Authority takes on the role of a body that provides compliance audit/inspection services in order to assess whether the processes used by the CEs in the certification activities meet the minimum requirements set out in the laws and regulations in force. Its main attributions are the following:

a) Accredit the certification entities;

b) Audit the certification entities;

c) Assess the activities undertaken by authorized certification entities in light of the technical requirements defined under the terms of the preceding paragraph;

d) Ensure adequate operation and effective service provision by the certification entities, in conformity with the legal and regulatory provisions set out for such activity.

- **External Service Providers**

The responsibilities endowed to the Entities that provide support services to the PKI of SISP are duly defined through contracts.

- **Security Auditor**

The security auditor is independent from the sphere of influence of the Certification Entity and is required by the Supervisory Authority. He/she is endowed with the task of auditing the infrastructure of the Certification Entity in what respects equipment, human resources, processes, policies and rules, being bound to submit an annual report to the Supervisory Authority.

1.4. Certificate Usage

The certificates issued by SISPROOTCA02 are exclusively for signing certificates of the Certifying Entities of the level immediately subsequent to its own, its LRC (List of Revoked Certificates) and its OCSP, with the objective of guaranteeing the following services:

- Authentication;
- Secrecy;
- Integrity;
- Privacy;
- Authenticity 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 cipher algorithms, along with mechanisms to establish and distribute keys managed by certified cryptographic equipment. Relying parties can validate the chain of trust and thus guarantee the holder's authenticity and identity.

1.4.1. Proper Use of the Certificate

The requirements and rules defined in this document apply to all certificates issued by the SISPROOTCA02 certification entity.

The certificates issued by SISPROOTCA02 are also used by relying parties to verify the chain of trust, as well as to guarantee the authenticity and identity of the issuer of a certificate for web data transmission via the TLS/SSL protocol, the ownership of the domain, the identity of the website/organization, the confidentiality and security in the exchange of information between the user and the website.

1.4.2. Unauthorized Use

The certificates issued by SISPROOTCA02 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 are not designed for or authorized for use in high-risk activities or activities that require a fail-safe activity, such as those related to the operation of hospital facilities, nuclear facilities, air traffic control, rail traffic control, or any other activity where failure may lead to death, personal injury, or serious damage to the environment.

1.5. Policy Management

1.5.1. Document Organization and Management

The Security Working Group is responsible for administering this CPS.

1.5.2. Contact Details of the Entity

Table 5: Contact Details of the Entity

Name:	Security Working Group
Address:	SISP, SA Conj. Habitacional Novo Horizonte, Rua Cidade de Funchal, Achada Santo António – Praia, Cabo Verde
E-mail:	pki@sisp.cv
Site:	www.sisp.cv
Telephone:	2606310/2626317

1.5.3. Entity that ensures the Adequacy of the CPS to the Policies

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

1.5.4. Procedures for the Approval of the CPS

Validation of this CPS (and/or respective CPs) and subsequent amendments (or updates) shall be carried out by the Security Working Group. Any corrections or updates 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 the 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 Group, which is the entity responsible for approving and authorizing any corrections or amendments to this type of document.

1.6. Definitions and Acronyms

1.6.1. Definitions

Table 6: Definitions

Definitions	
Term	**Definition**
Electronic Signature	Data in electronic form which are attached to or logically associated to a data message and which serve as a method of authentication.
Advanced Electronic Signature	An electronic signature that meets the following requirements: i) Uniquely identifies the holder as the author of the document;

	ii) Affixing it to the document depends solely on the willingness of the holder; iii) It is created using means that the holder can maintain under his sole control; iv) Its connection with the document allows the detection of any supervening change in its content.
Qualified Electronic Signature	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 secure signature creation device.
Supervisory Authority	Entity responsible for accrediting and supervising the Certification Entities.
Certificate	Digital record that links signature-verification data to the signatory and confirms the identity of the holder.
Qualified Certificate	Electronic signature certificate issued by a qualified trust service provider under the laws of a particular jurisdiction.
Private Key	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	An element of the asymmetric key pairs meant to be disclosed, with which the digital signature affixed on the electronic document by the holder of the asymmetric key pair is verified, or with which an electronic document to be transmitted to the holder of the same key pair is enciphered.
Accreditation	The act whereby upon request an entity is recognized as having the right to exercise the activity of an accredited certification body.
Signature-creation Data	Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.
Signature-verification Data	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	Software or equipment device used to enable data processing for signature creation.
Secure Signature-Creation Device	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	Document prepared by electronic data processing.
Electronic Address	Identification of appropriate computer equipment to receive and store electronic documents.

1.6.2. Acronyms

Table 7: Acronyms

Acronyms	
C	*Country*
CA	*Certification Authority (the same as CE)*
CE	*Certifying Entity*
CN	*Common Name*
CP	*Certificate Policy*
CPS	*Certification Practices Statements*
CRL	*Certificate Revocation List (the same as LRC)*
DN	*Distinguished Name*
HSM	*Hardware Security Module*
LRC	*List of Revoked Certificates*
O	*Organization*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
OU	*Organization Unit*
PKI	*Public Key Infrastructure*
PKCS	*Public Key Cryptography Standards*
SHA	*Secure Hash Algorithm*
SSl/TLS	*Secure Sockets Layer / Transport Layer Security*
SSCD	*Secure Signature Creation Device*

1.6.3. Bibliographical References

- *RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List Profile, 2008;*
- *RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;*
  CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4;
- *Regulation (EU) No 910/2014;*
- *ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.*

2. Publication Responsibility and Repository

2.1. Repositories

SISP is responsible for the repository duties of SISPROOTCA02, publishing among others, information regarding the practices adopted and the status of the certificates issued (LRC).

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

- The LRC and the CPS can only be changed through well-defined processes and procedures,
- The technological platform of the repository is duly protected by the most current techniques of physical and logical security,
- The human resources who manage the platform have adequate education and training for the service in question.

2.2. Publication of Certification Information

SISP maintains a repository in a Web environment, allowing Relying Parties to perform online searches regarding revocation and other information on the status of the Certificates, 24 (twenty-four) hours a day, 7 (seven) days a week.

SISP makes available to all its Certifying Entities the following public online information at *URL* http://pki.sisp.cv to all its Certifying Entities:

- Certificates of the CEs;
- An updated copy of the CE's CPS;
- An updated electronic copy of the CEs' CPs;
- A list of the CEs linked to each Root CE;
- A list of the Revoked Certificates of the CEs (LRC);
- A list of the related Registration Entities and the addresses of the respective technical facilities in operation.

Additionally, all previous versions of the CPS of Subordinate CEs will be kept, making them available to those who request them (as long as justified), remaining, however, outside the open-access public repository.

SISP also makes available, publicly and on its website, a tool that allows holders of web certificates to test and validate the chain of trust of valid, revoked and expired certificates.

2.3. Publication Periodicity

SISP ensures that updates to this CPS and its policies will be published whenever a change needs to be made. A new LRC of SISPROOTCA02 will be published at least every three months.

2.4. Repository Access Controls

The information published by SISP will be available on the Internet, subject to access control mechanisms (read-only access). SISP has implemented logical and physical security measures to prevent unauthorized people from adding, deleting or modifying repository records.

3. Identification and Authentication

3.1. Naming

This section describes the procedures used to authenticate the entities before they are issued certificates, as well as issues regarding name disputes.

3.1.1. Types of Names

SISP guarantees the issuance of certificates containing a X.509 *Distinguished Name* (DN) defined according to RFC 5280, and issues certificates to requesters that submit documentation containing a verifiable name.

SISP will ensure, within its trust infrastructure, the non-existence of certificates that, containing the same DN, may identify distinct entities.

The unique name of these certificates is identified in their respective Certificate Policies.

3.1.2. Need for Meaningful Names

SISP shall ensure that the names used in the certificates it issues identify their users in a meaningful way. That is, it shall be ensured that the DN used is appropriate for the user in question and that the *Common Name* component of the DN represents the user in a way that is easily understood. SISPROOTCA02 ensures that the *Common Name* field in the certificate's *Subject DN* matches one of the *Subject Alternative Names*, and that it has been validated using at least one of the methods listed in section 3.2.2.4 of the *Baseline Requirements CA/B Forum.*

3.1.3. Holder Anonymity or Pseudonym

Nothing to report.

3.1.4. Name Format Interpretation

The rules used by SISP to interpret the format of the names follow what is established in RFC 5280, ensuring that all *DirectoryString* attributes of the *issuer* and *subject* fields in the certificate are encoded in a *UTF8String*, with the exception of the *country* and *serial* number attributes that are encoded in a *PrintableString*

3.1.5. Uniqueness of Names

SISP will control the existing names in order to guarantee that a certificate contains a unique DN, related to one entity only and that it is not ambiguous.

3.1.6. Trademark Recognition, Authentication and Roles

The names issued by SISP will respect registered trademarks as much as possible. SISP will deliberately not allow the use of registered names whose ownership cannot be proven by the applicant. However, it may refuse to issue certificates with registered brand names if it believes that other identification is more convenient.

3.2. Identity Validation at Initial Registration

SISPROOTCA02 is responsible for authenticating the identity of the entities applying for a certificate.

It is responsible for the safekeeping of all the documentation used to verify the identity of the certifying entity, making sure that the identity of its legal representatives is duly checked by legally recognized means, and guaranteeing sufficient powers of the representative appointed by the entity for the said issue.

The issuance of qualified certificates within the SISP's hierarchy of trust requires the SISPROOTCA02 to proceed to a rigorous process of verification of the identity of the titleholder and the related data.

3.2.1. Method of Proof of Private Key Possession

In cases where SISPROOTCA02 is not responsible for generating the key pair to be attributed to the titleholder, it should ensure prior to issuance that the titleholder is in possession of the private key corresponding to the public key included in the certificate request (CSR).
The greater the importance and type of the certificate requested, the more rigorous the method of proof should be. Moreover, this should be duly specified in the Certificate Policy at stake.

3.2.2. Identity Authentication of the Organization and Domain

The DNs issued by SISPROOTCA02 take into consideration the registered brands, not allowing the deliberate use of registered names whose ownership cannot be proven and may refuse to issue the certificate if it concludes that another identification is more appropriate.

SISPROOTCA02 verifies the authenticity of the data in one of the following ways:

a) By means of official documents issued by government entities, namely, a Certificate of Commercial Registry;
b) Authentication of the certificate request form containing the organization's data by an entity with powers to do so (Notary's office, registry office, or other equivalent);
c) From a reliable third-party database that is updated periodically (D&B, for example);
d) From a site visit by the CA itself or by an Agent on its behalf;
e) From the proof of control of the email address whenever it is included in the Distinguished Name or Subject Alternative Name;
f) By validating the right to use and control the domain name/address in the Common Name and Subject Alternative Name of the certificate. SISPROOTCA02 performs this validation using at least one of the methods described in section 3.2.2.4 of the CAB Forum Baseline Requirements.

3.2.2.1. Identity

Nothing to report.

3.2.2.2. Registered Trademarks

Nothing to report.

3.2.2.3. Country Check

Nothing to report.

3.2.2.4. Authorization Validation or Domain Control

Nothing to report.

3.2.2.5. Authentication of an IP address

Nothing to report.

3.2.2.6. Validation of the Wildcard Domain

Nothing to report.

3.2.2.7. Accuracy of Data Sources

Nothing to report.

3.2.2.8. CAA Records

Nothing to report.

3.2.3. Identity Authentication of the Individual

Verification of the holder and/or subscriber's identity is performed by the registries working group in one of the following ways:

- Through the physical presence of the natural person or an authorized representative of the legal person, and in the presence of two registry operators;
- remotely, using electronic identification means, for which the physical presence of the natural person or of an authorized representative of the legal person has been ensured prior to issuance of the qualified certificate, and which meet the requirements set out in Article 8 for the "substantial" or "high" level of assurance as described in eIDAS Regulation No. 910/2024; or
- By means of a qualified electronic signature certificate or qualified electronic seal issued under the Public Key Infrastructure of Cabo Verde (only for citizens and residents in Cabo Verde).

3.2.3.1 Identification of a Natural Person

If the holder is a natural person, the identity can be verified through:

- the Subscriber's full name
- the date and place of birth
- an identification document officially recognized by the country's authorities
- a document equivalent to the physical presence with legal probative value.

If the holder is a natural person representing a legal person:

- the Subscriber’s full name
- the date and place of birth
- an identification document officially recognized by the country’s authorities
- a document equivalent to the physical presence with legal probative value
- the legal name and identification number of the legal person
- legal evidence proving the power of representation

If the holder is a natural person and has a professional capacity:

- the Subscriber’s full name
- the date and place of birth
- an identification document officially recognized by the country's authorities
- a document equivalent to the physical presence with legal probative value
- Evidence of the occupation held
- License number issued by the professional body
- Area/Department to which he/she is assigned

3.2.3.2 Identification of a Legal Person

If the subscriber is a legal person, identity may be ascertained through:

- Identification documents and data, such as:
  - The entity’s full and legal name, e.g., certificate of commercial registration
  - Address
  - Tax Identification Number
  - Commercial Registration Number

3.2.3.3 Identification of a Device or Application

The identification must be authenticated by using one of the following provisions:

- Be officially recognized in the jurisdiction in which the subscriber/holder is registered;
- By the subscriber/holder's full name and address;
- Possessing at least one identification document containing a photograph or
- Unique legal identification number recognized by the jurisdiction where it was issued.

SISPROOTCA02 shall verify whether the applicant is entitled to obtain the certificate in question. In case of qualified web authentication certificates, SISPROOTCA02 is required to perform the verification of the name and address of the legal representative and check if the address of the entity is the one stated in the official documents or where it develops its activity.

3.2.4. Non-Verified Information on the Subscriber/Holder

The entire information included in the certificate shall be validated.

3.2.5. Validation of Authority

See sections 3.2.2 and 3.2.3.

3.2.6. Interoperability or Certification Criteria

Certificates issued by SISPROOTCA02 are executed in a hierarchy of trust. In order to ensure full interoperability between applications that use digital certificates, it is recommended to use only alphanumeric characters, without accents, spaces, underscores, minus sign, period ([a-z], [A-Z], [0-9], " ", "_", "-", ".") in X.509 directory entries.

3.3. Identification and Authentication for Key Renewal

3.3.1. Identification and Authentication for Routine Key Renewal

There is no routine key renewal. The renewal of certificates follows the procedures for authentication and initial identification where new key pairs are generated.

3.3.2. Identification and Authentication for Renewal after Revocation

If a certificate is revoked, the individual/organization will undergo the entire initial registration process in order to obtain a new certificate

3.4. Identification and Authentication for a Revocation Request

The revocation request must obey to the conditions described in detail in section 4.9.

4. Operational Requirements of the Certificate Lifecycle

4.1. Certificate Application or Request

The certificate request shall be made by filling out the proper form made available by SISP. The signature on the form may be handwritten or digital, using a qualified signature.

4.1.1. Who Can Apply for a Certificate

The certificate application may be made by:

- The legal representative of the holder, duly mandated for that purpose when the holder is a legal person or
- A representative of SISP.

4.1.2. Registration Process and Responsibilities

Once the documentation is received, the process of validating its authenticity and the identity of the holder begins. This process is performed by two registry administrators. All applications accepted or rejected will be retained and preserved for a period of 7 years in accordance with section 5.5.2 of the CA Browser Forum.
SISPROOTCA02 has no external registration entity.

4.2. Certificate Application Processing

4.2.1. Performance of Identification and Authentication Duties

SISPROOTCA02 shall, soon after receiving the certificate issuance request form and the information deemed necessary to issue it, proceed to validate all the information made available in order to verify the authenticity of the data contained (see section 3.2) therein.

4.2.2. Approval or Rejection of Certificate Requests

SISPROOTCA02 only accepts the certificate issuing request if all data contained in the application are authentic, in which case the request is approved.

In case the information contained is not true or is incomplete, the CE rejects the certificate issuing request and informs the person responsible for the request accordingly.

SISPROOTCA02 does not issue certificates for internal domains.

4.2.3. Deadline for Issuing the Certificate

Nothing to report.

4.3. Certificate Issuance

4.3.1. CA's Actions during Certificate Issuance

The certificate issuance is performed in the auditor's presence by two members of the working groups, through authentication (card + PIN), being one of them responsible for entering the data and the other for validating and approving the request.

The issuance of the certificate results from the interaction with the cryptographic module (HSM), by following a specific procedure, and in accordance with the respective certificate policy. The certificate issued and signed by the hierarchically superior Certification Authority is imported in the corresponding SubCA and the first LRC is generated.

The validity of the certificate starts upon issuance.

4.3.2. Notification to the Subscriber/Holder by the CA that Issued the Certificate

Nothing to report.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The certificate is considered accepted after the certificate issuing and acceptance form is signed by the representative(s) of the subordinate entity.

It should be noted that, before the certificate is made available to the representatives and consequently all the functionalities required for the use of the private key and certificate are made available to them, it is necessary to make sure that the titleholder is duly aware of:

- Its rights and responsibilities;
- The certificate's functionalities and content.

The certificate and its conditions of use are formally accepted by signing the Certificate Receipt Form.

4.4.2. Publication of the Certificate by the CA

SISPROOTCA02 does not publish the list of certificates issued.

4.4.3. Notification of Certificate Issuance to Other Entities

SISPROOTCA02 does not notify other entities about its certificate issuing activity.

4.5. Certificate and Key Pair Usage

4.5.1. Usage of Certificate and Key Pair by Subscriber/Holder

The holder must use his private key and ensure the protection of this key as provided for in this CPS.
Its use is only allowed:

- To whomever is designated as the responsible party or representative of the requesting entity in the application form;
- Upon acceptance of the terms and conditions of use, as defined in **section 4.4.1**;
- While the certificate remains valid and is not in the LRC of SISPROOTCA02.

4.5.2. Use of Certificate and Public Key by Relying Parties

Relying parties should use applications/software that conform to the x.509 standard and should trust the certificate only if it is valid. SISPROOTCA02 provides services that allow to validate the certificate status at all times and in real time, namely: OCSP and LRC.

4.6. Certificate Renewal

Certificate renewal is the process of issuing a new certificate with a new key pair. The data and functions of the previous request can be used as long as they remain unchanged.

4.6.1. Circumstances for Certificate Renewal

Nothing to report.

4.6.2. Who Can Apply for Certificate Renewal

Nothing to report.

4.6.3. Processing Certificate Renewal Requests

Nothing to report.

4.6.4. Notification of New Certificate Issuance to Subscriber/Holder

Nothing to report.

4.6.5. Conduct Constituting Acceptance of Certificate Renewal

Nothing to report.

4.6.6. Publication of Certificate Renewal by the CA

Nothing to report.

4.6.7. Notification of Certificate Renewal by the CA to Other Entities

Nothing to report.

4.7. Certificate Re-Keying

4.7.1. Circumstances for Certificate Re-Keying

SISPROOTCA02 does not support the Re-Keying process of certificates.

4.7.2. Who Can Request Certification of a New Public Key

Nothing to report.

4.7.3. Processing Re-Keying Requests

Nothing to report.

4.7.4. Notification of New Certificate Issuance to Subscriber

Nothing to report.

4.7.5. Conduct Constituting Acceptance of Re-Keyed Certificate

Nothing to report.

4.7.6. Publication of Re-Keyed Certificate by the CA

Nothing to report.

4.7.7. Notification of Re-Keyed Certificate by the CA to Other Entities

Nothing to report.

4.8. Certificate Modification

Certificate modification is a process by which a certificate is issued to a subscriber/holder or sponsor while maintaining the same keys, with changes only to the certificate information.
Certificate modification is not supported by SISPROOTCA02.

4.8.1. Circumstances for Certificate Amendment or Modification

Nothing to report.

4.8.2. Who Can Request Certificate Modification

Nothing to report.

4.8.3. Processing the Certificate Modification Request

Nothing to report.

4.8.4. Notification of New Certificate Issuance to Subscriber

Nothing to report.

4.8.5. Conduct Constituting Acceptance of the Modified Certificate

Nothing to report.

4.8.6. Publication of the Modified Certificate by the CA

Nothing to report.

4.8.7. Notification of the Modified Certificate by the CA to Other Entities

Nothing to report.

4.9. Certificate Revocation and Suspension

Certificate revocation is a procedure through which the certificate ceases to be valid before the end of its validity period, so losing its operability. After being revoked, certificates cease to be valid.

4.9.1. Reasons for Revocation

SISPROOTCA02 shall revoke the certificate within a maximum of 7 days if one or more of the following situations occurs:

- The SubCA requests in writing the revocation of the certificate;
- A SubCA notifies SISP Root CA2 (Issuing CA) that the initial certificate request was not authorized and does not guarantee authorization on a retroactive basis;
- The Issuing CA obtains evidence that the Private Key of the SubCA corresponding to the Public Key in the certificate has been compromised or no longer meets the requirements of Section 6.1.5 and Section 6.1.6;
- The Issuing CA has evidence that the certificate was incorrectly used;
- The Issuing CA is informed that the Certificate has not been issued accordingly or the SubCA has not complied with this document or the applicable Certificate Policy;
- The Issuing CA determines that one or more of the information appearing on the Certificate is inaccurate or untrue;
- The Issuing CA or the SubCA ceased operations and did not create conditions for another CA to provide revocation support for the Certificate;
- Revocation is required under the Issuing CA Certification Policy.

4.9.2. Who Can Request the Revocation

The following entities are entitled to submit the revocation request:

- The Certifying Entity;
- SISP S.A.;
- The Supervisory Authority;
- A relying party, whenever it demonstrates that the certificate was used for purposes other than those foreseen.

4.9.3. Procedures for the Revocation Request

All revocation requests must be addressed to SISP S.A. in writing, through the web portal available at https://pki.sisp.cv/ or by digitally signed e-mail, in the revocation request form made available for that purpose.

The request is processed within 24 hours following receipt of the request. Before processing the request, SISPROOTCA02 will verify the identity and authenticity of the requesting entity and keep a record of the request after its execution.

4.9.4. Grace Period of the Revocation Request

The titleholder may request the revocation of the certificate at any time. However, in case of suspicion of compromise of the private key, it is recommended that the request be made within 24 hours after detection.

4.9.5. Time within which Revocation Request must be processed by the CA

The revocation request must be immediately handled and processed and this shall, under no circumstances, exceed **24** (twenty-four) hours.

4.9.6. Revocation Checking Requirements for Relying Parties

Before using a certificate, the relying parties are responsible for checking the state of the certificate through the LRC or an online certificate status server (OCSP).

4.9.7. LRC Issuance Frequency

SISPROOTCA02 shall publish a new LRC in the repository whenever there is a revocation. When there is no change in the validity status of the certificates, i.e. if no revocation has occurred, SISPROOTCA02 shall publish a new LRC every **60 minutes**.

The LRC can be found in the following repository: http://crl.sisp.cv/sisprootca02.crl.

4.9.8. Maximum Period between LRC Issuance and Publication

The maximum period between issuance and publication of the LRC should not exceed 3 hours.

4.9.9. Online Status/Revocation Checking Availability

SISPROOTCA02 works offline and does not have an online certificate status validation service, OCSP.

4.9.10. Online Revocation Checking Requirements

Before making use of a certificate, the relying parties have the responsibility to verify the status of all the certificates through the LRC.

The LRC can be accessed at https://pki.sisp.cv/document_repository which is available 24 hours a day, 7 days a week, except during periods of scheduled maintenance downtime when relying parties will be notified accordingly.

The expiration of a certificate occurs when its validity period expires or is revoked.

4.9.11. Other Forms Available for Disseminating the Revocation

Nothing to report.

4.9.12. Special Requirements regarding Private Key Compromise

Complementarily to the reasons mentioned in section 4.9.1 of this CPS (Certification Practices Statement), the parties may use the pki@sisp.cv email to report the compromise or suspicion of compromise of the private key of the acquired certificates.

4.9.13. Circumstances for Suspension

Nothing to report.

4.9.14. Who Can Request Suspension

Nothing to report.

4.9.15. Procedures for a Suspension Request

Nothing to report.

4.9.16. Limits of the Suspension Request

Nothing to report.

4.10. Certificate Status Services

4.10.1. Operational Features

The status of issued certificates is publicly available via LRC and the OCSP service.

4.10.2. Service Availability

The certificate status service is available 24 hours a day, 7 days a week. If a certificate is revoked, it shall not remain on the LRC after the expiration date.

4.10.3. Optional Resources

No stipulation.

4.11. End of Subscription

The termination of a certificate signature occurs when the validity period expires or the certificate is revoked as set forth in RFC 3647.

4.12. Key Custody and Recovery

4.12.1. Policies and Practices of Key Custody and Recovery

SISP retains the private key of SISP ROOT CA2 and SISP QWAC and stores them in a secure environment.

The keys are encrypted and stored in an HSM and cannot be transferred to another device. SISP has a backup copy of the keys that are stored in a safe place with the same security level as the originals.

4.12.2. Policies and Practices of Session Key Encapsulation and Retrieval

See section 4.12.1

5. Physical Security, Management and Operational Controls

SISP has implemented several rules and policies focusing on physical, procedural and human controls, which support the security requirements contained in this CPS.

These rules and policies follow the best practices recommended by the main international standards in terms of information security, namely ISO 27001.

5.1. Physical Security Checks

5.1.1. Physical Location and Type of Construction

SISP's PKI facilities were designed to provide an environment capable of controlling and auditing access to certification systems, being physically protected from unauthorized access, damage or interference. The architecture uses the concept of in-depth defense, that is, by security levels, ensuring that access to a higher security level is only possible when the previous level has been reached.

5.1.2. Physical Access to the Premises

The SISP PKI systems are protected by a minimum of 4 hierarchical physical security levels, ensuring that access to a higher security level is only possible when the necessary privileges for the immediately preceding level have previously been achieved.
Sensitive operational activities of the CE, creation and storage of cryptographic material, any activities within the lifecycle of the certification process such as authentication, verification, and issuance take place within the strictest high security zone. Physical accesses are automatically logged and recorded for auditing purposes.

5.1.3. Energy and Air Conditioning

SISP's PKI environment has redundant equipment, which ensures 24 hour/7 day operating conditions of:

- Power supply ensuring continuous uninterruptible power supply with enough power to maintain the power grid autonomously during periods of power failure and to protect the equipment against electrical fluctuations that could damage it (redundant equipment consists of uninterruptible power supply batteries and diesel electricity generators);
- Refrigeration/ventilation/air conditioning that control the temperature and humidity levels, guaranteeing adequate conditions for the correct functioning of all the electronic and mechanical equipment present inside the environment.

5.1.4. Exposure to Water

Nothing to report.

5.1.5. Fire Prevention and Protection

The SISP PKI environment has in place the necessary mechanisms to prevent and extinguish fires or other incidents derived from flames or smoke. These mechanisms comply with the existing regulations:

- Fire detection and fire alarm systems are installed on the various physical security levels;
- Fixed and mobile fire extinguishing equipment are available, placed in strategic and easily accessible locations so that they can be quickly used at the start of a fire and successfully extinguished;
- Well-defined emergency procedures in case of fire.

5.1.6. Safeguarding of Storage Media

All sensitive information media are stored in security vaults and cabinets within the high security zone, as well as in a separate environment outside the building with appropriate physical and logical access controls to restrict access to authorized members of the Working Groups only.

5.1.7. Waste Disposal

Documents and paper materials that contain sensitive information are shredded prior to disposal. It is guaranteed that it is not possible to recover any information from the information supports used to store or transmit sensitive information before they are eliminated. Cryptographic equipment or physical logical access keys are physically destroyed or follow the destruction recommendations of the respective manufacturer prior to their elimination.

Other storage equipment (hard drives, tapes, etc.) are properly cleaned so that no information can be retrieved.

5.1.8. External (alternative) Facilities for Security Recover

Alternative facilities have the same safety levels as the main facility.

5.2. Process Safety Measures

The activity of a Certifying Entity (hereinafter referred to as CE) depends on the coordinated and complementary intervention of a wide range of human resources, namely because:

- Given the safety requirements inherent to the operation of a CE, it is vital to ensure an adequate segregation of responsibilities, which minimizes the individual importance of each of the intervening parties;
- It is necessary to guarantee that the CE can only be subject to denial-of-service type attacks by means of the collusion of a significant number of actors;
- When the same entity holds several CEs of different security levels or hierarchy, it is at times desirable that the human resources associated with a CE do not accumulate functions (or at least the same ones) in a different CE.

Based on the above, this section describes the requirements necessary to recognize the trust roles and responsibilities associated with each of these roles. This section also includes the separation of duties, when it comes to the roles that cannot be performed by the same individuals.

5.2.1. Working Groups

Authenticated persons are defined as all employees, suppliers and consultants who have access to or control cryptographic or authentication operations.

The PKI of SISP established that the trust roles were grouped into six different categories (corresponding to five different Working Groups) in order to ensure that sensitive operations are performed by different authenticated persons, possibly belonging to different Working Groups, so ensuring that there are two members in each group.

5.2.1.1. Audit Group

It is responsible for performing the internal audit of all relevant and necessary actions to ensure the operability of the CE.

5.2.1.2. Security Group

The Security Administration Working Group is responsible for proposing, managing, and implementing all CE policies, ensuring that they are up-to-date and that all information that is indispensable for the operation and auditing of the CE is available over time. The Security Administration Working Group also assumes the HSM Operation role.

5.2.1.3. Systems Administration Group

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

5.2.1.4. Registration Group

The Registration Administration Work Group is responsible for executing the routine tasks that are essential for the CE's good functioning and operability, as well as all incidents that occur. It is also this group's mission to operate the CE with regards to certificate issuing, suspending, and revoking.

This group's responsibilities consist of issuing, suspending, and revoking certificates.

5.2.1.5. Management Group

It is responsible for appointing the members of the remaining groups and for making critical level decisions for the CE. This group must comprise a minimum of four (4) members.

5.2.2. Number of Persons required per Task

Strict control procedures are in place that require the division of responsibilities based on the specifics of each Working Group and to ensure that sensitive tasks can only be performed by a multiple set of authenticated people.

The internal control procedures were elaborated to guarantee a minimum of 2 authenticated individuals to have physical or logical access to the security equipment.

5.2.3. Identification and Authentication for each Function

See section 5.2.1.5.

5.2.4. Duties that Require the Separation of Responsibilities

The following matrix defines the incompatibilities (marked by X) between belonging to the group/subgroup identified in the left column and belonging to the group/subgroup identified in the first row, in the context of this CE:

Table 8: Duties that require the separation of responsibilities

Working Group	Incompatible with				
	(a)	(b)	(c)	(d)	(e)
Security Administration (a)		X	X	X	
Systems Administration (b)	X		X	X	
Registration Administration (c)	X	X		X	
Audit (d)	X	X	X		X
Management (e)				X	

5.3. Staff Security Measures

5.3.1. Requirements Regarding Qualifications, Experience, Background and Accreditation

Each staff member performing trust functions at the PKI of SISP must meet the following requirements:

- Have been formally appointed to the position to be performed;
- Provide evidence of the background, qualifications and experience necessary to perform his duties;
- Have received adequate education and training to perform the respective function;
- Guarantee confidentiality as to sensitive information about the CE or identification data of the titleholders;
- Guarantee knowledge of the terms and conditions for performing the respective role, and
- Guarantee that he/she does not perform any other duties that may conflict with its responsibilities in the CE's activities.

5.3.2. Background Checking Procedures

Background checks stem from the credentialing process of the individuals nominated to hold positions in any of the positions of trust. Background checks include:

- Confirmation of identification, using documentation issued by reliable sources and,
- Criminal record checks.

5.3.3. Education and Training Requirements

The members of the Working Groups are provided with adequate education and training in order to carry out their tasks satisfactorily and competently.
The members of the Working Groups are additionally subject to an education and training plan covering the following topics:

- Digital Certification and Public Key Infrastructures;
- General concepts on information security;
- Specific training for their role within the Working Group;
- Operational functioning of the PKI of SISP;
- Certificate Policy and Certification Practices Statement;
- Disaster Recovery;
- Procedures for business continuity and,
- Basic legal aspects related to the provision of certification services.

5.3.4. Frequency and Requirements for Recycling Schemes

Whenever necessary, additional training and education will be provided to the Working Group members so as to ensure the desired level of professionalism for the competent and satisfactory execution of their responsibilities. In particular,

- Whenever there is any technological change, introduction of new tools or modification of procedures, the appropriate training shall be carried out for all staff assigned to the PKI of SISP;
- Whenever changes are introduced in the Certificate Policies or Certification Practices Statement, refresher sessions shall be held for the SISP PKI staff.

5.3.5. Frequency and Sequence of Job Rotation

Nothing to report.

5.3.6. Sanctions for Unauthorized Actions

Unauthorized actions are considered to be all actions that disregard the Certification Practices Statement and the Certificate Policies, whether performed deliberately or through negligence.
Sanctions are applied according to SISP PKI rules and national security laws to all individuals who perform unauthorized actions or make unauthorized use of the systems.

5.3.7. Requirements for Service Providers

Consultants or independent service providers are allowed access to the high security zone as long as they are always accompanied and directly supervised by the Working Group members and their access is registered in the proper Presence Book.

5.3.8. Documentation provided to Staff

The members of the Working Groups are provided with all the appropriate information so that they can carry out their tasks in a competent and satisfactory manner.

5.4. Security Audit Procedures

5.4.1. Type of Events Recorded

All significant auditable events must be recorded, in particular the following:

- Access attempts (with or without success) to request, generate, sign, issue or revoke certificate keys;
- Access attempts (with or without success) to create, modify or delete information on the certificate subscribers;
- Access attempts (with and without success) and changes to the security parameters of the operating system;
- Issuing and publishing LRCs;
- Starting and stopping applications;
- Access attempts (with and without success) to login and logout;
- Access attempts (with and without success) to create, modify, delete system accounts;
- Data backups, recovery or archiving;
- Software and hardware changes or updates;
- Systems maintenance;
- Operations performed by members of the Working Groups;
- Changes in Human Resources;
- Access attempts (with or without success) to the facilities by authorized or unauthorized personnel;
- The key generation ceremony and systems involved therein, such as application servers, database and operating system.

5.4.2. Record Audit Frequency

The records are analyzed and reviewed on a daily basis and in an automated manner, producing alerts to the Audit working group and whenever there are suspicions or abnormal activities or threats of any kind. Actions taken, based on the information in the records are also documented.

5.4.3. Audit Record Retention Period

The records are available online during the validity period of the certification, following which they are archived as described in section 6.5.

5.4.4. Protection of Audit Records

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

The records are protected by auditable electronic mechanisms, in order to detect and prevent the occurrence of attempts at modification, removal or other schemes of unauthorized manipulation of the data.

The backup copies of the SISP PKI records are stored in a safe place and in vaults that comply with the EN 1143 standard.
The destruction of an audit file can only be made after express authorization of the Management Group and executed in the presence of at least two elements, a security element and an audit element, and this act shall be recorded in the Audit log.

5.4.5. Procedures for Backing up Records

Regular backup copies of the records are created on high-capacity storage systems, namely tape and storage.

5.4.6. Data Collection Systems (internal/external)

The audit record collection and keeping process consists of a combination of automatic and manual processes performed by the operating systems, the SISP PKI applications and the staff that operates them. All audit records are stored in the SISP's internal PKI systems.

5.4.7. Notification of Event Causing Agents

Auditable events are recorded in the audit system and stored securely, without notification to the subject causing the event to occur.

5.4.8. Vulnerability Assessment

Auditable records are regularly reviewed in order to minimize and eliminate potential attempts to breach system security. Four intrusion tests are performed per year so as to check and assess vulnerabilities. The result of the analysis is reported to SISP's PKI Management Group to review and approve an implementation plan and correction of the vulnerabilities detected.

5.5. Record File

5.5.1. Type of Data Archived

All auditable data is archived (as indicated in section 6.4.1), as well as information on certificate requests and documentation supporting the lifecycle of the various operations.
The information and events that are recorded and archived are:

- The audit records specified in item 6.4.1 of this CPS;
- The backup copies of the systems that make up the SISP's PKI infrastructure;
- All the documentation relative to the lifecycle of the certificates, namely:
    - Procedures for issuing and revoking certificates of service;
    - Forms for the issue and receipt of certificates of service;
- Confidentiality agreements;
- Protocols established with the Subscribing Entities;
- Contracts established between the PKI of SISP and other entities - only made available to those who request to see them, after previous evaluation and approval of the request;
- Authorizations for access to information systems;
- Access to existing artefacts in the custodies.

5.5.2. Retention Period in Archive

Data subject to archiving is retained for the period of time defined by the national legislation or for the period of 7 years as recommended by the CAB Forum, whichever is longer.

5.5.3. Archive Protection

The file is protected in such a way that:

- Only authorized members of the Working Groups may consult and access the file;
- Archive is protected against any modification or attempt to remove it;
- Archive is protected against deterioration of the media on which it is stored, through periodic migration to new media;
- Archive is protected against the obsolescence of hardware, operating systems and other software, by preserving the hardware, operating systems and other software that becomes part of the archive itself, in order to allow timeless access and use of the stored records;
- Files are stored securely in secure offsite environments in accordance with the Data Retention Policy. Backups of the PKI of SISP are stored in secure locations and in vaults that comply with EN 1143 standard.

5.5.4. Procedures for Archive Backup

Files are backed up incrementally or completely and stored in WORM (Write Once Read Many) devices.

5.5.5. Requirements for Chronological Validation of Records

Some of the file entries contain date and time information, which is provided by an accurate time reference service.

5.5.6. Archive Data Collection System (Internal/External)

Archive data collection systems are internal.

5.5.7. Procedures for Retrieving and Checking Archived Information

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

Integrity verifications of the electronic archives (backup copies) are carried out automatically when they are created; in case of errors or unexpected behavior, a new archive must be made.

5.6. Key Renewal

Nothing to report.

5.7. Recovery in the Event of Disaster or Compromise

This section describes the requirements related to notification and recovery procedures in the event of a disaster or compromise.

5.7.1. Procedures in Case of Incident or Compromise

Security copies of the CEs' private keys (generated and maintained according to section 6.2.3.1) and archived records (section 5.5.1) are stored in external secure environments and available in case of disaster or compromise. In the event that the SISPROOTCA02 CA private key is compromised, the latter will take the following actions:

- Proceed to its immediate revocation;
- Revoke all certificates depending on it;
- Inform all certificate titleholders and known third parties;
- Inform all the Entities that comprise the PKI of SISP.

5.7.2. Corruption of Computing Resources, Software and/or Data

In case computer resources, software and/or data are corrupted or corruption is suspected, backup copies of the CE's private key and archived records may be obtained to verify the integrity of the original data.

If it is confirmed that computer resources, software and/or data are corrupted, appropriate incident response actions should be taken. The incident response may include restoring the corrupted equipment/data, using similar equipment and/or recovering backups and archived records. Until safe conditions are restored, the CE shall suspend its services and notify all entities involved. If this situation is verified as having affected issued certificates, the titleholders of these certificates shall be notified and the respective certificates revoked.

5.7.3. Procedures in Case of Compromise of the Entity's Private Key

In the event that the CE's private key is compromised or is suspected of being compromised, appropriate incident response measures should be taken. Responses to such incident may include:

- Informing the Mozilla Root Repository and other repositories with which the PKI of SISP has established relations;
- Revocation of the CE certificate and of all certificates issued in the "branch" of the CE's hierarchy of trust;
- Notification of all titleholders of certificates issued in the "branch" of the CE's hierarchy of trust;
- Generation of a new key pair for the CE and inclusion in the various systems/browsers;
- Renewal of all certificates issued in the "branch" of the CE's hierarchy of trust.

5.7.4. Business Continuity Capacity in Case of Disaster

The PKI of SISP has the computing resources, software, backup copies and records stored in its secondary security facilities, necessary to restore or recover essential operations (issuance and revocation of certificates, with the publication of revocation information) based on procedures defined in the Contingency Plan, after a natural disaster or other event.

5.8. Procedures in Case of CE or RE Termination

In case of cessation of activity as a Certification service provider, the CE performs the procedures foreseen in the SISP PKI Plan on the Termination of Activity, namely:

- Inform the Mozilla Root Repository and other repositories with which the PKI of SISP has established relationships;
- Revocation of all certificates;
- Guarantee the transfer, for its retention by another organization, of all information related to the CE's activity;

- Proceed with the destruction of all classified information or guarantee its transfer for its retention by another organization.

In case of changes in the body/structure responsible for managing the CE's activity, the latter should inform the Supervisory Authority and the IPC-CV's Managing Council of such fact.

6. Technical Security Checks

This section defines the security measures implemented by the PKI of SISP for the CEs in order to protect cryptographic keys generated by them and respective activation data. The security level assigned to key maintenance shall be maximum so that private keys and secure keys, as well as activation data, are always protected and only accessed by duly authorized people.

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The generation of the CE key pairs is processed according to the requirements and algorithms defined in this policy.

The generation of the CE's cryptographic keys is done by a Working Group comprising duly authorized members, in a ceremony planned and audited in accordance with the written procedures for the operations to be carried out. All key generation ceremonies are registered, dated, and signed by the elements involved in the Working Group.

The cryptographic hardware used for generating the CE's keys complies with the requirements of FIPS 140-2 level 3 and/or Common Criteria EAL 4+ and performs key maintenance, storage, and all operations involving cryptographic keys using hardware exclusively. Access to critical keys is protected by security policies, division of roles among the Working Groups, as well as through limited user access rules. The backup copies of cryptographic keys are made using only hardware, allowing these copies to be properly audited and that, in the event of data loss, a full and secure recovery of the keys can be achieved.

The private key for the natural person and the legal person certificates are generated by the CEs using cryptographic hardware that complies with the requisites of FIPS 140-1 level 3 and/or Common Criteria EAL 4+.

The CE operates in online mode.

6.1.2. Delivery of the Private Key to the Titleholder

Nothing to report.

6.1.3. Delivery of the Public Key to the Certificate Issuer

As per the procedures indicated in section 4.4.1.

6.1.4. Delivery of the CE's Public Key to the Relying Parties

As stipulated in section 2.2.

6.1.5. Key Sizes

The length of the key pairs shall be large enough to prevent possible cryptanalysis attacks that discover the private key corresponding to the key pair during its period of use. The size of the keys follows the recommendations of the ETSI TS 119 312 - Electronic Signatures and Infrastructures, Cryptographic Suite standard, and is the following:

- 4096 bits RSA for the CE's key,
- 4096 bits RSA for the keys associated to the final users' certificates issued by the CE, with signature algorithm sha512RSA.

6.1.6. Generation of Public Key Parameters and Quality Checking

The key generation process is done directly on the cryptographic module (HSM) and the certificates are signed by SISPROOTCA02, which works offline.

The CE keys are generated based on the use of random/pseudo-random processes described in ANSI X9.17 (Annex C), as stipulated in PKCS#11.

6.1.7. Purposes of the Keys (*"Key Usage" X.509 V3 field*)

As stipulated in section 1.4.1.

6.2. Private Key Protection and Cryptographic Module Features

This section considers the requirements for the protection of private keys and the CE's cryptographic modules. The PKI of SISP implemented a combination of physical and logical controls and procedures, properly documented, in order to ensure confidentiality and integrity of the CE's private keys.

6.2.1. Standards and Security Measures for the Cryptographic Module

For the generation of the key pairs of the CE, as well as for the storage of private keys, the PKI of SISP uses a cryptographic module in hardware that complies with the following standards:

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

6.2.2. Multi-Personal (N of M) Control for the Private Key

The multi-personal control is only used for CE keys since the certificate's private key is under the exclusive control of its titleholder.

The PKI of SISP has implemented a set of mechanisms and techniques that require the participation of several Working Group members to perform sensitive cryptographic operations in the CE.

All operations are performed with a minimum of two people in qualified duties within the entity and in a separate task.

In practice, at least two people (N=2) are employed in the various functions out of the total set of people with assigned functions within the entity (M=staff).

The private keys of the PKI of SISP are held by more than one element. It is activated by initializing the CE software through a combination of HSM operators and administrators. This is the only method of activating the private key.

6.2.3. Private Key Retention (*Key Escrow*)

SISP only retains its private key.

The CE's private keys are stored in an HSM, being backed up using a direct hardware to hardware connection with two-factor authentication and by representatives of different Working Groups.

The security hardware with the backup copy of the CE's private key is stored in a secure vault in secondary secure facilities, and accessible only to authorized members of the Working Groups. The security copy of the CE's private key can be recovered in case of malfunction of the original key. The key recovery ceremony uses the same two-factor and multi-person authentication mechanisms that were used in the backup copy ceremony.

6.2.4. Backup Copy of the Private Key

The private key of the CEs has at least one backup copy, with the same security level as the original key.

6.2.5. Private Key Archive

The CE's private keys, the target of backup copies, are stored as identified in section 6.2.3.

6.2.6. Transferring the Private Key to/from the Cryptographic Module

The CE's private keys are not extractable from the FIPS 140-2 level 3 cryptographic token.

If a backup copy of the CEs' private keys is made to another cryptographic token, this copy is made directly hardware to hardware, ensuring the transport of keys between modules in an encrypted transmission.

6.2.7. Storing the Private Key in the Cryptographic Module

The CEs' private keys are stored in encrypted form in the cryptographic hardware modules, as described in section 6.2.3.

6.2.8. Private Key Activation

SISPROOTCA02 is an online Certification Authority whose private key is activated when the CE system is turned on. This activation takes effect when HSM administrators perform authentication in the cryptographic module, with two-factor authentication required. At least two people must be authenticated to activate the private key. Once the key is activated, it will remain so until the deactivation process is performed.

6.2.9. Private Key Deactivation

The CE's private key is deactivated when the CE's system is shut down. Once deactivated, it will remain inactive until the activation process is performed.

6.2.10. Destruction of the Private Key

The CE's private keys (including backup copies) are erased/destroyed in a duly identified and audited procedure at least 30 days after the end of their validity date (or if revoked before this period).

The PKI of SISP destroys the private keys, guaranteeing that no residues remain that might allow their reconstruction. To that end, it uses the formatting function (zero initialization) made available by the cryptographic hardware or other appropriate means, in order to guarantee the total destruction of the CE's private keys.

6.2.11. Capabilities of the Cryptographic Module

As described in section 6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archive

A backup copy of all the CE's public keys is made by the members of the Working Group and remains stored after the expiration of the corresponding certificates to verify the signatures generated during their validity period.

6.3.2. Validity Period of the Certificate and Keys

The period to use the keys is determined by the certificate's validity period and, therefore, after the certificate expires the keys can no longer be used, originating the permanent cessation of their operability and of the use for which they were meant.

As a consequence, the validity of the various types of certificates and the period in which they must be renewed is as follows:

- The certificate of the subordinate CE's of the SISP has a validity of 6 years, being used to sign certificates during its first 3 years of validity and reissued after the 3rd year of validity;
- The OCSP (Online Certificate Status Protocol) certificates have a validity of 5 years and 4 months, being used during their first four years of validity and reissued after the fourth year of validity;
- End user certificates (SSL EV) are valid for a minimum of one year and a maximum of two years.

6.4. Activation Data

6.4.1. Generation and Installation of Activation Data

The activation data needed for the use of the CE's private key is divided into several parts (stored in PED keys - small digital identification tokens with smartcard format - identifying the different roles in accessing the HSM), being the responsibility of different members of the Working Group. The distinct parts are generated as established in the key generation process/ceremony and comply with the requirements defined by FIPS 140-2 level 3 standard.

6.4.2. Protection of the Activation Data

The activation data of the private keys are stored in safes in a secure location.

6.4.3. Other Aspects of the Activation Data

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

6.5. Computer Security Checks

6.5.1. Specific Technical Requirements

Access to the CE's servers is restricted to the Working Group members with a valid reason for that access. The CEs have online operation, and the requests for issuing certificates are made from the RA operation module. The CEs and the RA Management have protection devices, namely a firewall, which meets the necessary requirements for the identification, authentication, access control, administration, audits, reuse, responsibility, and service recovery and information exchange.

6.5.2. Computer Security Level

The various systems and products employed by the CEs are reliable and protected against modification. The hardware cryptographic module of the Sub CA's meets the EAL 4+ Common Criteria for Information Technology Security Evaluation and/or FIPS 140-2 level 3.

6.6. Lifecycle of Technical Safety Measures

6.6.1. System Development Measures

Applications are developed and implemented by third parties according to their system development and change management rules.

Auditable methodology is provided that allows to verify that the CE's software has not been changed before its first use. All configuration and software changes are performed and audited by members of the PKI Working Groups of SISP.

6.6.2. Security Management Measures

All SISP's PKI systems are installed in a High Security Zone. Through the controls installed, it is possible to ensure the identification, authentication and management of all accesses.

6.6.3. Lifecycle of Security Measures

The updating and maintenance operations of the products and systems of the CEs follow the same control as the original equipment and are installed by the members of the Working Group with adequate training, following the procedures defined for that purpose.

6.7. Network Security Checks

The CEs have protection devices, namely firewall systems, and comply with the requirements for the identification, authentication, access control, administration, audits, reuse, responsibility and recovery of services and information exchange. Accordingly, the PKI of SISP has assured that the set of controls implemented are in compliance with all the network security requirements contained in the "CAB/Browser Forum - Network and Certificate System Security Requirements*".*

6.8. Chronological Validation (*Time-Stamping*)

Certificates, LRC's and other entries in the database always contain information about the date and time of that entry. These entries are digitally signed by a certificate issued for this purpose. The entire infrastructure has time synchronized by an NTP with an atomic clock and three alternative UTC sources:

- United States Naval Observatory (USNO), Washington DC, USA
- Royal Observatory of Belgium (ROB), Brussels, Belgium
- Real Observatório de La Armada (ROA), Madrid, Espanha

7. Certificate Profiles, LRC and OCSP

The certificate profiles issued by SISPROOTCA02 are in accordance with the recommendation of ITU.T X.509 version 3 and meet the following standards

- ETSI EN 319 401 – *General Policy Requirements for Trust Service Providers* and others related to the provision of qualified trust services;
- *CAB Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*
- *EU Regulation No.910/2014*
- National Legislation

The certificate profiles can be found in the Certificate Policy documents associated with this CPS.

7.1. Certificate Profile

7.1.1. Version Number

The "version" field of the certificate describes the version used in encoding the certificate. In this profile, the version used is 3 (three).

7.1.2. Certificate Extensions

The components and extensions defined for X.509 v3 certificates provide methods for associating attributes to users or public keys, as well as for managing the certification hierarchy.

7.1.3. OID of the Algorithm

The certificate's "*signatureAlgorithm*" field contains the OID of the cryptographic algorithm used by the CE to sign the certificate: 1.2.840.113549.1.1.13 (sha512WithRSAEncryption*).*

7.1.4. Name Format

As defined in section 3.1.

7.1.5. Name Conditioning

SISP may include conditionals on names, in the "nameConstraints" field, whenever justified.

7.1.6. OID of the Certificate Policy

Nothing to report.

7.1.7. Using the Policy Constraint Extension

Nothing to report.

7.1.8. Syntax and Semantics of Policy Qualifiers

Nothing to report.

7.1.9. Processing Semantics for the Critical Extension *Certificate Policies*

Nothing to report.

7.2. LRC Profile

The LRC is a list with temporal identification of the revoked certificates, signed by the CE and made freely available in a public repository. Each revoked certificate is identified in the LRC by its serial number.

When an application uses a certificate (for example, to verify the digital signature of a remote user), the application verifies the signature and validity of the certificate, obtains the most recent LRC, and checks that the certificate's serial number is not part of it. It should be noted that a CE issues a new LRC on a regular periodic basis.

7.2.1. Version Number (s)

The LRC "version" field describes the version used in encoding the LRC. In this profile, the version used is 3 (three).

7.2.2. *LRC and LRC Extensions*

The components and extensions defined for X.509 v3 certificates provide methods for associating attributes to users or public keys, as well as for managing the certification hierarchy.

7.3. OCSP Profile

7.3.1. Version Number (s)

Nothing to report.

7.3.2. OCSP Extensions

Nothing to report.

8. Compliance Audit and Other Assessments

8.1. Evaluation Frequencies and Circumstances

SISP conducts regular audits, at least once a year, and conformity assessments to ensure compliance of the Certifying Entities within its hierarchy of trust with the applicable national legislation, as well as with international standards.

The audits will be carried out by an external entity registered and accredited for this purpose, and the results will be communicated to the supervisory entity.

8.2. Auditor Identity and Qualifications

The audits will be performed by an auditor accredited and qualified to perform trust service provider audits in accordance with the requirements set forth in section 8.4 of the CA-Browser Forum BR 1.8.4.

8.3. Relationship of the Auditor with the Audited Entity

The Auditor is an independent figure and does not act partially or discriminatorily in relation to the audited entity. The absence of any contractual link is ensured in the relationship between the Auditor and the audited entity. The Auditor and the audited party must not have any current or expected financial, legal, or other relationship that could lead to a conflict of interests. In performing its work, the Auditor shall focus on compliance with the provisions of the legislation in force in the aspects related to the protection of personal data when accessing the data contained in the files of the certificate holders issued by the SISPROOTCA02 CA.

8.4. Topics covered by the Audit

The security audit is performed based on the requirements defined in this CPS and in accordance with the applicable national legislation. Its purpose is to determine the conformity of the SISPROOTCA02 CA services with this statement of practice and certificate policies as well as the adequacy in relation to other documents, namely policies related to logical and physical security, management of CA services, personnel selection, among others. It may be general or partial and may impact any type of documents / processes.

8.5. Correction of Non-Conformities

When non-conformities are detected in an audit, the Auditor must:

- Document any deficiencies found during the audit;
- At the end of the audit process, meet with the persons responsible for the audited authority and present a brief report of first impressions;
- Prepare the audit report in accordance with the rules and practices established by the Supervisory Body;
- Submit the audit report to the audited Authority;
- The audited entity must submit a plan for the correction of nonconformities to the Supervisory Authority, describing actions, methodology and the time required to correct the deficiencies;

After analyzing the plan presented, and depending on the degree of severity / seriousness of the irregularities, the Supervisory Body must select one of the three following options:

- Accept the terms allowing business continuity until the next inspection;
- Allow the continuity of the authority's business for a maximum period of 90 days for the correction of irregularities;
- Immediate cessation of activities.

8.6. Reporting Audit Results

The results of the process must be communicated to SISP and the Supervisory Entity.

8.7. Internal Audits

SISPROOTCA02 periodically conducts internal audits with the aim of ensuring the quality of service and the observation of the applicability of standards, policies and certification practices. This audit, involving between 1 and 5% of the certificates issued, is performed by the Audit Working Group.

9. Other Situations and Legal Issues

9.1. Fees

9.1.1. Fees for Certificate Issuance or Renewal

To be identified in a formal proposal to be made by SISP.

9.1.2. Certificate Usage Fees

Nothing to report.

9.1.3. Fees to Access Certificate Status or Revocation Information

Access to information about the status or revocation of certificates (LRC) is free of charge.

9.1.4. Fees for other services

Nothing to report.

9.1.5. Refund Policy

Nothing to report.

9.2. Financial Accountability

9.2.1. Insurance Coverage

SISP maintains a compulsory civil liability insurance as per article 45 of Decree-Law 33/2007, of September 24.

9.2.2. Other Insurance

Nothing to report.

9.2.3. Insurance or Guarantee Coverage for Holders

SISP maintains a compulsory civil liability insurance, as per article 45 of Decree Law 33/2007, of September 24, and paragraph 8.4 of the Guidelines for the Issuance and Management of Extended Validation Certificates Version 1.7.6 of the CAB Forum.

9.3. Confidentiality of Information

9.3.1. Scope of Confidentiality of Information

Confidential information is expressly declared to be one that may not be disclosed to third parties without explicit authorization. This information is under custody and only duly authorized Working Groups can have access to it.

9.3.2. Information outside the Scope of Confidentiality

Public access information is deemed to be:

- Certificate Policies;
- Certification Practices Statements;
- LRC and,

all information classified as "public" (information not expressly considered as "public" shall be considered confidential).

SISPROOTCA02 CA allows access to non-confidential information without prejudice to security controls necessary to protect its authenticity and integrity.

9.3.3. Responsibility for Protecting the Confidentiality of Information

Working Group members or other entities who receive confidential information are responsible for ensuring that it is not copied, reproduced, stored, translated or transmitted to third parties by any means without prior written consent from SISP.

The coordination of this responsibility is done by the CISO. In case of a breach of trust, the CISO should be contacted at ciso@sisp.cv .

9.4. Privacy and Personal Data Protection

9.4.1. Measures to Ensure Privacy

SISPROOTCA02 CA is responsible for implementing measures to ensure the privacy of personal data in light of the Cabo Verdean legislation.

9.4.2. Private Information

Private information is considered to be all information provided by the holder that is not in the public domain.

9.4.3. Information Not Protected by Privacy

All the information provided by the certificate's titleholder that is made available in the titleholder's digital certificate is considered as information not protected by privacy.

9.4.4. Responsibility to Protect Private Information

As per the Cabo Verdean legislation.

9.4.5. Notification and Consent to Use Private Information

As per the Cabo Verdean legislation.

9.4.6. Disclosure Resulting from Legal or Administrative Procedures

No provision is made for ceding data to third parties, except in the case of a court order.

9.4.7. Other Circumstances for Information Disclosure

No provision is made for ceding data to third parties, except in the case of a court order.

9.5. Intellectual Property Rights

All intellectual property rights, including those referring to certificates, LRC, OID, CPS and CP, as well as any other document owned by the SISPROOTCA02 CA belong to SISP S.A.

The private keys and the public keys are property of the titleholder, regardless of the physical means used for their storage.

The titleholder shall always retain the right over brands, products or commercial names contained in the certificate.

9.6. Obligations and Warranties

9.6.1. Obligations and Warranties of the Certification Entity (CA)

SISPROOTCA02 CA is bound to:

- Conduct 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 the X.509 standard;
- Issue certificates that are in accordance with the information known at the time of their issue and free of data entry errors;
- Guarantee confidentiality in the process of generating the signature creation data and its delivery through a secure procedure to the subscriber;
- Use reliable systems and products that are protected against any alteration and that guarantee the technical and cryptographic security of the certification processes;
- Use reliable systems for storing recognized certificates that can prove their authenticity and prevent unauthorized persons from altering the data;
- Archive the issued certificates without any alteration;
- Ensure that they can accurately determine the date and time they issued or terminated or suspended a certificate;
- Employ personnel with the necessary qualifications, knowledge and experience to provide certification services;

- Revoke certificates pursuant to section 4.9 of this document and publish revoked certificates on the LRC of the SISPROOTCA02 CA, with the frequency stipulated in section 4.9.7;
- Publish its CPS and the applicable Certificate Policies in its repository, guaranteeing access to current versions, as well as to previous versions;
- Notify the titleholders of the certificates with the necessary speed, by email, in case the CE revokes or suspends them, indicating the reason that originated this action;
- Collaborate with the audits conducted by the Supervisory Authority to validate the renewal of its own keys;
- Operate in accordance with the applicable law;
- Protect the keys under its custody;
- Guarantee the availability of the LRC in accordance with the provisions of section 6.10.10;
- In case it ceases its activity it shall inform all titleholders at least three months in advance of the certificates issued, as well as the Supervisory Authority;
- Comply with the specifications contained in the standard on Personal Data Protection;
- Retain all the information and documentation relative to a recognized certificate and the Certification Practices Statements in force at any given time and for twenty years from the time of issue.

9.6.2. Obligations and warranties of the registration entity

Registration Entities are bound to:

- Receive requests for the issuance of certificates;
- Validate and authenticate the data of the certificate applicants;
- Validate other data of certificate applicants that are submitted to them, whose verification is delegated to the certificating entity for the approval of certificates with certain competencies, such as, the quality of representative of a legal entity, quality of employee of an organization, quality of member of a professional group, among others;
- Forward approved requests to the certifying entity to which it is bound;
- Receive and validate the requests for certificate suspension or revocation and remit them to the certifying entity;
- Collaborate for the carrying out of inspections and audits by the Supervisory Authority and its auditors;
- Guarantee delivery of the certificate to its titleholder, or to whoever legally represents it; and
- Contract with the titleholders under the terms and model defined by the Certifying Entity.

SISPROOTCA02 CA counts only and exclusively on Internal Registration Units.

9.6.3. Obligations and Warranties of Titleholders

It is the obligation of the holders of the certificates issued:

- To limit and adapt the use of the certificates according to the uses foreseen in the Certificate Policies;
- To take all the necessary care and measures to ensure the possession of their private key;
- To request the immediate revocation of a certificate in case of having knowledge or suspicion of compromise of the private key corresponding to the public key contained in the certificate, in accordance with section 4.9.1;
- Not to use a digital certificate that has lost its effectiveness, either because it has been revoked, suspended or because the validity period has expired;

- To submit to the Certification (or Registration) Entities the information that they consider accurate and complete with relation to the data they request to carry out the registration process. Must inform the CE of any changes to this information, and,
- Not to monitor, manipulate or "reverse engineer" the technical implementation (hardware and software) of the certification services without prior written authorization from SISP's PKI.

9.6.4. Obligations and Warranties of Relying Parties

It is the duty of the parties that trust the certificates issued by the PKI of SISP to:

- Limit the reliability of the certificates to the uses allowed for them in conformity with the provisions of the corresponding Certificate Policy;
- Verify the validity of the certificates when carrying out any operation based on them;
- Take responsibility for the correct verification of digital signatures;
- Take responsibility for proving the validity, revocation, or suspension of the certificates in which it trusts;
- Have full knowledge of the guarantees and responsibilities applicable to the acceptance and use of the certificates in which it trusts and accept to be subject to them.

9.6.5. Obligations and Warranties of Other Participants

Nothing to report.

9.7. Disclaimer of Warranties

SISPROOTCA02 rejects all service guarantees that are not bound by the obligations set out in this CPS.

9.8. Limitations on Obligations

SISPROOTCA02 is liable for any damages caused to end users and third parties that may arise from its activity under the terms set forth in the applicable laws. It is not responsible for any loss or damage derived from abusive use or outside the scope of the contract established with trusted users and / or parties. SISPROOTCA02 assumes no responsibility in case of failure of the services related to force majeure reasons, such as natural disasters, war or other similar events.

9.9. Indemnities

As per the legislation in force.

9.10. Termination and Cessation of Activities

9.10.1. Validity

The documents related to the PKI of SISP (including this CPS) become effective as soon as they are approved by the Management Working Group and are only eliminated or changed by its order.

This CPS becomes effective from the moment of its publication on the SISP's PKI repository.

This CPS will be in effect until it is expressly revoked by the issuance of a new version or by the renewal of the SISPROOTCA02 keys, time at which a new version must be compulsorily drafted.

9.10.2. Replacement and Revocation

The Management Working Group may decide in favor of deleting or amending a document related to the PKI of SISP (including this CPS) when:

- Its contents are considered incomplete, inaccurate or erroneous;
- Its contents have been compromised.

In this case, the eliminated document will be replaced by a new version.

This CPS shall be replaced by a new version with independence of the transcendence of the changes made to it, so that it shall always be applied in its entirety.

When the CPS is revoked, it will be removed from the public repository, guaranteeing, however, that it will be kept for the data retention period stipulated by SISP.

9.11. Individual Notification and Communication to Participants

All participants should use reasonable methods to communicate with each other. These methods may include digitally signed email, postal mail, signed forms, or other, depending on the criticality and subject matter of the communication.

9.12. Changes or Amendments

9.12.1. Procedures for Changes or Amendments

In order to change this document or any of the certificate policies, a formal request must be submitted to the Security Working Group, indicating (at least):

- The identification of the person who submitted the change request;
- The reason for the request;
- The requested changes.

The Security Working Group will review the request made and, if it finds it relevant, make the necessary updates to the document, resulting in a new draft version of the document. The new draft document is then made available to all members of the Working Group and to affected parties (if any) to allow it to be scrutinized. Counting from the date of availability, the various parties will have to submit their comments within 15 working days. When this period is over, the Security Working Group has another 15 working days to review all comments received and, if relevant, incorporate them into the document, after which the document is approved and provided to the Management Working Group for validation, approval and publication, with the changes becoming final and effective.

9.12.2. Notification Timeframe and Mechanism

If the Management Working Group concludes that the changes to the specification can affect the acceptability of the certificates for specific purposes, it shall inform the users of the corresponding certificates that a change has been made and that they should consult the new CPS in the repository established.

9.12.3. Reasons to Change the OID

The Security Working Group should determine whether changes to the CPS require a change in the OID of the Certificate Policy or the URL pointing to the CPS.

In the cases in which, in the judgment of the Security Working Group, the changes to the CPS do not affect the acceptance of the certificates, the minor version number of the document and the last Object Identifier number (OID) that represents it shall be increased, maintaining the major version number of the document, as well as the rest of its associated OID. It is not considered necessary to report this type of changes to the users of the certificates.

In the case in which the Security Working Group judges that the changes to the specification may affect the acceptability of the certificates for specific purposes, the largest version number of the document shall be increased and the smallest version number shall be set to zero. The last two numbers of the Object Identifier (OID) that represent it shall also be modified. This type of changes shall be communicated to the certificate users in accordance with the provisions of section 9.12.2.

9.13. Provisions for Dispute Settlement

All complaints between users and the PKI of SISP shall be communicated by the party in dispute to the Supervisory Authority in order to try and settle it between the same parties.

For the resolution of any conflict that may arise with respect to this CPS, the parties, with waiver of any other forum, must submit it to the Jurisdiction of the District of Praia and the Cabo Verdean law.

9.14. Applicable Laws

The following specific laws are applicable to the activities of the certifying entities:

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.

9.15. Compliance with the Legislation in Force

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

In case of conflict between this CPS and the legislation in force in the jurisdiction/country where the CA operates, such requirement must be reformulated to the minimum extent necessary for it to be valid and legal. This applies only to operations or issuance of certificates that are subject to the laws of that jurisdiction. SISP undertakes to notify the CAB Forum of the facts, circumstances and laws involved so that it can reassess these Guidelines appropriately.

It is the responsibility of the Management Working Group to ensure compliance with the applicable laws listed in section 9.14.

9.16. Miscellaneous Provisions

9.16.1. Full Agreement

All trusting parties assume in its entirety the content of the last version of this CPS.

In case one or more stipulations of this document are or tend to be invalid, null or unclaimable in legal terms, they shall be considered non-effective.

The above situation is valid only in cases where such stipulations are not deemed essential. It is the responsibility of the Management Working Group to evaluate their essentiality.

9.16.2. Transfer of Rights

Trusted parties operating under this CPS or applicable agreements may not assign their rights or obligations without the prior written consent of SISP.

9.16.3. Severity

Nothing to report.

9.16.4. Lawsuits (Attorneys’ fees and waiver of rights)

Nothing to report.

9.16.5. Force Majeure

The force majeure clauses are part and parcel of the General Conditions for the Issuance of the Digital Certificate.

9.17. Other Provisions

Nothing to report.

Bibliographical References

- RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List Profile, 2008;
- RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;
- CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4;
- CA/ Browser Forum-EV-Guidelines –v1.7.6;
- Regulation (EU) No 910/2014;
- ETSI 319 412-4 v1.1.1: Electronic Signatures and Infrastructures (ESI); Certificate Profile for Website;
- ETSI 319 412-5 v2.2.3: Electronic Signatures and Infrastructures (ESI); Certificate Profile-QCStatements;
- ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.