SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTOS

SISP ROOT CA02

Certificate Policy

Code:	PLRC012
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 the Amendment
06/14/2022	01	Ruben Veiga	Document creation

Table of Contents

TABLE INDEX

1. Introduction

- **Scope**

The present document is a Certificate Policy and aims to disseminate the general practices for issuing and managing certificates, followed by the Root Certification Entity SISPRootCA02, as a qualified trust services 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 is likely to undergo regular updates.

- **Target Audience**

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

The certificates issued by SISPROOTCA02 contain a reference to this CP, Document Code no. PLRC00X.01, in order to allow relying parties and other interested persons to find information on 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, it is recommended that the reader study these topics beforehand for a better understanding of 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, and the remaining two are dedicated to Audit/Compliance and legal issues, respectively.

1.1. General Context

This CP 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 a Certificate Policy (CP) represented on a certificate through a single number named as "Object Identifier" (OID). The OID associated with this paper is 1.3.6.1.4.1.4146.1.60.

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

Table 1: Document Information

DOCUMENT INFORMATION	
Document Name	Certificate Policy of SISPROOTCA02
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 are made to the document where applicable.

1.2.1. Reviews

Version	Creation	Approval	Reason for Review
1.0	06/14/2022	06/15/22	Creation
	Security Administrator	Management Team	
	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 PKI Management Entity, SISP complies with the provisions set forth in the standards and applicable legislation, assuming the competencies described therein, being responsible for providing services and ensuring the procedures that may guarantee the functionalities listed below:

1. Generation of the cryptographic key pairs associated with each of the Certification Authorities;

2. Reception and validation of the requests for issuing certificates made by the Subordinate Certification Entities (CE), as well as the other subscribers;

3. Issuing certificates related to the certificate requests that are in accordance with the format required by the SISP Certification Entities;

4. Reception and validation of certificate suspension and revocation requests;

5. Publishing the certificates (when, where and if appropriate) and information about their status;

6. Ensuring the continuous availability of public information for all its users.

The PKI of SISP includes the following CEs:

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

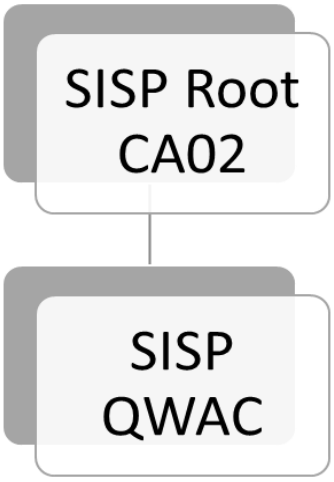

Illustration 1: Structure of the PKI of SISP

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, which can issue qualified and non-qualified TLS/SSL web authentication certificates and code sign certificates.

Table 3: Certificate Information (SISP Root CA02)

CERTIFICATE INFORMATION

Distinguished Name	C = CV, O = SISP, OR = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Root Certifying 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, OR = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Root Certifying 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 accordance 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, OR = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN= SISP QWAC
Signature Algorithm	sha512WithRSAEncryption
Serial Number	77a5aacfb1eb23c603e9f429b724826dbc78add6
Validity	June 29, 2028 07:22:55
Thumbprint	35:6F:2C:CF:BE:F4:CE:4C:FB:17:21:B8:9D:DB:43:B1:03:F6:AC:18:00:AA:42:49:06:8F:64:3B:1B:EA:AE:9B:F5:DA:7E:10:2C:16:9B:9E:52:CD:8E:31:7D:79:DA:AC:EC:C3:4A:8A:D7:DB:B5:5C:55:15:F3:03:24:FA:7D:5D
Issuer	C = CV, O = SISP, OR = SISP-Sociedade Interbancária e Sistemas de Pagamentos, CN = Root Certifying Entity of SISP 02

1.3.2. Registration Entities or Units

Registration Entities or Units are entities to which the CEs delegate the provision of identification services, 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 party entities so that they can perform this role.

- **Internal Registration Entities**

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

- **External Registration Entities**

The trust hierarchy of SISPROOTCA02 does not include external registration entities.

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 those whose name is inscribed in the certificate's "Subject" field and use the certificate and respective private key as set out in 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 certificate 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

The relying parties or recipients are natural persons, entities or equipment that trust the validity of the mechanisms and procedures used in the association process of the titleholder's name with its public key, that is, they trust that the certificate corresponds in reality to whom it says it belongs.

In this CP, a relying party is considered to be the one that trusts the content, validity and applicability of the certificate issued in the trust hierarchy of the PKI of SISP.

1.3.5. Other Participants

- **Supervisory Authority**

The Supervisory Authority assumes the role of an entity that makes available conformity auditing/inspection services intended to check if the processes used by the CE in its certification activities are consistent with the minimum requirements established in the legislation and regulations in force. Its main duties are the following:

a) Accredit the certification entities;

b) Audit the certification entities;

c) Evaluate the activities developed by the authorized certification entities according to the technical requirements defined under the terms of the previous paragraph;

d) Watch over the appropriate operation and efficient provision of services by the certification entities in accordance with the legal and regulatory provisions set out for the activity.

- **External Services Providers**

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

- **Security Auditor**

This position is independent from the Certification Authority's circle of influence required by the Supervisory Authority. Its mission is to audit the Certification Authority infrastructure in what concerns equipment, human resources, processes, policies and rules. Moreover, the Security Auditor is bound to submit an annual report to the Supervising 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;
- Confidentiality;
- Integrity;
- Privacy;
- Authenticity and
- Non-repudiation.

These services are obtained with the use of public key cryptography, through its use in the trust structure that the PKI of SISP provides. Thus, the identification and authentication, integrity and non-repudiation services are obtained by using digital signatures. Confidentiality is guaranteed through the use of cipher algorithms when combined with mechanisms to establish and distribute keys managed by certified cryptographic equipment. Trusted parties can validate the chain of trust and thus guarantee the authenticity and identity of the holder.

1.4.1. Proper Use of the Certificate

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

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, confidentiality and security in the exchange of information between the user and the website.

1.4.2. Unauthorized Use

Certificates issued by SISPROOTCA02 may not be used for any function outside the scope of the uses described above.

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 could lead to death, personal injury, or serious damage to the environment.

1.5. Policy Management

1.5.1. Document Organization and Management

Management of this CP is the responsibility of the Security Working Group.

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 suitability of the CP to the policies

The Security Working Group determines the compliance and internal application of this CP (and/or the respective CPS) and submits it to the Management Group for approval.

1.5.4. Procedures for the Approval of the CP

The validation of this CP (and/or the respective CPS) and corrections (or updates) shall be carried out by the Security Working Group. Corrections (or updates) shall be published as new versions of this CP (and/or related CPS), replacing any CP (and/or related CPS) previously defined.

The Security Working Group should also determine when changes to the CP (and/or its CPS) lead to a change in the object identifiers (OID) of the CP (and/or its CPS).

After the validation phase, the CP (and/or respective CPS) is submitted to the Management Group, which is the entity responsible for approving and authorizing changes 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	*Certificate Practices Statement*
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 functions 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*:

- 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 their respective addresses for 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 certificates in the valid, revoked and expired condition.

2.3. Publication Periodicity

SISP ensures that updates to this CP 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, can 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 of 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 only to one entity 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 entities applying for a certificate.

SISP is responsible for the safekeeping of all the documentation used to verify the identity of the certifying entity, ensuring the verification of the identity of its legal representatives by legally recognized means and guaranteeing the 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 that SISPROOTCA02 carries out a rigorous process of verification of the identity of the titleholder and 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 all. Moreover, this should be duly specified in the Certificate Policy at stake.

3.2.2. Organization and Domain Identity Authentication

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

The identity verification of the holders and/or subscribers 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 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.

SISPROOT CA02 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 made 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 Purposes

3.3.1. Identification and Authentication for Routine Key Renewal

There is no routine key renewal. The renewal of certificates uses 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 form can be signed in a handwritten or digital way by 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 former 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 the authenticity of the documentation 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.

SISPROOT CA02 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 the request, 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 is 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, thus informing the person responsible for the request.

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 certificates results from the interaction with the cryptographic module (HSM) by following a specific procedure and in accordance with the respective certificate policy. The certificate so issued and signed by the highly ranked Certifying Entity is imported into the corresponding SubCA as the first LRC is generated.

.

The validity of the certificate starts upon issuance.

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

Nothing to report.

4.4. Acceptance of the Certificate

4.4.1. Conduct Constituting Acceptance of the Certificate

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

It should be noted that, before delivering the certificate to the representatives and consequently all the functionalities for the use of the private key and certificate are made available to them, it is ensured that:

- They become aware of the related rights and responsibilities;
- They become aware of the certificate functionalities and content;
- The certificate and the conditions for its 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 issued certificates.

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. Subscriber/Holder Usage of Certificate and Key Pair

The holder must use his private key and ensure the protection of this key as provided for in this CP. 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 CRL.

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 Certificate 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 the Re-Keyed Certificate by the CA

Nothing to report.

4.7.7. Notification of the 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 Modification of the Certificate

Nothing to report.

4.8.3. Processing a 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.
Certificate suspension is not supported by SISPROOTCA02 CA.

4.9.1. Reasons for Revocation

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

- The SubCA requests in writing the revocation of the certificate;
- The 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 obtained evidence that the Certificate has been misused;
- The Issuing CA is informed that the Certificate has not been properly issued 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 SubCA has ceased operations and has not created conditions for another CA to provide revocation support for the Certificate;
- Revocation is required under the Issuing CA's Certification Policy.

4.9.2. Who Can Request 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 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 after 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 condition of all certificates through the LRC or an online certificate status server (OCSP).

4.9.7. CRL 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 **3 months**.

The CRL 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 time 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 CP (Certificate Policy), the parties may use the email pki@sisp.cv 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 to Request Suspension

Nothing to report.

4.9.16. Limits of the Suspension Period

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, according to RFC 3647.

4.12. Key Custody and Recovery

4.12.1. Key Custody and Recovery Policies and Practices

SISP retains the private key of SISP QWAC and SISPROOTCA2 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. Session Key Encapsulation and Retrieval Policies and Practices

See section 4.12.1.

5. Physical Security, Management and Operational Controls

Physical security, management and operational controls are described in the Certification Practices Statement of SISPROOTCA02.

6. Technical Security Checks

Technical security checks are described in the Certification Practices Statement of SISPROOTCA02.

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*
- ETSI 319 412-5 v2.2.3: Electronic Signatures and Infrastructures (ESI); Certificate Profile-QCStatements;
- *EU Regulation No.910/2014*
- National Regulation

7.1. Certificate Profile

7.1.1.1. Certificate Profile of SISPROOTCA

Certificate Component	Certificate Component	Section in the RFC5280	Value	Type	Comments
tbsCertificate	**Version**	4.1.2.1	3	m	Value 3 identifies the use of ITU-T X.509 version 3 certificates
	Serial Number	4.1.2.2	<assigned by the CE to each certificate>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.13	m	Value MUST match the OID in signatureAlgorithm (below)
	Issuer Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.4	 "CV" "SISP" "SISP-Sociedade Interbancária e Sistemas de Pagamentos" "Root Certification Entity of SISP 02"	m	
	Validity Not Before Not After	4.1.2.5	 <date of issue> <date of issue + 12 years>	m	For the purposes of this profile, GeneralizedTime values MUST be expressed in Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero. GeneralizedTime values MUST NOT include fractional seconds Validity of 12 years renewed every 6 years.
	Subject Country (C)	4.1.2.6	<SISP Root CA2> "CV"	m	

	Organization (O) Organization Unit (OU) Common Name (CN)		"SISP" "SISP-Sociedade Interbancária e Sistemas de Pagamentos" "Root Certification Entity of SISP 02"		Self-signed CE
	Subject Public Key Info Algorithm subjectPublicKey	4.1.2.7	1.2.840.113549.1.1.13 <Public Key with modulus n of 4096 bits>	m	Used to contain the public key and identify the algorithm with which the key is used (e.g., RSA, DSA or Diffie-Hellman). The rsaEncryption OID identifies RSA public keys. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 3} The rsaEncryption OID must be used in the algorithm field with a value of the type AlgorithmIdentifier. The field parameters MUST include ASN.1 to NULL for the identifier of this algorithm.24
	Unique Identifiers	4.1.2.8		m	The "unique identifiers" is present so as to enable the possibility of reusing the names of subject and/or issuer 20
	X509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier KeyIdentifier	4.2.1.1	< The key Identifier is composed of the 160-bit SHA-I hash of the BIT STRING value of the subjectPublicKey (excluding the tag, length, and unused bit number)>	m	
	Subject Key Identifier	4.2.1.2	< The key Identifier is composed of the 512-bit SHA 512 hash of the BIT STRING value of the subjectPublicKey (excluding the tag, length, and unused bit number)>	m	
	Key Usage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature Encipher Only Decipher Only	4.2.1.3	"0" selected "0" selected "0" selected "0" selected "0" selected "1" selected "1" selected "0" selected "0" selected	mc	This extension is marked as CRITICAL
	Certificate Policies	4.2.1.4		o	
	Basic Constraints	4.2.1.9		mc	

	CA PathLenConstraint		TRUE	m o	Indicates the type of Entity to whom the certificate is destined; basic restriction, if CA = true the certificate can sign a CE
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sisprootca2.crl	o m	
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.13	m	MUST contain the same OID as the algorithm identifier of the signature field in the tbsCertificate sequence field. sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13
	Signature Value	4.1.1.3	<contains the digital signature issued by the CE>	m	When generating this signature, the CE certifies the connection between the public key and the certificate's titleholder (subject).

7.1.1.2. Certificate Profile of SISP QWAC CA

Certificate Component	Certificate Component	Section in the RFC5280	Value	Type	Comments
tbsCertificate	**Version**	4.1.2.1	3	m	Value 3 identifies the use of ITU-T X.509 version 3 certificates
	Serial Number	4.1.2.2	<assigned by the CE to each certificate>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.13	m	Value MUST match the OID in the signatureAlgorithm (below)
	Issuer Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.4	 "CV" "SISP" "SISP-Sociedade Interbancária e Sistemas de Pagamentos" "Root Certification Entity of SISP 02 "	m	 Official Name of CE of SISP 02 – CE sequence
	Validity Not Before Not After	4.1.2.5	 <date of issue> <date of issue + 5 years and 4 months>	m	 Maximum validity of 6 years.
	Subject Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.6	 "CV" "SISP" "SISP-Sociedade Interbancária e Sistemas de Pagamentos" "SISP QWAC"	m	 Official Name of the CE of SISP
	Select Public Key Info	4.1.2.7		m	Used to contain the public key and identify the algorithm with which the key is used (e.g., RSA, DSA or Diffie-Hellman).

	Algorithm				The rsaEncryption OID identifies RSA public keys. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 3} The rsaEncryption OID must be used in the algorithm field with a value of the type AlgorithmIdentifier. The field parameters MUST have type ASN.1 to NULL for the identifier of this algorithm.24
	subjectPublicKey		1.2.840.113549.1.1.13 <Public Key with modulus n of 4096 bits>		
	Unique Identifiers	4.1.2.8		m	The "unique identifiers" is present so as to enable the possibility of reusing the names of subject and/or issuer 20
	X509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier KeyIdentifier	4.2.1.1	The key Identifier is composed of the 512-bit SHA-512 hash of the BIT STRING value of the subjectPublicKey (excluding the tag, length, and unused bit number)>	m	
	Subject Key Identifier	4.2.1.2	The key Identifier is composed of the 512-bit SHA-512 m hash of the BIT STRING value of the subjectPublicKey (excluding the tag, length, and unused bit number)>	m	
	Key Usage	4.2.1.3		mc	This extension is marked as CRITICAL
	Digital Signature		"1" selected		
	Non Repudiation		"0" selected		
	Key Encipherment		"1" selected		
	Data Encipherment		"1" selected		
	Key Agreement		"0" selected		
	Key Certificate Signature		"1" selected		
	CRL Signature		"1" selected		
	Encipher Only		"0" selected		
	Decipher Only		"0" selected		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.4146.1.60	m	Identifier of the Certification Practices Statement of SISP ROOT CA 02 (id-qt-cps PKIX CPS Pointer Qualifier)
	policyQualifiers		<policyQualifierID> cPSuri: https://pki.sisp.cv/document_repository	o	OID Description: "The cPSuri attribute contains a link to the Certification Practices Statement published by SISP ROOT CA 02. The link is in the form of a URL."
	policyIdentifier		1.3.6.1.4.1.4146.1.60	m	Identifier of the Certification Practices Statement of SISP ROOT CA 02 (id-qt-cps PKIX CPS Pointer Qualifier)
	policyQualifiers		<policyQualifierID> cPSuri: https://pki.sisp.cv/document_repository	o	OID Description: "The cPSuri attribute contains a link to the Certification Practices

					Statement published by SISP ROOT CA 02. The link is in the form of a URL."
	Basic Constrains CA PathLenConstraint	4.2.1.9	 TRUE 0	o m o	Indicates the type of Entity to whom the certificate is intended; basic restriction, if CA = true the certificate may sign a CE
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sisprootca2.crl	o m	
	Extended Key Usage Server Authentication Client Authentication	4.2.1.12	 1.3.6.1.5.5.7.3.1 1.3.6.1.5.5.7.3.2	 m m	 Server Authentication Client Authentication
	Internet Certificate Extensions				
	Authority Information Access accessMethod accessLocation accessMethod accessLocation	4.2.2.1	 1.3.6.1.5.5.7.48.1 http://ocsp.sisp.cv/ 1.3.6.1.5.5.7.48.2 https://pki.sisp.cv/document_repository	o	 OID Value: (id-ad-ocsp) URL to access the OCSP OID Value: (id-ad-ca) URL to access the CA Certificate
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.13	m	MUST contain the same OID of the algorithm identifier of the signature field in the field of the tbsCertificate sequence. sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13
	Signature Value	4.1.1.3	<contains the digital signature issued by the CE>	m	When generating this signature, the CE certifies the connection between the public key and the certificate titleholder (subject).

7.1.2. 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).

7.1.3. 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.

7.1.4. Algorithm OID

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

7.1.5. Name Formats

As defined in section 3.1.

7.1.6. Name Conditioning

SISP can include conditionals on names in the "*nameConstraints*" field whenever justified.

7.1.7. Certificate Policy OID

Nothing to report.

7.1.8. Using Policy Constraint Extension

Nothing to report.

7.1.9. Syntax and Semantics of Policy Qualifiers

Nothing to report.

7.1.10. 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, it verifies the signature and validity of the certificate, obtains the most recent LRC and verifies 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.

LRC Component	Certificate Component	Section in the RFC5280	Value	Type	Comments
tbsCertList	**Version**	5.1.2.1	3	m	Value 3 identifies the use of Version 3 of the ITU X.509 standard
	Signature	5.1.2.2	1.2.840.113549.1.1.13	m	Contains the algorithm identifier used to sign the LRC. The value MUST match the OID in the signatureAlgorithm field (below)
	Issuer Country (C) Organization (O) Common Name (CN)	5.1.2.3	 "CV" "SISP" "Root Certification Entity of SISP 02 "	m	

	thisUpdate	5.1.2.4	<date of issue of the LRC>	m	For the purposes of this profile, GeneralizedTime values MUST be expressed in Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero. GeneralizedTime values MUST NOT include fractional seconds
	nextUpdate	5.1.2.5	<date of next LRC issue = thisUpdate + N>	m	This field indicates the date when the next LRC will be issued. The next LRC can be issued before the date indicated, but will not be issued after that date. LRC issuers MUST issue LRCs with a nextUpdate time greater than or equal to all previous LRCs. Implementations MUST use UTC time until 2049, and after that must use GeneralisedTime. N will be a maximum of 90 dias.
	revokedCertificates	5.1.2.6	<list of revoked certificates>	m	
	CRL Extensions	5.1.2.7		m	
	Authority Key Identifier KeyIdentifier	5.2.1	The key Identifier is composed of the 512-bit SHA-512 hash of the BIT STRING value of the subjectPublicKey (excluding the tag, length, and unused bit number)>	o	
	CRL Number	5.2.3	< unique incremented sequence number >	m	
	Issuing Distribuition Point DistributionPointName	5.2.5	http://crl.sisp.cv/sisprootca02.crl	c	
	CRL Entry Extensions Reason Code	5.3 5.3.1		o	Value has to be one of the following: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 - Compromise
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.13	m	MUST contain the same OID as the algorithm identifier of the signature field in the tbsCertificate sequence field. sha512WithRSAEncryption OBJECT IDENTIFIER ::= {

					iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13
	Signature Value	5.1.1.3	<contains the digital signature issued by the CE>	m	When generating this signature, the CE certifies the connection between the public key and the certificate's titleholder (subject).

7.2.1. Version Number(s)

The CRL "version" field describes the version used in encoding the CRL. 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.

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.