SISP – SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTO

Certificate Policy (CP) of

- SISPCA01 Issuing Certification Authority -

Code:	PLRC004.02
Version:	2.0
Version Date:	June 30, 2019
Created by:	SISP
Approved by:	Board of Directors
Level of Confidentiality:	Public

Change Control Log

Date	Version	Created by	Description of the Amendment
July 31, 2018	1.0	SISP	Document creation. Established.
September 3, 2018	1.1	SISP	Change of profiles
June 30, 2019	2.0	SISP	Web Authentication Certificate Profile

Related Documents

Certification Practices Statement of SISPCA01

Jair Elísio Andrade Ferreira Silva

Digitally signed by Jair Elísio Andrade Ferreira Silva
DN: email=jsilva@sisp.cv, cn=Jair Elísio Andrade Ferreira Silva, serialNumber=CV-4874, givenName=Jair Elísio, sn=Andrade Ferreira Silva, title=Diretor-Geral, ou=Direção SISP, ou=Certificado para pessoa singular - Assinatura Qualificada, o=Sociedade Interbancária e Sistemas de Pagamentos S.A., l=Praia, st=Santiago, c=CV
Date: 2020.03.10 10:13:38 -01'00'

Table of Contents

1. INTRODUCTION

1.1. OBJECTIVES

This document aims at defining the policies used by SISPCA01 Certification Authority in the certificate issuance process.

1.2. TARGET AUDIENCE

This is a public document and is intended for all those who relate with SISPCA01 Certification Authority, hereinafter referred to as SISPCA.

1.3. DOCUMENT LAYOUT

It is assumed that the reader is already familiar with the concepts of cryptography, public key infrastructure, and electronic signature. If this is not the case, it is recommended that those concepts and knowledge be deepened before reading the document.

This document should be read together with and as a complement to the Certification Practices Statement of SISPCA.

2. ACRONYMS AND DEFINITIONS

A list of relevant acronyms and definitions used in this document is provided below:

2.1. ACRONYMS

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

2.2. DEFINITIONS

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

Certificate, as anticipated in DL no. 33/2007, of September 24	Digital record that links signature-verification data to the signatory and confirms the identity of that person.
Qualified certificate, as set forth in DL no. 33/2007, of September 24	Certificate that includes all the elements referred to in Article 67 of the DL 33/2007 [6] and is issued by a certification authority that complies with the requirements defined in Article 45 of DL 33/2007.
Private key, as provided for in DL no. 33/2007, of September 24	An element of the pair of asymmetric keys that is kept secret by its holder, and that is used to affix the digital signature to the electronic document or to decrypt electronic records previously encrypted with the corresponding Public Key.
Public Key, as set forth in DL no. 33/2007, of September 24	The key of a key pair that may be publicly disclosed and that is used to verify digital signatures created by the holder of the asymmetric keys or to encrypt messages to be sent to the holder of the said key pair.
Accreditation, as set forth in DL no. 33/2007, of September 24	The act whereby upon request an entity that performs the role of certification entity is acknowledged to fulfil the requirements defined in the DL no. 33/2007, of September 24, for the purposes anticipated therein.
Signature-creation data, as provided for in DL no. 33/2007, of September 24	Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.
Signature-verification data, as set forth in DL no. 33/2007, of September 24	A set of data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.
Signature-creation device, as anticipated in DL no. 33/2007, of September 24	Configured software or hardware used to implement the signature-creation data.
Secure signature-creation device, as set forth in DL no. 33/2007, of September 24	A signature-creation device that ensures, by appropriate technical and procedural means, that: i) Data required for the creation of a signature, used for signature generation, can occur only once and their secrecy is fully guaranteed; ii) Data required for the creation of a signature, used for signature generation, cannot, with reasonable

	assurance, be derived and the signature is protected against forgery using currently available technology; iii) Data required for the creation of a signature, used for signature generation, can be reliably protected by the holder against the illegitimate use by third-parties; iv) Data to be signed cannot be altered and may be submitted to the holder prior to the signature process.
Electronic document, as laid down in DL no. 33/2007, dated September 24	Document prepared by electronic data processing.
Electronic address, as laid down in DL no. 33/2007, dated September 24	Identification of appropriate computer equipment to receive and store electronic documents.

3. GENERAL CONTEXT

3.1. OBJECTIVE

The present document is a Certificate Policy (CP) and seeks to define a set of policies and data required for certificate issuance and validation and safeguard the reliability of such certificates. It is not meant to list legal rules or obligations but rather inform the parties involved. Therefore, this document is intended to be clear, straightforward, and understood by a larger audience, including those who do not hold any technical or legal knowledge.

This document describes the policies followed by SISP Certification Authority (SISPCA01) in the certificate issuance and management process.

All certificates issued by SISPCA01 conform with the requirements of ICP-CV and are based on the following standards:

a) RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework;
b) RFC 5280 – Internet X.509 Public Key Infrastructure – Certificate and CRL Profile.
c) ETSI TS 102 042 V2.4.1
d) CABForum-EV Guidelines V1.7.0

Any certificates issued by SISPCA01 shall include a reference to the present Certificate Policy and document code, so as to enable the Relying Parties and other interested persons to obtain information on the certificate and the issuing entity.

3.2. OVERVIEW

This CP meets and complements the requirements laid down in the Certification Practices Statement of SISPCA01 Certification Authority.

3.3. DOCUMENT IDENTIFICATION

This document is the Certificate Policy (CP) of the Certification Authority SISPCA01. The CP is represented on a certificate through a unique number named as “Object Identifier” (OID). The OID associated with this paper is 2.16.132.1.2.2.3.2.

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

DOCUMENT INFORMATION	
Document Version	Version 2.0
Document Status	Approved
OID	2.16.132.1.2.2.3.2
Date of Issue	June 30, 2019
Validity	Not applicable
Location	http://pki.sisp.cv/

3.4. POLICY ADMINISTRATION

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

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

4. IDENTIFICATION AND AUTHENTICATION

4.1. NAMING

Naming shall follow the convention determined by the CPS of SISPCA01.

4.1.1. TYPES OF NAMES

The certificates issued by SISPCA01 are identified by the unique name (DN - Distinguished Name) in accordance with the standard X.509. The unique name of the certificate of SISPCA01 is identified through the following components:

4.1.1.1. Qualified Certificate of Digital Signature

Feature	Code	Value
Country	C	<Country of nationality of the certificate holder>
Organization	O (optional)	<Organization to which the certificate holder belongs>
Organization Unit	OU	<Certificate for natural person – Qualified Signature>
Organization Unit	OU (optional)	<Area/Department of the organization to which the certificate holder belongs>
Locality	L (optional)	<Place of residence of the holder>
State or Province	ST (optional)	<State, province, island of residence of the holder>
Title	T (optional)	<Quality of the certificate holder within the scope of its use for qualified digital signature>
Serial Number	serialNumber	<CIN or PAS>[1] - <Country Code> - <Identification Number>
Common Name	CN	<Name of Certificate Holder>
Surname	SN	<Family Names of Certificate Holder>

[1] CIN – Civil Identification Number; PAS - Passport

Given Name	givenName	<First Name of Certificate Holder>
E-mail	eMail	<e-mail of holder associated with the certificate>

4.1.1.2. Qualified Certificate of Electronic Seal

Feature	Code	Value
Country	C	<Country of nationality of the organization>
Organization	O	<Organization name as recorded by the relevant authorities>
Organization Unit	OU	<Electronic Seal – Qualified Signature>
Organization Unit	OU (optional)	<Area/Department of the organization>
Organization Identifier	OI	<VAT>[2] - <Country Code> - <Taxpayer Identification Number>
Common Name	CN	<Organization name under which it is known>
E-mail	eMail	<Holder's e-mail>

4.1.1.3. Certificate of Authentication

Feature	Code	Value
Country	C	<Country of nationality of the certificate holder>
Organization	O (optional)	<Organization to which the certificate holder belongs>
Organization Unit	OU	<Certificate for natural person – Authentication>

[2] Value Added Tax

Organization Unit	OU (optional)	<Area/Department of the organization to which the certificate holder belongs>
Common Name	CN	<Name of Certificate Holder>
Surname	SN	<Family Names of Certificate Holder>
Given Name	givenName	<First Name of Certificate Holder>
Serial Number	serialNumber	The same as the holder’s Tax Identification Number

4.1.1.4. Certificate of Web Authentication (SSL)

Feature	Code	Value
Country	C	<Country of nationality of the organization>
Organization	O	<Organization name as recorded by the relevant authorities>
Organization Unit	OU (optional)	<Area/Department of the organization>
Common Name	CN	< Fully Qualified Domain Name of the web server >
Street		<Street of residence of the organization>
Locality	L (optional)	<Place of residence of the organization>
Postal Code	(optional)	<Postal Code>
Serial Number	serialNumber	<Value Added Tax Number>
Subject Jurisdiction of Incorporation	subject Jurisdiction	<Country whereas the organization is doing business>
Subject Business Category Field	subjectBCField	<Organization Business Category: "Private" “Government Entity” “Business Entity” “Non-Commercial Entity”>

Subject Alternative Name	DNS<fully qualified domain name of the web server>

4.1.2. CERTIFICATE AND KEY PAIR USAGE BY THE TITLEHOLDER

The Common Name defines the titleholder of the certificate. The Qualified Certificate of Digital Signature assumes the identification of a natural person while the Qualified Certificate of Electronic Seal relates to a legal person.

The certificates of qualified signature associate the validation data of the electronic signature to a natural person while the qualified certificate of electronic seal relate to a legal person, so securing data source and integrity.

The certificates issued in accordance with this policy are equivalent to qualified digital certificates as defined in the applicable Cabo-Verdean legislation and international standards.

4.2. INITIAL IDENTITY VALIDATION

SISPCA01 is responsible for validating the identity of the entities applying to a certificate.

The Qualified Certificates of Digital Signature and Authentication are issued for natural persons who are responsible for their usage. A Qualified Certificate of Electronic Seal as well as the Web Authentication Certificate is issued for an Organization (Legal Person) to which a natural person, identified as “technical manager” but not represented in the certificate, is linked and is responsible for handling and using the certificate on behalf of the organization.

4.2.1. METHOD OF PROVING POSSESSION OF PRIVATE KEY

The key pair and certificate are provided in a cryptographic token (SmartCard or USB token) with encrypted chip, physically customized for the titleholder. Possession of the private key is proved by issuing and customizing the cryptographic token, thus guaranteeing that:

- The key pair is generated in the encrypted HSM and inserted in the cryptographic token through direct, secure communication, without leaving any records whatsoever in any device;
- The cryptographic token is customized for its holder;
- The public key is forwarded to SISP for the purposes of issuing the corresponding digital certificate, which is also inserted in the cryptographic token;
- The cryptographic token is delivered on-site.

When issuing a qualified certificate for electronic seal or a web authentication certificate there is also the possibility of the key being generated by the assignee indicated by the legal person (Organization) in a proper HSM. In that case:

- The assignee and respective organization will assume the responsibility for the key generated and the HSM used for that purpose;
- All necessary documentation is sent to SISP, along with a CSR;

- The certificate is returned to the assignee following validation of the documents delivered.

4.2.2. AUTHENTICATION OF A NATURAL PERSON'S IDENTITY

The process of authenticating the identity of a natural person must compulsorily guarantee that the person to whom the certificate shall be issued is really who he/she claims to be.

The actions required to attain this objective include:

1. Verifying, based on officially recognized documents bearing a photograph:
   a) The subscriber's full name;
   b) The unique identification number;
   c) The contact details, including the address, if any.
2. Guaranteeing the physical presence of the subscriber at the time of registration, unless a relationship of trust already exists that is previously based on such physical presence of the subscriber;
3. Verifying, when it comes to quality certificates, that the applicant is entitled to such benefits or privileges;

4.2.3. VALIDATION OF A LEGAL PERSON'S IDENTITY

The process of authenticating the identity of a legal person shall necessarily guarantee that the legal person is really who it claims to be, and that the creation of a signature through a signature creation device demands the intervention of natural persons who, legally or statutorily, represent that legal person.

The documentation on which the issuance of a qualified certificate of electronic seal is based must include namely the following items:

a) Documents for the purposes of identifying the legal person and its legal name, e.g. commercial registry certificate;
b) Tax identification number, headquarters, corporate object, names of the members of the corporate bodies and other persons who have the power to bind the legal person;
c) Full name, identification card number or any other document that enables the unique identification of the natural persons who, legally or statutorily, represent the legal person;
d) Full name, identification card number or any other document that enables the unique identification of the technical manager, designated to handle the certificate;
e) Address and other contact details. Wildcard emails such as Hotmail, Gmail, Yahoo or similar are not accepted.

The validation of applicants is carried out using the same documents stated in points a), b), c) and d) mentioned above.

Web authentication certificates are issued after the legal existence of the domains and their respective ownership has been proven, through the use of tools provided by the corresponding services, (namely RIPE, AFRINIC).

In addition, confirmation of the certificate issuance request, is made by calling the technical responsible indicated on the form.

4.2.4. NON-VERIFIED INFORMATION ON THE SUBSCRIBER/TITLEHOLDER

SISP reserves the right to reject any certificate applications in such situations when the validation process described in paragraphs 4.2.2 and 4.2.3 has failed compliance.

4.2.5. VALIDATION OF A COMPETENT AUTHORITY

No stipulation.

4.2.6. INTEROPERABILITY CRITERIA

No stipulation.

4.3. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION PURPOSES

Any entity may request revocation of a particular certificate if it has knowledge or suspicion that the titleholder's private key was compromised or of any other act that recommends this action, namely:

- The certificate holder, in the case of natural persons certificates;
- The legal representative(s) of the entity entitled to attest the quality of the certificate holder, as affixed in the digital certificate, whenever that quality ceases to be valid;
- The relying party, whenever it proves that the certificate has been used for purposes other than those anticipated.

For that purpose, a specific form must be filled out, including the following information:

- Legal name of the titleholder;
- Legal person's number, headquarters, business purpose, names of the members of the corporate bodies and other authorized persons, registration number at the Commercial Registry and/or full name, identification number or any other information enabling the unique identification of the entity (or its representative) requesting the revocation;
- Address and other contact details;
- Reasons for revoking the certificate.

The identification and authentication process underlying the revocation request of a natural person or legal person's certificate is carried out through one of the following methods:

- Qualified digital signature of the form;
- Handwritten signature of the form to be delivered by the subscriber at the head office of SISP S.A. located in the city of Praia or at any designated RE;
- Handwritten signature of the form, duly certified by a notary.

The REs of SISPCA01 shall keep all documents used to verify the identity and authenticity of the entity that requests revocation of the certificate of qualified digital signature.

5. CERTIFICATE AND CRL PROFILES

5.1. CERTIFICATE PROFILE

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

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

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

The profile of the certificates issued by SISPCA01 is in conformity with the requirements of ICP-CV and 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) ETSI TS 102 042 V2.4.1
d) CA–Browser-Forum-EV Guidelines V1.7.0
e) National applicable laws and regulations.

5.1.1. VERSION NUMBER

The field “version” of the certificate describes the version used in certificate coding. In this profile, the version used is 3 (three).

5.1.2. CERTIFICATE EXTENSIONS

The components and extensions defined for certificates X509 v3 provide methods to associate features with users or public keys, as well as to manage the certification hierarchy.

5.1.3. PROFILE OF A QUALIFIED CERTIFICATE OF DIGITAL SIGNATURE

Certificate Component	Certificate Component	Section no. RFC5280	Value	Type	Comments
TbsCertificate	**Version**	4.1.2.1	3	m	Value 3 identifies the usage of certificates ITU-T X.509 version 3
	Serial Number	4.1.2.2	< Allocated by the CA to each certificate >	m	
	Signature	4.1.2.3	2.16.840.113549.1.1.11	m	Value MUST be equal to OID in signatureAlgorithm (below)
	Issuer Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.4	"CV" "ICP-CV" "SISP – Sociedade Interbancária e Sistemas de Pagamentos" "Certification Authority of SISP <nn>"	m	
	Validity Not Before Not After	4.1.2.5	< Date of issue> < Date of issue + 2 years >	m	Validity of 2 years.
	Subject Country (C) Organization (O) Organization Unit (OU) Organization Unit (OU) Locality (L) State or Province (ST) Title (title) Serial Number (serialNumber)	4.1.2.6	<CV> < Organization to which certificate holder belongs> < Natural person certificate – Qualified Signature> < Area/Department of organization to which certificate holder belongs> < Place of residence of holder> < District, state, island of residence of holder> < Quality of certificate holder within the scope of its use for qualified digital signature> < NIC or PAS > (1) < country code> – < identification number>	m m o m o o o o m	Optional. Only for professional purposes.
	Common Name (CN) Surname (SN) Given Name (givenName) e-mail		< Name of certificate holder > < Family names of certificate holder > < First name of certificate holder > < e-mail of certificate holder >	m m m m	

	Select Public Key Info Algorithm SubjectPublicKey	4.1.2.7	1.2.840.113549.1.1.1 <Public Key with modulus n of 2048 bits>	m	Used to keep the public key and identify the algorithm which the key is used with (e.g., RSA, DSA or Diffie-Hellman). 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 1} rsaEncryption OID must be used in algorithm field with a value of AlgorithmIdentifier type. The field parameters MUST be of ASN.1 to NULL type for the identifier of this algorithm.24
	Unique Identifiers	4.1.2.8		m	"unique identifiers" is always present in order to enable to reuse the names of subject and/or issuer 20
	X509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier Key Identifier	4.2.1.1	< The key identifier is composed by hash of 160-bit SHA-I >	m	The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits)
	Subject Key Identifier	4.2.1.2	< The key identifier is composed by hash of 160-bit SHA-I >	m	< The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits) >
	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	"O" selected "I" selected "I" selected "O" selected "O" selected "O" selected "O" selected "O" selected "O" selected	mc	This extension is marked as CRITICAL
	Certificate Policies policyIdentifier policyQualifiers	4.2.1.4	2.16.132.1.2.2.3.2 < policyQualifierID > cPSuri: https://pki.sisp.cv	O M o	Identifier of the Certificate Policy of SISP CA OID Description: The cPSuri feature contains a link for the Certificate Policy published by SISP CA. The link comes in URL form

	policyIdentifier policyQualifiers		2.16.132.1.3.2.3.2 < policyQualifierID > cPSuri: https://pki.sisp.cv	o o	Identifier of the Certification Practices Statement of SISP CA OID Description: The cPSuri feature contains a link for the Certification Practices Statement published by SISP CA. The link comes in URL form.
	Extended Ket Usage KeyPurposeId	4.2.1.12	Id-kp-emailProtection	o	OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sispca.crl	o o	URL to access CRL
	Qualified Certificate Statement id-qcs-pkixQCSyntax-v2 id-qcs-pkixQCSyntax-v2 id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance="0.4.0.1862.1.1" id-etsi-qcs-QcSSCD="0.4.0.1862.1.4" id-etsi-qcs-QcType="0.4.0.1862.1.6.1"		Statement made by the CE of PKI of SISP indicating that this certificate is issued in accordance with the ETSI TS 101 862. Statement made by the CE of PKI of SISP indicating that this certificate is issued in accordance with the SSCD policy, as per ETSI TS 101 862. Statement made by the CE of PKI of SISP indicating that this certificate is of qualified signature.
	Internet Certificate Extensions				
	Authority Information Access accessMethod accessLocation	4.2.2.1	1.3.6.1.5.5.7.4.8.2 http://ocsp.sisp.cv	o o o	OID value: (id-ad-ocsp) URL to access the OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same OID of algorithm identifier of the field signature in field of tbsCertificate sequence. sha256WithRSAEncryption OBJECT IDENTIFIER::= {iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20}
	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 holder (subject).

5.1.4. PROFILE OF A QUALIFIED CERTIFICATE OF ELECTRONIC SEAL

Certificate Component	Certificate Component	Section no. RFC5280	Value	Type	Comments
TbsCertificate	**Version**	4.1.2.1	3	m	Value 3 identifies the usage of certificates ITU-T X.509 version 3
	Serial Number	4.1.2.2	< Allocated by the CE to each certificate >	m	
	Signature	4.1.2.3	2.16.840.113549.1.1.11	m	Value MUST be equal to OID in signatureAlgorithm (below)
	Issuer Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.4	"CV" "ICP-CV" "SISP – Sociedade Interbancária e Sistemas de Pagamentos" "Certification Authority of SISP <nn>"	m	
	Validity Not Before Not After	4.1.2.5	< Date of issue> < Date of issue + 2 years >	m	Validity of 2 years.
	Subject Country (C) Organization (O) Organization Unit (OU) Organization Unit (OU) Organization Identifier (OI) Common Name (CN) e-mail	4.1.2.6	<CV> < Organization name as recorded by relevant authorities> < Qualified Electronic Seal> < Area/Department of the organization> < Tax identification number of certificate holder> < Organization Name as it is known> < Titleholder's e-mail>	m m m m o m m m	Type of Certificate E-mail used to send bulk messages.
	Select Public Key Info Algorithm	4.1.2.7			Used to keep the public key and identify the algorithm which the key is used with (e.g., RSA, DSA or Diffie-Hellman). rsaEncryption OID identifies RSA public keys.

	SubjectPublicKey		1.2.840.113549.1.1.1
			<Public Key with modulus n of 2048 bits>
				m	Pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }
					rsaEncryption OBJECT IDENTIFIER ::= {pkcs-1 1}
					rsaEncryption OID must be used in algorithm field with a value of AlgorithmIdentifier type. The field parameters MUST be of ASN.1 to NULL type for the identifier of this algorithm.24

	X509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier Key Identifier	4.2.1.1	< The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits) >	m	
	Subject Key Identifier	4.2.1.2	< The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits) >	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	"O" selected "I" selected "I" selected "O" selected "O" selected "O" selected "O" selected "O" selected "O" selected	mc	This extension is marked as CRITICAL
	Certificate Policies policyIdentifier policyQualifiers	4.2.1.4	2.16.132.1.2.2.3.2 < policyQualifierID > cPSuri: https://pki.sisp.cv	O M o	Identifier of the Certificate Policy of SISP CA OID Description: The cPSuri feature contains a link for the Certificate Policy published by SISP CA. The link comes in URL form
	policyIdentifier		2.16.132.1.2.2.3.2		Identifier of the Certification Practices Statement of SISP CA

	policyQualifiers		< policyQualifierID > cPSuri: https://pki.sisp.cv	o o	OID Description: The cPSuri feature contains a link for the Certification Practices Statement published by SISP CA. The link comes in URL form.
	Extended Ket Usage KeyPurposeId	4.2.1.12	Id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sispca.crl	o o	URL to access CRL
	Qualified Certificate Statement				
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance="0.4.0.1862.1.1"		Statement made by the CE of PKI of SISP indicating that this certificate is issued in accordance with the ETSI TS 101 862.
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD="0.4.0.1862.1.4"		Statement made by the CE of PKI of SISP indicating that this certificate is issued in accordance with the SSCD policy, as per ETSI TS 101 862.
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcType="0.4.0.1862.1.6.2"		Statement made by the CE of PKI of SISP indicating that this certificate is an Electronic Seal.
	Internet Certificate Extensions				
	Authority Information Access accessMethod accessLocation	4.2.2.1	 1.3.6.1.5.5.7.4.8.2 http://ocsp.sisp.cv	o o o	 OID value: (id-ad-ocsp) URL to access the OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same OID of algorithm identifier of the field signature in field of tbsCertificate sequence. sha256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20}
	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 holder (subject).

5.1.5. PROFILE OF AN ADVANCED AUTHENTICATION CERTIFICATE

Certificate Component	Certificate Component	Section no. RFC5280	Value	Type	Comments
TbsCertificate	**Version**	4.1.2.1	3	m	Value 3 identifies the usage of certificates ITU-T X.509 version 3
	Serial Number	4.1.2.2	< Allocated by the CE to each certificate >	m	
	Signature	4.1.2.3	2.16.840.113549.1.1.11	m	Value MUST be equal to OID in signatureAlgorithm (below)
	Issuer Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.4	“CV” “ICP-CV” “SISP – Sociedade Interbancária e Sistemas de Pagamentos” “Certification Authority of SISP <nn>”	m	
	Validity Not Before Not After	4.1.2.5	< Date of issue> < Date of issue + 2 years >	m	Validity of 2 years.
	Subject Country (C) Organization (O) Organization Unit (OU) Title (title) Common Name (CN) Surname (SN) Given Name (givenName) Serial Number (serialNumber)	4.1.2.6	<CV> < Organization name as recorded by relevant authorities> < Natural person certificate – Authentication> < Quality of certificate holder under its use, for authentication> < Name of certificate holder> < Family names of certificate holder> < Given names of certificate holder> < Unique identifier of certificate holder>	m m o m o m m m m	Change for optional Certificate type Equal to holder’s tax ID number.
	Select Public Key Info Algorithm				Used to keep the public key and identify the algorithm which the key is used with (e.g., RSA, DSA or Diffie-Hellman). rsaEncryption OID identifies RSA public keys.

	SubjectPublicKey	4.1.2.7	1.2.840.113549.1.1.1
			<Public Key with modulus n of 2048 bits>
				m	Pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }
					rsaEncryption OBJECT IDENTIFIER ::= {pkcs-1 1}
					rsaEncryption OID must be used in algorithm field with a value of AlgorithmIdentifier type. The field parameters MUST be of ASN.1 to NULL type for the identifier of this algorithm.24

	X509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier Key Identifier	4.2.1.1	The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits)	m	
	Subject Key Identifier	4.2.1.2	The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits)	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	“I” selected “O” selected “O” selected “O” selected “O” selected “O” selected “O” selected “O” selected “O” selected	mc	This extension is marked as CRITICAL
	Certificate Policies policyIdentifier policyQualifiers	4.2.1.4	2.16.132.1.2.2.3.2 < policyQualifierID > cPSuri: https://pki.sisp.cv	O m o	Identifier of the Certificate Policy of SISP CA OID Description: The cPSuri feature contains a link for the Certificate Policy published by SISP CA. The link comes in URL form
	policyIdentifier policyQualifiers		2.16.132.1.3.2.3.2 < policyQualifierID > cPSuri:	o	Identifier of the Certification Practices Statement of SISP CA

			https://pki.sisp.cv	o	OID Description: The cPSuri feature contains a link for the Certification Practices Statement published by SISP CA. The link comes in URL form.
	Extended Ket Usage Client Authentication	4.2.1.12	1.3.6.1.5.5.7.3.2	o	
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sispca.crl	o o	URL to access CRL
	Internet Certificate Extensions				
	Authority Information Access accessMethod accessLocation	4.2.2.1	1.3.6.1.5.5.7.4.8.2 http://ocsp.sisp.cv	o o o	OID value: (id-ad-ocsp) URL to access the OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same OID of algorithm identifier of the field signature in field of tbsCertificate sequence. sha256WithRSAEncryption OBJECT IDENTIFIER::= {iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20}
	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 holder (subject).

5.1.6. PROFILE OF AN WEB AUTHENTICATION CERTIFICATE

Componente do Certificado	Certificate Component	Section No. RFC5280	Value	Tipo	Comments
tbsCertificate	**Version**	4.1.2.1	3	m	Value 3 identifies the usage of certificates ITU-T X.509 version 3
	Serial Number	4.1.2.2	<Allocated by the CA to each certificate>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.11	m	Value MUST be equal to OID in signatureAlgorithm (below)
	Issuer	4.1.2.4		m	
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"SISP-Sociedade Interbancaria e Sistemas de Pagamentos"		
	Common Name (CN)		"Entidade Certificadora da SISP <nn> "		Oficial Designation of SISPCA
	Validity	4.1.2.5		m	Must use UTC Time until 2049, using *GeneralisedTime thereafter*
	Not Before		<date of issue>		
	Not After		<date of issue + 1 year>		Validity of 1 year.
	Subject	4.1.2.6		m	
	Country (C)		<Country>	m	
	Organization (O)		<Organization Name as recorded by relevant authorities >	m	
	Common Name (CN)		<Fully Qualified Domain Name of Web Server>	m	
	Organization Unit (OU)		<Area/Department of the Organization>	o	
	Street		<Organization Address>	m	
	Locality (L)		<Locality >	m	
	State or Province (ST)		<District, State, Island >	m	
	PostalCode		<Postal Code>	o	In accordance to the

	Serial Number (serialNumber) Subject Jurisdiction of Incorporation or Registration Field (OID 1.3.6.1.4.1.311.60.2.1.3) Subject Business Category Field		<Organization Unique ID as recorded by relevant authorities> <Country whereas the organization is doing business> <Organization Business Category: “Private” “Government Entity” “Business Entity” “Non-Commercial Entity”>	m m m	Guidelines for the Issuance and Management Of Extended Validation Certificates chapter 9.2.6: Subject:serialNumber In accordance to the Guidelines for the Issuance and Management Of Extended Validation Certificates chapter 9.2.5: subject:jurisdictionCountryName In accordance to the Guidelines for the Issuance and Management Of Extended Validation Certificates chapter 9.2.4: subject:businessCategory
	Select Public Key Info Algorithm subjectPublicKey	4.1.2.7	1.2.840.113549.1.1.1 < Public Key with modulus n of 2048 bits >	m	Used to keep the public key and identify the algorithm which the key is used with (e.g., RSA, DSA or Diffie-Hellman). 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 1} rsaEncryption OID must be used in algorithm field with a value of AlgorithmIdentifier type. The field parameters MUST be of ASN.1 to NULL type for the identifier of this algorithm.24
	Unique Identifiers	4.1.2.8		m	
	X509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier KeyIdentifier	4.2.1.1	The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits)	m	
	Subject Key Identifier	4.2.1.2	The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits)	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		“0” selected		
	CRL Signature		“0” selected		
	Encipher Only		“0” selected		
	Decipher Only		“0” selected		
	Cerificate Policies	4.2.1.4		m	
	policyIdentifier		2.16.132.1.3.2.3.2	m	Identifier of the Certification Practices Statement of SISP CA
	policyQualifiers		<policyQualiflierID> cPSuri: https://pki.sisp.cv	m	OID Description: The cPSuri feature contains a link for the Certification Practices Statement published by SISP CA. The link comes in URL form.
	policyIdentifier		2.16.132.1.2.2.3.2	m	Identifier of the Certificate Policy of SISP CA
	policyQualifiers		<policyQualiflierID> cPSuri: https://pki.sisp.cv	m	OID Description: The cPSuri feature contains a link for the Certificate Policy published by SISP CA. The link comes in URL form
	policyIdentifier		<2.23.140.1.1>	m	Identifier of the CAB Forum Certificate Policy for Extended Validation certificates
	Subject Alternative Name				
	GeneralName		DNS=<fully qualified domain name of the web server>	o	Maximum 10 domains Wildcard domains not acceptable
	CRLDistributionPoints	4.2.1.13		m	
	distributionPoint		http://crl.sisp.cv/sispca.crl	m	URL to access CRL
	Extended Key Usage	4.2.1.12			
	Server Authentication		1.3.6.1.5.5.7.3.1	mc	Server Authentication
	Client Authentication		1.3.6.1.5.5.7.3.2	mc	Client Authentication

	Qualified Certificate Statement id-qcs-pkixQCSyntax-v2 id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance="0.4.0.1862.1.1" id-etsi-qcs-QcType="0.4.0.1862.1.6.3"	m m	WEB Authentication Certificate
	Internet Certificate Extensions				.
	Authority Information Access accessMethod accessLocation	4.2.2.1	1.3.6.1.5.5.7.48.1 http://ocsp.sisp.cv/	m	OID Value: (id-ad-ocsp) URL to access the OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same OID of algorithm identifier of the field signature in field of tbsCertificate sequence. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20
	Signature Value	4.1.1.3	<Contains the digital signature issued by the CA>	m	When generating this signature, the CE certifies the connection between the public key and the certificate holder (subject).

5.1.7. OID OF THE ALGORITHM

The field “*signatureAlgorithm*” of the certificate contains the OID of the encrypted algorithm used by the CA to sign the certificate: 2.16.840.113549.1.1.11 (sha256WithRSAEncryption).

5.1.8. NAME FORMAT

As defined in section 4.1.

5.1.9. NAME CONSTRAINTS

In order to ensure total interoperability between the applications using digital certificates, it is recommended that only non-accented alphanumeric characters, space, underscore, dash, and period (⟦a-z⟧, ⟦A-Z⟧, ⟦0-9⟧,’’,’_’,’- ‘,’.’) be used in entries of Directory X.500. The use of accented characters is the sole responsibility of the Management Working Group of the PKI of SISP.

5.1.10. OID OF THE CERTIFICATE POLICY

The extension “certificate policies” includes the sequence of one or more informative expressions on the policy, each one of which consists of a policy identifier and optional qualifiers.

5.1.11. USAGE OF THE POLICY CONSTRAINTS EXTENSION

No stipulation.

5.1.12. SYNTAX AND SEMANTICS OF THE POLICY QUALIFIER

The extension “certificate policies” contains a policy qualifier to be used by certificate issuers and those who drafted the certificate policies. The qualifier type is “cPSuri”, which includes a link in the URL form for the Certification Practices Statement published by the CA, and a link, as an URL, for the Certificate Policy.

5.1.13. PROCESSING SEMANTICS FOR CRITICAL EXTENSION “CERTIFICATE POLICIES”

No stipulation.

5.2. SPECIMEN CERTIFICATE

The “specimen” certificates may be issued whenever it becomes necessary to validate the profile, the issuance process and/or its use. The specimen certificate may be issued for testing purposes, based on a liability agreement to be entered upon between SISP and the applicant Entity. This certificate differs from the usual certificates deemed final in the following:

- Certificate Profile: the prefix “specimen“ is added to the CommonName (CN);
- Certificate Issuance: pursuant to a specific form for internal use only.

The presence of the Auditor and the Security Administrator is mandatory when issuing “specimen” certificates.

5.3. PROFILE OF THE CERTIFICATE REVOCATION LIST (CRL)

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

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

The CRL is a list including the time-based identification of revoked certificates, signed by the CA and freely made available in a public repository. Each revoked certificate is identified in the CRL by its series number.

When an application makes use of a certificate (for example, to verify the digital signature of a remote user), the application verifies the certificate’s signature and validity and simultaneously obtains the most recent CRL and checks if the series number of the certificate is not contained therein. It should be noted that every CE shall issue a new CRL on a regular and periodic basis.

The CRL profile is in accordance with the:

a) Recommendation ITU.T X.509;
b) RFC 5280; and
c) National applicable legislation.

5.3.1. VERSION NUMBER

The field “version” of the CRL describes the version used in coding the CRL. In this profile, the version used is 2 (two).

5.3.2. PROFILE OF SISPCA01 CERTIFICATE REVOCATION LIST (CRL)

CRL Component	Certificate Component	Section no. RFC5280	Value	Type	Comments
tbsCertList	**Version**	5.1.2.1	1	m	Value 1 identifies the usage of version 2 of ITU X.509 standard
	Signature	5.1.2.2	1.2.840.113549.1.1.11	m	Contains the identifier of the algorithm used to sign the CRL. Value MUST be equal to OID in signatureAlgorithm field (below)
	Issuer Country (C) Organization (O) Common Name (CN)	5.1.2.3	"CV" "ICP-CV" "Root Certification Authority of Cabo Verde 01"	m	
	thisUpdate	5.1.2.4	< Date of issue of CRL>	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 CRL issue = thisUpdate + N>	m	This field indicates the date on which the next CRL will be issued. The next CRL may be issued prior to the date indicated but no later than that date. The issuers of the CRL MUST issue the CRL considering the time of nextUpdate greater or equal to all previous CRLs. Implementation MUST use the UTC time until 2049 and, from that date onwards, they must use the GeneralisedTime. N will be a maximum of 24 hours..
	revokedCertificates	5.1.2.6	<List of Revoked Certificates>	m	
	CRL Extensions	5.1.2.7		m	
	Authority Key Identifier Key Identifier	5.2.1	< The key identifier is composed by hash of 160-bit SHA-256 in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits) >	o	
	CRL Number	5.2.3	<unique, incremented sequential number>	m	
	CRL Distribution Point	5.2.5		c	

	DistributionPointName		http://crl.sisp.cv/sispca.crl		
	CRL Entry Extensions Reason Code	5.3 5.3.1		o	Value must 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	1.2.840.113549.1.1.11	m	MUST contain the same OID of algorithm identifier of the field signature in field of tbsCertificate sequence. sha256WithRSAEncryption OBJECT IDENTIFIER::= {iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20}
	Signature Value	5.1.1.3	<Contains the digital signature issued by the CA>	m	When generating this signature, the CE certifies the connection between the public key and the certificate holder (subject).

5.4. OCSP CERTIFICATE PROFILE

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

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

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

The profile of OCSP online validation certificates is in conformity with the following standards:

a) Recommendation ITU.T X.509;
b) RFC 5280; and
c) National applicable laws and regulations.

5.4.1. VERSION NUMBER

The field “version” of the certificate describes the version used in coding the certificate. In this profile, the version used is 3 (three).

5.4.2. CERTIFICATE EXTENSIONS

The components and extensions defined for certificates X.509 v3 provide methods to associate features with users or public keys, as well as to manage the certification hierarchy.

5.4.3. PROFILE OF THE OCSP CERTIFICATE OF SISPCA01

Certificate Component	Certificate Component	Section no. RFC5280	Value	Type	Comments
tbsCertificate	**Version**	4.1.2.1	3	m	Value 3 identifies the usage of certificates ITU-T X.509 version 3
	Serial Number	4.1.2.2	< Allocated by the CA to each certificate >	m	
	Signature	4.1.2.3	2.16.840.113549.1.1.11	m	Value MUST be equal to OID in signatureAlgorithm (below)
	Issuer Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.4	"CV" "ICP-CV" "SISP-Sociedade interbancária e Sistemas de Pagamentos" "Name"	m	Name of Subordinate CA of SISP
	Validity Not Before Not After	4.1.2.5	< Date of issue> < Date of issue + 5,4 years >	m	MUST use UTC time up to 2049, date from which *GeneralisedTime* will be used. Validity of 5 years and four months.
	Subject Country (C) Organization (O) Organization Unit (OU) Organization Unit (OU) Common Name (CN)	4.1.2.6	"CV" "ICP-CV" "Online Validation" "SISP–Sociedade Interbancária e Sistemas de Pagamentos" "Online Validation Service of SISPCA01 <nnnn>"	m	<nnn> - Certificate sequence
	Select Public Key Info Algorithm SubjectPublicKey	4.1.2.7	1.2.840.113549.1.1.1 <Public Key with modulus n of 4096 bits>	m	Used to keep the public key and identify the algorithm which the key is used with (e.g., RSA, DSA or Diffie-Hellman). 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 1} rsaEncryption OID must be used in algorithm field with a value of AlgorithmIdentifier type. The field parameters MUST be of ASN.1 to NULL type for the identifier of this algorithm.24

	X509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier Key Identifier	4.2.1.1	< The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits) >	m	
	Subject Key Identifier	4.2.1.2	< The key identifier is composed by hash of 160-bit SHA-I in the value of BIT STRING of subjectPublicKey (excluding tag, length, and number of unused bits) >	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	“I” selected “I” selected “O” selected “O” selected “O” selected “O” selected “O” selected “O” selected “O” selected	mc	This extension is marked as CRITICAL
	Certificate Policies policyIdentifier policyQualifier	4.2.1.4	2.16.132.1.2.2.3.2 policyQualifierID cPSuri: http://pki.sisp.cv	o m o	Identifier of the Certificate Policy of SISP CA OID Description: “the feature cPSuri contains a link for the Certification Practice Statement published by SISP CA. The link is under the form of an URL”
	policyIdentifier policyQualifier		2.16.132.1.3.2.3.2 policyQualifierID cPSuri: http://pki.sisp.cv	o o	Identifier of the Certification Practices Statement of SISP CA OID Description: “the feature cPSuri contains a link for the Certification Practice Statement published by SISP CA. The link is under the form of an URL”
	Extended Ket Usage OCSP signer	4.2.1.12	1.3.6.1.5.5.7.3.9	c	OID description: Indicates that the private key corresponding to the X.509 certificate may be used to sign OCSP replies.
	OCSPNocheck		NULL	o	

					It is not an extension defined in the RFC 3280. Defined on http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.48.1.5 html, this extension must be included in an OCSP signature certificate. This extension advises the OCSP customer that this signature certificate may be reliable even when not validated by the OCSP server (whereas the reply would be signed by the OCSP server and the customer would have to validate the status of the signature certificate).
	Internet Certificate Extensions				
	Authority Information Access AccessMethod AccessLocation	4.2.2.1	1.3.6.1.5.5.7.48.1.2 http://ocsp.sisp.cv	o o o	This extension HAS to be critical OID Value: (id-ad-ocsp) URL to access the OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same OID of algorithm identifier of the field signature in field of tbsCertificate sequence. sha256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20}
	Signature Value	4.1.1.3	<Contains the digital signature issued by the CA>	m	When generating this signature, the CE certifies the connection between the public key and the certificate holder (subject).

6. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE'S LIFE-CYCLE

6.1. CERTIFICATE APPLICATION

6.1.1. WHO CAN SUBMIT A CERTIFICATE APPLICATION

The application for a certificate must be submitted on the specific form made available on the website of SISP, S.A. or at the CAs.

The qualified certificates of digital signature or authentication may be subscribed by:

- The certificate holder, whenever the certificate is issued for a natural person;
- The titleholder and the legal representatives of the entity, whenever the certificate is issued for a natural person associated to (on behalf of) an entity.

The qualified certificate of electronic seal and web authentication may be subscribed by:

- The representatives of the legal or collective person that legally and statutorily bind it, who must appoint a physical person responsible for handling and operating the certificate. This person shall be named as "Technical Manager".

6.1.2. ENROLMENT PROCESS AND RESPONSIBILITIES

The application for a qualified certificate is the responsibility of the stakeholders identified in the previous section. Likewise, they are responsible for the accuracy of the information provided and for making available all documents supporting such information.

The registration process is deemed effective once the information included in the application is verified and confirmed by SISP or a designated RE.

The registration process starts by filling out the form made available on SISP's website or at any designated RE.

6.2. CERTIFICATE APPLICATION PROCESSING

Once received by the designated RE, the certificate applications are considered valid if they meet the following requisites:

a) Verification of all documents and authorizations required;
b) Verification of the applicant's identity;
c) Verification of the accuracy and integrity of the certificate application;
d) Certificate request is addressed to SISPCA.

Sections 4.2, 6.2.1 and 6.3 describe the entire process in detail.

6.2.1. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

6.2.1.1. Certificate for a Natural Person

As indicated in section 4.2.

6.2.1.2. Certificate for a Legal Person

As indicated in section 4.2.

6.2.2. APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

In order to be approved, a certificate application must comply with the provisions set in paragraphs 6.2 and 6.2.1.

Where this is not provided, the certificate application must be rejected.

6.2.3. TIME TO PROCESS CERTIFICATE APPLICATIONS

Following approval of the certificate application, the certificate shall be issued within no later than five (5) working days.

6.3. CERTIFICATE ISSUANCE

6.3.1. ACTIONS DURING CERTIFICATE ISSUANCE

Certificate issuance is automatically performed by the SISPCA platform after recording and validating the certificate application, being the key pair generated on the card (or USB token) with encrypted chip or by subscriber via a CSR.

6.3.2. NOTIFICATION OF CERTIFICATE ISSUANCE TO HOLDER

The certificate holder is deemed notified of the certificate issuance upon its receipt.

6.4. CERTIFICATE ACCEPTANCE

6.4.1. PROCEDURES FOR CERTIFICATE ACCEPTANCE

The certificate is deemed to have been accepted once received.

It is important to note that before making available the certificate to the representative(s) and, consequently, providing them with all the functionalities required for the use of the private key and certificate, it must be ensured that the subscriber:

a) Is aware of his rights and responsibilities;
b) Is aware of the certificate's functionalities and contents;
c) Formally accepts the certificate and the terms and conditions for its use by duly signing the certificate receipt and acceptance form;

d) The procedures needed in case of certificate expiration, revocation, and renewal, as well as the terms, conditions, and scope of use of such certificate, are defined in this Certificate Policy and the respective Certification Practices Statement.

6.4.2. PUBLICATION OF THE CERTIFICATE

SISPCA01 shall not publish the certificates issued, making them fully available to the subscriber in the conditions referred to in 6.4.1.

6.4.3. NOTIFICATION OF CERTIFICATE ISSUANCE TO OTHER ENTITIES

No stipulation.

6.5. KEY PAIR AND CERTIFICATE USAGE

6.5.1. SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers or certificate titleholders shall use their private keys only for the purpose for which these are meant (as set forth in the “KeyUsage” certificate field) and always lawfully.

Their use is only permitted:

a) To anyone appointed for that purpose on the “Subject” field of the certificate;
b) Under the terms defined in section 3.5 of the Certification Practices Statement (CPS);
c) As long as the certificate is valid and does not appear in the CRL of SISP CA.

6.5.2. USE OF CERTIFICATE AND PUBLIC KEY BY RELYING PARTIES

In using the certificate and the public key, relying parties may only rely on the certificates, considering only the provisions of this Certificate Policy and respective CPS.

To that end, relying parties shall ensure compliance with the following conditions:

a) Be aware of, and understand, the usage and functionalities provided by public key and certificate cryptography;
b) Be responsible for its proper use;
c) Read and understand the terms and conditions described in the certification policies and practices;
d) Verify the certificates (validation of trust chains) and CRL by paying particular attention to its extensions marked as critical, as well as to key objectives;
e) Rely on the certificates, using them while they are valid.

6.6. CERTIFICATE RE-KEY

Renewal of the certificate keys (certificate re-key) is the process in which a titleholder (or sponsor) generates a new key pair and submits a request for the issuance of a new certificate certifying the new public key. This process, within the scope of the present Certificate Policy, is called certificate renewal with new key pair generation.

Certificate renewal with new key pair generation is executed as stipulated in section 6.3.

6.6.1. CIRCUMSTANCES FOR CERTIFICATE RE-KEY

The following are considered valid reasons for renewing the certificate with new key pair generation:

a) The certificate is about to expire;
b) The certificate support is about to expire;
c) The information contained in the certificate has been changed.

6.6.2. WHO CAN REQUEST CERTIFICATION OF A NEW PUBLIC KEY

As outlined in section 6.1.1.

6.6.3. PROCESSING CERTIFICATE RE-KEYING REQUESTS

As outlined in sections 6.1.2 and 6.2.

6.6.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

As outlined in section 6.3.2.

6.6.5. CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

As outlined in section 6.4.1.

6.6.6. PUBLICATION OF THE RE-KEYED CERTIFICATE

As outlined in section 6.4.2.

6.6.7. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO OTHER ENTITIES

As outlined in section 6.4.3.

6.7. CERTIFICATE SUSPENSION AND REVOCATION

In practice, certificate suspension and revocation are 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 cannot be validated again. Conversely, suspended certificates may recover their validity.

6.7.1. CIRCUMSTANCES FOR SUSPENSION

SISPCA01 will not suspend certificates.

6.7.2. WHO CAN REQUEST SUSPENSION

No stipulation.

6.7.3. PROCEDURE FOR SUSPENSION REQUEST

No stipulation.

6.7.4. LIMIT OF PERIOD OF SUSPENSION

No stipulation.

6.7.5. CIRCUMSTANCES FOR REVOCATION

A certificate shall be revoked due to one of the following circumstances:

- Private key is compromised;
- Card/token has been lost or stolen;
- Data update/change;
- Card/token is damaged or deteriorated;
- The quality of the certificate holder, as affixed in the digital certificate, ceases to be valid;
- Powers of representation included in the certificate have been suspended or changed;
- Improper use of the certificate;
- Failure in using the card/token;
- By court order or, provided it is duly justified by the entities comprised in the IPC-CV, namely:
    - The Managing Board of the ICP-CV;
    - The Accreditation Authority;
    - The ECR-CV.
- Termination of service.

The certificate shall be revoked within a maximum of 24 hours.

6.7.6. WHO CAN REQUEST REVOCATION

The following entities are entitled to request revocation whenever one of the circumstances described in 6.7.5 above occur:

- The legal representatives of the Subordinate Certification Authority;
- SISP, S.A.;
- A relying party, provided that it proves that the certificate has been used for purposes other than those anticipated.

SISPCA01 should store all information used to verify the identity and authenticity of the entity requesting revocation, guaranteeing the verification of the identity of its legal representatives by legally recognized means, and rejecting any powers of representation for certificate revocation purposes.

6.7.7. PROCEDURES FOR REVOCATION REQUEST

Subscribers requesting revocation are required to follow the procedures below indicated:

- All revocation requests must be addressed to SISP, S.A. or to Registration Entities in writing or by digitally signed electronic message, in a specific form indicating the reasons or circumstances underlying the revocation request;
- Identification and authentication of the entity that submits the revocation request;
- Recording and archiving the revocation request form;
- Analysis of the revocation request by the Authentication Working Group of the PKI of SISP, which shall approve or reject the revocation request;
- Where a certificate is revoked, the revocation shall be published in the respective CRL.

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

- Date of the revocation request;
- Name of the certificate titleholder;
- Detailed description of the circumstances or reasons for the revocation request;
- Name and position of the person who requested the revocation;
- Contact details of the person who requested the revocation;
- Signature of the person who requested the revocation.

6.7.8. DATE ON WHICH REVOCATION BECOMES EFFECTIVE

Revocation shall be immediately executed. After complying with all the procedures and verifying the validity of the request, the latter can no longer be cancelled.

6.7.9. TIME WITHIN WHICH REVOCATION REQUEST MUST BE PROCESSED

The revocation request must be immediately handled and processed within a maximum of 24 (twenty-four) hours.

6.7.10. REVOCATION CHECKING REQUIREMENTS BY RELYING PARTIES

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

6.7.11. CRL (CERTIFICATE REVOCATION LIST) ISSUANCE FREQUENCY

SISPCA01 shall make available a new CRL database on a daily basis.

6.7.12. MAXIMUM PERIOD BETWEEN CRL ISSUANCE AND PUBLICATION

The maximum period between issuance and publication of the CRL cannot exceed 60 (sixty) minutes.

6.7.13. ONLINE CERTIFICATE REVOCATION/STATUS CHECKING AVAILABITY

SISPCA01 provides online certificate status checking services via the OCSP. This service may be accessed through http://ocsp.sisp.cv.

The maximum period between revocation and online validation via the OCSP cannot exceed 30 (thirty) minutes.

6.7.14. ONLINE REVOCATION CHECKING REQUIREMENTS

The relying parties must have software capable of executing the OCSP protocol in order to obtain information on certificate status.

6.7.15. OTHER FORMS AVAILABLE FOR DISSEMINATING REVOCATION

The certificate holder shall be notified accordingly whenever the certificate is revoked.

6.7.16. SPECIAL REQUIREMENTS REGARDING PRIVATE KEY COMPROMISE

In case the private key of SISPCA01 is compromised, appropriate measures must be taken to cope with the incident.

The responses to such incident may include:

- Revocation of SISPCA01 certificate and all certificates issued within the trust hierarchy of SISPCA;

- Notification of the Accreditation Authority and all titleholders of certificates issued within the trust hierarchy of SISP CA;
- Generation of a new key pair for SISPCA;
- Renewal of all certificates issued within the trust hierarchy of SISPCA.

7. AUDITS AND SECURITY STANDARDS

Described in sections 7, 8, and 4.3 of the Certification Practices Statement available on http://pki.sisp.cv.

BIBLIOGRAPHICAL REFERENCES

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