SISP – SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTO

SISP Certificate Policy

- CP of SISP Root Certification Authority -

Code:	PLRC003.05
Version:	5.0
Version Date:	June 30, 2019
Created by:	SISP
Approved by:	Board of Directors
Level of Confidentiality:	Public

Change Control Log

Date	Version	Created by	Description of the Amendment
January 16, 2018	1.0	SISP	Document creation. Established.
March 21, 2018	2.0	SISP	Document updated
April 13, 2018	3.0	SISP	Updating of the document model
July 31, 2018	4.0	SISP	Change to the PKI hierarchical structure
June 39, 2019	5.0	SISP	Web Authentication (SSL) Certificate

Related Documents

Certification Practice Statement of SISP Root CA

Jair Elísio Andrade Ferreira Silva

Digitally signed by Jair Elísio Andrade Ferreira Silva
DN: email=jsilva@sisp.cv, cn=Jair Elísio Andrade Ferreira Silva, serialNumber=CV-4874, givenName=Jair Elísio, sn=Andrade Ferreira Silva, title=Diretor-Geral, ou=Direção SISP, ou=Certificado para pessoa singular - Assinatura Qualificada, o=Sociedade Interbancária e Sistemas de Pagamentos S.A., l=Praia, st=Santiago, c=CV
Date: 2020.03.26 17:16:57 -01'00'

Table of Contents

1. INTRODUCTION 6

1.1. OBJECTIVES 6

1.2. TARGET AUDIENCE 6

1.3. DOCUMENT LAYOUT 6

2. ACRONYMS AND DEFINITIONS 6

2.1. ACRONYMS 7

2.2. DEFINITIONS 8

3. GENERAL CONTEXT 11

3.1. OBJECTIVE 11

3.2. OVERVIEW 11

3.3. DOCUMENT IDENTIFICATION 11

3.4. POLICY ADMINISTRATION 12

4. IDENTIFICATION AND AUTHENTICATION 12

4.1. NAMING 12

4.1.1. TYPES OF NAMES 12

4.1.2. CERTIFICATE AND KEY PAIR USAGE BY HOLDER 13

4.2. INITIAL IDENTITY VALIDATION 13

4.2.1. METHOD OF PROVING POSSESSION OF PRIVATE KEY 13

4.2.2. AUTHENTICATION OF A LEGAL PERSON'S IDENTITY 13

4.2.3. AUTHENTICATION OF A NATURAL PERSON'S IDENTITY 14

4.2.4. NON-VERIFIED INFORMATION ON THE SUBSCRIBER/TITLEHOLDER 14

4.2.5. VALIDATION OF A COMPETENT AUTHORITY 14

4.2.6. INTEROPERABILITY CRITERIA 14

4.3. IDENTIFICATION AND AUTHENTICATION FOR A REVOCATION REQUEST 14

5. CERTIFICATE AND CRL PROFILES 14

5.1. CERTIFICATE PROFILE 14

5.1.1. VERSION NUMBER 15

5.1.2. CERTIFICATE EXTENSIONS 15

5.1.3. CERTIFICATE PROFILE 15

5.1.4. OID OF THE ALGORITHM 18

5.1.5. NAME FORMAT 18

5.1.6. NAME CONSTRAINTS 18

5.1.7. OID OF THE CERTIFICATE POLICY 18

5.1.8. USAGE OF THE POLICY CONSTRAINTS EXTENSION 18

5.1.9. SYNTAX AND SEMANTICS OF THE POLICY QUALIFIER 18
5.1.10. PROCESSING SEMANTICS FOR CRITICAL EXTENSION "CERTIFICATE POLICIES" 18
5.2. PROFILE OF THE CERTIFICATE REVOCATION LIST (CRL) 18
5.2.1. VERSION NUMBER 19
5.2.2. PROFILE OF THE CRL OF SISP ROOT CA 19
5.3. OCSP CERTIFICATE PROFILE 22
5.4. CERTIFICATE PROFILE OF SUBORDINATE CERTIFICATION ENTITIES 22
5.4.1. VERSION NUMBER 22
5.4.2. CERTIFICATE EXTENSIONS 22
5.4.3. CERTIFICATE PROFILE 23
6. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE'S LIFE-CYCLE 26
6.1. CERTIFICATE APPLICATION 26
6.1.1. WHO CAN SUBMIT A CERTIFICATE APPLICATION 26
6.1.2. ENROLMENT PROCESS AND RESPONSIBILITIES 26
6.2. CERTIFICATE APPLICATION PROCESSING 26
6.2.1. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS 26
6.2.2. APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS 27
6.2.3. TIME TO PROCESS CERTIFICATE APPLICATIONS 27
6.3. CERTIFICATE ISSUANCE 27
6.3.1. ACTIONS DURING CERTIFICATE ISSUANCE 27
6.3.2. NOTIFICATION TO SUBSCRIBER OF ISSUANCE OF CERTIFICATE 28
6.4. CERTIFICATE ACCEPTANCE 28
6.4.1. PROCEDURES FOR CERTIFICATE ACCEPTANCE 28
6.4.2. PUBLICATION OF THE CERTIFICATE 28
6.4.3. NOTIFICATION OF CERTIFICATE ISSUANCE TO OTHER ENTITIES 28
6.5. KEY PAIR AND CERTIFICATE USAGE 28
6.5.1. SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE 29
6.5.2. USE OF CERTIFICATE AND PUBLIC KEY BY RELYING PARTIES 29
6.6. CERTIFICATE RE-KEY 29
6.6.1. CIRCUMSTANCES FOR CERTIFICATE RE-KEY 29
6.6.2. WHO CAN REQUEST CERTIFICATION OF A NEW PUBLIC KEY 30
6.6.3. PROCESSING CERTIFICATE RE-KEYING REQUESTS 30
6.6.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER 30
6.6.5. CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE 30
6.6.6. PUBLICATION OF THE RE-KEYED CERTIFICATE 30
6.6.7. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO OTHER ENTITIES 30

6.7. CERTIFICATE SUSPENSION AND REVOCATION 30
6.7.1. CIRCUMSTANCES FOR SUSPENSION 30
6.7.2. WHO CAN REQUEST SUSPENSION 30
6.7.3. PROCEDURE FOR SUSPENSION REQUEST 30
6.7.4. LIMIT OF PERIOD OF SUSPENSION 31
6.7.5. CIRCUMSTANCES FOR REVOCATION 31
6.7.6. WHO CAN REQUEST REVOCATION 31
6.7.7. PROCEDURES FOR REVOCATION REQUEST 31
6.7.8. DATE ON WHICH REVOCATION BECOMES EFFECTIVE 32
6.7.9. TIME WITHIN WHICH REVOCATION REQUEST MUST BE PROCESSED 32
6.7.10. REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES 32
6.7.11. CRL ISSUANCE FREQUENCY 32
6.7.12. MAXIMUM PERIOD BETWEEN CRL ISSUANCE AND PUBLICATION 33
6.7.13. ONLINE REVOCATION STATUS/CHECKING AVAILABITY 33
6.7.14. ONLINE REVOCATION CHECKING REQUIREMENTS 33
6.7.15. OTHER FORMS AVAILABLE FOR DISSEMINATING REVOCATION 33
6.7.16. SPECIAL REQUIREMENTS REGARDING PRIVATE KEY COMPROMISE 33
BIBLIOGRAPHICAL REFERENCES 34

1. INTRODUCTION

1.1. OBJECTIVES

This document aims at defining the policies used by SISP Root Certification Authority (SISP Root CA) in the certificate issuance process.

1.2. TARGET AUDIENCE

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

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 Practice Statement of SISP Root CA.

2. ACRONYMS AND DEFINITIONS

Alist of relevant acronyms and definitions used in this document are provided below:

2.1. ACRONYMS

Acronym	
ANSI	American National Standards Institute
CA	Certification Authority (the same as for CE)
CE	Certification Entity
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DL	Decree-Law
DN	Distinguished Name
ICP-CV	Public Key Infrastructure of Cabo Verde
MAC	Message Authentication Codes
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
SHA	Secure Hash Algorithm
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.	Digital record that links signature-verification

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

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

3. GENERAL CONTEXT

3.1. OBJECTIVE

The present document is a Certificate Policy (CP) and seeks to define a set of policies and data required for certificate issuance and validity 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 Root Certification Authority (SISP Root CA) in the certificate issuance and management process.

All certificates issued under SISP ROOT CA 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 Practice Framework;
b) RFC 5280 – Internet X.509 Public Key Infrastructure – Certificate and CRL Profile.

Any certificate issued by SISP Root CA shall include a reference to the present Certificate Policy, Document Code no. PLRC003.05, 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 complements the requirements laid down in the Certification Practice Statement of SISP Root Certification Entity.

3.3. DOCUMENT IDENTIFICATION

This document is the Certificate Policy (CP) of SISP Root Certification Authority. The CP is represented on a certificate through a single number named as “Object Identifier” (OID). The OID associated with this paper is 2.16.132.1.2.2.3.

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

DOCUMENT INFORMATION	
Document Version	Version 5.0
Document Status	Approved
OID	2.16.132.1.2.2.3
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 SISP Root CA.

4.1.1. TYPES OF NAMES

The certificate of SISP Root CA is identified by the single name DN (Distinguished Name) in accordance with the standard X.509. The single name of the certificate of SISP Root CA is identified through the following components:

Feature	Code	Value
Country	C	Cabo Verde
Organization	O	SISP – Sociedade Interbancária e Sistemas de Pagamentos, SA
Common Name	CN	SISP Root CA

4.1.2. CERTIFICATE AND KEY PAIR USAGE BY HOLDER

SISP is the titleholder of the certificate of SISP Root CA signed by ECR-CV (Root Certification Entity of Cabo Verde), by using its private key to sign certificates of Issuing Certification Authorities, certificate of the Time-Stamping Certification Entity (SISP TSA), the respective Certificate Revocation List (CRL), as well as certificates destined to the OCSP service, in light of its CPS.

4.2. INITIAL IDENTITY VALIDATION

4.2.1. METHOD OF PROVING POSSESSION OF PRIVATE KEY

In the certificate of SISP Root CA, proving possession of the private key is ensured through the physical presence of the relevant Working Groups and a representative of the Accreditation Entity at the issuance ceremony of such certificates. The certificate request will be submitted in the ceremony and generated in the format PKC#10, whose signature over the public key information will be validated by the ECR-CV.

4.2.2. AUTHENTICATION OF A LEGAL PERSON'S IDENTITY

SISP should store all information used to verify the identity of the certification entity, guaranteeing the verification of the identity of its legal representatives by legally recognized means, and, in case the latter are not present in the certificate issuance ceremony, that the petitioner holds enough powers to request the mentioned subscription.

The process of authenticating a legal or collective 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 which, statutorily, represent that legal person.

The document on which the issuance of a CA certificate is based includes, *inter alia*, the following items:

a) Documents for the purposes of identifying the CA and its legal name;
b) Tax identification number, headquarters, corporate object, names of the members of the corporate bodies and other persons who have the power to bind the CA;
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 CA;
d) Address and other contact details;
e) Indication that the certificate is issued for the entity, as a CA under the supervision of SISP Root CA, in the trust hierarchy of PKI of SISP and ICP-CV, in conformity with the present CP;
f) Distinguished name (DN) to be allocated to the CA certificate;
g) Information, if required, related with the identification and powers of the representatives appointed by the CA to participate in the certificate issuance ceremony;

h) Additional information concerning the certificate request to be submitted during the CE's certificate issuance ceremony.

4.2.3. AUTHENTICATION OF A NATURAL PERSON'S IDENTITY

No stipulation.

4.2.4. NON-VERIFIED INFORMATION ON THE SUBSCRIBER/TITLEHOLDER

The entire information referred to in paragraphs 4.2.2 and 4.2.3 is checked.

4.2.5. VALIDATION OF A COMPETENT AUTHORITY

No stipulation.

4.2.6. INTEROPERABILITY CRITERIA

No stipulation.

4.3. IDENTIFICATION AND AUTHENTICATION FOR A REVOCATION REQUEST

Given the consequences of revoking the certificate of SISP Root CA, a formal document of the Board of Directors of SISP is required, including namely:

a) The decision of the Board of Directors to revoke the certificate of SISP Root CA;
b) The reasons underlying the certificate revocation;
c) Information, if necessary, related to the identification and powers of the representatives appointed by the entity to be present in the certificate revocation ceremony of SISP Root CA.

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 CA and validate the user's public key. As a rule, validation of a user's public key may require a chain of multiple certificates, including the user's public key certificate signed by a CA and zero or more additional certificates of CAs signed by other CAs.

The profile of the certificates issued by SISP Root CA 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 Practice Framework;
b) RFC 5280 – Internet X.509 PKI – Certificate and CRL Profile;
c) 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. CERTIFICATE PROFILE

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" "ARME-Agencia Nacional de Comunicacoes" "Entidade de Certificacao Raiz de Cabo Verde 01"	m	Official Name of the CRE Cabo Verde
	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 renewable every 6 years.
	Subject Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.6	<SISP Root CA> "CV" "ICP-CV" "SISP – Sociedade Interbancária e Sistemas de Pagamentos" "Entidade de Certificacao Raiz da SISP 01"	m	
	Subject 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

	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 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 "O" selected "O" selected "O" selected "O" selected "I" selected "I" selected "O" selected "O" selected	mc	This extension is marked as CRITICAL
	Certificate Policies	4.2.1.4		o	
	Basic Constraints CA PathlenConstraint	4.2.1.9	TRUE	o m o	Indicates the Entity type whom the certificate is intended for; basic restriction, if the CA = true the certificate may sign a CE
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sisprootca.crl	o m	
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	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).

5.1.4. OID OF THE ALGORITHM

The field "*signatureAlgorithm*" of the certificate contains the OID of the cryptographic algorithm used by the CA to sign the certificate: 2.16.840.113549.1.1.11 (sha256WithRSAEncryption12).

5.1.5. NAME FORMAT

As defined in section 4.1.

5.1.6. 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.

5.1.7. OID OF THE CERTIFICATE POLICY

The extension "certificate policies" is not active in the certificate of SISP Root CA.

5.1.8. USAGE OF THE POLICY CONSTRAINTS EXTENSION

No stipulation.

5.1.9. SYNTAX AND SEMANTICS OF THE POLICY QUALIFIER

No stipulation.

5.1.10. PROCESSING SEMANTICS FOR CRITICAL EXTENSION "CERTIFICATE POLICIES"

No stipulation.

5.2. PROFILE OF THE CERTIFICATE REVOCATION LIST (CRL)

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

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

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

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

The CRL profile is in accordance with the:

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

5.2.1. 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).

5.2.2. PROFILE OF THE CRL OF SISP ROOT CA

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	2.16.840.113549.1.1.11	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" "Entidade de Certificacao Raiz de 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 90 days.
	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	<incremented sequential number>	m	
	Issuing DistributionPoint DistributionPointName	5.2.5	http://crl.sisp.cv/sisprootca.crl	c	

	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	2.16.840.113549.1.1.11	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).

5.3. OCSP CERTIFICATE PROFILE

No stipulation.

5.4. CERTIFICATE PROFILE OF SUBORDINATE CERTIFICATION ENTITIES

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 CA and validate the user's public key. As a rule, validation of a user's public key may require a chain of multiple certificates, including the user's public key certificate signed by a CA and zero or more additional certificates of CAs signed by other CAs.

The profile of the certificate of Subordinate Certification Entities 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 Practice Framework;
b) RFC 5280 – Internet X.509 PKI – Certificate and CRL Profile;
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. CERTIFICATE PROFILE

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" "ARME-Agencia Nacional de Comunicacoes" "Entidade de Certificacao Raiz de Cabo Verde 01"	m	Official Name of the CE of SISP
	Validity Not Before Not After	4.1.2.5	< Date of issue> < Date of issue + 6 years>	m	Validity of 6 years renewable every 3 years.
	Subject Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.6	"CV" "ICP-CV" "SISP – Sociedade Interbancária e Sistemas de Pagamentos" "SISP Certification Entity < nn>"	m	
	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

	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 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 "O" selected "O" selected "O" selected "O" selected "I" selected "I" selected "O" selected "O" selected	mc	This extension is marked as CRITICAL
	Certificate Policies policyIdentifier policyQualifier	4.2.1.4	2.16.132.1.1.2.3 policyQualifierID cPSuri: http://pki.sisp.cv	o m o	Identifier of the Certification Practice Statement of EC Raiz da SISP (id-qt-cps PKIX CPS Pointer Qualifier) OID Description: "the feature cPSuri contains a link for the Certification Practice Statement published by SISP ROOT CA. The link is under the form of an URL"
	policyIdentifier policyQualifier		2.16.132.1.2.2.3 policyQualifierID cPSuri: http://pki.sisp.cv	m o	Identifier of the Certification Practice Statement of EC Raiz da SISP (id-qt-cps PKIX CPS Pointer Qualifier) OID Description: "the feature cPSuri contains a link for the Certification Practice Statement published by SISP ROOT CA. The link is under the form of an URL"
	Basic Constraints CA PathlenConstraint	4.2.1.9	TRUE	o m o	Indicates the Entity type whom the certificate is intended for; basic restriction, if the CA = true the certificate may sign a CE

	CRLDistributionPoints distributionPoint	4.2.1.13	 http://crl.sisp.cv/sispca.crl	o m	
	Internet Certificate Extensions				
	Authority Information Access AccessMethod AccessLocation	4.2.2.1	1.3.6.1.5.5.7.48.2 http://ocsp.sisp.cv	m m	OID Value: (id-ad-ocsp)
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	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

An application for the certificate of CA SISP Root can only be completed and submitted by the Board of Directors of the SISP – Sociedade Interbancária e Sistemas de Pagamentos, S.A.

The certificate of the Subordinate CA may only be submitted by the representatives(s) of the legal or collective person that legally and statutorily binds it.

6.1.2. ENROLMENT PROCESS AND RESPONSIBILITIES

The process of registering the CA's certificate includes the following steps to be taken by the relevant Working Groups:

- Key generation process (public and private key) in appropriate cryptographic environment;
- Generation of the corresponding PKCS#10 in appropriate cryptographic environment.

6.2. CERTIFICATE APPLICATION PROCESSING

The certificate application is processed as follows:

a) Creation of the certificate key pair and signature in appropriate cryptographic environment, in accordance with the profile defined in this policy;
b) Making available the certificate.

Sections 6.2.1 and 6.3 describe the entire process in detail.

6.2.1. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The relevant Working Groups shall execute the identification and authentication of all information deemed necessary in accordance with the stipulations of section 6 of this document.

1. The relevant Working Groups shall approve the application for the issuance of a SISP Root CA Certificate when:
   a. Express consent has been given by the Management Group of the PKI of SISP.
2. Certificate for a Issuing Certification Authority:

a. Successful identification and authentication of all information deemed necessary under the terms set forth in section 4 – all information used for verifying the identity and powers shall be kept;
b. PKCS#10 is valid.

In any other situation, the certificate application will not be accepted.

Following issuance of the certificate, the relevant Working Groups shall provide the certificate to the Management Group of the PKI of SISP and, where appropriate, to the legal representatives of the Subordinate Certification Entity.

6.2.2. APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

In order to be approved, any 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 performed in a ceremony held in the high security area of the CA, at which the following participants will be present:

- The legal representatives of SISP, S.A., its proxies or those of the subordinate entities appointed for that specific purpose;
- At leas three (3) members of the Working Groups;
- An auditor of ARME, to generate the key pair of SISP Root CA, and SISP Auditor, in the case of the Subordinate CAs;
- Any observers, as accepted by the Management Working Group of the PKI of SISP.

The certificate issuance ceremony comprises the following steps:

- Identification and authentication of all persons present at the ceremony, ensuring that the representative(s) and the members of the Working Group hold the powers required for the acts to take place;
- The members of the Working Group make the startup procedures for certificate processing and issue the Certificate Request Signature (CRS) (corresponding to the PKCS#10 generated on the HSM), which is stored in a technological support (non-rewritable);

- The certificate issued and signed by the hierarchically higher Certification Entity is imported to the corresponding CA;
- Generation of the initial CRL;
- The issuance ceremony is concluded with the execution of the completion procedure of the certificate processing phase by the members of the Working Group.

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

6.3.2. NOTIFICATION TO SUBSCRIBER OF ISSUANCE OF CERTIFICATE

Certificate issuance is conducted on site, or face-to-face, in conformity with the previous section.

6.4. CERTIFICATE ACCEPTANCE

6.4.1. PROCEDURES FOR CERTIFICATE ACCEPTANCE

The certificate is deemed to have been accepted after signature of the certificate application and acceptance form by the representative(s) in conformity with the issuance ceremony (section 6.3.1).

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 application and acceptance form.

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 Practice Statement.

6.4.2. PUBLICATION OF THE CERTIFICATE

SISP Root CA shall not publish certificates issued for Issuing Certification Authorities, 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

The Accreditation Authority shall be invited to the certificate issuance ceremony of SISP Root CA and notified accordingly whenever a certificate of a subordinate CA is issued.

6.5. KEY PAIR AND CERTIFICATE USAGE

6.5.1. SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers or certificate titleholders shall use their private key 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 Practice Statement (CPS);
c) As long as the certificate is valid and does not appear in the CRL of SISP Root 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, before any act of reliance, 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 whenever 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

SISP Root CA 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 in the following circumstances:

- Private key is compromised;
- Private key of SISP Root CA is compromised;
- Private key is lost;
- Serious inaccuracies in the data provided;
- Technological equipment is no longer used under SISP Root CA;
- Compromise or suspected compromise of the password and access to private key (example: PIN);
- Loss, destruction, or damage of the private key support unit (e.g., cryptographic support/token);
- Non-compliance with the responsibilities anticipated in the present Certificate Policy and/or Corresponding CPS on the part of SISP Root CA or the subscriber;
- Whenever there are reasonable grounds suggesting that the certification services may have been compromised, which means that the certificate's reliability is at stake;
- 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 Entity;
- SISP, S.A.;
- A relying party, whenever it proves that the certificate has been used for purposes other than those anticipated.

SISP Root CA 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 meant to revoke the certificate of SISP Root CA or the Subordinate Certification Entities.

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. 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;
- Record and archive the revocation request form;
- Analysis of the revocation request by the Authentication Working Group of the PKI of SISP, which shall propose, to the Management Working Group, the approval or rejection of the revocation request;
- Following the opinion given by the Authentication Working Group of the PKI of SISP, the Management Working Group shall decide on the approval or rejection of the certificate revocation request;
- 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 FOR 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 ISSUANCE FREQUENCY

SISP Root CA shall make available a new CRL database every 3 (three) months.

6.7.12. MAXIMUM PERIOD BETWEEN CRL ISSUANCE AND PUBLICATION

The maximum period between issuance and publication of the CRL cannot exceed 3 (three) hours.

6.7.13. ONLINE REVOCATION STATUS/CHECKING AVAILABITY

Online certificate status checking is not provided by SISP Root CA via OCSP.

6.7.14. ONLINE REVOCATION CHECKING REQUIREMENTS

No stipulation.

6.7.15. OTHER FORMS AVAILABLE FOR DISSEMINATING REVOCATION

No stipulation.

6.7.16. SPECIAL REQUIREMENTS REGARDING PRIVATE KEY COMPROMISE

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

The responses to such incident may include:

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

BIBLIOGRAPHICAL REFERENCES

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