DECLARATION OF PRACTICES OF

CERTIFICATION AND POLICY OF CERTIFICATES

OF THE VENEZUELA's ROOT CERTIFICATION AUTHORITY

CONTROL OF VERSIONS

VERSION (EDITION)	REASONS FOR CHANGE	PUBLICATION
1	Creation	February 2007
2	General Updating	September 2007
2.1	General Updating	April 2008
2.2	Modifications in the fields. Distribution point of CRL, access to the information of OCSP authority and Certificate Policies	July 2008

INDEX

PROCEDURE

1. DIRECTORATE

NAME	SUSCERTE POST
Niurka Hernandez	Superintendent
Maria del Carmen Liendo	Director of Registration and Accreditation
Francis Ferrer	Director of Inspection and Auditing
Emerson Medina	Director of Research and Technological Development
Esther Gonzalez	Director of the Office of Administrative Management
Argenis Grillo	Legal Counselor

2. WORK GROUP: General

COORDINATOR:

PERMANENT MEMBERS:

NAME	UNIT	POST

3. SPECIAL COMMISSION:

POST:

4. GUEST(S) SPECIALIST(S)

NAME	ENTITY	POST
	SUSCERTE	

REMARKS

RESPONSIBLE FOR THE EDITION

COORDINATOR:

DATE: SIGNATURE:

SUPERINTENDENT:

DATE: SIGNATURE:

APPROVAL APPLICATION IN: DATE:

SIGNATURE:

1. OBJECT AND FIELD OF APPLICATION

The Declaration of Practices of Certification (DPC) of the Venezuela's Root Certification Authority (CA), sets up the necessary elements for the management of certificates to the Certification Service Suppliers (CSS) of the public and private sector. The Certificates Policy (CP) with the kind of certificates and the set of rules, indicates the procedures followed to render the services of certification, creating the National Infrastructure of Electronic Certification.

2. PRESCRIPTIVE REFERENCES

2.1. Organic Law of Administrative Procedures (LOPA)
2.2. Decree with Legal Force 1,204 On Data Messages and Electronic Signatures (LSMDFE) (February 2001)
2.3. Partial Regulation of the Law on Data Messages and Electronic Signatures. (December 2004)
2.4. SUSCERTE's Administrative Providence No. 016 National Infrastructure of Certification
2.5. RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999.
2.6. RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol OCSP 1999
2.7. RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate. Revocation List (CRL) Profile". April 2002
2.8. RFC 3647 "Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".
2.9. ETSI SR 002 176 Algorithms Parameters for secure electronics signature.
2.10. ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates", considering the criteria of the CWA14172-2 ("EESSI Conformity

Assessment Guidance - Part 2: Certification Authority services and processes").

2.11. FIPS 140-2 Level 3. Security Requirements for Cryptographic Modules, (December 2002).

2.12. CWA 14172-2. EESSI Conformity Assessment Guidance - Part 2 - Certification Authority Services and processes 2004.

3. DEFINITIONS AND TERMINOLOGIES

For purposes of this guide, the following definitions and terminologies are set up:

ACCREDITATION	Title granted by the Superintendence of Electronic Certification Services to the Certification Service Suppliers (CSS) to provide electronic certificates, once the requirements and conditions set up in Decree-Law 1,204 have been fulfilled.
REGISTERED AUDITOR	A natural person acting on his/her own or as a representative of a juridical person registered in SUSCERTE and endorsed by it, in order to realize the technical evaluations and audits of the applicants and CSS.
ELECTRONIC CERTIFICATE	Data Message provided by a Certification Service Supplier who attributes certainty and validity to the Electronic

DECLARATION OF PRACTICES OF CERTIFICATION	A document in which the Service Supplier of Electronic Certification defines the procedures concerning the handling of the electronic certificates issued.
POLICY OF CERTIFICATES	A document in which the Service Supplier of Electronic Certification, defines the rules to be followed for the use of an Electronic Certificate in a given community of users or application and its requirements of safety.
ROOTVE	An application developed to create and manage electronic X.509 certificates of the Root Certification Authority.
REPOSITORY	An information system utilized for the storage and access of the electronic certificates and the information associated with them.
ACCREDITATION REQUEST	A request addressed to SUSCERTE in order to obtain the Accreditation to provide electronic certificates, and other activities foreseen in the Law-Decree 1,204.
SUPERINTENDENCE OF ELECTRONIC CERTIFICATION SERVICES (SUSCERTE)	An Autonomous Service belonging to the Ministry of the Power for Telecommunications and Informatics, whose object is to accredit, supervise and control, according to the provisions of the Law-Decree 1,204 (LSMDFE) and its Partial Regulation, the public or private Suppliers of Certification Services.
ITSEC	European recommendation of safety which sets up the criteria that permit to select arbitrary safety functions (safety objectives that the system under study must fulfill, considering the laws and regulations).

4. SYMBOLS AND ABBREVIATIONS

For purposes of this guide, the following definitions and terminologies are set up:

AAP	Authority of Policies Approval
CA	Certification Authority
RA	Registry Authority
DCP	Declaration of Certification Practices
FUNDACITE	Foundation for the Development of Science and Technology
HSM	Cryptographic Hardware Module
IPK	Infrastructure of Public Key
ITSEC	Information Technology Security Evaluation Criteria.
LOAP	Organic Law of Public Administration
LOPA	Organic Law of Administrative Procedures
LRC	List of Revoked Certificates
LSMDFE	Law on Data Messages and Electronic Signatures
MPPTI	Ministry of the Popular Power for the Telecommunications and Informatics
OCSP	Online Certificate Status Protocol
PC	Policy of Certificates
PIN	Personal Identification Number
CSS	Certification Services Supplier
BRV	Bolivarian Republic of Venezuela
RFC	Request for Comments
RPLSMDFE	Partial Regulation of the Law on Data Messages and Electronic Signatures
SUSCERTE	Superintendence of Electronic Certification Services

5. PROCEDURE

5.1 Basic Principle

This document is constituted from the Declaration of Certification Practices and Certificates Policy of the Root Certification Authority of the Country, which follows the structure set up by the RFC 3647.

6. DECLARATION OF CERTIFICATION PRACTICES AND CERTIFICATES POLICY OF THE ROOT CERTIFICATION AUTHORITY OF VENEZUELA

6.1 Presentation

The Root CA is the Root Certification Authority of the National Infrastructure of Electronic Certification whose main function is to issue the electronic certificates to the CSS. Where the electronic certificate links the identity of a subject (authority, individual, device, etc.) with its respective public key and one or more attributes.

The specific case of a root certificate belongs to a certificate that no authority of superior confidence signs digitally as root, i.e., it possesses a self signed certificate and it is there where the assurance chain starts from. This self signing process causes that the fields of the root certificate fulfill the international and applicable standards that guarantee the interoperability.

Then, the Root CA disposes of a self signed certificate with its private key, with which it signs the certificates of public key of the CSS, which on time use their private keys to sign the certificates of the final entities, so all the hierarchy is covered by the confidence of the Root CA.

The application of the National Infrastructure of Electronic Certification of the Root CA has been developed by FUNDACITE Merida, a body attached to the Ministry of Science and Technology (MCT) in Free Software according to the Presidential Decree 3390.

The electronic certificate is generated in accordance with the version 3 standard X.509
The X.509 is the fundamental standard defining the structure of the public key certificate. Said standard is generated by the sector of standardization of Telecommunication of the International Telecommunications Union (International Telecommunications Union-Telecommunications, ITU-T).
The general architecture, at a hierarchical level, of the National Infrastructure of Electronic Certification is shown in the Figure 1:

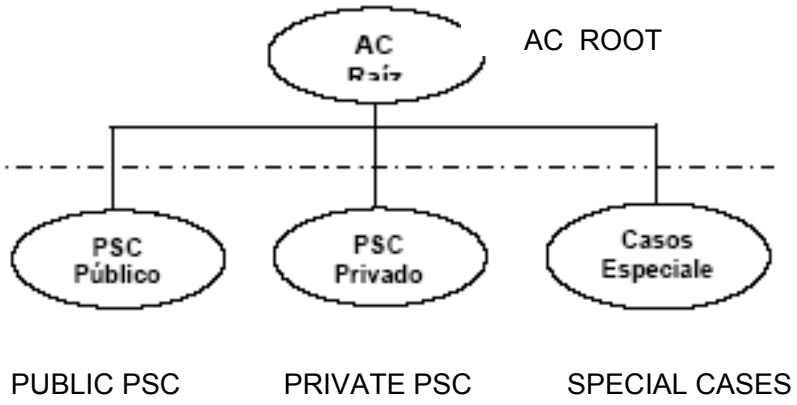

Figure No. 1. *Architecture of the National Infrastructure of Electronic Certification at a hierarchical level*

The hierarchical architecture starts from the Root, anchor of the Confidence Chain of the electronic certification, called Root Certification Authority (CA). The confidence relations are built from the most reliable CA until the ones the National Infrastructure of Electronic Certification may have, where there is no other CA that can sign the certificate of the Root CA. This is the only case in which the Root CA creates a self signed certificate by

itself, and then, once it has been accredited before SUSCERTE, according to the Law on Data Messages and Electronic Signature (LSMDFE), it signs the electronic certificate of the CSS of the public and private sector, besides the List of Revoked Certificates (LRC).

In the next step we find the Subordinated CA of the Root CA called CSS. Once accredited before SUSCERTE according to the LSMDFE, they must issue the certificates in accordance with the purpose of the electronic certificates specified in their own DPC and PC.

It is worth mentioning that SUSCERTE is responsible for elaborating and approving this DCP, as well as its modifications, following the model that SUSCERTE itself provides for the elaboration. Should it be deemed necessary to modify the structure, then the chosen one shall be the model to be followed for all those who request to be accredited as CSS. Furthermore, it evaluates the DCP of each CSS of the National Infrastructure of Electronic Certification of Venezuela.

Consequently, the DCP must have the specifications of the requirements used by the Root CA, for the generation, publication and administration of certificates of electronic signature to the Subordinated CSS, based on RFC 3647.

6.2 Name of the ID Document

Name of the document	Declaration of Certification Practices (DCP) and Certificate Policy (CP) of the Root CA
Document version	2.0
Document status	APPROVED
DPC/OID Reference (Object Identifier)	2.16.862.1.2. Root CA CP
Date of issuance	July 23 2008
Due date	The DCP and CP must be revised with a minimum periodicity of 2 years
Localization	This DCP and CP is in:http://acraiz.suscerte.gov.ve

6.3 User's community and applicability

CERTIFICATE FIELD	**Value of the Root Certificate**
Version	V3
Serial	Sole identifier of the certificate: Less than 32 hexadecimal characters
Signature Algorithm	It must contain the OID of the algorithm and if necessary, the parameters associated used by the certifier. The algorithms permitted are SHA1 and SHA256 with RSA Encryption.
DATA OF THE EMITTER (DN)	
CN	Root Certification Authority of the Venezuelan State
O	National System of Electronic Certification
OU	Superintendence of Electronic Certification Services
C	VE (Country)
E	acraiz(5)suscerte.gob.ve
L	(Address)
ST	(State)
VALIDITY PERIOD	
Not before	Date of start of the validity period of the certificate
Not after:	Due date of the validity period of the certificate

SUBJECT's DATA	
CN	Root Certification Authority of the Venezuelan State
O	National System of Electronic Certification
OU	Superintendence of Electronic Certification Services
C	VE (Country)
E	acraiz(5)suscerte.gob.ve
L	(Address)
ST	(State)
(SUBJECT PUBLIC KEY INFO)	
Public Key Algorithm	Algorithm used to generate the Public Key (RSA)
Size of the public key	4096 bits
EXTENSIONS	
Basic Constraints	It allows identifying if the signatory of a certificate is a certifier. It must contain the CA attribute AC: True and path length = 2
Issuer Alternative Name	
DNS Name	DNS Name (suscerte.gob.ve)
Other Name. Identification No. OÍD 2.16.862.2.2	FIR-G-20004036-0
(Subject Key Identifier)	A mean to identify certificates containing a particular public key. It facilitates the building of certification routes (hash)
Subject Key Identifier	A mean to identify the public key corresponding to the private key used to sign a certificate
key ID	Key Identifier
Issuer	It contains all the data of the issuer.
Serial	Serial Number
Key usage	It defines the purpose of the certificate key. It must be defined as critical value: Electronic signature of the certificate and LRC's signature
Subject Alternative Name	
DNS Name	DNS Name (suscerte.gob.ve)
Other Name	Other Name
LRC Distribution Point	It indicates how to obtain the LRC information with SHA1 URL: http://www.suscerte.gob.ve/lcr/certificado-raiz-sha1crlder.crl with SHA256 URL: ldap://acraiz.suscerte.gob.ve/certificado-raiz-sha256crlder.crl

Access to the Information Authority	OCSP, URI:http://ocsp.suscerte.gob.ve
Certificate Policies	It includes all the information about the Policy needed to validate the certificate (Place in Internet from where the DPC and PC are unloaded) URI:http://www.suscerte.gov.ve/dpc

Table No. 1. *Data structure of the Root CA certificate*

6.3.3 Registry Authority (RA)

The activities of identification and registry of the CSS must be realized by SUSCERTE together with the process of accreditation, not existing additional registry authorities in the ambit of the root certification authority.

6.3.4 Subjects of Certificates

The certificates issued by the Root CA have as Subjects the own Root CA, the accredited CSS and special cases, as it is established in the LSMDFE and its Partial Regulation.

6.3.4.1 Certification Services Suppliers

The Subordinated CA is called CSS of the public and private sector of the country. Within the Venezuelan legal framework, these are derived from the hierarchy of the Root CA, where they require that the Root CA signs their certificate so that they, on time, issue certificates to the final signatories, following with the confidence chain from the root point of the National Infrastructure of Electronic Certification. Every one of these CSS must elaborate its own DCP and Policy of Certificates, coherent with the general

requirements established by the LSMDFE, its Partial Regulation and others that SUSCERTE may deem necessary.

The use of Sha1withRSA is temporarily permitted due to interoperability with systems that do not hold Sha256withRSA. In a term of 2 years the DCP must be revised to exclude Sha1with RSA.

The data structure of the electronic certificate for the CSS is shown in Table No. 2:

CERTIFICATE FIELD	**Value of the Certificate of the main CA of the CSS**
Version	V3
Serial	Sole identifier of the certificate: Less than 32 hexadecimal characters
Signature Algorithm	It must contain the OID of the algorithm and, if necessary, the associated parameters used by the certifier. The algorithms permitted are SHA1 and SHA256 with RSA Encryption
DATA OF THE EMITTER (DN)	
CN	Root Certification Authority of the Venezuelan State
O	National System of Electronic Certification
OU	Superintendence of Electronic Certification Services
C	VE (Country)
E	E-mail (acraiz(5)suscerte.gov.ve)
L	(Address)
ST	(State)
VALIDITY PERIOD	
Not before:	Date of start of the validity period of the certificate
Not after:	Due date of the validity period of the certificate
SUBJECT'S DATA	
CN	Identification of the Supplier of Certification Services
O	National System of Electronic Certification

OU	Name or business name as appears in the articles of association
C	Country
E	E-mail
L	(Address)
ST	(State)
SUBJECT PUBLIC KEY INFO	
Public Key Algorithm	Algorithm used to generate the Public Key (RSA)
Size of the public key	4096 bits
EXTENSIONS	
Basic constraints	It allows identifying if the signatory of a certificate is a certifier. It must contain the CA attribute AC: True and path length = 1
Issuer Alternative Name	
DNS Name	DNS Name (suscerte.gob.ve)
Other Name	Other Name
Identification Number: OID 2.16.862.2.2	FIR-G-20004036-0
Subject Key Identifier	A mean to identify certificates containing a particular public key; it facilitates the building of certification routes (hash)
Subject Key Identifier	A mean to identify the public key corresponding to the private key used to sign a certificate
key ID	Key Identifier
Issuer	It contains all the data of the issuer.
Serial	Serial Number
Key usage	It defines the purpose of the certificate key It must specify as critical value: Electronic signature of the certificate and LRC's signature
Subject's Alternative Name	
DNS Name	(dominion name of the CSS registered in nic.ve)
Other Name	Other Name
OÍD 2.16.862.2.1	Accredited PSC's identification code, assigned by SUSCERTE
OÍD 2.16.862.2.2	FIR (PSC's FIR) according to the Annex No. 1 of this norm
Distribution point of the LRC	It indicates how to obtain the LRC information

Access to the Authority of Information	With SHA1 URL:http://www.suscerte.gov.ve/lcr/certificado-raiz-sha1crlder.crl con SHA256 URL:ldap://acraiz.suscerte.gov.ve/certificado-raiz-sha256crlder.crl
Access to the Information Authority	(Link to the OCSP) service optional Field URL:http://ocsp.suscerte.gov.ve
Certificate Policies	It includes all the information about the Policy necessary to validate the certificate (Place in Internet from whICH the DPC and PC are unloaded) URI:http://www.suscerte.gov.ve/dpc

Table No. 2. *Data structure of the CSS certificate*

6.3.5 Bona fide third parties

Are all those persons realizing transactions utilizing electronic certificates coming from the National Infrastructure of Electronic Certification who decide to accept and rely upon these certificates.

6.4 Use of certificates

6.4.1 Uses permitted for the certificates

The root electronic certificate can only be used for the identification of the own Root CA and for the safe distribution of its private key.

The use of the certificates issued by the Root CA shall be limited to the signature of electronic certificates for subordinated authorities and the signature of the lists of the respective revoked (LRC) certificates.

6.4.2 Uses not permitted for the certificates

The uses not permitted for the certificates issued by the Root CA are all those not explicitly permitted in the previous paragraph.

6.5 Administration Policies of the Root CA

6.5.1 Specifications of the Administrative Organization

Name	Superintendence of Electronic Certification Services
E-mail	superintendencia(5)suscerte.gob.ve
Address	Av. Universidad, Esquina El Chorro. Torre MCT. Piso 8. Caracas Venezuela
Phone:	(058-212) 564.8028
Fax:	(058-212) 564.5993
Web site	http://www.suscerte.gob.ve

6.5.2 Contact Person

Name	SUSCERTE's Superintendent
E-mail	superintendencia(5>suscerte.gob.ve
Address	Av. Universidad, Esquina El Chorro. Torre MCT. Piso 8. Caracas Venezuela
Phone:	(058-212) 564.8028
Fax:	(058-21) 564.5993
Web site	**http://www.suscerte.gob.ve**

6.5.3 Competence to determine the fitness of the DPC to the policies

The AAP of the Root CA is responsible for determining the fitness of the DCP to the norms and best practices in the matter.

7. PUBLICATION OF INFORMATION OF THE CA ROOT AND REPOSITORES OF CERTIFICATES

7.1 Repositories

The Certificates of the Root CA must be available during 365 days per year, 24 hours per day and in case of interruption due to force majeure, the service shall be reestablished as soon as possible.

- **For the certificates of the Root CA and the CSS accredited:**

  Web site: http://acraiz.suscerte.gob.ve/

  Section: Certificates

- **For the list of revoked certificates (LRC):**

Web site: http://acraiz.suscerte.gob.ve/

Section: List of Revoked Certificates

LDAP: ldap://acraiz.suscerte.gob.ve

- **For the DCP:**

Web site: http://acraiz.suscerte.gob.ve/

Section: Declaration of Practices of Certification

- **Validation Service on line which implements the OCSP protocol:**

Web site: http://ocsp.suscerte.gob.ve/

The public repository of the Root CA does not contain any confidential or private information.

7.2 Publication

It is the duty of the Root CA and the CSS belonging to the hierarchy of the National Infrastructure of Electronic Certification, the disclosure of the information relating to its DCP, the certificates and an updated status of said certificates.

The disclosures realized by SUSCERTE of any information classified as public, shall be announced in its Web site as follows:

- The List of Revoked Certificates (LRC) is available in LCR V2 format, in the repository of the Root CA.
- The Certificate Policy of the Root CA is available in the Web site of the Root CA: http://acraiz.suscerte.gob.ve/dpc in PDF format.
- All the versions of this document are public and are available in the Web site of the Root CA: http://acraiz.suscerte.gob.ve in PDF format.

- The certificate of the Root CA is available in the public repository, in format X.509 v3 and in the address http://acraiz.suscerte.gob.ve. Section: certificates

- The certificates issued by the Root CA are available in the public repository, in format X.509 v3 and in the address: http://acraiz.suscerte.gob.ve. Section: certificates

- The SUSCERTE's contact data are in the address: http://www.suscerte.gob.ve/contactos.

7.3 Frequency of Publication

7.3.1 Certificates of the Root CA

The publication of the electronic certificate shall be realized before its coming into force through the Official Gazette. Its validity period is twenty years.

7.3.2 PSC Certificates

The publication of the electronic certificate shall be realized before its coming into force through the Official Gazette. Its validity period is ten years.

7.3.3 List of Revoked Certificates (LRC)

The LRC is in the SUSCERTE's public repository. This list is updated:

- **Periodically:**

  - Every 6 months, unless an accreditation or revocation of a certification comes out within the National Infrastructure of Electronic Certification.
  Should anyone of these events take place, the 6 month period is restarted.

- **Fortuitously:**
  - Each time a certificate is accredited or revoked within the National Infrastructure of Electronic Certification.
  - Each time an electronic certificate is issued by the Root CA.

7.3.4 Declaration of Practices of Certification

The Root CA publishes in the repository the new versions of this Document, immediately after its approval.

7.4 Access Control to the Certificates Repository

The access to the information published by the Root CA shall only be for consultation and may not be modified by non authorized persons. The public information shall only be updated by the personnel in charge of this function, working for SUSCERTE. Furthermore, the consultation to LRC and DCP's previous and updated versions is guaranteed.

8. IDENTIFICATION AND AUTHENTICATION

8.1 Registry of Names

8.1.1 Kind of Names

The Root CA only generates and signs certificates with name types in compliance with the X.500 standard 500.
For the certificate of the Root CA: The subject and the issuer are formed by the following attributes:

- CN = Root Certification Authority of the Venezuelan State
- O = National System of Electronic Certification
- OU = Superintendence of Electronic Certification Services
- C = VE
- E = acraiz@suscerte.gob.ve

The alternate name of the Root CA is formed by the following attributes:

- DNS Name = suscerte.gob.ve
- Other Name =
- OÍD 2.16.862.2.2=FIR-G-20004036-0

For the CSS certificates: The subject of the CSS certificates is formed by the following attributes

- CN = Supplier of Certification Services [Supplier's Identification]
- O = National System of Electronic Certification
- OU = [Name or business name]
- C = VE
- E = [E-mail of CSS's contact]

The Issuer of the CSS certificates is formed by the following attributes:

- DNS Name=[name of the CSS's domain registered in nic.ve]
- Other Name =
  - OID 2.16.862.2.1 =[Identification Code of the accredited CSS assigned by SUSCERTE]
  - OID 2.16.862.2.2=FIR-[PSC's FIR]

SUSCERTE sets up in this policy the issuance of three kinds of certificates. Each kind of certificate shall be identified by a sole OID (Object Identifier), included in the certificate as an identifier of the policy, within the extension X.509 Certificate Policies.

Type I Certificate – Certificates for the Root CA
(Policy OID 2.16.862.1.2)
This certificate is generated by the Certification Authority for its identification. This is the first level root certificate self signed of the National Infrastructure of Electronic Certification. The use of this certificate is framed in the activities of the Root CA.

Type II Certificate – Certificates of the CA for CSS
(Policy OID 2.16.862.1.3)
These certificates shall be issued to the CSS accredited before SUSCERTE, according to the provisions of the LSMDFE and its partial regulation. This kind of certificate can issue other certificates and it has the privilege of Subordinate CA of the National Infrastructure of Electronic Certification.

8.1.2 Necessity of significance for the names

SUSCERTE guarantees that the distinctive names (DN) of the certificates are sufficiently significant to link the public key with one identity.

8.1.3 Interpretation of names formats

The rules utilized to construe the distinguished names in the certificates issued are described in the ITU-T X.500 Distinguished Name (DN). Additionally all the certificates issued utilize the UTF8 codification for all the attributes, according to the RFC 3280.

8.1.4 Uniqueness of names

The Root CA defines the DN (Distinguished Name) field of the Certificate of Authority as unique and with no ambiguity. For that purpose, the name or business name of the CSS shall be included as part of the DN, specifically in the OU field. Hence, the uniqueness is guaranteed by means of the confidence in the uniqueness of the mercantile names in the national mercantile registry.

8.1.5 Settlement of conflicts relating the names

SUSCERTE does not act as an arbitrator or mediator; neither it settles any conflict relating the titularity of names of persons or organizations, domain names, trademarks or business names, etc. Likewise, this body reserves the right to disapprove a request for a certificate due to names conflict.

8.2 Initial validation of Identity

8.2.1 Test Methods of possession of the private key

The system of certification implemented and utilized by SUSCERTE for the administration of the life cycle of its certificates, automatically controls and guarantees the issuance of the certificate signed to the holder of the private key corresponding to the public key included in the application. This guarantee is achieved by means of the PKCS#10 format, which includes in the application itself, an electronic signature of the same, realized with the private key corresponding to the public key of the certificate.

8.2.2 Authentication of the Identity of an organization

The CSS must submit the accreditation request to SUSCERTE with the following papers and information:

- Full identification of the applicant.
- Economic and financial information, proving the capacity to render services as CSS.
- A copy of the contracts corresponding to those services rendered to third parties, if any.
- Contract projects to be subscribed with the signatories.
- Policy of certificates and Declaration of Practices of Certification.
- Audited financial statements and income tax return of the last two fiscal years.
- Audit report according to the provision of article 5 of the LSMDFE, elaborated by independent auditors, DIRECTORATE not linked and

enrolled in the registry kept by SUSCERTE for that purpose.

- A document with a detailed description of the infrastructure plans and procedures setup in Chapter VIII of the LSMDFE. If all or part of the infrastructure is rendered by a third party, it must include a copy of the contracts or agreements with the third party.

To facilitate the organization of the papers that the CSS must submit to SUSCERTE, the Norm 027 A Guide for the Accreditation of Certification Services Suppliers, which specifies the classified documentation required whether it's of a legal, economic-financial, technical or auditing kind, is available.

The authentication shall require the presence of the representatives of the organization, according to the provision of SUSCERTE called Delivery procedure of the credential to the legal representative of the applicant.

Said norms are available in the Web site http://ww.suscerte.gob.ve/, in the section of Electronic Certification, specifically in the link called: Prescriptive.

After the verification of the data and previous to the issuance of the certificate, the signature of a contract with SUSCERTE shall be required.

8.2.3 Verification of the faculties of representation

The verification of the CSS's representation before SUSCERTE

must be realized by the verification of a legal document, indicated in the LSMDFE, which qualifies it as a legal representative. SUSCERTE shall issue a credential to the legal representative which shall allow it to realize the accreditation requests to SUSCERTE.

8.2.4 Criteria to operate with external CA

The Root CA may operate with external CA provided that the accreditation of the AC is guaranteed, according to the legal provisions of its country. Thus guaranteeing the requirements of safety, validity and force of the certificate.

8.3 Identification and Authentication of requests for key renewal

8.3.1 For the routine renovations

The identification and authentication for the renewal of the certificate must be realized utilizing the techniques for the initial authentication and identification. This method of renovation requires that the private key is neither lapsed nor revoked.

8.3.2 For renewals of the key after a renewal – non committed key

The policy of identification and authentication for the renewal of a certificate after a revocation without compromise of the key shall be the same one used for the initial registration. Additionally the CSS must satisfactorily prove to SUSCERTE that the previous causes for

the revocation are no longer present in its ICP.

SUSCERTE may deny, in its absolute discretion, the extraordinary renewal of a certificate for CSS.

8.4 Identification and Authentication of requests for key revocation

The policy of identification for the requests for revocation may be equal to the one used for the initial registration. The policy of authentication accepts requests for revocation digitally signed by the subscriber of the certificate or the manual signature in the facilities of SUSCERTE.

The Policy of certificates of the subordinate CSS can define other policies of identification, provided that the possibility of authentication of identity, in accordance with the LSMDFE and its Partial Regulation, is guaranteed.

The Root CA or anyone of the authorities making it up can request by official letter the revocation of a certificate if they know or suspect the commitment of the private key of the subscriber, or any other fact recommending to undertake said action.

9. THE LIFE CYCLE OF CERTIFICATES FOR CSS

9.1 Request of Certificates

The operating procedures implemented by SUSCERTE for the accreditation is the responsibility of the CSS aspirant to the accreditation. This process can be

carried out manually, in the offices of SUSCERTE or through the following E-mail: http://www.suscerte.gob.ve/.

The accreditation of the CSS establishes that they operate in conformity with the policies and procedures set up by SUSCERTE.

9.1.1. Authorities that can request accreditation

All the public and private entities of the Venezuelan State complying with the requisites requested by SUSCERTE can request the accreditation to the confidence chain. The lineaments demanded by the law about data messages and electronic signatures are:

- Enough economic and financial capacity to render the services authorized as CSS. In the case of public bodies, these must count on an expense and income budget to allow it the performance of this activity.
- Technical capacity and elements necessary to provide Electronic Certificates.
- To guarantee a fast and safe service of revocation or cancellation of the Electronic Certificates provided by it.
- A free access, permanent, updated and efficient system of information, where the policies and procedures applied to render its services, as well as the Electronic Certificates that it has provided, revoked, suspended or

- cancelled and the constraints or limitations applicable to them, are disclosed.

- To guarantee that in the issuance of the Electronic Certificates provided by it, it has utilized tools and standards adequate to the international usage, and protected against corruption or modification, thus guaranteeing the technical safety of the processes of certification.

- In the case of juridical persons, these must be legally organized, according to the laws of their country of origin.

- The proper technical personnel, with specialized knowledge on the matter and skilled in the service to be rendered.

- The others pointed out by the regulation of the LSMDFE.

9.1.2 Process of accreditation and responsibilities

The accreditation process and the persons responsible for it are hereinafter described:

RESPONSIBLE	ACTION
APPLICANT	1. The applicant gathers from the SUSCERTE's Web site (www.suscerte.gob.ve) or at its office, the requisites to obtain the accreditation as CSS
AUDITOR	2. The auditor performs the respective audit, and issues a report
APPLICANT	3. The Applicant delivers the completed request for accreditation together with the legal, financial-economic, technical and audit documents.

SUSCERTE	4. It receives the request for accreditation and classified documents. 5. It verifies the completeness of the documents a. If the documents are complete i. It admits the request for accreditation ii. In case of lack of any document, it notifies the applicant of this iii. It indicates the applicant which documents are missing. iv. Go to step 3 6. It evaluates if the applicant fulfills all the requisites demanded to accredit it. a. If it fulfills the requisites: i. The accreditation is approved by the DIRECTORATE ii. It notifies it to the applicant b. If it does not fulfill the requisites: i. The accreditation is denied by the DIRECTORATE ii. It sends a notice to the applicant. iii. The processes finalizes
APPLICANT	7. He/she receives the notice of approval 8. He/she transacts and sends the guarantees demanded by the LSMDFE and its Partial Regulation
SUSCERTE	9. It receives the guarantees constituted a. If the guarantees correspond to the model presented and approved in the documents: i. Go to step 10 If the guarantees do not correspond to the model presented and approved in the documents: ii. The DIRECTORATE denies the application. The end of the process
APPLICANT	10. He/she deposits in the banking entity indicated by SUSCERTE, the respective fee for the accreditation 11. The applicant delivers the deposit voucher to SUSCERTE
SUSCERTE	12. It issues the Administrative Providence with the accreditation of the applicant as a CSS, and publishes it in the Official of the BRV. 13. It issues the root certificate.

	14. The end of the process

9.2 Request procedure for a certificate

9.2.1 Realization of the functions of identification and authentication

The functions of identification and authentication are realized by offices and the personnel in charge of operating the systems of accreditation of SUSCERTE.

These offices play the role of registration operators, and count on a safe dispositive to create a signature (officer's card) for the control of access to the application of issuance and integrity control and non repudiation of the operations and transactions realized.

9.2.2 Certificate approval or denial

The certification requests of those suppliers complying with all the technical, economic and legal requirements and lineaments demanded by SUSCERTE in this DCP, shall be approved. The system guarantees that the certificate issued is within the National Infrastructure of Electronic Certification.

9.2.3 Term to process a certificate

The Superintendence of Electronic Certification Services, previous verification of the documents to request the accreditation must decide about the accreditation of the Certification Service Supplier, within the

twenty (20) business days following the date of submission of the request.

9.3 Certificate Issuance

After verifying and approving the demands established in the LSMDFE, the system of the CA shall proceed to issue the certificate to the CSS by means of its publication in the Official Gazette of the Bolivarian Republic of Venezuela.

9.3.1 Actions of the CA during the issuance of the certificate

The issuance of the certificates implies the authorization of the request, by the system of the Root CA. After approving the application, the certificates shall be issued in a safe way and the certificates shall be made available to the CSS.

In the issuance of the certificates, the CA:

- Utilizes a procedure of generation of certificates which links in a safe way the certificate to the information of registration, including the certified public key
- It protects the confidentiality and integrity of the registration data

All the certificates shall come into force at the moment indicated in the certificate itself. The field of "not before" shall be used for that purpose.

No certificate shall be issued with a validity period starting before the present date. Nevertheless, certificates whose period of validity starts in the future or at a date later than the present, may be issued.

9.3.2 Notice to the applicant by the Root CA about the issuance of its certificate

The CSS shall know about the effective issuance of the certificate by means of a letter to the legal representative, issued by SUSCERTE. Likewise, the authorization for the applicant to start operating as a CSS is published in the journal with the highest nationwide circulation.

9.4 Acceptance of Certificates

9.4.1 How the certificate is accepted

The certificate issued by the Root CA to the CSS is considered as accepted after its publication in the repository of the National Infrastructure of Electronic Certification.

9.4.2 Publication of the certificate by the CA

SUSCERTE provides several kinds of communication like E-mails, written communications, LDAP repository, Web repository, OCSP, Official Gazette and those ones considered appropriate to publish the acceptance of a certificate.

9.4.3 Notification of the issuance of the certificate by the CA to other Authorities

SUSCERTE must notify the entities, government bodies and private companies about the issuance of a certificate by means of the SUSCERTE's Web site, the journal with the highest nationwide circulation and through the Official Gazette of the Bolivarian Republic of Venezuela.

9.5 Use of the key pair and the certificate

The uses of the certificates issued by the Venezuela's Root CA are the ones foreseen in the LSMDFE and its Partial Regulation.

9.5.1 Use of the private key of the certificate by the PSC

The subject can only utilize the private key and the certificate for the uses authorized in this DCP. SUSCERTE issues certificates in the fields of private key use limited to signature of certificates and LRC.

9.5.2 Use of the public key and the certificate by bona fide third parties

The bona fide third parties can only trust in the certificates, for the purpose set up by this DCP.

The bona fide third parties can realize operations of public key in a

satisfactory way, relying on the certificate issued by the confidence chain. Likewise, they must assume the responsibility of verifying the status of the certificate, utilizing the media set up in this DCP.

9.6 Renovation of a certificate with key change

9.6.1 Reasons to renew a certificate

The reason to renew a certificate by the CSS is the caducity.

9.6.2 Entity that can request the renewal of the certificate

The entities authorized to request the renewal of a certificate with change of the key of a CSS of the National Infrastructure of Electronic Certification are:

- The Supplier of Certification Services
- The Root Certification Authority

9.6.3 Request procedure for a certificate renewal

The CSS must follow again the process of accreditation in order to request the renewal of a certificate. On account of that, the request procedure for the certificate renewal is the same followed for the accreditation, which is described in the paragraph 9.1.2.

9.6.4 Notification of the issuance of a new certificate to the CSS

SUSCERTE must notify the CSS about the effective issuance of a new certificate by means of a letter to the legal representative, issued by the DIRECTORATE of the Superintendence. Likewise, it publishes it in the journal with the highest nationwide circulation.

9.6.5 Publication of the certificate renewed by the CA

SUSCERTE shall provide several kinds of communication like E-mails, written communications, LDAP repository, Web repository, OCSP, Official Gazette and the ones considered appropriate to publish the renewal of a certificate.

9.6.6 Notification of the issuance of the certificate by the CA to other entities

SUSCERTE shall notify the entities, government bodies and private companies, the renewal of a certificate through its Web site, the highest nationwide circulating journal and through the Official Gazette of the Bolivarian Republic of Venezuela

9.7 Modification of certificates

It has not been decided to realize any modification of the fields in the Root CA or in the CSS during the life of a certificate.

9.8 Renewal and suspension of a certificate

9.8.1 Circumstances for the revocation of the CSS's certificate

The circumstances to revoke a certificate of the CSS are the following:

- Compromise of the private key of the Root CA.
- Compromise or suspect of the private key associated to the CSS's certificate.
- When the CSS requests from the Root CA, the temporary suspension of its certificate.
- By judicial or administrative resolution commanding it.
- Due to variation in the certificate data.

9.8.2 Entity that can request the renewal

When the CSS's key becomes compromised, the confidence chain is broken. In those cases, the entities authorized to request the revocation of accreditation of a CSS of the National Infrastructure of Electronic Certification are:

- The authority qualified to the conformity with the LSMDFE

- The CSS
- The Root CA.

9.8.3 Request procedure for the revocation

The steps to revoke the accreditation of a CSS before SUSCERTE are:

RESPONSIBLE	ACTION
SUSCERTE	1. The DIRECTORATE of SUSCERTE determines the suspension of the accreditation of a CSS.
CSS	2. It receives the notice of suspension of the accreditation as CSS, decided by the SUSCERTE's DIRECTORATE 3. Immediately, it suspends the negotiation with new users, maintaining the service of the existing signatories, until further notice 4. It decides to solve the problem, based on the reasoning given by the SUSCERTE's DIRECTORATE to the suspension a. It complies with the decision for being in agreement with it. b. It objects the decree of suspension of its accreditation, setting out its argumentation before the SUSCERTE's DIRECTORATE.
SUSCERTE	5. The SUSCERTE's DIRECTORATE agrees with the CSS the actions to be taken, in accordance with its argumentation. a. It agrees the mechanism to activate the suspension applied to it, within a term of fifteen (15) days allowed to it for that purpose b. It receives the CSS's arguments against the suspension of the accreditation, utilizing the ten (10) days that the LOPA assigns to it to set forth its allegations
CSS	6. It carries out the actions agreed with the SUSCERTE's DIRECTORATE a. It submits to SUSCERTE the Improvement Plan to solve the problem that caused the suspension of its accreditation b. It sends to SUSCERTE a report justifying the reasons for its disagreement before the suspension of the accreditation

SUSCERTE	7. It admits the documents of the CESS a. It adjusts and approve the Improvement Plan of the CSS i. It authorizes its application within a fixed time, supporting its execution to solve the suspension status of the Accreditation b. It analyzes the claim interposed by the CSS i. It reaffirms the suspension for the accreditation, after proving again the breaches originating it ii. It readjusts its decision, if the allegations of the CSS have a good foundation, and reactivates the accreditation by means of a resolution 8. It sends the notice to the CSS.
CSS	9. It receives the notice a. It performs the Improvement Plan b. It decides in relation with its claim: i. To elaborate an Improvement Plan to avoid the revocation of its accreditation, within the time available for that purpose ii. Or to restart its ordinary activities 10. It informs SUSCERTE the result of its procedure
SUSCERTE	11. It periodically verifies the status of the CSS in relation with the status of suspension of the accreditation and the actions in process 12. If the CSS complies with all the requirements and obligations demanded by the Law-Decree 1,204, its Partial Regulation and Norms of SUSCERTE a. Its accreditation is reactivated b. The renovation of accreditation is revoked. 13. The process is finished

9.8.4 Grace period of the revocation request

The revocation shall be carried out after the procedure of each request confirmed as valid. SUSCERTE does not consider any grace period associated with this process in which the request for the revocation can be nullified.

9.8.5 Circumstances for the suspension

The circumstances for the suspension of a CSS certificate are the following:

- Compromise of the private key of the Root CA.
- Compromise or suspect of the private key associated to the CSS's certificate.
- When the CSS requests from the Root CA, the temporary suspension of its certificate.
- When the CSS knows about the undue use of the Electronic Signature.
- By judicial or administrative resolution commanding it.
- Due to variation in the certificate data.

9.8.6 Entity that can request the suspension

The entities authorized to request the renewal of a certificate of a CSS of the National Infrastructure of Electronic Certification are:

- The qualified authority to the conformity with the LSMDFE
- The CSS
- The Root CA.

9.8.7 Procedure for requesting the suspension (temporary)

The steps to request the suspension of the service of the CSS before SUSCERTE are:

RESPONSIBLE	ACTION
SUSCERTE	1. Receives from the CSS, well in advance, the maintenance and/or improvement plan to its facilities, equipment and systems, attaching the chronogram of temporary suspension of the service for said activities. 2. It revises the planning of activities and the chronogram for the temporary suspension to prove the connection between them, and always pending not to permit to surpass the lapses foreseen. 3. It requests from the CSS to adjust the planning and the chronogram, if it is not in agreement. 4. It approves the plan and the chronogram, when they fit to the provisions of the Law-Decree 1,204 and the internal norms of SUSCERTE 5. It sends the plan and the approved chronogram of temporary suspension of the service, authorizing it to perform said suspension on the programmed date and time, during the term accepted.
CSS	6. It receives from SUSCERTE the approved plan and the chronogram of suspension of service. 7. It sends to its signatories the chronogram of suspension of the service, approved by SUSCERTE. 8. It forwards to SUSCERTE a copy of the notice through which it informed its signatories about the chronogram of suspension of the service.
SUSCERTE	9. It receives a copy of the notice in which the signatories are informed about the chronogram of the temporary suspension of the service. 10. Remains pending to control the actions to be taken by the CSS to suspend the service, on the date and time approved.
CSS	11. It sends a notice to the signatories recalling them the date and time of the suspension of the service 12. It sends SUSCERTE a copy of the notice sent to its signatories 13. It opportunely stops the service on the date and time stated. 14. It restarts the service, complying with the lapse approved for the suspension.

	15. It informs its signatories about the restart of the service. 16. It forwards to SUSCERTE a copy of the notice of the restart of the service, already sent to its signatories.
SUSCERTE	17. It receives from the CSS a copy of the notice about the restarting of the service. 18. It checks the fulfillment of the programming set up. 19. It notifies the CSS the adequate application of the legal provisions and SUSCERTE's regulations. 20. End of the process.

9.8.8 Limits of the suspension period The limit set up by SUSCERTE for the suspension of a certificate must not be longer than forty-eight (48) hours.

9.8.9 Frequency of issuance of LCR

The Root CA disposes of a Web server, available from Internet to anybody who needs to consult it. The access to the information of the server is available 24 hours per day, 7 days per week.

The certificates revoked remain inserted in the LRC until the caducity date specified in their issuance. The frequency of issuance of each LRC is every time a certificate is revoked.

The LRC indicates the date of publication of the next list and its specific points of distribution. The LRC is issued and signed by the Root CA.

9.8.10 Requirements of verification of the LRC

The information relating to the status of the LRC certificates of the CSS is available in the following address: http://acraiz.suscerte.gob.ve/

9.8.11 Availability of verification on-line of the revocation

The Root CA possesses an OCSP to verify on-line the status of the certificates. The repository where the verification can be carried out on-line is described in the paragraph 9.8.10.

9.8.12 Requirements to verify the revocation on-line

The OCSP server has free access and there is not any requirement to use it, except the ones derived from the use of its own OCSP protocol, as defined in RFC 2560.

The Root CA also disposes of a repository to consult the validity status of the certificates issued.

9.8.13 Other ways available of disclosure of information about revocation

Through the E-mail ldap://acraiz.suscerte.gob.ve and in the Official Gazette of the Bolivarian Republic of Venezuela.

9.9 Services of verification of the certificates status

9.9.1 Operating Characteristics

For the validation of the electronic certificates, you have available several Validation Service lenders which provide information about the status of the certificates issued by the hierarchy of certification. It is a question of an on-line validation service (Validation Authority, VA) which implements the On-line Certificate Status Protocol following the RFC 2560.

By using that protocol, you can determine the present status of an electronic certificate, without requiring the LRC. A customer of OCSP sends a request about the status of the certificate to the VA, which, after consulting its Database, presents an answer about the status of the certificate via HTTP.

9.9.2 Availability of the Service

The service of verification of status of certificates is usable continuously, all the year-round.

9.9.3 Additional Characteristics

To use the Verification Service on-line, it is the responsibility of the bona fide third party to dispose of an OCSP Customer who complies with the RFC 2560.To.

9.10 Termination of the subscription

The termination of the subscription of a certificate takes place in the following cases:

- Revocation of the certificate due to any of the reasons gathered in the paragraph.
- Caducity of the validity of the certificate.

9.11 Key custody and recovery

9.11.1 Practices and policies of key custody and recovery

The private key of the Root CA is guarded by an HSM cryptographic device. To access the repository of the private keys the Shamir's limit threshold limit (k, n) is used, both in the software and in cryptographic devices.

10. CONTROLS OF PHYSICAL, MANAGEMENT AND OPERATIONS SAFETY

10.1 Physical Safety Controls

10.1.1 Location and building

All the critical operations of the Root CA are physically protected with all the necessary safety measures for the most critical elements and with surveillance 24 hours per day, 7 days per week. These systems are separate from others of SUSCERTE, so that only the authorized personnel may accede to them.

The Data Process Center of the Root CA fulfills the following physical requirements:

- To avoid possible damages, the facilities are far out from fumes uptake.
- There are not windows outside the tower.
- Closed TV circuit in the critical areas or of restricted access.
- Control of biometric access.
- Systems of fire detection and extinction:
  detectors, fire extinguishers, training of the personnel to act in case of fire, etc.

10.1.2 Physical Access

The physical access to the facilities of the Root CA is protected by various access controls, so that only the authorized personnel can accede to them. The access, zones and processes controls are defined in the safety policies.

The systems of the Root CA will be physically separated from other systems of SUSCERTE, so that only the authorized personnel can accede to them, and the independence of the other informatic systems is guaranteed.

The date, time of entrance and exit are registered, as well as the activity performed by all the persons entering the metering center.

10.1.3 Electrical supply and air conditioning

The premises where the equipment is located count on the necessary conditions of power and ventilation to avoid power breaks or other electrical anomalies in the electric systems.

The cabling of the equipment is protected to avoid damages, and special measures have been adopted to avoid losses of information caused by the interruption in the electrical flow supply, by connecting the most critical components to uninterrupted power supply (UPS) to guarantee a continuous electric supply, with enough power to maintain the electrical network during the controlled power cuts of the system and to protect the equipment against electrical fluctuations which could damage them.

The air conditioning systems keep the premises of the equipment with adequate conditions of humidity and temperature for their right operation and maintenance.

10.1.4 Exposure to water

The installation of the Root CA is protected to avoid their exposures to water, by means of humidity detectors, flooding and other safety mechanisms appropriate for the environment.

10.1.5 Fire protection and prevention

The installation of the Root CA counts on an intelligent system of fire detection and extinction.

10.1.6 Storage Systems

The information related with the infrastructure of the Root CA is stored in a safety way in flame proof closets and safes, according to the classification of the information contained by them.

10.1.7 Elimination of residues

The Root CA maintains checking mechanisms operated by an authorized personnel, of all the disposable materials present where the information is stored (CD-ROMs, paper, films). These are checked, before their disposal or reutilization, to prove if they contain appreciable information, being physically destroyed, except if they can be reutilized as a backup medium, in which case the information is eliminated in a safe way.

10.1.8 Storage of backup copies

All the backup copies are stored in entities far apart from the Root CA. These dependencies are protected with safety media and mechanisms, following international safety good practices.

10.2 Functional Controls

10.2.1 Confidence Papers

The Root CA counts on personnel subject to special control procedures, given its level of responsibility, because its activity is essential for the right functioning of the National Infrastructure of Electronic Certification. Thus, the following persons have the consideration of confidence roles:

- Responsible of the keys pair of the Root CA.
- HSM Administrator.
- ROOTVE User.
- Safety coordinator.
- Internal Auditor.
- Coordinator of Certification Authority.
- Director of the Department.

10.2.2 Number of persons required per role

As a safety measure, the responsibilities are shared among the various roles and persons, thus the negligent or malfeasance of anyone of them, does not affect seriously the activity of SUSCERTE as Root CA.

10.2.3 Identification and authentication for each role

The users in charge of each of the roles described in the foregoing paragraphs are authenticated by using strong cryptography. This authentication is carried out utilizing private keys protected by means of intelligent cards and/or biometric devices.

10.3 Personal Safety Controls

10.3.1 Requirements of records, qualification, experience and accreditation

The personnel realizing activities in the facilities or in the system of the Root CA must be qualified and skilled in environments of rendering services of certification.

10.3.2 Requirements of education

The SUSCERTE's personnel must be subject to training to carry out its function within the institution.

- Formation in the basic legal aspects relating to rendering services of certification.
- Conscience of the physical, logical and technical safety.
- The services provided by the Authority of Certification
- Operation of the software and hardware for each specific role.

- Basic concepts about ICP.
- Declaration of Certification Practices (DCP) and the Policies of pertinent certificates.
- Management of incidences

10.3.3 Requirements and frequency of actualization of the formation

SUSCERTE will provide inductions to its staff in front of the technological changes of the environment, introduction of new tools, or modification of operative procedures.

Furthermore, SUSCERTE will carry out training sessions in front of changes in the Declaration of Certification Practices, Certificates Policy or other documents, relevant for the operation, administration and/or management of the Root CA.

10.3.4 Frequency and sequence of rotation of roles

This paragraph does not apply.

10.3.5 Sanctions for non-authorized actions

The practices of the SUSCERTE's personnel define the procedure to sanction the employees who breach said practices, and specify the punishment for carrying out an action non authorized, the non authorized use of the authority or the systems.

In any case, should SUSCERTE suspect that any employee is performing a non authorized action; it automatically suspends his/her permit of access, and considers the possibility of his/her dismissal, in accordance with the juridical ordination in force.

10.3.6 Documentation provided to the personnel

SUSCERTE provides its employees with all the documentation necessary for the right performance of their tasks. Among the documentation provided there is:

- Declaration of Practices of Certification
- Instruction manuals of operation, administration, installation and utilization of the Root CA's tools.
- Safety norms and plans
- Emergency procedures
- Policy of certificates
- Policy of Safety of the Information
- Organization chart and functions of the personnel

10.4 Safety Control Procedure

10.4.1 Kind of events registered

The Root CA stores electronic records of events (logs) relating to its activity, as CA of the National Infrastructure of Electronic Certification.

These records are kept in an automatic manner and in the other cases, in hard copy on paper or other media. These files are available to the auditor when it is deemed necessary.

10.4.2 Frequency of process of logs registries

The logs are analyzed in the presence of extraordinary events. Every extraction of logs also leaves traces of audits for its later revision.

10.4.3 Period of retention for the audit logs

The Root CA will retain all the audit records generated by the system.

10.4.4 Protection of the audit logs

The integrity of the audit logs is protected by the signature of each event with the private key of the person who carries out the action. Additionally, these logs are protected with the same safety measures used for the information classified as confidential.

10.4.5 Backup procedures of the audit logs. This paragraph does not apply.

10.4.6 System of audit information gathering

The system of gathering the audit information is realized by: operating systems, processes in the application of the Root CA and by the staff who operates them. Therefore, this system is a combination of automatic and manual processes. The characteristics of this system are the following:

- It allows verifying the integrity of the database.
- It ensures the no repudiation by the authors, of the operations realized with the data. This is achieved by means of the electronic signatures.
- It saves a historical record of data updating, i.e., it stores successive versions of each record resulting from various operations realized by it.

10.4.7 Notification to the subject causing the event

This paragraph does not apply.

10.4.8 Analysis of vulnerability

This paragraph does not apply.

10.5 File of Information and Records

10.5.1 Kind of information and events registered

Regarding the life cycle of the keys of the Root CA:

- Generation of the keys of the Root CA
- Installation of cryptographic keys and their consequences.
- Back up copy of the keys.
- Storage of the keys
- Recovery of the cryptographic keys
- Use of the keys
- Keys destruction

Relating to the life cycle of the certificates:

- Reception of requests for Certificates.
- Generation of certificates.
- Distribution of the public keys
- Revocation of certificates
- Requests for validation of certificates and answers.

Relating to the life cycle of the cryptographic devices:

- Reception of devices.
- Entry or transfer to the place of storage.
- Use of devices.
- De-installation of devices.
- Designation of the device for service or repair.
- Withdrawal of devices.

Others:

- Updating of the CSS.
- Confidentiality agreements.
- Accesses and modifications of the documentation requested by the auditors.
- Agreements made by SUSCERTE.
- Authorization of access to the information systems.

10.5.2 Period of retention for the file

The traces of the files are kept during a period of twenty years.

10.5.3 File protection

The safety measures defined are aimed at protecting the files against (internal or external) non authorized accesses, so that only authorized persons can consult, modify or eliminate the files. The files are stored in safe places, with all the necessary safety measures to protect them against natural factors.

10.5.4 Procedures of file backup

This paragraph does not apply.

10.5.5 Requirements for the time stamping of the registries

SUSCERTE is presently performing the project to incorporate the time stamping to the electronic signature.

10.5.6 Repository system of audit files (internal vs. external)

The system of files repository is realized utilizing flame proof and time resistant media.

10.5.7 Procedures to obtain and verify the information filed

Only the authorized personnel can accede to the physical files of backups and computer files, in order to carry out verifications of integrity or others.

This verification must be realized by the Auditor of the System, who must have access to the tools of verification and integrity control of the registry of events of the ICP. The integrity of the electronic files is proved automatically, at the moment of their generation and an incidence is created in the case of mistakes or unplanned behaviors.

10.6 Key change

The keys of the certificates issued by the Root CA will be no longer valid at the same moment that its self signed certificate ceases to have it. Once expired, the Root CA will generate a new pair of keys which self signs, in order to generate the new root certificate.

10.7 Recovery in case of disaster

The requirements of notification and the recovery procedures in case of compromise of the private key or disaster are the following:

10.7.1 Procedures of management of incidents and vulnerabilities

SUSCERTE has in place a Continuity Plan which defines the actions to be taken, the resources to be utilized and the personnel to employ if a deliberate or accidental event disabling or degrading the resources and services of certification rendered by the Root CA, takes place.

10.7.2 Corruption of hardware and software resources and/or data

The Root CA has a plan of continuity of activities allowing it to continue operating if the hardware, software and/or data are corrupted (but not destroyed). It also updates from time to time this plan, in order to ensure its validity at any time.

The plan includes the procedures necessary to guarantee the continuity of the activity during the period elapsed between the disaster and the reset of the original situation (giving priority to the publication of the LRC).

10.7.3 Acting procedure before the vulnerability of the private key of an authority

The continuity plan of the business of the Root CA considers the compromise or suspicion of its private key as a disaster. In this case, the Document foresees the publication and immediate diffusion of the revocation of its certificate, in order to prevent the confidence in it.

The continuity plan of the Root CA foresees the revocation of its certificate as an immediate consequence of the compromise of the private key.

10.7.4 Safety of the facilities after a natural or other kind of disaster

The Root CA counts on external locations to maintain the safety copies stored, to minimize the effects in case of natural or other kind of disaster on the primary installations.

10.8 Cessation of the activity

The Root CA will not be able to notify the culmination of its activities of certification services. By its nature of Root CA of the confidence hierarchy of the National Infrastructure of Electronic Certification of the Country, in case of having its key committed, it must create immediately a new self signed electronic certificate and sign the certificates in force of the CSS accredited.

11. TECHNICAL SAFETY CONTROLS

11.1 Generation and installation of key pair

11.1.1 Generation of the key pair

The Root CA generates the key pair (Public and Private) utilizing a cryptographic hardware device (HSM) which complies with the requirements established in a profile of protection of electronic signature safe device of normalized authority of certification, in accordance with FIPS 140-2 Level 3 or higher security level.

The generation procedure of the keys for the CSS accredited before SUSCERTE is identical, in its own HSM.

11.1.2 Delivery of the private key to the CSS

The CSS is responsible for the generation of its key pair and therefore it is responsible for its guard and custody.

11.1.3 Delivery of the public key to the CSS

The public keys generated under the control of the CSS are sent to SUSCERTE, as part of an accreditation request. This request is realized in PKCS#10 format, digitally signed with the private key corresponding to the public key, whose certification is requested.

11.1.4 Availability of the public key

The public key of the Root AC will be continuously available in http://acraiz.suscerte.gob.ve, 24 hours per day and 7 days per week.

11.1.5 Size of the keys

The cryptographic algorithms employed by the Root CA to sign the certificates and the LCR are SHAIwihtRSA and SHA256withRSA. The length of the key with the RSA algorithm of the Root CA and the CSS is 4096 bits.

The use of ShaiwithRSA is temporarily permitted due to interoperability with systems that do not hold Sha256 with RSA. In a term of 2 years the DCP must be revised to exclude ShaiwithRSA.

11.1.6 Generation parameters of the public key and verification of quality

The Root CA and the CSS must generate their key pairs, according to RFC 3280 and PKCS#1. The algorithm of key generation is the RSA. The verification of the quality is realized in accordance with the special report of the ETSI SR 002 176, which indicates the quality of the algorithms of the electronic signature.

The signature algorithms and parameters utilized by the Root CA and CSS for the signature of electronic certificates and lists of certificates revoked are the following:

- Signature Algorithm: RSA
- Parameters of signature algorithm: Module length = 4096
- Keys generation algorithm: rsagen1

- Filling method: emsa-pkcs1-v1_5
- Cryptographic functions of summary SHA-1/SHA-256

11.1.7 Keys generation Hardware / Software

The Root CA generates its key pair utilizing a cryptographic hardware module (HSM). The authentication against the HSM requires of, at least, 2 or 3 operators. This procedure follows the shamir (k, n) limit scheme of threshold with the non persistent mode of the cryptographic device. In this mode, it is necessary to guarantee the physical connection of the last cards set in the HSM reader, to open the private key of the Root CA.

11.1.8 Purposes of utilization of the keys

The certificates issued by the Root CA include the Key usage extension, to restrict the purpose of the public key of the certificate, indicating that the key is only for:

- Certificate signature
- LCR signature

11.2 Protection of the private key

The private key of the Root CA is protected by a safety world generated by a cryptographic device. In order to maintain the guard of the private keys of the self signed certificate, the private key is never deciphered outside the HSM. The safety copies keep the secret of the private key in the same way in which the original private key is guarded.

11.2.1 Standards for the cryptographic modules

The HSM utilized by the Root CA to generate its keys is certified Level 3 FIPS 140-2. The public key has been stored in signed electronic format, so that they are protected against electronic faults and/or troubles with the electric power.

Therefore, the starting of a CA implies the following tasks:

- Initialization of the status of the HSM module.
- Creation of administration and operator cards.
- Generation of the CA keys.

11.2.2 "N" of "M" control of the private key

The private key, both of the Root CA and the CSS, is under multiperson control. It is activated by means of the initialization of the CA software by a combination of CA operators, HSM administrators

and users of the Operating System. This is the sole method of activation of said private key.

11.2.3 Custody of the private key

The private key of the Root CA is located in a cryptographic device. It complies with the requirements set in a protection profile of safe device of electronic signature of normalized certification authority, according to FIPS 140-2 safety Level 3.

The private keys of the Root CA and CSS are located in cryptographic hardware devices with level 3 FIPS 140-2 certification.

The Rest of the private keys of operators and administrators are contained in cryptographic intelligent cards in the hands of the administrators of each authority.

11.2.4 Security copy of the private key

This paragraph does not apply.

11.2.5 File of the private key

This paragraph does not apply.

11.2.6 Insertion of the private key in the cryptographic module

The private keys are created within the cryptographic module at the moment of initializing it. Later on, the private key generated inside the HSM is exported in under code form.

11.2.7 Method of activation of the private key

It consists of the utilization of intelligent cards to repeat the access in various persons and roles. Explicitly, the sole combination to activate the private key requires the presence of two out of three administrators of the HSM, three out of eight operators of the HSM and one administrator of the Operating System of the application.

11.2.8 Method of deactivation of the private key

One administrator of the Operating System can proceed to the deactivation of the private key of the Root CA. After having been activated by the combination described in the foregoing paragraph, the operator may proceed to the deactivation by means of the ROOTVE application.

11.2.9 Method of destruction of the private key

The Root CA will eliminate its private key when its validity term expires or when it has been revoked.
The destruction will be realized utilizing the commands set to physically erase from the memory of the HSM the part where the key was recorded.

11.2.10 Ranking of the cryptographic module

The cryptographic module utilized both by the Root CA and the CSS must possess the level 3 FIPS 140-2 certification.

11.3 Other aspects of the management of the key pair

11.3.1 File of the public key

The public key of the Root CA is filed according to the standard format PKCS#7, for a term of 20 years.

11.3.2 Operating periods of the certificates and usage period for the key pair

The key pair of the Root CA will have a validity of twenty (20) years; where as the one of the CSS will have a validity of ten (10) years. On the other hand, the periods of operation of the certificates will be the half of the validity period.

11.4 Activation Data

11.4.1 Generation and installation of activation data

The activation data of the Root CA and CSS must be generated and stored in intelligent cards. Their protection is guaranteed by means of a PIN (Personal Identification Number) in the hand of authorized personnel.

11.4.2 Protection of activation data

Only the authorized personnel have the cryptographic cards with activation capacity of the private keys of the CA; likewise they know the PINs necessary for its utilization.

The Personal key of access (PIN) is confidential, personal and not transferable and it is the parameter that protects the private keys, allowing the utilization of the certificates of the Root AC and CSS.

11.5 Safety controls of the computer

11.5.1 Specific Technical Requirements

SUSCERTE has defined in the document of the safety policies, the controls and techniques applicable to the computers. These controls refer to such aspects like the use of equipment, discretional and mandatory access controls, audits, identification and authentication.

11.5.2 Qualifications of computational safety

SUSCERTE utilizes certified products, at least by the E3 Level of the ITSEC norms.

11.6 Safety controls of the life cycle

11.6.1 Controls of system development

This paragraph does not apply.

11.6.2 Safety administration Controls

SUSCERTE must maintain an inventory of all the computer assets and realize their classification, according to their requirements of protection.

11.6.3 Safety qualifications of the life cycle

During the whole life cycle of the system, safety controls allowing implementing and auditing each phase of the systems of the Root CA, must be implemented.

11.7 Network safety controls

The technological infrastructure of the Root CA is not connected to the network. It remains off-line to guarantee a reliable and honest service.

11.8 Engineering controls of the cryptographic modules

The Root CA utilizes cryptographic modules, hardware and software commercially available, developed by third parties. The Root CA only utilizes cryptographic modules with level 3 FIPS 140-2 certification.

12 CERTIFICATE PROFILES, LCR AND OCSP

12.1 Certificate Profile

The certificates of the Root CA and CSS are issued according to the following standards:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certifícate and LRC Profile, April 2002.
- ITU-T Recommendation X.509 (2005): Information Technology - Open Systems Interconnection - The DIRECTORATE: Authentication Framework.
- ETSI TS 101 862 V1.3.1 (2004-03): Qualified Certifícate Profile, 2004.
- RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certifícate Profile, March 2004 (prevailing the TS 101 862 in case of conflict).

12.1.1 Version number

The Root CA bears and issues X.509 version 3 certificates. X.509 is a standard developed by the International Telecommunications Union (International Organization of the United Nations for the coordination of telecommunication networks services between Governments and companies) for the infrastructures of Public Key and the electronic certificates.

12.1.2 Certificate extensions

The extensions of the certificate of the Root CA allow codifying additional information in the certificates.

The standard X.509 extensions define the following fields:

- Subject Key Identifier
- Authority Key Identifier
- Basic Constraints. Marked as critical
- Certifícate Policies. Marked as critical
- Key Usage. Marked as critical
- LRC Distribution Point. Marked as critical
- Subject Alternative Name. Marked as critical

12.1.3 Object identifiers (OID) of the algorithms

The OID of the cryptographic algorithms utilized by the Root CA are:

- SHAlwithRSA Encryption (1.2.840.113549.1.1.5)
- SHA256withRSAEncryption (1.2.840.113549.1.1.11)

12.1.4 Name formats

The certificate of the Root CA contains as DN, the names of the emitter and holder of the certificate in the emitter and subject fields, in X.500 format.

12.1.5 Name restrictions

The names contained in the certificates are restricted to X.500 distinguished names, unique and non ambiguous.

12.1.6 Object identifier (OID) of the Certification Policy

The Root CA has a defined policy of assignation of the OID's within its numbering private tree. The OID of the CP of the Root CA is: 2.16.862.1.

12.2 LCR's Profile

12.2.1 Version number

The Root CA issues LRC with X.509 v.2 format

12.2.2 Extensions of the LCR

The extensions of the LRC issued by the Root CA are the ones defined by the IETG in its RFC 2459, i.e.:

- Authority Key Identifier
- LRC Number
- Issuing Distribution Point

12.3 OCSP Profile

12.3.1 Version number

The certificates of the OCSP will utilize the standard version 3 X.509 (X.509 v3)

12.3.2 Extensions of the OCSP

The X509v3 extensions utilized in the OCSP's certificates are:

- Subject Key Identifier
- Authority Key Identifier
- Key Usage.
- ext Key Usage.
- Certifícate Policies.
- Policy Identifier
- URLDPC
- Notice Reference
- Basic Constraints.
- Subject Type
- Auth Information Access
- OCSP No Check

13 AUDIT OF CONFORMITY

13.1 Frequency of the conformity controls for each entity

The accreditation system of the Root CA will be submitted to a yearly internal audit, according to the Audit Plan elaborated by SUSCERTE. This way, the fitness of the functioning and operativity with the stipulations included in this DCP and CP, is guaranteed.

Additionally, SUSCERTE will carry out internal audits under its own criterion or at any moment, in case of suspicion of non-performance of any safety measure or for compromise of the keys.

Likewise, every year, it will carry out an external audit to evaluate the degree of conformity regarding the technical specification ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates", considering the criteria of the CWA 14172-2 ("EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes").

13.2 Auditors

The auditor will be selected at the moment of realizing each audit.

Any company or person hired to realize a safety audit on the Root CA or the CSS must comply with the following requirements:

- Adequate and accredited training and experience in ICP, safety and audit process of information systems.
- Organizational independence of the authority of the Root CA, in the case of external audits.

13.3 Relation between the auditor and the authority audited

The relation between the auditor and the authority audited must be strictlylimited to the processes and information required for the audit.

Therefore, the part audited (Root CA or CSS) must not have any relation, financial, legal or of any other kind, present or planned, which may lead to a conflict of interest with the auditor. In the case of internal auditors, these cannot have any functional relation with the area subject to the audit.

13.4 Topics covered by the conformity control

All the technical, functional and organizational requirements are audit objects; among them are:

- The DCP and CP utilized
- Safety Policies
- Administration of the Root CA.
- Considerations of Confidentiality
- Physical security
- Plan of Contingency and Recovery from Disasters.
- Plan of Continuity of the Activities.
- Operating Personnel

13.5 Actions to be taken as result of a shortcoming

The identification of any anomaly in the audit will cause the immediate application of corrective measures, in order to resolve them as soon as possible.

In the case of a severe deficiency, the DIRECTORATE of SUSCERTE can determine the temporary suspension of the operations of the Root CA until the

deficiencies are corrected, the revocation of the certificate of the authority, changes in personnel, etc.

13.6 Communication of the result

The auditor must disclose the results of the audit to the AAP and to the responsible for the various areas where the nonconformities are detected.

14 COMMERCIAL AND LEGAL REQUIREMENTS

14.1 Tariff schedules

The Root CA of the Venezuela's National Infrastructure of Electronic Certification is not subject to duties payment. Only the CSS accredited before SUSCERTE are bound to comply with the duties levied in the LSMDFE, specified in Article 24 The Duties, Chapter V of the Superintendence of Electronic Certification Services of the LSMDFE. The CSS made up by public entities of the Venezuelan nation will be exempt from paying the duties of this article.

14.1.1 Registration rates for accreditation or renewal of the CSS

The CSS must pay the registration fees for the issuance and renewal of accreditation, before SUSCERTE:

- For the Accreditation of the CSS, subordinate CAs of the Venezuela's Root CA, SUSCERTE will charge a fee of one thousand tributary units (1,000 T.U.)

For the renewal of the accreditation of the CSS, a duty of five hundred tributary units (500 T.U.) will be charged

14.1.2 Registration rates for cancellation of accreditation

For the payment of the accreditation of the CSS before SUSCERTE, a duty of five hundred tributary units (500 T: U) will be charged.

14.1.3 Registration rates for the certificates granted by foreigner CSS

The foreigner CSS must pay a duty of five hundred tributary units (500 T.U.)

14.1.4 Rates of other services as information of policies

No tariff will be applied for the service of information about the CP, DCP or other additional services known at the moment of drafting this document.

14.2 Financial Capacity

14.2.1 Indemnification to third parties who rely upon the certificates issued by the CSS

The CSS must present a guarantee issued by an underwriter or banking entity authorized to operate within the country, and its conditions must cover all the contractual and extra contractual of the signatories and bona fide third parties

14.2.2 Financial capacity of the CSS

As foreseen in the LSMDFE, the CSS must have economic and financial capacity to be able to guarantee the continuity of the services.

14.2.3 Administrative processes

SUSCERTE must guarantee ongoing audits to the administrative processes and procedures established in a regular fashion. These audits will be carried out both internally and externally.

14.3 Confidentiality policies

The Root CA commits itself to protect all the data which it can have access to, as a consequence of its activity as CA of the Venezuela's National Infrastructure of Electronic Certification.

However, the Root CA reserves the right to disclose to the employees and external or internal consultants, the confidential data necessary to realize its activities as Root CA. In this case, the employees and/or consultants are informed about the obligations of confidentiality

These obligations do not apply if the information qualified as "confidential" is demanded by the Courts or competent administrative bodies or enforced by any law.

14.3.1 Confidential information

The following information is considered as confidential:

- Registration information. All the data concerning the registry of certificates are considered as confidential.
- The business information provided by its suppliers and other persons to whom SUSCERTE is bound to keep secret, legally or conventionally established.
- Information about the life of the certificates; all the data relating the issuance and revocation (except its publication in the LRC) of the CSS's certificates.
- All the information classified as "Confidential"

14.3.2 No confidential information

It is considered as no confidential information:

- The content of the certificates issued
- The List of Revoked Certificates (LRC)
- The public key of the Root CA
- The DCP's versions
- The Certificates' Policy (CP)
- The following Documents: Contingency and recovery plan in case of disasters, systems safety plan and in general, any document that the CA requires for its operation.

- The LSMDFE and its Regulation.
- Any other information identified as "Public"

14.3.3 Publication of information about the revocation or suspension of a certificate

The Root CA possesses an LDAP DIRECTORATE, which acts as repository of the Root CA, for the publication of information relating the renewal or suspension of certificates.

14.3.4 Disclosure of information as part of a judicial or administrative process

The Root CA can disclose information qualified as confidential to the relevant Judicial Authority which requires it formally.

14.4 Protection of the private / secret information

14.4.1 Information considered as private

The following data are considered as private information:

- Certificates requests, approved or denied, as well as any other personal information obtained for the issuance or maintenance of certificates.
- Private keys generated and/or stored by the Root CA.

- Password of personal access to the system of the Root CA.
- All the private keys generated as a pair of public-private key and stored in an intelligent card or any other repository.
- The personal identification numbers (PIN) which protect the private keys in intelligent cards.
- Any other information identified as "Private / secret information".

Likewise, the data got by the CSS have the legal consideration of basic level data.

14.4.2 Information not considered as private

The information does not have a private character, by legal requirement ("public data"), but it is only published in the deposit, if the subscriber so agrees.

In any case, the following information is considered as non confidential:

- The certificates issued or under procedure to be issued
- The name and surnames of the subscriber of the certificate, as well as any other circumstances or personal data of the subject, supposing that they are significant, in function of the purpose of the certificate, according to this document.

- The electronic address of the subscriber of the certificate.
- The economic uses and limits listed in the certificate.
- The term of validity of the certificate, as well as the date of issuance of the certificate and the expiration date.
- The series number of the certificate.
- The various status or situations of the certificate and the starting date of each of them; specifically:
  pending of generation and/or delivery, valid, revoked, suspended or lapsed and the reason that caused the status change.
- The lists of revoked certificates (LRC), as well as the rest of information of status of revocation.
- The information contained in the Deposit of the Root CA.

14.4.3 Responsibilities to protect the private / secret information

The Root CA guarantees the fulfillment of its legal duties as certification service render, in accordance with the Law.

14.4.4 Consent lending the use of the private / secret information

The Root CA must obtain the consent of the CSS in order to utilize its private information provided during the Process of accreditation.

The consent will be considered as obtained with the signature of the certification contract and the withdrawal of the certificates by the CSS.

14.4.5 Communication of the information to the administrative and/or judicial authorities

The Root CA can only disclose information classified as private / secret in those cases where they are required by the competent public authority and in the legally foreseen assumptions.

14.5 Copyrights

The copyright and proprietary rights of this Document belong to the Superintendence of Services of Electronic Certification (SUSCERTE).

14.6 Obligations and civil liability

14.6.1 Obligations of the Registry Authority

The Registry Authority must carry out the following duties:

- To realize its operations in accordance with this DCP.
- To realize its operations in accordance with the CP enforceable for the kinds of certificates requested in each case.
- To exhaustively verify the identity of the organizations accredited, for which it will require

the physical presence of the legal representative and the necessary documents described in this DCP.

Not to store or copy data of firm creation of the organizations it has accredited.

To inform the requesting organization, before the accreditation, about the duties it is assuming, among which are the following:

- The way in which it must guard the data of creation of the firm.
- The procedure it must follow to communicate the loss or misutilization of the data or devices of creation and of firm verification.
- Of its price
- Of the precise conditions for the utilization of the certificate
- Of its limitations of use and the way it guarantees its possible proprietary responsibility
- Of the Web site where it can consult any information about the Root CA, the DCP and the CP in force and previous.
- The governing Law
- The certifications obtained
- The procedures enforceable for the extrajudicial

resolution of conflicts that may arise from the exercise of the activity.

- To formalize the Certification Contract with the subscriber, according to the provision of the Certificate Policy enforceable.
- To request the revocation of a certificate when it is aware or suspects of the compromise of a private key.
- To authenticate the requests of the CSS for renewal or revocation of their certificates; to generate requests or renewal or revocation digitally signed
- In the case of approval of a request for an accreditation, to notify the subscriber the issuance of its certificates and the way to obtain them.
- In case of rejection of a request for an accreditation, to notify the applicant said rejection and the reason for it.
- To maintain under strict control, the transactions tools for electronic certificates.
- To receive and immediately transact the presential requests for revocation received by it, after having performed a reliable identification of the legal representative of the organization, based on the norms stated in this DCP.

14.6.2 Obligations of the Certification Authority

- To ensure the protection of the private key of the same Root CA.

- To verify that the CSS comply with the requirements to be a member of the confidence hierarchy of the National Infrastructure of Electronic Certification.
- To publish in the SUSCERTE's Web site this DCP of the Root CA.
- To ensure that its public key, the DCP, CP and other documents of public character, are available for anybody interested who requires them.
- To guarantee the adoption of the necessary measures to avoid the falsification of the Electronic Certificates and the Electronic Signatures provided by them.
- To perform internal audits to the application National Infrastructure of Electronic Certification of the Root CA, at least once per year.
- To revoke or suspend the certificate of a CSS if any of the causes exposed in the LSMDFE, its Partial Regulation or the DCP, arises.
- To keep an updated registry of the CSS's certificates that have been granted, revoked or suspended.
- To revoke or suspend those certificates that after having been issued, the suspect or knowledge of violation of the secret of the private key arises.

To keep during 20 years, all the information and documentation relating the certificates, in electronic or magnetic media or the ones established by the legislation in force, for their consultation.

14.6.3 Obligations of the Certification Services Supplier

The Certification Services Supplier (CSS) must:

- Be conscious of the necessary steps for the accreditation before SUSCERTE.
- Act diligently to avoid the non-authorized use of its Electronic Signature.
- Guarantee and protect its private keys in cryptographic devices which comply with the Level 3 FIPS 140-2.
- Notify the Root CA that its Electronic Signature has been controlled by non-authorized third parties or it has been unduly utilized, when it becomes conscious of it.
- Maintain the architecture scheme of ICP with the hierarchy in the form of a tree, for the authorities starting from it.
- Issue, distribute, revoke or suspend the certificates of the Certification Authorities subordinated to the CSS.
- Elaborate its own DCP and CP.
- Comply with Article 35 of the Obligations of the Suppliers, Chapter VI, The Certification Service Suppliers of the LSMDFE.

16.6.4 Obligations of the bona fide third parties

It is the obligation of the bona fide third parties who rely upon the certificates issued by the CA Root:

- To limit the reliability of the certificates to the uses allowed to them, in accordance with the provision stated in the extensions of the certificates and the pertinent CP.
- To verify the validity of the certificates at the moment of realizing or verifying any operation based on them.
- To assume its responsibility in the right verification of the electronic signatures.
- To assume its responsibility in the verification of the validity, revocation or suspension of the certificates which it relies upon.
- To have full knowledge of the guarantees and responsibilities applicable in the acceptance and use of the certificates which it relies upon and to accept to attach to them.

14.6.5 Obligations of the repository

- To maintain the set of certificates issued by the Root CA, available for all the participants of the National Infrastructure of Electronic Certification.
- To maintain the information of the certificates revoked, in LRC format, available for all the participants of the National Infrastructure of Electronic Certification.

14.7 Guarantee Waivers

The Root CA can reject all the guarantees of the service not linked to obligations established by the LSMDFE, especially those guarantees of adaptation for a particular purpose or guarantee of mercantile use of the certificate.

14.8 Limitation of Liabilities

The Root CA complies with all the norms, policies, lineaments, international standards in this matter. On the other hand, the CSS accredited most follow the LSMDFE, its Partial Regulation, the international standards, the norms and procedures of accreditation, audits and others that SUSCERTE may deem necessary.

14.8.1 Demarcation of liabilities

SUSCERTE does not assume any responsibility in case of loss or prejudice:

- From the services it renders, in case of war, strikes, unemployment, coups d'état, natural disasters or any other case of force majeure.
- Caused by the use of certificates exceeding the limits set out by the same, the CP and DCP.
- Caused by the undue or fraudulent use of the certificates or LRC issued by the Root CA.
- Occasioned to bona fide third parties, if the addressee of the

documents electronically signed, does not prove or keep in mind the constraints present in the certificate regarding its possible uses, or when it does not consider the suspension or loss of validity of the certificate, published in the LRC, or when it does not verify the electronic signature.

14.8.2 Limitations of losses

Except the provisions set up in this DCP, the Root CA does not assume any commitment neither offers any other guarantee, nor it assumes any other responsibility before subscribers or bona fide third parties.

14.9 Term and finalization

14.9.1 Term

This DCP will be in force while it is not expressly derogated by the issuance of a new version or by the renewal of the keys of the Root CA, when, compulsorily, a new version will be dictated.

14.9.2 Finalization

The obligations and constraints set out by this DCP, regarding confidential information, audits, obligations and responsibilities arisen during its validity, will subsist after its substitution or derogation by a new version, in all the aspects not opposed to this one.

14.10 Notices

Any notice, claim, request or any other communication required under the practices written in this DCP, will be given by means of an electronic document or message digitally signed, in accordance with this one or in written form, by means of registered mail addressed to anyone of the addresses contained in the paragraph 6.5.2 contact person. The electronic communications will be effective once the remitee, to whom they are addressed, receives them.

14.11 Modifications

14.11.1 Procedures of specifications of changes

The Authority with attributions to realize and approve changes upon this DCP is the Authority of Approval of Policies (AAP)

14.11.2 Procedures of publication and notice

Any modification of this DCP or the Documents of Certificate Policy will be published in the SUSCERTE's Web site http://ww.suscerte.gov.ve.

14.11.3 Procedures of approval of the Declaration of Certification Practices

The procedure for the approval of the declaration of certification practices is the one resolved by the Authority of Approval of Policies. Likewise, it is a competence of the AAP the approval and authorization of the modifications in said documents.

14.12 Disputes Settlement

14.12.1 Extrajudicial disputes settlement

The Root CA may establish, through the juridical instruments by means of which the relation with the CSS and verifiers is articulated, the procedures of mediation, arbitration and disputes settlement deemed opportune, all that without prejudice of the legislation on administrative procedure.

14.12.2 Competent jurisdiction

The conflicts brought up in the rendering of the certification services by the Root CA, will be submitted to the jurisdiction, in accordance with the provision of the LSMDFE and its Partial Regulation.

14.13 Governing Law

The functioning and operation of the Root CA, as well as this DCP is ruled by the Venezuelan legislation in force, at every moment. Explicitly, the following laws are assumed to be enforced:

- Decree 1,204 with Legal Force on Data Messages and Electronic Signatures (LSMDFE)

- Partial Regulation of the Law on Data Messages and Electronic Signatures LSMDFE).
- Organic Law of Administrative Procedures (LOPA)
- Organic Law of Public Administration (LOAP)
- SUSCERTE's administrative providence No. 016: National Infrastructure of Electronic Certification

14.14 Conformity with the Governing Law

The Root CA states that this DCP and CP comply with the provisions of the LSMDFE. Additionally, it is the responsibility of the AAP, to watch to the compliance with the applicable legislation gathered in the paragraph 14.13.