PROCERT Certificate Provider, C.A.
Certification Practices Statement (CPS)
For Resource Public Key Infrastructure (RPKI)

Date	October 2025
Edition	25
Version	1
Prepared by	General Management October 2025
Approved	Senior Management October 2025
Description	Certification Practice Statement (CPP)
In effect	Yes

1. Introduction.

This document is the Certificate Provider PROCERT, C.A. Certification Practices Statement (CPS). It describes the practices employed by the Certificate Authority (CA) Certificate Provider PROCERT, C.A. in the Resource Public Key Infrastructure (RPKI). These practices are defined in accordance with the requirements of the Certificate Policy (CP) [RFC6484] for the RPKI.

The RPKI is designed to support validation of claims by current Internet Number Resource (INR) holders (Section 1.6) according to the records of the organizations acting as CAs in this RPKI. The ability to verify such claims is essential to ensure the unique and unambiguous distribution of these resources.

This PKI parallels the existing INR distribution hierarchy. These resources are distributed by the Internet Assigned Numbers Authority (IANA) to Regional Internet Registries (RIRs). In some regions, National Internet Registries (NIRs) form a level of hierarchy below the RIRs for the distribution of INRs. Internet Service Providers (ISPs) and network subscribers form additional tiers below the records.

Conventions used in this document:

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" herein shall be interpreted as described in [RFC2119].

Likewise, this document constitutes the declaration by Supplier of Certificates PROCERT, C.A., for the purpose of informing and documenting its certification processes, for a better understanding and understanding by its Senior Management, staff, Customers, Suppliers and Interested Party.

This Statement of Certification Practices allows Senior Management, staff, Customers, Suppliers and Interested Parties of Certificate Provider PROCERT, C.A., to know each of the processes and sub-processes involved in the life cycle of electronic certificates; document the disaster recovery processes, cryptographic key management and give an overview of the equipment and infrastructure that supports the trust scheme in the RPKI of Certificate Provider PROCERT, C.A.

1.1. Overview.

The Statement of Certification Practices (CPP) is the guide to the best management and operation principles of Certificate Provider PROCERT, C.A., which are adjusted to the basic requirements for the issuance and administration of publicly trusted S/MIME certificates of the CA / Browser Forum and is part of the documentation that PROCERT Certificate Provider must maintain. C.A. for the operation of its RPKI. This document of the Statement of Certification Practices (DPC) of Certificate Provider PROCERT, C.A. is adjusted periodically and applies to the Registration Authority (RA) of Certificate Provider PROCERT, C.A., and any change must be reported to the Senior Management, staff, Customers, Suppliers and Interested Party of the PSC PROCERT.

This Statement of Certification Practices (DPC) of Certificate Provider PROCERT, C.A., contemplates the certificates issued by the RPKI of Certificate Provider PROCERT, C.A., under the Root of Certification of the Venezuelan State

(RCEV) and through a SubCA that is signed by the Root CA of the Venezuelan State, which is administered and controlled by the Superintendence of Certification Services (SUSCERTE), an entity belonging to the Venezuelan state. The SubCA of Certificate Provider PROCERT, C.A., complies with the international standard and standards applicable to an RPKI as established in the CA/Browser Forum, with respect to the Server Certificate Working Group, the issuance and management of publicly trusted S/MIME certificates, the Network Security Working Group and the Code Signing Certificate Working Group; the issuance of certificates additionally complies with all the regulations issued by SUSCERTE and the current legislation of the Bolivarian Republic of Venezuela regarding electronic certificates and the operation of Certification Service Providers (PSC). With respect to the Signatories, we comply with the terms and conditions established in the contract for the use of the service for the provision of electronic signature certificates for the end entity.

1.2. Name and identification of the document.
The name of this document is Certificate Provider PROCERT, C.A., Statement of Certification Practices for Public Key Resource Infrastructure (RPKI)." https://www.procert.net.ve/Internas/AC.aspx. This Statement of Certification Practices (CPP) has been subject to changes and adjustments, which are listed below indicating the editions and versions that are modified and the current edition with its corresponding version:

Version	Reason for Change	Publication	Validity
Edition 01	Emission	01/01/2008	No
Edition 02	Semi-Annual Correction (Update)	08/07/2009	No
Edition 03	Semi-Annual Control and Correction (Update)	05/01/2010	No
Edition 04	Semi-Annual Control and Correction (Update)	29/07/2010	No
Edition 05	Semi-Annual Control and Correction (Update)	13/01/2011	No
Edition 06	Semi-Annual Control and Correction (Update)	16/06/2011	No
Edition 07	Semi-Annual Control and Correction (Update)	03/01/2012	No
Edition 08	Semi-Annual Control and Correction (Update)	16/07/2012	No
Edition 09	Semi-Annual Control and Correction (Update)	26/02/2013	No
Issue 10	Semi-Annual Control and Correction (Update)	22/08/2013	No
Issue 11	Semi-Annual Control and Correction (Update)	15/01/2014	No
Issue 12	Semi-Annual Control and Correction (Update)	10/07/2014	No
Issue 13	Semi-Annual Control and Correction (Update)	17/11/2014	No
Issue 14	Semi-Annual Control and Correction (Update)	07/04/2015	No

Issue 15	Semi-Annual Control and Correction (Update)	06/10/2015	No
Issue 16	Semi-Annual Control and Correction (Update)	01/02/2016	No
Issue 17	Semi-Annual Control and Correction (Update)	16/03/2016	No
Issue 18	Semi-Annual Control and Correction (Update)	09/05/2016	No
Issue 19	Semi-Annual Control and Correction (Update)	05/06/2017	No
Issue 20	Semi-Annual Control and Correction (Update)	11/07/2017	No
Issue 21	Control and Correction (Technical Update)	22/09/2017	No
Issue 22	Control and Correction (Technical Update) Control, Review and Adjustment by Remediation of Accreditation 2019.	06/01/2018 06/06/2018 05/01/2019 07/07/2019 06/11/2019	No
Issue 23	Semi-Annual Control, Review and Adjustment (Update) Control and Adjustment (Update) Daycohost Migration. Control, Review and Adjustment Semi-Annual (Update) Control, Review and Semi-annual Adjustment (Observation of SUSCERTE 2023 Audit Report subparagraph (C1) Control, Review and Adjustment Semi-Annual (Update) Algorithm Change	02/08/2020 07/06/2021 07/12/2021 08/06/2022 06/12/2022 10/01/2023 17/07/2023 14/12/2023 24/02/2024 10/06/2024 10/10/2024	No
Issue 24	Standardization to CA /Browser Forum	17/08/2025	No
Issue 25	Standardization to CA /Browser Forum	28/10/2025	Yes

1.3. RPKI participants.

Next, we will proceed to inform about the entities that are part of the RPKI under the applicable and accepted certification scheme within the Bolivarian Republic of Venezuela.

1.3.1. Certification authorities.

The Certification Authority of the Venezuelan State is created by Presidential Decree Law, which also creates the Superintendence of Electronic Certification Services (SUSCERTE), which is the government entity in charge of administering the Venezuelan Root Certificate, which is in charge, after compliance with standards and requirements, of issuing the certificates of the SubCAs that operate within the Bolivarian Republic of Venezuela and in accordance with its laws. as Certification Service Providers (PSCs) and who are responsible for issuing electronic certificates for users or end entities.

The Venezuela Root Certificate complies with the periodic publication of its List of Revoked Certificates (LCR); and also maintains an OCSP online service for the validation of the certificates of the SubCAs that are under said root of certification. The address for validation and access to the LCR of Certificate Provider PROCERT, C.A., is as https://www.procert.net.ve/Internas/AC.aspx. The OCSP service access address of Certificate Provider PROCERT, C.A., is as follows. http://ocsp.suscerte.gob.ve.

Certificate Provider PROCERT, C.A., is a private company not belonging to any government entity, which operates its own RPKI under a SubCA scheme subordinated to the Root CA of the Venezuelan State and which is duly accredited and authorized by SUSCERTE to issue electronic certificates for end users.

The SubCA of Certificate Provider PROCERT, C.A., is a CA that provides services to the general public by providing its services as a PSC and issuing certificates for final entities, complying with and keeping updated, all the requirements established by the CA / Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela. applicable for the operation of an RPKI. The address for validation and access to the LCRs of the SubCA of Certificate Provider PROCERT, C.A., is as follows: S/MIME: http://www.procert.net.ve/ecc-crl/smime-ca.crl. The OCSP service access address for the PROCERT, C.A. Certificate Provider SubCAs for S/MIME is as follows: http://ocspsmime.procert.net.ve/ocsp. Certificate Provider PROCERT, C.A., does not own RPKIs outsourced or managed by third parties.

At the time of issuance of this DPC, the RPKI of Certificate Provider PROCERT, C.A. has one (1) partition identified as follows, SubCA for the issuance and management of publicly trusted S/MIME certificates. The SubCA for the issuance and management of publicly trusted S/MIME certificates is active and is designated as a SubCA in production.

The SubCA for the issuance and administration of publicly trusted S/MIME certificates of Certificate Provider PROCERT, C.A. within its obligations to the Signatories must comply with the following: i) Manage the life cycle of the Signatories' certificates; ii) Maintain the LCR and the OCSP active and within the framework authorized by this DPC and the CA/Browser Forum, the rules and procedures established by SUSCERTE and the legislation

of the Bolivarian Republic of Venezuela, applicable for the operation of an RPKI; (iii) Maintain high availability on its certificate management web portal; iv) Keep its RPKI and its documentation updated in accordance with those established by the CA / Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela, applicable for the operation of an RPKI.

All contingency management, disaster recovery and RPKI management processes are developed in this DPC of Proveedor de Certificados PROCERT, C.A.

1.3.2. Registration authorities.

The Registration Authority (AR) is the organization in charge of validating and verifying the identification and data provided by legal or natural persons who purchase electronic certificates and in order to be able to publicly attest that the customer who holds and uses an electronic certificate is the one who effectively claims to be or represents in the case of a legal person. thus guaranteeing the identity of the Signatory owner of an electronic certificate and consequently, establishing the non-repudiation, legal responsibility and obligations derived from the use of the electronic signature under the assumptions of the CA / Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela.

All those interested in obtaining an electronic certificate with legal value and proof must go to a PSC accredited by SUSCERTE. Certificate Provider PROCERT, C.A. is a PSC accredited by SUSCERTE that has a functional AR within its structure.

The AR of Proveedor de Certificados PROCERT, C.A. is in charge of reviewing the documentation, email, identity and biometric data as well as the supports presented by the Signatories, for the purpose of carrying out the verification, face-to-face and documentary validation of the records, supports and other documents that prove the identity and/or representation of the Signatories. as well as their status as representatives of legal entities that opt for an electronic certificate issued by the PSC Provider of Certificates PROCERT, C.A.

The PSC Certificate Provider PROCERT, C.A. does not have outsourced or external ARs. All Signatories must attend an interview in order to verify their identity and data provided in the process of acquiring an electronic certificate. Applications from Signatories who do not attend the interview scheduled by the RA will be cancelled and a penalty will be applied, discarding the consequence. The supporting documentation used to validate the Signatories will be stored by the AR of the PSC Certificate Provider PROCERT, C.A., for a period of ten (10) years from the effective date of the certificate or any of its renewals.

The AR of the PSC Certificate Provider PROCERT, C.A. operates from the administrative headquarters of the aforementioned PSC, maintaining a management scheme aimed at guaranteeing operational continuity and

provision of services with high standards of quality, timeliness and security. The HR manages the requests of the Signatories regarding the life cycle of the certificates and the administrative and legal processes associated with the issuance of electronic certificates in compliance with the CA/Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela.

As of the date of publication of this DPC, the RPKI of Certificate Provider PROCERT, C.A. has one (1) partition identified as follows, SubCA for the issuance and management of publicly trusted S/MIME certificates. The SubCA for the issuance and administration of publicly trusted S/MIME certificates is designated as a SubCA in production and that the AR will be in charge of validating the identification and information provided by the Signatories that manage electronic signatures within the Bolivarian Republic of Venezuela. The information required for the issuance of publicly trusted S/MIME certificates is detailed within the automated contracting system on the web portal of Certificate Provider PROCERT, C.A. The use and attributes of the publicly trusted S/MIME certificate are defined and established in the Certificate Policy (CP) of Certificate Provider PROCERT, C.A.

Upon receipt of the documentation from the Signatories who contract the use of publicly trusted S/MIME certificates, the AR of the PSC Certificate Provider PROCERT, C.A. will proceed to set an opportunity for the identity validation interview to take place, which may be face-to-face, via web or supplemented with a video uploaded by the Signatory on the web portal of the PROCERT Certificate Provider. C.A. During the interview or as a result of the verification of the video uploaded by the Signatory, the AR operator of the PSC Certificate Provider PROCERT, C.A. will approve the application or request the additional information that is necessary for the purpose of establishing and guaranteeing the identity of the Signatory. Once the application is approved, the application for the issuance of the certificate for the validated Signatory will be processed before the RPKI of the Certificate Provider PROCERT, C.A. The management process is automated and after the approval of the electronic file of each Signatory, the RA system informs the RPKI operators about the existing and pending approval requests.

The RA maintains a distribution list to deal with cases associated with RA procedures, the address is registro_01@procert.net.ve, this distribution list has associated with the personal email addresses of RA personnel.

1.3.3. Subscribers.

They are the Signatories and organizations that use the end-user electronic certificates that are generated by RPKI of Certificate Provider PROCERT, C.A inside and outside the Bolivarian Republic of Venezuela. The Signatories are obliged to comply with the conditions of the DPC and PC that are established regarding the authorized use of the electronic certificates issued by Proveedor de Certificados PROCERT, C.A.

1.3.4. Trusted parties.

They are all the Signatories or entities that use electronic certificates and products derived from the RPKI of the PROCERT Certificate Provider, C.A. and that, for the purpose of establishing the trust and validity scheme of the electronic certificates, proceed to the validation of the LCR and/or access to the OCSP service of the RPKI of the PROCERT Certificate Provider. C.A., for the purpose of verifying the validity and operation expected in accordance with the international and national standard within the Bolivarian Republic of Venezuela of the electronic certificates issued by the aforementioned RPKI.

Bona fide third parties are people or legal entities who rely on an electronic signature, electronic certificate, list of revoked certificates or information generated by the PSC Certificate Provider PROCERT and on whom they can place their confidence in accordance with this Statement of Certification Practices (CPP) document. The RPKI of the PROCERT Certificate Provider PSC, is contractually obligated, directly or indirectly (through a chain of contracts) with all customers, suppliers and/or interested parties that are Signatories or not and that use electronic signatures or certificates generated by the PROCERT Certificate Provider PSC.

1.3.5. Other participants.

The PSC Certificate Provider PROCERT, C.A. maintains commercial and contractual relationships and strategic alliances with companies that provide services, software and technology that allow the provision of certification services and the RPKI.

1.4. Use of certificates.

The certificates issued by the PSC Certificate Provider PROCERT, C.A. are generated under the Certification Root of the Venezuelan State and allow establishing the link between a natural person or entity with a public key, which is the product of a validation of their identity through the AR and is generated by the trusted entity PROCERT Certificate Provider. C.A. through its RPKI in compliance with the CA/Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela.

The electronic certificate generated by the PSC Certificate Provider PROCERT, C.A. it works as an identification of the Signatory on the Internet, allowing to guarantee the identity, integrity of the data, the non-repudiation of the transaction and therefore the legal proof of the operation or electronic message, creating a state of trust that allows other users to trust the electronic certificate and the identity of the Signatory issuing the document or electronic message. Through the electronic certificate generated according to standard. which allows other users to securely trust the user's identity on the Internet, as it contains data such as name, surname, ID or professional association number, address, certificate serial number and the public key associated with it.

1.4.1. Appropriate uses of the certificate.

The use of the certificates issued by the RPKI of the PSC Certificate Provider PROCERT, C.A. shall be limited to the use established in the CP of the Certificate Provider PROCERT, C.A., signing of electronic certificates

for subordinate authorities, signing of the lists of revoked certificates and the signing of all certificates established in the CP in compliance with the CA/Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela.

1.4.2. Prohibited uses of the certificate.

The Signatory and trusted third parties users of electronic certificates generated by the RPKI of the PSC Certificate Provider PROCERT, C.A. they are obliged to use them as described in Section 1.4.1. and the uses permitted and indicated in the CP and in the CA/Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela.

1.5. Policy management.

The Senior Management and Operational and AR Staff of the PSC Certificate Provider PROCERT, C.A. will keep this Statement of Certification Practices (DPC) and the Certificate Policy (PC) updated and in accordance with the requirements of the CA/Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela. In this section the Signatory will find information of interest regarding the organizations in charge of the Administration of the policies and documents of the PSC Provider of Certificates PROCERT, C.A.

1.5.1. Organization that administers the document.

This DPC, the PC and documents related to the management of the RA and RPKI of the PSC Provider of Certificates PROCERT, C.A. are maintained, managed and updated by the security and compliance officer; any changes must be approved by the Information Security and Risk Committee, which can be found at the following contact address: Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, oficina B-123, Municipio Chacao, Caracas, República Bolivariana de Venezuela. soporte@procert.net.ve.

1.5.2. Contact person.

Legal Consultancy which is located at the following contact address: Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, oficina B-123, Municipio Chacao, Caracas, República Bolivariana de Venezuela. soporte@procert.net.ve, www.procert.net.ve

Contact person to manage revocation.

The Signatory through the AR system found on the PSC web portal PROCERT, C.A. www.procert.net.ve you can revoke your own RPKI certificate. Likewise, the Signatory may inform the AR about its reasoned request for revocation of the electronic certificate through the address registro_01@procert.net.ve. The HR will validate the information and proceed with the revocation. Any complaint or report regarding the unadjusted operation of the RPKI must be sent to the following address soporte@procert.net.ve, indicating the reasons and evidence. The RPKI operations department will respond to reports of failures in the RPKI's operation.

1.5.2. Person who determines CPS's suitability for the policy.

The security and compliance officer is in charge of determining the suitability of this document considering the opinions of independent auditors duly accredited and with credentials recognized by the CA / Browser Forum and that are the product of follow-up or accreditation audits; compliance with the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela must also be guaranteed.

1.5.4. CPS approval procedures.

Any changes to this CPD. in the PC, as well as in the operating manuals of the PSC Certificate Provider PROCERT, C.A. and that merit a modification other than the semi-annual review of the documentation and derived from any change in the CA / Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela or as a result of remedies ordered by follow-up or accreditation audit reports; it must be managed by the security officer and complied with before the Information Security and Risk Committee of the PSC Certificate Provider PROCERT, C.A., and the changes must be approved in a supported manner and with minutes of approval from the aforementioned Committee.

1.6. Definitions and acronyms.

In order to offer an appropriate interpretation of the meaning and scope of this document, a series of concepts will be set out below, whose denominations in the plural or singular will meet the meaning assigned below:

Trusted Party Agreement: Means the service contract that the Signatory accepts at the time of acquiring an electronic certificate generated by the PSC Certificate Provider PROCERT, C.A. and that contemplates the terms and conditions applicable to such contracting.

Certification Authority (CA): Means an authority trusted by customers and that administers an RPKI aimed at creating, issuing and managing the life cycle of electronic certificates, which for the purposes of Venezuelan legislation must have the accreditation granted by SUSCERTE and additionally comply with the rules of the CA / Browser Forum.

Compliance Audit: means the review and examination of the system of records and activities executed by an authorized professional and whose purpose is to evaluate the adequacy and effectiveness of the system controls to ensure compliance with the policies and operating procedures established and recommended for the operation of a PSC and the RPKI. Detecting the necessary changes in controls, policies and procedures and ensuring the implementation of such changes over time and in compliance with the CA/Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela.

Registration Authority: means the entity whose purpose is to provide local support to the RPKI of the PSC Certificate Provider PROCERT, C.A. in the process of validating the identity and documentation of a Signatory that manages the purchase of an electronic certificate issued by the PSC Certificate Provider PROCERT, C.A.

Baseline Requirements (BR) means the basic CA/Browser Forum requirements for the compliant operation of an RPKI and the fine-tuned issuance of electronic certificates for end entities. www.cabforum.org.

Certificate Chain: Means a chain of multiple certificates required to validate a certificate. Certificate chains are constructed by linking and verifying the electronic signature on a certificate with a public key found on a certificate issued by the PSC Certificate Provider PROCERT, C.A., which is subordinated to and signed by the root certificate of the Venezuelan state and is administered by SUSCERTE.

Electronic certificate: It means a data structure that uses the CCITT ITU X.509 standard, which contains the public key of an entity together with associated information and presented as "unforgettable", by means of an electronic signature of the certification authority that generated it.

Private Key: It means the asymmetric key of an entity, which will only be known by that entity.

Public Key: Means the key to an asymmetric key pair of an entity that can be made public, although it is not necessarily available to the general public since it can be restricted to a predetermined group.

Certification Practice Statement (CPP): means the statement of practices used by a Certificate Authority in its certificate generation process, certificate lifecycle management, information about security control processes and risk remediation mechanisms and disaster recovery procedures, which must be known to the Signatories who rely on the electronic certificates issued by the PSC PROCERT Certificate Provider, C.A.

Open Public Key Resource Infrastructure (RPKI): Means any entity that owns and manages a CA and that provides end entities, certification services under a PKI that complies with the standards and regulations imposed by the CA/Browser Forum, the rules and procedures established by SUSCERTE and the legislation of the Bolivarian Republic of Venezuela, for the compliant operation of a PSC.

Data Integrity: Means the quality or condition of being accurate, complete, and valid and not being altered or destroyed in an unauthorized manner.

Interoperability: Interoperability implies that the equipment and procedures used by two or more entities are compatible and, therefore, it is possible for them to assume common or related activities.

List of Revoked Certificates (LCR): means the list of certificates that have been revoked or suspended by the PSC Certificate Provider PROCERT, C.A. and are no longer trusted by the general public. The LCR is valid for twenty-four hours and the LCR is published by the RPKI periodically, complying with the twenty-four-hour period between each publication.

Online Certificate Status Protocol (OCSP) is an online service that allows you to validate the status of an electronic certificate issued by the PSC Certificate Provider PROCERT, C.A. The response to the requests includes three (3) statuses: valid, revoked or unknown.

Asymmetric Key Pair: Means the pair of related keys where the private key defines the private transformation and the public key defines the public transformation.

CP Certificate Policy. It is the document containing the set of rules and technical characteristics and use of the electronic certificates generated by the PSC Certificate Provider PROCERT, C.A. under its RPKI.

PSC: Stands for Certification Service Provider

Audit Log: Means the discrete unit of data recorded in the audit trail when an event occurs that is logged. An audit log consists of a set of audit descriptions, each of which has a set of audit attributes associated with it. Each audit log has an audit description for the log header and usually has additional audit descriptions that describe the entity(ies) and object(s) involved in the event.

Certificate Revocation: Means the process of changing the status of a certificate from valid to suspended or revoked. When a certificate has revoked status, this means that an entity should no longer be trusted for any purpose. The revocation in the case of the PSC Supplier of Certificates PROCERT, C.A. PSC, can be self-managed by the Signatory or requested from the RA.

Certification Services: Means the services that can be provided in relation to the management of the lifecycle of certificates at any level of the RPKI hierarchy including ancillary services such as OCPS services, time-sharing services, identity verification services, revoked certificate list (LCR) hosting, among others.

Signatory: Means the entity that has requested the issuance of a certificate within the RPKI of the PSC Certificate Provider PROCERT, C.A. In international standard, the Signatory is the Subscriber or party that uses an electronic certificate or receives electronic certification services.

SUSCERTE: It means the Superintendence of Electronic Certification Services, which is the governing body in matters of Electronic Certification within the government organizations in the Bolivarian Republic of Venezuela.

Certificate Usage: Means the set of rules that indicate the applicability of a particular community's certificate and/or the class of application with common security requirements. Certificate uses are defined in the PC Certificate Policy document.

Validation: means the process of verifying the validity of a Certificate in terms of its status (e.g. suspended or revoked).

1.6.1. Acronyms.

AATL	Adobe Approved Trust List
AC	Certificate Authority
BR	Baseline Requirements
DNS	Domain Name Service
DPC	Certification Practices Statement
DV	Domain Validated
ETSI	European Telecommunications Standards Institute EU
ECDSA	Elliptic curve algorithm

FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Working Group
IGTF	International Federation of Trust in the Network
CSF	Certificate Revocation List
OID	Object Identifier
PC	Certificate Policy
RFC	Request for Feedback
SAINT	Subject's alternative name
SSL	Secure sockets layer
TLD	Top-Level Domain
	Transport Layer Security
TSA	Time-stamping authority
TST	Timestamp Token
TTL	Time to live.
ITU	International Telecommunication Union
UTC	Coordinated Universal Time
X.509	The ITU-T standard for certificates and its corresponding authentication framework

2. Publishing and repository responsibilities.

2.1. Repositories.

According to the CP, RPKI-signed certificates, CRLs, and objects MUST be available for download by all relying parties to enable them to validate this data. The PSC Certificate Provider PROCERT, C.A. RPKI CA will publish RPKI certificates, CRLs, and signed objects through a repository that can be accessed through the AC section on the PROCERT website www.procert.net.ve at the https://www.procert.net.ve/Internas/AC.aspx link. This repository will conform to the structure described in [RFC6481].

2.2. Publication of certification information.

The PSC Certificate Provider PROCERT, C.A. will publish certificates, CRLs and RPKIs issued by it to a repository that functions as part of a globally distributed system of RPKI repositories. The publication links are as follows:

On the Web.
CPS
https://www.procert.net.ve/Internas/AC.aspx.

PC
https://www.procert.net.ve/Internas/AC.aspx.

CSF

- PROCERT ECDSA SubCA
  - S/MIME CRL: www.procert.net.ve/ecc-crl/smime-ca.crl

OCSP

- PROCERT SubCA OCSP EDCSA

- S/MIME OCSP: http://ocspsmime.procert.net.ve/ocsp

- SUSCERTE OCSP ECDSA
  http://ocsp-ecdsa.suscerte.gob.ve/

Certificates issued
- https://www.procert.net.ve/ConsultaPublica/index.aspx

CA Certificates
- PROCERT ECDSA
  - S/MIME cert: www.procert.net.ve/ecc-crt/smime-ca.crt

SUSCERTE PSC PROCERT certificate
EDCSA www.procert.net.ve/ecc-chain/cadena.p7b

Life cycle management
https://www.procert.net.ve/sistemaAR/login.aspx . Through the AR System, the user is able to generate or revoke their certificate, following the steps contained in the user manual, which can be accessed through the PROCERT ITFB, C.A. Certificate procert.net.ve/Docs/Proveedor - General Usuario.pdf Manual

Support
https://www.procert.net.ve/Internas/Soporte.aspx

By email: soporte@procert.net.ve
By phone: +58 (212]) 2674880
In person: Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, oficina B-123, Municipio Chacao, Caracas, República Bolivariana de Venezuela.

2.3. Time or frequency of publication.
The PSC Certificate Provider PROCERT, C.A. must generate a list of revoked certificates (LCR) every twenty-four (24) hours, which constitutes a mechanism for validating and checking the status of the electronic certificates and verifying which ones are revoked. All certificate revocation processes are informed by PSC Certificate Provider PROCERT, C.A., via email to the Signatory. This notification is reported monthly to SUSCERTE and is included in the digitized deposit maintained by the PSC Supplier of PROCERT Certificates, C.A.

The PSC Certificate Provider PROCERT, C.A. CA will publish its LCR every day at 14:00 hours GMT Caracas and is the nextUpdate LCR scheduled and issued in advance by the RPKI CA of the PSC Certificate Provider PROCERT, C.A.

2.4. Access controls in repositories.
Access to the trusted repositories of the PSC Certificate Provider PROCERT, C.A. has been configured so that the Signatories or users of such repositories can only query them, in the case of service validators such as OCSP and LCR. In the case of consulting certification chains, downloading them is allowed and in the case of documentation, downloading the required files and documents

and for reading them is also allowed. Permission to write, change information, or execute code is not authorized for the purpose of preventing security events against the RPKI.

3. Identification and authentication.
   3.1. Nomenclature.
      3.1.1. Types of names.
      The subject of each certificate issued by this organization is identified by a distinctive name (DN) X.500. The distinctive name shall consist of a single Common Name (CN) attribute with a value generated by PSC Proveedor de Certificados PROCERT, C.A. The serial number attribute is included together with the common name (to form a set of terminal relative distinguishing names), to distinguish between successive instances of certificates associated with the same entity.

      3.1.2. Need for names to be meaningful.
      The Certificate Provider PROCERT, C.A. uses within its certificate structure, distinctive names that allow both the Signatory or user entity that uses the certificate, and the entity issuing said certificate, thus establishing the information that allows linking a certificate issuer with its Signatory or end user.

      3.1.3. Anonymity or pseudonyms of subscribers.
      Although the names of the subjects on certificates issued by this organization MUST NOT be meaningful and may appear "random," anonymity is not a function of this RPKI; therefore, the Certificate Provider PROCERT, C.A. does not issue electronic S/MIME certificates under anonymity or with pseudonyms for final entities or signatories.

      3.1.4. Rules for the interpretation of the different forms of names.
      The rules of the names used for the issuance of certificates and identification of the Signatories or end users and the issuing entity shall be those established by RFC 2253 and ITU-T X.500.

      3.1.5. Uniqueness of names.
      The Certificate Provider PROCERT, C.A. certifies that the names of the subjects are unique among the certificates it issues, as well as their serial numbers, in order to make the necessary differentiation between different Signatories of the RPKI. Name uniqueness is applied within the RPKI of Certificate Provider PROCERT, C.A. as follows:

      - S/MIME Certificates: Identifies a person and also allows electronic signature, MUST require for its issuance the Signatory's own names and surnames, unique identity number and email, which are associated with a unique RPKI certificate series. At the time of issuance of this version of DPC, the Certificate Provider PROCERT, C.A. has a SubCA S/MIME in operation.

      3.1.6. Recognition, authentication and function of trademarks.
      The Certificate Provider PROCERT, C.A., will only issue S/MIME certificates belonging to legal entities that do not violate the right of ownership

over duly registered domains. The right to use a trademark or trade name or existing disputes over such marks is not verified; the Certificate Provider PROCERT, C.A., only verifies the veracity of the company and domain ownership documents, for the purposes of the issuance of the certificates by the RPKI, after validation and authorization by the AR. The Certificate Provider PROCERT, C.A. is not obligated to issue certificates when an entity has a commercial name dispute and reserves the right to revoke a certificate when there is a commercial dispute regarding the trade name or domain of a company or legal entity.

3.2. Initial identity validation.

The Certificate Provider PROCERT, C.A., in order to comply with the international standard and the laws of the Bolivarian Republic of Venezuela, is obliged to carry out a rigorous examination of the information that is provided by the Signatories or end users of electronic certificates or certification services; in this sense, the AR of Provider of Certificates PROCERT, C.A., uses all legal means and governmental or non-governmental links, which are public and that allow establishing the suitability and legality of the information provided by the Signatories or end users of electronic certificates or certification services, during the process of contracting them, in order to generate legal consequences and non-repudiation.

3.2.1. Method for proving possession of a private key.

Signatories who use electronic certificates generated by Certificate Provider PROCERT, C.A., must comply with an identity validation process that must be positive in terms of the validation of the information provided and prior to the process of generating their cryptographic key pair. The generation of the private key varies in each case but always validates that it is the end user who owns the certificate, who generates and manages their certificate. The methods of validating the identity possession of a private key in Certificate Provider PROCERT, C.A., are as follows:

- S/MIME Certificate: The Signatory or end user provides all the information required for its identification validation; this information is recorded in the corresponding certificate template and once the RA approval steps have been completed, the Signatory from the Certificate Provider portal PROCERT, C.A., will proceed to generate the cryptographic key pair of its certificate. Once the request has been generated, the CA of Certificate Provider PROCERT, C.A., proceeds to approve the certificate and the user will download their certificate including a security key to manage the signing of their certificate by demonstrating the proof of possession (PoP) of the private key corresponding to the public key of the certificate. In the online signature system, the electronic signature is managed with a username and password to access the portal, plus a unique one-time key that reaches the Signatory via email or SMS text message, thus demonstrating the proof of possession (PoP) of the private key corresponding to the certificate's public key.

3.2.2. Authentication of the organization's identity.

Certificate Provider PROCERT, C.A., through the RA, executes the identity validation and verification of all the data provided by the Signatories and end entities that use electronic certificates generated by the RPKI.

- S/MIME certificates under the legislation of the Bolivarian Republic of Venezuela, in compliance with the international standard, depending on the certificate that is managed and after being carried out in accordance with the validation of identity and the documentation provided by the Signatory by the RA; they prove the identity of the Signatory or end user of the certificate, their affiliation with a certain guild or entity and grant the non-repudiation of the transactions carried out by the Signatory in question. The data and information provided by the Signatory are safeguarded with confidentiality criteria. The verification of the information is carried out by HR against government sources in order to establish the accuracy of the data provided by the Signatories and therefore prove their identity.

  Certificate Provider PROCERT, C.A., within the verification elements executed by the AR, contemplates the verification of both the domain and email procession, including the use of secure email within the attributes of the electronic certificate. Emails identifying a Signatory may not be or contain general definitions and must clearly identify Signatories by their first and last name. A mechanism for validating ownership and control of the email address is included that the Signatory must successfully complete to the satisfaction of the RA, without which the electronic certificate will not be issued.

  However, the certificates are issued by the RPKI to the Signatories in a manner that preserves the accuracy of the INR distributions represented in Certificate Provider PROCERT, C.A. Additionally, Certificate Provider PROCERT, C.A., has on its web portal the following link https://www.procert.net.ve/ConsultaPublica/index.aspx, through which, any entity or person may determine whether an electronic certificate issued by the Certificate Provider PROCERT, C.A., belongs to a specific Signatory.

3.2.3. Authentication of individual identity.

Certificate Provider PROCERT, C.A., for the purpose of managing and issuing an electronic certificate of a person or entity, executes information and identity validation procedures through the AR; These procedures are as follows:

- S/MIME certificates.
  - Names and surnames of the Signatory
  - Signatory contact telephone number (Mobile or landline)
  - Email from the Signatory.
  - Validation of email ownership and control through an email account confirmation process.
  - Digitized copy of the identity document.

- Review of the Signatory's identity document in order to certify that it is a person duly registered with the national identity service.
- Digitized copy of the Tax Information Registry (RIF) of the Signatory.
- Review of the Signatory's RIF in order to certify its validity and existence.
- Public service bill showing the Signatory's home address.
- Video identification of the Signatory indicating their intention to contract an electronic certificate.
- If you are a professional, accompany the proof of registration in Professional Associations.
- Identity validation interview in case of being considered by the RA.

- S/MIME certificates for company representatives.
  - Names and surnames of the Signatory
  - Signatory contact telephone number (Mobile or landline)
  - Email from the Signatory.
  - Validation of email ownership and control through an email account confirmation process.
  - Digitized copy of the identity document.
  - Review of the Signatory's identity document in order to certify that it is a person duly registered with the national identity service.
  - Digitized copy of the Tax Information Registry (RIF) of the Signatory.
  - Review of the Signatory's RIF in order to certify its validity and existence.
  - Public service bill showing the Signatory's home address.
  - Video identification of the Signatory indicating their intention to contract an electronic certificate.
  - In the case of being a company representative or public official, attach the documents that prove their representation (Act, power of attorney or Statutes) or the Official Gazettes of designation in office.
  - Identity validation interview in case of being considered by the RA.
  - Details of the constitutive or creation document of the legal entity it represents and its status and position.
  - Digitized copy of the Tax Information Registry (RIF) of the Signatory.
  - Review of the RIF of the legal entity it represents in order to certify its validity and existence.
  - Public service bill showing the address of the legal entity.
  - Public service bill showing the address of the legal entity.

3.2.4. Unverified subscriber information.

Certificate Provider PROCERT, C.A., does not include data of unverified subscribers in certificates issued under this certificate policy, including for access to subject information (SIA) [RFC6487].

3.2.5. Authority validation.

As established in point 3,2,3 above, the AR of Certificate Provider PROCERT, C.A., once it has the information and documentation requested from the Signatory or final entity using the certificate, the AR will proceed to validate it against public government and independent registries in order to contract its validity and establish the mechanisms for verifying email

control. telephone and domain. In cases where the validation is successful, the electronic certificate will be processed. In cases where objections occur to the documentation or in the process of checking the control of email, telephone and domain, the generation of the certificate will not be processed until the observations and non-conformities are corrected.

3.2.6. Interoperability criteria.
Certificate Provider PROCERT, C.A., does not currently have subordinate CAs or a cross-certification scheme with other CAs. Notwithstanding the foregoing, it declares that it is capable of establishing these operating schemes, which will mediate through agreements signed and authorized by SUSCERTE for cases of operation within the Bolivarian Republic of Venezuela.

3.3. Identification and authentication for key change requests.

3.3.1. Identification and authentication for routine key re-entry.
Certificate Provider PROCERT, C.A. maintains a policy of non-remittance of keys for S/MIME certificates. In cases where the key is compromised or a new certificate is required, the Signatory must make a new request that must be validated in order to be able to issue the certificate, discounting the period of validity of the certificate in the new issuance process.

3.3.2. Identification and authentication for key re-entry after revocation.
Certificate Provider PROCERT, C.A. maintains a policy of non-remittance of keys for S/MIME certificates. In this case, the procedure is as indicated in point 3.3.1. In the case of certificates, the procedure indicated in point 3.3.1 also applies.

3.4. Identification and authentication for the revocation request.
Certificate Provider PROCERT, C.A., maintains an operation and management scheme, where the Signatory or final entity using an electronic certificate generated by RPKI of Certificate Provider PROCERT, C.A., directly manages the process of revocation of its own electronic certificate; in this case the S/MIME certificate may be revoked by following the steps below:

- The Signatory or authorized representative must log into the AR system by entering their username and password.
- The Signatory or authorized representative must enter the revocation section of the certificate and indicate the reason for revoking their certificate. The system will send an alert email to the registered email address indicating the start of the revocation process.
- Next, the Signatory or authorized representative must enter the one-time password (OTP) that is sent to the phone associated with their account. If you successfully pass this process, the revocation button will be activated.
- Once the revocation button is activated, the Signatory or authorized representative will proceed to revoke the certificate.
- The AR system will send an email to the AR to inform about the revocation of the electronic certificate.

4. Certificate lifecycle operational requirements.

4.1. Request for a certificate.

4.1.1. Who can submit a certificate application?

Any current subscriber who holds INR distributed by Certificate Provider PROCERT, C.A., may submit a certificate application to this CA. (The exact meaning of "up to date" is in accordance with the Privacy Policy.) PROCERT Certificate Provider, C.A. All Signatories or representatives of the final entity that uses the certificate must comply with the delivery of the documentation and the validation steps established by the AR of Proveedor de Certificados PROCERT, C.A., without which their application will not be processed.

4.1.2. Enrollment Process and Responsibilities.

Signatories and end entities interested in obtaining electronic certificates from the RPKI of Certificate Provider PROCERT, C.A., must enter the URL www.procert.net.ve and access the AR system through procert.net.ve/sistemaAR/login.aspx and manage their registration in case they do not have electronic certificates. The following steps must be completed in the registration process:

- The Signatory registers in the AR system and The Signatory will select the type of electronic certificate generated by the CA of Certificate Provider PROCERT, C.A.
- The Signatory must attach the documentation required for each S/MIME certificate.
- The Signatory must upload the documentation in PDF format and a video of identity and validation of use of the certificate.

Any person or company that meets the legal conditions provides the documentation and legal and technical requirements, passing the validation process of the RA will be eligible for an electronic certificate issued by the RPKI of Proveedor de Certificados PROCERT, C.A.

4.2. Processing of the certificate application.

The AR of PROCERT Certificate Provider is in charge of building the electronic file of the Signatory in order to include in it the regulatory and legal requirements demanded inside and outside the Bolivarian Republic of Venezuela, for the compliant issuance of the type of certificate requested by the Signatory and Provider of PROCERT Certificates. C.A. is able to offer. Once the file of each Signatory has been validated and the documentation review and identity validation processes are satisfied, the AR system will send the Signatory an email indicating that it can generate its certificate request or upload its CSR depending on the type of certificate that the Signatory manages.

4.2.1. Performing identification and authentication functions.

The AR of Certificate Provider PROCERT, C.A., after receiving the documents and supports delivered by the Signatories or final entities using electronic certificates, in compliance with the international and legal standards applicable within the Bolivarian Republic of Venezuela, will proceed to review them, in order to verify and record the declarations and

documentation provided by the Signatories or final entities using certificates Electronic; This process will be carried out as follows:

- S/MIME Certificates: The AR of Certificate Provider PROCERT, C.A., proceeds to validate the identification and the Tax Information Registry (RIF) that are provided by the Signatory through systems that are integrated into the National Integrated System of Customs and Tax Administration (SENIAT), the National Electoral Council (CNE) and the Administrative Identification Service. Migration and Foreigners (SAIME); for the purposes of determining the validity and accuracy of such information. Likewise, and in the event that the email addresses correspond to legal entities, the existence of the domains is validated through the use of the information provided by https://whois.domaintools.com/ Whois Lookup, Domain Availability & IP Search - DomainTools, ICANN Lookup and NIC.ve . The domains of the companies are validated and a letter from the company's human resources representative is requested in order to record that the Signatory works for said company; in the case of company representatives, the documents, powers of attorney, minutes or records that prove their representation of the company are requested, and in the case of public officials, the Official Gazette is additionally requested where their designation and position appear. Gmail email addresses are validated for the purpose of verifying their existence and control over them and are only accepted for natural person certificates. The Signatory's physical address is validated against the official records provided and a utility receipt provided by the Signatory and required to manage their certificate.

- SSL Certificates: The AR of Certificate Provider PROCERT, C.A., proceeds to validate the identification and the Tax Information Registry (RIF) that are provided by the Signatory or representative of the final entity using the electronic certificate, through systems that are integrated into the National Integrated System of Customs and Tax Administration (SENIAT) and the Administrative Identification Service. Migration and Foreigners (SAIME); for the purposes of determining the validity and accuracy of such information. Likewise, and in the event that the email addresses correspond to legal entities, the existence of the domains is validated through the use of the information provided by https://whois.domaintools.com/ Whois Lookup, Domain Availability & IP Search - DomainTools, ICANN Lookup and NIC.ve . The domains of the companies are validated and a letter from the company's IT representative is requested in order to record that the domain belongs to them and they are in the process of managing the certificate indicating its use; company representatives must attach the documents, powers of attorney, minutes or records that prove their representation of the company and in the case of public officials, the Official Gazette is additionally requested where their designation and position appear. The Signatory's physical address is validated against the official records provided and a utility receipt provided by the Signatory and required to manage their certificate.

4.2.2. Approval or Rejection of Certificate Requests.

Certificate Provider PROCERT, C.A., establishes that all requests for certificates made by Signatories or final entities using certificates will be processed and approved as long as the validation process described in 4.2.1. is satisfactorily complied with by the HR on the documentation, collections and validations that must be complied with by the Signatory or final entity using electronic certificates. Without exception, applications for certificates that do not meet the requirements established by Proveedor de Certificados PROCERT, C.A. and that are based on national and international norms and standards that regulate RPKI's activity will not be processed.

4.2.3 Processing time for certificate applications

Certificate Provider PROCERT, C.A., establishes a maximum process of forty-eight (48) hours for the issuance of electronic certificates once the Signatories or final entities using electronic certificates have complied with and passed satisfactorily for the Signatory or final entity using electronic certificates. All the processes contemplated on 4.2.1.

4.3. Issuance of certificates

4.3.1. CA Actions During Certificate Issuance

The CA of Certificate Provider PROCERT, C.A., will only validate and manage those requests for electronic certificates that pass the validation and verification process of the AR of Certificate Provider PROCERT, C.A. Once the request for an electronic certificate has been approved by the Signatory or final entity using the electronic certificate, the AR will approve the procedure and immediately the AR System of Certificate Provider PROCERT, C.A, will activate the button to generate the certificate request; then the Signatory will click on the button to generate the certificate request and the AR System will send its certificate request to the CA of PROCERT Certificate Provider, C.A. The operator of the CA of Certificate Provider PROCERT, C.A. will verify the information contained in the certificate for the purposes of compliance with the national and international standard and will proceed to press the approval button of the certificate application; then the CA will issue the certificate and inform the Signatory via email about the issuance of its certificate.

4.3.2. Notification to the subscriber by the CA of the issuance of the certificate

Certificate Provider PROCERT, C.A. automatically notifies the Signatory via email about the approval of its certificate. The signatory must enter the AR System of Certificate Provider PROCERT, C.A., access the certificate download section, enter the access key to that section and will have in view for a single time the private key of their certificate, which they require to export it securely, following the procedure established by PROCERT Certificate Provider. C.A. and including a key for the use of your certificate from your computer. Additionally, the user will be able to sign online with their certificate using the AR System of Certificate Provider PROCERT, C.A. and including the two-factor authentication factors that are presented, without which they will not be able to sign. In the case of SSL certificates. The end users of the electronic certificate will receive the certificate with the certification chain via email with the corresponding installation instructions.

4.3.3. Notification of the issuance of certificates by the CA to other Entities.
Certificate Provider PROCERT, C.A. must notify SUSCERTE through a monthly report, about the electronic certificates it has issued during the month immediately prior to the date of the report.

4.4. Certificate acceptance

4.4.1. Conduct Constituting Acceptance of the Certificate
When a certificate is issued, the CA of the Certificate Provider PROCERT, C.A. proceeds to publish them in its repository of certificates issued Public Consultation (procert.net.ve) so that they can be consulted by interested third parties and notifies the Signatory or end user of the certificate directly and by email. Once issued, the Signatories or final entities using the certificates will proceed to install them on their computers and manage the signing process with the security mechanisms that the AR System has and offers for S/MIME certificates.

4.4.2. Publication of the certificate by the CA
The certificates will be published for public consultation (procert.net.ve), following the conduct described in section 4.4.1. The publication will be made within forty-eight (48) hours following the satisfactory validation by the RA.

4.4.3. Notification of the issuance of certificates by the CA to other entities.
Certificate Provider PROCERT, C.A. must notify SUSCERTE through a monthly report, about the electronic certificates it has issued during the month immediately prior to the date of the report.

4.5. Using key pairs and certificates.
Certificate Provider PROCERT, C.A. informs the Signatories, final entities using the electronic certificates and interested third parties about the use of the electronic certificates and the responsibilities arising from such use.

4.5.1. Use of the subscriber's private key and certificate.
Certificates issued by Proveedor de Certificados PROCERT, C.A. to the subordinate INR and their holders are CA certificates. The private and public key associated with each of these certificates is used according to the established use and improved use of each certificate, which are described in the CP of Proveedor de Certificados PROCERT, C.A.

4.5.2. Use of relying party certificates and public keys.
The primary relying parties of this RPKI are organizations that use the electronic certificates generated by the Certificate Provider PROCERT, C.A. CA and that establish trust in the use of the certificate that comply with X.509, IETF RFC, and other applicable RPKI and AR standards and with the international standard established by the CA Browser Forum, the rules issued by SUSCERTE and the legislation that regulates the matter within the Bolivarian Republic of Venezuela.

In any case, users must rely on the certificates that, once verified through the LCR or the OCSP service, allow them to establish that they are valid

and current and that all signatures made during the period of validity of said certificate will be understood as valid and will enjoy non-repudiation, integrity and legal proof. The conditions of use of the certificates issued by the RPKI of Certificate Provider PROCERT, C.A. are described in the PC and must be reviewed by the Signatories in order to know their scope and use. In addition, the contract and terms of use of the certificates establish the obligation of the Signatories regarding the use of the electronic certificates.

4.6. Renewal of the certificate.

4.6.1. Circumstance for the renewal of the certificate.

Certificate Provider PROCERT, C.A. informs all Signatories or final entities using S/MIME electronic certificates that the circumstances that apply to opt for the renewal of an electronic certificate issued by the RPKI is the expiration of the validity period or the commitment of the private key of the electronic certificate. In both cases, a new pair of keys will always be generated and as indicated in numeral 4.7. The AR of Proveedor de Certificados PROCERT, C.A. notifies its Signatories thirty (30) days in advance, regarding the expiration of the certificate. For SSL certificates, a new CSR will be submitted. In both cases, the previous process of validation of the RA applies, without which certificates will not be issued.

4.6.2. Who can apply for renewal?

The Signatory or end entities using electronic certificates can start the process of renewing their electronic certificate. The AR of Certificate Provider PROCERT, C.A. will validate the identity and documentation that must be presented by the Signatories or final entities using electronic certificates and will proceed as indicated in point 4.2.1. of this DPC.

4.6.2. Processing applications for renewal of certificates.

Applications for renewal of certificates will be managed by the Signatory themselves through the portal of Signatories or final entities using electronic certificates www.procert.net.ve and select the link of the AR system through procert.net.ve/sistemas/login.aspx and will proceed to include and enter the information that is required in accordance with X.509, IETF RFC and other applicable standards in terms of RPKI and AR and with the standard established by the CA Browser Forum, the rules issued by SUSCERTE and the legislation that regulates the matter within the Bolivarian Republic of Venezuela. The verification of all this information and of the entity of the Signatory or end user of the electronic certificate will be carried out in accordance with the provisions of point 4.2.1. that precedes.

4.6.4. Notification of the issuance of a new certificate to the subscriber.

Certificate Provider PROCERT, C.A. automatically notifies the Signatory via email about the approval of its certificate. This notification shall be made in accordance with the provisions of point 4.3.2.

4.6.5. Conduct constituting acceptance of a renewal certificate.

The acceptance process will be understood as the one contemplated and described in section 4.4.1. of this CPD.

4.6.6. Publication of the renewal certificate by the CA.
See section 4.4.2.

4.6.7. Notification of the issuance of certificates by the CA to other entities.
See section 4.4.3.

4.7. Certificate key change.

4.7.1. Circumstance for the re-entry of the certificate key.
Certificate Provider PROCERT, C.A. does not renew keys. In the event that the issuance of a new electronic certificate is required, it may only proceed under the occurrence of the following cases:

- Private key compromise.
- Expiration of the validity period of the certificate.

The verification of all this information and of the entity of the Signatory or end user of the electronic certificate will be carried out in accordance with the provisions of point 4.2.1. that precedes.

4.7.2. Who can request certification of a new public key?
Only a certificate holder can request a new key. In addition
PROCERT Certificate Provider, C.A. Initiates a new key based on a validated key compromise or expiration notification. If the signatory or final entity using the electronic certificate requests a new certificate, it must comply with the steps provided for and contained in section 4.2. of this DPC. However, the AR System of Certificate Provider PROCERT, C.A. allows the Signatory to manage the life cycle of its certificate and proceed to revoke the certificate if it deems it necessary, indicating for this purpose the cause of the revocation. Applications that are not self-managed will be validated by the AR of Provider of Certificates PROCERT, C.A., requiring the approval of the AR to proceed with the revocation.

4.7.3. Processing certificates rekey requests.
Certificate Provider PROCERT, C.A. does not renew keys. In the event that the issuance of a new electronic certificate is required, the Signatory must fully comply with each of the steps and processes contemplated in section 4.2.

4.7.4. Notification of the issuance of a new certificate to the subscriber.
Certificate Provider PROCERT, C.A. automatically notifies the Signatory via email about the approval of its certificate. This notification shall be made in accordance with the provisions of point 4.3.2.

4.7.5. Conduct that constitutes acceptance of a certificate with a new key.
When a new certificate is issued, the CA will publish it in the archive in the repositories indicated and in accordance with the provisions of point 4.4.1 of this DPC.

4.7.6. Publication of the new key certificate by the CA.
Certificate Provider PROCERT, C.A. does not renew keys. For the process of issuing a certificate by the CA, see section 4.4.2. of this CPD.

4.7.7. Notification of the issuance of certificates by the CA to other entities.
Certificate Provider PROCERT, C.A. must notify SUSCERTE through a monthly report, about the electronic certificates it has issued during the month immediately prior to the date of the report.

4.8. Modification of the certificate.
Certificate Provider PROCERT, C.A. does not modify certificates. In the event that the issuance of a new electronic certificate is required, the Signatory must fully comply with each of the steps and processes contemplated in section 4.2.

4.8.1. Circumstance for the modification of the certificate.
Certificate Provider PROCERT, C.A. does not modify certificates. In the event that the issuance of a new electronic certificate is required, the Signatory must fully comply with each of the steps and processes contemplated in section 4.2.

4.8.2. Who can request the modification of the certificate?
Certificate Provider PROCERT, C.A. does not modify certificates. In the event that the issuance of a new electronic certificate is required, the Signatory must fully comply with each of the steps and processes contemplated in section 4.2.

4.8.3. Processing of certificate modification requests.
Certificate Provider PROCERT, C.A. does not modify certificates. In the event that the issuance of a new electronic certificate is required, the Signatory must fully comply with each of the steps and processes contemplated in section 4.2.

4.8.4. Notification of the issuance of modified certificates to the subscriber.
Certificate Provider PROCERT, C.A. does not modify certificates. In the event that the issuance of a new electronic certificate is required, the Signatory must fully comply with each of the steps and processes contemplated in section 4.2.

4.8.5. Conduct that constitutes acceptance of the modified certificate.
Certificate Provider PROCERT, C.A. does not modify certificates. In the event that the issuance of a new electronic certificate is required, the Signatory must fully comply with each of the steps and processes contemplated in section 4.2.

4.8.6. Publication of the modified certificate by the CA.
Certificate Provider PROCERT, C.A. does not modify certificates. In the event that the issuance of a new electronic certificate is required, the Signatory must fully comply with each of the steps and processes contemplated in section 4.2.

4.8.7. Notification of the issuance of certificates by the CA to other entities.
Certificate Provider PROCERT, C.A. does not modify certificates. In the event that the issuance of a new electronic certificate is required, the Signatory must fully comply with each of the steps and processes contemplated in section 4.2. Certificate Provider PROCERT, C.A. must notify SUSCERTE through a monthly report, about the electronic certificates it has issued during the month immediately prior to the date of the report.

4.9. Revocation and suspension of the certificate.
The revocation of a certificate is the process that ends the useful life of the certificate and its use as it is invalidated, so that other Signatories do not have to rely on that certificate. The CA of Certificate Provider PROCERT, C.A. places in the LCR the certificates that are revoked, in order to maintain the confidence of the Signatories. Likewise, the RPKI of Supplier of PROCERT Certificates, C.A. maintains the OCSP so that Signatories, interested third parties or information systems can validate online if a certificate is revoked, thus increasing confidence in the use of electronic certificates. To revoke a certificate, the Signatory holder of the certificate must request it from the AR of Proveedor de Certificados PROCERT, C.A. Suspension is the process by which the temporary validity of an electronic certificate is modified and can only be requested by the Signatory who holds the electronic certificate. The AR of Supplier of Certificates PROCERT, C.A., after verification, proceeds to place a certificate out of use for a certain period of time, which may be activated again after the suspension period has expired.

4.9.1. Circumstances for revocation.
PROCERT Certificate Provider, C.A. in compliance with the international standard, it establishes that the request for revocation of the certificate when it is not made directly by the Signatory in the AR System, can only be processed by the Signatory before the AR of Proveedor de Certificados PROCERT, C.A. and based on one of the following assumptions:

- Compromise of the certified private key.
- Expiration of the validity period of the certificate.
- Renewal of the certificate.
- Signatory's request for a new certificate for an update or change of use as established on the PC.
- Judicial Request.
- Death of the Signatory.
- Disincorporation of the Signatory from the legal entity it represents.
- Compromise or loss of the device or certificate storage media.
- Change or modification of the international and national standard that make it necessary to revoke the certificate.

4.9.2. Who can request the revocation?
Only the Signatory or final entities that own the electronic certificates issued by the RPKI of Certificate Provider PROCERT, C.A., can initiate the process of revocation of their electronic certificate. The AR will validate the identity and documentation that must be presented by the Signatory or final entities using electronic certificates and the certificate will be revoked.

In the same way, the Signatory or final entities that own the electronic certificates, will be able to enter and comply with the authentication steps and place the one-time security key (OTP), necessary to authorize the transaction within the AR System and proceed to revoke their certificate online.

4.9.3. Procedure for the request for revocation.

The Signatory or final entities that own the electronic certificates issued by the RPKI of Certificate Provider PROCERT, C.A., when they request the revocation of their certificate, must send their request in electronically signed mail, through their email account registered in PROCERT Certificate Provider, C.A. The request must be based on one of the grounds established in section 4.9.1. Once the application has been received, the HR will validate the identity and documentation to be submitted by the Signatory or final entities using electronic certificates and the certificate will be revoked. You will be informed via email about the revocation of the certificate. In the same way, the Signatory or final entities that own the electronic certificates, will be able to enter and comply with the authentication steps and place the one-time security key (OTP), necessary to authorize the transaction within the AR System and proceed to revoke their certificate online.

4.9.4. Grace period of the revocation request.

The Signatory or final entities that own the electronic certificates issued by the RPKI of Certificate Provider PROCERT, C.A., must request the revocation of their certificate, within twenty-four (24) hours following the occurrence of any of the causes for revocation indicated in section 4.9.1.

4.9.5. Time frame within which the CA must process the revocation request.

PROCERT Certificate Provider, C.A. in compliance with the international standard establishes that the request for revocation of the certificate when made through email soporte@procert.net.ve will be processed within one (1) hour following the validation by the RA. In the same way, the Signatory or final entities that own the electronic certificates, will be able to enter and comply with the authentication steps and place the one-time security key (OTP), necessary to authorize the transaction within the AR System and proceed to revoke their certificate online.

4.9.6. Revocation check requirement for parties relying on trust.

PROCERT Certificate Provider, C.A. In compliance with the international standard X.509, IETF RFC and RFC 6484 establishes within its RPKI two (2) methods of checking the status of the certificates issued by the CA of Certificate Provider PROCERT, C.A.; the first is the List of Revoked Certificates (LCR), which consists of a periodic publication of the certificates that are revoked in order to make them public and generate greater confidence in the Signatories of the RPKI. The second method of checking the status of the certificate is the Online Certifífícate Status Protocol (OCSP) which allows you to validate the status of a certificate online and check if it is revoked. The link to the LCR of Supplier of Certificates PROCERT, C.A. is as follows: S/MIME: http://www.procert.net.ve/ecc-crl/smime-ca.crl,; the link for the OCSP is as follows: S/MIME: http://ocspsmime.procert.net.ve/ocsp

4.9.7. CRL emission frequency.

PROCERT Certificate Provider, C.A. in compliance with the international standard X.509, IETF RFC and RFC 6484 establishes within its RPKI a periodic scheme for the publication of the LCR of the PROCERT Certificate Provider CA, C.A. The publication of the LCRs runs every twenty-four (24) hours and is available to the general public through the links: S/MIME: http://www.procert.net.ve/ecc-crl/smime-ca.crl.

4.9.8. Maximum latency for CRL.

PROCERT Certificate Provider, C.A. in compliance with the international standard X.509, IETF RFC and RFC 6484 establishes within its RPKI a latency period in the publication of the LCR of fifteen (15) minutes after being generated and until they are placed in the repository.

4.10. Certificate Status Services.

PROCERT Certificate Provider, C.A. in compliance with the international standard X.509, IETF RFC and RFC 6484 establishes within its RPKI a method of checking the status of the online certificate called Online Certify Status Protocol (OCSP) which allows validating in real time the status of the electronic certificates issued by the PROCERT Certificate Provider CA, C.A. The OCSP provides three answers to the queries that must be executed and that can be made through the link http://ocspsmime.procert.net.ve/ocsp. The answers generated by the OCSP regarding the status of the electronic certificates generated by the CA of Certificate Provider PROCERT, C.A. are as follows:

- Valid**:** The certificate is current and has not been revoked.
- Revoked**:** The certificate has been revoked and should not be relied upon.
- Unknown**:** The OCSP server has no information about the status of the certificate.

The OCSP consultation service within the RPKI of Certificate Provider PROCERT, C.A. is duly published and permanently available.

5. Facility, management, and operations controls.

5.1. Physical controls.

PROCERT Certificate Provider, C.A. provides its RPKI services based on a technological platform installed in data centers that have security, operation and controlled access mechanisms and controls that allow them to offer the Signatories or final entities using electronic certificates the necessary confidence in them. All the measures implemented for the RPKI of Certificate Provider PROCERT, C.A. are aimed at business continuity and disaster recovery, guaranteeing the logical and physical security of the equipment and personnel that make up the RPKI and deterrence against actions that intend to affect the expected performance of the RPKI.

5.1.1. Site location and construction.

Certificate Provider PROCERT, C.A. operates its RPKI from data centers that have TIER 3 and 4 categories, thus ensuring high standards of operation and performance that allow establishing the confidence of the Signatories in the proper functioning of the electronic certificates. The data

centers used by Certificate Provider PROCERT, C.A. are located within the Bolivarian Republic of Venezuela. The data center from which PROCERT, C.A. Certificate Provider operates. maintains the policies or instruments issued by solvent and recognized insurance companies, for the purpose of maintaining a backup in the event of a contingency that affects the physical integrity of the aforementioned administrative headquarters and can thus offer a guarantee of its operational continuity. PROCERT Certificate Provider, C.A. maintains an alternate center operation contract in the event of permanent damage that makes it impossible and restricts the regular operation of the data center. The AR operates from the administrative office of Proveedor de Certificados PROCERT, C.A. which is located in a different location from the data centers and in the city of Caracas, Bolivarian Republic of Venezuela.

5.1.2. Physical access.

PROCERT Certificate Provider, C.A. within its RPKI, it maintains both logical (certification application) and physical (equipment) access control measures, guaranteeing the integrity and security of the services provided. Access is restricted to persons who are not duly authorized operators of the RPKI Certificate Provider PROCERT, C.A. has implemented a physical access control system that has seven (7) layers of security, from the outside to the servers where the CA of Certificate Provider PROCERT, C.A. is installed. In addition to security procedures that restrict access only to authorized personnel with authorization to access each of the seven (7) layers of physical security and require access information (username and password) of the operating system of the equipment that make up the CA of Certificate Provider PROCERT, C. A. and the physical security mechanisms for the management of the CA. Physical access to the inside of the rack (opening) must be allowed only to PSC PROCERT personnel.

5.1.2. Electricity and air conditioning.

The data centers where Certificate Provider PROCERT, C. A. operates and its administrative headquarters where the AR operates have service facilities. The data centers have high redundancy in order to guarantee their operational continuity, and the management of the AR allows remote operation in case the administrative office of Proveedor de Certificados PROCERT, C. A. is compromised.

5.1.3. Exposure to water.

The data centers where Certificate Provider PROCERT, C. A. operates have support personnel in order to prevent any failure or event that affects the operation of the CA. The administrative headquarters where the AR operates has incident response personnel in order to attend any event. AR information is located in a secure and controlled environment within data centers. If for any reason the operation of the AR from the administrative headquarters is compromised, the AR may operate remotely via the web.

5.1.4. Fire prevention and protection.

The data centers where Certificate Provider PROCERT, C. A. operates have security, prevention and firefighting mechanisms in order to prevent any failure or event that affects the operation of the CA and guarantee

operational continuity. The administrative headquarters where the AR operates has fire prevention, detection and fighting mechanisms that are regularly maintained in order to attend any event. AR information is located in a secure and controlled environment within data centers. If for any reason the operation of the AR from the administrative headquarters is compromised, the AR may operate remotely via the web.

5.1.5. Media storage.

The data centers where Certificate Provider PROCERT, C. A. operates have security, prevention and firefighting mechanisms in order to prevent any failure or event that affects the operation of the CA and guarantee operational continuity. The administrative headquarters where the AR operates has fire prevention, detection and fighting mechanisms that are regularly maintained in order to attend any event. AR information is located in a secure and controlled environment within data centers. If for any reason the operation of the AR from the administrative headquarters is compromised, the AR may operate remotely via the web.

5.1.6. Waste disposal.

Certificate Provider PROCERT, C.A. has established processes and procedures for the secure disincorporation of hardware and software, documentation, and information. It maintains a classification scheme for physical and intangible assets to properly manage its divestiture process without affecting in any way the operational continuity of the RPKI of Proveedor de Certificados PROCERT, C. A.

5.1.7. External backup.

Certificate Provider PROCERT, C. A. maintains a management and backup scheme for information in order to guarantee at all times operational continuity and recovery in the event of any disaster that may compromise the operation of the RPPKI of Certificate Provider PROCERT, C. A. Backups are stored securely in systems specially designed for them in order to be able to have access to and handling of the backed up data at all times and if required. The handling of the access keys to such information is handled securely and for the purpose of preventing data leaks or data extraction by unauthorized personnel of Proveedor de Certificados PROCERT, C. A.

5.2. Procedural controls.

PROCERT Certificate Provider, C. A. proceeds to establish the procedures, controls and resources that it manages in order to maintain its RPKI and to be able to issue electronic certificates in a compliant manner for the Signatories or final entities using electronic certificates.

5.2.1. Trusted roles.

Certificate Provider PROCERT, C. A. maintains an internal operational scheme that establishes roles and functions within the RPKI, assigning certain activities and reserving to trusted personnel the execution of functions that require high training and confidence and that applies to the maintenance and operation activities of the CA and RA of PROCERT Certificate Provider, C. A. All staff maintain contractual obligations of

confidentiality of information and job descriptions that establish and delimit their responsibilities. Prior training is required for permanence within the RPKI of PROCERT Certificate Provider, C. A. and regular mechanisms for testing and reviewing compliance with roles and functions are established, which are segregated and established in such a way that they require concurrent operation involving the staff and senior management of PROCERT Certificate Provider. C. A. in the operation and management of the CA and RA of Proveedor de Certificados PROCERT, C. A.

5.2.2. Number of people needed per task.

Certificate Provider PROCERT, C.A. maintains an internal operational scheme that establishes roles and functions within the RPKI, which are segregated and established in such a way that they require the concurrent operation that involves the staff and senior management of Certificate Provider PROCERT, C.A. in the operation and management of the CA and RA of Certificate Provider PROCERT, C. A. For the administration of the CA there are two administrators who validate and authorize the issuance of the keys, for the operation of the AR there are two administrators in charge of validating the identity of the Signatories or final entities using electronic certificates, for the regular operation of the CA there is a body of operators duly qualified for the task and an auditor in charge of verifying compliance with the internal procedures and methods within the PROCERT Certificate Provider, C. A.

5.2.3. Identification and authentication of each role.

Certificate Provider PROCERT, C. A. maintains an internal security scheme with policies that contemplate the periodic review of authentication mechanisms, in order to update and recurrently improve logical access keys. All access to the CA, RA and the administrative and management systems of Certificate Provider PROCERT, C.A., is controlled and verified with secure verification mechanisms that include biometrics, temporary codes and robust access keys, all depending on the level of criticality and confidentiality of the information.

5.2.4. Functions that require separation of duties.

Certificate Provider PROCERT, C. A. has an internal policy of segregation of roles, functions and job descriptions within the CA and AR, which allows establishing the required and necessary differentiations to prevent operational risks, handling of the Signatories' passwords or the information provided by them; all of them to prevent a person from assuming multiple functions within the RPKI, which can translate into risk and therefore loss of confidence in Proveedor de Certificados PROCERT, C. A. By job description, those in charge of the CA may not assume other functions not indicated in their job description; as well as those of the RA, the compliance officer and the systems auditor.

5.3. Personnel controls.

5.3.1. Qualifications, experience and authorisation requirements.

Certificate Provider PROCERT, C. A. has a personnel recruitment and selection policy that establishes the process of entry of qualified personnel for each task of the CA and the RA. Once the personnel have joined, the

personnel training and training policy is applied, in order to ensure that each new employee knows the operation of the CA or AR that has been assigned to him. Only after satisfactorily and proven passing the evaluations of its functional capabilities, is when it is assigned a role within the CA and AR of PROCERT Certificate Provider, C. A. By proceeding in this way, Provider of Certificates PROCERT, C. A. ensures that its personnel manage in an expected way the functions, roles and professional competencies assigned to their charge, increasing the level of trust of the Signatories. An active supervision scheme is maintained and there are automated mechanisms such as the SOC and NOC that allow the immediate establishment of the occurrence of an event derived from some non-observance or non-compliance with the roles and functions of the RPKI workers of the PROCERT Certificate Provider, C. A.

5.3.2. Background check procedures.

Certificate Provider PROCERT, C. A. has a recruitment and selection policy that establishes the process of verification of identity of candidates, validation of identity documents, personal references and compliance with the know-your-employee policy. Within the Bolivarian Republic, it is unconstitutional to carry out criminal background checks for the purposes of job selection.

5.3.3. Training requirements.

Certificate Provider PROCERT, C. A. has a personnel recruitment and selection policy, together with a job description policy, which allow a preliminary validation of the competencies and capabilities of the personnel to be hired. In addition, internal tasks are periodically carried out to train personnel in the tasks to which they are assigned within the regular operation of the CA and AR of Certificate Provider PROCERT, C. A. and in order to guarantee an expected response in case of disaster recovery, conformal validation of the Signatories and the secure management of the keys. Among the strengths and training granted to the staff of the Certificate Provider PROCERT, C. A. are the management of basic, intermediate and advanced knowledge of RPKI operation, information security, disaster recovery, compliance with the guidelines of the CA Browser Forum, international standards and legislation of the Bolivarian Republic of Venezuela, procedures for verification of documentation and validation of entities and people in order to comply the requirements of the RA.

5.3.4. Frequency and retraining requirements.

Certificate Provider PROCERT, C. A. has a personnel training and development policy that includes the planning of the competencies required by the different positions within the RPKI to perform their positions in compliance with the best practices and national and international standards in RPKI operation, information security, disaster recovery, compliance with the guidelines of the CA Browser Forum, international standards and legislation of the Bolivarian Republic of Venezuela, procedures for verification of documentation and validation of entities and persons in order to comply with the requirements of the RA.

5.3.5. Frequency and sequence of job rotation.
Job rotation is not contemplated; there is a job description associated with each position.

5.3.6. Penalties for unauthorized actions.
Supplier of PROCERT, C.A. Certificates, in its employment contracts and in its internal policy documents, establish the corrective measures for non-compliance or omission of the obligations imposed by the employment relationship with Supplier of Certificates PROCERT, C. A.; establishing the preventive and punitive measures that contemplate disincorporation from the job and the execution of measures that may be of an administrative, civil and/or criminal nature. The same provisions apply to service providers and suppliers that fail to comply with the policies of the PROCERT, C.A. Certificate Provider.

5.3.7. Independent Contractor Requirements.
Certificate Provider PROCERT, C. A. has a policy of selection and contracting of suppliers of goods and services that establishes that in the areas that involve the contracting of goods and services for the RPKI, the goods or services must comply with the international standard established by the CA Browser Forum, the rules dictated by SUSCERTE and the legislation that regulates the matter within the Bolivarian Republic of Venezuela. The model contract of Certificate Provider PROCERT, C. A. includes a clause that establishes the provision for the declaration of an independent contractor and one of confidentiality of information. Likewise, said contract establishes that non-compliance with the contractual rules and regulations of Certificate Provider PROCERT, C. A., may lead to the imposition of administrative, civil and/or criminal sanctions.

5.3.8. Documentation provided to staff.
Certificate Provider PROCERT, C. A. has a policy of Roles and Functions and Information Security that establishes that RPKI personnel that include CA and AR operators, will only have access to the information and documentation required for the performance of their position and the job description established by PROCERT Certificate Provider. C. A. and in order to guarantee compliance with the international standard established by the CA Browser Forum, the rules issued by SUSCERTE and the legislation that regulates the matter within the Bolivarian Republic of Venezuela. Non-compliance by the personnel of Provider of Certificates PROCERT, C. A. may generate the application of sanctioning measures that may be of an administrative, civil, labor and/or criminal nature.

5.4. Audit Trail Procedures.
Certificate Provider PROCERT, C.A., configures and maintains a record of the audit events of the RPKI platform, establishing a backup and protection scheme for the RPKI audit logs, which include the CA and AR. Electronic event audit logs are records that allow the traceability of the activities and operations executed within the RPKI platform of Proveedor de Certificados PROCERT, C. A. These records are stored automatically and electronically.

5.4.1. Types of events logged.

The electronic event audit logs that must be maintained by each of the PROCERT, C.A. Certificate Provider SubCAs include the following RPKI events or activities:

- Events of the teams that make up the CA platform:
  - Operating system installation and configuration.
  - Installation and configuration of any application installed on the computer.
  - Certificate Authority Installation and Configuration.
  - Installation and configuration of the cryptographic module.
  - Access or attempts to access the computer.
  - Updates.
  - Backing up
  - Generation and management of CSF.
  - Maintenance and operation of the OCSP.
  - Generation of certificates.
  - Certificate lifecycle management.
  - Management of certificate templates and changes to them.
  - Certification Software Events:
    - User management.
    - Role management.
    - Certificate template management.
    - Access Control List (ACLs).
    - Certificate management (everything contemplated in the life cycle)
  - Events related to physical access:
    - Staff access to the data center.
    - Personnel access to equipment and systems.
  - Corrective Action Events:
    - Hardware errors.
    - Software errors.

Each event log includes data regarding the date and time it occurred, serial number, description of the event, and the system or person that originated it.

5.4.2. Record of treatment frequency.

Electronic event audit logs are performed anytime an operation is performed within the RPKI of Certificate Provider PROCERT, C.A., which includes CA and AR. Operations personnel notify their security administrator when a process or action causes a critical security event or discrepancy in accordance with PROCERT, C.A.'s internal policy regarding the handling of the SOC, NOC, and PROCERT Certificate Provider's comprehensive risk and information security plan. C. A.

Electronic event audit logs are maintained in your PROCERT, C.A. Certificate Provider SubCA. The review of the electronic event audit logs (logs) is notified by the operations personnel who detect the situation in the SOC, NOC or the logs generated by the RPKI platform, escalating the case to their supervisors, in order to activate the necessary mechanisms in case of a security event or failure in any of the components of the RPKI. In any

case, the process of event registration and corresponding operational control that involves the Information Security Committee must be complied with, which will establish the steps to be followed.

5.4.3. Retention period for the audit log.
Electronic event audit logs are retained for a period of ten (10) years.

5.4.4. Audit trail protection.
Electronic event audit logs are centralized by a service that collects and signs them electronically in order to guarantee their integrity and prevent their manipulation. The system is maintained by means of access control mechanisms and separation of roles in relation to the software and hardware that handle the automatic collection and by means of confidentially documented operational procedures, known and followed by the personnel of Proveedor de Certificados PROCERT, C. A.

5.4.4. Audit trail protection.
Electronic event audit logs are centralized and are extracted in an automated way from the equipment, segregating the equipment or service from where they are generated; being electronically signed to prevent their manipulation or alteration. Electronic event audit logs are stored securely and have an access control policy that restricts and prevents unauthorized access, modification, replacement, or destruction. For the logs of the time stamping service, the log that shows the time token assignments is made available to users in order to make the validation process of the service expeditious and simple.

5.4.5. Audit log backup procedures.
These electronic event audit logs allow you to audit and verify harmful access attempts, accesses, and operations, whether intentional or unintentional. Electronic event audit logs are also stored in a cloud backup at a secure site other than the main data center. The backups of the electronic audit records of events (logs), periodic backups are scheduled for security costs under a daily, weekly and monthly incremental scheme, which allows to have the information required in the event of a disaster recovery event.

5.4.6. Audit Collection System (Internal vs. External).
Electronic event audit logs are centralized by a service of PROCERT, C.A. Certificate Provider. that collects and signs them electronically in order to guarantee their integrity and prevent their manipulation; the collection of logs is automated and from the beginning of operation of the equipment or services; these records are stored securely and confidentially. There is a system for monitoring the operation of the electronic audit records of events (logs) system, which sends alert messages to the SOC, regarding failures in the operation of the log logging system, activating remediation activities aimed at the restoration of said service and the proper recording of all RPKI logs.

5.4.7. Notification to the subject causing the event [OMITTED].
Under the legislation in force within the Bolivarian Republic of Venezuela, any subject who by action or omission causes damage or affects a

computer system will be responsible for the fact. Provider of Certificates PROCERT, C. A. reserves the right to take action against any Signatory or employee or contractor of Provider of PROCERT, C. A. Certificates who, through the registration of Logs, evidences his responsibility or action of damage or sabotage of any nature against the RPKI of Provider of Certificates PROCERT, C. A.

5.4.8. Vulnerability assessments.

Certificate Provider PROCERT, C. A., in order to comply with the provisions of the CAB Browser Forum, the Webtrust and SUSCERTE, maintains an annual audit scheme of compliance with the requirements imposed to apply for certification as a recognized entity and provider of certification services within the Bolivarian Republic of Venezuela. In addition to the foregoing and in accordance with the Information Security Policy of Certificate Provider PROCERT, C.A., periodic compliance audits are carried out in order to verify and verify full compliance by the personnel, managers and contractors of Provider of Certificates PROCERT, C.A., with all PKI information security, confidentiality and maintenance standards applicable to a CA. Among the activities contemplated are the security of the systems, the integrity of the certificate generation process, vulnerability analysis of the RPKI; These analyses are carried out by trusted personnel duly trained and authorized to do so.

5.5. Records file [REDACTED].

Certificate Provider PROCERT, C. A., within its information security policy and comprehensive risk and information security plan, contemplates the execution of electronic audit records of events (logs), their safekeeping, protection and storage in main and alternate centers, administration and management by the personnel of PROCERT Certificate Provider. C. A. The safeguarding of electronic event audit records (logs) is aimed at complying with the best international practices as provided by the CAB Browser Forum, the Webtrust and SUSCERTE. The records maintained by Certificate Provider PROCERT, C.A. are indicated in section 5.4.1. (Types of Events Recorded) of this CPS and the ten (10) year retention period.

5.6. Change of password.

Certificate Provider PROCERT, C. A., contemplates that the key change processes involving the S/MIME SubCA will be executed in compliance with the best international practices and the provisions of the CAB Browser Forum, the Webtrust and SUSCERTE. The new keys will be generated and safeguarded securely and the corresponding verification links corresponding to the LCR and OCSP of these new keys will be published. The keys that are replaced by a change of algorithm will remain in force until the certificates generated under the replaced algorithm are reissued. In the event of the expiration of the validity of the corresponding SubCA certificate, the new key pair will be issued for the period of time that fits the period contracted by the Signatory or end entity user of electronic certificates issued by the RPKI of PROCERT Certificate Provider, C. A.

5.7. Disaster engagement and recovery.

Certificate Provider PROCERT, C. A., has implemented a business continuity and disaster recovery plan. Under a scenario that establishes an eventual partial or total commitment of the RPKI that affects the CA or RA. The disaster recovery plan is reviewed every six months in light of changes in environmental risks and in order to keep it up to date. The disaster recovery plan includes the following points:

- Failures/corruption of computing resources.
- Commitment to Key Integrity; and
- Natural disasters and termination.

The business continuity and disaster recovery (PRD) plan specifies the procedure to be carried out in each of the scenarios considered as a disaster and is executed by the staff of Proveedor de Certificados PROCERT, C. A. The total or partial commitment of the RPKI is notified to the Signatories, final entities using electronic certificates and SUSCERTE. The personnel of Proveedor de Certificados PROCERT, C. A., must take the corrective measures and undertake the necessary activities to restore the RPKI at the time of a disaster scenario in order to restore its operation in the shortest term and maintain confidence in the RPKI.

5.7.1. Alteration of resources, hardware, software and/or data.

Certificate Provider PROCERT, C. A., contemplates the periodic review of its systems, software and other elements that constitute its RPKI platform, if the periodic reviews and evaluations determine the compromise of one or more of the computer resources; the partial or total commitment will be declared immediately and the certificates involved or the services of the Certificate Provider PROCERT, C. A., that are affected, will be revoked, duly notifying the Signatories or the final entities using electronic certificates. Once the points that generated the partial or total impact have been corrected and the RPKI duly restored, new passwords will be provided to the Signatories and the services that have been interrupted will continue to be provided.

5.7.2. Procedure for action in the event of vulnerability of an authority's private key.

Provider of Certificates PROCERT, C. A., declares that in the eventuality of the compromise of its private key of one of its SubCAs, that it will be detected, evaluated and established by the staff of Provider of PROCERT Certificates, C. A, the following procedure shall be followed:

- Disaster scenario declaration.
- Notification to SUSCERTE of the compromise of the key, for the immediate revocation of the certificate of Supplier of PROCERT Certificates, C. A.
- Publication of the event on the Website of Provider of Certificates PROCERT, C. A.
- Notification to Signatories.

- Notify the insurance company that it maintains the operating bond of Proveedor de Certificados PROCERT, C. A.
- Analyze the reason for the compromise and prepare a technical report detailing the reasons why the private key of Proveedor de Certificados PROCERT, C. A. was compromised.
- Agree together with SUSCERTE on the actions to be taken for the re-activation of the certificate issuance service.

5.7.3. Facility security following a natural or other disaster.

Certificate Provider PROCERT, C. A., has implemented a business continuity and disaster recovery plan. Under this plan, two data center facilities are maintained that are sufficiently differentiated and separated territorially and geographically in order to guarantee that in the event of a catastrophic event or disaster that compromises the operation of a data center, there is an alternate one to continue providing RPKI services. PROCERT Certificate Provider, C. A.

5.8. Rescission of CA or RA.

Certificate Provider PROCERT, C. A., has contemplated that the assumptions for a cessation of operations to occur are the following cases:

- Termination due to expiration of accreditation.
- Termination due to cessation of operations.
- Termination due to revocation of accreditation. In this case, and only for proven reasons of non-compliance, the guarantee requested by SUSCERTE at the time of accreditation will be enforced.
- Extinction is derived from technological aspects.

In the event of the occurrence of any of the aforementioned assumptions, Certificate Provider PROCERT, C. A., will be obliged to make available to SUSCERTE the repository of all the certificates issued during its management, including the status of each of them. Certificate Provider PROCERT, C.A., will also proceed with the Signatories as follows:

- Notify the Signatories of the termination and termination date by email, thirty days prior to the termination date.
- Inform the Signatories which entity assumes the operation or the RPKI.
- In the event that no entity assumes the PKI, provide access to SUSCERTE to keep the publishers of the LCR and OCSP active until the expiration of the certificates that have been issued by Proveedor de Certificados PROCERT, C. A.

6. Technical safety controls.

This section describes the security controls used by Certificate Provider PROCERT, C. A., for the management, management and generation of cryptographic keys.

6.1. Generation and installation of key pairs.

6.1.1. Key pair generation.

Certificate Provider PROCERT, C.A., generates the key pair (public and private) of your SubCA S/MIME using a FIPS 140-2 Level 3 compliant

cryptographic hardware device (HSM). The generation of the key pair of each SubCA of the PROCERT C.A. Certificate Provider is configured to be segregated into several trusted persons within the PROCERT, C.A. Certificate Provider and following the international standard of security in the operation of the CA. The concurrent participation of the persons who administer the CA is required to carry out operations within the CA that go beyond simple administration. All functions and roles are described in the CA Operating Model and Manual document. The generation of the key pair of the SubCAs of the Certificate Provider PROCERT, C.A., are executed in compliance with the pressures of the CA Browser Forum and the standards imposed by SUSCERTE. The CA is configured in such a way as to leave a log in Logs of the people and activities that have interacted or have been executed within the CA.

SubCA S/MIME Signatories must generate their cryptographic key pair online in order for their certificate application to be processed and approved. Certificate Provider PROCERT, C.A., does not generate the Signatory key pair. The requests generated by the Signatories are made through the AR System, having to enter their usernames and passwords to access, then the Signatory must upload all their information and be validated by the RA; once validated by the AR, the AR operator approves within the AR System. Once the Signatory has been approved by the AR, the system sends a message to access the AR System and generate its certificate request through the AR System. Once the request is generated, it is notified by mail to the AR and the AC operator, so that they can proceed to approve the Signatory's request against the HSM device. being properly stored. Once the key pair has been approved, the Signatory must log in with their username and password within the AR System and select to download the certificate; then the system will send an OTP to the user's phone and the user must enter the security pin to be able to access the certificate download. To download, the system will require the user to enter a security key to access their certificate. In S/MIME certificates generated by the PROCERT Certificate Provider, C.A. CA, the id-kp-emailProtection value must be present and the id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage values must not be present.

By virtue of the above, if the client loses his private key, a new certificate must be issued and he must comply again with the contracting process of Proveedor de Certificados PROCERT, C. A. The public key will always be in the repository, in accordance with the provisions of this CPS.

6.1.2. Delivery of private key to the subscriber.

The process for delivering the key pair generated by the PROCERT, C.A. Certificate Provider CA in the S/MIME SubCA is described below and for the purposes of the Signatory taking the necessary precautions to ensure the protection of the private key:

- The end user must enter the website of Certificate Provider PROCERT, C. A., (http://www.procert.net.ve) click on the AR SYSTEM button (procert.net.ve/sistemaAR/login.aspx) and thus enter the web service.

- There you must verify that the data contained is correct**,** said application is composed of four (04) parts:

    - User Information: This section contains the name and surname of the user that was provided to Proveedor de Certificados PRO-CERT, C. A.
    - Subject: General user information that, depending on the type of certificate, some fields will be mandatory, then the fields are listed and which are mandatory by certificates
    - Alternative name information: This section must contain the RIF or C.I. number of the signatory.
    - Key options: In this section, the Cryptographic Service Provider (CSP) must be chosen, then the user must accept the terms and conditions to enable the generate button. After pressing the generate button, the user will have the option to protect their private key with a high level of security using a password.

- Next, the HR reviews and evaluates the Signatory's application and, if it is satisfied, proceeds to approve it. Once the Signatory's request is approved, it goes to the approval of the CA and that is when the key pair generation button is activated for the CA operator, who against the HSM proceeds to approve the Signatory's request.

- After the approval of the application by the CA, a link will be sent to the user's email, through which the Signatory will be able to download the certificate. The aforementioned key pair generation procedure guarantees the privacy of the user's private key, since the user is the one who generates it, Certificate Provider PROCERT, C. A., only guarantees the link of the individual with the public key, said public key is in turn associated with the private key.

6.1.3. Delivery of the public key to the certificate issuer.

The CA of the Certificate Provider PROCERT, C. A., at the time of receiving the CSR generated by the Signatory, proceeds to sign and generate the pair of cryptographic keys that form the certificate. The public key is kept within the certificate and is stored automatically by the CA in its repository of issued certificates.

6.1.4. Delivery of CA public keys to trusted users.

Certificate Provider PROCERT, C. A., is obliged to keep its public key in its repository and available, which any client or interested party can access through the PROCERT website (https://www.procert.net.ve/Consulta-Publica/index.aspx).

6.1.5. Key sizes.

The Certificate Authority (CA) Certification Root modules and keys are at least 4096 bits long and use the RSA algorithm and at least 256 bits in the case of the ECC Elliptic Curve Algorithm (ECDSA).

6.1.6. Generation of public key parameters and quality control.

The parameters used for the generation of the public keys comply with FIPS 140-2 Level 3 requirements. The generation of the key pair (public and private) used by the certification platform of Certificate Provider PROCERT, C.A., is a simple process, but it requires special precautions and is generated with an HSM computer.

6.1.7. Key usage purposes (based on the X.509 v3 key usage field).

Certificate Provider PROCERT, C.A., generates its electronic certificates under the international standard X.509v3 and includes key usage extension fields that specify the intended use of the electronic certificate as established in the CP. Uses other than those declared in the COP are not permitted. Additionally, and as it is subordinated to the Certification Root of the Venezuelan State, Certificate Provider PROCERT, C. A., the issuance of certificates for Signatories users of electronic certificates through a SubCA identified as S/MIME is contemplated. The following are the limitations applied to the certificates generated by the SubCAs indicated above, which are as follows:

- Issuance limitations for S/MIME end entity certificates:
  - The id-kp-emailProtection value must be present.
  - The values id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage should not be present.

The class usage of the PROCERT, C.A. Certificate Provider SubCA varies depending on the use assigned to the certificate and which is contemplated and described in detail in the CP. The uses assigned to the keys of the SubCAs of the Certificate Provider PROCERT, C. A. are listed below:

- Signing Certificates to S/MIME SubCAs.
- Signing of certificates established in the CP.
- Signing the Certificate Required for the OSCP Service
- Signing the list of revoked certificates.
- Signing of certificates required for the operation of the RPKI and other services of Certificate Provider PROCERT, C. A.

6.2. Private key protection and cryptographic module engineering.

6.2.1. Standards and controls of cryptographic modules.

The cryptographic module used by the RPKI of Certificate Provider PROCERT, C.A., is certified to meet the requirements of FIPS 140-2 Level 3, Common Criteria EAL 4+ or equivalent. In the case of the PROCERT certification root, the PROCERT certification module is kept offline.

6.2.2. Private key (n of m) Multi-person control.

The Private Keys of the SubCAs of the Certificate Provider PROCERT, C.A., are under multi-person control. These are triggered by initializing the CA software through a combination of CA operators, HSM Administrators, and operating system users. This is the only method of activating such keys. Access and control mechanisms are executed through tokens or smart cards and differentiated keys associated with certain roles within the administration of the RPKI CA

6.2.3. Private key custody.

The private key of the PROCERT Certificate Provider CA is protected by an HSM. The CA has established the steps to follow for the installation of the HSM, which are detailed below:

- Driver Installation: The drivers corresponding to the HSM must be installed on the CA server.
- Physical installation.
- Creation of the World of Security.
- Profiles and roles are created and assigned within the security world.
- The various roles within the CA and RPKI are configured with the tokens and cards.

6.2.4. Private Key Backup.

The backups of the private keys of the SubCAs that are generated in the HSM are stored securely, in a vault external to the operation site of the CA of Certificate Provider PROCERT, C. A. and require controlled access in order to be able to have such copies. For the restoration of the security world of the SubCAs, the concurrent participation of trusted persons of Certificate Provider PROCERT, C. A. is necessary, without which the backups cannot be used. The Signatories of the SubCA S/MIME generate their own private keys that are managed through the CA but are stored in the repositories of the Signatories.

6.2.5. Private Key File.

Certificate Provider PROCERT, C. A., establishes that upon expiration of the clairvoyance of the certificates of the SubCA S/MIME, it is filed in the vault for a period of ten (10) years in accordance with the obligations imposed by the SUSCERTE.

6.2.6. Private key transfer to or from a cryptographic module.

Certificate Provider PROCERT, C. A., establishes as a rule that all keys must be generated through an HSM that must have the proper configuration of roles and segmentation of functions in order to establish a multi-person authorization scheme, For the purposes of their backup, the private keys can be exported and encrypted to store them in a secure device in a vault located in a different place to the RPKI operation site but accessible in case of activating a disaster recovery process. The compromise of the private key generates its immediate revocation and activation of the disaster recovery protocols.

6.2.7. Storage of private keys in the cryptographic module.

Certificate Provider PROCERT, C. A., has established the parameters and guidelines under which the generation of the S/MIME SubCA keys will be carried out in order to guarantee their integrity and comply with the guidelines of the CA Browser Forum and SUSCERTE. These guidelines and parameters are detailed below:

- A world of security will be generated for each SubCA.

- The certificate authority will be installed under the Subordinate modality and the certificate request for each SubCA will be generated from the HSM.
- SUSCERTE will sign the application for the certificate of each SubCA.
- Each SubCA's certificate will be installed and activated in the HSM.

The PROCERT C.A. Certificate Provider HSM complies with the FIPS 140-2 Level 3 standard. All root private keys in the PROCERT Certificate Provider, C.A. SubCAs are stored offline.

6.2.8. Private Key Activation Method.

For the activation of the private keys, it is necessary to use the distribution of security tokens that were created when creating the security world and the management of the RPKI and the smart cards assigned to each of the roles, in the distribution of concurrent or necessary roles for each activity, additionally, it is necessary to access the operating system of the certification server and the data center where the AC.

Signatories of Certificate Provider PROCERT, C.A., must comply with the instructions for use and download of the electronic certificate, which indicate the obligation of the Signatory to assign a key of use for its certificate. The Signatories are solely responsible for safeguarding the security of their private key, any compromise of the private key must generate the revocation of the certificate through the self-management of the Signatory through the AR System or the due notification of the key commitment to Certificate Provider PROCERT, C. A., through the email soporte@procert.net.ve.

6.2.9. Private key deactivation method.

The HSM of the PROCERT, C.A. Certificate Provider has the attributes so that through commands assigned to shared HSM management roles it is possible to temporarily deactivate the private keys of each or all of the PROCERT, C.A. Certificate Provider SubCAs. However, the SubCas of the Certificate Provider PROCERT, C.A., remain active but managed through a participation of tokens and cards with predefined management roles and that require concurrent activity of trusted personnel. The final certificates of Signatories cannot be suspended by them; it is only possible to suspend users of the AR System through the intervention of the AR and CA personnel and by duly justified and supported action. Certificates only accept revocation as a method of termination or restriction of use.

6.2.10. Method of destruction of the private key.

The HSM of the PROCERT, C.A. Certificate Provider has the attributes so that through commands assigned to shared HSM management roles, it is possible to revoke or destroy the private keys of each or all of the SubCAs of the PROCERT, C.A. Certificate Provider. Private keys corresponding to certificates that have completed their lifecycle or have been revoked can be deleted from the HSM's secure repository. The final certificates of Signatories can be revoked and the private key deleted from the repository where they are stored; this action can be executed directly

by the Signatory through the AR System or through the intervention of the staff of the AR and CA, by duly justified and supported action. The elimination of the private key of each of the SubCAs also includes those that have been backed by security and business continuity issues, once the validity time of the corresponding certificate has been revoked or expired.

6.2.11. Classification of the cryptographic module.

The HSM of Certificate Provider PROCERT, C.A., is a hardware device composed of a cryptographic module that is used to securely store the private key of each of the SubCAs. This cryptographic module, or HSM brand Gemalto and Luna K6 Base model, has FIPS 140-2 certification up to level 3. These devices are within the category of high security hardware, which are used by banking and state security entities around the world, enjoying experience and proven security.

6.3. Other aspects of key pair management.

6.3.1. Public key file.

The public keys of the SubCAs of the Certificate Provider PROCERT, C.A., are archived in PKCS#7 format, for a period of 10 years. The public key file is executed as described in point 5.5. of this CPS.

6.3.2. Periods of operation of the certificate and periods of use of the key pair.

The certificates of the SubCa of Certificate Provider PROCERT, C.A., will be valid for 10 years. The signatures and electronic certificates generated by each of the Sub-CAs of the Certificate Provider PROCERT, C.A., have a cycle of one (1) year from the date of activation of the electronic certificate by the CA of the Certificate Provider PROCERT, C.A. The key pair associated with each electronic certificate also has the same period of validity as the certificate in question.

6.4. Activation data.

6.4.1. Generation and installation of activation data.

The generation of the key pair (public and private) used by the SubCAs and served by the RPKI of the PROCERT, C.A. Certificate Provider is a simple process, but it requires special precautions. The following are the steps to follow for the generation of the key pair and what precautions must be taken to ensure that the private key is protected:

The validation of the individual's identity is carried out by the RA which, once the Signatory has been created, registered and validated within the AR System, sends the CA the necessary information for the creation of the Signatory's key pair and thus guarantee the linking of the person's identity with his or her key pair. The Signatory must enter the PROCERT website (http://www.procert.net.ve), within the AR System (procert.net.ve/sistemaAR/login.aspx) and click on the request generation link. The system will indicate that you generated your request correctly. The same AR System informs the AR and CA operator about the existence of the request, which once validated is approved by an AC manager. The approval is informed via email to the Signatory, who must enter the AR System in order to download their electronic certificate.

The signatory, when pressing the Generate button, creates a request against the CA and generates its key pair (public and private), that request is automatically sent to the RA registry so that the identity of the Signatory who is making the certificate request is validated.

The aforementioned key pair generation procedure guarantees the privacy of the user's private key, since the user is the one who generates it, Certificate Provider PROCERT, C. A. only guarantees the link of the individual with the public key, said public key is in turn associated with the private key.

Once the identity has been validated by the AR and the certificate generated by the CA, the Signatory proceeds to download their electronic certificate in the repository of their computer, accepting the source of issuance of the certificate and assigning a key of use as a requirement within the terms and conditions of use.

6.4.2. Activation data protection.
The activation of the certificates issued by the SubCAs of the Certificate Provider PROCERT, C.A. is executed using the RPKI and limited to the computer or device where the request for the electronic certificate by the Signatory has been generated.

6.4.3. Other aspects of activation data.
None.

6.5. Computer security controls.
Certificate Provider PROCERT, C. A. has an Information Security Policy and a Manual and Operation Model of the CA and AR, which establish and contemplate the execution of a series of processes aimed at establishing a scheme for the prevention, protection and safeguarding of the information and computer assets of the RPKI that includes the CA and the AR. Among the activities included in the Information Security Policy are those described below:

- Creation of a Security and Risk Committee that establishes information security management as a fundamental part of the objectives and activities of Proveedor de Certificados PROCERT, C. A.
- It delimits and establishes how the Formation of the Safety and Risk Committee, in order to fulfill its objective and the due segregation of roles and functions.
- It establishes the parameters and principles that contemplate the contracting of external resources that offerspecialized counseling.
- Classifies and assigns control in the management of physical and intangible assets.
- It establishes the principles applicable to the management andsafety of human resource management.
- It establishes the principles applicable tophysical and environmental safety.
- It sets the criteria for access control.
- It establishes the applicable criteria for the establishment of passwords.
- Protection against malware and use of networks by Proveedor de

Certificados PROCERT, C. A.

- File sharing and information management of Certificate Provider PROCERT, C. A.
- Established use for theinternal and external electronic processing of Proveedor de Certificados PROCERT, C. A.
- Rules and protocols forInternet connection.
- Rules and protocols for software maintenance and updating.
- Establishment of rules applicable toperimeter security.
- Establishment of guidelines for access to the systems and management of the AC and RA.
- Regulation of the use ofmobile computing and remote work.
- Rules for acceptable useand team assignment.
- Rules and procedures forthe control of change in the RPKI including the CA and the RA.
- Rules and procedures for maintaining and updating the RPKI software and that it is differentiated and separated into AC and RA.
- Rules and protocols for the registration, management and safeguarding of event logs.
- Rules, procedures and responsibilities in the management and managementof incidents.
- Setting the due Role synchronization.
- Establishment of the rules and processes that must be complied with for Outsourcing and its contracting.
- Establishment of preventive control mechanisms for the proper maintenanceof hardware and software.
- Establishment of the principles and rules for the acquisition, development and/or maintenance of information systems and hardware.
- Rules, protocols, functions and roles in risk management.
- Rules, protocols, functions and roles in the managementof business continuity.
- Rules and functions for the prevention of malicious code, spyware and malware.

6.6. Technical controls of the life cycle.

6.6.1. System development controls.

Certificate Provider PROCERT, C. A. has a Software Development policy, which establishes and contemplates the processes that must be complied with for the development, maintenance and testing of the CA and RA software that is created within Certificate Provider PROCERT, C. A. In the process of generating its own software, Certificate Provider PROCERT, C. A. manages the establishment of different software management and testing environments (development, quality and production) to guarantee the proper operation and compliance of the software with the international standards established by the CA Browser Forum and SUSCERTE for the management of an RPKI including the CA and RA of PROCERT Certificate Provider, C. A., and in the processes of putting software into operation and its updates, contemplating the following aspects:

- Establishment of the development model.

- Characterization of the development model and rules applicable to them.
- Requirements for the in-house developer or consultant hired.
- Establishment of the activities to be executed by the developer.
- Conditions of the development environment.
- Establishment of the conditions and requirements for approval of versions and certifications of the software.

6.6.2. Security management controls.

Certificate Provider PROCERT, C. A. has a Manual and Operation Model of the AC and a Manual and Operation Model of the AR, which establish the security processes applicable to the management and updating of the software that is used for the management of the CA and AR. The aforementioned manuals are aimed at ensuring that the operating systems and software that serve the CA and AR guarantee and maintain their expected use, integrity and security.

6.6.3. Lifecycle security controls.

Certificate Provider PROCERT, C. A. has an Information Security Policy and a CA Operation Manual and Model and an AR Operation Manual and Model, which establish and contemplate the execution of a series of processes aimed at the adjusted management of RPKI and CA and RA which are adjusted to the best practices and international guidelines within which are those established by the CA Browser Forum and SUSCERTE

6.7. Network security controls.

Certificate Provider PROCERT, C. A., in addition to the activities contemplated in section 6.5, establishes within its Information Security Policy, CA Operating Manual and Model and the AR Operating Manual and Model, the development of the following activities:

- Managing change controls for upgrades, modifications, or remediations within SubCA and RA systems and software.
- Proper segmentation and configuration of RPKI networks.
- SubCA certificates are securely maintained on HSM devices in secure data centers.
- Recurrent updating of passwords for access to the platform and establishment of access to the SubCA for its management and modification through tokens, smart cards and segmentation of roles that concurrently allow the execution of certain operations.
- Secure connection protection between SubCA and AR with certificate management software.
- SubCA certificates are securely maintained on HSM devices in secure data centers.
- Protecting connections to SubCA and RA using firewalls and network configurations.
- Application of the Information Security Policy regarding access to the CA, RA and networks and systems of Certificate Provider PROCERT, C. A. complying with the due segmentation of roles and functions of the staff and the Signatories.

- Proper configuration and maintenance of the validation mechanisms of electronic certificates, which are constituted by the LCR and the OCSP service.
- Periodic review of the connections and access to ports of the platform that constitute the RPKI.
- Review of the website of Certificate Provider PROCERT, C. A. in order to prevent and solve vulnerabilities.
- Due backup of the records and processes of the SubCA and the AR of Proveedor de Certificados PROCERT, C. A.
- Encryption of sensitive information and TLS/SSL connection between the different RPKI services.

6.8. Time stamping.
Certificate Provider PROCERT, C.A., has a SubCA that issues the certificate for the time stamping service. This SubCA is in the process of certification and at the time of issuance of this CPS it is not active to the public. Once the aforementioned SubCA has the due national and international accreditation, it will be included as an active service in a future edition of this CPS.

7. Certificate and CRL profiles.
Certificate Provider PROCERT, C.A., uses the ITU X.509 standard, version 3 to build digital certificates for use within its RPKI. Certificate Provider PROCERT, C.A., adds certain certificate extensions to the basic certificate structure for the purposes provided by X.509v3 under Amendment 1 of ISO/IEC 9594-8, 1995. Certificate Provider PROCERT, C.A., uses a number of certificate extensions for the purposes provided by X.509v3, according to Amendment 1 of ISO/IEC 9594-8, 1995. X.509v3 is an International Telecommunication Union standard for digital certificates.

7.1. Certificate profile.
The certificates of Certificate Provider PROCERT, C. A., are issued in accordance with the following standards:

- RFC 6818: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, January 2013
- ITU-T Recommendation X.509 (2016): Information Technology – Open System Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.3 (2006-01): Qualified Certificate Profile, 2006
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March2004 (TS 101 862 prevailing in case of conflict).

7.2. Certificate Extensions:
Certificate Provider extensions PROCERT, C.A., allow you to encode additional information into certificates. Standard X.509 extensions define the following fields: i) SubjectKeyIdentifier; ii) AuthorityKeyIdentifier; iii) BasicConstraints; iv) Certificate Policies; v) KeyUsage; vi) LCRDistribucionPoint; vii) SubjectAlternativeName; and (viii) AuthorityInformationAccess.

7.3. Object identification (OID) of algorithms.
The OID of the cryptographic algorithm used by Certificate Provider PROCERT, C. A., is: For P-384 keys, the namedCurve SHALL be secp384r1 (OID: 1.3.132.0.34).

7.4. Name formats.
Certificate Provider PROCERT, C.A., only generates and signs certificates with names according to the x500 standard. For PROCERT, C.A. Certificate Provider SubCAs: The distinctive name (DN) of the is made up of the following attributes:

SMIME subordinate.
- CN=PROCERT SMIME ECC CA
- O=PROCERT Certificate Provider
- C=VE

The alternative name (AN) of Certificate Provider PROCERT, C.A., is made up of the following attributes.

- DNSName: procert.net.ve.
- otherName:
- OID 2.16.862.2.1. (Accredited PSC PROCERT identification code)
- OID 2.16.862.2.2.: RIF J- 31635373-7

For Subscribers: The signatory's distinctive name (DN) is made up of the following attributes depending on the category:

SMIME Subscriber
Mailbox-validated.
- CN= infoprocert
- E= info@procert.net.ve

Organization-validated.
- CN= Matheu Dilon
- O= PROCERT Certificate Provider, C.A.
- OU= Operations
- OI= J316353737 or G200040360
- SERIALNUMBER= V22222222 or P1994455
- E= matheu.dilon@procert.net.net.ve
- ST= Av. Libertador, Multicentro Empresarial del Este
- L= Chacao
- S= Miranda
- POSTALCODE= 1060
- C= VE

Sponsor-validated.
- CN= Matheu Dilon
- O= PROCERT Certificate Provider, C.A.
- OU= Operations
- OI= J316353737 or G200040360
- G= Matheu
- SN= Dilon
- SERIALNUMBER= V22222222 or P1994455
- E= matheu.dilon@procert.net.net.ve
- T= Computer Engineer

- ST= Av. Libertador, Multicentro Empresarial del Este
- L= Chacao
- S= Miranda
- POSTALCODE= 1060
- C= VE

Individual-validated.
- CN= Matheu Dilon
- G= Matheu
- SN= Dilon
- SERIALNUMBER= V22222222 or P1994455
- E= matheudilon@gmail.com
- T= Computer Engineer
- ST= Calle Bolívar, Chacao, Caracas
- L= Caracas
- S= Miranda
- POSTALCODE= 1060
- C= VE

The signatory's alternative name (AN) is made up of the following attributes:

- otherName: OID 2.16.862.2.2.: (Identity Card or Passport Number)

7.4.1. Need for meaningful names.

Certificate Provider PROCERT, C. A., will require from the contracting clients of electronic signatures or certificates their full and conforming names and surnames represented in the laminated identity card that the applicant of the signature or electronic certificate has. Data corresponding to diminutives of names, aliases or pseudonyms with which the customer is intended to be identified will not be accepted or processed by the RA.

In the case of indigenous populations, the names that appear on their identity card or passport will be considered. In any case, Certificate Provider PROCERT, C. A., guarantees that the DNs contained in the fields of the certificates are sufficiently distinctive and significant to be able to link the identity of a customer to their signature or electronic certificate.

7.4.2. Interpretation of name formats.

The rules used for the interpretation of distinguished names in issued certificates are described in ISO/IEC 9595 (X.500) DintinguishName (DN). Additionally, all certificates issued by Certificate Provider PROCERT, C.A., use UTF8 encoding for all attributes, according to RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013.

7.4.3. Uniqueness of names.

The Certificate Authority of SUSCERTE defines the DN field of the authority certificate as unique and unambiguous. To this end, the name or company name of Certificate Provider PROCERT, C. A. will be included as part of the DN, specifically in the OU field, the uniqueness is guaranteed

by confidence in the uniqueness of the commercial names in the national registry.

In addition, and with respect to customers; If there is a customer who has a contract and has acquired more than one type of signature or electronic certificate, the database of Certificate Provider PROCERT, C. A., will maintain a uniform and egalitarian scheme of data of the contracting customer and dissimilar personal data that corresponds to the same customer will not be allowed or processed by the RA.

7.4.4. Resolution of conflicts related to names.

In the event of a name conflict between customers and that corresponds to the same name and surname, the RA will proceed to make the distinction of identity and authentication of the RA through the use of the identity card number and personal RIF of each customer of Certificate Provider PROCERT, C. A., with which the name conflict has been generated.

Certificate Provider PROCERT, C. A., will use the definition of the OID's assignment policy according to the private numbering tree assigned by the Superintendence of Electronic Certification Services (SUSCERTE).

7.5. LCR/OCSP Profile:

The revoked certificate list (LCR) is a list of electronic signatures and certificates, in which, specifically, the serial numbers of the electronic signatures or certificates revoked by a CA are shown, the serial numbers that have been revoked are no longer valid, and therefore the user should not trust any certificate included in the LCR of the system. An LCR is a file that contains:

- Name of the issuer of the LCR;
- Serial numbers of the signature or certificate;
- Date of revocation of signatures or certificates,
- The effective date and date of the next update, and
- The reason for the revocation. This list is electronically signed by the CA that issued it.

When a user wishes to check the validity of a certificate, he must download and install the updated LCR from the servers of the same CA that issued the electronic certificate, when doing this, the signatures or certificates that are installed on the computer where the LCR is installed, are automatically validated, if they are revoked, they are invalidated; the status of any other certificate can also be checked through the serial number located in the LCR.

The authenticity of the list is verified thanks to the electronic signature of the certificate authority.

The structure of the LCR of Certificate Provider PROCERT, C. A., has the following structure, depending on the category:

General

FIELD	VALUE
Version	V2

Issuer *Issuer*	CN= [CA Certificate Common Name] O= [CA Certificate Organization] C= [CA Certificate Country Name]
Valid from	Date (UTC)
Valid until	Date (UTC)
Signature Signature Algorithm	Sha384ECDSA
Signature hashing algorithm	sha384
EXTENSIONS	
Authority Key *Identifier (required*)	Key ID= 4882344ee6311103e6532c8123d14746b5ea946e
CSF Number CRLNumber	Integer numeric value

Revocation List.

- serialNumber
- revocationDate

If a reasonCode CRL input extension exists, the CRLReason must indicate the most appropriate reason for the certificate revocation, unless the reason is not specified. The CA Browser Forum TLS specifies the following reason codes from RFC 5280, Table 83, Section 7.2.2., as appropriate for most cases when used in accordance with the practices in this section and this CPS:

- Unspecified (0)
- keyCompromise (1)
- affiliationChanged (3)
- Superseded (4)
- cessationOfOperation (5)
- certificateHold (6)
- privilegeWithdrawn (9)

Certificate Provider PROCERT, C.A., states that the indicated CRLReason MUST NOT be unspecified (0). If there is a CRL reasonCode entry extension, CRLReason MUST indicate the most appropriate reason for certificate revocation, the certificate certification reasons are as follows:

For S/MIME certificates.

- keyCompromise: This reason is used when Certificate Provider PROCERT, C.A., has received reasonable evidence or suspicion of key compromise for revoked certificates.
- Compromise: This reason is used when Certificate Provider PROCERT, C.A., has received reasonable evidence or suspicion of key compromise from the Signatory.
- AffiliationChanged: This reason is used when the subject name or other subject identity information in the certificate has changed
- Superseded: This reason is used when the Subscriber has requested a replacement or Certificate Provider PROCERT, C.A., has obtained information

that the validated information is not reliable and does not comply after the electronic certificate is issued to the Signatory.

7.5.1. Version number(s).
The Certificate Provider OCSP Responder PROCERT, C.A., complies with RFC 6960 and 5019.

7.5.2. OCSP extensions.
Unique extensions of an OCSP response MUST NOT contain the reasonCode CRL input extension (OID 2.5.29.21). PSC PROCERT certificate extensions allow additional information to be encoded into certificates.

Standard X.509 extensions define the following fields: i) SubjectKeyIdentifier; ii) AuthorityKeyIdentifier; iii) BasicConstraints; iv) Certificate Policies; v) KeyUsage; vi) LCRDistribucionPoint; vii) SubjectAlternativeName; and (viii) AuthorityInformationAccess.

SMIME.
The singleExtensions of an OCSP response MUST NOT contain the reasonCode (OID 2.5.29.21)

8. Compliance auditing and other assessments.
Certificate Provider PROCERT, C. A. in compliance with international information security standards, the provisions of the CA Browser Forum and the standards of SUSCERTE has established a scheme of annual and periodic audits aimed at complying with the industry standards indicated above and satisfying the requirements of the WebTrust Program for an open CA.

8.1. Types of Audits and Evaluations.
Certificate Provider PROCERT, C. A. within its system and process audit scheme, maintains an annual schedule that includes the execution of national and international audits with an annual and quarterly regime; as well as other types of evaluations aimed at verifying and providing certainty of compliance with industry standards. These audits and their application scheme are indicated below:

Type of Activity	Coverage	Frequency
Webtrust	Verification of compliance with industry standards applicable to open CAs serving the general public.	Annual
Accreditation audit before SUSCERTE	Verification of compliance with the requirements established by SUSCERTE for the operation of a Certification Service Provider within the Bolivarian Republic of Venezuela.	Annual
Control and monitoring audit in information security and processes of the CA.	Audit aimed at verifying compliance with the control and assurance mechanisms of operation of a CA, in compliance with the industry standards applicable to open CAs that provide services to the general public and that are documented in the CPS and	Quarterly

	the policies of the PROCERT Certificate Provider, C. A.	
Control and monitoring audit in administrative processes and RA processes.	Audit aimed at verifying compliance with the control and assurance mechanisms of an RA, in compliance with industry standards and which are documented in the CPS and the policies of the PROCERT Certificate Provider, C. A.	Quarterly
Penetration test	Executed on the platform and website of Certificate Provider PROCERT, C. A. and aimed at detecting and determining the existence of vulnerabilities and applying remediation.	Annual

The audits contracted by Proveedor de Certificados PROCERT, C. A. are carried out by qualified independent auditors and with an obligation of confidentiality of the information. Likewise, the evaluation mechanisms are contracted with duly accredited and qualified technicians for the purpose of verifying compliance with the provisions of this CPS and guaranteeing the security of the information.

8.2. Audit and experts.

Certificate Provider PROCERT, C. A. within its operating scheme maintains a policy of contracting services that establishes the evaluation of the qualification and sufficiency of the personnel who will execute the audits and evaluations of the processes and systems of Certificate Provider PROCERT, C. A. In any event, and for the purposes of international audits, auditors must comply with the requirements of Section 8.2 of the CAB Forum Reference Requirements and Section 3.1 of the Mozilla Root Store Policy, where applicable. For the audit before SUSCERTE, auditors must have their auditor identification number accredited by SUSCERTE. For other evaluations, a selection process based on industry ratings and recommendations will be conducted for independent third-party audits. The auditors must sign a confidentiality contract and a service contract and it will be verified under oath that they do not have a direct financial or commercial interest in the results of the audit or have a family relationship with personnel or directors of Provider of Certificates PROCERT, C. A. in the second degree of consanguinity and fourth degree of affinity.

8.3. Scope of audits and assessments.

The scope of the audits and evaluations is aimed at compliance by Proveedor de Certificados PROCERT, C. A. of the provisions and obligations that a commercial CA must have under the principles of this CPS and the CA Browser Forum, the Webtrust, the ETSI standard and the information security standards that guide the expected operation of the RPKI and the compliance by the Certificate Provider PROCERT, C. A. with its commercial and legal obligations.

8.4. Audit and compliance reports.

Certificate Provider PROCERT, C.A. will manage the audit reports or evaluations in accordance with the audit or work plan established before each of the processes indicated in point 8.1. The remediation plan shall be prepared with an agreement between the auditor and the staff of Proveedor de Certificados PROCERT, C.A. and shall establish the points of review and improvement, which

shall be documented and submitted for the purpose of correction before the completion of the audit or within the period established by the auditor for that purpose. In the case of the Webtrust, the audit reports will be available to interested third parties through the link https://www.procert.net.ve/Internas/AC.aspx In the case of the SUSCERTE audit, the accreditation report is located in the security repositories of Certificate Provider PROCERT, C. A. In the case of security assessments, they will be treated in accordance with the provisions of the Information Security Policy of the Certificate Provider PROCERT, C. A.

9. Other business and legal matters.

This section is aimed at establishing the commercial and legal aspects of the operation of the Certificate Provider PROCERT, C. A. with its Signatories and final entities using electronic certificates issued by the SubCA of Certificate Provider PROCERT, C. A.

9.1. Rates.

The fees and charges associated with the provision of the services and issuance of the certificates of the Certificate Provider PROCERT, C. A. contemplate the total investment required by a Signatory or final entity using electronic certificates, for the acquisition of an electronic certificate or TSA service and its use according to standard for a period of one (1) year. The rates of the certificates and services of Provider of Certificates PROCERT, C. A. can be consulted through the following link: https://www.procert.net.ve/

Certificate Provider PROCERT, C. A. periodically reviews the cost of its electronic certificates and services, in order to improve them if possible and make its services and certificates more affordable for its Signatories and final entities that use electronic certificates.

Within its tariff scheme, Certificate Provider PROCERT, C. A. contemplates actions of social responsibility of the company, aimed at groups or entities that require social action and commitment of the company to the environment.

9.1.1. Certificate issuance or renewal fees.

Certificate Provider PROCERT, C. A. contemplates in its tariff structure a single payment per Signatory for a non-transferable subscription, which can be divided into monthly direct debit payments. The rates of the certificates and services of Provider of Certificates PROCERT, C. A. can be consulted through the following link: https://www.procert.net.ve/

9.1.2. Certificate access fees.

Certificate Provider PROCERT, C.A. charges an affordable and reasonable fee for access to your certificate database, use of your electronic certificates, TSA service, and professional services.

9.1.3. Revocation or Status Information Access Fees [REDACTED]

Certificate Provider PROCERT, C.A. does not contemplate the charge of concepts or establishment of fees for the use of its services for the verification of the life cycle of certificates such as the LCR and the OCSP. There are also no charges or costs for the revocation of certificates or the verification of Signatories through the link https://www.procert.net.ve/Consulta-Publica/index.aspx

9.1.4. Fees for other services.

PROCERT Certificate Provider, C. A. it does not include additional charges or costs for access to certificate lifecycle validators or for RPKI CPS or CP documentation. Professional implementation and configuration services in electronic certificate systems are not included in the certificate fee and must be requested separately.

9.1.5. Refund Policy.

The Signatories of PROCERT Certificate Provider, C. A. they can only request the refund of the fee paid for their certificate before the management of the certificate and approval of their certificate by the AR through the conformation of the Signatory's electronic file in the AR System of Provider of Certificates PROCERT, C. A. The refund request must be made through the mail soporte@procert.net.ve

9.2. Financial responsibility.

9.2.1. Insurance coverage.

The limits of the liability of the Certificate Provider PROCERT, C.A. towards its Signatories is regulated by contractual agreements with such customers. The liability of Certificate Provider PROCERT, C.A. to the Signatories and any other end entity using electronic certificates generated by Certificate Provider PROCERT, C.A., is limited against claims of any kind, including contractual, illegal, extra-contractual and criminal in nature, in each particular certificate regardless of the number of transactions, electronic signatures or causes of action arising out of or related to such certificate or any services provided with respect to such certificate and on a cumulative basis. Any and all claims arising out of the RPKI of Certificate Provider PROCERT, C.A. in relation to a certificate (without regard to the entity causing the damage), shall be subject to the limits of liability applicable to them in accordance with this CPS and the CP.

9.2.2. Other assets.

No stipulations.

9.2.3. Insurance or guarantee coverage for final entities.

Subject to the limitations set forth in 9.2.1., the limit of aggregate liability of the CA of Certificate Provider PROCERT, C.A. to all Signatories, nor for the entire period of validity of a certificate issued by Certificate Provider PROCERT, C.A. to all persons in connection with such certificate is fifteen thousand tax units (15,000 Tax Units) of the Bolivarian Republic of Venezuela. In no event shall the liability of the CA exceed the aforementioned limit.

9.3. Confidentiality of commercial information.

9.3.1. Scope of Confidential Information.

Certificate Provider PROCERT, C. A. maintains provisions for confidentiality of information and access to information in contracts with Signatories, maintains a confidentiality policy and a confidentiality plan for the purpose of securing sensitive information from unauthorized persons by identifying certain information as confidential and therefore not accessible to

untrusted personnel. The information that is classified as confidential is the following:

1. Access to private keys.
2. Activation data used to access private keys or to gain access to the AR system.
3. Business continuity, incident response, contingency, and disaster recovery plans.
4. Security schemes and procedures used to protect data, confidentiality, integrity, and availability of information.
5. Internal audit records.
6. Log log of the systems that make up the RPKI, including CA and AR.
7. Financial and financial audit records.
8. Records of archiving information classified as confidential.
9. Information from Signatories.
10. Disaster recovery procedures and plans.
11. Internal procedures on handling and configuring the RPKI including AC and AR.
12. Password management and access controls.
13. All information that has a legal reserve of confidentiality.

9.3.2. Information that does not fall within the scope of confidential information.
Certificate Provider PROCERT, C. A. informs that it will not consider the following information as confidential:

1. The CPS and the CP.
2. All certificates issued by the RPKI, for public use, may be publicly disclosed.
3. All certificates were revoked.
4. Any information that is not classified as private and confidential.

9.3.3. Responsibility to Protect Confidential Information.
Proveedor de Certificados PROCERT, C. A. maintains provisions for confidentiality of information and access to information in the contracts with the Signatories, maintains a confidentiality policy and a plan of confidentiality of information which establish the responsibility of the representatives and employees of Proveedor de Certificados PROCERT, C. A. in relation to the management, protection, use and safeguarding of the confidential information of the Signatories and the entire operation of the RPKI; being instructed in this regard and about their legal responsibilities for unauthorized handling and use of confidential information.

9.4. Privacy of Personal Information.

9.4.1. Privacy plan.
Certificate Provider PROCERT, C. A. maintains a confidentiality policy and a confidentiality plan for the information and in the employment and service contracts with its employees and suppliers establish mechanisms for the protection and safeguarding of information. Certificate Provider PROCERT, C. A. maintains a privacy policy on its website which is accessed through https://www.procert.net.ve/Docs/Pol%C3%ADtica%20Privacidad.pdf. The information of the Signatories may only be disclosed by

means of a court order duly issued by a judicial authority and in compliance with the pertinent legal requirements.

9.4.2. Information treated as private.
Certificate Provider PROCERT, C. A. establishes in its internal policies and the contract with its Signatories that all information received in the process of contracting an electronic certificate will be treated as private information of the Signatories and consequently will have protection regarding its use. unauthorized access, publication.

9.4.3. Information not considered private.
Certificate publishing data and records and their certificate lifecycle validators, such as LCR and OCSP, are not private data.

9.4.4. Responsibility to protect private information.
Provider of Certificates PROCERT, C. A. establishes that it is the responsibility of its employees and suppliers to properly handle private information and will comply with the provisions contained in their employment and service contracts, guaranteeing at all times the privacy of the data of the Signatories and of the Provider of Certificates PROCERT, C. A. All information considered as private is safeguarded following the guidelines of the information security policy of Provider of PROCERT Certificates, C. A. Provider of PROCERT Certificates, C. A., its employees and suppliers are also obliged to comply with national and international legislation regarding the handling of private data of the Signatories.

9.4.5. Notice and Consent to Use of Private Information.
Certificate Provider PROCERT, C. A., maintains a policy of safeguarding and protection of the Private Information of the Signatories, which will only be possible to disclose due to a final court order issued by a competent authority and previously informed to the Signatory. Certificate Provider PROCERT, C.A., may determine without the consent of the Signatories whether a certificate is active or revoked.

9.4.6. Disclosure pursuant to judicial or administrative process.
Based on the provisions of the subscription contract with the Signatories and the contracts with contractors, Provider of Certificates PROCERT, C. A., establishes the power to share the private data of the Signatories or contract information with suppliers, provided that there is an effective and final court order and limited to the data required for the creation of an electronic certificate.

9.4.7. Other circumstances of disclosure of information.
There are no other stipulations.

9.5. Intellectual Property Rights (if applicable).

copyrights in all certificate directories, LCR lists, and certificates; unless explicitly stated otherwise, all practices, policies, operational and security documents relating to the RPKI (electronic or otherwise) as well as contracts, belong to and remain the property of Proveedor de Certificados PROCERT, C.A. Through the corresponding contracts for the provision of certification services, Certificate Provider PROCERT, C.A. may grant a license to third parties for the use of certificates, LCRs and other authorized practices and policy documents to the extent they require it for the provision of certification services in accordance with this CPS and CP document.

9.6. Representations and Warranties.

9.6.1. CA Representations and Warranties.

Proveedor de Certificados PROCERT, C.A. declares that it does not make any representations regarding the electronic certificates it generates and the services they provide in general, except those related to the operation and use of such certificates and services, which are indicated below:

- Certificate Provider PROCERT, C.A. complies with its obligations in accordance with the provisions of the CA Browser Forum and the rules of SUSCERTE.
- Certificate Provider PROCERT, C.A. Complies with keeping available and active the mechanisms for validating the life of electronic certificates such as the LCR and the OCSP.
- Certificate Provider PROCERT, C.A. Complies with keeping your RPKI available and in operation.
- Certificate Provider PROCERT, C.A. complies with the provisions, procedures and declarations contained in the CPS and the CP.
- Certificate Provider PROCERT, C.A. complies with the provisions and obligations contemplated in the service contract signed with its Signatories.
- Certificate Provider PROCERT, C.A. complies with the legal order that regulates the operation of a Certification Service Provider within the Bolivarian Republic of Venezuela.
- Certificate Provider PROCERT, C.A. Complies with maintaining information mechanisms for the Signatories in the event of private key compromise or cessation of operation.
- Certificate Provider PROCERT, C.A. Complies with keeping available and active the mechanisms for generating electronic certificates through the AR System.
- Certificate Provider PROCERT, C.A. Complies with maintaining the bonds required by SUSCERTE.

9.6.2. Subscriber Representations and Warranties.

Certificate Provider PROCERT, C.A. declares that it does not make any declarations regarding the electronic certificates it generates and the services they provide in general, except for those related to the operation of the RA verification mechanisms, which are indicated below:

- Certificate Provider PROCERT, C.A. complies with its obligations for the purposes of the RA in accordance with the provisions of the CA Browser Forum and the rules of SUSCERTE.
- Certificate Provider PROCERT, C.A. Complies with keeping the AR validation mechanisms available and active.
- Certificate Provider PROCERT, C.A. complies with the provisions, procedures and declarations of RA contained in the CPS and the CP.
- Certificate Provider PROCERT, C.A. complies with the provisions and obligations contemplated in the service contract signed with its Signatories.
- Certificate Provider PROCERT, C.A. complies with the legal system that regulates the activity of RA within the Bolivarian Republic of Venezuela.
- Certificate Provider PROCERT, C.A. complies with the RA maintaining the mechanisms for verification and validation of identity.
- Provider of Certificates PROCERT, C.A. complies with the purposes that the information processed by the RA is handled and maintained with a criterion of confidentiality and privacy of the information.
- Certificate Provider PROCERT, C.A. ®. comply for the purposes of ensuring that the RA maintains electronic records of the Signatories.

9.6.3. Representations and warranties from the relying party.

Certificate Provider PROCERT, C.A. declares that it does not make any representations regarding the electronic certificates it generates and the services they provide in general and that, under the signed contract, the Signatories make the following statements:

- Use the certificate for the purpose for which you were hired.
- Comply with the terms and conditions of use of the contract that regulates the contracted electronic certificate.
- Comply with the legislation in force within the Bolivarian Republic of Venezuela.
- Generate your key pair.
- Assign a usage key for the certificate in accordance with the electronic certificate user and download manual.

9.7. Disclaimers of Warranties.

Certificate Provider PROCERT, C.A. declares that there is a CP that establishes the use of each of the electronic certificates it generates; said CP establishes the authorized and unauthorized uses; It also describes the scope of the certificate, the platform that supports it, thus establishing the expected use and operation of the certificates. In this way, Provider of Certificates PROCERT, C.A. limits its liability to that established in the CPS and CP, establishing such situation in the terms and conditions contained in the contract of use signed and accepted by the Signatory.

9.8. Limitations of Liability.

Certificate Provider PROCERT, C.A. declares that it will not assume responsibility for data and procedures that are not contemplated and indicated in the terms and conditions of the contract signed by the Signatory.

9.8.1. Compliance with legal requirements.

Certificate Provider PROCERT, C.A. declares that it will not assume responsibility for data and procedures that are not contemplated and indicated in the applicable legal norm decree law on data messages and electronic signatures (LSMDFE), the regulations (RLSMDFE) and the regulations of SUSCERTE, within these procedures, guarantees and processes the following are stated:

- That of achieving specific results.
- Of merchantability or fitness for a specific purpose,
- In relation to the accuracy or reliability of the information contained in the Certificates that are not supplied and/or verified by the RA.
- That is not related to the topics covered by this SCP and the COP.
- On the commercial or financial liability or stability of third parties who provide the certification services under their own authority or use or depending on the certification services, in cases of double certification.
- On the legal validity, ability to satisfy formal requirements or the status of proof of electronic signatures, certificates, or cryptographic keys and
- In relation to matters outside the reasonable control of the CA.
- If the CA is responsible for its failure to comply with the guarantees or for any other reason, the compensation provided for in the bond established by SUSCERTE will be applicable, however, it will be observed at all times that the payment of excessive damages that are intended to be fixed will not apply to those activities that are not directly related to the conditions of the certification services (in the same way that a public authority cannot be responsible for what a person does with an "Electronic Signature"). The CA therefore requires that members of the RPKI community consent to the fact that PROCERT Certificate Provider, C.A. It assumes no liability for any damages of any kind arising out of the circumstances described below (including special, consequential, incidental, indirect, or punitive damages), whether or not it has been advised of them (or their potentiality), or whether or not they are reasonably foreseeable.
- Underlying transactions between customers and third parties, including dependent parties.
- The services and/or products of Third Parties (including hardware and software) that interact with or use certification services, certificates, electronic signatures, etc.
- If there are a delay, mutilation, or loss or other errors in relation to the data or documents while they are being created, stored, or communicated.
- Unacceptable reliance on a Certificate, electronic signature, cryptographic key or key pair, or certification services to which this CPS and the CP refer.
- Non-compliance by third parties (including members of the RPKI community of Proveedor de Certificados PROCERT, C.A.) with local data protection or privacy legislation, consumer protection legislation or any other legislative or regulatory compliance required by the local jurisdiction; or

- Any indirect or consequential damage, loss of profits, loss of goodwill, loss of estimated savings, loss of profits, loss of business, business interruption; or loss of information.
- For greater protection from the risks related to the condition of certification services and to ensure the long-term stability of the RPKI, the amount of any damage recognized is also limited under the conditions set forth in the insurance policy required by SUSCERTE for the operation of Proveedor de Certificados PROCERT, C.A.

9.8.2. Loss Limitations.

The limits of the liability of Proveedor de Certificados PROCERT, C.A. towards the Signatories, is regulated by contractual agreements. As a reference to these contracts, this document of the CPS and CP and the other accreditation policies prepared by the Certificate Provider PROCERT, C.A. are incorporated. and referred to in the Information Security Policy of the latter.

Unless explicitly agreed or explicitly incorporated into a certificate, the responsibility of PROCERT, C.A. to customers, suppliers or interested parties, is limited against claims of any kind, including those in contract, illegal, tort and tortious nature, in each particular certificate regardless of the number of transactions, electronic signatures or causes of action arising out of or related to such certificate or any services provided with respect to such certificate and cumulatively.

Any and all claims arising out of the RPKI in connection with a certificate (without regard to the entity causing the damage or the entity that issued the certificate or provided the certification services), shall be subject to the limits of liability applicable to them in accordance with this CPS and COP document. The maximum liability per RPKI certificate shall be set forth in the corresponding certificate.

This certificate liability limit shall apply without regard to the number of transactions, electronic signatures, or causes of action arising out of or related to such certificate or any services provided with respect to such certificate and on a cumulative basis. subject to the foregoing limitations, the PROCERT Certificate Provider CA's aggregate liability limit, C.A. to all Signatories is fifteen thousand tax units (15,000 TU). In no event shall liability exceed the aforementioned limit.

9.9. Indemnities.

All compensation will be the product of a process of investigation and analysis or resolution of conflicts through administrative or judicial channels that are definitively firm and where the liability of Proveedor de Certificados PROCERT, C.A. derived from negligence or incompetence is determined.

9.10. Term and Termination.

9.10.1. Term.

Certificate Provider PROCERT, C.A. maintains a document management policy that establishes a review of all company policies and documentation every six (6) months or when changes occur that warrant it: and through

which the documentation is updated by review of its update, regulatory and legal modifications, update of applicable standards, among other points. A record is kept in the documentation to inform the numbers of editions and versions of each document, within the same documents of Proveedor de Certificados PROCERT, C.A.

9.10.2. Rescission.
The document management policy of Certificate Provider PROCERT, C.A. establishes that the documentation, including the CPS and the CP, will be in force until they require modifications or updates derived from changes that merit it and revisions based on their semi-annual verification, due to regulatory and legal changes, or by court order if applicable.

9.10.3. Effect of rescission and survival.
Certificate Provider PROCERT, C.A. declares that the change of the CPS or the CP and the issuance of a version or edition later than the one in force when a Signatory acquired a certificate, will not affect the conditions and terms of services contracted with PROCERT under the standard of the CA Browser Forum or SUSCERTE and will not affect the validity period of the certificate. In any case, the following conditions will apply:

- Certificate Provider PROCERT, C.A. will maintain the stipulations contained in the contract it maintains with its Signatories.
- Certificate Provider PROCERT, C.A. will maintain the guarantees required by SUSCERTE for the operation as a Certification Services Provider, unless, by way of change in the CA Browser Forum, the SUSCERTE standards or judicial measure signs, a modification in said guarantees is established, being necessary the due participation and information on the part of the PROCERT Certificate Provider. C.A. to its Signatories, about the changes that have taken place.
- Certificate Provider PROCERT, C.A. will duly inform its Signatories about changes in editions or versions of the CPS and the CP.
- Certificate Provider PROCERT, C.A. will maintain the obligations of confidentiality and handling of private information, unless, by way of change in CA Browser Forum, the SUSCERTE regulations or judicial signature measure, it is established that such information is no longer confidential or private.
- Certificate Provider PROCERT, C.A. will duly inform its Signatories about changes in the signing algorithms that due to changes and due compliance with the CA Browser Forum standard or the SUSCERTE standards, it is required to be carried out; in which case the Signatories must revoke their electronic certificate, after issuance by Certificate Provider PROCERT, C.A. of a new electronic certificate that contemplates the remaining term of the period contracted by the Signatory in question.

9.11. Individual notices and communications with participants.
Certificate Provider PROCERT, C.A. informs that all information notice, request for change or revision of the CPS and the CP may be sent by signed email, which must have the complete data of the applicant including, names and surnames, identity card number or identity document, complete address including

zip code, Telephone contact and valid email address. An acknowledgment of receipt generated by the server and email handler of Proveedor de Certificados PROCERT, C.A. will be issued. Once the information has been received, the Certificate Provider PROCERT, C.A. will have a period of ten (10) business days, within which it will respond to the information or notice received. The response will be made by signed email and will contain acknowledgement of receipt and reading. Once the response has been received from the Certificate Provider PROCERT, C.A., the Signatory or sender of the notice or information must respond regarding the receipt of the response from the Certificate Provider PROCERT, C.A. within three (3) days following its receipt, which will end the process.

9.12. Modifications.

9.12.1. Modification procedure.

Supplier of Certificates PROCERT, C.A. establishes that any change of this CPS or the CP is executed in accordance with the provisions of the document management policy of Supplier of Certificates Provider PROCERT, C.A., which establishes a review of all company policies and documentation every six (6) months or when changes occur that warrant it as indicated in point 9.10.1. Updates must comply with the authorization process by the authorities of Certificate Provider PROCERT, C.A. and will be duly informed to the Signatories; being automatically replaced in the documentation repository of Certificate Provider PROCERT, C.A., including the new versions of the CPS and the CP. The link to consult the current and updated versions of the CPS and the COP is available to the Signatories at link https://www.procert.net.ve/Internas/AC.aspx.

9.12.2. Notification mechanism and deadline.

Certificate Provider PROCERT, C.A. establishes that any change to this CPS or the CP is duly informed via email to the Signatories and published at the link https://www.procert.net.ve/Internas/AC.aspx. on the website of Proveedor de Certificados PROCERT, C.A. www.procert.net.ve

9.13. Dispute Resolution Provisions.

Supplier of Certificates PROCERT, C.A. contemplates in the contract it has with its Signatories a clause for the resolution of differences or disputes, which establishes that if the controversy has not been resolved through negotiation between Supplier of Certificates PROCERT, C.A. and the Signatory or complaining party, within fifteen (15) business days after the claim is initiated, then, at the request of the Signatory or claimant, the controversy will be submitted to SUSCERTE, the governing body in the matter of electronic certification within the Bolivarian Republic of Venezuela, by virtue of the provisions of numeral 13 of article 22 of the Decree with the Force of Law on Data Messages and Electronic Signatures. The solution reached with the mediation of SUSCERTE and accepted by the Certificate Provider PROCERT, C.A. and the Signatory or complaining party, will be binding and mandatory. Certificate Provider PROCERT, C.A. and the Signatory or complaining party will also be free to go to the body in charge of the protection, education and defense of the contracting user in accordance with the Law that regulates the matter. In the event that no agreement is reached, the avenue of claim will be free by ordinary judicial process before the Courts of the Jurisdiction of the Metropolitan Area of Caracas, to the exclusion of any other.

9.14. Applicable law.

This CPS and the CP shall be governed and interpreted in accordance with the provisions of the rules of the CA Browser Forum, the regulations of SUSCERTE for the operation of Certification Service Providers and the legislation applicable to the matter within the Bolivarian Republic of Venezuela, establishing as a special domicile to the exclusion of any other the city of Caracas to the jurisdiction of whose courts the Signatories agree to submit to the exclusion of any other.

9.15. Compliance with applicable law.

Certificate Provider PROCERT, C.A. and the Signatories undertake to comply with the guidelines and processes established in the CPS and the CP and in the legislation that regulates the matter of electronic certificates within the Bolivarian Republic of Venezuela for the purposes of providing the service.

9.16. Miscellaneous provisions.

9.16.1. Entire Agreement.

This CPS and the CP contain all the conditions, processes and contractual agreements on which Proveedor de Certificados PROCERT, C.A. contemplates the operation of its RPKI within the Bolivarian Republic of Venezuela; for the purposes of the issuance of electronic certificates, the validation of the identity of the Signatories by the RA, the management of the life cycle of the certificates, the management of information and the mechanisms of assurance of operation on which the Signatories accept and agree on the use of electronic certificates generated by the PROCERT Certificate Provider, C.A. and on which it is obligated. What is not contemplated in the CPS and CP does not constitute the basis of the service contracted by the Signatory and therefore will not be required of the Certificate Provider PROCERT, C.A.

9.16.2. Cession.

This CPS and the obligations it establishes towards the Signatories may be assigned to other entities that assume by transfer, sale, merger or contract the operation of the RPKI of Certificate Provider PROCERT, C.A. including the activities of the CA and AR within the Bolivarian Republic of Venezuela. The assignments of this CPS in other entities will not be effective if they constitute debt novations or fraud against the Law.

9.16.3. Severability.

Certificate Provider PROCERT, C.A. establishes that if any part of the CPS is declared invalid, null or inapplicable due to non-compliance with the CA Browser Forum, the rules of SUSCERTE or by a final judgment of a court of the Bolivarian Republic of Venezuela, it will proceed in accordance with the provisions of point 9.10.1., duly informing the Signatories and replacing the editions and versions replaced by the current one. The link to consult the current and updated versions of the CPS and the COP is available to the Signatories at link https://www.procert.net.ve/Internas/AC.aspx. Publications of the CPS or CP with partial null or inapplicable will not be maintained and in the eventuality that they have not been replaced by the current ones, the parts that are not applicable will be indicated with a message within the CPS or CP.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights).

Provider of Certificates PROCERT, C.A. that each and every one of the parts that make up this CPS and the CP are in force and applicable, if for any reason Provider of Certificates PROCERT, C.A. or the Signatory do not exercise their right established within the CPS or the CP, this will not be understood as a waiver of the rights that assist them under the Law. No waiver of rights shall be valid without prior written notice. Likewise, Provider of Certificates PROCERT, C.A. reserves the right to exercise actions and collection of fees against persons who have acted against the provisions of the CPS or the CP, causing damage, losses or costs associated with the attention and remediation of situations derived from the aforementioned actions.

9.16.5. Force majeure.

Supplier of Certificates PROCERT, C.A. shall be relieved of its responsibilities for total or partial, definitive or temporary involuntary breach of its obligations under this CPS and the CP, when such obligations are due to causes that cannot be attributed to Supplier of Certificates PROCERT, C.A., which is unforeseeable, unavoidable and whose occurrence implies an absolute impossibility for Supplier of PROCERT Certificates, C.A. to comply with the obligations assumed under this CPS or the CP, either because the non-compliance is due to:

- Fortuitous event or force majeure, understood as those unforeseeable and unavoidable events that prevent the fulfillment of the obligation in an absolute manner and that are independent of the conduct of Proveedor de Certificados PROCERT, C.A. and that cannot be attributed to it.
- The act of the third party shall be understood as those events caused by persons independent of Proveedor de Certificados PROCERT, C.A. that prevent it from fulfilling its obligations under this service order.
- The act of the prince must be understood as any legal or sub-legal provision emanating from competent organs of the state and that affect or regulate the activity of the Certificate Provider PROCERT, C.A. and that absolutely prevent the fulfillment of the obligations contracted by the Certificate Provider PROCERT, C.A. under this CPS or the CP; and
- The loss of the thing due when the obligation is the delivery of a certain and determined thing and the loss is not attributable to Supplier of Certificates PROCERT, C.A., will be understood as such, when the liability of Supplier of Certificates PROCERT, C.A. perishes, disappears or becomes insufficient for the purposes of this CPS or the CP or remains out of commerce as long as Supplier of PROCERT Certificates, C.A. is not in arrears.

From now on, each of the aforementioned conditions will be individually referred to as a non-attributable extraneous cause or force majeure and will activate the disaster recovery and business continuity plans of Proveedor de Certificados PROCERT, C.A. If a non-attributable extraneous cause or force majeure occurs, PROCERT, C.A. notify the Signatories explaining in detail the event, as well as the extent to which it will affect the performance of their obligations under this CPS or the COP. During the

period of duration of the event that qualifies as a non-attributable extraneous cause or force majeure PROCERT, C.A. it will seek to find alternative means that allow it to comply with the obligations assumed under the CPS or the CP, and to mitigate any negative effects or impacts derived from the non-attributable extraneous cause or force majeure on the provision of the electronic certification service. At the conclusion of the event that qualifies as a non-attributable extraneous cause or force majeure, Certificate Provider PROCERT, C.A. will notify the Signatories, and the provision of the service will continue. If the event that qualifies as a non-attributable extraneous cause or force majeure does not cease within a period of thirty (30) calendar days, following the date of notification to the Signatories, Supplier of Certificates PROCERT, C.A. will proceed to the cessation of operation by notifying SUSCERTE, the Signatories for such purposes and initiating the process of delivery to SUSCERTE of the RPKI for its operation.

9.16.6. Other Provisions.
They are not contemplated.

10. Normative references.

- Webtrust (Compliance Web Link)
- CA Browser Forum (Compliance Web Link)
- Decree-Law on Data Messages and Electronic Signatures and its Regulations.
- Regulations of the Superintendence of Electronic Certification Services (SUSCERTE).
- PROCERT Regulations.
- ITU-T X.500 international standard.
- ITU-T X.509 V3 International Standard.
- ITU-T X.609 International Standard.
- ISO 9001:2015 standard.
- ISO/IEC 9594-8 standard.
- ISO/TR 10013:2021 standard.
- ISO/IEC 27001:2022 standard.
- ISO/IEC 27002:2022 standard
- ISO/IEC 27002:2022 standard
- 27011:2022
- RFC 5280.
- RFC 6484.
- RFC 6485.
- RFC 6487.
- FIPS 140-2
- FIPS 140-3