Certification Practice Statement (CPS)
And Certificate Policies (PC)

Index

Page

1. Version control

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

Edition 13	**Semiannual Control and Correction (Update)**	**17/11/2014**	**No**
Edition 14	**Semiannual Control and Correction (Update)**	**07/04/2015**	**No**
Edition 15	**Semiannual Control and Correction (Update)**	**06/10/2015**	**No**
Edition 16	**Semiannual Control and Correction (Update)**	**01/02/2016**	**No**
Edition 17	**Semiannual Control and Correction (Update)**	**16/03/2016**	**No**
Edition 18	**Semiannual Control and Correction (Update)**	**09/05/2016**	**No**
Edition 19	**Semiannual Control and Correction (Update)**	**05/06/2017**	**No**
Edition 20	**Semiannual Control and Correction (Update)**	**11/07/2017**	**No**
Edition 21	**Technical Update**	**29/9/2017**	**Yes**

2. **Title:** Certification Practices Statement (CPS) and Certificate Policy (PC) document.

3. **Code**: AC-D-0003.

4. **Introduction:** This document consists of the declaration by Proveedor de Certificados (PROCERT), C.A., for the purpose of informing and documenting its certification processes, for a better understanding and understanding by its Senior Management, personnel, Customers, Suppliers and Stakeholder PSC PROCERT.

   The Certification Practice Statement (CPS) allows senior management, staff, customers, suppliers and stakeholders of the PSC PROCERT to know each of the processes and subprocesses involved in the life cycle of electronic certificates; document disaster recovery processes, manage cryptographic keys and give an overview of the equipment and infrastructure supported by the PSC PROCERT trust scheme.

   The policies of the certificates allow the High Management, personnel, Customers, Suppliers and Stakeholder of the PSC PROCERT to know the authorized use of each type of certificate issued by the PSC PROCERT, its structure and its functions. The Senior Management, personnel, Customers, Suppliers and Stakeholder of the PSC PROCERT that use the electronic certificates issued by PSC PROCERT, must comply with this document of the Certification Practices Statement (CPS) and Certificate Policy (PC) and shall be liable for any consequences arising out of the unadjusted use of an electronic certificate or failure to comply with the instructions contained in this document.

5. **Definitions:** In order to provide an adequate interpretation of the meaning and scope of this document, a set of concepts will be set out below, the plural or singular names of which will follow the meaning given below:

   5.1. **Key File:** Means the process of storing used keys or their ID and / or certificates as a record in long term storage for future recoveries.
   5.2. **Audit:** Means the review and review of the system of records and activities to assess the adequacy and effectiveness of system controls to ensure compliance with established and recommended operational policies and procedures for the operation of a PSC and to detect the necessary changes in controls, policies and procedures and ensure the implementation of such changes over time.
   5.3. **Compliance Audit**: Means the review and review of system records and activities to test the adequacy of system controls to ensure compliance with established policy and operational procedures, detect security gaps and recommend changes in controls, Politics and procedures.

5.4. Certification Authority (CA): It means an authority on which customers trust to create, issue and manage the life cycle of certificates, which for the purposes of the decree law of data messages and electronic signatures must be accredited granted by SUSCERTE.

5.5. Registration Authority: Means the entity whose purpose is to provide local support to the public key infrastructure (PKI) of a Certification Authority (CA). The Registration Authority performs a set of functions oriented to the validation, verification and conformation of the documentation supplied, as well as the physical identity of a client that opts for the purchase of an electronic signature or electronic certificate generated by PSC PROCERT.

5.6. Certificate String: Means a multiple certificate string required to validate a certificate. The certificate chains are constructed by linking and verifying the electronic signature in a certificate with a public key that is in a certificate issued by the PSC PROCERT, which is subordinate and signed by the root certificate generated by the SUSCERTE.

5.7. Certificate: 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 "un-forgettable" by an electronic signature of the certification authority that generated it.

5.8. Public Key Certificate: Means the electronic certificate that links the Public Key of an entity with the entity's distinctive identifier and which indicates a specific validity period.

5.9. Encryption: Means the process by which the simple data of a text are transformed to hide its meaning. Encryption is a reversible process that is performed through the use of a cryptographic algorithm and a key.

5.10. Key: It means the sequence of symbols that controls the operation of a cryptographic transformation (eg encryption, decryption, cryptographic verification, computation function, generation or signature verification).

5.11. Cryptographic Key: Means the parameter used in conjunction with an algorithm for validation, authentication, encryption and decryption purposes.

5.12. Private Key: Means the asymmetric key of an entity, which will normally be known only by that entity.

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

5.14. Client: Means the entity that has requested the issuance of a certificate within the public key infrastructure (PKI) of PROCERT. For the purposes of the decree law of data messages and electronic signatures and its regulations the customer will be understood as the signatory and vice versa.

5.15. Confidentiality: Means the property of not disclosing or making available to third parties and without authorization of the owner, the information and data corresponding to persons, entities and / or processes.

5.16. Access Control: Means the prevention of unauthorized use of a resource, including prevention of unauthorized use of a resource.

5.17. Cryptography: Means the discipline that encompasses principles, means and methods for the transformation of information and data for hidden contents of information or data, in order to avoid unauthorized modifications and / or to prevent unauthorized use of information or data, as appropriate.

5.18. Certification Practice Statement (CPS): Means the statement of practices that the certification authority uses to issue certificates and manage their life cycle.

5.19. Recipient: Means the entity that obtains (receives or retrieves) a message.

5.20. Key Destruction: Means the process of removing all copies of a key using the key management system.

5.21. Availability: Means the ownership of information to be accessible and usable upon request by an authorized entity or process.

5.22. Entity: Means any person (natural or legal) or system (mechanical or electronic).

5.23. Public Key Infrastructure Entity (PKI) Subordinate: Means any entity that has the authority to operate and provide Certification Services under SUSCERTE's public key infrastructure (PKI).

5.24. Evaluation: Means the evaluation against defined criteria to give a measure of confidence in the sense that the corresponding requirements are met.

5.25. Audit Event: Means an action internally detected by the system that can generate an audit record. If an event causes an audit record to be generated [to record on an audit trail]. This is a "registered event". Otherwise it is an "unregistered event". The system decides, to the extent that each event is detected, whether it should generate an audit record by preselecting the audit algorithm. The set of audit events is based on the security policy of the system.

5.26. **Electronic Signature**: Means the added data or a cryptographic transformation of a data unit that allows the receiver of the data unit to test the source and integrity of the data and protect against counterfeiting, for example, the recipient.

5.27. Cryptographic Tab: Means the medium in which a key is stored (eg smart card, cryptographic key).

5.28. Certificate Generation: It means the process of creating a certificate from input data that is specific to the application and the client.

5.29. Key Generation: Means the process by which cryptographic keys are created. It is the function of generating the variables required to meet the particular attributes of the key.

5.30. Identification Information: It means the information obtained to positively identify an entity and provide the certification services it requests.

5.31. Public Key Infrastructure (PKI): Means the infrastructure needed to generate, distribute, manage and archive certificate revocation keys, certificate revocation lists, and certificate status protocol (PECL) transponders.

5.32. Operational Infrastructure: It means the technological infrastructure through which certification services are provided. This infrastructure does not necessarily coincide with the legal infrastructure or relationships that exist or are developed between entities that are part of the public key infrastructure (ICP) of PROCERT or that use public key infrastructure (PKI) of PROCERT in any form.

5.33. **Data Integrity**: Means the quality or condition to be accurate, complete and valid and not be altered or destroyed in an unauthorized manner.

5.34. Interoperability: Interoperability means that the equipment and procedures used by two or more entities are compatible and, therefore, they may assume joint or related activities.

5.35. Post-Suspension Investigation: Means the investigation made by the general management and the technology consultant of PSC PROCERT after suspending a certificate to determine if said certificate should be revoked or reinstituted as valid.

5.36. Certificates Revoked List (CRL): Means the list of certificates that have been revoked or suspended by the PSC PROCERT.

5.37. Key Management: Means the administration and use of the generation, registration, certification, disincorporation, distribution, installation, storage, archiving, revocation, diversion and destruction of key material in accordance with the security policy.

5.38. Audit Level: Means a series of requirements and regulations associated with the Certificate Types as shown in this Certification Practices Statement (CPS) and Certificate Policy (PC) and against which PSC accredited to SUSCERTE are audited

5.39. Key Pair: The keys in an asymmetric cryptographic system are defined as having one of the key pairs decrypting what the other key pair encrypts.

5.40. Parameters Asymmetric: It means the pair of related keys where the private key defines the private transformation and the public key defines the public transformation.

5.41. Interested Party: Means the organization or person that has an interest in the performance or success of PSC PROCERT.

5.42. Verification Process: Means the process that takes the signed message, verification key and domain parameters as input and outputs the result of the signature verification: valid or invalid.

5.43. Online Certificate Status Protocol (OCSP): This is a protocol used to validate the status of a certificate in real time. The application response includes three (3) status: valid, revoked or unknown. Its definition in English is OCSP (Online Certificate Status Protocol).

5.44. Supplier: Means the organization or person providing a product or service for the PSC PROCERT.

5.45. PSC: Means Certification Service Provider

5.46. Audit Log: Means the discrete data unit registered 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 trail has an audit trail

description for the log header and usually has additional audit descriptions describing the entity (s) and object (s) involved in the event.

5.47. Summary of Information: Means the basic information required for the production of a public key certificate for the verification of an electronic signature, the validation of the certificate status, as well as the information produced as a result of this verification.

5.48. Revocation: Means the change of status of a valid or suspended certificate to "revoked" from a specific date onwards.

5.49. Certificate Revocation: Means the process of changing the status of a valid certificate or suspended or revoked. When a certificate has revoked status, this means that an entity should no longer be trusted for any purpose.

5.50. Physical Security: Means the measures used to provide physical protection to resources against deliberate and accidental threats.

5.51. Certification Services: Means the services that can be provided in relation to the lifecycle management of certificates at any level of the PKI hierarchy, including ancillary services such as OCPS services, timeshare services, identity verification services, certificate revocation list hosting (CRL), etc

5.52. Applicant: Means the entity that requested the issuance of a certificate within the public key infrastructure (PKI) of PROCERT. The verification process varies according to the nature and, where applicable, the operational role within the public key infrastructure (PKI) corresponding to the certificate that the entity is requesting.

5.53. Certificate Request: Means the request authenticated by an entity by its parent authority to issue a certificate that links the identity of that entity to a public key.

5.54. Certificate Usage: Means the set of rules that indicate the applicability of the certificate of a particular community and / or the class of application with common security requirements. For example, a particular policy certificate may indicate the applicability of a type of certificate for the authentication of mobile communications for the marketing of products within a given price range.

5.55. Validation: Means the process of verifying the validity of a Certificate in terms of its status (eg suspended or revoked).

6. Objective: Certification practice statement (CPS) and certificate policy, constitute the guide to the best principles of management and operation of the PSC PROCERT, which must be documented and informed to senior management, personnel, customers, Suppliers and Interested Party of PSC PROCERT.

The electronic certificates issued by PSC PROCERT under the "Electronic Signature" class, for the purposes of the application of the decree law of data messages and electronic signatures and their regulations, will provide the owner of the "electronic signature" with the opportunity to have an electronic instrument that will be considered as full proof for the purposes of Venezuelan legislation and that will additionally provide

the conditions of identity recognition, information authentication within a public and private key system, the possibility of establishing non-repudiation of the "Electronic Signature" and will offer the possibility of guaranteeing the integrity of the message and the data contained in the "electronic signature", significantly expanding the universe of activities and transactions that may have full legal validity within the spectrum of the Internet and in different fields, within which may be mentioned, government online, online commerce, online education, among others. The registration authority (AR) of PSC PROCERT will establish and give faith, about the identity and data supplied by the client to whom an electronic certificate is assigned.

This information will be transmitted to the certification authority (CA) of PSC PROCERT, in order to authorize the activation of the electronic certificate. Registration authorities (RAs) operate globally or separately from certification authorities (CAs). The PSC PROCERT maintains within its internal organization the registration authority (AR).

7. **Scope:** This PSC PROCERT Certification Practice Statement (CPS) and Certificate Policy (CP) document applies to the Senior Management, Personnel, Clients, Suppliers and Stakeholder of the PSC PROCERT for the process of issuance, revocation or renewal of certificates and operation of the technological platform of certification of PSC PROCERT.

8. **Limitations:** Numeral 31.15 of this document establishes the limit of liability that may be required for faults in the management and operation of the PSC PROCERT.

9. **Community of users and applicability**:

9.1. Approval of policies: All PSC PROCERT documentation related to the process of certificate generation or revocation, operation of the PSC PROCERT under the principles of the decree law of data messages and electronic signatures (LSMDFE) and its regulations, will be elaborated by the personnel and senior management of PSC PROCERT and submitted to the approval of SUSCERTE.

9.2. Documentation update: The PSC's High Management PROCERT establishes the conditions that apply for the revision or modification of the documentation. These elements are as follows:

- Organizational changes.
- Changes in the regulations for accreditation as PSC by SUSCERTE or entity that regulates electronic certification activity within the Bolivarian Republic of Venezuela.
- Changes in the International regulation that regulates the activity of the CPS.

- Changes in the legislation that regulates the activity of the CPS within the Bolivarian Republic of Venezuela.
- Changes in the processes and / or subprocesses that need to be documented.
- Documentation with more than six (6) months, without modification or update, should be printed as a new version

9.3. Certification Authority (CA): The PSC PROCERT is a mercantile company, with strict private initiative, constituted and designed for the purpose of being constituted as the first PSC in compliance with the decree law of data message and electronic signatures, its regulation or regulatory bodies to replace them; offer electronic signatures and certificates to public and private individuals, natural or legal, public and private, provide technical support and applications for electronic signatures and certificates; conduct training activities in electronic signatures and certificates, electronic commerce, other applications and uses that involve their use; development, maintenance, as well as offer applications for online procedures with entities of centralized and decentralized public administration, governorates and municipalities of the Bolivarian Republic of Venezuela. PSC PROCERT has located its administrative offices in the city of Caracas, Capital District of the Bolivarian Republic of Venezuela.

9.3.1. PSC PROCERT Certificate Root: PSC PROCERT Root Certificate: PSC PROCERT is a second level certification authority and is subordinate to the root certification authority of the Venezuelan state and will only be in operation during the conduct of the operations for which it is established. The structure of the root certificate of the PSC PROCERT is as follows:

Certificate fields	Certificate Value
Version	V3 (Version number of the certificate).
Serial number:	(Identificador único menor de 32 caracteres hexadecimales.)
Signature Algorithm:	SHA-384RSA (Signature Algorithm)
Issuer data	
CN	Autoridad de Certificación Raíz del Estado Venezolano
O	Sistema Nacional de Certificación Electrónica
OU	Superintendencia de Servicios de Certificación Electrónica
C	VE
E	acraiz@suscerte.gob.ve
L	Caracas
ST	Distrito Capital
Period of validity	

Valid from:	(Start date of certificate)
Valid until:	(Expiration of the period of validity of the certificate).
Data of the holder	
CN	PSCPROCERT
O	National Electronic Certification System
OU	Proveedor de Certificados PROCERT C.A.
C	VE
E	contacto@procert.net.ve
L	Chacao
ST	Miranda
Public Key Information	
Public Key Algorithm	RSA(Algorithm with which the public key was generated)
Public key size	(4096)
Extensions	
Basic Restrictions	CA: TRUE Y LOGONITUD DEL PATH = 1
Alternate name of the issuer	
Dns name	suscerte.gob.ve
Other name	
OID 2.16.862.2.2	RIF-G-20004036-0 (RIF de SUSCERTE)
Keyword holder	(Holder Key Identifier)
Identificador de clave de autoridad certificadora	
Key ID	(Key identifier Identificador de la clave)
Certificate Issuer	(Issuer data)
Certified serial number	(Serial number)
key usage	Electronic signature of the certificate and signature of CRL
Nombre alternativo del titular	
DNSName	**PROCERT.net.ve**
Other name	
OID 2.16.862.2.1	PSC-000002
OID 2.16.862.2.2	J-31635373-7

Distribution point CRL	http://www.suscerte.gob.ve/lcr/CERTIFICADO-RAIZ-SHA384CRLDER.crl
Information of the issuer	http://ocsp.suscerte.gob.ve
Certificate Policy	http://www.suscerte.gob.ve/dpc

9.3.2 PSC PROCERT Certification Root: PSC PROCERT has a certification platform audited and authorized by SUSCERTE which complies with international standards for the operation of a public key infrastructure under the X-509 V3 standard. The PSC PROCERT is able to issue electronic certificates for different uses. The cryptographic keys are generated by the user through the CSP contained in the browsers. The SUSCERTE after evaluation of compliance with the requirements of Law, signs a certificate request with the platform of the root certificate of the Venezuelan state. Once the certificate is signed, the PSC PROCERT becomes a second level certification authority and is subordinated to SUSCERTE.

The root certificate generated by SUSCERTE must be integrated by PSC PROCERT within its certification platform in order to be able to generate and assign electronic certificates under the parameters of the decree law on data messages and electronic signatures (LSMDFE) and its regulation (RLSMDFE).

The PSC PROCERT must generate every twenty-four (24) hours a certificates revoked list (CRL), which constitutes a mechanism for validating and checking the status of electronic certificates and verifying which ones are revoked. All process of revocation of certificate is informed by the PSC PROCERT, via electronic mail to the Client that owns the electronic certificate. This notification is reported monthly to SUSCERTE and is included in the digitized deposit maintained by the PSCPROCERT.

9.3.3. Operation model of PSC PROCERT.

9.3.3.1. Administrative Headquarters: The administrative headquarters manages the administrative, financial, fiscal and human resources processes required for the operation of the PSC PROCERT; Likewise, the registration authority (AR) is in charge of managing the verification of the documentation and identity of the contracting clients and provide public faith for the review and compilation of the data provided by each one of them. customers of electronic certificates. The physical address of the administrative headquarters is as follows: Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, Office B-

132, Chacao Municipality of the City of Caracas, Bolivarian Republic of Venezuela. The opening hours for the general public from the administrative headquarters of PSC PROCERT are as follows: from 8:00 a.m. at 12:00 m and 1:00 p.m. at 5:00 p.m.), from Monday to Friday of each week, from each calendar month, from each calendar year. The PSC PROCERT will provide electronic signature certificates to all natural and / or legal persons that comply with the requirements set forth in the decree law of data message and electronic signatures and regulation and that successfully complete the process of contracting and acceptance of terms contractual obligations; setting a term of validity for the certificates that are issued, one (1) year.

The PSC PROCERT, contemplates that in the event of the occurrence of an event that permanently affects the integrity of its administrative headquarters, proceed to start operations from a new headquarters that meets the requirements imposed by SUSCERTE.

However, in case of disaster that disables or destroys the administrative headquarters of PROCERT, a contractual provision is maintained with the Simón Bolívar University in order to be able to operate from the headquarters of its data center, for the contingency period.

9.3.3.2 Relationship with technology providers and associated companies: Relationship with technology providers and associated companies: PSC PROCERT maintains business relationships and strategic alliances with the following companies: i) Wisekey; (ii) Microsoft; iii) Ncipher; (iv) SafeNet; and v) Level 3.

9.3.3.3. Website: The PSC PROCERT maintains a web portal (www.procert.net.ve) with high availability. The web page of PSC PROCERT on its home page maintains the following links: i) Purchase of Certificates, where the user can obtain information to facilitate the purchase of certificates step by step, inquire about the prices of certificates that provides the PSC PROCERT and its electronic signatures of legal validity; ii) Certification System, where the user will be able to access his electronic certificate lifecycle management box; iii) EN / ES, where the user clicks to change the language of the web portal from Spanish to English and vice versa; iv) List of Revoked Certificates, where the user can download the CertificatesRevoked List (CRL) issued daily by PSC PROCERT; v) Root Certificate SUSCERTE,

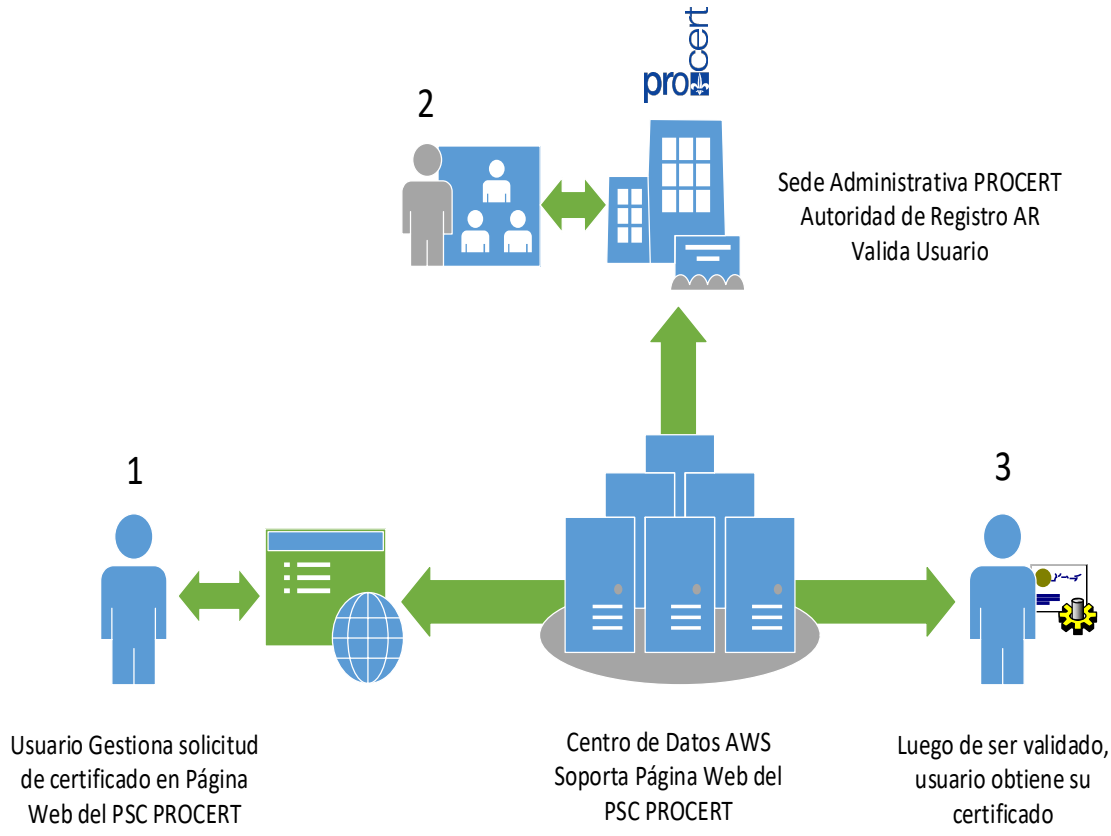
where users can download the chain of certification of the Venezuelan state. vi) Issued, where the user can consult the certificates issued by PSC PROCERT; vii) App and Uses, to be informed about the use of the electronic certificates, of the management of the certificate during the life cycle of the certificate; viii) Management, where the user can inquire about the use of the electronic certificates, the management of the certificate during the life cycle of the certificate ix) AC PROCERT, where the user can access the PSC PROCERT technical documentation and certificate policies ; x) Online signature, where PSC PROCERT users can sign on line and with certificates issued by PSC PROCERT, electronic documents in .PDF format; xi) Support, where it is possible to access information related to the systems and software supported by certificates issued by PSC PROCERT, find a list of frequently asked questions and access tutorial videos about the use of electronic certificates and electronic signature; xii) PKI, where the user can advise on the creation of a public key infrastructure; xiii) SSL, where the user can obtain information regarding security certificates, price, use, and classification. xiv) Contact us where the user can by clicking directly send an email to the address of the PSC PROCERT in addition to obtaining their contact telephone number. xv) Twitter, where the user can access technical information published on different portals or produced by PSC PROCERT regarding electronic certificates.

9.3.3.4. Data center: The PSC PROCERT maintains an operational scheme aimed at guaranteeing the operational continuity and provision of services with high standards of quality, timeliness and security. The data center is constituted in the operational headquarters of PSC PROCERT and from where the platform of emission of certificates operates. The data center meets and maintains the operational requirements imposed by the international regulations on security associated with information technology, the legislation of the Bolivarian Republic of Venezuela and the standards imposed by SUSCERTE. The maintenance and operation of the technological platform of certification of the PSC PROCERT is executed by its own personnel. The data center is located in the city of Caracas and belongs to the company Level 3. The data center operates twenty-four (24) hours a day, three hundred sixty-five (365) days of the year and maintains a superior operational autonomy to two (2) months. Additionally, the data center meets the conditions and characteristics of anti-seismic construction

and fire and flood prevention, maintains a security perimeter and has seven (7) levels of access security.

The data center from which PSC PROCERT operates maintains the policies or instruments issued by recognized and solvent insurance companies in order to maintain support in the event of a contingency that affects the physical integrity of said administrative center and can thus offering a guarantee of its operational continuity. The certification authority (AC) PROCERT maintains an alternate center operation contract in case of permanent damage that makes it impossible and restricts the regular operation of the data center.

9.3.3.5. Scheme of the operational model of the PSC PROCERT.



9.4. Registration Authority (RA): It is the internal organization within the PSC PROCERT responsible for validating and verifying the identification and data provided by legal or natural persons who purchase electronic certificates and in order to be able to give public faith that the client that holds and uses an electronic certificate, it is who effectively claims to be or represent in the case of legal person, thus guaranteeing the identity of the Client of an electronic certificate and consequently, legality of the responsibilities and obligations derived from the use of the electronic signature under the assumptions of the decree law on data messages and electronic signatures and its regulations.

All those interested in obtaining an electronic certificate under the decree law on data messages and electronic signatures, its regulations and the regulations of SUSCERTE, must send a copy of the supporting documentation of their data and go to the appointment set by the AR of the PSC PROCERT for the purpose of verifying, validating face-to-face and documentary records, media and other proofs that prove their identity and / or representation of representatives of legal entities that option for an electronic certificate.

If the interested party does not attend the interview scheduled by the HR of PSC PROCERT will be annulled his request or request for registration and will apply the withholding penalty, and consequently the Customer interested again to register their application for electronic certificate on the website of PSC PROCERT). Support documentation used to validate customers or customers requesting electronic certificates, will be stored by PSC PROCERT, during the period of ten (10) years as of the validity of the certificate or any of its renewals.

9.4.1. Model of operation of RA.

9.4.1.1. Administrative Headquarters: The AR of PSC PROCERT maintains a management scheme aimed at ensuring operational continuity and provision of services with high standards of quality, timeliness and security. The AR operates from the administrative headquarters of PSC PROCERT and is in charge of validating and giving agreement on the identity of contracting customers of electronic certificates, so that once verified the information and identity of contracting customers, proceed with the registration of customers and subsequent generation of electronic certificates.

9.4.1.2. Validation of identity: Received the documentation of the clients of the AR of PSC PROCERT to set an opportunity for the identity validation interview to take place, which may be face-to-face or via web with an interview recorded for such purposes.

During the interview, the HR operator of PSC PROCERT requests information from the client and requests that the client, under oath, state that his / her data is true. To validate domain names, the AR of PSC PROCERT makes the appropriate consultation to http://www.whois.net/ and http://www.nic.ve/. The customer must provide the information that matches his registration in Whois.net or Nic.ve. With the information provided by the clients, the validation of Whois or Nic.ve is executed; in order to validate the truth of it.
The information provided by the client, must match the records of Whois.net or Nic.ve. Without proper documentation and registration, PSC PROCERT will refrain from processing any request. To validate the email address, the PSC PROCERT AR sends an email requesting information to the client.

All emails sent by the AR of PSC PROCERT are electronically signed. The email messages will require the authorization of the owner of the email account. Each of the emails sent by the PSC PROCERT must request different requirements associated with the validation process in each case.

These PSC PROCERT e-mail messages are not predictable, since information that only the customer knows is required. In addition, PSC PROCERT staff must verify all information (affidavits, statutes, RIF, business identification, utility bills).

The PSC PROCERT AR will request a statement regarding domain ownership and authorization letter in the case of SSL certificates. Certificate requests (CSRs) must meet the requirements of the CA Browser Forum. Customers will respond to the email with all the information requested by AR PROCERT. For support issues, PROCERT uses support@procert.net.ve.

In the case of SSL certificates, only the certificate requests (CSR) generated in compliance with the national and international standards will be processed, paying particular attention to those established by the CA Browser Forum, which are listed below:

According to the CA-Browser-Forum-BR-1.5.2 standard in section 7.1.4.

"Name Forms":

1) SAN: This extension MUST contain at least one entry. MUST be a dNSName that contains the full domain name or iP address of the server
2) SAN: This field must not contain reserved IP address or Internal name
3) Common Name: The common name must be in the SAN
4) Common Name: Do not put in this field https: //
5) SAN and Common Name: Should not have the following characteristics:

    - The use of the dot (.)
    - The use of blank or other value that indicates missing or incomplete value
    - Using the minus symbol (-)

All other optional attributes, when present in the subject field, MUST contain information that has been verified by the CA. Optional attributes MUST NOT contain metadata such as '.', '-' and " characters (ie, space), and / or any other indication that the value is missing, incomplete, or not applicable.

All emails are signed by PROCERT staff. The AR of PSC PROCERT will execute the telephone calls, in order to validate all the information of the client. The PSC PROCERT AR uses the telephone number provided by the customer in the information provided to the PSC PROCERT. This information must be validated with the official and public records of the website of the National Telephone Company.

When a customer requests information to purchase a certificate, they will receive an email from the AR of PSC PROCERT with complete information; offering in this way the guarantee to provide in every moment all the information that the client needs. The documents that must be presented by the clients for the contracting of electronic certificates, vary according to the type of gone by type of certificate and are communicated to the clients via email signed by the AR of PSC PROCERT.

These documents may vary and customers are informed by signed email at every opportunity. This, in order to prevent the constant changes in the present document, derived from changes in the requirements (inclusion or exclusion of any of them). The integrity of this document will protect you from unnecessary changes.

Customers contracting for electronic signatures or certificates must go to the Administrative Office of PROCERT located in Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, Office B-132, Chacao Municipality in the city of Caracas, Bolivarian Republic of Venezuela, on the date and time established by the PROCERT hiring system within working hours from 8:00 am to 12:00 p.m. and from 1:00 p.m. to 5:00 p.m., from Monday to Friday of each week of each calendar month, of each calendar year.

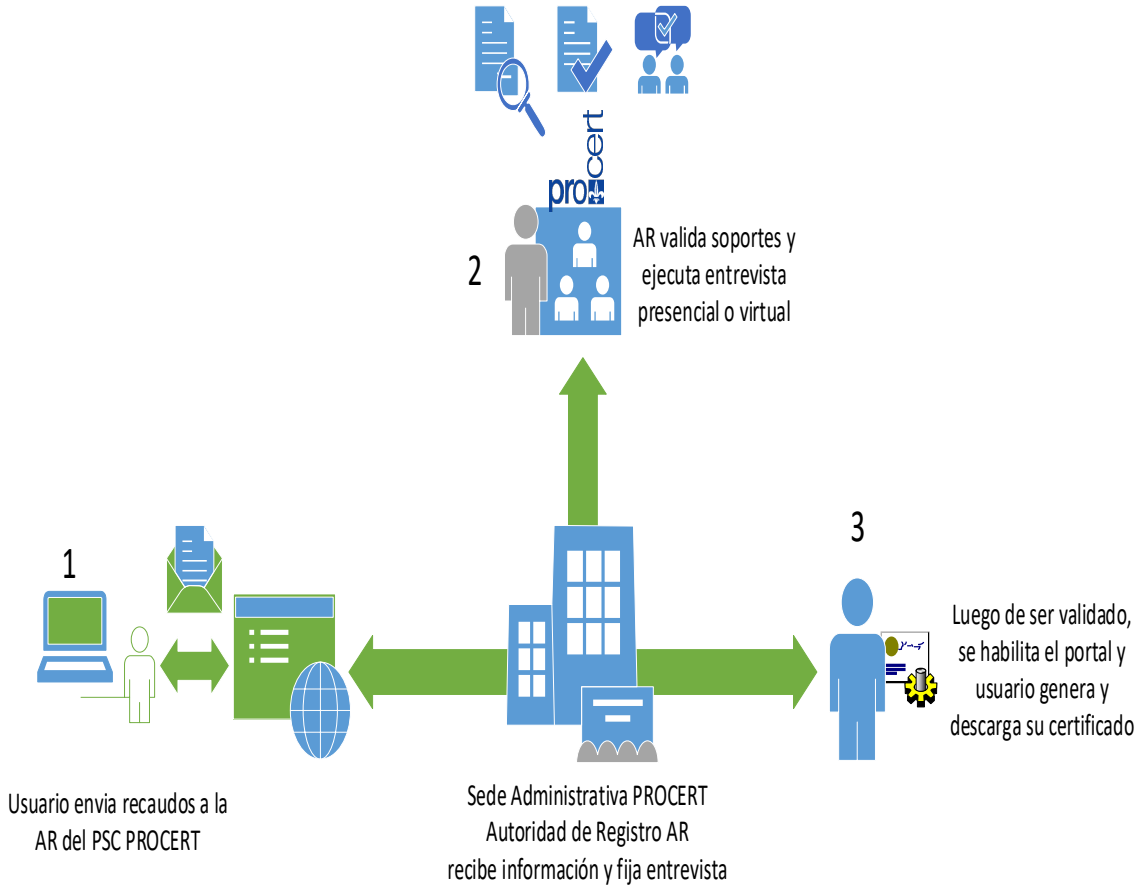
It is also possible to validate the identity of the user via electronic interview that is recorded and associated with the client's information, all of which is required to authorize the generation of the certificate.

The contracting client must notify the limitations or impossibility of attending the appointment set by electronic mail to the support@procert.net.ve address with not less than forty eight (48) hours before the date set for the appointment.

The AR of PSC PROCERT will reprogram the opportunity for identity validation for a single occasion and notify the contracting user by email. If the contracting client does not notify the impossibility of attending the rescheduled appointment, and it is not possible to validate the identity; then the AR of PSC PROCERT will proceed to cancel the application and apply the corresponding penalty.

Regarding the validation of foreign certificates, provided for in the Decree Law of Electronic Data and Electronic Signatures and its Regulations, the AR of PSC PROCERT will keep updated the data provided by the PSCs with which it maintains relation of recognition and validation of electronic certificates, preventing at all times the use of revoked certificates. Audits of control and validation of the documentation and identity of contracting customers of electronic certificates will be scheduled annually. The documentation will be kept in electronic storage stored in vault.

9.4.1.3. Diagram of the RA model.



9.5. Confidence Model: It is the guide or bibliographic technical reference through which the client knows the scheme of operation, management and legal validity of the electronic certificates generated by the PSC PROCERT, allowing the client to verify the validity of the electronic certificates and thus rely on the operation and management model of the PSC PROCERT. Likewise, the trust model allows to inform the client about the certification root or authority that signs to the PSC PROCERT.

9.5.1. Model Applied for the Bolivarian Republic of Venezuela: The Certification Authority (CA) Root is designed and operates under the principle of "Self Signed Certification Authority"; under such a scheme the Root Certification Authority (CA) is not subordinate to a certification chain or foreign certification body, and self-certifies a single root certificate for the certification of electronic signatures or issuance of electronic certificates. In Venezuela, the governing body of the subject is SUSCERTE. SUSCERTE complies with internationally recognized technological and legal standards applicable to the subject of electronic certification and is in charge of carrying out the custody of the root certificate to which all public or private PSCs legally accredited to operate in the Bolivarian Republic of Venezuela.

The activities of SUSCERTE and accredited providers of certification services are regulated by the Decree Law of Electronic Data and Signatures and its Regulations. All PSC within the Bolivarian Republic of Venezuela, abide by and comply with the resolutions and technical regulations issued by SUSCERTE and the legal framework applicable to the matter.

9.5.2. Accreditation as PSC: Within the Venezuelan model and the legal regulations contained in the Decree Law of Electronic Data and Signatures, it is contemplated that all interested parties, whether public or private, comply with an accreditation process before the Superintendence of Certification Services Electronics (SUSCERTE), which entails the following steps:

9.5.1.1 Audit prior to the application for accreditation to SUSCERTE, which must be performed by an IT Auditor accredited by said office. The accredited auditor will issue a technical audit report on compliance with applicable standard and standards for the operation of the PSC. Said technical audit report constitutes one of the requirements to make the application for accreditation or renewal of accreditation before SUSCERTE.

9.5.1.2. Presentation of the request for accreditation or renewal of accreditation with SUSCERTE, which means compliance to the previous audit mentioned in 8.4.1. and compliance with the financial requirements and standards set by SUSCERTE.

9.5.1.3. Once points 8.4.1 are met. and 8.4.2., present the guarantee required by the State in order to be able to operate as a PSC.

9.5.1.4. Once all the requirements of Law have been fulfilled, the SUSCERTE will issue the accreditation and operation number assigned to the PSC in case of first request or proceed to the issuance of the administrative renewal order of accreditation in case of PSC already accredited; subsequently in the case of the first application, the SUSCERTE with the PSC will proceed to the ceremony of keys and install in the technological platform of the PSC the root certificate issued and signed by SUSCERTE. In the cases of renewal, the process culminates with the publication of the administrative renewal order in the official gazette.

9.5.2. Model Applied by PSC PROCERT: PSC PROCERT is a mercantile company of strict private initiative, constituted and designed for the purpose of becoming the first provider of electronic certification services in compliance with the provisions of the Data Message Decree Law and Electronic Signatures, its regulation or the normative bodies that substitute these; offer electronic signatures and certificates to natural or legal persons, public and private, provide the hosting service to public, governmental or private sector entities; providing technical and support services to applications for electronic and hosting signatures and certificates; conduct training activities in electronic signatures and certificates, electronic commerce, electronic auctions and other applications and uses that involve its use; develop, maintain and offer applications for online procedures with entities of centralized and decentralized public administration, governorates and municipalities of the Bolivarian Republic of Venezuela; purchase, sale, distribution, import and / or export of products, goods and services, software and hardware, as well as the realization of all kinds of commercial, commercial and licit industrial activities, representation of national and foreign companies and all those legal acts trade permitted by law, whether or not included in the foregoing list of activities. Our main market will consist of Commercial Banking, insurance companies, large companies and small and medium industry.

The PSC PROCERT has located its headquarters in the city of Caracas, Capital District of the Bolivarian Republic of Venezuela and complies with the technical and economic financial requirements required by SUSCERTE, through the exhaustive regulations issued to such effects by said regulatory body. the activity of the PSC.

The PSC PROCERT operates under the technological standard and subordinate authority cryptographic keys, which facilitates the installation of the root certificate issued by SUSCERTE and the independence and security of

the database of certificates issued by the PSC PROCERT. The certification platform of PSC PROCERT derives from cryptographic hardware and software, which are called in the case of the hardware "HSM" and in the case of the cryptographic software "Platform of Services of Certification", which is property of the company PROCERT.

The PSC PROCERT is able to issue electronic certificates for different uses. Cryptographic keys are kept offline at the Data Center from which the PSC PROCERT operates. The PSC PROCERT publishes the Certificates Revoked List (CRL), which is a record of all those certificates that, having fulfilled their process of generation and assignment of Law, are revoked when their password is compromised, at the request of the user, for improper use of the certificate, for reasons attributable to the user or for the cessation of operation of PSC PROCERT.

The CRL is updated every twenty-four (24) hours on the PROCERT website (www.procert.net.ve), during the three hundred and sixty-five (365) days of each calendar year, while the PSC PROCERT is in operation. In addition, the PSC PROCERT has an OCSP link, which allows online status validation of certificates.

Any certificate expiration or revocation process is automatically notified by email to the signatory owner of the certificate. The development of a trust model established by the PSC PROCERT is contained in the document issued by the PSC PROCERT called Confidence Model, distinguished by the nomenclature AC-D-0001.

9.6. Public Access Registry: The Public Access Registry is a document to support this Certificate Practice Statement (CPS) and Certificate Policies (PC) and allows to supply the information related to access to the website of the Certification Authority (AC), brief description of the technology used for the generation of certificates, security measures applicable to the protection of the website and its functionalities, in compliance with the guidelines imposed by the Superintendence of Electronic Certification Services (SUSCERTE) for the purposes to be able to operate as a Certification Services Provider (PSC). The public access registry allows among other points the following:

- Ensure access to relevant descriptive information of the system by the Clients.
- Provide a description of the PROCERT Certification Services Provider (PSC) website.

- Indicate the services and products offered by the PROCERT Certification Service Provider (PSC).
- Describe the technology (hardware and software) used.
- Description of the process of contracting electronic certificates.
- Information about the security mechanisms used in the Certification Services Provider (PSC) web portal.

9.6.1. Regarding the Detail of the PROCERT Website: PROCERT's technology platform has an electronic access site available twenty-four (24) hours each day, during the three hundred and sixty-five (365) days of each calendar year. The operation of said website is monitored twenty-four (24) hours of each day, during the three hundred and sixty-five (365) days of each calendar year.

Any failure of the system should be addressed in accordance with PROCERT's Business Recovery and Disaster Recovery Plan (DRP) (AC-P-0001).

9.6.2. Regarding the Content of the PROCERT Website: The PROCERT website contains the information necessary to understand the process of contracting, use and applications of electronic certificates and information related to the electronic certification activity and the company PROCERT; also the user'swill find the documentation of the Certification Authority (AC) PROCERT; of the Registration Authority (RA) PROCERT; and the information produced and derived from SUSCERTE. The addresses contained in the PROCERT website are as follows

9.6.2.1. Address for requesting / activating certificates.
9.6.2.2. Address for reporting events occurring on the PROCERT platform.
9.6.2.3. Address for the search of issued certificates.
9.6.2.4. Address to access the Certificates Revoked List (CRL), whose publication will be published every twenty-four (24) hours in accordance with the document of the Policy and Structure of the Certificates Revoked List (CRL).
9.6.2.5. Address to perform the revocation or suspension of valid certificates.
9.6.2.6. Resolutions of the Superintendence of Electronic Certification Services (SUSCERTE).
9.6.2.7. Document of Certification Policy and Statement of Certification Practices in PDF format.
9.6.2.8. Address where the Products and Services offered by PROCERT are described.

9.6.2.9. Technical Documentation on the installation and uses of electronic certificates.

9.6.2.10. General information about electronic certification (advantages and trends).

9.6.2.11. Contact information PROCERT.

9.6.3. The development of the Public Access Registry established by the PSC PROCERT is contained in the document issued by PSC PROCERT called Public Access Registry, distinguished by the nomenclature AC-R-0002.

9.7. Electronic certificates: The PSC PROCERT is in capacity of 9.7. Electronic certificates: The PSC PROCERT is able to generate electronic signature certificates with a key from 2048 to 4096. The standard approved by SUSCERTE for national certificates is 2048 bit of key length. The PSC PROCET currently has authorization from SUSCERTE to issue the electronic certificates indicated below:

• Electronic signature certificate for company employees.
• Electronic signature certificate for representatives of public companies.
• Electronic signature certificate for legal representative of private company.
• Electronic signature certificate for qualified professionals.
• Electronic signature certificate for natural person.
• Electronic certificate of signature for public official.
• SSL electronic certificate.
• Electronic certificate for control of logical access.
• Electronic certificate for transaction signature.
• Electronic certificate of electronic invoice.
• Electronic Banking Electronic Certificate.

9.7.1. Uses of certificates: The different types of electronic signature certificates issued by PSC PROCERT are described below:

9.7.1.1. Electronic signature certificate for company employees: The assigned use for this type of certificate is as follows:

- Online Transactions.
- Identify employees or employees of public or private companies online.
- Electronic communications without representation of public or private companies.

- Does not confer legal representation of public or private companies.

9.7.1.2. Structure of the electronic signature certificate for company employees.

Certificate Field	Certificate Value
Version	V3 (Número de versión del certificado).
Serial number	(Identificador único menor de 32 caracteres hexadecimales.)
Signing algorithm	Sha-256RSA (Algoritmo de Firma)
Issuer Information	
CN	PSCPROCERT
O	National electronic certification system
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Chacao
ST	Miranda
Period of validity	
Valid from:	(Start date of certificate)
Valid until:	(Expiration of the period of validity of the certificate).
Owner Details	
CN	(Name the employee to certify)
T	(Position of the holder)
O	(Organization name's)
OU	(Organizational Unit Name) Optional
OU	(Identity card or passport number)
C	(Country)
E	(email)
L	(Address
ST	(State)
Public Key Information	
Public Key Algorithm	RSA(Algorithm with which the public key was generated)
Public key size	2048
Extensions	
Basic Restrictions	CA: False
Alternate Name of Issuer	

DNS name	procert.net.ve
Other name	
OID 2.16.862.2.1	(Code of the PSC PROCERT assigned by SUSCERTE)
OID 2.16.862.2.2	RIF-J31635373-7(RIF del PSC PROCERT)
Key Holder Identification	(key holder ID)
Certifying Authority Key Identifier	
Key ID	(Key identifier)
Certificate Issuer	(Issuer data)
Certified serial number	(Serial number)
key usage	Electronic signature, non-repudiation, encryption and data encryption
Alternate name of holder	
Other name	
OID 2.16.862.2.2	(ID Number or Passport)
Distribution point CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl http://www.procert.net.ve/lcr/PROCERTca.crl
Information of the issuer	http://ura.procert.net.ve/ocsp
Certificate Policy	http://www.procert.net.ve/dpc-pc/

9.7.1.3. Use of the signature certificate for company employees.

Use	Improved use
Electronic signature, no repudiation, encryption and signature of mail.	Signature of documents, Secure mail

9.7.1.4. Electronic signature certificate for representatives of public companies: The assigned use for this type of certificate is as follows:

- Certify a person as a legal representative of a public legal entity
- Public or private online transactions, representing companies or Public Law Entities.
- Private or public communications on behalf of Companies or Public Law Entities.

- E-commerce in representation of Companies or Public Law Entities.
- Declarations or online proceedings before the government on behalf of Companies or Public Law Entities.

9.7.1.5. Structure of the electronic signature certificate for representatives of public companies.

Certificate Field	Certificate Value
Version	V3 (Número de versión del certificado).
Serial number	(Identificador único menor de 32 caracteres hexadecimales.)
Signing algorithm	Sha-256RSA (Algoritmo de Firma)
Issuer Information	
CN	PSCPROCERT
O	Sistema nacional de certificación electrónica
OU	PROCERT
C	VE(País)
E	contacto@procert.net.ve
L	Chacao
ST	Miranda
Period of validity	
Valid from:	(Inicio vigencia del certificado)
Valid until:	(Expiración del periodo de validez del certificado).
Owner Details	
CN	(Nombre del funcionario a certificar)
T	(Cargo del funcionario)
O	(Organización campo opcional)
OU	(Unidad organizacional) campo opcional
C	(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Public Key Information	
Public Key Algorithm	RSA (Algoritmo con el que se generó la clave pública)
Public key size	2048
Extensions	
Basic Restrictions	CA: False
Alternate Name of Issuer	

DNS name	PROCERT.net.ve
Other name	
OID 2.16.862.2.1	(Code of the PSC PROCERT assigned by SUSCERTE)
OID 2.16.862.2.2	RIF-J31635373-7(RIF del PSC PROCERT)
Key Holder Identification	(key holder ID)
Certifying Authority Key Identifier	
Key ID	(Key identifier)
Certificate Issuer	(Issuer data)
Certified serial number	(Serial number)
key usage	Electronic signature, no repudiation, Encryption
Alternate name of holder	
Other name	
OID 2.16.862.2.2	(ID Number or Passaport)
Distribution point CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl http://www.procert.net.ve/lcr/PROCERTca.crl
Information of the issuer	http://ura.procert.net.ve/ocsp
Certificate Policy	http://www.procert.net.ve/dpc-pc/

9.7.1.6. Authorized use of the electronic signature certificate for representatives of public companies.

Use	Improved use
Electronic signature, non-repudiation, encryption and email signature	Signature of documents, secure email

9.7.1.7. Electronic signature certificate for legal representative of private company.

The assigned use for this type of certificate is as follows:

- Certify a person as legal representative of a private legal entity.
- Public or private online transactions, representing a commercial, civil or other corporate form.
- Private or public communications on behalf of a commercial, civil or other corporate form.

- E-commerce in representation of a commercial, civil or other corporate form.
- Online declarations or formalities before the government on behalf of a commercial, civil or other corporate form.

9.7.1.8. Structure of electronic signature certificate for legal representative of private company.

Certificate Field	Certificate Value
Version	V3 (Número de versión del certificado).
Serial number	(Identificador único menor de 32 caracteres hexadecimales.)
Signing algorithm	Sha-256RSA (Algoritmo de firma)
Datos del emisor	
CN	PSCPROCERT
O	Sistema nacional de certificación electrónica
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Chacao
ST	Miranda
Período de validez	
Valid from:	(Inicio vigencia del certificado)
Valid until:	(Expiración del período de validez del certificado).
Datos del titular	
CN	(Nombre del representante legal a certificar)
T	(Cargo del representante legal a certificar)
O	(Nombre de la organización)
OU	(Nombre de la unidad organizativa) opcional
C	(País)
E	(Correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave publica	
Public Key Algorithm	RSA(Algoritmo con el que se generó la clave pública)
Public key size	2048
Extensiones	
Basic Restrictions	CA: False

Nombre alternativo del emisor	
DNS name	procert.net.ve
Other name	
OID 2.16.862.2.1	(Código del PSC PROCERT asignado por SUSCERTE)
OID 2.16.862.2.2	RIF-J31635373-7(RIF del PSC PROCERT)
Key Holder Identification	(Identificador de clave del titular)
Identificador de clave de autoridad certificadora	
Key ID	(Identificador de la Clave)
Certificate Issuer	(Datos del emisor)
Certified serial number	(Número de Serial)
key usage	Firma electrónica, no repudio, cifrado
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cedula de identidad o pasaporte)
Distribution point CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl http://www.procert.net.ve/lcr/PROCERTca.crl
Information of the issuer	http://ura.procert.net.ve/ocsp
Certificate Policy	http://www.procert.net.ve/dpc-pc/

9.7.1.9. Authorized use of the electronic signature certificate for legal representative of private company.

Use	Improved use
Electronic signature, non-repudiation, encryption and email signature.	Signature of documents, secure email

9.7.1.10. Electronic signature certificate for qualified professionals.

The assigned use for this certificate is as follows:

- Online transactions associated with the exercise of profession or trade with tuition and legal recognition within the Bolivarian Republic of Venezuela.
- Private or public communications associated with the exercise of profession or trade with tuition and legal recognition within the Bolivarian Republic of Venezuela.

- E-commerce associated to the exercise of profession or trade with tuition and legal recognition within the Bolivarian Republic of Venezuela.
- Declarations or online proceedings before the government associated with the exercise of profession or trade with tuition and legal recognition within the Bolivarian Republic of Venezuela.

9.7.1.11. Structure of the electronic signature certificate for qualified professionals.

Campo del certificado	Valor del certificado
Versión	V3(Número de versión del certificado)
Número de serie	Identificador único menor de 32 caracteres hexadecimales.
Algoritmo de firma	Sha-256RSA(Algoritmo de Firma)
Datos del emisor	
CN	PSCPROCERT
O	Sistema nacional de certificación electrónica
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Chacao
ST	Miranda
Período de validez	
Válido desde	(Inicio vigencia del certificado)
Válido hasta	(Expiración del período de validez del certificado).
Datos del titular	
CN	(Nombre del signatario)
T	(Título profesional)
O	(Organización) campo opcional
OU	(Unidad organizacional) campo opcional
C	VE(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave pública	
Algoritmo de clave pública	RSA (Algoritmo con el que se generó la clave pública)
Tamaño de clave publica	2048

Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
DNS name	procert.net.ve
Other Name	
OID 2.16.862.2.1	(Código del PSC PROCERT asignado por SUSCERTE)
OID 2.16.862.2.2	RIF-J31635373-7 (RIF del PSC PROCERT)
Identificador clave titular	(Identificador de clave del titular)
Identificador de clave de autoridad certificadora	
Id. de clave	(Identificador de la Clave)
Emisor de certificado	(Datos del emisor)
Número serie certificado	(Número Serial)
Uso de clave	Firma electrónica, no repudio, cifrado.
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cédula de identidad o pasaporte)
Punto distribución CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl http://www.procert.net.ve/lcr/PROCERTca.crl
Información emisor	http://ura.procert.net.ve/ocsp
Política de certificados	http://www.procert.net.ve/dpc-pc/

9.7.1.12. Authorized use of the electronic signature certificate for qualified professionals.

Use	Improved use
Electronic signature, no repudiation, encryption and signature of mail.	Signature of documents, secure email

9.7.1.13. Electronic signature certificate for natural person.

The assigned use for this type of certificate is as follows:

- Private transactions, other than the provision of professional services.
- Private or public communications in a personal capacity.
- Electronic purchases for natural persons.

- Declarations or online proceedings before the government for natural persons.

9.7.1.14. Structure of electronic signature certificate for natural person.

Campo del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado)
Número de serie	Identificador único menor de 32 caracteres hexadecimales.
Algoritmo de firma	Sha-256RSA (Algoritmo de firma)
Datos del emisor	
CN	PSCPROCERT
O	Sistema nacional de certificación electrónica
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Chacao
ST	Miranda
Período de validez	
Válido desde	(Inicio vigencia del certificado)
Válido hasta	(Expiración del período de validez del certificado).
Datos del titular	
CN	(Nombre del signatario)
C	VE (País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave publica	
Algoritmo de clave publica	RSA(Algoritmo con el que se generó la clave pública)
Tamaño de clave publica	2048
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
DNS Name	procert.net.ve
Other Name	
OID 2.16.862.2.1	(Código del PSC PROCERT asignado por SUSCERTE)

OID 2.16.862.2.2	RIF-J31635373-7 (RIF del PSC PROCERT)
Identificador clave titular	(Identificador de clave del titular)
Identificador de clave de autoridad certificadora	
Id. de clave	(Identificador de la Clave)
Emisor de certificado	(Datos del emisor)
Número serie certificado	(Número Serial)
Uso de clave	Firma electrónica, no repudio
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cedula de identidad o pasaporte)
Punto distribución CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl http://www.procert.net.ve/lcr/PROCERTca.crl
Información del Emisor	http://ura.procert.net.ve/ocsp
Política de certificados	http://www.procert.net.ve/dpc-pc/

9.7.1.15. Authorized use of the electronic signature signing certificate for natural person.

Use	Improved use
Electronic signature, no repudiation, encryption and signature of mail.	Signature of documents, secure email

9.7.1.16. Certificate of electronic signature for public official: The assigned use for this type of certificate is as follows:

- To certify a person as a public career official, of free appointment or removal or of popular election and to which entity of government is attached or belongs.
- Public or private online transactions, representing centralized or decentralized government entities.
- Private or public communications on behalf of Centralized or Decentralized Government Entities.
- E-commerce on behalf of centralized or decentralized government entities.

- Declarations or online procedures before the government on behalf of centralized or decentralized government entities.
- Electronic Signature of Electronic Mail and Electronic Documents.

9.7.1.17. Structure of electronic signature certificate for civil servant.

Campo del certificado	Valor del certificado
Versión:	V3 (Número de versión del certificado).
Número de serie:	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de firma:	Sha-256RSA (Algoritmo de firma)
Datos del emisor	
CN	PSCPROCERT
O	Sistema nacional de certificación electronica
OU	PROCERT
C	VE(País)
E	contacto@procert.net.ve
L	Av. Libertador Multicentro Empresarial del Este piso 13 Oficina B-132 Torre Libertador Núcleo B
ST	Miranda
Período de validez	
Válido desde:	(Inicio vigencia del certificado)
Válido hasta:	(Expiración del período de validez del certificado).
Datos del titular	
CN	(Nombre del funcionario a certificar)
T	(Cargo del funcionario)
O	(Organización campo opcional)
OU	(Unidad organizacional) campo opcional
OU	(Número de cédula de identidad o pasaporte)
OU	(Tipo de instrumento utilizado para el nombramiento)
OU	(Número del instrumento de nombramiento)
OU	(Fecha de emisión)
OU	(Fecha efectiva)
OU	(Publicación)
C	(País)
E	(correo electrónico)
L	(Dirección)

ST	(Estado)
Información de clave publica	
Algoritmo de clave pública	RSA (Algoritmo con el que se generó la clave pública)
Tamaño de clave publica	(2048)
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
Dns name	PROCERT.net.ve
Other name	
OID 2.16.862.2.1	(Código del PSC PROCERT asignado por SUSCERTE)
OID 2.16.862.2.2	RIF-J31635373-7 (RIF del PSC PROCERT)
Identificador clave titular	(identificador de la clave del titular)
Identificador de la clave de autoridad certificadora	
Id. de clave	41 0f 19 38 aa 99 7f 42 0b a4 d7 27 98 54 a2 17 4c 2d 51 54
Emisor de certificado	E= acraiz@suscerte.gob.ve OU= SUSCERTE O= Sistema Nacional de Certificación Electrónica S= Distrito Capital L= Caracas C= VE CN= Autoridad de Certificación Raíz del Estado Venezolano
Número serie certificado	0b
Uso de clave	Firma electrónica, no repudio y Cifrado
Uso mejorado	Firma de documentos, correo Seguro
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cédula de identidad o pasaporte)
OID 2.16.862.2.3	(Tipo de Instrumento utilizado para el nombramiento)
OID 2.16.862.2.4	(Número del instrumento de nombramiento)
OID 2.16.862.2.5	(Fecha de emisión)
OID 2.16.862.2.6	(Fecha efectiva)
OID 2.16.862.2.7	(Publicación)
Punto distribución CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl

	http://www.procert.net.ve/lcr/PROCERTca.crl
Información del Emisor	http://ura.procert.net.ve/ocsp
Política de certificados	http://www.procert.net.ve/dpc-pc/

9.6.1.1. Authorized use of the electronic signature signing certificate for a civil servant.

Use	Improved use
Electronic signature, no repudiation, encryption and signature of mail.	Signature of documents, secure email

9.6.1.2. SSL electronic certificate: The assigned use for this type of certificate is as follows:

- Protection of online transactions between servers and clients belonging to an integrated information technology system.
- Protection of online communications between servers and clients belonging to an integrated information technology system.

9.6.1.3. Structure of the SSL electronic certificate.

Campo del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado)
Número de Serie	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma	Sha-256RSA(Algoritmo de firma)
Datos del emisor	
CN	PSCPROCERT
O	Sistema nacional de certificación electrónica
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Chacao
ST	Miranda
Período de validez	
Válido desde	(Inicio vigencia del certificado)
Válido hasta	(Expiración del período de validez del certificado).
Datos del titular	
CN	(Dominio o dirección IP)

O	(Organización)
OU	(Unidad organizacional) campo opcional
C	VE(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave pública	
Algoritmo clave pública	RSA (Algoritmo con el que se generó la clave pública)
Tamaño de clave publica	(2048) / (4096)
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
DNS Name	procert.net.ve
Other Name	
OID 2.16.862.2.1	(Código del PSC PROCERT asignado por SUSCERTE)
OID 2.16.862.2.2	RIF-J31635373-7 (RIF de PROCERT)
Identificador clave titular	(Identificador de clave del titular)
Identificador de clave de autoridad certificadora	
Id. de clave	(Identificador de la Clave)
Emisor de certificado	(Datos del emisor)
Número serie certificado	(Número Serial)
Uso de clave	No Repudio, Cifrado de Clave, Cifrado de Datos
Uso mejorado de Clave	Autenticación del servidor
Nombre alternativo del titular	
DNS Name	(Nombre de dominio del servidor)
Other name	
OID 2.16.862.2.2	(Número de RIF de la empresa)
Dirección IP	IP del Servidor
DNS Primario	DNS
Punto distribución CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl http://www.procert.net.ve/lcr/PROCERTca.crl
Información del Emisor	http://ura.procert.net.ve/ocsp

Política de certificados	http://www.procert.net.ve/dpc-pc/

9.6.1.4. Authorized use of SSL certificate.

Use	Improved use
Non-repudiation and encryption	Server Authentication

9.6.1.5. Electronic Certificate for Transaction Signature: The assigned use for this type of certificate is as follows:

- On-line or off-line transaction protection.
- Proof of transaction record.
- Integrity of Information.
- No repudiation.
- Electronic signature of electronic files and documents.

9.6.1.6. Structure of electronic certificate for transaction signature.

Campo del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado).
Número de serie:	(Identificador único 32 caracteres hexadecimales.)
Algoritmo de firma:	Sha-256RSA (Algoritmo de Firma)
DATOS DEL EMISOR	
CN	PSCPROCERT
O	Sistema Nacional de Certificación Electrónica
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Av. Libertador Multicentro Empresarial del Este piso 13 Oficina B-132 Torre Libertador Núcleo B
ST	Miranda
Periodo de validez	
Válido Desde:	(Inicio vigencia del certificado)
Válido Hasta:	(Expiración del periodo de validez del certificado).
Datos del titular	
CN	(Identificador del objeto)
T	(Ubicación) opcional

O	(Nombre de la organización)
OU	(Nombre de la unidad organizativa) opcional
OU	(Número de RIF)
C	(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave pública	
Algoritmo clave pública	RSA(Algoritmo con el que se generó la clave pública)
Tamaño clave pública	(2048)
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
Dns name	procert.net.ve
Other name	
OID 2.16.862.2.1	(Código del PSC PROCERT asignado por SUSCERTE
OID 2.16.862.2.2	RIF-J31635373-7 (RIF de PROCERT)
Identificador de clave del Titular	(Identificador de clave del titular)
Identificador de clave de autoridad certificadora	
Id. de clave	Identificador de la clave
Emisor de certificado	(Datos del emisor)
Número serie certificado	(Número de serial)
Uso de la clave	Firma electrónica, No Repudio, Cifrado.
Uso Mejorado de la clave	Firma de Documentos
nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cedula de identidad, pasaporte o RIF)
Punto distribución CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl http://www.procert.net.ve/lcr/PROCERTca.crl
Información del emisor	http://ura.procert.net.ve/ocsp

Política de certificados	http://www.procert.net.ve/dpc-pc/

9.6.1.7. Authorized Use of Certificate for Transaction Control.

Use	Improved use
Electronic signature, no repudiation	Signature of documents

9.6.1.8. Electronic Certificate for Electronic Invoice Signature: The use assigned to the Certificate of Electronic Certificate of Electronic Invoice is the following:

- Online transaction protection.
- Legal proof of the electronic voucher.
- Integrity of Information.
- No repudiation
- Electronic signature of electronic documents.

9.6.1.9. Electronic Invoice Certificate Structure.

Campo del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado).
Número de serie:	(Identificador único 32 caracteres hexadecimales.)
Algoritmo de firma:	Sha-256RSA (Algoritmo de Firma)
DATOS DEL EMISOR	
CN	PSCPROCERT
O	Sistema Nacional de Certificación Electrónica
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Av. Libertador Multicentro Empresarial del Este piso 13 Oficina B-132 Torre Libertador Núcleo B
ST	Miranda
Periodo de validez	
Válido Desde:	(Inicio vigencia del certificado)
Válido Hasta:	(Expiración del periodo de validez del certificado).
Datos del titular	
CN	(Identificador del objeto)
T	(Ubicación) opcional
O	(Nombre de la organización)

OU	(Nombre de la unidad organizativa) opcional
OU	(Número de RIF)
C	(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave pública	
Algoritmo clave pública	RSA(Algoritmo con el que se generó la clave pública)
Tamaño clave pública	(2048)
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
Dns name	procert.net.ve
Other name	
OID 2.16.862.2.1	(Código del PSC PROCERT asignado por SUSCERTE
OID 2.16.862.2.2	RIF-J31635373-7 (RIF de PROCERT)
Identificador de clave del Titular	(Identificador de clave del titular)
Identificador de clave de autoridad certificadora	
Id. de clave	CN = Venezolano Autoridad de Certificación Subordinada del Estado Venezolano O = Sistema Nacional de Certificación Electrónica OU = Proveedor de Certificados PROCERT C.A.
Emisor de certificado	(Datos del emisor)
Número serie certificado	(Número de serial)
Uso de la clave	Firma electrónica, No Repudio, Cifrado.
Uso Mejorado de la clave	
nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cedula de identidad, pasaporte o RIF)

Punto distribución CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl http://www.procert.net.ve/lcr/PROCERTca.crl
Información del emisor	http://ura.procert.net.ve/ocsp
Política de certificados	http://www.procert.net.ve/dpc-pc/

9.6.1.10. Authorized use of electronic certificate of Electronic Invoice.

Use	Improved use
Electronic signature, no repudiation	N/A

9.6.1.11. Electronic Banking Electronic Certificate: The use assigned to the Electronic Banking Electronic Certificate is as follows:

- Authentication.
- Electronic Signature.
- Online transaction protection.
- Legal proof of the electronic voucher.
- Integrity of Information.
- No repudiation

9.6.1.12. Structure of the Electronic Banking Electronic Certificate.

CAMPO DEL CERTIFICADO	VALOR DEL CERTIFICADO
Versión	**V3** (Número de versión del certificado).
Número de Serie	(Identificador único del certificado. Menor de 32 caracteres hexadecimales.)
Algoritmo de Firma	**Sha-256RSA** (Algoritmo de Firma)
DATOS DEL EMISOR	
CN	PSCPROCERT
O	Sistema Nacional de Certificación Electrónico
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Chacao
ST	Miranda
PERIODO DE VALIDEZ	

Valido Desde	(Fecha en que el periodo de validez del certificado comienza).
Válido Hasta	(Fecha en que el periodo de validez del certificado culmina al cumplir 6 meses de vigencia).
DATOS DEL TITULAR	
CN	(Nombre del Representante Legal a Certificar)
T	(Cargo del Titular) dependiendo del tipo de certificado a instalar en el dispositivo móvil.
O	(Nombre de la Organización)
OU	(Nombre de la Unidad Organizativa) Opcional
C	(País)
E	(Correo Electrónico)
L	(Dirección)
ST	(Estado)
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo de Clave Publica	**RSA** (Algoritmo con el que se generó la Clave Publica)
Tamaño de Clave Publica	2048
EXTENSIONES	
Restricciones básicas	CA: False
NOMBRE ALTERNATIVO DEL EMISOR	
DNS Name	procert.net.ve
Other name	
OID 2.16.862.2.1	(Código de identificación de PROCERT acreditado asignado por SUSCERTE)
OID 2.16.862.2.2	**RIF-J31635373-7** (RIF de PROCERT)
Identificador de clave de Titular	(Identificador de clave del titular)
IDENTIFICADOR DE CLAVE DE AUTORIDAD CERTIFICADORA	
Id. de clave	(Identificador de la Clave)
Emisor de certificado	(Datos del emisor)

Número de serie del Certificado	(Número de Serial)
Uso de la Clave	Firma electrónica, No Repudio, Cifrado de Clave, Cifrado de Datos
NOMBRE ALTERNATIVO DEL TITULAR	
Other name	
OID 2.16.862.2.2	(Número de Cedula de Identidad o Pasaporte)
Punto de distribución de CRL	- http://ura.procert.net.ve/lcr/procertca.crl - http://www.procert.net.ve/lcr/procertca.crl
Acceso a la Información de la Entidad Emisora	http://ura.procert.net.ve/ocsp (Enlace al Servidor OCSP)
Política de certificados	http://www.procert.net.ve/dpc-pc/

9.6.1.13. Authorized Uses of the Electronic Banking Electronic Certificate.

Use	Improved use
Electronic Signature, Authentication, Integrity and Non-Repudiation.	N/A

9.6.1.14. Electronic certificate for virtual private networks (VPN)

The use assigned to the Electronic Certificate for Virtual Private Networks (VPN) is as follows:

- Protection of transactions in a Virtual Private Network.
- Protection of communications in a Virtual Private Network

9.6.1.15. Structure of the electronic certificate for virtual private networks (VPN)

Campo del certificado	Valor del certificado
Versión:	V3 (Número de versión del certificado)
Número de serie:	(Identificador único 32 caracteres hexadecimales.)
Algoritmo de firma:	Sha-256RSA. (Algoritmo de Firma)
Datos del emisor	
CN	PSCPROCERT

O	Sistema Nacional de Certificación Electrónica
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Av. Libertador Multicentro Empresarial del Este piso 13 Oficina B-132 Torre Libertador Núcleo B
ST	Miranda
Período de validez	
Válido desde:	(Inicio vigencia del certificado)
Válido hasta:	(Expiración del periodo de validez del certificado).
Datos del titular	
CN	(Dominio o Dirección IP)
O	(Organización Campo)
OU	(Unidad Organizacional) Campo Opcional
OU	(Número de RIF)
C	VE(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave publica	
Algoritmo de clave publica	RSAAlgoritmo con el que se generó la clave pública
Tamaño de clave publica	(2048) / (4096)
Extensiones	
Restricciones básicas	CA: false
Nombre alternativo del emisor	
DNS Name	procert.net.ve
Other Name	
OID 2.16.862.2.1	(Código del PSC PROCERT asignado por SUSCERTE)
OID 2.16.862.2.2	RIF-J31635373-7 (RIF de PROCERT)
Identificador de clave del Titular	(Identificador de clave del titular)
Identificador de clave de autoridad certificadora	

Id. de clave	Identificador de la clave
Emisor de certificado	(Datos del emisor)
Número de serie del Certificado	(Número serial)
Uso de clave	Firma electrónica, no repudio, cifrado de clave, cifrado
Uso mejorado de Clave	Seguridad IP y Cifrado
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de RIF)
Dirección IP	Dirección IP
Punto distribución CRL	http://ura.PROCERT.net.ve/lcr/PROCERTca.crl http://www.PROCERT.net.ve/lcr/PROCERTca.crl
Información del emisor	http://ura.PROCERT.net.ve/ocsp
Política de certificados	http://www.procert.net.ve/dpc-pc/

9.6.1.16. Allowed Uses

Type of certificate	**Use**	Improved use
Electronic certificate for virtual private networks (VPN)	Authentication, non-repudiation, key encryption	IP Security and Encryption

9.7. Third parties in good faith: Third parties in good faith are individuals or legal entities that rely on an electronic signature, electronic certificate, list of revoked certificates or information generated by PSC PROCERT and on which they may deposit their trust in accordance with the present document of the declaration of Certification Practices Statement (CPS) and Certificate Policy (CP). The public key infrastructure (PKI) of PSC PROCERT is contractually obligated, directly or indirectly (through chain of contracts) with all customers, suppliers and / or interested parties users of electronic signatures and electronic certificates generated by PSC PROCERT.

In order to belong to such a closed community and to place its trust in its services, it is required the consent of the clients (third parties of good faith), the conditions of the contract of acquisition of electronic signatures or electronic certificates generated by the PSCPROCERT.

10. Uses of certificates.

10.1. Allowed Uses: The use of the subordinate certificate of the PSC PROCERT shall be limited to the signing of electronic certificates for subordinate authorities, signing of revoked certificate lists and signing of all certificates established in this document. The use of the electronic certificates issued by the PSC PROCERT will be limited according to the type of certificate and was described in a previous way.

10.2. Uses not allowed: The contracting client of electronic signatures or electronic certificates generated by PSC PROCERT is obliged to use them according to the permitted uses and indicated in the previous section and those established by the decree with force of law on data messages and electronic signatures, its regulations and other current norms of sublegal character or any normative text that substitutes them and regulates the activity of electronic certification within the Bolivarian Republic of Venezuela and for the use for which it was acquired, being expressly indicated that any violation to the norms, uses and / or laws of the Bolivarian Republic of Venezuela is under the responsibility of the contracting client, as well as the damages and damages that will cause and in a whole will be applicable the provisions that for the effect are contained in the law of cybercrime and supplementary penal code and Venezuelan criminal proceedings.

The electronic certificate whose signatory violates the authorized use will be revoked. In addition, the contracting client assumes responsibility for compensating PSC PROCERT for damages caused to third parties arising from claims, actions, effects of action, losses or damages (including legal fines) that are generated by the improper use of the contracted service.

11. CA management policy: It is the policy and obligation of PSC PROCERT to maintain, document and inform customers about the generation of electronic certificates, in order to educate and inform customers of electronic certificates about the uses, applications, responsibilities and obligations of the PSC PROCERT, cycle of life certificates and information of interest associated with them, which allows to prevent potential fraudulent actions derived from false certificates issued by non-accredited entities and establish the conditions required to apply the trust model, with respect to electronic certificates issued by the PSC PROCERT.

11.1. Specifications of the administrative organization: The PSC PROCERT is organized as administrative and technical as follows:

- General Management to which they report:
- The technology consultant.

- Information Security and Compliance Consultant
- Auditor
- Computer operators.
- Registration authority (RA).
- The management staff.
- Outsourced services.

11.1.1. Detail of the administrative organization: Below is a detail of the functions of the different units that make up the administrative organization of the PSC PROCERT.

11.1.1.1. General Manager: The PSC PROCERT maintains within its design the position of General Manager, which is a managerial position in charge of the management, administration and supervision of the activities of the certification authority (CA) and the registration authority (RA), maintaining at all times the control of the administrative, operational and human resource management. The position of general manager can be filled by a company administrator, a process engineer, a lawyer or an economist or a senior management representative and reports directly to the top management of PSC PROCERT.

11.1.1.1.1. General Manager Responsibilities.

- Ensure compliance with company policies in the areas of information technology, administration and human resources.
- Maintain and update the technology standards applicable to the registration area.
- Maintain a positive management balance, which issues an exercise oriented to the economy and fulfill the expected and planned return in the business plan of the certification authority (CA) PROCERT.
- Prepare and submit to the approval of the senior management the annual budget of operation of the registration authority.
- Compliance with labor regulations and other social court laws that regulate the relationship between

the PROCERT registration authority (RA) and its workers.

- To maintain the institutional and operational relations and communications of the Registration Authority with SUSCERTE.
- To fulfill and enforce to the personnel the PROCERT registration authority (AR), the legal rules applicable to the subject of electronic certification and the legal framework applicable to the regular management of the certification authority (CA) and the registration authority (RA).
- Ensure the provision of services in compliance with the highest standards of quality, safety, timeliness, profitability, ethics and effectiveness aimed at customer satisfaction and achievement, based on safety and technology principles established by the legal framework and the company.
- To exercise the representation of the company in all its instances before governmental entities and of the different levels of government, judicial and administrative organs, representatives of the public and private productive sectors, regular companies with or without legal personality and individual subjects of law that realize commercial and legal activities within and outside the Bolivarian Republic of Venezuela.
- To exercise the disciplinary functions applicable to the personnel of the registration authority (RA) and certification authority (CA) of PROCERT.
- Approve the contracting of works and services, personnel, consumer goods and financial instruments.
- To fulfill and enforce the tax obligations imposed by the applicable legal framework within the Bolivarian Republic of Venezuela.
- Plan and implement the marketing and advertising management of the registration authority (RA) and certification authority (CA) of PROCERT.

- Plan and establish the development and training plan applicable to the personnel of the registration authority (RA) and certification authority (CA) of PROCERT.
- Plan and establish the remuneration plan applicable to the personnel of the registration authority (RA) and certification authority (CA) of PROCERT.
- Comply and enforce the guidelines and obligations imposed by the Organic Law on Prevention, Conditions and Working Environment (LOPCYMAT).
- Maintain updated and effective management guidelines and controls applicable to the regular operation of registration authority (RA) and certification authority (CA) of PROCERT.
- Encourage and design new business initiatives that foster and encourage the use of new technologies.
- To foster, promote and consolidate strategic partnerships with other registration authorities (RA) and certification authority (CA), in order to establish cross-recognition of data supporting electronic certificates between different entities or Certification Authorities
- Approve payments and requests for suppliers.
- Comply with the guidelines of the High Management of the PSC PROCERT.
- Manage and Manage the Cloud Services Schema.
- Execute the activities inherent to certification authority (CA).

11.1.1.2. Technical Consultant: PSC PROCERT maintains within its design the position of technology consultant, which is a managerial position in charge of the management, administration and supervision of the activities of the certification authority (CA). The technology consultant maintains the operational and human resource control of the certification authority (CA). The position of

technology consultant may be filled by a Systems Engineer or Computer Engineer, and report directly to the General Manager.

11.1.1.2.1. Responsibilities of technology consultant.

- Plan, coordinate and manage the technological infrastructure of the personnel assigned to the certification authority (CA) in accordance with the strategic guidelines of PSC PROCERT, in order to obtain the greatest use of the technological resources and provide solutions of information systems that the organization requires, ensuring timely service with security, quality and optimal management of resources.
- Guarantee an optimum operation of the technological platform that supports the certification authority (CA) through the establishment of an updated, efficient and economically sustainable information infrastructure.
- Ensure the availability and protection of the data, so that it can comply with the legal requirements and the requirements imposed by SUSCERTE.
- Provide reliable and secure information to senior management and general manager on trends and best practices in computing resources and to facilitate decision making at these levels and support them.
- Identify and propose improvements applicable to the certification authority (CA) through the use of information technology available in the market, contributing to the satisfaction of internal and external customers.
- To seek high yields of the computer tool, guaranteeing reliable and quality operation that results in an excellent quality of service and produce greater income to the company.
- Guarantee to the client a service with the highest standards of quality, safety, opportunity, profitability, ethics and efficiency oriented to the achievement and satisfaction of the client, based on safety and

technology principles established by the legal framework and the company.

- Ensure compliance with company policies in the areas of information technology, administration and human resources.
- Maintain and update the technology standards applicable to the registration area.
- Together with the general management, comply with the labor regulations and other social court laws that regulate the relationship between PSC PROCERT and its workers
- Together with the general management, comply and enforce the personnel of the certification authority (CA) with the legal rules applicable to the subject of electronic certification and the legal framework applicable to the regular management of the certification authority (CA).
- To fulfill and enforce the tax obligations imposed by the applicable legal framework within the Bolivarian Republic of Venezuela.
- Together with the general management, plan and establish the remuneration plan applicable to the personnel of the certification authority (CA).
- Comply and enforce the guidelines and obligations imposed by the Organic Law on Prevention, Conditions and Working Environment (LOPCYMAT).
- Maintain up-to-date and current guidelines and management controls applicable to the regular operation of the certification authority (CA).
- Comply with the guidelines of the senior management and general manager of PSC PROCERT.
- Manage and Manage the Cloud Services Schema.
- Execute the activities inherent to certification authority (CA) for authorization.

11.1.1.3. Information Security and Compliance Consultant: PSC PROCERT maintains in its design the position of Consultant of

Information Security and Compliance, which is a position in charge of ensuring compliance with and establishing best practices in the area of security of information, and compliance with the national and international standards applicable to the operation of Certification Authorities. The position of Information Security and Compliance Consultant may be occupied by a Systems Engineer, Computer Engineer or IT Technician with a background in the subject, and report directly to the General Manager.

11.1.3.1.1. Responsibilities of the Information Security and Compliance Consultant.

- Plan, coordinate and establish compliance with best practices in information security, in accordance with the strategic guidelines of PSC PROCERT, in order to obtain the greatest use of technological resources and provide solutions of information systems that the organization requires, ensuring timely service with security, quality and optimal management of resources.
- Ensure the availability and protection of the data, so that it can comply with the legal requirements and the requirements imposed by SUSCERTE.
- Provide reliable and secure information to senior management of the company and general manager about IT trends and best practices and to facilitate decision making at these levels and support them.
- Identify and propose applicable improvements in information security and compliance with standards and standards applicable to the Certification Authority (CA) and Registration Authority (RA) through the use of available computer technology in the market, contributing to the satisfaction of internal and external customers.
- Achieve high performance of the IT tool, guaranteeing reliable, safe and quality operation that results in an excellent quality of service and produce higher income for the company.
- Guarantee to the client a service with the highest standards of quality, safety, opportunity,

profitability, ethics and efficiency oriented to the achievement and satisfaction of the client, based on safety and technology principles established by the legal framework and the company.

- Ensure compliance with company policies regarding IT security, administration of international norms and standards and compliance with them.
- Maintain and update the technology standards applicable to the Certification Authority (CA) and Registration Authority (RA).
- Together with general management, comply with the regulations of information security and regulatory compliance.
- Together with the general management, comply and enforce the PSC PROCERT personnel with the legal norms, standards and principles of information security.
- Together with general management, plan the training of personnel in information security and regulatory compliance.
- Comply and enforce the guidelines and obligations imposed by the standards, standards and national and international legislation that regulates the operation of the PSC PROCERT.
- Maintain current and current guidelines and management controls applicable to the regular operation of the certification authority (CA).
- Comply with the guidelines of the senior management and general manager of PSC PROCERT.
- Monitor the cloud services schema.
- Execute the activities inherent to the position.

11.1.1.4. In charge of RA: The PSC PROCERT maintains within its organizational design a person in charge of the validation of the data and identity accreditation of the signatories. The position may be occupied by a Licensed Administrator, Public Accountant or Lawyer and report directly to the General Manager of the Certification Authority (CA) of PSC PROCERT.

11.1.1.4.1. Responsibilities of the RA.

- Verify that the signatories send all necessary documentation according to the type of electronic certificate they wish to acquire.
- Validate that the information provided by the signatory is correct.
- To accredit all those signatories that comply with the requirements established by the PSC PROCERT.
- Identify and propose improvements in the accreditation process, in order to facilitate the accreditation process of the signatories.
- Comply with company policies in the areas of information technology, administration and human resources.
- Comply with the labor regulations and other laws of social court that regulate the relationship between the PSC PROCERT its workers.
- Comply with the legal rules applicable to the subject of electronic certification and the legal framework applicable to the regular management of PSC PROCERT.
- Comply with the guidelines and obligations imposed by the Organic Law of Prevention, Conditions and Working Environment (LOPCYMAT). Comply with the guidelines and management controls applicable to the regular operation of the PSC PROCERT.
- Comply with the guidelines of the senior management and general manager of PSC PROCERT.
- Create in system to the users whose documentation and identity are proven.

11.1.1.5. Auditors: The PSC PROCERT contemplates the internal audit process within its processes and in order to guarantee the timely compliance with the standards, norms, legislation and internal policies that regulate the operation of the PSC PROCERT.

The position of Auditor should be occupied by a systems engineer or a senior computer technician and report directly to the general manager.

11.1.1.5.1. Responsibilities of the Auditors:

- Verify that internal processes and results of external audits are complied with and executed.
- Validate that the information provided by the signatories to the Registration Authority is correct.
- Identify and propose improvements in the internal processes of PSC PROCERT.
- Comply with company policies in the areas of information technology, administration and human resources.
- Comply with labor regulations and other laws of social court that regulate the relationship between the PSC PROCERT its workers.
- Comply with the legal rules applicable to the subject of electronic certification and the legal framework applicable to the regular management of the PSC PROCERT.
- Comply with the guidelines and obligations imposed by the Organic Law on Prevention, Conditions and Working Environment (LOPCYMAT). Comply with the guidelines and management controls applicable to the regular operation of PSC PROCERT.
- Comply with the guidelines of the senior management and general manager of PSC PROCERT.

11.1.1.6. Computer Operators: The PSC PROCERT maintains within its organizational design a working group conformed by the computer operators which can be assigned to the management and operation of the registration authority (RA) and certification authority (CA) of PSC PROCERT. Computer operators maintain control and monitoring of certification authority (CA) data.

The position of computer operator should be filled by a systems engineer or top computer technician and report directly to the technology consultant and general manager.

11.1.1.6.1. Responsibilities of computer operators.

- Operate the certification authority (CA) infrastructure. in order to obtain the greatest use of technological resources and provide solutions of information systems that the organization requires, ensuring timely service with security, quality and optimal management of resources.
- Support the technology consultant in order to ensure an optimal functioning of the certification authority (CA). through the establishment of an updated, efficient and economically sustainable information infrastructure.
- Support the technology consultant in order to ensure the availability and protection of the data, so that it can comply with the legal requirements and the requirements imposed by the SUSCERTE.
- Provide reliable and secure information to the technology consultant, general manager and senior management on trends and best practices in data entry, computer resources and to facilitate decision making at these levels and to support same.
- Identify and propose improvements applicable to the certification authority (CA) through the use of information technology available in the market, contributing to the satisfaction of internal and external customers.
- To seek high yields of the computer tool, guaranteeing reliable and quality operation that results in an excellent quality of service and produce greater income to the company.
- Guarantee to the client a service with the highest standards of quality, safety, opportunity, profitability, ethics and efficiency oriented to the achievement and satisfaction of the client, based on safety and technology principles established by the legal framework and the company.
- Comply with company policies in the areas of information technology, administration and human resources.

- Meet and assist the technology consultant and general manager to keep up to date the technology standards applicable to the area of identity registration.
- Comply with labor regulations and other social court laws that regulate the relationship between the certification authority (CA) and its workers
- Comply with the legal rules applicable to the subject of electronic certification and the legal framework applicable to the regular management of the certification authority (CA).
- Comply with the guidelines and obligations imposed by the Organic Law of Prevention, Conditions and Working Environment (LOPCYMAT).
- Comply with the guidelines and management controls applicable to the regular operation of the registration authority (RA) and the certification authority (CA).
- Support the technology consultant and general manager in the promotion and development of new business initiatives that encourage and encourage the use of new technologies.
- Comply with the guidelines of the senior management, the general manager and the technology consultant.
- By delegation of the technology consultant or general manager and only in case of contingency, support the registry authority in the creation of the electronic file corresponding to the documentation delivered by the clients.

11.1.1.7. Administrative assistant: The PSC PROCERT maintains within its organizational design a position of administrative assistant who is in charge of assisting the general management in the regular administrative management of PSC PROCERT. The administrative assistant is in charge of the management of payment procedures for products and services required by PSC PROCERT and keep the management up to date with customers and suppliers.

The position of administrative assistant should be occupied by a superior technician in administration or marketing and marketing, and report directly to the manager.

11.1.1.7.1. Description of responsibilities:

- Comply with company policies in the areas of information technology, administration and human resources.
- Comply with labor regulations and other social court laws that regulate the relationship between PSC PROCERT and its workers
- Comply with the legal rules applicable to the subject of registration of identity and the legal framework applicable to the regular management of PSC PROCERT.
- Ensure the provision of services in compliance with the highest standards of quality, safety, timeliness, profitability, ethics and effectiveness aimed at customer satisfaction and achievement, based on safety and technology principles established by the legal framework and the company.
- Processing payments and requests for suppliers.
- To fulfill and enforce the tax obligations imposed by the applicable legal framework within the Bolivarian Republic of Venezuela.
- Support the General Management in the advertising management of PSC PROCERT.
- Comply with the guidelines and obligations imposed by the Organic Law on Prevention, Conditions and Working Environment (LOPCYMAT).
- Comply with the guidelines and management controls applicable to the regular operation of the PSC PROCERT.
- Comply with the guidelines of the senior management of the authority and general manager of the PSC PROCERT.

11.2. Contact person: The present Certification Practices Statement (CPS) and Certificate Policy (PC) document is administered by the senior management and general manager of PSC PROCERT. Questions or other communications about this document and regarding the operation and generation of PSC PROCERT certificates should be addressed to: Certificate Supplier (PROCERT), C.A. Multicentro Empresarial del Este, Nucleus B, Torre Libertador, Pio 13, Office B-132, Chacao Municipality, Caracas. E-

mail: contacto@procert.net.ve, Postal Code 1063, Telephone number: + 58-0212-2674880, Fax: + 58-0212-2671270.

11.3. Competence to determine the adequacy of CPD to policies: The top management of the PSC PROCERT is in charge of validating and conforming the adequacy of the CPS to the different operating and certification policies required for the operation of a PSC. In any case, the validation carried out by the senior management of PSC PROCERT regarding the adequacy of the CPS to the different policies of operation and generation of certificates will be subject to review and approval by the SUSCERTE.

12. Publication of PSC information and certificate repositories.

12.1. Repositories: In order to ensure the complete availability of this document from the Certification Practices Statement (CPS) and Certificate Policy (PC) document, and other essential documents, PSC PROCERT maintains a repository within its Website:http://www.procert.net.ve/. For the certificate of the PROCERT Subordinate CA, the certificates issued by said CA and the CPS:

- https://www.procert.net.ve/ac.html
- For the list of Revoked Certificates
  https://ura.procert.net.ve/lcr/procertca.crl
  http://www.procert.net.ve.ve/lcr/procertca.crl
- For the online validation service (OCSP)
  http://ura.procert.net.ve/ocsp The PSC PROCERT public repository does not contain any confidential or private information.

12.2. Publication: It is the obligation of PSC PROCERT to publish the information regarding its practices, its certificates and the updated status of said certificates. The publications made by PSC PROCERT, of all information classified as public, will be announced on their respective website as follows:

- The list of Certification Revoked List (CRL) is available in CRL V2 format, in
  https://ura.procert.net.ve/lcr/procertca.crl
- This document is available on:
  https://www.procert.net.ve/ac.html
- The PROCERT Subordinate CA certificate is available at:
  https://www.procert.net.ve/ac.html
- The certificates issued by the PROCERT Subordinate CA are in:
  https://www.procert.net.ve/ac.html
- The contact data of the PSC PROCERT at the address:
  https://www.procert.net.ve/index.html#contacto

– The PSC PROCERT technical documentation at the address: https://www.procert.net.ve/ac.html

12.3. Frequency of publication.

12.3.1. PSC Certificates: The publication of the certificate will be made once the accreditation has been obtained by SUSCERTE. The period of validity is ten years.

12.3.2. List of certificate revoked list (CRL): Publishing the revoked certificate list is done every 24 hours.

12.3.3. Declaration of certification practices: Unless explicitly stated otherwise in this Certification Policy and Certification Practices Statement (CPS) policy document, new versions of this document will be posted on the PSC PROCERT website (www.procert.net.ve) document, once they are approved by the top management of PSC PROCERT and SUSCERTE.

13. Certificate repository access controls: Access to information published by PSC PROCERT will be consulted and may not be modified by unauthorized persons. The public information will only be updated by the personnel in charge of this function that works in the PSC PROCERT. In addition, the CRL is consulted on the issued certificates, the OCSP server and the present document.

14. Identification and authentication.

14.1. Types of names: The PSC PROCERT only generates and signs name certificates according to the standard x 500.

For PSC PROCERT: The distinguishing name (DN) of the PSC PROCERT consists of the following attributes:

- CN: PSCPROCERT
- O: National Electronic Certification System.
- OU: PROCERT Certificate Provider
- C: VE.
- E: contacto@procert.net.ve
- L: Chacao
- S : Miranda

The alternative name (AN) of the PSC PROCERT consists of the following attributes:

- DNSName: procert.net.ve.
- otherName:
- OID 2.16.862.2.1. (PROCRC accredited PSC identification code)

- OID 2.16.862.2.2.: RIF J- 31635373-7

For Signatories: The distinguishing name (DN) of the signatory is formed by the following attributes**:**

- CN: (Name of owner)
- O: (Organization name's).
- C: VE.
- E: (email)
- L: Municipality
- S: State

The alternative name (AN) of the signatory is formed by the following attributes:

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

14.2. Need for meaningful names: The PSC PROCERT will require of the contracting clients of electronic signatures or certificates their full name and surnames and conform they are represented in the identity card laminated that owns the applicant of the electronic signature or certificate.

The data corresponding to diminutives of names, aliases or pseudonyms with which the customer is to be identified will not be admitted or processed by the registration authority (AR).

In the case of indigenous populations, the names on their identity card or passport will be considered. In any case, the PSC PROCERT guarantees that the DN contained in the fields of the certificates are sufficiently distinctive and significant enough to be able to link the identity of a client to its signature or electronic certificate.

14.3. 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). In addition, all certificates issued by PSC PROCERT use UTF8 encoding for all attributes, according to RFC 6818 ("Internet X.509 Public Key Infrastructure and Certificate Revocation List (CRL) Profile").

14.4. Uniqueness of names: The Certification Authority of SUSCERTE defines as DN field of the certificate of authority as unique and unambiguous. To this end, the name or corporate name of the PSC PROCERT will be included as part of the DN, specifically

in the OU field, therefore, uniqueness is guaranteed by the trust on the uniqueness of the commercial names in the national registry.

Additionally, and with regard to customers; if a client holds a contract and has acquired more than one type of electronic signature or certificate, the PSC PROCERT database shall maintain a uniform and equal scheme of contracting client data and shall not be permitted or processed by the Registration Authority (RA) of the PSC, dissimilar personal data and corresponding to the same client.

14.5. Conflict resolution regarding names: In the event of an occurrence of name conflict between clients and that corresponds to the same name and surnames, the registration authority (RA) of the PSC PROCERT will proceed to distinguish the identity and authentication of the same through the use of the number identity card and personal RIF of each client of the PSC PROCERT with which the name conflict was generated.

15. Initial validation of identity.

15.1. Private Key Possession Test Method: The PSC PROCERT operating scheme and its technological certification platform are configured so that the client generates its key pair (public and private).Accordingly, once each certificate is issued, it is the customer who has the custody and safekeeping of his private key, presuming that he owns it and protects himself according to the law, unless denounced by the same client of commitment of his private key, in which case the corresponding electronic signature or certificate will be revoked.

15.2. Authentication of the identity of an organization: The registration authority (RA) of PSC PROCERT in the case of electronic signatures accrediting companies or public entities will proceed as follows:

15.2.1. Public entity: The registration authority (AR) will proceed to verify the publication in the official gazette of the Bolivarian Republic of Venezuela of the resolution that creates the entity or public company. Every electronic certificate of organization must be associated with a human responsible for said certificate. The registration authority (AR) of PSC PROCERT will follow the verification and verification of identity and representation.

Once verified the identity of the organization and the powers of representation will proceed to validate the rest of the information requested by the contracting system of PSC PROCERT and successfully completed the procedure, the registration authority (RA) will communicate to the certification

authority (CA) of the PSC PROCERT, its conformity with the data to proceed with the generation of the electronic certificate contracted by the customer.

15.2.2. Private entity: The registration authority (RA) will verify the existence of the private company through the revision of its constitutive-statutory document, duly registered in the commercial registry office corresponding to the judicial district of the domicile of the Private company, as the publication of the business register in a business journal. Every electronic certificate of organization must be associated with a human responsible for said certificate. The registration authority (AR) of PSC PROCERT will follow the verification and verification of identity and representation.

Once verified the identity of the organization and the powers of representation will proceed to validate the rest of the information requested by the contracting system of PSC PROCERT and successfully completed the procedure, the registration authority (RA) will communicate to the certification authority (CA) of the PSC PROCERT, its conformity with the data to proceed with the generation of the electronic certificate contracted by the customer.

15.3. Verification of powers of representation: The registration authority (RA) of PSC PROCERT in the case of electronic signatures that accredit the representation of companies will proceed as follows:

15.3.1. Public entity: The registration authority (RA) will proceed to verify the publication in the official gazette of the Bolivarian Republic of Venezuela of the resolution that creates the entity or public company. Subsequently validate the publication in the official gazette of the Bolivarian Republic of Venezuela of the normative or statutory body that indicates the functions and attributions of the representative of the public body and delimits its exercise of function. Subsequently, the registration authority (AR) of PSC PROCERT will validate the publication in the official gazette of the Bolivarian Republic of Venezuela of the designation in charge of the representative of the public entity or company.

Once verified the powers of representation will proceed to validate the rest of the information requested by the contracting system of PSC PROCERT and successfully completed the procedure, the registration authority (RA) will communicate to the certification authority (CA) PSC PROCERT, their conformity with the data for the generation of the electronic certificate contracted by the customer.

15.3.2. Private entity: The registration authority (RA) will verify the existence of the private company through the revision of its Constitutive-Statutory document, duly registered in the commercial registry office corresponding to the judicial district of the domicile of the private company, as the publication of the business register in a commercial newspaper.

Subsequently, they will be validated with a view to the constitutive document of the private company or the assemblies that have modified it, the functions and attributions of the representative of the private company and its duration in charge. Subsequently, the registration authority (RA) of the PSC PROCERT will validate the appointment in a position held at an ordinary or extraordinary meeting of the private company, duly registered and published in the corresponding commercial registry office and subsequently published in a commercial newspaper.

Once verified the powers of representation will proceed to validate the rest of the information requested by the contracting system of PSC PROCERT and successfully completed the procedure, the registration authority (RA) will communicate to the certification authority (AC) PSC PROCERT, their conformity with the data for the generation of the electronic certificate contracted by the customer.

15.4. Criteria for operating with external AC: The operation with certification authorities (CA) external to PSC PROCERT is not regulated or developed by SUSCERTE. However, the decree law on data messages and electronic signatures, if it contemplates this possibility, leaving open the possibility of establishing schemes of operation with external certification authorities once you have the regulations that regulate the subject.

16. Identification and authentication of applications.

16.1. Suspension or revocation of key: Under the operating scheme of PSC PROCERT and its technology certification platform, the client generates its key pair (public and private) and that is why the commitment of the client's private key will obligatorily produce the need to revoke the generated certificate for that client.

Suspension of electronic signatures or certificates generated by the certification authority (CA) usually precedes revocation and where such revocation proceeds shall be done according to the specific procedures described in apart.

16.1.1. Circumstances for suspension.

16.1.1.1. The Client's Private Key has been lost, has been revealed without authorization, has been stolen or compromised in any way.

16.1.1.2. The security, trust, and integrity of the public key infrastructure (ICP) is materially affected by the private key commitment of PSC PROCERT.

16.1.1.3. An improper or defective issuance of a certificate has occurred because:

16.1.1.3.1. A material prerequisite for issuing the certificate was not met;

16.1.1.3.2. A material fact is known in the certificate, or reasonably believed to be false.

16.1.1.4. Any other circumstance requiring investigation to ensure the security, integrity or trust of the public key infrastructure (PKI).

16.1.1.5. The result of the investigation will be the order of the senior management or general manager to produce a request for suspension or a decision to proceed with the suspension.

16.1.2. Who can request a suspension or revocation?: A Suspension or revocation may be requested by the following entities:

16.1.2.1. The owner of the certificate or a representative with express power to execute suspensions or revocation requests.

16.1.2.2. A PROCERT representative who has explicitly been given authority to make suspensions or revocation requests.

16.1.2.3. The decision of a court by which a precautionary or executory decision is declared enforceable requesting the suspension or revocation of an electronic signature or certificate issued by PROCERT.

16.1.2.4. A valid request for suspension or revocation received from any of the aforementioned entities will result in an immediate suspension and the initiation of a post-suspension investigation to determine whether a revocation will follow the suspension or whether the suspension should be lifted.

16.1.2.5. The suspension or revocation of an electronic signature or certificate may also be requested by the General Management and Information Technology Management.

16.1.2.6. A request for suspension of senior management or general management will result in the immediate suspension of the electronic signature or certificate and at the beginning of a post-suspension investigation.

16.1.3. Limits of the suspension period: The electronic signatures or certificates issued by the Certification Authority (CA) certification root shall remain suspended for a maximum of twenty (20) days. Upon termination or prior to termination, PROCERT will determine whether the certificate should be revoked or re-established as valid.

16.1.4. Procedure for requesting suspension: To process a suspension request for the PSC PROCERT certification root, you will do the following:

16.1.4.1. Suspend the certificate, record the reason for the suspension and keep the relevant documentation.

16.1.4.2. Notify the Client of the suspended certificate, stating the details of the certificate and the date and time of the suspension.

16.1.4.3. Continue safeguarding the public key associated with the certificate suspended until the expiration date of the Certificate, at which time it must be destroyed.

16.1.4.4. Notify (where appropriate) their subordinate public-key infrastructure (PKI) in a timely manner, suspension of its certificate.

16.1.5. Circumstances for Revocation: An electronic signature or certificate issued by the Certification Authority (CA) certification root in all cases shall be revoked by a certificate revocation request issued by senior management or general management and only in the following cases:

16.1.5.1. When after going through the entire suspension procedure it is determined that a revocation is required due to material circumstances that are being investigated in the post-suspension investigation that warrants the revocation of the certificate;

16.1.5.2. When the PSC PROCERT senior management requests the revocation of a certificate regardless of whether the post-suspension investigation has been carried out.

16.1.6. Procedure for requesting revocation: To process a revocation request for the PSC PROCERT certification root, you will do the following:

16.1.6.1. It will revocate the certificate, record the reason for the revocation and keep the relevant documentation.
16.1.6.2. It will immediately generate an CRL (certificate revocation list).
16.1.6.3. It will notify the Client of the revoked certificate, indicating the details of the certificate and the date and time of the revocation.
16.1.6.4. Continue to safeguard the public key associated with the revoked certificate until the expiration date of the Certificate, at which time it must be destroyed.
16.1.6.5. Notify (where appropriate) their subordinate public-key infrastructure (PKI) in a timely manner, revocation of its certificate.

16.1.7. Request for revocation and / or suspension: The revocation or suspension of certificates is made when the person (natural or legal) has ceased to exist or ceased in the activities for which the certificate is granted, also, applies in case the security of the private key has been seen engaged.

The revocation or suspension of an electronic certificate may be made by the owner of the certificate or at the request of the senior management or general manager of the PSC PROCERT. To make the request for suspension or revocation you must follow the following steps:

Step 1: Notification of the suspension or revocation, clearly indicating the reasons, using any of the following means:
Master Telephone: **(58-212) 267.48.80**
Fax: **(58-212) 267.12.70**
E-mail para revocación: soporte@procert.net.ve

Step 2: Ratification face-to-face of the request for revocation or suspension: The signatory must be identified before the registration authority (RA) and ratify the revocation or suspension of the certificate.

16.1.8. Revocation request grace period: Requests for revocation must be processed within twenty-four (24) hours of receipt of a final decision from the certification authority (CA) certification root, to revoke a certificate in accordance with the PSC PROCERT operational procedures.

16.2. From the renewal of the key.

16.2.1. Routine: The identification and authentication for the renewal of the certificate must be made using the techniques for authentication and initial identification.

16.2.2. Key after a renewal - uncommitted key: The PSC PROCERT operating scheme and its certification technology platform are configured so that the client generates its key pair (public and private). Always and in any case the key commitment will derive from the same client as the PSC PROCERT does not generate the pair of keys (public and private).

The identification and authentication for the renewal of a certificate after a noncommittal revocation of the key will be the same as for the initial registration. Additionally, the signatory must satisfactorily demonstrate to PSC PROCERT that the causes of the previous revocation are no longer present.

17. Life cycle of PSC certificates: The electronic signatures and certificates generated by PSC PROCERT have a life cycle of one (1) year from the date of activation of the signature or electronic certificate by the certification authority (CA).

17.1. Request certificates: Customers interested in acquiring an electronic signature or certificate generated by PSC PROCERT must enter the PSC PROCERT website (www.procert.net.ve) and access the "Certificate purchase" link, select the type of certificate, accept the contracts, attend the interview with the registration authority (RA) of the PSC PROCERT, generate their keys and finally download their signature or electronic certificate.

17.1.1. Process of generating the request for certificates and responsibilities: The contracting client, once completed and completing the process of contracting the electronic certificate of his preference on the PSC PROCERT website (www.procert.net.ve), must send to the PSC PROCERT postal box the information required in each one of the windows of the contracting system of PSC PROCERT. Subsequently, it must go to the administrative offices of PSC PROCERT in order to comply with the assistance to the interviewed by the registration authority (RA) for the purpose of validating the data of the requesting client, whether natural or juridical person.

If the client does not attend the interview set by the registration authority (RA), it will be understood that he / she desists of his / her request and will proceed to impose the charge of penalty referred in the contracting system of PSC PROCERT.If the client notifies him of his inability to attend the established

date, he will be given a new opportunity. If the client does not attend the re-set date, it will be understood that he / she desists of his / her request and will proceed to impose the charge of penalty referred in the contracting system of PROCERT. Through this procedure there is an interaction between the certification authority (CA) and the registration authority (RA) since the procedure described above has to be performed before the CA can approve the certificate that the client requested. of the PSC registration authority (RA) PROCERT allows you to manage the certificate requests and send them to the certification authority (CA) module.

17.1.2. Certificate signing process: The PSC PROCERT, once validated the identity of the signatory must approve from the certification system the issuance of the certificate for the signature of the same, the process is as follows:

- The RA Manager notifies the technology consultant and the general manager of the approval of the application and approves the certificate using the PROCERT certification system.
- The technology consultant and the general manager activate the HSM and the certification server locally, and simultaneously approve the signing of the electronic certificate.

17.1.3. Process for the generation of the request for renewal of the certificate keys: The process for the renewal of a certificate will be the same as for the initial registration.

17.1.4. Procedure for making a request for revocation of a certificate: The revocation or suspension of certificates is made when the person (natural or legal) has ceased to exist or ceased in the activities for which the certificate is granted, also, applies in case the security of the private key has been seen engaged. The revocation or suspension of an electronic certificate can be made by the owner of the certificate or The senior management or general manager of the PSC PROCERT.

To make the request for suspension or revocation you must follow the following steps:

Step 1: Notification of the suspension or revocation, clearly indicating the reasons, using any of the following means:
Master phone: (58-212) 267.48.80

Fax: (58-212) 267.12.70
E-mail for Revocation: soporte@procert.net.ve
E-mail for suspension: soporte@procert.net.ve

Step 2: Face-to-face ratification of the request for revocation or suspension: The subscriber must identify himself / herself before the registration authority (RA) of PSC PROCERT and ratify the revocation or suspension of the certificate.

18. Processing of application for a certificate.

18.1. Performing identification and authentication functions: The identification and authentication functions of the clients that choose to purchase a signature or certificate are assigned to the registration authority (RA) of the PSC PROCERT. The detailed explanation of the functions and attributes of the registration authority (RA) of the PSC PROCERT are detailed in section 8.3.1 and 14 of this document of the certification practice statement (CPS) and certificate policy (CP).

18.2. Approval or denial of a certificate: The approval or denial of an electronic signature or certificate is assigned to the certification authority (CA) of PSC PROCERT. Any request for an electronic signature or certificate that is not validated by the registration authority (RA) of the PSC PROCERT will automatically be rejected and consequently denied.

The certification authority prior to initiating the approval process of an electronic signature or certificate will validate compliance with the following conditions:

18.2.1. Validate the payment made by the customer
18.2.2. Validate the report issued by the registration authority (RA)
18.2.3. Validate the type of certificate requested and process before the Universal Register Authority (URA), which is the certificate generation module.

Once verified and fulfilled to the satisfaction of the indicated steps, the certification authority (CA) of PSC PROCERT will proceed to generate the electronic signature or certificate and as the case may be.

18.3. Deadline for the processing of a certificate: The deadline for the processing and purchase process of the electronic signature or certificate selected by the client will depend to a great extent on the information provided by the same client and his / her attendance at the validation interview with the registration authority PSC PROCERT. If the interviewing authority determines that the client meets the requirements

established by the PSC PROCERT, it will inform the certification authority (CA) to proceed with the generation and signature of the electronic signature or certificate, according to correspond.

The period established by the PSC PROCERT for the approval and signing of the certificates is three (3) continuous days after the interview of validation of identity and data with the registration authority (RA) of the PSC PROCERT. The certification authority (CA) of PSC PROCERT will generate and sign the certificates within the said period and notify the client, so that the client can download and install the electronic signature or certificate.

19. Certificate issuance.

19.1. CA actions during issuance of a certificate: The PSC PROCERT is responsible for generating the certificates acquired by customers. Subsequent to the approval by the registration authority (RA) of the PSC PROCERT, the module manager of the Certification Authority (CA) approves and approves the issuance of the certificate; it is at this point where the certification application communicates via https with the certification authority (CA) and requests the signing of the public key of the certificate.

The certification authority (CA) signs the certificate and sends it to the certification application using the https communication as well. After issuing the certificate the signatory can download it and proceed with its installation.

19.2. Notification to the applicant by the CA about the issuance of its certificate: The certification authority (CA) of PSC PROCERT is responsible for notifying the client via email about the generation of his signature or electronic certificate and the steps that he must follow for the installation of the electronic signature or certificate, as appropriate. The AC system issues an automatic email, which is sent to the customer's email account.

20. Using the key pair and certificate.

20.1. Using the certificate's private key: Key delivery to customers is not performed and will not be delivered as each customer will generate their own key pair (public and private). The holder can only use the private key and the certificate for authorized uses in this CPS.

The client is solely responsible for the custody and care of his private key and must report to PSC PROCERT about the commitment of the client's private key, without prejudice to personally responding to the actions and consequences arising from the misuse of his signatures or certificates electronic communications by third parties.

20.2. Use of public key and certificate by third parties in good faith: The Certification Authority (CA) certification root certificate is made public for the purpose of validating the route. The certificate trace and public key infrastructure (PKI) certificates of the PROCERT certification authority (CA) are available on the PROCERT Web page (www.procert.net.ve).
Third parties in good faith must confirm the validity of copies of their certificates of the public key infrastructure (PKI) of the PROCERT certification authority (CA) using these footprints. The uses assigned to the certificates are defined in section 9 above of this certification practice statement (CPS) and certificate policy (CP).

21. Certificate renewal with key change.

21.1. Causes for the renewal of a certificate: Any electronic signature or certificate generated by PSC PROCERT may be renewed, provided that the following conditions are met:

21.1.1. That the term of validity of the electronic signature or certificate of which it is the owner has been fulfilled.

21.1.2. That the electronic signature or certificate has not been revoked by PSC PROCERT for reasons of illegal use of the electronic signature or certificate, as applicable.

21.1.3. That the applicant complies with the process of contracting PSC PROCERT and validation by the Registration Authority (RA) of PSC PROCERT.

21.2. Entity that can request the renewal of a certificate: Any owner of an electronic signature or certificate generated by PSC PROCERT that complies with the requirements requested by PSC PROCERT, may request from PSC PROCERT the new issue or generation of the electronic signature or certificate, as appropriate, unless there is a prohibition or express mandate contained in a final judgment and indicating the prohibition on issuing certificates to the applicant.

21.3. Application procedure for renewal of a certificate: Customers interested in renewing an electronic signature or certificate generated by the PSC PROCERT, must log on to the PROCERT website (www.procert.net.ve) and access the "certificate purchase" link, select the type of certificate, accept the contracts, enter your personal data, attend the interview with the registration authority (RA) of PSC PROCERT, generate your keys and finally download your signature or electronic certificate.

21.4. Notification of the issue of a new certificate to the RA: The certification authority (CA) of PSC PROCERT is responsible for notifying the client via email about the

issuance of a new electronic signature or certificate and the steps that must be followed for the installation of the electronic signature or certificate, as applicable

21.5. Publication of the certificate renewed by the CA: The certification authority (AC) PROCERT has a repository of all certificates issued and renewed both on its certification server and on a redundant database.
Access to the repository of the issued certificates is public and can be done by the clients, suppliers or interested parties through the PSC PROCERT website (www.procert.net.ve), accessing the "Issued Certificates" link and entering the data corresponding to the type of signature or electronic certificate and the name or surname of the client that owns the electronic signature or certificate.

21.6. Notification of the issuance of the certificate by the CA to other entities: The operation with certification authorities (CA) external to PSC PROCERT is not regulated or developed by SUSCERTE. However, the decree law on data messages and electronic signatures, if it contemplates this possibility, leaving open the possibility of establishing schemes of operation with external certification authorities once you have the regulations that regulate the subject.

22. Certificate Modification: The electronic signatures or certificates generated by PSC PROCERT must maintain their integrity during their period of validity and may not be subject to modification or change.

23. Revocation and suspension of a certificate.

23.1. Circumstances for the revocation of the certificate: The circumstances for the revocation of the certificate are those indicated in section 15.1.1 of this certification practice statement (CPS) and certificate policy (CP).

23.2. Entity that can request the revocation: The entity that may request the revocation of the electronic signature or certificate, as appropriate, is identified in section 15.1.2 of this certification practice statement (CPS) and certificate policy (CP).

23.3. Renewal application procedure: The procedure for requesting the renewal of the electronic signature or certificate, as appropriate, is the one indicated in section 15.1.6 of this Certificate of Certification Practices Document (CPS) and Certificate Policy (CP).

23.4. Revocation request grace period: The grace period for requesting the revocation of the electronic signature or certificate is twenty (20) days. Upon termination or prior to

termination, PROCERT will determine whether the certificate should be revoked or re-established as valid.

23.5. Circumstances for suspension: The circumstances for the suspension of signature or electronic certificate as appropriate, is that indicated in section 15.1.1 of this document of practice certification statement (CPS) and certificate policy (CP).

23.6. Procedure for requesting suspension: The procedure for suspension of electronic signature or certificate, as appropriate, is the one indicated in section 15.1.4 of this Certification Practice Statement Document (CPS) and certificate policy (CP).

23.7. Limits of the suspension period: The limit of the suspension period of electronic signature or certificate, as appropriate, is that indicated in section 15.1.3 of this certification practice statement (DPS) and certificate policy (PC).

23.8. Frequency of CRL emission: The list of revoked certificates (CRLs), constitutes a record of all those certificates that, having fulfilled their process of generation and allocation of Law, are revoked when their password is compromised, at the request of the Client, for improper use of the certificate, for reasons imputable to the Client or for the cessation of operation of the certification authority (CA). The list of Revoked Certificates (CRLs) is published every twenty-four (24) hours on the PSC PROCERT website (www.procert.net.ve).

23.9. Availability of on-line commitment of revocation and status of certificates: The certification authority (CA) has the ability to deliver the list of revoked certificates using the OCSP through the link http://ura.procert.net.ve/ocsp

23.10. Revocation on-line verification requirements: The client of PSC PROCERT can access online the verification of the status of a certificate for the purpose of verifying if it is suspended or revoked. The customer must enter the website of the PSC PROCERT (www.procert.net.ve) and access the module "AC PROCERT" then search for the option Publication of the revoked certificates AC PROCERT and select the option OCSP.

23.11. Other forms of disclosure of revocation information available: The PSC PROCERT will notify via e-mail to the corresponding client, about the suspension or revocation of its certificate.

24. Certificate Status Checking Service.

24.1. Operating characteristics: The PSC PROCERT has services of verification of state of the signature or electronic certificate. These services are the list of Certificate Revoked List (CRL) and OCSP access for online access to the verification of the status of electronic signatures and certificates generated by the PSC PROCERT.

The operation of the CRL is established in section 31.7 of this document certification practice statement (CPS) and certificate policy (PC). The operation of OCSP access is established in the preceding sections 23.9 and 23.10.

24.2. Availability of service: The PSC PROCERT maintains the CRL services and OCSP access available through its website (www.procert.net.ve). The certification authority (AC) PROCERT maintains its web portal in operation, complying with a high percentage of availability.

24.3. Additional Features: Additional features to CRL and OCSP access services are identified earlier in this Certification Practices Statement (CPS) and Certificate Policy (PC).

25. End of subscription: The client of the PSC PROCERT may give the allowed use of the electronic signature or certificate and during its period of validity. Upon completion of the validity period of the certificate, the customer may opt for the renewal and reissue process. If the client does not opt for the renewal or new issue, it will have to its availability in the files of the PSC PROCERT and for a period of ten (10) years, the records corresponding to the generation of its certificate.

26. Custody and recovery of the key.

26.1. Key custody and recovery practices and policies: The PSC PROCERT private key is stored in an HSM cryptographic device. Access to the private key repository requires the use of smart cards. The PSC PROCERT operating scheme and its technological certification platform are configured so that the client generates its key pair (public and private). Always and in any case the key commitment will derive from the same client as the PSC PROCERT does not generate the pair of keys (public and private).

Accordingly, if the client misappropriates his private key, a new certificate must be issued and he must comply with the process of contracting the PSC for such purposes. The public key will always be in the repository, in accordance with what is indicated in section 31.2.3 of this certification practice statement (CPS) and certificate policy (CP) document.

27. Physical security, management and operations controls.

27.1. Physical security controls: Location and construction of the PSC. The certification authority (CA) PROCERT maintains an operational scheme aimed at ensuring the operational continuity and provision of its services with high standards of quality, timeliness and safety.

The data center is constituted in the operational headquarters of the certification authority (CA) PROCERT and from where the platform of emission of certificates.

The data center meets and maintains the operational requirements that for this type of facilities imposes the international regulations regarding security associated with information technology, the legislation of the Bolivarian Republic of Venezuela and the standards imposed by SUSCERTE.

The operations staff of PSC PROCERT is responsible, in conjunction with the General Manager and IT consultant to manage and maintain the operation of the certificate generation technology platform installed in the data center located at 7th Street, Level 3 Data Center, La Urbina, Sucre Municipality of the City of Caracas, Bolivarian Republic of Venezuela.

The data center operates twenty-four (24) hours a day, three hundred and sixty-five (365) days of the year and maintains an operational autonomy of more than two (2) months. In addition, the data center meets conditions and characteristics of anti-seismic construction and fire and flood prevention, maintains a perimeter of security and has seven (7) levels of access security.

The data center from which the PROCERT certification authority (CA) operates operates the policies or instruments issued by solvent and recognized insurance companies, in order to maintain support in the event of a contingency that affects the physical integrity of the said administrative headquarters and can thus offer a guarantee of its operational continuity.

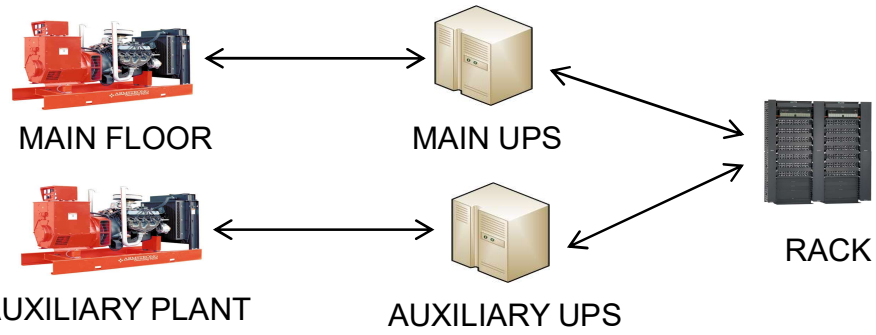
The certification authority (CA) PROCERT maintains an alternate center operation contract in case of permanent damage that makes it impossible and restricts the regular operation of the data center.

27.1.1. Physical access: The certification authority (CA) PROCERT within its technological platform of electronic certification, maintains measures of control of access both logical (application certification) and physical (equipment) guaranteeing the integrity and security of the services provided.

For physical access control there are seven (7) layers of security, from the outside to the servers where the certification application is installed. In addition to security procedures that restrict access only to authorized personnel authorized to access each of the seven (7) layers of physical security and know the access information (login and password) of the operating system of the equipment that make up the Certification Authority (CA) certification platform PROCERT. Physical access to the inside of the rack (opening) should only be allowed to PSC PROCERT personnel. Characteristics of the data center:

- Surveillance with armed personnel and digital cameras includes the service 7X24X365 days. At this level, portable computers are recorded.
- The perimeter fence limits physical access to the data center headquarters.
- The entrance control to the entrance of the internal area of the data center constitutes a mechanism of double insurance of entrance of the authorized personnel.
- The access control to the access corridor to the server area constitutes a triple mechanism of assuring access to the public area of the data center and the server area. In this control is valid the identity of the person authorized by PROCERT to enter the server area.
- The biometric device that is sensitive to heat and identity aims to block access to the server area for unauthorized personnel and accompanied by technical and operations personnel.
- The security magnetic card for access door to the internal area of control of the server area validates that in fact only the authorized personnel and holder of the card have access to the control area of servers.
- The access control to the server room is performed by the operators of the external control area of the server area. The operators validate the identity of the person who will enter the server area, then register their data and the time of entry and exit.
- The PROCERT server rack access key is in the possession of the PROCERT personnel to ensure the security and custody of the servers and the certification authority.
- The security mechanism of access to the door of the server rack of PROCERT is constituted in the security system that allows that only the operators of PROCERT will be able to accede to the servers of the certification platform.

27.1.2. Power supply and air conditioner: The rack where the servers of the certification platform of the AC PROCERT certification authority are installed have two (2) different power lines, one main and one auxiliary, these power lines are connected to two (2) power sources. uninterrupted power (UPS), which in turn are connected to two (2) power plants. Below is a reference chart of the power supply connection:



This distribution guarantees the supply of electric energy and consequently of air conditioning.

27.1.3. Water exposition: The data center meets and maintains the operational requirement that for this type of facilities imposes the international regulations regarding security associated with information technology, the legislation of the Bolivarian Republic of Venezuela and the standards imposed by SUSCERTE.

27.1.4. Fire protection and prevention: The data center meets and maintains the operational requirement that for this type of facilities imposes the international regulations regarding security associated with information technology, the legislation of the Bolivarian Republic of Venezuela and the standards imposed by SUSCERTE.

27.1.5. Storage Systems: The data center meets and maintains the operational requirement that for this type of facilities imposes the international regulations regarding security associated with information technology, the legislation of the Bolivarian Republic of Venezuela and the standards imposed by SUSCERTE.

27.1.6. Waste disposal: The data center meets and maintains the operational requirement that for this type of facilities imposes the international regulations

regarding security associated with information technology, the legislation of the Bolivarian Republic of Venezuela and the standards imposed by SUSCERTE.

27.1.7. Backup Storage: The data center meets and maintains the operational requirement that for this type of facilities imposes the international regulations regarding security associated with information technology, the legislation of the Bolivarian Republic of Venezuela and the standards imposed by SUSCERTE.

27.2. Functional controls.

27.2.1. Trusted papers: The certification authority (CA) and registration authority (RA) will maintain a management and operation scheme based on a flat structure, based on the interaction and interdependence of the personnel in their various roles and functions. The regular operation of the PSC PROCERT will be divided into functions of operation and administration.

Top management is the highest decision-making and command level within the organization. The operation and administration activities will be coordinated by the general manager and the technology consultant of PSC PROCERT, who will report directly to the top management.

The operation, control, monitoring and daily monitoring of the management of the technological platform of certification will be carried out by the computer operators. The group of computer operators will have an operator coordinator, who will be appointed by the general manager and the technology consultant and must have the approval of the top management.

The group of computer operators will be made up of a total of up to four (4) operators, who will be able to attend and resolve all operational requirements of the technological certification platform.

The regular management of the registration authority (RA) will be assigned to an identity and data accreditation manager. The regular management of the general manager will be supported by an administrative assistant, who will perform clerical and receptionist managements, process payments and coordinate the relationship with the outsourced services and maintain the inventory of administrative and logistical material required by the staff of PSC PROCERT.

27.2.2. Number of people required per role: The internal and medullary structure of the PSC PROCERT is broken down as follows:

- General management (1)
- The technology consultant (1).
- Information Security and Compliance Consultant (1)
- Auditor (1)
- Computer Operators (4).
- The registration authority (AR) (1).
- The management staff (1).
- Outsourced services (20)

27.2.3. Identification and authentication of each role: The identification and authentication of each role, as well as the establishment of new obligations or responsibilities will correspond to the High Management of PSC PROCERT. The functions and responsibilities associated with each position are indicated inside section 11.1.1., preceding.

27.3. Personal Security Controls.

27.3.1. Background, qualification, experience and accreditation requirements: All PSC staff involved in the operation of public key infrastructure (PKI) is subject to background investigation and verification. References are rigorously investigated in the case of operational personnel. The entire operation of the public key infrastructure (PKI) of PSC PROCERT is under the direct responsibility of top management.

Personnel involved in the control and operation of public key infrastructure (ICP) will be sufficiently trained to perform the functions assigned to their role and will receive ongoing training to ensure awareness levels about security policies and procedures.

The personnel training and development process is regulated by PROCERT's personnel training and development policy document (AC-D-005).

27.3.2. Training requirements: No PSC PROCERT staff member may have physical access or operate any public key infrastructure (PKI) component without prior training and without the presence of other designated staff members who have the skills required to confirm that they are not taken inappropriate or unauthorized actions or lack of appropriate training and training.

Procedures are defined and documented for all operations related to public key infrastructure (PKI). Operational procedures are regularly reviewed as new operational requirements emerge.

27.3.3. Penalties for unauthorized actions: Any procedure not contemplated in this Certification Practices Statement (CPS) and Certification Policy (CP), must have the express written approval of the senior management of PSC PROCERT and SUSCERTE otherwise it will be considered as act of sabotage for the internal purposes of PSC PROCERT and will be sanctioned with justified dismissal, for breach of the obligations imposed by the employment relationship.

27.4. Security Control Procedures.

27.4.1. Types of events recorded: The PSC PROCERT stores electronic event logs (logs) relating to its activity as PSC. These records are stored automatically and electronically and in the cases of physical access in paper format and other means. Each event log includes data relating to the date and time it was produced, serial number, event description and the system or person that originated it. The minimum audit records that must be maintained include:

- Events of the teams that make up the platform:
  - Installing and Configuring the Operating System.
  - installation and configuration of any application installed on the computer.
  - Installation and configuration of the certification authority.
  - Installation and configuration of the cryptographic module.
  - Access or attempts to access the computer.
  - Updates.
  - Performing backups
- Certification software events:
  - User management.
  - Role Management.
  - Managing Certificate Templates.
  - Access Control List (ACLs).
  - Certificate management (everything contemplated in the cycle of your life)
- Events related to physical access:
  - Access of staff to the data center.
  - Access of personnel to equipment and systems.

- Corrective action events:
  - Hardware Errors.
  - Software Errors.

27.4.2. Frequency of processed log records: Audit logs are performed at any time an operation is performed on the Certification Authority (CA) certification root of the PSC PROCERT, otherwise the Certification Authority (CA) certification root is maintained out of line. Operations personnel notify their security administrator when a process or action causes a critical security or discrepancy event.

Subordinate Public Key Infrastructure (PKI) entities (when applicable) are also required to notify any event that may cause a critical security or discrepancy event. In any case, the general management and the technology consultant will decide the next steps.

27.4.3. Retention period for audit logs: Audit records are retained for a period of ten (10) years.

27.4.4. Protection of audit logs: The PROCERT PSC Audit Collection System is a combination of automatic processes and manual procedures performed by the Certification Authority (CA) certification body of the PSC PROCERT, operating systems and by operational personnel. Therefore, the system is maintained through mechanisms of access control and separation of roles in relation to the software and hardware that handle the automatic collection and by operating procedures confidentially documented, known and followed by the personnel of the certification authority (CA) of the PSC PROCERT.

In addition, the integrity of audit events is protected by signing each event with the private key of the person carrying out the action.

27.5. Information and records archive: All records of the Public Key Infrastructure (PKI) of the Certification Authority (CA) of PSC PROCERT regarding the operation of its certification services are archived and retained for a minimum period of twenty (20) years.

The time resource for the Certification Authority (CA) certification root of the PSC PROCERT is periodically independently verified and all automated records of the PSC PROCERT certification root are associated with the time and date of its occurrence.

Records files are kept under strict access control and are subject to auditors' inspection.

All records files and identification information will be archived directly by the PSC Registration Authority (RA) PROCERT will require the registration authority (RA) to file the records and information for a period of ten (10) years from the date of expiration of the certificate and will make its best efforts for the chain to fulfill its obligations in this matter. In any case the records can be archived in paper or in electronic form.

27.5.1. Type of information and events recorded: The type of information and registration of events will be the same contemplated in the section 27.4.1., of this document of Certificate Practice Statement (CPS) and policy of certificates (PC).

27.5.2. Retention period for the file: The retention period for archiving shall be the same as that referred to in section 27.4.3. Of this Certification Practice Statement (CPS) and Certificate Policy (PC).

27.5.3. File protection: The method of file protection shall be the same as that described in section 27.4.4. of this document on the declaration of certification practices (CPS) and certificate policy (CP).

27.5.4. Requirement for stamping time for registration: The processes and steps that must be fulfilled by the PSC PROCERT to provide the time stamping service are regulated by SUSCERTE Superintendence, but the master clock is not in operation.

27.5.5. Audit file repository system (internal vs. external): Each of the teams present in the certification platform has a module to store event logs, specifically application, system and security events, including the certification application.

This event log allows auditing and verifying attempts at access, access and harmful operations, whether intentional or not. The event log is also stored on tapes and as indicated below. Three (03) weekly magnetic tapes, one (01) magnetic tape for monthly backup, five (05) magnetic tapes for annual backup, one (1) magnetic tape for occasional backup, one (1) magnetic tape for (1) magnetic tape in which the full backup will be made at the start of operations and a CD / DVD for the certification authority's (CA) private key for a total of 27 magnetic backup tapes and one CD / DVD.

Backup tapes are stored in an external vault to the data center. Custody and storage of magnetic media (magnetic tapes, disks, cartridges, diskettes, etc.) in a safe place, with controlled environmental conditions, automatic fire-extinguishing systems and restricted access, as a preventive measure in the event of a disaster or loss unintended critical and sensitive files from the PROCERT Certification Authority (CA) additionally offer an availability of access to stored media 24 hours a day, 365 days a year.

28. Change of keys: The PSC PROCERT operating scheme and its technological certification platform are configured so that the client generates its key pair (public and private). Always and in any case the key commitment will derive from the same client as the PSC PROCERT does not generate the key pair (public and private).

Accordingly, if the client misappropriates his private key, a new certificate must be issued and he must comply with the process of contracting the PSC for such purposes. The public key will always be in the repository, in accordance with what is indicated in section 31.1.4 of this certification practice statement (CPS) and certificate policy (CP).

29. Recovery in case of disaster.

29.1. Incident and vulnerability management procedure: PSC PROCERT has established a business continuity and disaster recovery plan (PRD) (AC-P-001), in the event of a possible partial or total compromise of the public key infrastructure (PKI) of the certification authority (CA) PROCERT. The disaster recovery plan is periodically reviewed in the light of changing environmental risks. The disaster recovery plan is geared towards:

29.1.1. Failure / Corruption of Computer Resources;
29.1.2. Commitment to Integrity of the key; And
29.1.3. Natural Disasters and Termination.

Top management, represented by a director, general manager, technology consultant and IT operators, must take corrective action and undertake the necessary activities to restore the certification technology platform at the time of a disaster scenario.

The business continuity and disaster recovery plan (PRD) (AC-P-001) specifies the procedure to be followed in each of the scenarios considered as a disaster and then the main responsibilities of each of the positions at the time the recovery plan is implemented: i) a director next to the general manager declares the disaster scenario and approves the activation of the contingency plan; (ii) the technology consultant

manages, monitors and supports the implementation of all disaster recovery activities; iii) Operators perform service restoration activities.

29.2. Alteration of resources, hardware, software and / or data: PSC PROCERT has established a business continuity and disaster recovery plan (PRD) (AC-P-001), in the event of a possible partial or total commitment of public key infrastructure (PKI). The disaster recovery plan is periodically reviewed in the light of changing environmental risks.

29.3. Procedure for action on the vulnerability of the private key of an authority: The PSC PROCERT, although it plans to activate the HSM (for the signing of certificates) locally and only in the presence of the technology consultant and the general manager, considers as one of its disaster scenarios the commitment of its private key, and the actions to be implemented after detecting the aforementioned commitment are as follows:

Immediate cessation of the sale service and generation of electronic certificates.

29.3.1. Declaration of the PSC PROCERT of the disaster scenario.
29.3.2. Notification to the SUSCERTE of the commitment of the key, for the immediate revocation of the certificate of the PSC PROCERT.
29.3.3. Publication of the event on the PSC PROCERT Web Page.
29.3.4. Notification to PSC PROCERT clients via email.
29.3.5. Notify the insurance company that maintains the PSC's operating bond.
29.3.6. Analyze the reason for the commitment and make a technical report detailing the reasons why the private key of the PSC PROCERT.
29.3.7. Agree together with SUSCERTE the actions to be taken for the reactivation of the service of emission of certificates.

29.4. Security of facilities following a natural or other disaster: The data center from which the certification authority (CA) operates operates the policies or instruments issued by solvent and recognized insurance companies, in order to maintain support in case of a contingency that affects the physical integrity of said administrative seat and can thus offer a guarantee of its operational continuity.

However, in the case of a disaster that disables the regular operation of the data center from where the PSC PROCERT operates. Likewise, the PSC PROCERT maintains agreement of operation of alternate center in case of permanent damage that precludes and restricts the regular operation of the data center of the company LEVEL 3.

30. Cessation of activity: The PSC PROCERT contemplates in the event that a cessation of operations occurs, the following assumptions:

30.1. Extinction due to expiration of accreditation.
30.2. Extinction for termination of operations.
30.3. Extinction for revocation of accreditation. In this case, and only for proven reasons of non-compliance, will proceed the execution of the guarantee requested by SUSCERTE at the time of accreditation.
30.4. Extinction derived from technological aspects.
In the event of any of the aforementioned assumptions, PCS PROCERT shall be obliged to place at the disposal of SUSCERTE the repository of all the certificates issued during its management, including the status of each of them.

31. Technical safety controls.

31.1. Generation and installation of the key pair.

31.1.1. Generating the key pair: The PSC PROCERT generates its key pair (public and private) using a cryptographic hardware device (HSM) that complies with FIPS 140-1 Level 3. The operating schema of the PSC PROCERT and its Technology Certification platform are found configured for the client to generate their key pair (public and private). Always and in any case the key commitment will derive from the same client as the PSC PROCERT does not generate the key pair (public and private). Accordingly, if the client misappropriates his private key, a new certificate must be issued and he must comply with the process of contracting the PSC for such purposes. The public key will always be in the repository, in accordance with the present certification practice statement (CPS) and certificate policy (CP).

31.1.2. Delivery of the private key: The PSC PROCERT operating scheme and its technology certification platform are configured so that the client generates its key pair (public and private) provided and in any case the key commitment will be derived from the same client as the PSC PROCERT does not generate the pair of keys (public and private). In view of the above, if the client loses his private key or is compromised, a new certificate must be issued and must comply with the process of contracting the PSC for such purposes.

31.1.3. Delivery of the public key: The PSC PROCERT operation scheme is configured so that the client generates its key pair (public and private). Always and in any case the key commitment will derive from the same client as the PSC PROCERT does not generate the key pair (public and private). If the client loses its private key, the previous certificate is revoked and it must

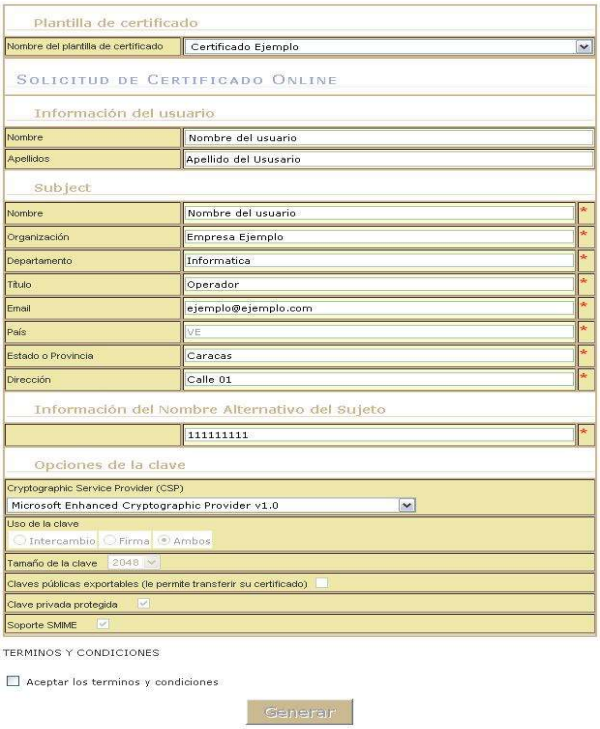
proceed to the generation of a new certificate. The public key will always be in the repository, in accordance with what is stated in this certification practice statement (CPS) and certificate policy (PC).

31.1.4. Availability of public key: The PSC PROCERT is obliged to maintain in its repository and available its public key, which any client or interested party can access through the PROCERT website (https://ura.procert.net.ve/pscprocert /cadena.p7b).

31.1.5. Size of keys: The Certification Authority (CA) certification root modules and keys have a length of at least 4096 bits and use the RSA algorithm.

31.1.6. Parameters of public key generation and quality verification: 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) using the PROCRC PSC certification platform is a simple process, but requires special precautions. The following describes the steps to be taken to generate the key pair and what precautions should be taken to ensure the protection of the private key:

- The end user must enter the web page of PSC PROCERT (http://www.procert.net.ve) click on the link system certification (https://ura.PROCERT.net.ve/CID/URA/ User / logon.aspx) and thus enter the certification system.
- There you must verify that the data contained is correct, said request is composed of four (04) parts:



User Information: This section contains the first and last name of the user that was supplied to PSC PROCERT.

Subject: General information of the user that, depending on the type of certificate, some fields will be mandatory, then the fields are listed and which are obligatory by certificates

Tipo de Certificado	Nombre	Organización	Departamento	Titulo	Email	País	Estado	Dirección
Representante legal de empresa privada	✓	✓	✓	✓	✓	✓	✓	✓
Representante de empresa publica	✓	✓	✓	✓	✓	✓	✓	✓

Empleados de Empresas	✓	✓	✓	✓	✓	✓	✓	✓
Profesional Titulado	✓			✓	✓	✓	✓	✓
Persona Natural	✓				✓	✓	✓	✓
Servidor Seguro SSL	✓	✓			✓	✓	✓	✓
Control de Acceso Lógico	✓	✓			✓	✓	✓	✓

Alternative Name Information: This section must contain the number of RIF or C.I. of the signatory

Key Options: In this section you must choose the Cryptographic Service Provider (CSP), it is important to take into account that, if the certificate is to be installed in a cryptographic Etoken, the drivers of that device must be previously installed on the leaving equipment to use to generate the key pair (public and private) of the user. Subsequently the user must accept the terms and conditions to enable the generate button. After pressing the generate user button you will have the option to protect your private key with a high security level using a password.

Subsequent to the approval of the request by the PSC certification authority PROCERT will send to the user's email a link where he can download the certificate. The mentioned key pair generation procedure guarantees the privacy of the user's private key, since the user is the one who generates it, the PSC PROCERT only guarantees the linking of the individual with the public key, that public key is associated with its to private key.

31.1.7. Key Generation Hardware / Software: The software used by PSC PROCERT for the generation of the key pair and certificates is a combination of the Microsoft certification authority and specialized electronic certification software.

The certification authority (CA) uses a cryptographic module to securely store its private key. This NCIPHER and HSM cryptographic module and nShield PCI 500 TPS, F3 SEE Ready, have FIPS 140-1 and FIPS 140-2 certifications, and all the technical specifications of this safety device are listed below:

31.1.7.1. Supported Cryptographic Algorithms.

31.1.7.1.1. Symmetric encryption.

- AES – Rijndael.
- ArcFour (compatible with RC4).
- CAST.
- DES.
- Triple-DES.

31.1.7.1.2. Public Key Encryption.

- DSA.
- The Gamal.
- RSA.

31.1.7.1.3. Key Exchange Mechanisms.

- DH.
- DES / DES3 XOR.
- HASH and HMAC functions.
- MD2.
- MD5.
- RIPEMD 160.
- SHA-2.
- SHA-1.

31.1.7.2. References: In order to document and provide information on the cryptographic hardware used by the certification authority (CA), the web address indicated below is indicated: https://www.thales-esecurity.com/knowledge-base. In addition, the cryptographic module used by the certification authority (CA) supports the generation of 4096-bit keys and has the ability to sign and encrypt.

31.1.8. Purposes of using keys: The PSC PROCERT Private Key can be used to:

31.1.8.1. Signing Certificates to Policy Certification Authorities.
31.1.8.2. Signature of certificates established in this CPS.
31.1.8.3. Signing certificate revocation lists.
31.1.8.4. Signature of certificates for cross certification, approved by SUSCERTE and general management and PROCERT technology consultant.

31.2. Private Key Protection.

31.2.1. Standards for Cryptographic Modules: The cryptographic module used by the public key infrastructure (PKI) of the PSC PROCERT is certified to meet

FIPS level 3 requirements. In the case of the PROCERT certification root, that module is kept offline.

31.2.2. "M" control of the private key: The private key of PSC PROCERT is under multi-person control. This is activated by initializing the CA software through a combination of CA operators, HSM Administrators, and operating system users. This is the only method of activating this key.

31.2.3. Custody of the private key: The private key of the certification authority (CA) is protected by an HSM. The certification authority (CA) has established the steps to follow for the installation of the HSM, these are detailed below:

- Installing the drivers: The drivers for the HSM must be installed on the certification server (CA).
- Physical installation
- Creating the Security World: The Security World will be created under the established commands and following the following parameters:
- Profiles and fools will be created within the security world.

31.2.4. Private Key Backup: The backup of the private key is done in two (2) CD / DVD drives (main and back) sealed with a seal and stored in a safe. The encryption key of the PSC PROCERT certification root only supports the purposes of disaster recovery.

31.2.5. Private key file: The private key of the certification authority (CA) is stored in a hardware component called HSM, which is responsible for backing up and encrypting it. Both backup and encryption are stored on a tape drive, which the the certification authority (CA) shall ensure that it is kept in a safe place outside the data center.

31.2.6. Inserting the private key into the cryptographic module: The certification authority (CA) has established the parameters and guidelines under which the generation of keys will be done, these are detailed below:

31.2.6.1. The new world of security will be generated.
31.2.6.2. The certification authority will be installed under Subordinate mode and the certificate request will be generated.
31.2.6.3. The SUSCERTE will sign the request of the certificate of PSC PROCERT.
31.2.6.4. The PSC PROCERT certificate will be installed and activated.

31.2.7. Private Key Activation Method: For the activation of the private key it is necessary to use smart cards, requires two of four administrator cards and one of two operator cards, in addition, access to the operating system of the certification server is required.

31.2.8. Method of destruction of the private key: The certification authority (CA) source private key can be destroyed by returning the HSM to its original factory state and deleting all backup symbols.

31.2.9. Ranking of the cryptographic module: The certification authority (CA) uses a cryptographic module to securely store its private key. This cryptographic module or HSM marks NCIPHER, model nShield PCI 500 TPS, F3 SEE Ready and has certifications FIPS 140-1 and FIPS 140-2. These devices fall into the category of high security hardware, which are used by banks and state security throughout the world, enjoying proven experience and security.

31.3. Other aspects of key pair management.

31.3.1. Public key file: The public key of the PSC PROCERT is archived according to the format PKCS # 7, for a period of 10 years.

31.3.2. Operative periods of certificates and period of use of the key pair: The PSC PROCERT certificate will be valid for 10 years. The electronic signatures and certificates generated by the PSC PROCERT have a cycle of one (1) year counted from the date of activation of the signature or electronic certificate by the Certification Authority (CA) of PROCERT. The key pair associated with each electronic signature or certificate, also has the same period of validity as the signature or certificate in question.

31.4. Activation data.

31.4.1. Generation and installation of activation data: The generation of the key pair (public and private) using the PROCERT certification authority (CA) certification platform is a simple process, but requires special precautions. The following describes the steps to be taken to generate the key pair and what precautions should be taken to ensure the protection of the private key:

31.4.1.1. The validation of the identity of the individual is executed by the registration authority (AR) which sends to the certification authority (CA) the necessary information so that the creation of the user within the system of and in this way guarantee the linking the person's identity with his or her public key. The end user must enter

the PROCERT website (http://www.procert.net.ve) and click on the Electronic Certificates link, then click on the box that indicates the Certification System (https: // ura.procert.net.ve / CID / URA / User / logon.aspx), access and register in the certification system.

31.4.1.2. After registering, you must enter the certificate request application by entering your login information (password and login) and validating your email address.

31.4.1.3. After validating your e-mail address, the user must access the certificate link and make a certificate request, selecting the type of certificate (electronic signature), entering the requested personal information, selecting the criptogtaphic service provider (CSP) and by pressing the Generate button. Note: Be very careful with the CSP and the equipment and / or device where the certificate request is being generated, since that is where the certificate will be installed.

31.4.1.4. Pressing the Generate button creates the key pair (public and private), and the certificate request is automatically sent to the registration authority to be validated face-to-face the identity of the user making the request.

31.4.1.5. The mentioned key pair generation procedure guarantees the privacy of the user's private key, since the user is the one who generates it, PSC PROCERT only guarantees the linking of the individual with the public key, that public key is associated in turn to the private key.

31.4.1.6. Once the identity is validated by the Registration Authority (RA) and the certificate is generated by the Certification Authority (CA), the client proceeds to download the electronic signature or certificate in the repository of his computer, accepting the certificate issuance source.

31.4.2. Activation Data Protection: The activation of the issued certificate is performed using the PSC PROCERT certification system, being limited to the equipment or device where the key pair was generated.

31.5. Computer security controls.

31.5.1. Specific technical requirements: PSC PROCERT has defined a series of security controls applicable to computer equipment, such as the use of equipment, physical and logical access controls, audit plans, authentication and security testing.

31.5.2. Computer Security Qualifications: The PSC PROCERT uses products certified at least by Level E3 of the ITSEC standards.

31.6. Lifecycle Security Controls.

31.6.1. System Development Controls: The CA software used by PROCERT's public key infrastructure (PKI) for certificate issuance and lifecycle management has been developed in accordance with the requirements of the ITSEC Information Technology Security Assessment Criteria acronym in English) Level E3. The HSM used by public key infrastructure (PKI) and Certification Authorities that meets FIPS 140-2 requirements.

31.6.2. Security Management Controls: The controls for the safety management are fulfilled by a rigid separation of the roles of the operator to fulfill the requirements of the established security policy.

31.6.3. Life Cycle Security Ratings: During the entire life cycle of the keys, security controls must be implemented to allow the instrumentation and audit of each phase of the systems of the certification authority (CA) of PSC PROCERT.

31.7. Network security controls: Hardware and software for the certification authority (CA) public key infrastructure (PKI) are maintained off-line in a high security installation within a comprehensive security control and rigorous internal access controls.

It maintains sophisticated intrusion detection systems to notify security personnel of any violation of access controls. In addition, the Certification Authority (CA) certification root is kept offline and is not related to any external component.

31.8. Cryptographic Modules Engineering Controls: The PSC PROCERT uses cryptographic modules (hardware and software) commercially available and developed by third parties. The PSC PROCERT only uses FIPS 140-2, Level 3 (nShield F3) and Level 2 (nShield F2) cryptographic modules).

32. CRL / OCSP certificate profiles.

32.1. Certificate Profile: PSC PROCERT certificates 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 (prevaleciendo en caso de conflicto la TS 101 862).

32.2. Version Number: As stated in 32.1. Above, the version number of the certificate is V3.

32.3. Certificate extensions: Extensions of PSC PROCERT certificates allow you to encode additional information on certificates. The X.509 standard extensions define the following fields: i) SubjectKeyIdentifier; ii) AuthorityKeyIdentifier; iii) BasicConstraints; iv) Certificate Policies; v) KeyUsage; vi) CRLDistributionPoint; vii) SubjectAlternativeName; and viii) AuthorityInformationAccess.

32.4. Object identifiers (OIDs) of the algorithms: The OID of the cryptographic algorithm used by the PSC PROCERT is: SHA256 with RSA Encryption (1.2.840.113549.1.1.11).

32.5. Name Formats: The format and meaning assigned to the names in each of the electronic signatures and certificates generated by the PSC PROCERT are detailed in section 14 of this document of the certification practice statement (CPS) and certificate policy (CP).

32.6. Object identifier (OID) of the PC.: PSC PROCERT, will use the OID assignment policy definition according to the private numbering tree assigned by the Superintendency of Electronic Certification Services (SUSCERTE).

32.7. CRL / OCSP's profile: The certificate revoked list (CRL) is a list of electronic signatures and certificates, in which the serial numbers of electronic signatures or certificates revoked by a certification authority (CA) are shown, serial numbers that have been revoked, are no longer valid, and therefore the user should not rely on any certificates included in the CRL of the system. One (CRL) is a file that contains: i)

Name of the CRL emitter; ii) Serial numbers of the firm or certificate; iii) Date of revocation of the signatures or certificates; iv) The effective date and date of the next update; and v) the reason for the revocation. This list is electronically signed by the certification authority (CA) that issued it**.**

When a user wishes to check the validity of a certificate, he must download and install the updated CRL from the servers of the same certification authority (CA) that issued the signature or certificate, in doing so, the signatures or certificates that are installed in the computer where the CRL is installed, are automatically validated, if they are revoked, are invalidated; you can also check through the serial number located in the CRL the status of some other certificate. The authenticity of the list is verified thanks to the electronic signature of the certification authority

Nombre del campo	Valor
Versión	V2 (Número de versión del certificado).
Algoritmo de Firma:	Sha-256RSA(Algoritmo de Firma)
Datos del emisor	
CN	PSCPROCERT.
O	Sistema Nacional de Certificación Electrónica
OU	PROCERT
C	VE (VENEZUELA)

E	contacto@procert.net.ve
L	Av. Libertador Multicentro Empresarial del Este piso 13 Oficina B-132 Torre Libertador Núcleo B
ST	MIRANDA
Período de validez	
Última Actualización:	Fecha y hora emisión CRL.
Próxima Actualización:	Fecha próxima CRL.
Lista de certificados revocados	
Certificados Revocados	Contiene la lista de certificados revocados (número de serie y fecha de revocación).
Extensiones	
Identificación clave autoridad certificadora	Proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una CRL (ID DE CLAVE)
Nombre alternativo del emisor	
Punto distribución CRL	http://ura.procert.net.ve/lcr/PROCERTca.crl http://www.procert.net.ve/lcr/PROCERTca.crl
Información del emisor	http://ura.procert.net.ve/ocsp
Política de certificados	http://www.procert.net.ve/dpc-pc/

The OCSP profile is detailed in sections 23.9 and 23.10 of the present document of the Certification Practices Statement (CPS) and Certificate Policy (PC).

32.8. Compliance audit: In the case of the Certification Authority (CA) certification root, it is monitored and audited annually by SUSCERTE, which at any time and at such frequency as it deems appropriate may carry out exhaustive or partial audits to determine if the management of the certification authority Cryptographic Key Certification Authority (CA) complies with the guidelines of Act to operate as PSC.

32.8.1. Frequency of conformity checks for each entity: The control and monitoring audits ordered by law and mandated by SUSCERTE will be carried out annually; and by means of these audits the level of compliance of the PSC PROCERT will be established on the law and technical, national and international regulations applicable to all PSCs in operation. Every PSC accredited to SUSCERTE must carry out the annual follow-up audit if it chooses to renew its accreditation for operation during the year following the audit process.

32.8.2. Auditors: Annual audits will be performed by the auditor selected by PSC PROCERT. The selected auditor must be accredited to the auditor's registry maintained by SUSCERTE.

In addition, PSC PROCERT has implemented a permanent internal auditing scheme, with its own staff reporting directly to the Management and Board of Directors in order to establish a mechanism for internal control and monitoring, ensuring compliance with the activities inherent to the services that lend the PSC PROCERT

32.8.3. Relationship between the auditor and the audited authority: Between PSC PROCERT and the selected auditor, there is only one non-dependency business relationship. PSC PROCERT will contract the follow-up audit ordered by SUSCERTE and the auditor will provide the service with the obligation to generate a compliance report, which will deliver to PSC PROCERT and SUSCERTE, and to maintain at all times the confidentiality of the information to which was accessed during the audit process.

32.8.4. Topics covered by conformity control: Topics covered by the Compliance Audit include:

32.8.4.1.1. Physical security.
32.8.4.1.2. Technology evaluation.
32.8.4.1.3. CA Service Management.
32.8.4.1.4. Personnel research.
32.8.4.1.5. Document of the certification practice statement (CPS) and certificate policy (PC) and other applicable policies and documents.
32.8.4.1.6. Contracts.
32.8.4.1.7. Data protection and privacy considerations.
32.8.4.1.8. Disaster Recovery Planning.

32.8.5. Actions to be taken as a result of a deficiency: Any point or observation generated by the auditor accredited to SUSCERTE regarding the operation and generation of PSC PROCERT certificates and that is considered as "nonconformity", will be submitted to a remediation and compliance plan, which shall establish the schedule and time set to overcome the "disagreement", in the event that it is declared. If PSC PROCERT does not exceed or complies with the "nonconformity" remediation process, it will not be eligible to renew its PSC accreditation and cease operation.

32.8.6. Communication of the result: The results of the audits are considered sensitive business information. Unless otherwise stipulated in the contract, they will be protected as confidential information in accordance with section 32.9.2 of this certification practice statement (CPS) and certificate policy (PC).

32.9. Commercial and legal requirements.

32.9.1. Duty: The decree law of data messages and electronic signatures establishes the obligation of PSC PROCERT to constitute guarantees for its operation as a body accredited by SUSCERTE. The regulations of the SUSCERTE establishes a fee payment of law for the purposes of qualifying for accreditation as a PSC, the amount of said tax is one thousand TAX UNITS (1000 U.T.). A bail is also requested in favor of SUSCERTE) whose amount is forty-one and one thousand tax units (41,000 U.T.). Said bond is constituted in order to guarantee the continuity of operation of PSC PROCERT and in the event of cessation of operation; situation in which SUSCERTE will assume control and operation of the PSC PROCERT technological platform. In addition, SUSCERTE establishes the obligation for PSC PROCERT to maintain a guarantee constituted in the form of an insurance policy and in favor of customers who use electronic signatures or certificates generated by PSC PROCERT.

32.9.1.1. Financial responsibility: The limits of responsibility of PSC PROCERT to its customers are governed by contractual agreements with these clients. The responsibility of PSC PROCERT to customers, dependent parties and any other entity that uses electronic signatures or certificates generated by the PSC is limited against claims of any kind, including contractual, illegal, extra contractual and criminal in nature, in each case. certificate in particular without regard to the number of transactions, electronic signatures or causes of action arising or related to said certificate or any service provided in respect of said certificate and cumulatively. Any and all claims arising out of the public key infrastructure (PKI) with respect to a certificate (without regard to the entity causing the damage) shall be subject to the liability limits applicable thereto in accordance with this document certification practice statement (CPS) and certificate policy (CP).

Subject to the above limitations, the aggregate liability of the PROCERT certification authority (CA) to all customers, dependent

parties and any other entity, or for the entire period of validity of a certificate issued by the certification authority (CA) (unless revoked or suspended before its expiration), to all persons in relation to said certificate is fifteen thousand tax units (15,000 UT). In no case shall the responsibility of the certification authority (CA) exceed the limit aforementioned.

32.9.2. Privacy policy.

32.9.2.1. Confidential information: All the compilation and use of the information compiled by the PROCERT certification authority (CA) is carried out in compliance with the Venezuelan legislation and based on the distinctions provided in this document of certification policy and declaration of certification practices (DCP) between "Summary of Information" and "Identification Information". Personal information collected and used by third-party certification service providers must comply with applicable data protection laws. In the absence of any local legislation, the CSPs will comply with the minimum standard referred to in this certification practice statement (CPS) and certificate policy (CP) standard. In the cases of cessation of operations, personal data and other relevant data will be transferred to SUSCERTE as the governing body of electronic certification services.

In any case, the storage and availability of such data should be sought in order to maintain the condition of certification services to the corresponding customers. Details on how PROCERT collects, processes, and stores personal data is found in the PSC PROCERT certification authority (CA) authority's (CA) operation model policy. In addition to the above, it is noted that the identification information is the information obtained to positively identify an entity and provide the certification services that it requests. Identification information will be treated as confidential information unless the entity to whom the information refers explicitly consents.

32.9.2.2. Non-confidential information: Types of information not considered confidential.

- Summary of information.
- All certificates issued by the Public Key Infrastructure (PKI) of the PSC PROCERT for public use may be publicly disclosed.

- All Certificates issued by the certification authority (AC) PROCERT in their condition certification services to third parties may also be publicly disclosed.

32.9.2.3. Publication of information about revocation or suspension of a certificate: The list of revoked certificates list (CRL), constitutes a record of all those certificates that, having fulfilled their process of generation and allocation of Law, are revoked when their key is compromised, at the request of the client, for improper use of the certificate, for reasons imputable to the client or for the cessation of operation of the certification authority (CA). The CRL is published every twenty-four (24) hours at (www.procert.net.ve). All process of revocation of certificate is informed by the PSC PROCERT via email to the Client that owns the electronic certificate. This notification is made with a copy to SUSCERTE and is included in the digitized deposit maintained by PSC PROCERT.

32.9.2.4. Disclosure of information as part of a judicial or administrative process: The reason(s) for the suspension or revocation of a certificate may be made public in accordance with applicable law or under the sole and absolute responsibility of PSC PROCERT. The information on suspension of certificates will be revealed only to the customer who owns the certificate or to the SUSCERTE under request derived from judicial process and under mandate of compliance. No document or register held by the certification authority (CA) or registration authority (AR) of the PSC PROCERT shall be delivered to the official agencies unless certain of the following events occur: i) a proper order or judicial application; ii) the official representative of the law is duly identified; and (iii) compliance with all other legal procedures. As a general principle, no confidential document or record kept by the certification authority (CA) and registration authority (AR) of the PSC PROCERT is delivered to any person except where: i) A duly documented request for information (eg has complied with all legal procedures); and ii) The person requesting the information is a person authorized to do so and is duly identified. Certification services provided under the authority of third parties may be the subject of such requests for information, such as civil evidence or for discovery purposes, relating to the PSC PROCERT Certification Authority (CA) in any

jurisdiction where appropriate legal procedures they have been fulfilled.

32.10 Protection of private / secret information.

32.9.3. Information considered private: The PSC PROCERT will consider private information, in accordance with the provisions of the Constitution of the Bolivarian Republic of Venezuela, the following: i) names and surnames; ii) identity card number and RIF; iii) Customer addresses and telephone information; and iv) data provided in the process of contracting an electronic signature or certificate.

32.9.4. Information considered not private: Types of information not considered confidential: i) summary of information; ii) all certificates issued by the public key infrastructure (PKI) for public use may be publicly disclosed; and iii) all certificates issued by the certification authority (CA) in their condition certification services to third parties may also be publicly disclosed.

32.9.5. Responsibilities to protect private / secret information: The PSC PROCERT is obliged to keep the information supplied by contracting clients of electronic signatures or certificates generated by PSC PROCERT. To this end, the data will be kept under electronic file with security certificates associated with the access of the same. Access to customer information will be limited to the representative of the registration authority (RA) and the General Manager of PSC PROCERT.

32.9.6. Provision of consent in the use of private / secret information: The information provided in files by PSC PROCERT will be handled as confidential information and it will not be supplied to third parties other than the client that owns the electronic signature or certificate, unless expressly approved and notarized by the client whose information in writing, via electronic signature signed or certified by the client who owns the signature or electronic certificate or derived from court order imposed by Court and derived from the cause in process.

32.9.7. Communication of information to administrative and / or judicial authorities: Regarding the communication of information, the principles and requirements set forth in section 31.9.2.4, which precedes and are part of this Certificate Practices Statement (CPS) and Certificate Policy (CP), shall be followed and applied.

32.10. Intellectual Property Rights.

32.10.1. General condition: Except for components that may be the intellectual property of Third Parties, all intellectual property rights, including copyrights in all certificate directories, revoked certificate lists (CRLs), and certificates; unless explicitly stated otherwise, all practices, policy, operational and security documents pertaining to the public key infrastructure (PKI) of the PSC PROCERT (electronic or otherwise) as well as the contracts, belong to and continue to be owned of PROCERT. Through the corresponding contracts for the provision of certification services, PSC PROCERT may grant a license to third parties for the use of certificates, revoked certificate lists (CRLs) and other authorized practices and policy documents to the extent that they require it for the provision of certification services according to the present document of certification practice statement (CPS) and certificate policy (CP).

32.10.2. Public and private keys: All intellectual property rights of the generated public and private keys will be protected by the entity by which those keys were generated or by the entity designated by it. Certification services operated under the authority of final customers will not obtain any rights whatsoever in relation to the certificates, their content, format or structure.

32.10.3. Certificate: At all times PSC PROCERT reserves the right to suspend or revoke any certificate in accordance with the procedures and policies set forth in this certification practice statement (CPS) and certificate policy (PC).

32.10.4. Distinguished names: Intellectual property rights in distinguished names and customer identification numbers are not the responsibility of PSCPROCERT unless otherwise specified in a contract or agreement.

32.10.5. Intellectual property: The intellectual property of this document of the Certificate Practice Statement (CPS) and policy of certificates (PC), as well as of all the information, publications and documents generated by the PSC PROCERT and contents or not within its web page (procert.net.ve), are the exclusive property of PSC PROCERT.

32.11. Representations and guarantees: The PSC PROCERT maintains an independent exercise as a commercial company, with respect to its trademarks and protected copyright. In addition, PSC PROCERT maintains representation agreements with

different IT companies, IT security and electronic certification, as well as providers of cryptographic hardware.

The guarantees associated with the products that PSC PROCERT sells and sells other than electronic signatures or certificates will be processed by PSC PROCERT and fulfilled before its domestic customers.

32.12. Obligations and civil liability.

32.12.1. Obligations of the registration authority (AR): The registration authority (AR) of the PSC PROCERT assumes under this document, compliance with a number of technical, legal and procedural requirements, which are listed below:

32.12.1.1. To abide by and comply with the mandates of the Constitution of the Bolivarian Republic of Venezuela, the Law on Data Messages and Electronic Signatures (LSMDFE), its regulation (RLSMDFE) and other regulatory bodies, laws, decrees, regulations or governmental resolutions are sanctioned and published in official gazette and that regulate the subject of electronic certification or of electronic certification authority and that they are of mandatory compliance. To abide by the guidelines and technical regulations emanating from SUSCERTE.

32.12.1.2. To fulfill and maintain in force the requirements and requirements for accreditation as a provider of electronic certification services under the mandates of the Electronic Data and Electronic Signatures Act (LSMDFE), its regulation (RLSMDFE) or the regulatory bodies that replace and regulate them the activity of certification authorities.

32.12.1.3. Present, maintain and comply with the validity of the insurance policy required by SUSCERTE to operate an electronic certification authority.

32.12.1.4. Comply with the contracts for the provision of certification services maintained with the clients of the certification authority.

32.12.1.5. Maintain and update the PSC PROCERT documentation.

32.12.1.6. Publish on the website (www.procert.net.ve) the certification practice statement (CPS) and certificate policy (PC), revoked certificate list (CRL) and life policy information of certificates of the PSC PROCERT, as well as all the documentation that is obligatory compliance in accordance with the provisions of the decree law on data messages and electronic signatures or the regulations issued by SUSCERTE.

32.12.1.7. Maintain and ensure the confidentiality of the information provided by the users of the electronic certification service. The only exception of confidentiality will be derived from a judicial or legal requirement of information from clients by a legitimate and competent judicial authority to make the request for information and always derived from legal procedure that guarantees the proper notification of the client who owns the information, in order to maintain the privacy protection provided for in the Constitution of the Bolivarian Republic of Venezuela.

32.12.1.8. Maintain a register and archiving of contracting services of PSC PROCERT for a period of ten (10) years as of the date of subscription of each of the contracts for the acquisition of electronic certification certificates.

32.12.1.9. Maintain and update the documentation that is mandatory under the provisions of the decree law on data messages and electronic signatures or SUSCERTE regulations.

32.12.1.10. Verify that the signatories to PROCERT send all necessary documentation according to the type of electronic certificate they wish to acquire.

32.12.1.11. Validate that the information provided by the signatory is correct.

32.12.1.12. To accredit all those signatories that comply with the requirements established by the PSC PROCERT.

32.12.1.13. Identify and propose improvements in the accreditation process, in order to facilitate the accreditation process of the signatories.

32.12.1.14. Comply with company policies in the areas of information technology, administration and human resources.

32.12.1.15. Comply with labor regulations and other social court laws that regulate the relationship between PSC PROCERT and its workers.

32.12.1.16. Comply with the legal rules applicable to the subject of electronic certification and the legal framework applicable to the regular management of PSC PROCERT.

32.12.2. Obligations of the certification authority (CA): The PSC PROCERT assumes under this document the fulfillment of a series of technical, legal and procedural requirements, which are indicated as follows:

32.12.2.1. To abide by and comply with the mandates of the Constitution of the Bolivarian Republic of Venezuela, the Law on Data Messages and Electronic Signatures (LSMDFE), its regulation (RLSMDFE) and other regulatory bodies, laws, decrees, regulations or governmental resolutions are sanctioned and published in official gazette and that regulate the subject of electronic certification or of electronic certification authority and that they are of mandatory compliance. To abide by the guidelines and technical regulations emanating from SUSCERTE.

32.12.2.2. To fulfill and maintain in force the requirements and requirements for accreditation as a provider of electronic certification services under the mandates of the Electronic Data and Electronic Signatures Act (LSMDFE), its regulation (RLSMDFE) or the regulatory bodies that replace and regulate them the activity of certification authorities.

32.12.2.3. Present, maintain and comply with the validity of the insurance policy required by SUSCERTE to operate an electronic certification authority.

32.12.2.4. Comply with the contracts for the provision of certification services maintained with the clients of the certification authority.

32.12.2.5. Maintain and update the PSC PROCERT documentation, in particular the certification practice statement (CPS) document and the certificate policy (PC), the revoked certificate list (CRL).

32.12.2.6. Publish on the website (www.procert.net.ve) the certification practice statement (CPS) and certificate policy (PC) document, information about the revoked certificate list (CRL), as well as all documentation that is mandatory under the provisions of the decree law on data messages and electronic signatures or the regulations issued by SUSCERTE.

32.12.2.7. Fulfill and ensure the performance of annual compliance audits by auditors accredited to SUSCERTE.

32.12.2.8. Maintain and ensure the confidentiality of the information provided by the users of the electronic certification service. The only exception of confidentiality will be derived from a judicial or legal requirement of information from clients by a legitimate and competent judicial authority to make the request for information and always derived from legal procedure that guarantees the proper notification of the client who owns the information, in order to maintain the privacy protection provided for in the Constitution of the Bolivarian Republic of Venezuela.

32.12.2.9. Maintain a register and archive of the contracting of electronic certification services for a period of ten (10) years as of the date of subscription of each of the contracts for the acquisition of electronic certification certificates.

32.12.2.10. Maintain and renew the contract for the provision of services with the data center from which the PROCERT certification authority (CA) certification platform operates.

32.12.2.11. Maintain and update documentation that is mandatory under the provisions of the decree law on data messages and electronic signatures or the regulations issued by SUSCERTE.

32.12.3. Obligations of third parties in good faith: End users of electronic certificates issued by the certification authority (CA) as well as third parties in good faith, must meet the following conditions:

32.12.3.1. Access the PSC PROCERT website (www.procert.net.ve) and activate the electronic certificate purchase buttons.

32.12.3.2. Select the type of certificate the customer wants.

32.12.3.3. Read and accept the content of the contract for the provision of certification services.

32.12.3.4. Read and accept the certification practices of PSC PROCERT.

32.12.3.5. To fulfill and complete under oath of faith the entry of data and contacts of legal or natural persons, as the case may be.

32.12.3.6. Cancel electronically the cost amount of the electronic certificate.

32.12.3.7. Generate your cryptographic keys.

32.12.3.8. Comply with the sending of information supporting your data and contacts, in original or certified copy to the mailbox posted on the website of PSC PROCERT (www.procert.net.ve).

32.12.3.9. Attend the interview set by the registration authority (RA) for validation of customer data and contacts.

32.12.3.10. Comply with the contracted and accepted use of the electronic certificate acquired by the client.

32.12.3.11. Assisting the administrative offices of PSC PROCERT within forty-eight (48) hours following the revocation and publication of the client's certificate on the Certificate Revoked List (CRL) of the PROCERT Certification Authority (CA).

32.12.3.12. Verify the costs associated with registration, renewal of the certificates on the Website (www.procert.net.ve).

32.12.3.13. In all cases, when accepting or receiving the certificate issued to the latter, the customer guarantees the following:

32.12.3.13.1. That the data contained in the certificate is accurate.

32.12.3.13.2. Relying on the content and use of the electronic certificate.

32.12.3.13.3. That the private cryptographic key associated with the public key contained in the certificate has not been compromised.

32.12.3.13.4. That it will only use the cryptographic key pair and the electronic certificates in accordance with the authorized uses for the corresponding type and / or class;

32.12.3.13.5. That it will exercise reasonable care to prevent unauthorized use of the private cryptographic key associated with the public key contained in the certificate;

32.12.3.13.6. That the client will comply with the tax obligations associated with the sale of the electronic certificate, established by the legislation that regulates the matter of taxes, fees or contributions within the Bolivarian Republic of Venezuela.

32.12.3.14. It will notify other users of the certificate, the certification authority (CA) and other Certification Services Providers that processed their issuance (eg Authorized Registration Authority), prior to the expiration of the Certificate, the following:

32.12.3.14.1. That the private key has been lost, stolen, or potentially compromised;

32.12.3.14.2. You have lost control of your private key because your password has been compromised or for another reason;

32.12.3.14.3. Inaccuracy or changes to the content of the certificate;

32.12.3.14.4. That the end customer wishes to suspend or revoke a certificate for any reason it deems appropriate.

All clients wishing to rely on the PSC PROCERT public key infrastructure (PKI), revoked certificate lists (CRLs), certificate chains, this certification practice statement (CPS) document, and (PCs), certificate policies or other certification services or any other information published by PSC PROCERT are required to be in accordance with the contracts for the acquisition of electronic signatures and electronic certificates that have been signed on the website by www.procert.net.ve and in addition to assume the following obligations:

- Verify the validity, suspension or revocation of the certificate, using up-to-date information on the status of the certificate in the CRL.
- Take into account any limitations on the use and limits of responsibility of the certificate;
- Trust Electronic Signatures and Certificates only when such trust is reasonable. In considering the feasibility of dependency, the aspects to be taken into account will include:

    - The Electronic Signature was created during the period of validity of the certificate
    - The Electronic Signature can be successfully verified
    - All public key fingerprints of the certificates within the corresponding certificate chains are successfully verified
    - Certificates in the certificate chain are successfully validated
    - There are no additional circumstances that may affect the reliability of the electronic signature, certificate, certificate chain, or revoked certificate list (CRL).

32.12.4. Obligations of the repository: PSC PROCERT is obliged to maintain in its repository and available its public key, which any client or interested party can access through the website (https://www.procert.net.ve /). In

addition, PSC PROCERT will keep all its issued certificates accessible, including information on its status.

32.13. Disclaimer of Warranties: The PSC PROCERT has guarantees constituted in favor of SUSCERTE and of the customers who own electronic signatures or certificates generated by PSC PROCERT. The warranty waiver will not be applicable in the best safeguard of the customers and SUSCERTE.

32.14. Limitation of Liability.

32.14.1. Limits of Liability and Limited Warranty: The approach of the certification authority (CA) in the use of public key infrastructures, certificates and electronic signatures is to enable large and small organizations, as well as individuals, to benefit from these technologies in the least stressful and efficient way.

To achieve this, the certification authority (CA) provides the certification services described in this Certification Practices Statement (CPS) and Certificate Policy (PC) certification document. This Certification Practice Statement (CPS) and Certificate Policy (PC) document includes the guarantees provided by PROCERT, which cover the safety and procedural regulations that provide various levels of safety and risk management (from low to high). high).

The certification authority (CA) follows the procedures established in the aforementioned guarantees and in doing so is not intended to provide one hundred percent security, which is impossible, with the operating conditions of the certification services. In doing so, the certification authority (CA) simply seeks to increase the overall level of security. Therefore, PSC PROCERT assumes responsibility for compliance with the procedures and safety measures described in the guarantees.

32.14.1.1. Disclaimer: The PSC PROCERT states that it will not assume responsibility for data and procedures that are not envisaged contemplated and indicated in the applicable law decree law on data messages and electronic signatures (LSMDFE), the regulation (RLSMDFE) and the regulations of the SUSCERTE, within these procedures, guarantees and processes the following are stated:

32.14.1.2. The achievement of specific results.

32.14.1.3. Of merchantability or fitness for a particular purpose,

32.14.1.4. Regarding the accuracy or reliability of the information contained in the Certificates that are not supplied and / or verified by the registration authority (AR).

32.14.1.5. They are not related to the topics covered by this Certification Practices Statement (CPS) and Certificate Policy (PC).

32.14.1.6. On the responsibility or commercial or financial stability of third parties that provide certification services under their own authority or using or depending on certification services, in cases of double certification;

32.14.1.7. On legal validity, the ability to satisfy formal requirements or the testing status of electronic signatures, certificates or cryptographic keys and.

32.14.1.8. With respect to matters beyond the reasonable control of the certification authority (CA).

32.14.1.9. If the certification authority (CA) is responsible for its non-compliance with the guarantees or for any other reason, the compensation will be provided for in the bond established by SUSCERTE, however it will be observed at all times that the payment of excessive damages that are (as a public authority can not be held responsible for what a person does with an "Electronic Signature"). In the case of an electronic signature, it is not possible to determine what is required. The certification authority (CA) therefore requires members of the PROCERT public key infrastructure community to consent to the fact that PROCERT assumes no liability for any damages arising out of the circumstances described below (including damages special, consequential, incidental, indirect or punitive damages), whether or not they have been notified of them (or their potentiality), or whether they are reasonably foreseeable or not.

32.14.1.10. Underlying transactions between customers and third parties, including dependent parties;

32.14.1.11. Third Party services and / or products (including hardware and software) that interact or use certification services, certificates, electronic signatures, etc;

32.14.1.12. If there is a delay, mutilation, or loss or other errors in relation to the data or documents while they are created, stored or communicated;

32.14.1.13. Unacceptable dependence on a Certificate, an electronic signature, a cryptographic key or key pair, or the certification

services to which this certification policy and declaration of certification practices statement (CPS) refer;

32.14.1.14. Non-compliance by third parties (including members of the PROCERT public key infrastructure (PKI) community) with local data protection or privacy legislation, consumer protection legislation, or any other legislative or regulatory compliance required by local jurisdiction; or

32.14.1.15. Any indirect or consequential damages, loss of profits, loss of goodwill, loss of estimated savings, loss of profits, loss of business, interruption of business; or loss of information.

32.14.1.16. For greater protection of risks related to the condition of certification services and to guarantee the long-term stability of public key infrastructure (PKI), the amount of any recognized damage is also limited under the conditions set out in the insurance policy required by the SUSCERTE for the operation of the PSC PROCERT.

32.14.2. Limitations of losses: The limits of the liability of PSC PROCERT to the clients, is regulated by contractual agreements with these clients. As a reference to these contracts are incorporated this document of the Certificate Practice Statement (CPS) and policy of certificates (PC) and the other accreditation policies elaborated by PSC PROCERT and referred in the Information Security Policy of this one.

Unless explicitly agreed or explicitly incorporated into an electronic signature or certificate, PROCERT's liability to customers, suppliers or interested parties is limited to claims of any kind, including contractual, illegal, extra-contractual and of a criminal nature, in each particular certificate regardless of the number of transactions, electronic signatures or causes of action arising or related to said certificate or any service provided in respect of said certificate and cumulatively.

Any and all claims arising from the public key infrastructure (PKI) in connection with an electronic signature or 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 Certification Practices Statement (CPS) and Certificate Policy (PC) statement. The maximum responsibility for the certificate of the Public Key Infrastructure (PKI) of the PSC PROCERT will be established in the corresponding certificate.

This limit of liability for certification shall apply without regard to the number of transactions, electronic signatures or causes of action arising or related to such certificate or any service provided in respect of such certificate and on a cumulative basis. subject to the above limitations, the aggregate liability of the certification authority (CA) of the PSC PROCERT to all customers, dependent parties and any entity other than subordinate public-key infrastructure (PKI) entities, or throughout the period of validity of a certificate issued by the certification authority (CA) of PSC PROCERT (unless revoked or suspended before its expiration), to all persons in relation to said Certificate is fifteen thousand tax units (15,000 UT). In no case shall the liability of PSC PROCERT exceed the above limit.

32.15. Compensation: All compensation will be the result of a process of investigation and analysis or of resolution of conflicts according to the section 31.19 of the present document and where in a proven way of determining the responsibility of PSC PROCERT derived from negligence or malice.

32.16. Deadline and termination.

32.16.1. Term: Any client who keeps or maintains a claim against PSC PROCERT, must notify it in the shortest time and within two (2) weeks following the occurrence of the fact considered as a basis or claim basis. All claims will be processed and will be directly related to the period of validity of the electronic signature or certificate generated by PSC PROCERT. No claims will be processed after the validity of an electronic signature or certificate expires.

32.16.2. Completion: All claims generated by client owners of electronic signature or certificate must be processed and substantiated by PSC PROCERT, maintaining written evidence of each process.

The agreement or termination of each claim will produce a document of agreement between the PSC PROCERT and the corresponding client, leaving the solution to the complaint, the date and the conformity and termination of Law granted by the client concernedTodo reclamo generado por cliente propietario de firma o certificado electrónico deberá ser tramitado y sustanciado por el PSC PROCERT, manteniendo evidencia escrita de cada proceso.

32.17. Notifications: Unless explicitly stated otherwise in this Certification Practices Statement (CPS) and Certificate Policy (PC) document, notifications must be made

either by an electronically signed message that can be verified with a certificate capable of being validated within the public key infrastructure PKI) of the PSC PROCERT or sent via registered mail or similar mail services that provide a receipt indicating the delivery. In both cases, the notification shall be effective upon receipt of a digitized acknowledgment or a receipt of regular mail indicating the delivery signed by the person or entity sending the notification. If it is not received within forty-eight (48) business hours from the time it was supposed to be received by the certification authority (CA) of PSC PROCERT, the notification shall be deemed not to have been received by the licensing authority. certification (CA) of PSC PROCERT. The notifications, according to the previous paragraph must be sent to the following email or postal address:

Proveedor de Certificados (PROCERT), C.A.
Multicentro Empresarial del Este, Núcleo B, Torre Libertador,
Piso 13, Oficina B-132, Municipio Chacao, Caracas
E-mail: contacto@procert.net.ve
Código Postal 1063
Teléfono máster: +58-0212-2674880
Fax: +58-0212-2671270.

32.18. Modifications.

32.18.1. Change specification procedure: The CPS change specification process shall be carried out in accordance with numeral 32.22 of this certification practice statement (CPS) and certificate policy (PC).

32.18.2. Procedures of publication and notification: The process of publication and notification of changes made to the documentation of the PSC PROCERT that requires a publication on its website (www.procert.net.ve) in accordance with the guidelines imposed by SUSCERTE must comply previously the steps contemplated in section 31.22 of this document, have the approval of SUSCERTE to proceed with its publication and notification to customers of the update via email. Internally, PSC PROCERT will record all changes made to its documentation through the use of the document adjustment format (AC-F-0001).

32.18.3. CPS approval procedure: The CPS adjustment process will be carried out in accordance with the provisions of section 31.22 of this certification practice statement (CPS) and certificate policy (PC).

32.19. Conflict resolution.

32.19.1. Out-of-court dispute resolution: PSC PROCERT and the contracting client acknowledge that a prompt and equitable settlement of disputes that may arise in connection with the operation, generation or sale of electronic signatures and electronic certificates will result in their own interests and in the execution of the contracted service. To this end, they declare their decision to make every possible effort to resolve any disputes that may arise through negotiation at the relevant levels. If the dispute has not been resolved through the aforementioned negotiation, within fifteen (15) working days after its commencement, then, at the request of the contracting user, the dispute shall be submitted to SUSCERTE), pursuant to established in number 13 of article 22 the Decree with force of law on data messages and electronic signatures. The solution reached with the mediation of SUSCERTE and accepted by the parties, will be binding and mandatory.

The User will also be free to go to the body responsible for the protection, education and defense of the user according to the Law that regulates the subject. In case of not reaching an agreement, the claim process will be free by ordinary process.

32.19.2. Competent jurisdiction. In the event of not having resolved the possible conflicts in accordance with what is established in section 31.19.1. that precedes, the contracting client will be free to go to the ordinary court, being the competent jurisdiction of the courts of the metropolitan area of Caracas.

32.20. Applicable legislation: The provisions of the Certification Practice Statement (CPS) and Certificate Policy (CP) are not regulated in accordance with current legislation and applicable to the matter within the Republic Bolivariana of Venezuela.

32.21. Compliance with applicable law: All processes, procedures, technical and legal information contained in this certification practice statement (CPS) and certificate policy (CP), are in an elaborated whole and in accordance with established in the decree law on data messages and electronic signatures and the norms of sublegal rank emanated from SUSCERTE.

32.22. Of the adjustments to the document: In any case the adjustments to the documentation required by the SUSCERTE for the operation of a PSC, will be realized in each opportunity that a change occurs in the normative and legal

framework applicable to the PSCs, when a technical change occurs that justifies the adjustment or change, when required by SUSCERTE or every six (6) months.

32.22.1. Document Development Mechanism: This document of the Certification Practices Statement (DPC) and Certification Policy (PC) is developed based on the accreditation regulations applicable to those interested in becoming a PSC. This accreditation regulation is issued and issued by SUSCERTE. In addition, this document of the Certification Practices Statement (DPC) and Certificate Policy (PC) complies with the requirements of the international regulations applicable to the electronic certification area.

32.22.2. Mechanism for adjustment of the document: Changes in the decree law of data messages and electronic signatures, its regulations, the regulations of SUSCERTE or the international regulations binding and required for the operation of the PSC, which contemplates substantial changes in the processes safety and operational procedures, which include changes in the procedures and activities of the PSCs, shall produce a revision of this Document, in order to adjust the processes and procedures to the standards and regulations applicable and approved by SUSCERTE for the operation of the PSCs. Any adjustment to this document of the Certification Practices Statement (DPC) and Certificate Policy (PC) will be the product of the work of the technical and legal team of the PSC PROCERT and will require for its implementation, with the approval of senior management, in accordance with the provisions of 32.22.3. Of the present apart.

The adjustment process will be documented and carried out in accordance with the documentation and document management policy document (AC-PO-0002).

32.22.3. Mechanism for approval of adjustments to the document: Any adjustment or modification of the certification practice statement (CPD) document and the certificate policy (PC), must have the approval of the PSC PROCERT senior management, be documented and be in writing, indicating the edition and revision number, date of elaboration, date of approval and the signature of the representative of the senior management that approves the adjustment or modification.
The adjustment or modification and its approval shall be documented in accordance with the documentation and document management policy document (AC-PO-0002)

33. **Legal and regulatory framework**.
    - Decree law of message of data and electronic signatures and its regulation.
    - Regulation of the superintendence of electronic certification services (SUSCERTE).
    - PROCERT regulations.
    - Internacional International standard ITU-T X.509 V3.
    - International Standard ITU-T X.609.
    - ISO 9000: 2005.
    - ISO / IEC 9594-8 standard.
    - ISO / TR 10013: 2001.
    - ISO / IEC 27001: 2006
    - CA BROWSER Forum, version 1.5.2 september 20 de 2017

34. **Functions and responsibilities within the certification authority (CA):** The roles and responsibilities of the different levels of the certification authority (CA) regarding the management, control and safeguard of this document are defined within the document for the establishment of roles and responsibilities (AC-PO-0003).

35. **Actors subject to the fulfillment of this document:** This document of the Certificate Practice Statement (CPS) and policy of certificates (PC), issued by PSC PROCERT according to the guidelines of SUSCERTE, constitutes a mandatory norm compliance and restraint by the actors listed below:

    35.1. High Direction of PSC PROCERT.
    35.2. Employees of PSC PROCERT.
    35.3. Users of electronic certificates issued by PSC PROCERT.
    35.4. Interested Party using electronic certificates by PSC PROCERT.

36. **Review, approval and modification**: The processes associated with the revision, approval, modification or adjustment of the PROCERT PSC documentation shall be governed by the documentation and document management policy (AC-PO-0002).