CHANGE CONTROLS

VERSION	DATE	DESCRIPTION	ELABORATED	REVISED	APPROVED
1	24/10/2019	NEW DOCUMENT	SGI CORDINATOR	POLICY COMMITTEE	POLICY COMMITTEE
2	15-11-2021	PKI SERVICES' Exclusion of Liability was included. -Reference is made to the models and minutes of the contracts to be used by the users. - Services 2 and 3 are related - The Revocation procedure set forth in the CPD was updated. - Adjustments were made to the Policy Administration. - The mechanisms used for identity validation were adjusted. - The Personnel Training requirements were reviewed and adjusted. - The Use of Keys and Certificates is reviewed and adjusted.	SGI CORDINATOR	POLICY COMMITTEE	POLICY COMMITTEE
3	12-03-2023	Point 11 was withdrawn, which was taken to point 4.1.3, which was also updated .	SGI CORDINATOR	POLICY COMMITTEE	POLICY COMMITTEE

CONTENT

1. INTRODUCTION

1.1. PRESENTATION OF THE DOCUMENT

This document constitutes the Certification Practices Statement (CPS) to provide digital certification services of PKI SERVICES S.A.S., in compliance with laws, regulations, technical standards and criteria, according to current legislation.

This CPS establishes the practices carried out by PKI SERVICES S.A.S. to issue, manage, revoke, and renew digital certificates, following the accepted international standards for public key infrastructure (PKI) such as the standard RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

This document is of public nature and is intended for all natural and legal persons, Applicants, Subscribers, Relying Third Parties and the general public.

In the event of vulnerabilities being detected, or the technical standards or infrastructure indicated in this CPS are no longer in force, PKI SERVICES S.A.S. will inform ONAC of such fact, to proceed with the respective update.

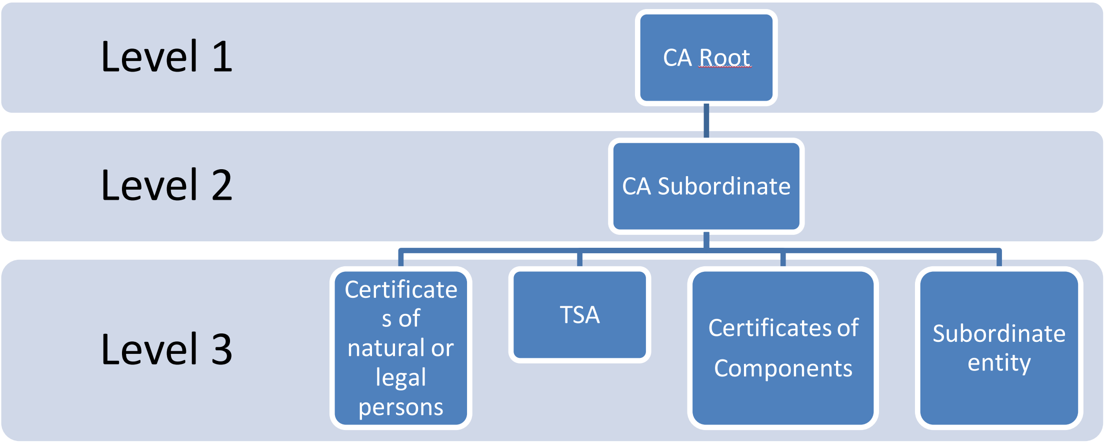
The General Manager administers and reviews annually the Certification Practices Statement, to ensure that it complies with the Specific Accreditation Criteria. This review must be done sufficiently in advance of the annual renewal of the policy.

1.2. DOCUMENTS NAME AND IDENTIFICATION

The identification data of the present document are specified in the initial table Document identification.

1.3. PARTICIPANTS OF THE PKI OF PKI SERVICES S.A.S.

1.3.1. HIERARCHY OF CERTIFICATES OF THE PKI OF PKI SERVICES S.A.S.


Level 1
CA Root
Level 2
CA Subordinate
Level 3
Certificates of natural or legal persons
TSA
Certificates of Components
Subordinate entity

Level 1: Root Certification Authority

Root Certification Authority (or Root CA) is the entity within the hierarchy that issues certificates to other Certification Authorities and whose public key certificate has been self-signed. Its function is to sign the certificate of the other CAs belonging to the Certification Hierarchy. The identification data of the current Root Certificate of PKI SERVICES S.A.S. ROOT, is detailed in the document Certificate

Policies - CP.

Level 2: Subordinate Certification Authority.

Subordinate Certification Authority is the certification authority within the hierarchy that inherits the trust of the ROOT CA and issues Level 3 Certificates. Its public key certificate has been digitally signed by the Root Certification Authority PKI SERVICES S.A.S. ROOT.In this case, the identification data of the current Level 2 Certificate, generated and managed by PKI SERVICES S.A.S. through which it issues Level 3 Certificates, is detailed in the document Certificate Policies - CP.

The PKI SERVICES S.A.S. Root CA also issues the Time Stamping Unit (TSU) certificate of the ECD PKI SERVICES S.A.S. Time Stamping Authority (TSA) (PKI SERVICES TSA - TSU 01).

Likewise, the PKI SERVICES S.A.S. Root CA may issue certificates from other Subordinate CAs of the PKI SERVICES group, which must be reflected in the corresponding TSAs of these Subordinate CAs. Therefore, PKI SERVICES Root CA may also be the Root CA of other PKI SERVICES PKIs.

Level 3: Intermediate Certification Authority.

Level 3 Intermediate or Subordinate Certification Authority is called the certification authority within the hierarchy that issues the entity certificates of end users, and its public key certificate has been digitally signed by the Subordinate Certification Authority of PKI SERVICES S.A.S. N2 Issues the final certificates to subscribers. In this case, PKI SERVICES S.A.S. will act as certification services provider for the SubCA located in Colombia. The SubCA has the following Level 3 Intermediate Certification Authority, whose most relevant information is detailed in the document Certificate Policies - CP. d) End User Certificates.

1.3.2 PKI SERVICES CA ROOT

PKI SERVICES Root is the Root Certification Authority (Root CA) of PKI SERVICES S.A.S. that issues the certificate of the Subordinate Certification Authority (Subordinate CA) of ECD PKI SERVICES S.A.S. (ECD PKI SERVICES). Therefore, PKI SERVICES Root is the Root CA of the PKI SERVICES S.A.S. PKI certificate hierarchy.

PKI SERVICES S.A.S., in its role of Digital Certification Entity (DCE), is the private legal entity that provides digital certification services indistinctly.

PKI SERVICES S.A.S., as ECD, will be responsible for carrying out all the necessary administrative formalities and procedures before ONAC to achieve and maintain the accreditation.

The ECD PKI SERVICES S.A.S., in its role as Subordinate CA, issues and revokes certificates, and provides revocation verification services through CRL and OCSP.

Likewise, ECD PKI SERVICES S.A.S. provides the services of Registration Authority, which is in charge of certifying the validity of the information provided by the Applicant of a digital certificate, through the verification of its identity and the respective evidence record, and of managing the requests for issuance and revocation of digital certificates.

Below are the identification data of ECD PKI SERVICES S.A.S. and its suppliers:

1.3.3. IDENTIFICATION OF THE ECD - AC PKI SERVICES S.A.S.

Company name: PKI SERVICES S.A.S.

N.I.T(Taxpayer Identification Number in Colombia): 901301044-4

N° registration in the Colombian Chamber of Commerce: 03136692

Certificate of existence and legal representation from the Chamber of Commerce

and Single Tax Registry (RUT in Colombia) can be consulted in the INF section.

CORPORATE of the PKI SERVICES web site: https://pkiservices.co/

Active status in the Colombian Chamber of Commerce: consult with NIT 901301044-4 at:

CONFECAMARAS (Confederation of Chambers of Commerce of Colombia): https://www.rues.org.co/ consult

DIAN: https://muisca.dian.gov.co/WebRutMuisca/DefConsultaEstadoRUT.faces

Social business address and comercial correspondence address: Calle 127B Bis No. 46-63, Bogotá D.C., Colombia

Address for physical correspondence and judicial notifications: Calle 127B Bis No. 46-63, Bogotá D.C., Colombia.

Telphone: +57 3506202222

E-mail address: info@pkiservices.co

PQRS Attention: It can be consulted in the CUSTOMER SERVICE section of the PKI SERVICES website, option PQRS SUPPORT. https://pkiservices.co/

Web page: www.pkiservices.co

Root CA and Subca Certificates: Can be consulted in the CUSTOMER SERVICE section of the PKI SERVICES web page. https://pkiservices.co/

OID: 1.3.6.1.4.1.54689.1

1.3.4. APPLICANT

Applicant: is the natural or legal person who requests ECD PKI SERVICES S.A.S. to issue a digital certificate or digital certification service

1.3.5. SUSCRIBER

Subscriber: is the natural or legal person in whose name ECD PKI SERVICES S.A.S. uses a digital certificate and, therefore, acts as the person responsible for it, and who, with knowledge and full acceptance of the rights and duties established and published in this CPS and in the corresponding CP and having signed the respective Subscription Contract with PKI SERVICES S.A.S., accepts the conditions of the certificate issuance service provided by the latter.

The Subscriber is responsible for the use of the private key associated with the certificate issued in his name by ECD PKI SERVICES S.A.S., who is exclusively bound to an electronic document digitally signed using said private key.

1.3.6. THIRD PARTY WHO TRUSTS

Tercero que confía (o Tercero aceptante) son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en un certificado digital emitido por la ECD PKI SERVICES S.A.S.

1.3.7. ENTITY TO WHICH THE SUBSCRIBER IS LINKED

The entity to which the Subscriber is related is, if applicable, the legal entity or natural person (whether it is a company, a public or private organization, a professional association or the natural person itself in the event that it carries out an economic activity of any kind and for the exercise of which it is obliged to register in a fiscal or tax registry) to which the Subscriber is related by means of the relationship accredited in the certificate.

1.3.8. TIME STAMPING

Time stamping is the ideal complement to the security offered by digital identity certificates. Through the application of time stamping, the exact moment in which the signature of a document was produced is guaranteed. The PKI SERVICES S.A.S. Time Stamping Service is based on the specification of the RCF 3161- Internet X509 Public Key Infrastructure standard, which is detailed in the document Certificate Policies - CP.

1.3.9. POLICY AUTHORITY

For the hierarchies described in this document the Policy Authority (PA) is the policy and security committee. This is therefore the Policy Authority (PA) of the Hierarchies and Certification Authorities described above, hence the General Manager is responsible for the administration of the CPD and the Policy Committee for approval.

To contact the policy authority (PA)	
Policy manager	General Manager
Policy approval	POLICY AND SECURITY COMMITTEE
E-mail address	info@pkiservices.co
Address	Street 127B bis #46-63
Telephone	(+57) 350 620 22 22
URL	http://pkiservices.co

1.3.10. CERTIFICATION SERVICE PROVIDER (DCE)

This CPS defines the Certification Service Provider (Digital Certification Entity - DCE) as the entity that provides specific services related to the life cycle of digital certificates and associated services such as the issuance of time stamps (time stamping), provision of signature devices or validation services. Esta CPS define al Prestador de Servicios de Certificación (Entidad de Certificación Digital - ECD) como aquella entidad que presta los servicios concretos relativos al ciclo de vida de los certificados digitales y servicios asociados como la emisión de sellos de tiempo (estampado cronológico), provisión de dispositivos de firma o servicios de validación.

Company name of the ECD - AC	PKI SERVICES S.A.S.
NIT	901301044-4
N.º Registration of Chamber of Commerce of Colombia	03136692
Active status in Chamber of Commerce	Active - https://www.rues.org.co/
Business and correspondence address	Street 127B Bis #46-63 of.102
Telephone	(+57) 350 620 22 22
E-mail	info@pkiservices.co
Web page	http://pkiservices.co
Office Responsible for subscriber and user petitions, inquiries, and complaints	http://pkiservices.co Customer Service, PQRS Support section

1.3.11. REGISTRATION AUTHORITY (RA)

A Registration Authority (RA) is responsible for the management of applications, identification and registration of Certificate applicants and any specific responsibilities established in this CPS and the Certification Policies. RAs are delegated authorities by the ECD, although the ECD is ultimately responsible for the service. The ECD may exercise at any time the duties of RA.

1.3.12. DECISION OFFICER

The OD Decision Officer is the officer(s) of the ECD responsible for making the decision to issue or revoke a digital certificate, or to provide or modify certification services.

1.4.1 DIGITAL CERTIFICATION SERVICES

1.4.1.1 TYPES OF DIGITAL CERTIFICATES

Information on the types of digital certificates that are offered by PKI SERVICES can be found in GE-PO-018 CERTIFICATE POLICY. AVAILABLE section of the PKI SERVICES web page. https://pkiservices.co/

1.4.1.2 OTHER DIGITAL CERTIFICATION SERVICES

Information on the types of digital certificates that are offered by PKI SERVICES can be found in GE-PO-018 CERTIFICATE POLICY. AVAILABLE in PKI SERVICES web page. La información de los tipos de certificados digitales que son ofrecidos por PKI SERVICES se encuentra en GE-PO-018 POLITICA DE CERTIFICADOS Puede consultarse en la sección INF. DISPONIBLE de la página web de PKI SERVICES https://pkiservices.co/

1.4.2 APPROPRIATE USES OF CERTIFICATES

In the description of each type of certificate in this CPS and in the corresponding CP, the respective appropriate uses of the certificates are indicated.

In the case of the use of certificates for centralized signature, the formats of digital signatures constructed by services offered by PKI SERVICES S.A.S. follow the following technical standards:

1.4.3. UNAUTHORIZED USES OF CERTIFICATES

Use contrary to Colombian regulations, customs, morals and public order is not permitted. The use different from what is established in this CPS and in the corresponding CP is not allowed either.

The certificates have not been designed, cannot be destined and are not authorized for use or resale as hazardous situation control equipment or for uses that require fail-safe performance, such as the operation of nuclear facilities, navigation or area communications systems, or weapons control systems, where a failure could directly lead to death, personal injury or severe environmental damage.

The certificates issued to Subscribers cannot be used to sign public key certificates of any kind, nor to sign certificate revocation lists.

The ECD PKI SERVICES S.A.S. does not offer the private key recovery service, and it is not possible to recover the encrypted data with the corresponding public key in case of loss or disablement of the private key or the device that holds it by the Subscriber. The Subscriber who decides to encrypt information will do so in any case under his own and sole responsibility, without PKI SERVICES S.A.S. having any responsibility for loss of information resulting from the loss of the encryption keys. Therefore, PKI SERVICES S.A.S. does not recommend the use of digital certificates for the encryption of information.

1.5. CPS AND PC ADMINISTRATION

1.5.1 RESPONSIBLE ORGANIZATION

This Declaration of Practices and the Certification Policies are property of PKI SERVICES S.A.S., the administration is the responsibility of PKI SERVICES S.A.S. Management.

1.5.2 CONTACT INFORMATION

For questions or comments related to this CPS or the associated CPs, the interested party may contact PKI SERVICES S.A.S. through any of the following means: registered office and correspondence -

commercial, telephone, fax, commercial email addresses or PQRS of the Digital Certification Entity indicated in section 1.3.3.

is available on our web page, section CUSTOMER SERVICE, option CONTACT of the PKI SERVICES web page https://pkiservices.co/

is available on our website, section CUSTOMER SERVICE, option PQRS SUPPORT of the PKI SERVICES website https://pkiservices.co/

1.5.3 APPROVAL PROCEDURE

This CPS and the associated CPs are approved by the PKI SERVICES S.A.S. Policy Committee before being published, controlling the versions of the same, in order to avoid unauthorized modifications and impersonations and the use of obsolete documentation.

The new approved versions of this CPS and associated CPs are sent to ONAC and published on the PKI SERVICES S.A.S. website. https://pkiservices.co/ section INF. AVAILABLE.

The changes in each new version will be indicated in the initial version history table.

1.6. DEFINITIONS AND ABBREVIATIONS

1.6.1 DEFINITIONS

Algorithm: a prescribed set of well-defined, ordered and finite instructions or rules that allows an activity to be carried out by means of successive steps that do not generate doubts for who must carry out the activity. Given an initial state and following the successive steps, a final state is reached and a solution is obtained.

Appeal (PQRS): request submitted by a client to reconsider any adverse decision made by ECD in relation to the services provided.

Certification Authority: Certification Authority (CA). It is a trusted entity, responsible for issuing and revoking digital certificates, publication of certificates, publication of revoked certificates lists, etc. Named within the Colombian regulations as Digital Certification Entity - ECD.

Registration Authority: legal person, with the exception of notaries public, or internal part of the ECD necessarily independent of its AC, which according to the regulations in force, is in charge of receiving the requests related to digital certification, for:

- Register the requests made by applicants to obtain a certificate.
- Check the veracity and correctness of the data provided by users in the requests.
- Send the requests that meet the requirements to a CA for processing.

Time stamping authority (TSA): Trusted entity that issues time stamps by means of one or more TSUs. Named within the Colombian regulations as Digital Certification Entity - DCE. The time stamps issued by the DCE, according to the regulation established by ONAC, include the date and time referenced by the Colombian legal time source.

AC Root: First level Certification Authority, trust base.

CA Subordinate:. Certification Authority of second level or more levels.
Private Key: see Signature Creation Data. Public Key: see Signature Verification Data.

Digital certificate: electronic data message signed by the DCE, which identifies both the issuing DCE and the subscriber and contains the subscriber's public key.

Client: in digital certification services, the term "client" identifies the natural or legal person with whom the DCE establishes a business relationship.

Corporation (Entity): legal entity or natural person, whether it be a company, a public or private organization, a professional association or the natural person itself in the event that it carries out an economic activity of any kind and for the exercise of which it is obliged to register in a fiscal or tax registry..

Signature Creation Data (Private Key): unique numeric values that, when used in conjunction with a known mathematical procedure, serve to generate the digital signature of a data message.

Signature Verification Data (Public Key): data that are used to verify that a digital signature was generated with the subscriber's private key.

Certification Practices Statement (CPS): A document detailing the procedures that the ECD applies to the provision of its services. A statement of the practices that EDC employs to issue, manage, revoke and renew certificates without and with change of keys.

Entity: see Corporation

Certification Entity : in accordance with the stated in Law 527 of 1999, Article 2, Section d, that natural or legal person that, authorized in accordance with said Law, is empowered to issue digital certificates in connection with digital signatures of persons, to offer or facilitate the services of registration and time stamping of the transmission and reception of data messages, as well as to perform other functions related to communications based on digital signatures.

Digital Certification Entities – DCE: denomination that is established to particularize and differentiate this type of organizations as Certification Entities from other Certification Bodies that ONAC accredits. Certification Entity that provides the service of issuing certificates, including other digital certificate management, in accordance with the regulations established by ONAC.

Chronological stamping (Time stamp, Time stamp, Time stamp or Time stamping):: digitally signed and time-stamped data message by a TSA that links to another data message with a specific point in time, which allows to establish with a proof that these data exist at that time and that they did not suffer any modification from the moment in which the stamping is made.

Centralized Signature: centralized signature" is the name given to the centralized management of digital certificates, so that these certificates operate from a single, controlled and secure repository. In practice, this implies that digital certificates are generated and stored on the server, which allows them to be used from any computer or mobile device.

Digital Signature: shall be understood as a numerical value that is attached to a data message and that, using a recognized mathematical procedure, linked to the originator's password and the text of the message, makes it possible to determine that this value has been obtained exclusively with the originator's password and that the initial message has not been modified after the transformation has been carried out.

Hash Function: operation performed on a set of data of any size, so that the result obtained is another set of data of fixed size, regardless of the original size, and which has the property of being univocally associated to the initial data.

Centralized HSM: cryptographic device in which the subscribers' cryptographic keys are generated, stored and protected in a secure way, allowing centralized signature or signature in the cloud.

List of Revoked Digital Certificates (CRL): aquella that list that must include all the certificates revoked by the ECD.

Log: event logging service of the information system, leaving the previous and current information, identifies who and when the event took place.

Security levels: different levels of guarantee offered by electronic signature variables whose benefits and risks must be evaluated by the person, company or institution that intends to opt for an electronic signature modality to send or receive data messages or electronic documents.

OID: unique object identifier (object identifier). OID. Acronym of the English term "Object Identifier", which consists of a unique identification number assigned on the basis of international standards and commonly used to identify documents, systems, equipment, etc., in order, among other things, to know the origin, ownership and age of the identified object.

Individual natural person: natural person that is not a Corporation or Entity.

Petición (PQRS): request submitted by a client or interested party regarding the services provided by ECD.

PKI: Public Key Infrastructure. It is the set of hardware, software, policies, procedures and technological elements that, through the use of a pair of cryptographic keys, a private one that only the subscriber of the service possesses and a public one, which is included in the digital certificate, achieve:

- Identify the sender of an electronic data message.
- Prevent other people from observing messages sent through electronic means.
- Prevent a third party from altering the information that is sent through electronic means.
- Prevent that the subscriber of the digital certification service that sent an electronic message can later deny such sending.

Certificate Policy (PC): set of rules indicating the requirements of a certificate in a particular community and/or class in particular, within the framework of legal, regulatory and common security requirements.

Supplier: The term "supplier" includes organizations, individuals, manufacturers, distributors, technology assemblers and others that supply products, goods and services. Among the suppliers of the DCEs are: Reciprocal entities, technology companies that provide services in their different modalities such as: hosting, colocation, document repository (electronic or physical), device provider, telecommunications provider, etc.

Complaint (PQRS): expression of a dissatisfaction presented by a client or stakeholder regarding the services provided by DCE or the complaint handling process itself.

Complaint (PQRS): expression of a dissatisfaction presented by a client or interested party with respect to the services provided by the ECD, for which some type of compensation is sought.

Revocation: process by which the issued digital certificate is disabled and its period of validity of use is terminated from the date of revocation, upon the occurrence of any of the causes established in the Declaration of Revocation of Certification.

Digital certification service: set of certification activities offered by DCE to certify the origin and integrity of data messages, based on digital or electronic signatures, time stamping, as well as on the applicability of technical standards admitted and in force in public key infrastructure – PKI.

Timestamp: see Chronological stamping

On-line OCSP certificate status service: real-time query activity to the DCE system on the status of a digital certificate through the OCSP protocol.

Applicant: natural or legal person who, with the purpose of obtaining digital Certification services from a DCE, demonstrates compliance with the requirements established in the CPD and the corresponding CP to access the digital Certification service. Natural or legal person that requests the issuance of a certificate to the DCE.

Suggestions (PQRS): recommendation proposed by a customer or stakeholder for the improvement of the services provided by CDE.

Subscriber: natural or legal person in whose name a digital certificate is issued. Natural or legal person who, having signed the respective Subscription Contract, accepts the conditions of the certificate issuance service provided by the DCE.

Relying Third Party (Third Party Acceptor): natural or legal person who receives a digitally signed document, log, notification or any other data, and who trusts the validity of the corresponding digital certificate issued by the DCE.

Token: cryptographic hardware device supplied by an CDE, which contains the subscriber's digital certificate and private key.

Time-stamping unit (TSU): a set of hardware and software that is managed as a unit and has a single time-stamp signing key active at an instant in time.

1.6.2 ACRONYM

CA Certification Authority

CRL Certificate Revocation List

DN Distinguished Name

CPS Certification Practices Statement

DCE Digital Certification Entity that provides digital certification services and is equivalent to a Certification Entity as defined in law 527 of 1999. It should also be understood as a Conformity Assessment Body - CAB as defined in ISO/IEC 17000

FIPS Federal Information Processing Standards (FIPS). These are publicly announced standards developed by the United States government for use by all non-military government agencies and government contractors. Many FIPS standards are modified versions of standards used in the broader communities (ANSA, IEEE, ISO, etc).

HSM Hardware Security Module

IEC International Electrotechnical commission

ISO International Organization for Standardization

ITU International Telecommunication Union

NIF Tax Identification Number

NIT Tax Identification Number

NOC Network Operation Center

OCSP Online Certificate Status Protocol

ONAC National Accreditation Organization of Colombia (Organismo Nacional de Acreditación de Colombia)

PC Certificate Policy

PKCS Public-Key Cryptography Standards. Public-key cryptography standards devised and published by RSA Laboratories

PKI Public Key Infrastructure

PQRS Petitions, Complaints, Grievances, Suggestions and Appeals

RA Registration Authority

RFC Request For Comments. A series of publications by the Internet Engineering Task Force (IETF) describing various aspects of the operation of the Internet and other computer networks, such as protocols, procedures, etc.

RSA Rivset, Shamir y Adleman. It is a public key cryptographic system developed in 1977. It is the first and most widely used algorithm of its kind and is valid for both encryption and digital signing

RUES Single Corporate and Social Registry (Registyro Único Empresarial y Social)

SHA Secure Hash Algorithm

SOC Security Operation Center

TSA Time Stamping Authority

TSU Time Stamping Unit (Unidad de sellado de tiempo)

2. RESPONSIBILITIES REGARDING REPOSITORIES AND PUBLICATION OF INFORMATION

2.1. REPOSITORIES

The following information can be consulted in the INF. AVAILABLE section of the PKI SERVICES web page https://pkiservices.co/

- **PKI SERVICES S.A.S. Root CA Certificate**
- PKI SERVICES S.A.S. Subordinate CA Certificate
- Revoked Certificates List (CRL)

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The PKI SERVICES S.A.S. Policy Committee is in charge of the approval of the CPD, the PC the policies and the Subscription Contract. It can be consulted in the INF. AVAILABLE section of the PKI SERVICES website. https://pkiservices.co/

2.3. TIME OR FREQUENCY OF PUBLICATION

Root CA and Subordinate CA Certificates

The certificates of the Root CA and the Subordinate CA will be published and will remain on the PKI SERVICES S.A.S. web page during all the time that the ECD is providing digital certification services.

List of Revoked Certificates (CRL)

PKI SERVICES S.A.S. will publish on its website the CRL of the Root CA and the Subordinate CA in the events and with the periodicity defined in section 4.9.6.

Certification Practice Statement (CPS), Certificate Policies (CP) and Subscription Contract

PKI SERVICES S.A.S will publish on its website each new approved version of the CPD, the CPs and the Subscription Contract, replacing the previous version that will not be maintained on the website.

2.4 REPOSITORY ACCESS CONTROLS

The aforementioned available repositories are freely accessible for consultation by the general public. PKI SERVICES S.A.S. is responsible for the integrity and availability of the information published.

The organization has the necessary resources and procedures to restrict access to these repositories for purposes other than consultation by persons outside PKI SERVICES S.A.S

3. IDENTIFICATION AND AUTHENTICITY

3.1.1 CUMPLIMIENTO AL PRINCIPIO CONSTITUCIONAL DE LA BUENA FE

PKI SERVICES S.A.S. must comply with Article 83 of the Colombian Constitution, on the principle of good faith: "The actions of individuals and public authorities must adhere to the postulates of good faith, which shall be presumed in all the steps that they advance before them".

3.1.2 FALSEHOOD IN PRIVATE DOCUMENT.

The applicants and/or subscribers must comply with LAW 599 OF 2000, by which the Penal Code is issued Article 289. "Falsehood in private document. Whoever falsifies a private document that may serve as evidence, shall incur, if he uses it, in prison from one (1) to six (6) years".

PKI SERVICES S.A.S. reserves the right not to issue the certificate if it considers that the facial biometric CHECK does not correspond, or if the identification document does not correspond, or if the applicant is on one of the money laundering lists or if documentation provided is not sufficient.

3.2. NAMES

3.2.1. TYPES OF NAMES

All certificates require a distinguished name (DN or distinguished name) of the certificate holder in accordance with the X.500 standard.

Additionally, certificate holder DNs are consistent with the following standards:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

3.2.2 NEED FOR THE NAMES TO HAVE MEANING

The fields of the DN of the certificate holder referring to Names and Surnames and/or Name or Company Name shall correspond to the legally registered data of the Subscriber, expressed exactly in the format that appears in the Citizenship Card, Alien Registration Card or Passport and/or in the Certificate of the Chamber of Commerce and/or Single Tax Registry (or equivalent documents).

In the event that the data contained in the DN of the certificate holder is fictitious or its invalidity is expressly indicated in the DN (e.g. by the word "PROOF" or "INVALID"), the certificate will be considered invalid, only valid for technical interoperability tests.

3.2.3. ANONYMITY AND PSEUDO-ANONYMITY OF SUBSCRIBERS

No anonymity or pseudonymity is allowed to identify subscribers.

3.2.4. UNIQUENESS OF NAMES

The distinguished name (DN) of issued certificate holders shall be unique for each Subscriber.

Attributes of the DN of the certificate holder containing the type and number of the identity document and/or tax identification number are used to distinguish between two identities when there is a problem of duplicity of names.

3.2.5. RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

SERVICES S.A.S. makes no commitments in the issuance of certificates with respect to the use by Subscribers of a commercial trademark.

PKI SERVICES S.A.S. does not knowingly permit the use of a name whose right of use is not owned by the Subscriber. However, ECD is not obliged to search for evidence of trademark ownership prior to the issuance of certificates.

3.3 IDENTITY VALIDATION

3.3.1 METHOD OF PROOF OF POSSESSION OF THE PRIVATE KEY

In the CP of each type of certificate the method of proof of possession of the private key for each of the types of media on which the corresponding certificates can be issued.

certificates can be issued is specified.

3.3.2 AUTHENTICATION OF A NATURAL PERSON'S IDENTITY

The RA will reliably verify the identity of the applicant Natural Person against his/her identity document online. To do so, the Natural Person must scan his/her face and send a legally recognized document that identifies him/her and show the original document during the videoconference. This authentication mechanism is called live biometric facial recognition.

The RA will validate that the identity document presented is apparently legitimate and that the data contained therein (country of issue, type and number of the identity document, names and surnames) are in accordance with the corresponding data entered in the certificate application form. It also validates that the face corresponds to the identity document presented.
The RA will keep the documentation related to the support of the validation of the identity of the individual natural person Subscriber and/or Applicant of the certificate.

3.3.3. ENTIDAD AUTHENTICATION OF AN ENTITY'S IDENTITY

In order to issue the digital certificates, the RA asks the applicant for the following data to authenticate the identity of the Legal Entity or Natural Person:

- The data relating to the name or company name of the Entity (Legal Entity or Natural Person).

- The data relative to the constitution and legal personality of the Entity (Legal Entity).

- The data related to the extension and validity of the powers of representation of the legal representative of the Entity (Legal Entity).

- The data related to the tax identification number of the Corporation or Entity (Legal Entity or Natural Person).

- The data related to the complete address of the Entity (Legal Entity or Natural Person). The RA will verify the above data through the following procedures:

- Request of the citizenship card or document recognized in law that identifies you.

- Request of Certificate of the Chamber of Commerce or equivalent document, in the applicable cases; issued in Colombia (by default) or in another country a maximum of 30 days before.

- Request of the Single Tax Registry or equivalent document, in all cases; issued in Colombia (by default) or in another country.

- Request for an additional official document supporting the scope of the digital certificate requested.

- The identification mechanism is online, by means of biometric facial identification, it is compared against a legally recognized identity document that identifies it, and the certificate of existence and representation against the Single Business Register. RUES of Confecámaras, to verify the existence of the entity and that it is active.

PKI SERVICES S.A.S. reserves the right not to issue the certificate if it considers that the documentation provided is not sufficient or for the verification of the aforementioned data.

The RA will keep the documentation related to the support of the validation of the identity of the Corporation or Entity identified in the certificate.

3.3.4. UNVERIFIED SUBSCRIBER AND APPLICANT INFORMATION

Under no circumstances shall RA omit the information verification efforts leading to the identification of the Subscriber and the Applicant as specified in Sections 3.2.

3.4. IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUESTS WITH CHANGE OF PASSWORDS

PKI SERVICES S.A.S. PKI SERVICES S.A.S. does not attend requirements for renewal of digital certificates with change of keys.

The cases in which a new digital certificate with change of keys is required, due to expiration, upcoming expiration or revocation of a certificate, are treated as a new certificate issuance, performing the same identity validation that was initially done for the first digital certificate, as specified in section 3.2.

3.5. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

The identification and authentication of the Subscriber or Applicant for a certificate revocation request may be performed by:

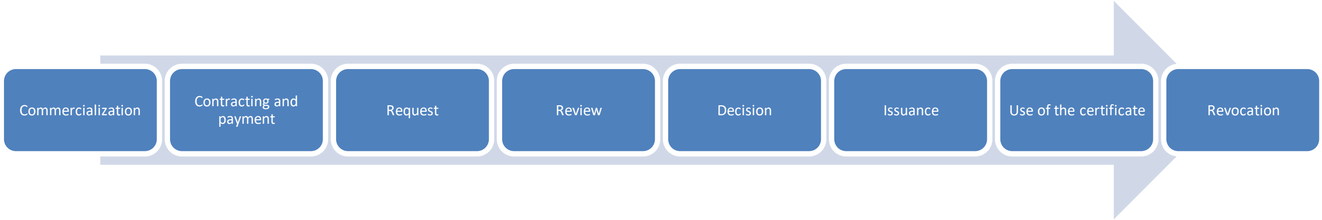
- ONLINE: The Subscriber or Requestor itself, in the event that the Subscriber or Requestor uses the online revocation procedure. The CP of each type of certificate specifies the method by which the Subscriber or Requestor is identified and authenticated for an online revocation request, depending on the type of certificate that has been issued.

-PQRS REQUEST: In case the Subscriber or Applicant uses the revocation procedure through PQRS request, he/she must be previously registered in our web page https://pkiservices.co followed by a communication sent through a Revocation request in the PQRs system, channel that receives and manages PQRS, and then forwards it to the Decision Officer.

- INTERNAL REQUEST: In the case that a revocation request is processed within PKI SERVICES, the applicant must use the revocation procedure through PQRS request, must be previously registered in our web page https://pkiservices.co followed by a communication sent through a Revocation request in the PQRS system, channel that receives and manages PQRS, and then forwarded to the Decision Officer.

4. OPERATIONAL REQUIREMENTS FOR THE CERTIFICATE LIFE CYCLE

The life cycle of digital certificates issued by PKI SERVICES S.A.S. PKI SERVICES S.A.S. extends from the initial marketing to the revocation or expiration of the certificate.



4.1. REQUEST FOR CERTIFICATES

4.1.1. WHO CAN APPLY FOR A CERTIFICATE

1) The prospective Subscriber who is a Natural Person and who correctly supports the information required by the RA, as specified in section 4.1.4 and in the respective CP.

2) An individual Natural Person (not Corporation or Entity) related to the future Subscriber Corporation or Entity (Legal Entity or Natural Person), including a legal representative, attorney-in-fact, employee or person authorized by a legal representative of the Subscribing Legal Entity or by the Subscribing Natural Person itself to request and obtain a certificate for digital signature systems for automated administrative action, who can correctly substantiate the information required by the RA, as specified

in section 4.1.4 and in the respective CP.

3) A Corporation or Entity (Legal Entity or Natural Person) other than the future Subscriber Corporation or Entity, that has been authorized by the legal representative of the Subscribing Legal Entity or by the Subscribing Natural Person itself to request and obtain a certificate for digital signature systems for automated administrative actions, that can correctly support the information required by the RA, as specified in section 4.1.4 and in the respective CP.

4.1.2 COMMERCIALIZATION

The Applicant and/or, where applicable, the Subscriber and/or the Entity to which the Subscriber is bound may receive information about the digital certification process in the following ways:

- By consulting the web page https://pkiservices.co

- By means of informative e-mail from the commercial address

- By dealing directly with Commercial Agents.

- By means of a PQRS available in the web page https://pkiservices.co section CUSTOMER SERVICE, option "SOPORTEPQRS"(SUPPORTPQRS).

By any of these means, they will be provided with information about such process, necessary requirements, fees or other related information.

After the Applicant has been informed, where applicable, the Subscriber and/or the Entity to which the Subscriber is linked shall indicate in the web page https://pkiservices.co/ section SERVICES

1) The type of certificate required and, if it allows several types of supports , the type of support required.

2) The validity of the certificate required.

3) The full name of the Applicant.

4) The type and number of the Applicant's identity document..

5) The email account of the Applicant that will be associated to the digital certificate and through which PKI SERVICES S.A.S. will send notifications and official communications. It should be noted that for personal certificates, the personal e-mail account must be indicated and for corporate certificates, the corporate e-mail account..

En los casos que sea aplicable:

6) The type of certificate required and, if it allows multiple support types, the type of support required.

7) The validity of the certificate required.

8) The full name of the Applicant.

9) The type and number of the Applicant's identity document..

10) The email account of the Applicant that will be associated to the digital certificate and through which PKI SERVICES S.A.S. will send notifications and official communications. It should be noted that for personal certificates, the personal email account must be indicated and for corporate certificates, the corporate email account..

Where applicable:

11) The name or company name of the Subscriber or of the Entity to which the Subscriber is linked.

12) The NIT (TIN in USA) of the Subscriber or of the Entity to which the Subscriber is related to..

If the Applicant is an individual Natural Person, the Commercial Area and/or an OD will send by e-mail to the Applicant and/or, where applicable, to the Subscriber and/or the Entity to which the Subscriber is linked: the Commercial Proposal, where applicable; the Subscription Contract; in the types of certificate that allow it, an authorization model for requesting and obtaining the certificate in case it is required; optionally, a link to the platform; and the respective indications..

4.1.3 CONTRACTING AND PAYMENT

In order to proceed to provide digital certification services or digital services, the Applicant and/or Subscriber, whether a natural person or legal entity, where applicable, must.

- Read and accept the terms and conditions that is the adhesion contract with electronic signature within the framework of decree 2364 of 2012. The evidence of this process of acceptance of terms and conditions, will be the purchase of the service step after acceptance of terms and conditions .
- It should be noted that, in addition to the adhesion contract of Acceptance of Terms and Conditions, at the request of the applicant and/or subscriber, a Service Provision Contract could be created between PKI SERVICES S.A.S. and the applicant and/or subscriber, whether a natural or legal person.

The minutes of the contracts that can be adjusted according to the parties are:

- GC-CN-001 CONTRATO DE SUSCRIPTORES Y/O SOLICITANTE
- GC-CN-002 CONTRATO DE SUMINISTRO DE MARCAS DE TIEMPO
- GC-CN-003 CONTRATO DE SUMINISTRO DE NOTIFICACIÓN ELECTRÓNICA
- GC-CN-004 CONTRATO DE REGISTRO, CUSTODIA Y ANOTACIÓN DE DOCUMENTOS ELECTRÓNICOS TRANSFERIBLES

Make the payment of the respective fee by a valid method and arranged by PKI SERVICES S.A.S., in the cases that are applicable. The evidence of this process will be the voucher or proof of payment.

4.1.4 APPLICATION

The issuance request process will depend on the type of certificate required. The CP for each type of certificate specifies the particular issuance request process for the corresponding certificates. The general issuance request process is described below.

To request the issuance of a digital certificate, the Applicant and/or, where applicable, the Subscriber and/or the Entity to which the Subscriber is linked must enter the system displayed on the web platform https://pkiservices.co/ . Within the platform, they will proceed to enter the required data and attach the requested documents, to finally save their request.

The RA of PKI SERVICES S.A.S. PKI SERVICES SAS. requests all the necessary information for the verification of the identity of the Applicant and/or the Subscriber. The required documents will depend on the type of certificate (specified in the respective PC), which may be and are not limited to the following:

- Citizenship Card, Foreigner ID, or Passport of the Applicant (Individual Natural Person); issued in Colombia (by default) or in another country (equivalent document)..

- Certificate of the Chamber of Commerce or equivalent document of the Subscriber or of the Entity to which the Subscriber is linked; issued in Colombia (by default) or in another country a maximum of 30 days before..

- Unique Tax Registration or equivalent document of the Subscriber or of the Entity to which the Subscriber is linked; issued in Colombia (by default) or in another country (equivalent document)..

- Authorization signed by the Legal Representative of the Legal Entity, or by the Natural Person of the Subscriber or of the Entity to which the Subscriber is linked, with the data of the Natural Person or of the Legal Entity authorized to request and obtain a digital certificate; issued a maximum of 30 days before.

- Identification document: Citizenship Card, Foreigner ID, or passport of the Legal Representative of the Legal Entity, or by the Natural Person who signs the authorization; issued in Colombia (by default) or in another country (equivalent document)..

Also, the RA of PKI SERVICES S.A.S. PKI SERVICES S.A.S. requests the following additional documents for the issuance of a certificate::

- Proof of payment of the certificate fee indicated in the Commercial Proposal, where applicable.

- Acceptance of terms and conditions and/or signed Subscription Agreement, as applicable.

PKI SERVICES S.A.S. has the right to request additional documents to guarantee the correct authentication of the Applicant and/or Subscriber and to carry out an adequate digital certification service.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1 REVIEW

It is the responsibility of the RA to perform the identification and authentication of the Applicant and/or Subscriber automatically and reliably online, according to the type of certificate requested, and as specified in sections 3.2.2 and 3.2.3 and in the corresponding CP, prior online payment.

If payments or documentation need to be regularized, the Applicant will be notified at the e-mail address provided by the Applicant..

Once the OD has validated the documents submitted and the data entered in the certificate request form and, in case the Applicant is an individual Natural Person, has verified his/her identity, the OD will approve the issuance request on the RA platform.

If the information or identity verification is not correct, the RA shall deny the request, contacting the Applicant to communicate the reason.

4.2.2 DECISION

The OD of PKI SERVICES S.A.S. PKI SERVICES S.A.S. is responsible for the decision taken with respect to the digital certification. That is, PKI SERVICES S.A.S. is responsible for approving or denying the digital certification. In the case of denial, PKI SERVICES S.A.S. is responsible for communicating the reason for the rejection to the Applicant.

4.3. ISSUANCE OF CERTIFICATES

4.3.1 ACTIONS OF PKI SERVICES S.A.S. DURING THE ISSUANCE OF CERTIFICATES

Once the application has been approved, the certificate will be issued, which must be securely issued to the Subscriber:

- Uses a certificate generation procedure that securely binds the certificate to the registration information, including the certified public key

- It protects the confidentiality and integrity of the registration data..

- All certificates will become valid at the time indicated on the certificate itself.

In the CP of each type of certificate the particular actions of PKI SERVICES S.A.S. during the issuance of the certificate are specified for each of the types of support in which the corresponding certificates can be issued.

4.3.2 NOTIFICATION TO THE APPLICANT BY PKI SERVICES S.A.S. OF THE ISSUANCE OF THE CERTIFICATE

PKI SERVICES S.A.S. PKI SERVICES S.A.S. will notify the Applicant of the issuance of the certificate and will send the digital certification documentation by e-mail.

The CP of each type of certificate specifies how PKI SERVICES S.A.S. notifies the Applicant of the issuance of the certificate and what documentation of the digital certification is sent, for each of the types of media on which the corresponding certificates can be issued.

4.4. ACCEPTANCE OF THE CERTIFICATE

4.4.1 FORM IN WHICH THE CERTIFICATE IS ACCEPTED

The certificate shall be deemed accepted by the Subscriber and the Applicant, once PKI SERVICES S.A.S. has notified the same to the Applicant, as specified in the respective CP.

4.4.2 PUBLICATION OF THE CERTIFICATE BY PKI SERVICES S.A.S.

SERVICES S.A.S. PKI SERVICES S.A.S. publishes the issued certificates in the repository.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY PKI SERVICES S.A.S. TO OTHER ENTITIES

PKI SERVICES S.A.S. PKI SERVICES S.A.S. does not notify the issuance of certificates to third parties.

4.5. USES OF THE KEY AND THE CERTIFICATE

4.5.1 USE OF THE PRIVATE KEY AND THE CERTIFICATE BY THE SUBSCRIBER

The certificates may be used as stipulated in this CPS and the respective CP.

The Key Usage and Extended Key Usage extensions may be used to establish technical limits to the uses of the private key of the corresponding certificate. The application of these limits will depend largely on their correct implementation by third party software applications, and their regulation is beyond the scope of this document.

4.5.2. USE OF THE PRIVATE KEY AND CERTIFICATE BY RELYING THIRD PARTIES

Relying Third Parties may use the certificates for the purposes set forth in this CPS and the respective PC.

It is the responsibility of the trusting Third Parties to verify the status of the certificate through the services offered by PKI SERVICES S.A.S. which can be consulted in the SERVICES section of the PKI SERVICES web page https://pkiservices.co/ specifically for this purpose and specified in this document.

4.6. CERTIFICATE RENEWAL WITHOUT CHANGE OF KEYS

PKI SERVICES S.A.S. PKI SERVICES S.A.S. does not attend digital certificate renewal requirements, the subscriber must request a new certificate.

The cases in which a new digital certificate is required, due to expiration, next expiration or revocation of a certificate, are treated as a new certificate issuance.

4.7. CERTIFICATE RENEWAL WITH CHANGE OF KEYS

PKI SERVICES S.A.S. PKI SERVICES S.A.S. does not attend digital certificate renewal requirements, the subscriber must request a new certificate.

The cases in which a new digital certificate is required, due to expiration, next expiration or revocation of a certificate, are treated as a new certificate issuance.

4.8. MODIFICATION OF CERTIFICATES

PKI SERVICES S.A.S. PKI SERVICES S.A.S. does not attend requirements of modification of digital certificates, it is revoked and the subscriber must request a new certificate.

The cases in which it is required to modify some data in a digital certificate (update of the information contained in a certificate) are treated as a certificate revocation and a new certificate issuance.

4.9. REVOCATION AND SUSPENSION OF CERTIFICATES

The revocation of a certificate means the loss of its validity and is irreversible. Revocations take effect from the moment they are published in the CRL, these can be consulted in the CUSTOMER SERVICE section of the PKI SERVICES website https://pkiservices.co/ . Likewise, the suspension of certificates that does not lead to an immediate revocation status is not allowed. PKI SERVICES S.A.S. ED does not perform certificate suspensions.

In case a certificate is revoked in relation to electronic or digital signatures, subsequently the same may NOT be reinstated by the ECD.

4.9.1 CERTIFICADO CIRCUMSTANCES OR CAUSES FOR REVOCATION OF A CERTIFICATE

The revocation of a digital certificate may occur either by request of the subscriber, or when the ECD knows, has evidence or confirmation of any of the following situations::

a) Due to compromise of the security for any reason, in any manner, situation or circumstance..

b) By death or supervening incapacity of the subscriber.

c) By liquidation of the represented legal entity that appears in the digital certification service.

d) By the confirmation that any information or fact contained in the digital certificate is false..

e) By the occurrence of new facts that cause that the original data do not correspond to reality..

f) By court order or by order of a competent administrative entity..

g) Due to loss or disablement of the digital certificate that has been reported to ECD.

h) Due to the termination of the subscription contract, in accordance with the grounds established in the contract.

i) For any cause that reasonably induces to believe that the certification service has been compromised to the point that the reliability of the service is put in doubt.

j) Improper handling by the subscriber of the digital certificate..

k) For non-compliance of the subscriber or the legal entity that represents or to which it is linked through the Digital Certification Service Contract provided by the ECD.

4.9.2 WHO MAY REQUEST A REVOCATION

The revocation of a certificate may be requested by:

a) The Subscriber and/or Applicant itself, who shall request the revocation of the certificate in the event of becoming aware of any of the established circumstances or causes for revocation..

b) Any person may request the revocation of a certificate if he/she is aware of any of the established circumstances or causes for revocation..

c) Officials authorized by PKI SERVICES S.A.S.

4.9.3 REVOCATION REQUEST PROCEDURE

There are two alternatives when requesting the revocation of the certificate. In any case, at the time the certificate is revoked, a communication shall be sent to the Subscriber, stating the time and cause of revocation.

4.9.3.1 Online Procedure

PKI SERVICES S.A.S. provides subscribers with the online certificate revocation service through the SERVICES section of the PKI SERVICES website https://pkiservices.co/ . Subscribers who wish to revoke their certificates must cite one of the established causes for revocation.

4.9.3.2 Throughout PQRS

PKI SERVICES S.A.S. provides the service of revocation of a certificate by generating a revocation request ticket in PQRS located in the section CUSTOMER SERVICE option PQRS SUPPORT of the PKI SERVICES website https://pkiservices.co , citing one of the established causes for revocation. This request will be transferred to the Decision Officer to validate the identity and cause for revocation, and make the decision to revoke or not.

Unilaterally PKI SERVICES can revoke a certificate as long as it attends to one of the established causes to revoke a certificate as follows:

–INTERNAL REQUEST: In the event that a revocation request occurs within PKI SERVICES, the applicant must use the revocation procedure by PQRS request, must be previously registered on our website https://pkiservices.co followed by a communication sent by Revocation request in the PQRs system, channel that receives and manages PQRS, then forwarded to the Decision Officer to make the decision to revoke or not..

4.9.4 TIME WITHIN WHICH PKI SERVICES S.A.S. MUST RESOLVE THE REVOCATION REQUEST

PKI SERVICES establishes a maximum of 5 working days to process a revocation..

4.9.5 OBLIGATION OF VERIFICATION OF THE REVOCATIONS BY THE THIRD PARTIES THAT ENTRUST

Verification of certificate status is mandatory for each use of certificates, either by querying the revocation list (CRL) or the OCSP service.

4.9.6 FREQUENCY OF ISSUANCE OF CRLS

The PKI SERVICES Root CA CRL is issued before 180 days have elapsed since the issuance of the previous CRL (prior to its end of validity) or when a revocation occurs.

PKI SERVICES S.A.S. PKI SERVICES CRL (Subordinate CA) is issued at least every 4 days (before the end of validity of the previous CRL); under normal conditions, the CRL is issued every 24 hours.

4.9.7 MAXIMUM TIME BETWEEN THE GENERATION AND PUBLICATION OF CRLS

Once the PKI SERVICES Root CA CRL is issued, it is published at least before the end of validity of the previous CRL (180 days after its issuance); under normal conditions, the CRL is published on the same day of its issuance.

Once the PKI SERVICES S.A.S. PKI SERVICES (Subordinate CA) CRL is issued, it is published at least before the end of validity of the previous CRL (4 days after its issuance); under normal conditions, the CRL is published at the time of its generation, so the elapsed time is considered zero or null.

4.9.8 AVAILABILITY OF THE ONLINE CERTIFICATE STATUS VERIFICATION SYSTEM

The information regarding the status of the certificates shall be available online 24 hours a day, 7 days a week through the PKI SERVICES web page https://pkiservices.co/ INF section. AVAILABLE.

In case of system failure, or any other factor not under PKI SERVICES S.A.S. control, PKI SERVICES S.A.S. will make every effort to ensure that this information service is not unavailable for longer than the maximum period of 8 hours.

4.9.9 ONLINE REVOCATION CHECK REQUIREMENTS

For the use of the freely available CRLs service, the following should be considered:

- The last issued CRL, which may be downloaded at the URL contained in the certificate itself in the CRL Distribution Points extension, must be checked in any case..
- The relevant CRL(s) of the Certification chain of the hierarchy must be additionally checked..
- It must be verified that the revocation list is signed by the authority that issued the certificate to be validated..
- CRL Revoked certificates that expire can be removed from the CRL..

The revocation can also be checked online through the OCSP service, freely accessible at the URL address contained in the certificate itself in the Authority Information Access extension.

4.10. CERTIFICATE STATUS INFORMATION SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

In order to provide information about the validity of an electronic certificate, and therefore the reliability of the electronic signature of a document, PKI SERVICES S.A.S., offers a free service of publication on the Web of Revoked Certificate Lists (CRL) without access restrictions.

PKI SERVICES S.A.S. offers a free service of access to online certificate validation through the OCSP protocol.

Additionally, PKI SERVICES S.A.S. can offer commercial certificate validation services.

4.10.2 SERVICE AVAILABILITY

Information regarding the status of certificates will be available online 24 hours a day, 7 days a week.

In case of system failure, or any other factor not under the control of PKI SERVICES S.A.S., PKI SERVICES S.A.S. will make every effort to ensure that this information service is not unavailable for longer than the maximum period of 8 hours.

4.10.3 ADDITIONAL CHARACTERISTICS

PKI SERVICES S.A.S. may have advanced certificate validation services that require a specific license.

4.11. TERMINATION OF THE SUBSCRIPTION

. The certificate subscription will end at the moment of expiration or revocation of the certificate.

4.12. KEY ESCROW AND RECOVERY

PKI SERVICES S.A.S. PKI SERVICES S.A.S. does not offer a service of custody of backup copies and recovery of subscribers' private keys (key escrow).

5. PHYSICAL, FACILITY, MANAGEMENT AND OPERATIONAL SECURITY CONTROLS.

The systems and equipment used for the operations of the digital certification service are managed in the outsourced Data Center , which is ISO 9001, ISO 27001 and TIER III certified.

The security controls cover the physical environment, networks, systems, among others, which are listed below.

5.1. PHYSICAL CONTROLS

PKI SERVICES S.A.S. has established physical and environmental security controls to protect the resources of the facilities where the systems and equipment used for operations are located.

The physical and environmental security applicable to certificate generation services offers protection against:

- Unauthorized physical access..
- Natural disasters.
- Fire.
- Failure of support systems (electric power, telecommunications, etc.).
- Floods
- Theft
- Unauthorized removal of equipment, information, media and applications related to components used for PKI SERVICES S.A.S. services.

The facilities have preventive and corrective maintenance systems with 24h- 365 days a year assistance with assistance within 24 hours of notification. The location of the facilities guarantees the presence of security forces within 30 minutes.

5.1.1 PHYSICAL LOCATION AND CONSTRUCTION

The data center facilities are built with materials that guarantee protection against brute force attacks, and are located in a low-risk disaster area that allows quick access.

Specifically, the room where cryptographic operations are carried out has a false floor, fire detection and extinguishing, anti-humidity systems, a cooling system and a power supply system.

5.1.2 PHYSICAL ACCESS

Physical access to the premises where Certification processes are carried out is limited and protected by a combination of physical and procedural measures

It is limited to expressly authorized personnel, with identification at the time of access and registration of the same, including CCTV filming.

Access to the rooms is through badge readers.

5.1.3 POWER SUPPLY AND AIR CONDITIONING

The data center facilities are equipped with power stabilizers and a duplicate power supply system for the equipment through a redundant generator set with fuel tanks that can be refilled from the outside.

The rooms that house computer equipment have temperature control systems with duplicate air conditioning equipment.

5.1.4 EXPOSURE TO WATER

housing computer equipment are equipped with a humidity detection system.

5.1.5 FIRE PREVENTION AND PROTECTION

Rooms housing computer equipment are equipped with automatic fire detection and extinguishing systems.

5.1.6 STORAGE SYSTEM

The server systems are run by deploying a highly available virtualized environment, supported by redundant computing devices, high-performance storage and independent production, management and storage networks.

5.1.7. DISPOSAL OF INFORMATION STORAGE MATERIAL

When the sensitive information is no longer useful, it is destroyed in the most appropriate way for the medium containing it:

- Printed matter and paper: by means of shredders or in garbage cans provided for this purpose to be subsequently destroyed, under control.

- Storage media: before being discarded or reused, they must be processed for erasure, either by physical destruction or by rendering the information contained therein unreadable.

5.1.8. OFF-SITE BACKUP COPIES

PKI SERVICES S.A.S. maintains a secure off-site storage facility for the custody of paper documents, electronic devices and documents separate from the Data Center.

At least two specifically authorized persons are required for access, deposit or removal of devices.

5.2. PROCEDURAL CONTROLS

5.2.1 TRUST ROLES

There are different trust roles for the administration and operation of the PKI SERVICES S.A.S. Root CA and Subordinate CA platforms, for the generation and administration of keys and the administration of certificate and CRL profiles of the PKI SERVICES S.A.S. Root CA and Subordinate CA, and for the administration and operation of the PKI SERVICES S.A.S. RA platforms (WEB, RA and Centralized HSM platforms), for the administration and operation of the PKI SERVICES S.A.S. Registration Authority.

In this way, a segregation of functions is guaranteed that disseminates control and limits internal fraud, not allowing a single person to control from start to finish all the Certification and registration functions.

The roles of trust established in the documents of the Integrated Management System Organizational Diagram for the administration of these platforms.

5.2.2. NUMBER OF PEOPLE REQUIRED PER TASK

PKI SERVICES S.A.S. guarantees at least two of three people to perform the tasks that require multi-person control, for access to the CA System, and which are detailed below:

- The generation of the CA key.
- The recovery and back-up of the CA's private key.
- The issuance of CA certificates.
- Revocation of CA certificates.
- CA private key activation.

5.2.3. IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

Each trusted role of the Root CA, Subordinate CA and RA is authenticated through the use of secure authentication mechanisms. Authentication within the previously mentioned platforms allows access to certain PKI SERVICES S.A.S. information assets.

Each person controls the assets required for his or her role, thus ensuring that no person accesses unassigned resources.

5.2.4. ROLES REQUIRING SEGREGATION OF DUTIES

The segregation of duties and incompatibilities are determined in the Organizational Chart.

CA roles (CA Auditor, CA Administrator) are incompatible with RA roles (RA Administrator, RA Agent, RA Auditor).

RA roles (RA Administrator, RA Agent, RA Auditor) are incompatible with each other.

5.3. PERSONNEL CONTROLS

5.3.1. REQUIREMENTS ON PROFESSIONAL QUALIFICATION, EXPERIENCE AND KNOWLEDGE

All personnel who perform tasks qualified as reliable without supervision, have been working at the technical operation center for at least two months and have a permanent employment contract.

All personnel are qualified and have been suitably instructed to perform the operations assigned to them.

PKI SERVICES S.A.S. ensures that the RA personnel are reliable personnel to perform the registration tasks. To this effect, an Authorization is required for their role within PKI SERVICES S.A.S.

PKI SERVICES S.A.S. will remove an employee from their trusted functions when it becomes aware of the existence of the commission of any criminal act that could affect the performance of these functions.

In the integrated management system, there is a procedure for the selection of personnel that defines all the requirements for the selection of personnel for professional roles.

5.3.2. BACKGROUND CHECK PROCEDURE

For entry and on an annual basis, relevant investigations are conducted prior to the hiring of any individual.

5.3.3. EDUCATIONAL REQUIREMENTS

The necessary courses are given to personnel to ensure the correct performance of the tasks assigned to their respective roles, and in accordance with each person's personal knowledge.

As a personnel hiring policy, we look for and hire personnel who are experts and experienced in the defined Roles.

5.3.4. REQUIREMENTS AND FREQUENCY OF TRAINING UPDATES

Training updates will be provided to personnel when modifications are made to the tasks assigned to a role that require it, or when requested by an individual.

5.3.5. SANCTIONS FOR UNAUTHORIZED ACTIONS

The internal work regulations allow PKI SERVICES employees to be sanctioned for unauthorized actions, which may lead to termination of the employee's employment.

5.3.6. REQUIREMENTS FOR HIRING THIRD PARTIES

Employees of PKI SERVICES S.A.S. technology infrastructure and local service providers that have a role assigned within the activity of PKI SERVICES S.A.S. to perform reliable tasks must previously sign the bilateral confidentiality agreement and the operational requirements used by PKI SERVICES S.A.S. Any action that compromises the security of the accepted critical processes may result in the termination of the employment contract.

5.3.7. DOCUMENTATION PROVIDED TO PERSONNEL

PKI SERVICES S.A.S. will make available to all staff the documentation detailing the functions entrusted, policies and practices governing these processes and security documentation.

Additionally, the documentation required by the personnel will be provided at all times, so that they can perform their duties competently.

5.4. SECURITY AUDIT PROCEDURES

5.4.1. TYPES OF LOGGED EVENTS

PKI SERVICES S.A.S. records and saves logs of all events related to PKI SERVICES S.A.S. security system. These include the following events:

- System startup and shutdown.
- Login and logout attempts.
- Unauthorized access attempts to PKI SERVICES S.A.S. systems through the network.
- PKI SERVICES S.A.S. application registration
- PKI SERVICES S.A.S. applications on and off.
- Changes in the configuration of PKI SERVICES S.A.S. and/or its keys.
- Changes in the creation of certificate profiles.
- Generation of own keys.
- Certificate life cycle events.
- Events associated with the cryptographic module.
- Records of the destruction of the media containing the keys, activation data.
- Additionally, PKI SERVICES S.A.S. keeps, either manually or electronically, the following information
- CA key creation ceremonies.
- Changes in personnel performing trusted tasks.
- Records of the destruction of material containing key information, activation data or Subscriber's personal information, if such information is managed.
- Possession of activation data, for operations with PKI SERVICES S.A.S. private keys.

5.4.2. AUDIT LOG PROCESSING FREQUENCY

Audit logs shall be reviewed annually and in any case when a system alert occurs due to the existence of an incident, in search of suspicious or unusual activity.

5.4.3. AUDIT LOG RETENTION PERIOD

Audit log information shall be stored for a period of three (03) years to ensure the security of the system depending on the importance of each specific log.

5.4.4. PROTECTION OF AUDIT LOGS

System logs are protected from tampering by mechanisms that ensure their integrity.

The devices are operated at all times by authorized personnel.

5.4.5. AUDIT LOG BACKUP PROCEDURES

PKI SERVICES S.A.S. has an adequate backup procedure, so that in case of loss or destruction of relevant files, the corresponding backup copies of the logs are available in a short period of time.

Daily incremental and weekly full copies are made.

5.4.6. AUDIT INFORMATION COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Event audit information is collected internally and automated by the operating system.

5.4.7. VULNERABILITY ANALYSIS

PKI SERVICES S.A.S. performs an annual vulnerability review and penetration test to analyze the PKI SERVICES S.A.S. infrastructure. Then the vulnerabilities that PKI SERVICES S.A.S. believes are a risk to it will be analyzed and corrected.

5.4.8. SUPERVISION

PKI SERVICES S.A.S. has a NOC (Network Operation Center) and a SOC (Security Operation Center) to monitor all security and communications supervision tasks of the services offered. The NOC is a service provided by the Data Center.

5.5. LOG FILING

5.5.1. TYPES OF ARCHIVED EVENTS

PKI SERVICES S.A.S. PKI SERVICES S.A.S. will keep the events that take place during the life cycle of the certificate. They will be stored by the CA or, by delegation of the CA, in the RA:

- All audit data,

- All data relating to certificates, including contracts with Subscribers and/or Applicants and data relating to their identification,

- requests for issuance and revocation of certificates,

- all issued or published certificates,

- CRL's issued or records of the status of certificates generated,

- the documentation required by auditors and

- communications between PKI elements

PKI SERVICES S.A.S. is responsible for the correct archiving of all this material and documentation.

5.5.2. RECORDS RETENTION PERIOD

All system data relating to the life cycle of the certificates shall be retained for the period established by the legislation in force when applicable. Certificates shall be retained for at least one year from their expiration. Contracts with Subscribers and/or Applicants and any information relating to the identification and authentication of the Subscriber and/or Applicant shall be retained for at least three (03) years from their termination or the period established by applicable law.

5.5.3. RECORD RETENTION PERIOD

PKI SERVICES S.A.S. ensures the correct protection of the files, including, among others, the information that is collected for the purpose of issuing certificates, by assigning qualified personnel for its treatment and storage in facilities outside the PKI SERVICES S.A.S. Data Center in cases where it is required.

In addition, technical and configuration documents are available detailing all actions taken to ensure the protection of files.

5.5.4. FILE BACKUP PROCEDURES

PKI SERVICES S.A.S. has an external storage center to guarantee the availability of copies of the electronic file archive. Physical documents are stored in secure locations with access restricted to authorized personnel only.

5.5.5. REQUIREMENTS FOR TIME STAMPING OF RECORDS

The records are dated with the reliable source of the National Institute of Metrology (INM) of Colombia, by synchronization through the NTP v4 protocol, according to the standard RFC 5905 "Network Time Protocol Version 4: Protocol and Algorithms Specification".

PKI SERVICES S.A.S. technical and configuration documentation includes a section on the time configuration of the equipment used in the issuance of certificates.

5.5.6. AUDIT INFORMATION ARCHIVING SYSTEM (INTERNAL OR EXTERNAL)

PKI SERVICES S.A.S.'s audit information archiving system is internal, although an external storage center is available to guarantee the availability of copies of the electronic file archive.

5.5.7. PROCEDURES FOR OBTAINING AND VERIFYING ARCHIVED INFORMATION

Recorded events are protected against unauthorized manipulation.

Only authorized personnel have access to physical media files and computer files to obtain and perform file integrity checks.

5.6. CHANGE OF KEYS

The procedure for providing, in the event of a change of keys of the Root CA or the Subordinate CA, the new public key of the CA to the Subscribers, Applicants and Third Party acceptors of the certificates issued with the new keys is the same as for providing the current public key of the Root CA and the Subordinate CA.

Consequently, the new CA certificate containing its new public key will be published on the PKI SERVICES S.A.S. website.

5.7. INCIDENT AND VULNERABILITY MANAGEMENT PROCEDURES

PKI SERVICES S.A.S. has established and tested the continuity and contingency plan aimed at ensuring the continuity of the certification service, in case of any event that compromises the provision of the service.

Any failure to achieve the goals set by this continuity and contingency plan will be treated as reasonably unavoidable unless such failure is due to a breach of the obligations of PKI SERVICES S.A.S. to implement such processes.

In the integrated management system, there is a security procedure for handling incidents, which complies with Annex A of ISO 27001.

The security incidents that are recorded by PKI SERVICES S.A.S., are:

- When the security of a PKI SERVICES S.A.S. private key has been compromised.

- When the security system of PKI SERVICES S.A.S. has been violated.

- When there are failures in the PKI SERVICES S.A.S. system that compromise the provision of the service.

- When the encryption systems become invalid because they do not offer the security level contracted by the Subscriber.

- When any other information security event or incident occurs.

5.7.1. RECOVERY IN CASE OF KEY COMPROMISE

The PKI SERVICES S.A.S. hierarchy contingency plan treats the compromise of a PKI SERVICES S.A.S. private key as a disaster.

In case of compromise of the Root CA's or Subordinate CA's private key, the security of the certificate issuance service will be severely affected, and will proceed according to the Key Management procedure to:

- Inform all subscribers, users and other ECDs with which it has agreements or other types of relationship of the commitment, at least by publishing a notice on the PKI SERVICES S.A.S. website.

- Indicate that certificates and revocation status information signed using this key are not valid.

5.7.2. BUSINESS CONTINUITY AFTER A DISASTER

PKI SERVICES S.A.S. in its integrated management system, has developed the continuity plan to recover all systems after a disaster. The continuity plan has two fronts, one which is the continuity plan of the data center to ensure compliance with 99.9% uptime, and from the front of PKI components.

5.8. TERMINATION OF THE CERTIFICATE ISSUANCE SERVICE

Facing the termination of the certificate issuance service PKI SERVICES S.A.S. shall proceed according to the procedure for the cessation of services as follows:

- Inform in the first instance to the Superintendence of Industry and Commerce and ONAC about the cessation of activities with a thirty (30) days anticipation and request its authorization.

- After having been authorized, inform by means of two notices published in newspapers of wide circulation and by the declared e-mail, to all the Subscribers with an interval of fifteen (15) days about the termination of its activity or activities, the precise date of cessation and the legal consequences of this with respect to the certificates issued.

In any case, the continuity of the service is guaranteed to users who have already contracted the services of PKI SERVICES S.A.S. PKI SERVICES S.A.S., directly or through third parties, without any additional cost to the services contracted.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. KEY PAIR GENERATION

The generation of the CA and SUBCA keys is performed, according to the documented key ceremony process, in certified hardware cryptographic devices (HSM) FIPS 140-2 level 3, by appropriate personnel according to the roles of trust and, at least with dual control and witnesses from PKI SERVICES S.A.S., from the PKI SERVICES S.A.S. holding organization and from an external auditor.

For end-entity certificates, key generation will be performed in devices that reasonably ensure that the private key can only be used by the Subscriber, either by physical means, or by the Subscriber establishing appropriate controls and security measures.

In cases where PKI SERVICES S.A.S. can guarantee that the Subscriber's cryptographic keys have been created in a cryptographic device that meets the minimum requirements (if the media type is Card/Token or Centralized HSM), it will be indicated' in the certificate itself by including the corresponding OID identifier in the Certificate Policies extension.

In any other case (if the media type is Other Devices), the certificates will be issued with a different OID identifier in the Certificate Policies extension.

6.1.2. DELIVERY OF THE PRIVATE KEY TO SUBSCRIBERS

The RA shall be responsible for guaranteeing the delivery of the certificate to the Subscriber and/or Applicant, either by delivering the signature device or by enabling the mechanisms for its download and/or installation and subsequent use, as specified in the respective CP. In this way, it is ensured that the Subscriber and/or Applicant uses, with a high level of confidence, under its exclusive control the signature creation data corresponding to the verification data contained in the certificate.

6.1.3. DEILVERY OF THE PUBLIC KEY TO THE ISSUER OF THE CERTIFICATE

The public key is sent to PKI SERVICES S.A.S. for certificate generation in a standard format, preferably in PKCS #10 or equivalent self-signed format, using a secure channel for transmission.

6.1.4. DELIVERY OF PKI SERVICES S.A.S. PUBLIC KEY TO TRUSTED THIRD PARTIES

. Relying Third Parties will be able to consult the certificates of the Root CA and the Subordinate CA, verify the Certification chain and its fingerprint. These certificates are available to users on the PKI SERVICES S.A.S. website.

6.1.5. KEY SIZE AND VALIDITY PERIOD

Certificate	Key suze RSA (bits)	Periodo validez
Root CA	4096	20 years From: 14/03/2018 13:50:35, time UTC Until: 14/03/2038 13:50:35, tiempo UTC
Subordinate CA	4096	From: 14/03/2018 13:59:37, time UTC Until: 14/03/2038 00:00:00, tiempo UTC
OCSP CA Subordinate	2048	From: 05/04/2018 10:53:48, tiempo UTC Until: 14/03/2038 00:00:00, tiempo UTC
Subscribers	2048	As a maximum, as established in currer legislation and regulations.

6.1.6. PARAMETERS OF PUBLIC KEY GENERATION AND QUALITY VERIFICATION

The parameters recommended in the ETSI TS 119 312 technical specification document are used.

Specifically, the parameters used are the following:

Signature suite	Hash function	Signature algorithm
sha256-with-rsa	SHA-256	RSA-PKCSv1_5

6.1.7 ALLOWED KEY USAGES (ACCORDING TO THE X.509 KEY USAGE FIELD)

All certificates include the Key Usage and Extended Key Usage extensions, indicating the enabled key usages.

The supported uses for Root CA and Subordinate CA certificates are certificate signing and CRL signing.

As for the permitted uses of the key for each end user certificate, they are defined in the corresponding Certification Policy.

6.2. PRIVATE KEY PROTECTION AND ENGINEERING CONTROLS FOR CRYPTOGRAPHIC MODULES

6.2.1. CONTROLS AND STANDARDS FOR CRYPTOGRAPHIC MODULES

The cryptographic modules used to generate and store PKI SERVICES S.A.S. keys are certified with the FIPS 140-2 level 3 standard.

The keys of the Centralized HSM certificate subscribers and of the certificates of operators and administrators of the RA on Card/Token are securely generated using a cryptographic device with FIPS 140-2 level 3, resulting in a high level of assurance to protect the private keys against risks such as:

- Malicious code attacks
- Unauthorized export of keys
- Spoofing due to carelessness of the Subscriber in the custody of cryptographic devices.
- Physical damage to the cryptographic module

6.2.2. MULTI-PERSON (N OF M) CONTROL OF THE PRIVATE KEY

Access to the private keys of the Root CA and the Subordinate CA is under multi-person control. That is, more than one person is required to access and activate the private key, in the case of PKI SERVICES at least 2 of 3 keys are required.

Such control ensures that one person does not have individual control, decentralizing the responsibility for activating and using the private keys of the Root CA and the Subordinate CA.

6.2.3. CUSTODY OF THE PRIVATE KEY

The Root CA's private key is guarded by a FIPS 140-2 level 3 certified hardware cryptographic device, in an off-line state totally disconnected from network and power, guaranteeing that the private key is never outside the cryptographic device. The activation and subsequent use of the private key requires the multi-person control detailed above. After the operation is completed, the session is closed and the private key is deactivated.

The private key of the Subordinate CA is kept in a secure cryptographic device certified with the FIPS 140-2 level 3 standard, guaranteeing that the private key is never outside the cryptographic device. The activation of the private key requires the multi-person control detailed above.

PKI SERVICES S.A.S. does not keep backup copies of the certificate subscribers' private keys (key escrow).

6.2.4. BACKUP COPY OF THE PRIVATE KEY

The copy of the private key of the root CA was made in another identical HSM, which is located in a security envelope in a safe deposit box, to which only the manager with dual control has access.

The SUBCA key is located in HA in the alternate data center.

The keys of the Root CA and the Subordinate CA can be restored by a multi-person process that requires the use of 2 of 3 keys.

6.2.5. ARCHIVING OF THE PRIVATE KEY

PKI SERVICES S.A.S. will archive the certificate signing private keys of the Root CA and the Subordinate CA after the expiration of their validity period or their revocation.

6.2.6. STORAGE OF PRIVATE KEYS IN A CRYPTOGRAPHIC MODULE.

There is a PKI SERVICES S.A.S. key ceremony document, where the private key generation processes and the use of cryptographic hardware are described.

6.2.7. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Las claves de la CA Raíz y la CA Subordinada se activan por un proceso multipersona que requiere la utilización 2 de 3 llaves.

6.2.8. METHOD OF ACTIVATION OF THE PRIVATE KEY

The Root CA and Subordinate CA keys are activated by a multi-person process that requires the use of 2 of 3 keys.

6.2.9 METHOD FOR DESTROYING THE PRIVATE KEY

Devices that have stored any part of the Root CA and Subordinate CA certificate signing private key or their activation data, including devices that contain copies of these keys or their activation data, shall be physically destroyed or reinitialized at a low level.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. PUBLIC KEY FILE

PKI SERVICES S.A.S. will keep all public keys for the period required by current legislation, when applicable, or while the Certification service is active and at least 6 months more, otherwise.

6.3.2. OPERATIONAL PERIODS OF THE CERTIFICATES AND PERIOD OF USE OF THE KEY PAIR

The period of use of a certificate will be determined by its temporary validity.

A certificate must not be used after its validity period, although the relying party may use it to verify historical data, taking into account that a valid online verification service is not guaranteed for that certificate.

6.4. ACTIVATION DATA

6.4.1. GENERATION AND INSTALLATION OF ACTIVATION DATA

The activation data for the Root CA and Subordinate CA keys were securely generated during the CA key creation ceremony.

In the case of operator and administrator certificates of the RA on Card/Token, the activation data (PIN and PUK) are generated at the time of initialization of the cryptographic device.

In the case of Subscriber certificates generated in Centralized HSM, the activation data will be generated at the same time as the keys in the Centralized HSM, at the instant prior to the issuance of the certificate (password), or each time a key is accessed in the Centralized HSM (code received on the cell phone).

6.4.2. PROTECTION OF ACTIVATION DATA

Only authorized personnel have knowledge of the activation data of the Root CA and Subordinate CA private keys.

For end-entity certificates, once the device and/or activation data has been delivered, it is the Subscriber's responsibility to maintain the confidentiality of this data.

6.4.3. OTHER ASPECTS OF THE ACTIVATION DATA

Does not apply.

6.5. INFORMATION TECHNOLOGY SECURITY CONTROLS

PKI SERVICES S.A.S. uses reliable systems and commercial products to offer its Certification services, according to the international standard ISO/IEC 27001.

The equipment used is initially configured with the appropriate security profiles by PKI SERVICES S.A.S. systems personnel, in the following aspects:

- Security configuration of the operating system.

- Security configuration of the applications.
- Correct sizing of the system.
- Configuration of users and permissions
- Event log configuration
- Backup and recovery plan.
- Network traffic requirements.
- Perimeter security is defined by PKI SERVICES, but is managed by the data center.

The technical and configuration documentation of PKI SERVICES S.A.S. details the architecture of the equipment that offers the Certification service, both in its physical and logical security.

6.5.1. SPECIFIC TECHNICAL SECURITY REQUIREMENTS

Each PKI SERVICES S.A.S. server includes the following functionalities:

- Access control to PKI SERVICES S.A.S. services and privilege management.
- Identification and authentication of roles associated to identities.
- Auditing of security-related events.
- Security self-diagnosis related to PKI SERVICES S.A.S. services
- PKI SERVICES S.A.S. system and key recovery mechanisms.

The exposed functionalities are provided through a combination of operating system, PKI software, physical protection and procedures.

6.5.2. NETWORK SECURITY CONTROLS

PKI SERVICES S.A.S. protects physical access to network management devices and has an architecture that orders the generated traffic based on its security characteristics creating clearly defined network sections. This division is made through the use of firewall firewalls, an exclusive VLAN for PKI and VPN for controlled remote access, which are managed by the data center following PKI SERVICES' indications.

6.5.3. LIFECYCLE SECURITY CONTROLS

6.5.3.1 SYSTEM DEVELOPMENT CONTROLS

PKI SERVICES S.A.S. does not develop software; however, it has a procedure for controlling changes in the versions of operating systems and applications that imply an improvement in their security functions or that correct any vulnerability detected.

6.5.3.2 SECURITY MANAGEMENT CONTROLS

6.5.3.2.1 Security Management

PKI SERVICES S.A.S. develops the necessary activities for the training and awareness of employees in security matters.

6.5.3.2.2 Classification and Management of Information and Assets

PKI SERVICES S.A.S. maintains an inventory of assets and documentation.

Each of the policies and procedures indicates its level of confidentiality. Documents are classified in three levels: PUBLIC, INTERNAL and CONFIDENTIAL.

6.5.3.3 Management operations

PKI SERVICES S.A.S. has procedures for incident management and business continuity.

PKI SERVICES S.A.S. has fireproof security boxes with dual control for the storage of physical media.

PKI SERVICES S.A.S. has documented all the procedures related to the roles and responsibilities of the personnel involved in the Certification process.

6.5.3.4 Media handling and security

All media will be handled securely in accordance with information classification requirements. Media containing sensitive data are securely destroyed if they are no longer required.

6.5.3.5 System Planning

The PKI SERVICES S.A.S. Systems department keeps a record of equipment capacities.

In conjunction with the resource control application of each system, a possible resizing can be foreseen.

6.5.3.6 System Access Management

PKI SERVICES S.A.S. makes every reasonable effort to confirm that access to the system is limited to authorized persons. In particular:

6.5.3.7 PKI SERVICES S.A.S. general management::

- Controls are in place based on high availability firewalls and perimeter security both managed by the data center.

- Sensitive data is protected by means of cryptographic techniques or access controls with strong authentication.

- There is a procedure in place for changing the owners and custodians of safes.

- A procedure is in place to ensure that operations are carried out in accordance with the Organizational Chart.

- Each person has an identifier associated with him/her to perform Certification operations according to his/her role.

- PKI SERVICES S.A.S. personnel will be responsible for their actions, for example, for retaining event logs.

• **Certificate generation** :

- PKI SERVICES S.A.S. facilities are provided with continuous monitoring systems and alarms to detect, record and be able to act upon an unauthorized and/or irregular access attempt to its resources.

- The authentication to perform the certificate issuance process is done through a system m of n operators for the activation of the private key of the Root CA and the Subordinate CA of PKI SERVICES S.A.S.

• **Revocation management:**

- PKI SERVICES S.A.S. facilities are provided with continuous monitoring systems and alarms to detect, record and be able to act upon an attempt to access its resources unauthorized and / or irregular to the revocation system.

- Revocation refers to the permanent loss of effectiveness of a digital certificate. The revocation will be performed by strong card authentication to the applications of an authorized administrator. The log systems will generate the proofs that guarantee the non-repudiation of the action performed by the PKI SERVICES S.A.S. operator.

• **Revocation status**

- The revocation status application has an access control based on certificate authentication to prevent attempts to modify revocation status information.

• **Cryptographic hardware lifecycle management**

- PKI SERVICES S.A.S. ensures that the cryptographic hardware used for signing certificates is not manipulated during its transportation.

- The cryptographic hardware is built on supports prepared to avoid any manipulation.

- PKI SERVICES S.A.S. registers all relevant information of the device to add to the PKI SERVICES S.A.S. asset catalog

- The use of the cryptographic certificate signing hardware requires the use of at least two trusted employees.

- The cryptographic device is only handled by trusted personnel.

- The configuration of the PKI SERVICES S.A.S. system as well as its modifications and updates are documented and controlled.

- The changes or updates are authorized by the security responsible and are reflected in the corresponding work minutes. These configurations will be made by at least two reliable people.

6.5.4. COMPUTERS AND INFORMATION TECHNOLOGY SECURITY ASSESMENT

The security of the equipment is reflected by an initial risk analysis in such a way that the security measures implemented are a response to the probability and impact produced when a group of defined threats can take advantage of security breaches.

Physical security is guaranteed by the facilities already defined above and personnel management is easy due to the small number of people working in the outsourced Data Center.

6.6. TIME SEALING

The time for PKI SERVICES S.A.S. services are obtained by consulting the Colombian legal time to the National Institute of Metrology (INM) of Colombia, in accordance with the provisions of Article 14 of Decree 4175 of 2011.

The servers are kept updated with UTC time, by synchronization through the NTP v4 protocol, according to the standard RFC 5905 "Network Time Protocol Version 4: Protocol and Algorithms Specification".

7. PROFILE CERTIFICATE, CRL AND OCSP

7.1. CERTIFICATE PROFILE

7.1.1. CERTIFICATE FORMAT

The certificates issued by PKI SERVICES S.A.S. PKI SERVICES S.A.S. are X.509 v3 certificates, according to the following standards:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

- ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

Additionally, the certificates issued by PKI SERVICES S.A.S. are consistent with the following standards:

The following table specifies the common profile of the certificates issued by the Root CA and the Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S.

COMMON PROFILE OF THE CERTIFICATES			
Certificate field		**Descrition**	**ValUE**
version		N° of version	v3
Serial Number		N° of series	Unique positive integer with respect to th CA issuing the certificate [1]
signature		Algoritmo de firma	OID [2] and signature algorithn parameters
Issuer		Issuer (DN)	DN of the CA issuing the certificate 3 [3]
validity	**notBefore**	Valid since	Date and time of start of validity of th certificate, UTC 4 time
	notAfter	Valid until	Date and time of end of validity of th certificate, time UTC [5]
subject		Subject (DN)	DN of the certificate holder [6]
subjectPublicKeyInfo		Public Key	OID [7] and algorithm parameters an public key value 8.
extensions		Extensions of th certificate	Extensions of the certificate

1. 20-byte random value
2. sha256WithRSAEncryption (SEE OID see in the section 7.1.3)
3. PKI SERVICES S.A.S. Root CA, Subordinate CA and TSU TSA certificates. PKI SERVICES S.A.S: see Root CA DN in section 7.1.4; PKI SERVICES S.A.S. OCSP Subordinate CA and Subscriber certificates. PKI SERVICES S.A.S.: see Subordinate CA DN in section 7.1.4
4. date and time of certificate issuance
5. certificates of Root CA, Subordinate CA and OCSP Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S: see period of validity in section 6.1.5; TSU TSA certificate of PKI SERVICES S.A.S. PKI SERVICES S.A.S. S: see validity period in the CPS for PKI SERVICES S.A.S. time stamping; PKI SERVICES S.A.S. Subscriber Certificates. PKI SERVICES S.A.S: see validity period in the PC corresponding to the type of certificate.
6. PKI SERVICES S.A.S. Root CA and Subordinate CA Certificates PKI SERVICES S.A.S: see DN in section 7.1.4; PKI SERVICES S.A.S. Subordinate CA OCSP Certificate PKI SERVICES S.A.S. PKI SERVICES S.A.S: see DN in section 7.4.4; PKI SERVICES S.A.S. TSU TSA Certificate PKI SERVICES S. A.S.: see DN in section 7.4.4; PKI SERVICES S.A.S. TSU TSA Certificate. A.S. PKI SERVICES S.A.S.: see DN in the CPS for PKI SERVICES S.A.S. time stamping; PKI SERVICES S.A.S. Subscriber Certificates PKI SERVICES S.A.S. PKI SERVICES S.A.S.: see DN of the holder in the PC corresponding to the type of certificate.

[7] rsaEncryption (see OID in the section 7.1.3)

[8] PKI SERVICES S.A.S. Root CA, Subordinate CA, OCSP Subordinate CA and Subscriber Certificates. PKI SERVICES S.A.S: see RSA key size in section 6.1.5; PKI SERVICES S.A.S. TSA TSU Certificate. PKI SERVICES S.A.S: see RSA key size in the PKI SERVICES S.A.S. Time Stamped CPD.

9 PKI SERVICES S.A.S. Root CA and Subordinate CA Certificates PKI SERVICES S.A.S: see extensions in section 7.1.2; PKI SERVICES S.A.S. Subordinate CA OCSP Certificate PKI SERVICES S.A.S. PKI SERVICES S.A.S: see extensions in section 7.4.2; PKI SERVICES S.A.S. TSU TSA Certificate PKI SERVICES S.A.S. PKI SERVICES S.A.S.: see extensions in section 7.4.2. A.S. PKI SERVICES S.A.S.: see extensions in the CPS for PKI SERVICES S.A.S. chronological stamping; PKI SERVICES S.A.S. Subscriber Certificates PKI SERVICES S.A.S. PKI SERVICES S.A.S.: see extensions in the PC corresponding to the type of certificate.

7.1.2. CERTIFICATE EXTENSIONS

The following tables specify the certificate extensions of the Root CA and Subordinate CA certificates of PKI SERVICES S.A.S. PKI SERVICES S.A.S.

ROOT AC CERTIFICATE EXTENSIONS – PKI SERVICES ROOT		
Extension	**Criticism**	**Value**
Subject Key Identifier	-	Identifier of the public key of the certificate, obtained from th SHA-1 hash of the certificate.
Key Usage	Yes	Digital Signature, Certificate Signing, Off-line CRL Signing, CRI Signing (86)
Certificate Policies	-	OID 1.3.6.1.4.1.54689.1 URL of the CPS: on the web page of PKI SERVICES https://pkiservices.co/ section INF. DIOSPONIBLE (availabl information)
Basic Constraints	Yes	CA: NONE

EXTENSIONS TO THE SUBORDINATE AC CERTIFICATE – ECD PKI SERVICES COLOMBIA		
Extension	**Criticism**	**Value**
Authority Key Identifier	-	Public key identifier of the Root CA certificate, obtained from th SHA-1 hash of the Root CA certificate.
Subject Key Identifier	-	Identifier of the public key of the certificate, obtained from th SHA-1 hash of the certificate.

Key Usage	Yes	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Certificate Policies	-	OID 1.3.6.1.4.1.54689.1 URL of the CPS: on the webpage of PKI SERVICES https://pkiservices.co/ section INF. DIOSPONIBLE (available information)
Basic Constraints	Yes	CA: TRUE pathLenConstraint: 0
CRL Distribution Points	-	URI of the CRL: on the webpage of PKI SERVICES https://pkiservices.co/ sección INF. DIOSPONIBLE (available information)
Authority Information Access	-	URI of the certificate of the CA Raíz: on the webpage of PKI SERVICES https://pkiservices.co/ section INF. DIOSPONIBLE (available information)

In section 7.4.2 the extensions of the OCSP certificate of the Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S. are specified.

In the PC of each type of certificate, the extensions of the corresponding PKI SERVICES S.A.S. PKI SERVICES S.A.S. Subscriber certificates are specified.

In the CPS for the PKI SERVICES S.A.S. time stamping, the extensions of the PKI SERVICES S.A.S. PKI SERVICES S.A.S. TSU certificate of the PKI SERVICES S.A.S. TSA are specified.

7.1.3. OBJECT IDENTIFIERS (OID) OF THE ALGORITHMS

Name	OID	Description
Sha512WithECDSAEncryption	1.3.6.1.4.1.54689.1	Certificate and CRL signing algorithm in Root CA
Sha384WithECDSAEncryption	1.3.6.1.4.1.54689.1	Certificate and CRL signing algorithm in subordinate CA.
SHA256WithRSAEncryption	1.3.6.1.4.1.54689.1	Certificate signing algorithm in common certificate profile.

7.1.4. FORMAT OF THE NAMES

The following tables specify the corresponding attributes of the DN of the Root CA and the Subordinate CA PKI SERVICES S.A.S. PKI SERVICES S.A.S.

DN OF THE CA ROOT – PKI SERVICES ROOT		
Attribute del DN	**Description**	**Value**

Country Name (C)	Country	CO [1]
State OD Province Name (ST	State/Province	Bogota DC [2]
Locality Name (L)	Locality	Bogota DC [2]
Street Address (STREET)	Address	see current address a https://pkiservices.co/
Organization Identifie (2.5.4.97)	Organization Identifier	901301044 [2]
Organization Name (O)	Name of the organization	PKI SERVICES SAS [2]
Common Name (CN)	Name	PKI SERVICES Root CA [2]

[1] Encoded in PrintableString

[2] Encoded in UTF8String

DN DE LA CA SUBORDINADA – ECD PKI SERVICES COLOMBIA		
Atributo del DN	**Descripción**	**Valor**
Country Name (C)	Country	CO
State OD Province Name (ST	State/Province	Bogota DC
Locality Name (L)	Locality	Bogota DC
Street Address (STREET)	Address	https://pkiservices.co/contacto
OrganizationIdentifier (2.5.4.97)	Organization identifier	901301044
Organization Name (O)	Name of the organization	PKI SERVICES SAS
Common Name (CN)	Name	ECD PKI SERVICES

In section 7.4.4 the DN of the OCSP certificate of the Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S. is specified.

In the CP of each type of certificate, the DN of the holder of the corresponding PKI SERVICES S.A.S. PKI SERVICES S.A.S. Subscriber certificates are specified.

In the CPS for the PKI SERVICES S.A.S. time stamping, the DN of the TSU certificate of the PKI SERVICES S.A.S. PKI SERVICES S.A.S. TSA is specified.

7.1.5. NAME RESTRICTIONS

As specified in sections 3.1 and 7.1.4 and in the CP of each type of certificate.

7.1.6. CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)

The PKI SERVICES S.A.S. PKI SERVICES S.A.S. Subordinate CA OCSP certificate policy OID is specified in section 7.4.2 and also below: 1.3.6.1.4.1.54689.1

The Certificate Policy OIDs of each type of PKI SERVICES S.A.S. PKI SERVICES S.A.S. Subscriber certificates are specified in section 1.4 and in the corresponding PC.

The PKI SERVICES S.A.S. PKI SERVICES S.A.S. TSA TSU certificate policy OID is specified in the PKI SERVICES S.A.S. PKI SERVICES S.A.S. PKI SERVICES S.A.S. TSU certificate policy OID is specified in the PKI SERVICES S.A.S. PKI SERVICES S.A.S. time stamping CPS.

1 Coded in PrintableString

2 Coded in UTF8String

7.1.7. USE OF THE POLICY CONSTRAINTS EXTENSION

The certificates issued by the PKI SERVICES S.A.S. Root CA. PKI SERVICES S.A.S. defines this extension with a value of zero (0). This indicates that the entity subordinate to the Root CA cannot generate new subordinates from itself.

7.1.8. SYNTAX AND SEMANTICS OF POLICY QUALIFIERS

The Certificate Policies extension of the certificates issued by the Root CA and the Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S. contains the following Policy Qualifiers:

- id-qt-cps (URI of the CPD): contains the URI where the latest version of the present CPD can be found, as well as, in the case of PKI SERVICES S.A.S. PKI SERVICES S.A.S. Subscriber certificates, the PC corresponding to the type of certificate.

7.1.9. CERTIFICATE POLICY SEMANTIC TREATMENT FOR THE CERTIFICATE POLICY EXTENSION

The Certificate Policies extension of the certificates issued by the Root CA and the Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S. PKI SERVICES S.A.S. PKI SERVICES S.A.S. PKI SERVICES S.A.S. PKI SERVICES S.A.S. allows identifying the policy that PKI SERVICES S.A.S. PKI SERVICES S.A.S. associates to the type of certificate and where the present CPD can be found, as well as, in the case of PKI SERVICES S.A.S. PKI SERVICES S.A.S. Subscriber certificates, the CP corresponding to the type of certificate.

7.2. CRL PROFILE

7.2.1. FORMAT AND PERIOD OF VALIDITY OF THE CRL

The CRLs issued by PKI SERVICES S.A.S. PKI SERVICES S.A.S. are X.509 v2 CRLs, according to the following standards:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL). Profile.

- ITU-T X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks and attribute certificate frameworks.

The following table specifies the common profile of the CRLs issued by PKI SERVICES S.A.S. Root CA and Subordinate CA.

CRL PROFILE

CRL Field		**Description**	**Value**
version		N° of version	v2
signature		Signature algorithm	OID [1] and parameters of the signature algorithm
Issuer		Issuer (DN)	DN of the CA, issued by the CRL[2]
ThisUpdate		Date and time of issuance of this CRL	Date and time of issuance of this CRL, time UTC
NextUpdate		Date and time of issuance of the next CRL	Date of end of validity of the CRL, UTC [3] time Date and time of issuance of this CRL
revokedCertificates	**userCertificate**	Serial no. of the revoked certificate	Serial no. of the revoked certificate
	revocationDate	Date and time of certificate revocation	Date and time of certificate revocation, UTC time
	crlEntryExtensions	CRL input extensions CRL input extensions	CRL input extensions CRL input extensions
CrlExtensions		CRL Extensions	CRL Extensions

7.2.2. CRL EXTENSIONS AND CRL INPUT EXTENSIONS

CRL EXTENSIONS		
Extension	**Criticism**	**Value**
Authority Key Identifier	-	Identifier of the public key of the certificate of the CA issuing the CRL, obtained from the SHA-1 hash of the certificate.
CRL Number	-	Incremental number, with respect to the CA issuing the CRL

CRL INPUT EXTENSIONS		
Extension	**Criticism**	**Value**
Reason Code	-	Certificate revocation reason code

[1] sha256WithRSAEncryption (see OID in section 7.1.3)

[2] Root CA CRL: see DN of Root CA in section 7.1.4; Subordinate CA CRL: see DN of Subordinate CA in section 7.1.4

3 Root CA CRL: 180 days; Subordinate CA CRL: 4 days

7.3. OCSP PROFILE

The OCSP profile of the PKI SERVICES S.A.S. Subordinate CA PKI SERVICES S.A.S. conforms to the RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" standard, with the following particularities:

- OCSP response signing algorithm: sha256WithRSAEncryption (see OID in section 7.1.3).

7.4. GSPC CERTIFICATE PROFILE

7.4.1. CERTIFICATE FORMAT

The format of the OCSP certificate of the Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S. complies with the specifications in section 7.1.1.

Additionally, the OCSP certificate of the Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S. is consistent with the following standards:

- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.

The OCSP certificate of the Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S. has been issued by the Subordinate CA itself (PKI SERVICES Colombia).

The key size and validity period of the certificate is indicated in section 6.1.6.

7.4.2. CERTIFICATE EXTENSIONS

The following table specifies the extensions of the OCSP certificate of the PKI SERVICES S.A.S. Subordinate CA. PKI SERVICES S.A.S.

Extension	Criticism	Value
Authority Key Identifier	-	Identifier of the public key of the certificate of the Subordinat CA, obtained from the SHA-1 hash of the certificate.
Subject Key Identifier	-	Identifier of the public key of the certificate, obtained from th SHA-1 hash of the certificate.
Key Usage	Yes	digitalSignature nonRepudiation
Certificate Policies	-	OID 1.3.6.1.4.1.54689.1 URL of the CPS: https://pkiservices.co/cinfodisponible/
Basic Constraints	Yes	CA: END ENTITY
Extended Key Usage	Yes	OCSPSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points	-	URI of the CRL: http://pkiservices.co/info-disponible/pkiservicessubcac1.crl
Authority Informatio Access	-	URI del certificado de la CA Subordinada http://pkiservices.co/infodisponible/pkiservicesrootca.crt

7.4.3. OBJECT IDENTIFIERS (OID) OF THE ALGORITHMS

As specified in section 7.1.3

7.4.4. NAME FORMATS

The following table specifies the corresponding attributes of the DN of the OCSP certificate of the PKI SERVICES S.A.S. PKI SERVICES S.A.S. Subordinate CA.

Attribute of the DN	Description	Value
Country Name (C)	Country	CO [1]
State OD Province Name (ST	State/Province	Bogota DC [2]
Locality Name (L)	Locality	Bogota DC [2]
Street Address (STREET)	Address	https://pkiservices.co/contacto/
Organization Identifie (2.5.4.97)	Organization Identifier	901301044-4 [2]
Organization Name (O)	Organization Name	PKI SERVICES S.A.S. [2]
Common Name (CN)	Name	PKI SERVICES – OCSP [2]

7.4.5. NAME RESTRICTIONS

As specified in sections 3.1, 7.1.4 and 7.4.4.4.

7.4.6. CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)

The OID of the OCSP certificate policy of the PKI SERVICES S.A.S. PKI SERVICES S.A.S. Subordinate CA is specified in section 7.4.2 and also as follows: 1.3.6.1.4.1.51362.0.2.0.1

7.4.7. USE OF THE POLICY CONSTRAINTS EXTENSION

The OCSP certificate of the Subordinate CA of PKI SERVICES S.A.S. PKI SERVICES S.A.S. does not contain the Policy Contraints extension.

[1] Coded in PrintableString

[2] Coded in UTF8String

7.4.8. SYNTAX AND SEMANTICS OF POLICY QUALIFIERS

As specified in section 7.1.8.

7.4.9. SEMANTIC TREATMENT FOR THE CERTIFICATE POLICY EXTENSION

As specified in section 7.1.9.

8. COMPLIANCE AUDIT AND OTHER CONTROLS

PKI SERVICES S.A.S. is subject to accreditation audits performed by ONAC in accordance with the provisions of Article 162 of Decree-Law 19 of 2012. Likewise, in accordance with the requirements of ONAC's Specific Accreditation Criteria, PKI SERVICES S.A.S. submits to internal audits and third party audits in accordance with the terms set forth in the aforementioned document.

If required, PKI SERVICES S.A.S. allows and facilitates audits by the Superintendence of Industry and Commerce of Colombia.

8.1. FREQUENCY OF AUDITS

Audits shall be conducted on an annual basis

8.2. AUDITOR'S IDENTITY/QUALIFICATION

PKI SERVICES S.A.S. accreditation audits are performed by auditors appointed by ONAC.

Internal and third party audits are carried out by auditors that comply with the ONAC Specific Criteria in force and following the internal audit procedure.

8.3. RELATIONSHIP BETWEEN THE AUDITOR AND THE AUDITED ENTITY

The companies that perform the external audits never represent any conflict of interest that may distort their performance in their relationship with PKI SERVICES S.A.S.

8.4. ASPECTS COVERED BY THE CONTROLS

The audits generally verify compliance with the principles established in the accreditation requirements (Specific Criteria of ONAC in force), the applicable legislation in force and the documentation established in the management system of PKI SERVICES S.A.S.. These aspects must be identified and controlled following the internal audit procedure.

8.5. ACTIONS TO BE TAKEN AS A RESULT OF THE DETECTION OF DEFICIENCIES

In the event that incidents or non-conformities are detected, the appropriate measures shall be taken to resolve them in the shortest possible time following the internal audit procedure.

8.6. COMMUNICATION OF RESULTS

The auditing body will communicate with PKI SERVICES S.A.S. through the interlocutor established in each case.

9. OTHER LEGAL AND COMMERCIAL MATTERS

9.1. RATES

9.1.1. CERTIFICATE ISSUANCE RATES

The fees specified in the CPs are referential, and may vary according to the type of certificate and the contract with each client.

The same rates are published on the PKI SERVICES S.A.S. website.

The final price including VAT (IVA in Colombia) for the requested certificate shall be indicated in the commercial proposal.

9.1.2. RATES OF ACCESS TO THE CERTIFICATES

Access to the consultation of the status of issued certificates is free of charge.

9.1.3. RATES FOR REVOCATION OR ACCESS TO STATUS INFORMATION

No rates are established for revocation of certificates, nor for access to certificate status information.

9.1.4. RATES FOR OTHER SERVICES

The rates applicable to other possible services will be negotiated between PKI SERVICES S.A.S. and the clients of the services offered.

9.1.5. REFUND POLICY

PKI SERVICES S.A.S. PKI SERVICES S.A.S. has the refund corresponding to the time remaining for the revocation on the cost of the certificate without including the cost of the device. This if there is one of the causes of revocation.

9.2. FINANCIAL RESPONSABILITIES

9.2.1. INSURANCE COVERAGE

PKI SERVICES S.A.S. has sufficient economic resources to face the risk of liability for damages to the users of its services and to third parties, guaranteeing its responsibilities in its activity as ECD as defined in the Colombian legislation in force (ART. 9 Decree 333 of 2014).

The aforementioned guarantee is established by means of a Civil Liability Insurance with a coverage equal to or higher than that required by the Colombian legislation in force.

The characteristics of such insurance are as follows:

- It is issued by an insurance company supervised by the Financial Superintendence of Colombia.
- Covers contractual and extra-contractual risks and damages of subscribers and third parties in good faith.
- Cover the above risks for an insured amount per event equal to or greater than the greater of:

  7.500 legal monthly minimum wages per event;
- The insurance company is responsible for previously informing ONAC of the termination of the insurance contract or if modifications are made that reduce the scope or amount of the agreed coverage.

The insurance will cover all amounts that PKI SERVICES S.A.S. is legally obliged to pay, up to the contracted coverage limit, as a result of any legal proceedings in which its liability may be declared, derived from any negligent act, error or unintentional breach of current legislation among others.

9.3. CONFIDENTIALITY OF INFORMATION

PKI SERVICES S.A.S. considers confidential all information that is not expressly classified as public. No information declared as confidential will be disseminated without the express written consent of the entity or organization that has granted the confidentiality, unless there is a legal requirement.

9.3.1. CONFIDENTIAL INFORMATION

In particular, the following information will be considered confidential:

- PKI SERVICES S.A.S. Root CA and Subordinate CA private keys.

- Certificate of Ceremony for the generation of the Root CA and Subordinate CA keys.

- Ceremony procedure for the generation of Root CA and Subordinate CA keys.

- The business information provided and/ or elaborated jointly with PKI SERVICES S.A.S by its clients, suppliers or other persons with whom PKI SERVICES is committed to keep secret legally or conventionally established.

- The results of identity validations of Subscribers and/or Applicants, provided by public or private sources.

- The information of the Subscriber and/or Applicant obtained by sources other than the Subscriber and/or Applicant and that has been classified as "Confidential".

- Data collected during digital certification.

9.3.2. NON-CONFIDENTIAL INFORMATION

The following information shall be considered non-confidential:

- That contained in this CPS.

- The information contained in the different Certificate Policies (CP)

- The information contained in the certificates, since for its issuance the Subscriber and/or Applicant previously grants its consent, including the different states or situations of the certificate.

- Certificate revocation lists (CRL's), as well as other revocation status information.

- Any information whose publicity is required by law.

9.4. DATA PROTECTION POLICY

PKI SERVICES S.A.S. guarantees the protection of personal data of Subscribers and/or Applicants of digital certification services, in compliance with the Statutory Law 1581 of 2012, partially regulated by National Decree 1377 of 2013; Decrees 1377 of 2013 and 886 of 2014, Law 1266 of 2008 and other related regulatory decrees, which regulates the provisions of Law 1581 of 2012, which issued the General Regime for the Protection of Personal Data, which aims to "(. ..) to develop the constitutional right of all persons to know, update and rectify the information collected about them in databases or files, and the other rights, freedoms and constitutional guarantees referred to in Article 15 of the Constitution; as well as the right to information enshrined in Article 20 of the Constitution" and the Specific Criteria for Accreditation of Digital Certification Entities - CEA-4.1-10 in force.

Personal data will be considered as, the information of names, address, email, and any information that can be linked to the identity of a natural or legal person, contained in the contracts and applications of the Subscribers and/or Applicants. This information will be considered confidential and will be used exclusively for the stipulated digital certification operations, unless there is prior consent of the end user of such data or there is a judicial or administrative order that so determines.

PKI SERVICES S.A.S. has a Privacy Policy of personal data that details the principles, collection and processing of personal data and is published on the website: https://pkiservices.co/

It is the responsibility of the Subscribers and/or Applicants to ensure that the information provided to PKI SERVICES S.A.S. is truthful and current. Likewise, they are responsible for any damage they may cause by providing false, incomplete or inaccurate information.

Applicants and/or subscribers must comply with LAW 599 OF 2000, by which the Penal Code is issued Article 289. "*Falsehood in private document. Whoever falsifies a private document that may serve as evidence, shall incur, if used, imprisonment from one (1) to six (6) years."*

9.5. INTELLECTUAL PROPERTY RIGHTS

In accordance with the provisions of national laws and international treaties, all intellectual and industrial property rights related to the systems, documents, procedures, revocation lists and any others, related to its activity as ECD, including this CPS and the associated CPs, shall correspond exclusively to PKI SERVICES S.A.S.".

9.6. OBLIGATIONS

9.6.1. OBLIGATIONS OF PKI SERVICES S.A.S.

PKI SERVICES S.A.S. PKI SERVICES S.A.S. is obliged with the provisions of this document, mainly to:

a) Respect the provisions of this CPS and the associated CPs, as well as the Subscription Contract.

b) To publish this CPS, the associated CPs and the Subscription Contract on its Web page, in its current version.

c) To inform about the modifications of this CPS and the associated CPs to the Subscribers, including such modifications in the initial version history table.

d) To have a civil liability insurance that covers the minimum value required by the regulations in force.

e) Use reliable systems to store certificates that allow checking their authenticity and prevent unauthorized persons from altering the data, restrict their accessibility in the cases or to the persons indicated by the Subscriber and/or Applicant, and allow detecting any change that affects these security conditions.

As far as certificates are concerned:

a) Issue certificates in accordance with this CPS, the corresponding CPs and application standards.

b) To issue certificates according to the information in its possession and free of data entry errors.

c) Issue certificates whose minimum content is the one defined by the regulations in force, when applicable.

d) Revoke certificates according to the provisions of this CPS and the corresponding CPs and publish the aforementioned revocations in the CRL (List of Revoked Certificates).

Custody of information:

a) Retain the information on the certificate issued for the minimum period required by the regulations in force, when applicable.

b) Not to store or copy the Subscriber's signature creation data, when so required by the regulations in force.

c) To protect, with due care, the signature creation data while in its custody, if so provided.

d) Protect their private keys in a secure way.

e) Establish the machanisms of generation and custody of the information relevant in the activities described, protecting them against lost, destructions, or falsification.

f) Submit to ONAC, on an annual basis, for the completion of Stage 1 of each accreditation evaluation:

- File with the issued certificates and their respective content.
- File with control totals (issued, valid, revoked and expired).

As Registration Authority (RA) it is also obliged in the terms defined in this CPS for the issuance of certificates, mainly to:

a) Respect the provisions of this CPS and the CP corresponding to the type of certificate it issues.

b) Respect the provisions of the contracts signed with the Subscriber. In the life cycle of the certificates:

- Verify the identity of the Certificate Applicants as described in this CPS or through another procedure that has been approved by PKI SERVICES S.A.S..

- Verify the accuracy and authenticity of the information provided by the Applicant.

- Inform the Subscriber, prior to the issuance of a certificate, of the obligations assumed, the way in which the signature creation data must be stored, the procedure to be followed to report the loss or misuse of the signature creation data or devices, its price, the precise conditions for the use of the certificate, its limitations of use and the way in which it guarantees its possible liability, and the web page where any information from PKI SERVICES S.A.S., the CPS and the PC corresponding to the certificate can be consulted.

- Tramitar y entregar los certificados conforme a lo estipulado en esta CPS y en la PC correspondiente.

- Process the Subscription Contract as established by the applicable Certification Policy.

- Archive, for the period stipulated in current legislation, the documents provided by the Subscriber and/or Applicant.

- Inform the SubCA of the causes for revocation.

- Communicate with the Subscribers, by the means deemed appropriate, for the proper management of the life cycle of the certificates. Specifically, carry out communications regarding the approaching expiration of certificates and certificate revocations.

9.6.2. OBLIGATIONS OF THE PROVIDERS

In the event that PKI SERVICES uses the services of a public key infrastructure provider, the latter is obliged to comply with the following requirements:

a) Responsibility and financing

b) Confidentiality

c) Requirements for resources

d) Process requirements - Digital Certificate Life Cycle

e) Management system requirements

f) CA requirements

g) RA requirements

h) Technical requirements

9.6.3. OBLIGATIONS OF APPLICANTS

The Applicant for a certificate shall be obliged to comply with the provisions of the regulations in force and also to:

a) Provide the RA with the real, true information necessary to make a correct identification.

Applicants and/or subscribers must comply with LAW 599 OF 2000, whereby the Penal Code is issued Article 289. "falsehood in a a private document that may serve as evidence, shall incur, if used, imprisonment from one (1) to six (6) years."

b) To make reasonable efforts to confirm the accuracy and truthfulness of the information provided.

c) Respect the provisions of the contractual documents signed with PKI SERVICES S.A.S.

d) Notify any change in the data provided for the creation of the certificate during its period of validity.

e) Inform as soon as possible of the knowledge of any cause for revocation.

f) Accept terms and conditions of services.

9.6.4. OBLIGATIONS OF SUBSCRIBERS

The Subscriber shall be obliged to comply with the provisions of the regulations in force and also to:

a) Diligently safeguard his/her private keys and/or the activation data thereof (such as passwords or secret codes defined or received by any means).

b) Use the certificate as established in this CPS and in the corresponding CP.

c) Respect the provisions of the legal instruments binding PKI SERVICES S.A.S.

d) To notify any change in the data provided for the creation of the certificate during its validity period.

e) Inform as soon as possible of the existence of any cause for revocation.

f) Not to use the private key or the certificate from the moment it is requested or is warned by PKI SERVICES S.A.S. or the RA of its revocation, or once the validity period of the certificate has expired.

9.6.5. OBLIGATIONS OF RELYING THIRD PARTIES

It shall be the obligation of the Relying Third Parties to comply with the provisions of the regulations in force and in addition:

a) Verify the validity of the certificates at the time of performing any transaction based on the same.

b) To know and be subject to the guarantees, limits and responsibilities applicable to the acceptance and use of the certificates on which they rely, and to accept to be subject to them.

c) Notify PKI SERVICES S.A.S. of any irregular situation with respect to the service provided by PKI SERVICES S.A.S.

9.6.6. OBLIGATIONS OF THE ENTITY TO WHICH THE SUBSCRIBER IS BOUND

In the applicable certificate types, the Entity to which the Subscriber is bound shall be obliged to comply with the provisions of the regulations in force, and also to:

a) Provide the Applicant and/or the RA with the necessary information to carry out a correct identification.

b) To make reasonable efforts to confirm the accuracy and veracity of the information provided.

c) Respect the provisions of the contractual documents signed with PKI SERVICES S.A.S.

d) Notify any change in their knowledge in the data provided for the creation of the certificate during its period of validity.

e) Inform as soon as possible of the knowledge of any cause for revocation.

9.6.7. OBLIGATIONS (DUTIES AND RIGHTS) OF THE APPLICANT AND/OR SUBSCRIBER

9.6.7.1. **USE OF BRAND.**

It is the duty and right of applicants and subscribers, as well as all related parties, to comply with any restrictions or limitations on the use of the PKI SERVICES name and the accreditation mark as the certification mark, and on the manner of making reference to the digital certification granted.

1. The use of the ONAC mark, may only be used by PKI SERVICES S.A.S. in compliance with the provisions of RAC-3.0-03 Regulations for the use of the Accredited and/or Associate symbols that can be consulted at https://onac.org.co/, it is the duty of applicants, subscribers and suppliers not to use the ONAC mark.

2. The use of the PKI SERVICES mark will be authorized to the subscriber and third parties, as indicated in the Policy: GE-PO-017 POLICY FOR USE OF SYMBOLS that is available in the PKI SERVICES web page https://pkiservices.co/ section INF. AVAILABLE option Corporate Policies.

9.6.7.2. DUTIES OF APPLICANTS.

The Applicant for a certificate (either directly or through an authorized third party) undertakes to comply with the legal provisions and to:

1 Deliver truthful and real information to the RA (Article 289, Law 599 DE 2000).
2 Provide all the information required for the registration of the account.
3 Provide accurate and truthful information and provide the documentation indicated in each Application process.
4 Accept and respect the provisions established in the documents subscribed with the SubCA and the RA
5 Accept the terms and conditions policy.

9.6.7.3. RIGHTS OF APPLICANTS.

1 The applicant has the right to request a digital certificate or digital certification service free of any discrimination.
2 The applicant has the right to be informed about the processing of his application.
3 The applicant has the right to access the PKI SERVICES website and all available information.
4 Receive clear and timely response to the PQRS or support required by the Applicant.

9.6.7.4. DUTIES OF SUBSCRIBERS

Article 39, Law 527 of 1999. Duties of the subscribers. The duties of subscribers are
1. Use the certificate in accordance with this CPS and the applicable Certification Policies.
2. Respect the provisions established in the documents signed with the SubCA and the RA.
3. Report any cause for suspension / revocation as soon as possible.
4. Report any change in the data provided to create the certificate during its validity period.
5. Do not use the private key or the certificate once the SubCA requests or reports the suspension or revocation of the certificate, or once the validity period of the certificate has expired.
6. Receive the digital signature from the certification authority or generate it, using a method authorized by it.
7. Provide the information required by the certification authority.
8. Maintain the control of the digital signature.
9. To timely request the revocation of the certificates.
10. Custody and protect in a responsible way the information of the Certificate and the private key.
11. Not to use its digital certification in a way that contravenes the law or causes bad reputation for ECD.
12. Once the digital certification service has expired or been revoked, the subscriber must immediately stop using it in all advertising material containing any reference to the service.

9.6.7.5. **SUBSCRIBERS' RIGHTS**

1 Article 40, Law 527 of 1999. Liability of subscribers. The subscribers shall be liable for the falsehood, error or omission in the information provided to the certification authority and for the breach of their duties as subscriber.
2 To request the revocation of the Digital Certificate in attention to one of the authorized causes of revocation.

9.7. RESPONSIBILITIES

9.7.1. RESPONSIBILITIES OF PKI SERVICES S.A.S.

a) Comply with laws, regulations, technical standards, requirements for its operation.
b) Guarantee that the certificates comply with all the material requirements established in the CPS and that there are no factual errors in the information contained in the certificates, known or made by PKI SERVICES S.A.S. PKI SERVICES S.A.S.
c) To comply with Article 83 of the Colombian Constitution, on the principle of good faith: "The actions of individuals and public authorities must adhere to the principles of good faith, which shall be presumed in all the steps they take before them".
d) Provide the Subscriber and the Applicant with the latest version of the necessary documents.
e) Provide the Subscriber with information on how to validate the certificate, including the requirement to check the status of the certificate and the conditions under which the certificate can be reasonably relied upon, which applies when the Subscriber is acting as a Relying Party
f) Notify the Subscriber about changes in the policies and practices of PKI SERVICES S.A.S. PKI SERVICES S.A.S.
g) Notify the Subscriber of any changes in the basic terms and conditions (policy identifiers, limitations of use, Subscriber obligations, form of validation of a certificate, dispute resolution procedure, period within which audit trails will be retained, applicable legal system and compliance with ONAC requirements).
h) The use of the symbols that characterize the accreditation of PKI SERVICES S.A.S. of PKI SERVICES S.A.S. will be restricted to the accredited scope, and may not be transferred to third parties or inherited outside the digital certification services, persons, processes and third parties evaluated by ONAC; as described in the PKI SERVICES S.A.S. Symbol Use Policy document.
i) Exercise control over the accredited digital certification services, regarding the ownership and use of symbols, certificates, any other mechanism to indicate that the digital certification service is accredited.
j) References to the scope of accreditation granted, or the misleading use of the scope of accreditation granted, symbols, certificates, and any other mechanism to indicate that a digital certification service, or that PKI SERVICES S.A.S. is accredited, in documentation or other advertising will be subject to compliance with the ONAC Accreditation Rules.
k) Attend and respond to requests, complaints, claims and appeals from Subscribers and related parties.
l) Regarding its activities as RA, notify ONAC when a new Registration Office is established, where it will follow the same procedures and comply with the same requirements as PKI SERVICES S.A.S. Main Office.
m) Act impartially in accordance with its Impartiality and Non-Discrimination Policy.

9.7.2 EXCLUSION OF LIABILITY OF PKI SERVICES S.A.S

PKI SERVICES assumes no responsibility in case of loss or damage:

1. Of the services it provides, in case of war, strikes, stoppages, coups d'état, natural disasters or any other case of force majeure.
2. Caused by the use of certificates that exceeds the limits established by the same or the Certification Practices Statement (CPS) of PKI SERVICES.
3. Caused by involuntary omission of professionals or third parties who work or provide a service for PKI SERVICES S.A.S.
4. Caused by the improper or fraudulent use of certificates or CRL'S issued by PKI SERVICES S.A. S.A.
5. Due to the introduction of a computer virus or malicious code in the SSPS by the User or a third party.
6. Internet connection failures, attributable to the User or the User's Internet Service Provider.
7. Caused to third parties in good faith if the recipient of the digitally signed documents does not check or take into account the restrictions contained in the certificate regarding its possible uses, or when not taking into account the suspension or loss of validity of the certificate published in the CRL, or when not verifying the digital signature.

9.7.3. RESPONSIBILITIES OF THE SUBSCRIBER

a) To act in accordance with the stipulations of this CPS of PKI SERVICES S.A.S. PKI SERVICES S.A.S.

b) Provide complete, current and truthful information to PKI SERVICES S.A.S. PKI SERVICES S.A.S.

c) Properly use the certificate regarding its application, limitations and prohibitions of use; as established in the PKI SERVICES S.A.S. CPS.

d) Comply with the requirements stipulated by PKI SERVICES S.A.S. for the respective digital certification service.

e) Comply with new requirements, when PKI SERVICES S.A.S. implements changes in the digital certification services, prior communication of such changes by PKI SERVICES S.A.S. to the Subscriber.

f) That the statements about the certification are consistent with the scope of the digital certification service.

g) Not to use its digital certification in a way that contravenes the law or causes bad reputation for PKI SERVICES S.A.S. PKI SERVICES S.A.S. and does not make any statement related to its certification that PKI SERVICES S.A.S. may consider misleading or unauthorized. Which in turn implies not to monitor, manipulate or reverse engineer the technical implementation of ONAC and PKI SERVICES S.A.S. PKI SERVICES S.A.S. PKI SERVICES S.A.S.; or intentionally compromise the security of the ONAC Hierarchy and PKI SERVICES S.A.S. PKI SERVICES S.A.S. PKI SERVICES S.A.S.

h) Immediately after the cancellation or termination of the digital certification, stop using it in all advertising material containing any reference to it, and take the actions required by the digital certification service and any other previously notified measures.

i) When making reference to the digital certification service in media, such as documents, brochures or advertising, inform that it complies with the requirements specified in the respective PKI SERVICES S.A.S. CP.

j) Comply with the requirements that may be prescribed by the digital certification service in relation to the use of marks of conformity and information related to the service.

k) Inform PKI SERVICES S.A.S., without delay, about the changes that may affect the digital certification that was issued by PKI SERVICES S.A.S.

l) Be diligent in the custody of your private key and the access passwords that protect your private key, in order to avoid unauthorized uses.

m) At all times be responsible for protecting your private key, access passwords and the cryptographic device where your private key is stored without being able to transfer this responsibility to any third party.

n) Request the revocation of the digital certificate in case of: loss, theft or misplacement of the electronic security device that stores your private key; potential compromise of the private key; loss of control over your private key, due to the compromise of the activation data or any other cause; inaccuracies or changes in the content of the certificate that you know or could know.

o) To stop using the private key, after the term of validity of the certificate has elapsed.

p) Failure to validly use the expired certificate from the date on which it expires.

q) Request the revocation of certificates when it fails to comply with the obligations to which it is committed within the requirements of ONAC.

r) Report that it complies with the stipulations of the PKI SERVICES S.A.S. CPD, when it makes reference to the digital certification service in the media (articles, documents, brochures or advertising).

9.8. LIMITATIONS OF RESPONSABILITY

PKI SERVICES S.A.S., will not be responsible in any case when facing any of these circumstances:

a) State of War, natural disasters, malfunction of electrical services, telematic and/or telephone networks or computer equipment used by the Subscriber or Third Parties, or any other case of force majeure.

b) For improper or fraudulent use of the directory of certificates and CRL's (List of Revoked Certificates) issued by the CA.

c) For the improper use of the information contained in the Certificate or CRL.

d) For the content of the messages or documents signed or encrypted by means of the certificates.

e) In relation to actions or omissions of the Applicant and Subscriber:

- Lack of veracity of the information provided to issue the certificate.

- Delay in communicating the causes for revocation of the certificate.

- Absence of certificate revocation request when applicable

- Negligence in the conservation of its signature creation data, in the assurance of its confidentiality and in the protection of any access or disclosure.

- Use of the certificate outside its period of validity, or when PKI SERVICES S.A.S. PKI SERVICES S.A.S. or the RA notifies the revocation of the certificate.

- Extralimitation in the use of the certificate, as provided in the current regulations and in the PKI SERVICES S.A.S. CPD, in particular, exceeding the limits that appear in the electronic certificate in terms of its possible uses and the individualized amount of the transactions that can be made with it or not using it in accordance with the conditions established and communicated to the Subscriber by PKI SERVICES S.A.S.

f) In relation to actions or omissions of the Third Party relying on the certificate:

- Failure to verify the restrictions contained in the electronic certificate or in the PKI SERVICES S.A.S. CPD regarding its possible uses and the individualized amount of the transactions that may be made with it.

- Lack of verification of the loss of validity of the electronic certificate published in the consultation service on the validity of the certificates or lack of verification of the electronic signature.

9.9. INDEMNITIES

9.9.1. INDEMNIFICATIONS FOR DAMAGES CAUSED BY PKI SERVICES S.A.S.

PKI SERVICES, S.A.S. will assume the corresponding indemnities for damages caused to Applicants, Subscribers, Third Parties who trust or any other interested party based on the terms established in the regulations governing the provision of services for the issuance, revocation and distribution of digital certificates, as well as this CPS and the associated PCs.

9.9.2. INDEMNITIES FOR DAMAGES CAUSED BY APPLICANTS, SUBSCRIBERS AND RELYING THIRD PARTIES

Both Subscribers, Applicants, and relying Third Parties are liable for seizing, destroying, modifying, improperly altering the data of a digital signature or certificate during or after the date of creation of the certificate and shall be subject to the payment of compensation for the corresponding damages caused as established in the regulations governing the provision of services for the issuance, revocation and distribution of digital certificates.

9.10 PERIOD OF VALIDITY

9.10.1. PLAZO

This DCP and the associated PCs shall enter into force from the moment of their publication on the PKI SERVICES S.A.S. website and shall remain in force as long as they are not expressly repealed by the publication of a new version.

9.10.2. REPLACEMENT AND REPEAL OF THE CPD AND THE PC'S

This CPS and the associated PCs shall be replaced by new versions regardless of the significance of the changes made to it, so that it shall always apply in its entirety. When the CPS is repealed, it will be removed from the PKI SERVICES S.A.S. website, although it will be kept for at least three (03) years from its termination or the period established by the legislation in force.

9.10.3. EFFECTS OF TERMINATION

The obligations and restrictions established in this CPS and the associated PC, in reference to audits, confidential information, obligations and responsibilities of PKI SERVICES S.A.S. born under its validity, will survive after its replacement or repeal by a new version in everything that does not oppose it.

9.11. PQRS

Requests, complaints, claims, suggestions and appeals (PQRS) about the services provided by PKI SERVICES S.A.S., are received directly by the PKI SERVICES S.A.S. PQRS Manager.

The Applicants, Subscribers, Third Parties who trust or the general public will indicate their PQRS regarding the digital certification services offered by PKI SERVICES S.A.S. by sending an email to the address https://pkiservices.co/ section CUSTOMER SERVICE, option PQRS SUPPORT, detailing the situation for which it is presented.

The PQRS will be managed by the PQRS Manager of PKI SERVICES S.A.S., who will be responsible for referring the incident to the respective Department or role. Such management will be carried out, resulting in a solution in a period not exceeding fifteen (15) days. The user will receive an e-mail message confirming receipt of the PQRS and when it is resolved. PKI SERVICES S.A.S. has the PQRS procedure for the treatment of PQRS that details each of the processes and is published on the PKI SERVICES S.A.S. website.

9.12. CHANGES TO CPS AND PC

All changes to this CPS and associated PCs will require new versions of the documents.

The changes in each new version will be indicated in the initial version history table.

The new approved versions of this CPS and associated CPs are sent to ONAC and published on the PKI SERVICES S.A.S. website.

9.13. CLAIMS AND DISPUTE RESOLUTIONS

For the resolution of any dispute that may arise in relation to this CPS or the associated PCs, the parties, waiving any other jurisdiction that may correspond to them, submit to the Colombian Courts, regardless of the place where the issued certificates have been used.

9.14. APPLICABLE LAW

The legislation applicable to this document, as well as to the associated PCs and the operations deriving from them is recorded in the internal document, including the following, as well as the regulations that modify or complement them:

a) Law 527 of 1999
b) Statutory law1581 of 2012
c) Decree Law 0019 of 2012
d) Decree 1074 of 2015

e) Decree 333 of 2014

f) Decree 1471 of 2014

9.15. COMPLIANCE WITH APPLICABLE LAW

It is the responsibility of PKI SERVICES S.A.S. to ensure compliance with the applicable law listed in the previous section.

9.16. MISCELLANEOUS STIPULATIONS

9.16.1. SUBSCRIPTION CONTRACT

The Subscription Contract (GC-CN-001 Subscription Contract) for the current certificate issuance service is published in the following web page: https://pkiservices.co/ section INF. AVAILABLE

The same contract model is used for all types of certificates. In the contract the type of contracted certificate and its validity must be filled in.

9.16.2. FULL ACCEPTANCE CLAUSE

All Applicants, Subscribers, Relying Third Parties and any other interested parties fully accept the contents of the latest version of this CPS and the associated PCs.

9.16.3. INDEPENDENCE

In the event that any of the sections contained in this CPS or in the associated CPs is declared, partially or totally, null and void or illegal, this shall not affect the rest of the document.

9.17. OTHER STIPULATIONS

Not comtemplated

10. POLICIES OF DIGITAL CERTIFICATES ISSUED BY PKI SERVICES

The procedure for the issuance of certificates is detailed in Section 4 Life Cycle of the certificates of this document.

The available means to generate digital certificates and digital certification services, is in our web page PKI SERVICES https://pkiservices.co/ section SERVICES.

It is a requirement to have validated the identity of the applicant in accordance with the provisions of numeral 3.2 - Validation of identity.

The Certificate Policy can be found in GE-PO-018 CERTIFICATE POLICY V2, document that is an integral part of this CPD, published in our web page PKI SERVICES https://pkiservices.co/ section AVAILABLE INFORMATION.

10.6. RATES

The value set by PKI SERVICES for the provision of digital signature Certificate Services is established in accordance with the contractual conditions agreed with the service applicants and will be properly calculated and settled by PKI SERVICES.

The rate for the provision of the digital signature certificate service will be established based on the client's needs and in accordance with the volume of digital signature certificates that the client requires. Rates can be found in GE-PO-018 CERTIFICATES POLICY V2