Code:	DYD-L-003
Date:	09/09/2024
Version:	019
Label:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

Certification Practices Statement

Code: DYD-L-003

Date: September 2024

Version: 019

certicámara.

Code:	DYD-L-003
Date:	09/09/2024
Version:	019
Label:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

Content

Code:	DYD-L-003
Date:	09/09/2024
Version:	019
Label:	PUBLIC

CERTIFICATION PRACTICE STATEMENT

1. INTRODUCTION

This document presents the Certification Practices Statement (DPC), which consists of a public manifestation of the Open Digital Certification Entity where standards and practices of the Certification Authority are established for the provision of digital certification services in accordance with Law 527 of 1999, Decree 1074 of 2015 that compiles Decree 333 of 2014, Decree 620 of 2020, Law 2106 of 2019, Law 1581 of 2012, Law 1898 of 2018 Article 10 and Decree Law 019 of 2012, especially the activities of Article 161, for the accredited services of: Digital Signature Certificate, Chronological Stamping, Certified Biometric Fingerprint, Certified Electronic Mail, Generation Of Digital Signatures, Generation Of Certified Electronic Signatures provided by the Digital Certification Chamber Society Certicámara S.A.

This document is addressed to all those natural or legal persons, applicants, subscribers, and in general to users of digital certification services and third parties who rely on them as legal and evidentiary evidence, in the field in which they are implemented.
This document is written according to the RFC 3647 standard.

1.1 Identification of the digital certification entity

The Digital Certification Chamber Society Certicámara S.A., hereinafter Certicámara, is a corporation established by the Chambers of Commerce of Bogotá, Medellín, Cali, Bucaramanga, Cúcuta, Aburrá Sur and Confecámaras, with the purpose of providing digital certification services, being a subsidiary of the Chamber of Commerce of Bogotá.

Certicámara is an Open Digital Certification Entity, whose main purpose is to be the trusted third party for security products and services in electronic media, providing the necessary tools for entrepreneurs and other Internet users in the country to conduct electronic business with legal certainty.

Name	Digital Certification Chamber Society Certicámara S.A.
NIT	830.084.433-7
Commercial registration	1079279
Certificate of existence	https://web.certicamara.com/nosotros

and legal representation	
Main domicile	Bogotá
Address	Carrera 7 Nº 26-20 Pisos 18, 19 y 31
Telephone (administrative matters)	(601) 9157808
Email	info@certicamara.com
Telephone (sales, customer service and technical support)	(601) 7442727 o (601) 7442725
National free hotline	018000181531 – Not valid for cell phones
Responsible for receiving requests, queries and complaints from subscribers and users	Relationship Manager
Responsible for the review and approval of responses to requests, inquiries and complaints from subscribers and users	Relationship Manager
PQRS Email	certicamararesponde@certicamara.com
WEB Address	www.certicamara.com
Accreditation Certificate No.	16-ECD-002
Certificate of Accreditation	https://onac.org.co/certificados/16-ECD-002.pdf

1.2 Name and identification of the document

Certicámara, in order to provide its different services, establishes the following information for the present document.

Name	Certification Practices Statement - DPC
Date of publication	09/09/2024
Version	019
Code	DYD-L-003
Location	https://web.certicamara.com/marco-normativo

Note: If you need to consult a previous version of this document, please contact info@certicamara.com so that your request can be attended to.

1.3 PKI Participants

1.3.1. Certification Authorities

A trusted entity that provides certification services. It is empowered to issue, manage, and revoke digital certificates acting as a trusted third party between the subscriber and the certificate holder user, or trusted third parties.

Certicámara has the following CAs:

Certification Authority Root CA: The Root CA, is the Certification Authority origin of the digital certification hierarchy. This component of Certicámara is responsible for the issuance of digital certificates that accredit its issuing platform.

Its data structure is:

- Root Certificate field
- Root Certificate Value
- Root CA Key 4096 bits
- Valid until May 24, 2031, 01:39:46 pm
- Version V3
- Certificate Serial Number
- Unique certificate identifier. Less than 32 hexadecimal characters.

- Certificate signing algorithm: SHA256withRSAEncryption
- SHA1: 54 63 28 3b 67 93 ff 55 27 7c ed e3 90 98 e8 04 22 f9 12 f7
- Serial Number: 43 1c 28 c6 74 0f ed 25 57 44 9f f2 fd 0e 5e 14

Subordinate certifiers

In the Colombian regulatory framework, these are derived from the hierarchy of the Root CA, where they require the Root CA to sign their certificate so that they in turn issue certificates to end subscribers following the chain of trust from the root point of Certicámara, as an Open Digital Certification Entity accredited by ONAC under the Certificate of Accreditation number 16-ECD-002.

For all CA's belonging to the public key infrastructure of Certicámara, what is expressed in the CPD applies, consistent with the general requirements established by the legal framework described in the section on normative references.

The structure of the certificate data for subordinate authorities is:

- Root CA Certificate field.
- Public key of the SUBORDINATE ENTITY 4096 bits
- Version V3
- Certificate serial number
- Unique identifier of the certificate. Less than 32 hexadecimal characters.
- Certificate signing algorithm SHA256withRSAEncryption
- Issuer data
- CN
- Root Certification Authority of the certification chain.
- SHA1: 26 c5 8f b4 36 4f f6 21 ce 2a 04 c7 3e bf b2 ac 09 c3 5f 56
- Serial Number: 58 1f 6a de 78 78 fe 8c 56 ac db d7 a6 77 58 10

Time Stamping Authority

The "**Time Stamp**" is provided by **Certicámara** in a secure and suitable electronic format defined in such a way that it is incorporated into the data message generated, transmitted or received by the subscriber preventing its subsequent alteration. The "**Time Stamp**" of a data message is unique to that data message and cannot be incorporated into one or more other data messages.

The timestamping service can be found at the following URL http://tsa.certicamara.com:9233/ where the subscriber must have a username and password to use the respective service.

This is explained as follows: (i) A user wants to obtain a time stamp for an electronic document that he possesses; (ii) A digital summary (technically a hash) is generated for the

document on the device requesting the stamping; (iii) This summary forms the request that is sent to the certification authority providing the **time stamping service**; (iv) The certification authority providing the **time stamping service** generates a time stamp (or chronological stamp) with this digital summary, the date and time obtained from a trusted source, and the digital signature. Thus, by time stamping this summary representation of the document, what is actually being done is to stamp the original document; (v) The time stamp is sent back to the user; and (vi) The certification authority providing the **time stamping services** keeps a record of the stamps issued for future verification. The structure of the Time Stamp Authority (TSA) service is described in RFC 3628 and the Time-Stamp Protocol (TSP) is described in RFC 3161.

1.3.2. Registration Authorities

Registration Authority (RA): It is in charge of receiving the requests related to digital certification, registering the requests made by the applicants to obtain a certificate, checking the veracity and correctness of the data provided by the users in the requests, sending the requests that meet the requirements to a CA to be processed.

The Certicámara registration authority is composed of:

- **RA software:** Facilitates the registration of requests and enables the management of the certification request lifecycle.
- **RA Agents:** RA users with privileges. They are responsible for the review and validation of the information contained in the documents submitted by the applicant for the issuance of an DCA service.
- **RA Administrator:** The person responsible for administering and configuring the RA.
- **System Auditor:** The person responsible for auditing compliance with the RA procedures and systems, validating compliance with the Certification Practices Statement (DPC) and Certification Policies (PC).

1.3.3. Subscribers

Subscriber is the natural person to whom the digital certification services are issued or activated and therefore acts as subscriber and/or responsible for the same, with knowledge and full acceptance of the rights and duties established and published in this CPS and the certification policy of the service purchased.

1.3.4. Relying Parties

Natural or legal person other than the subscriber and/or responsible party who decides to accept and trust the certification services provided by Certicámara.

1.3.5. Other participants

- Service Providers

Critical providers contracted to provide Datacenter services comply with the minimum requirements established in the CEA 3.0-7 Specific Accreditation Criteria document published on ONAC's website. To this effect, they shall be required to comply with the requirements described in the CEA 3.0-7 Specific Accreditation Criteria published by ONAC when applicable.

Name:	Comunicación Celular S.A. Comcel S.A.
NIT	800.153.993-7
Commercial Registration	487585
Certificate of Existence and Legal Representation	https://web.certicamara.com/nosotros
Main Location	Bogotá
Address	Carrera 68 A N° 24 B 10
Telephone	(601) 7480000 - 7500300
Email	notificaciones@claro.com.co
Web Site	www.claro.com.co

Name	SENCINET LATAM COLOMBIA S.A.
NIT	800.255.754 - 1
Commercial Registration	637298
Certificate of Existence and Legal Representation	https://web.certicamara.com/nosotros

Main Location	Bogotá
Address	Calle 113 N 7-21 Torre A Of 1112
Telephone	(601) 6292262
Email	maria.diaz@sencinet.com
Web Site	https://sencinet.com/

1.4 Use of certificates

1.4.1. Appropriate certificate uses

The root digital certificate may only be used for the root certification authority itself and for the distribution of its public key in a secure manner. The use of certificates issued by the root CA shall be limited to the signing of digital certificates and the signing of the corresponding revoked certificate lists.

General uses applicable to the digital certificates issued by Certicámara

a) The **subscriber** can only use the digital certificates for the uses specified in the contract signed with Certicámara individually, those permitted in this **Certification Practices Statement, in the Certification Policies** and those permitted under Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014). The contract entered into with the subscriber may limit the scope of uses, depending on the environment within which the digital certificate is being used, or the special characteristics of the project being developed. Any other use will be considered a violation of this **Declaration of Certification Practices and Certification Policies** and will constitute grounds for revocation of the digital certificate and termination of the contract with the **subscriber**, without prejudice to any criminal or civil actions that may be applicable.

b) The **subscriber** considers and accepts that the products and services advertised are as they are individually offered, that the digital certificates mainly certify the identity of the natural person appearing as the subscriber of the service, that there is no implicit information implying services or benefits additional to those expressly mentioned and that the use thereof is the sole responsibility of the subscriber, taking into account the

provisions of Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014).

c) The use of the digital certificate and the data messages that are digitally signed with it, including electronic monetary transactions, regardless of their amount, are the TOTAL responsibility of the corresponding subscriber and, therefore, Certicámara has no responsibility whatsoever regarding the verification or public faith of the signed data messages, since it does not know and has no legal obligation to know the digitally signed messages or the amount of the transactions that are made with the digital certificate in electronic transaction systems of third parties. In general, Certicámara as an Open Digital Certification Entity and Trusted Third Party does not commit its responsibility in the use made by the subscriber of the digital signature certificates, therefore, there are no financial limits applicable in this regard. For this purpose, the subscriber must comply with its duties under Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014), as well as must meet the burden of responsibility imposed by such rules.

1.4.2. Prohibited uses of the certificate

a) The digital certificates may not be used under any circumstances for illicit purposes or operations under any legal regime in the world.

b) Any use of the digital certificates that is contrary to Colombian legislation, international agreements signed by the Colombian State, supranational norms, good customs, sound commercial practices, and everything contained in this Declaration of Certification Practices and in the contracts signed between Certicámara and the Subscriber is strictly prohibited.

c) Any use of the digital certificates with the purpose of violating any intellectual property rights of Certicámara or third parties is prohibited.

d) The physical support of the digital certificate provided by Certicámara (if applicable) can only be used within the context of the Digital Certification System. No information other than that expressly authorized by Certicámara may be incorporated in the physical support provided, nor may it be used outside the Digital Certification System.

1.5 Policy Administration

1.5.1. Organization that manages the document

All information contained in this **Certification Practice Statement (DPC) and Certification Policies (CP)** is the intellectual property of Certicámara, therefore, its administration is carried out according to the guidelines defined within.

1.5.2. Contact Person

Certicámara has established that the contact person for issues related to this **Declaration of Certification Practices (DPC) and Certification Policies (CP)** is the Deputy Manager of Product and Innovation.

Name	Anthony Molina Gamboa
Position	Assistant product and innovation manager
Email	info@certicamara.com
Telephone	(601) 9157808
Address	Carrera 7 Nº 26-20 Piso 18, 19 y 31

1.5.3. Procedures for approval of the DPC

The Certification Practice Statement shall be updated whenever required by legal, regulatory and/or applicable issues to the accredited services.

For the above, the DPC and CP change committee will meet to evaluate the changes and/or modifications to be made, which will be approved by the Executive President.

The Director of Planning and Management is responsible for managing the update on the Certicámara website, at the following link https://web.certicamara.com/marco_legal.

1.6 Definitions and acronyms

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

CERTIFICATION PRACTICE STATEMENT

- **Certification Authority (CA):** Trusted entity, responsible for issuing and revoking certificates.
- **Time Stamp Authority (TSA):** Time Stamp Authority.
- **Validation Authority (VA):** Trusted entity that provides information about the validity of digital certificates.
- **Root CA:** First level certification authority, trust base.
- **Subordinate CA:** Certification Authority of second level or more levels.
- **Digital Certificate:** Electronic data message signed by the digital certification authority, which identifies both the issuing certification authority 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 DCA establishes a business relationship.
- **Signature Creation Data (Private Key):** These are unique numeric values that, used in conjunction with a known mathematical procedure, serve to generate the digital signature of a data message.
- **Signature Verification Data (Public Key):** Data, such as codes or public cryptographic keys, that are used to verify that a digital signature was generated with the subscriber's private key.
- **Certification Practice Statement (DPC):** Declaration of certification practices. Official document presented by the Digital Certification Entity, which defines standards and practices of the Certification Authority for the provision of digital certification services.
- **Declination of the service request:** It is the rejection of a digital certification service, which is not within the scope of the accreditation granted by ONAC or due to non-compliance with the law. In this case, there will be no room for correction by the user.
- **Open Certification Entity:** The one that offers to the general public, services of the DCEs, such as: its use is not limited to the exchange of messages between the entity and the subscriber, and receives remuneration.
- **Digital Certification Authority (DCA):** A person who, authorized under this law, is empowered to issue certificates in relation to digital signatures of persons, offer or facilitate the services of recording and time stamping the transmission and receipt of data messages, as well as perform other functions related to communications based on digital signatures.
- **Time Stamping:** A data message digitally signed and time-stamped by a TSA that links another data message to a specific point in time, which makes it possible to establish with proof that this data existed at that time and did not undergo any modification from the time the stamping was performed.
- **ETSI:** European Telecommunications Standards Institute
- **FIPS:** Federal Information Processing Standards are publicly announced standards developed by the U.S. 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 (ANSI, IEEE, ISO, etc.)

- **Digital Signature:** Shall be understood as a numerical value that is attached to a data message and that, using a known mathematical procedure, linked to the originator's key and the text of the message makes it possible to determine that this value has been obtained exclusively with the originator's key and that the initial message has not been modified after the transformation has been carried out.
- **Electronic Signature:** When any standard requires the presence of a signature or establishes certain consequences in the absence thereof, in relation to a data message, such requirement shall be deemed to be satisfied if:
  a. A method has been used to identify the originator of a data message and to indicate that the content has his approval.
  b. The method is both reliable and appropriate for the purpose for which the message was generated or communicated.
- **HASH function:** An operation performed on a data set of any size, such that the result obtained is another data set of fixed size, regardless of the original size, and which has the property of being uniquely associated with the initial data.
- **HSM:** Hardware Security Module
- **LDAP:** Lightweight Directory Access Protocol
- **List of Revoked Digital Certificates (CRL):** It is the list of digital certificates that have been revoked by the Certification Authority (CA), that have not met their scheduled expiration date and that should no longer be trusted.
- **Log:** Event log service of the information system, leaving the previous and current information, identifies who and when the event took place.
- **Denial of the service request:** A digital certification service will be denied for reasons beyond the control of Certicámara S.A., and which are the responsibility of the user, as long as they can be corrected by the latter.
- **Technological Neutrality:** Principle of non-discrimination between information recorded on paper and information communicated or filed electronically, as well as non-discrimination, preference or restriction of any of the various techniques or technologies that can be used to sign, generate, communicate, store or file information electronically.
- **OID:** Unique Object Identifier. OID. "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., with the purpose, among other things, of knowing the origin, ownership and age of the identified object.
- **PKI (Public Key Infraestructure):** 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.
- **Certificate Policies (PC):** It is the set of rules that indicates the requirements of a certificate in a particular community and/or class, within the framework of legal and regulatory requirements, and with common security requirements.

- **Recommendation for decision:** Communication issued by the Registration Authority (RA) to the Certification Authority (CA), to approve the request of Certicámara S.A. to provide services to the applicant.
- **Revocation:** For this document, it is the process by which the digital certificate issued is disabled and its validity period of use is terminated from the date of revocation; upon the occurrence of any of the causes established in the certification practices statement.
- **Digital Certification Service:** Set of certification activities offered by the DCA to certify the origin and integrity of data messages, based on digital or electronic signatures, time stamping, as well as the applicability of technical standards supported and in force in public key infrastructure – PKI.
- **Online Certificate Status Service OCSP:** Real-time query activity to the DCA 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 DCA, demonstrates compliance with the requirements established in the DPC and CP of these, to access the digital certification service.
- **Subscriber:** Natural or legal person in whose name a digital certificate is issued.
- **Token:** Cryptographic hardware device provided by a DCA, which contains the digital certificate and the subscriber's private key.
- **UpTime:** Commitment in terms of percentage of available time of an information system, which the company providing it commits to offer to its customer per year.
- **Usability:** A term used to denote the way in which a person can use a particular tool effectively, efficiently and satisfactorily, in order to achieve a specific goal.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Certificates of the Root CA, Subordinate CA and list of revoked CRL certificates shall be available for consultation 365 days a year, 24 hours a day, 7 days a week. This service will be provided with an availability agreement of 99.8% and in case of interruption due to force majeure, the service will be restored in the time established according to the availability percentage. In the case of the PKI, an availability of 99.8% is established.

2.2 Publication of certification information

a) For certificates of the Root CAs and the Accredited Subordinate Entity:

- WEB:

Root CA Certicámara S.A

http://www.certicamara.com/repositoriorevocaciones/ac_offline_raiz_certicamara_.cer

- Subordinate CA Certicámara S.A.

  http://www.certicamara.com/repositoriorevocaciones/ac_online_subordinada_certicamara_.crt
  http://www.certicamara.com/repositoriorevocaciones/ac_online_subordinada4096_certicamara_.crt

b) For the list of revoked certificates (CRL):

- WEB:
  - Root CA Certicámara S.A.
    http://www.certicamara.com/repositoriorevocaciones/ac_raiz_certicamara.crl
  - Subordinate CA Certicámara S.A.
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara.crl
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.crl
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_4096.crl?crl=crl
    http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_4096.crl?crl=crl

c) For the DPC:

- WEB:

  https://web.certicamara.com/marco-normativo

d) For OCSP certificate revocation status verification

- WEB:

  http://ocsp.Certicamara.com
  http://ocsp.Certicamara.co
  http://ocsp4096.certicamara.co

Through this URL the user can directly consult the revocation of a certificate, for this it is necessary to have an OCSP Client that complies with RFC 6960. If the user does not have this OCSP Client, he/she must download the complete list of revoked certificates (CRL).

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

2.3 Time or frequency of publication

2.3.1. Root CA Certificates

The publication of the certificate shall be made prior to the certificate becoming effective through the Certicámara website. The validity period is until Saturday, 24 May 2031 13:39:46.

2.3.2. List of Revoked Certificates (CRL)

The publication of the list of Revoked Certificates of the Subordinate CA Certicámara S.A. (CRL) is made with validity of three (3) days:

- The publication may be made no more than eight (8) hours after the last revocation, at any time of the day.

2.3.3. OCSP certificate revocation status

The service is continuously available 24 hours a day, 365 days a year for consultation via the web and is automatically updated in the following cases:

- Each time a digital certificate is revoked.

2.4 Repository access controls

Access to the information published by the Root CA shall only be for consultation and may not be modified by unauthorized persons. Public information shall only be updated by the personnel in charge of this function working in Certicámara.

In addition, consultation of the CRL, issued certificates, OCSP and DPC server in their previous and updated versions is guaranteed.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Denomination

All certificates have a section called Subject whose purpose is to identify the subscriber of the certificate, this section contains a DN or Distinguished Name characterized by a set of attributes that make up an unequivocal and unique name for each subscriber of the certificates issued by Certicámara.

3.1.1. Types of names

The attributes of each certificate type are established in the certificate issuance policy. Each certificate type will be identified by a unique OID (Object Identifier), included in the certificate as a policy identifier, within the certificate properties.

OID	Type of Policy
1.3.6.1.4.1.23267.50.1.1	Company / Entity Membership Certificate in local and/or centralized devices
1.3.6.1.4.1.23267.50.1.2	Company / Entity Representation Certificate in local and/or centralized devices.
1.3.6.1.4.1.23267.50.1.3	Certificate of Public Function Holder in local and/or centralized devices
1.3.6.1.4.1.23267.50.1.4	Certificate of Qualified Professional in local and/or centralized devices
1.3.6.1.4.1.23267.50.1.5	Digital certificate natural person / legal entity in local and/or centralized devices
1.3.6.1.4.1.23267.50.1.8.5	Digital certificate natural person PKCS#10
1.3.6.1.4.1.23267.50.1.8.4	Digital certificate legal entity PKCS#10

3.1.2. Need for meaningful names

The policies defined ensure that the distinguished names (DN) of certificates are sufficiently meaningful to link the public key to an identity.

3.1.3. Anonymity or pseudonymity of subscribers

Certicámara does not allow anonymity or pseudonymity to identify the name of a natural or legal person. In the case of an entity or legal person the name must be exactly the same as the corporate name, abbreviated names are not allowed. In the case of a natural person, the

name must consist of the first and last names as they appear in the recognized identification document.

3.1.4. Rules for interpreting various forms of names

The rules used for the interpretation of distinguished names in issued certificates are described in ISO/IEC 9595 (X.500) Distinguished Name (DN). Additionally, all issued certificates use UTF8 encoding for all attributes, according to RFC 5280 ("Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile").

3.1.5. Name uniqueness

The Root CA defines the DN (Distinguished Name) field of the Certificate Authority as unique and unambiguous. For this purpose, the name or company name of the certificate holder shall be included as part of the DN, specifically in the CN field.

3.1.6. Recognition, Authentication and Function of Marks

The DCA makes no commitments in the issuance of certificates regarding the use by Subscribers of a trademark, therefore, the DCA is not required to seek evidence of trademark ownership prior to the issuance of certificates.

A certificate applicant retains all rights it owns (if any) in any trademark, service mark or trade name contained in any certificate application and distinguished name within any certificate issued to such certificate applicant.

3.2 Initial identity validation

3.2.1. Method for proving possession of the private key

The certification system implemented and used by Certicámara for the administration of the life cycle of its certificates automatically controls and guarantees the issuance of the signed certificate to the holder of the private key corresponding to the public key included in the request. This guarantee is achieved through the PKCS#10 format that includes in the request itself a digital signature of the request, made with the private key corresponding to the public key of the certificate.

3.2.2. Authentication of the identity of the organization or person

For the authentication of the identity of the organization or person, the applicant must provide the supports required for each accredited service. The applicant must provide Certicámara with truthful, sufficient and adequate information regarding the requirements.

3.2.3. Verification of powers of representation

The verification of the applicant's powers of representation before Certicámara will be carried out by cross-checking with the Single Business and Social Registry (RUES) or by verifying the legal documents established in the Colombian regulations that qualify and empower the applicant as a legal representative.

3.2.4. Identity validation mechanisms

3.2.4.1 Identity verification

Certicámara, as an Open Digital Certification Entity, shall perform the identity verification through the defined mechanisms, using reliable data sources provided by third parties with whom Certicámara has a valid contract for this purpose.

3.2.4.2 Identity Verification by Biometrics

If required, Certicámara may perform the validation of the applicant from the biometric identification provided to ensure that the applicant is who he/she claims to be.

3.2.5. Unverified Subscriber Information

Certicámara, as an Open Digital Certification Entity, validates the applicant's information that can be backed up with supporting evidence. For information that cannot be supported with evidence such as physical address, email and others, the principle of good faith of the applicant at the time of providing the information is taken as a starting point.

3.2.6. Interoperability Criteria

Certicámara as an Open Digital Certification Entity does not contemplate interoperability with other external DCAs. It only contemplates the issuance of digital certificates with its Subordinate.

Notwithstanding the above, if the need arises, for commercial and/or regulatory reasons, to perform interoperability with another DCA, the different scenarios for its execution must be evaluated to ensure the proper provision of the service.

3.3 Identification and Authentication for Key Renewal Requests

Certicámara does not contemplate the renewal process of digital certificates under the same key pair of the subscriber.

If the renewal of a previously issued certificate is required, the process of requesting the issuance of a new certificate containing a new key pair must be carried out.

4. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFE CYCLE

4.1 Certificate application

The application process may be carried out in any of the following ways:

- In person at Certicámara's facilities.
- Through the Contact Center.
- Or by any other electronic means available to Certicámara.

The applications made will be reviewed by the RA (registration authority) according to the specific accreditation criteria of ONAC and those defined by Certicámara. This review will be executed in a maximum of two (02) working days from the completion of the documents, payment support and validation of successful identity of the owner of the signature attached. Subsequently, the applications will be escalated to the CA (certification authority) for issuance, which has a maximum time of one (01) business day.

The documentation submitted by the applicant must be in Spanish only, in accordance with the internal policies of Certicámara S.A. Those documents that are in a different language must be translated into any of these languages by an official translator endorsed by the Ministry of Foreign Affairs and will be stored in accordance with the document retention tables generated by Certicámara. The applicant's information will not be published by Certicámara unless with his/her explicit consent.

The applicants who make use and subscribe electronically the digital signature certificate of CERTICÁMARA S.A. imply the full acceptance, without reservations and in its entirety, of the Terms and Conditions of the digital signature certification service of Certicámara S.A., the Declarations and Commitments regarding the prevention of ML/FT/FPDAM and C/ST, the Declaration of Certification Practices, the Certification Policy, the privacy notice - digital signature certificate and the organizational policies of CERTICÁMARA S.A., published through the website of Certicámara S.A. and that are an integral part of this document and in the contract for the provision of digital certification services.

The terms and conditions apply from the moment you express to CERTICÁMARA S.A. your interest in acquiring the digital signature certificate and will be maintained until the validity of the digital signature certificate along with the general conditions of service contracting.

Therefore, applicants must take into account the following points before requesting the service(s) to Certicámara:

CERTIFICATION PRACTICE STATEMENT

a. To have read in its entirety the Terms and Conditions of the digital signature certification service of Certicámara S.A., the Declarations and Commitments regarding the prevention of ML/FT/FPDAM AND C/ST, the present Declaration of Certification Practices and the Certification Policy - digital signature certificate, the privacy notice.

b. Verify the information mentioned by CERTICÁMARA S.A., which must be known to make an informed decision on the provision of the digital signature certificate, in accordance with the provisions of Ley 527 of 1999, Decreto 019 of 2012, Ley 1341 of 2009, Ley 1978 of 2019, Decreto 1074 of 2015, Decreto 358 of 2020, Decreto 1538 of 2020 and Decreto 620 of 2020.

c. To know all the technological and security requirements for the use of the digital signature certificate. Be aware of the characteristics of the digital signature certificate of CERTICÁMARA S.A., its level of reliability, the limits of responsibility of the same, the obligations assumed as a client and the security measures that must be met for its use.

d. Know that CERTICÁMARA S.A. may reserve the right not to provide a digital signature certificate due to technical conditions, without this decision generating any type of responsibility.

e. CERTICÁMARA S.A., as an Open Digital Certification Entity, will previously perform the identity verification, using reliable sources and data provided by third parties with whom CERTICÁMARA S.A. has a valid contract for this purpose.

f. Certicámara reserves the right to request additional documents to those required in the application form or photocopies of these when it deems necessary to verify the identity or any quality of the applicant, as well as to exonerate the presentation of any of them when the identity of the applicant has been sufficiently verified by Certicámara through other means. Without limiting itself to them, Certicámara may additionally require any of the following documents:

- Commercial references of the company.
- Applicant's personal references.
- Bank certifications.
- Valid driver's license.
- Military passbook.
- Document of affiliation to the social security health system.
- Affiliation document to the professional risk management company.

- Other documents that allow verifying the identity or powers of the subscriber or the entity, for the issuance of any of the types of certificates issued by Certicámara.

g. It may consult identity information databases provided for such purpose by private or public sector entities in order to perform the identity validations necessary to issue the digital certificate to the subscriber.

h. Consult the databases necessary to comply with the SAGRILAFT, prior acceptance by the applicant of the Declarations and Commitments regarding the prevention of money laundering, financing of terrorism, financing of the proliferation of weapons of mass destruction, corruption and transnational bribery published on the website of Certicámara S.A. and which are an integral part of this document.

i. It will issue digital signature certificates with a maximum validity of two (2) years.

j. Certicámara S.A. will decline the issuance of a digital certificate to an applicant, when it is not within the scope of the accreditation granted by ONAC, for non-compliance with the law and/or when, in its opinion, it is detrimental to the good name of the ECD. In this case, there will be no room for correction by the user.

k. If Certicámara decides to deny or decline the request for the issuance of the digital signature certificate, it will notify the applicant by e-mail, indicating the reasons that justify it.

l. We are currently developing the infrastructure that will allow compatibility for the issuance of digital signature certificates for the Mac OS operating system.

4.1.1. Who can submit a certificate request

The certificate request can be made by any person, of legal age and capable of assuming the obligations and responsibilities inherent to the type of certificate requested.

The certificate linked to the identity of a legal entity may be requested by a legal representative, attorney-in-fact, employee or person authorized by a legal representative of the legal entity who can correctly support the information required by the RA.

4.2 Issuance of certificates

4.2.1. Actions of the CA during certificate issuance

Once the certificate issuance request is approved, the CA generates the corresponding certificate linked to a key pair, which will be signed by the CA certificate that is part of the **Certicámara** chain of trust.

The issuance of the certificates implies the authorization of the request by the Subordinate CA's system. After approval of the request, the certificates will be securely issued and made available to the subscriber.

In issuing certificates, the Subordinate CA:

- Uses a certificate generation procedure that securely binds the certificate to the registration information, including the certified public key.
- Protects the confidentiality and integrity of the registration data.
- All certificates will start their validity at the time of issuance by the CA, such validity is recorded in the certificate properties.
- No certificate shall be issued with a validity period that begins earlier than the current date.

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

The subscriber shall know about the effective issuance of the certificate by a notification sent to his/her registered email.

4.3 Delivery of the digital certificate to subscribers by physical means

4.3.1. Coverage

The delivery of the digital certificates will be made in accordance with the delivery service coverage matrix of the logistics operator that has a valid contract with Certicámara to perform this task or by direct delivery by the Certicámara's logistics area collaborator, complying with the necessary security requirements to ensure that the delivery is personal and that the confidentiality of the subscriber's private key of the certificate is maintained at all times.

The digital certificates will be sent through the logistics operator to the destination filled out in the application form or may be claimed at the facilities of Certicámara, prior information of the subscriber.

4.3.2. Delivery requirements

The logistic operator's guide will serve as evidence of the acknowledgement of receipt of the digital signature certificate.

4.3.3. Delivery management time - Physical Certificates

At Bogota and municipalities close to the urban perimeter, the delivery time from the issuance of the certificate to the delivery to the applicant will be approximately two (2) working days.

At departmental capitals, the delivery time from the issuance of the certificate to the delivery to the applicant will be between two (2) to four (4) working days approximately.

In other municipalities, the delivery time from the issuance of the certificate to the delivery to the applicant, will be between four (4) to five (5) working days approximately.

For municipalities or special destinations, the delivery time from the issuance of the certificate to the delivery to the applicant will be between six (6) to fifteen (15) working days approximately.

For all destinations, if delivery is impossible, a second attempt will be made, in case of failure, the logistics operator will return the digital certificate to Certicámara's facilities.

In the events in which the delivery of the certificate is not possible due to a cause associated to the subscriber, Certicámara and/or the logistic operator will contact the applicant to coordinate the delivery process. If there is no express response with the date of delivery or collection of the digital signature certificate, Certicámara will keep them in custody for a period of three (3) months from the date of issuance. Once this term has expired and the subscriber has not manifested, it will be understood that he/she abandons the property and Certicámara will proceed with the revocation. If the applicant requires the issuance of the digital signature certificate, he/she must initiate the application process as established by Certicámara.

4.3.4. Download Time - Virtual Certificate

In the case of virtual certificates, it is understood that, with the certificate download notification, the subscriber can make use of its digital certificate.

In the events in which the download of the certificate is not possible due to a cause associated to the subscriber, Certicámara will contact the applicant to coordinate the download process. If no response is received with the download date of the digital signature certificate, Certicámara will block the download link and will only be reactivated upon request of the client for a period of three (3) months from the date of issuance.

Once this term has expired and the subscriber has not manifested, it will be understood that he/she has abandoned the property and Certicámara will proceed with the revocation. If the applicant requires the issuance of the digital signature certificate, he/she must initiate the application process as established by Certicámara.

4.4 Acceptance of the certificate

No confirmation is required from the subscriber as acceptance of the service received. It is considered that the digital certificate service is accepted from the moment it requests its issuance, therefore, if the information contained in the service activation communication does not correspond to the current status of the same or was not provided correctly, the subscriber must notify Certicámara through any of our channels for the relevant correction procedures.

4.4.1. Publication of the certificate by the CA

The registration authority server will enter the public keys of the digital certificates issued by the subordinate certification authority in the LDAP (Lightweight Directory Access Protocol) directory structure of the PKI, at the time the certificate is issued.

In case of any technical inconvenience that prevents its publication, this will occur within the following month after the issuance of the certificate according to the result of the technical analysis that has prevented its immediate publication.

4.4.2. Notification of certificate issuance by the CA to other entities

Certicámara has a repository of LDAP digital certificates, in which entities, government agencies, private companies and other interested parties may consult the issuance of certificates. It is available at the following URL: https://ar.certicamara.com:8443/Search/. The publication in this repository is done once the certificate has been issued.

4.5 Withdrawal

In the case where the user has made the payment of any of the accredited services offered by Certicámara, and has not completed the necessary documentary requirements, the user will have a term to complete the information of ninety (90) days after the date of requesting the service.

In the event that the applicant does not fill out the required information, it will be understood as the withdrawal of the acquisition of the service, having as a consequence the non-refund of the money.

4.6 Non refundability

In no case shall Certicámara be obliged to return the money to the applicant, except in the exceptions foreseen by law.

4.7 Use of key pairs and certificates

4.7.1 Use of certificate and subscriber's private key

The **certification policy** details the uses and purposes for each of the types of certificates issued by Certicámara.

4.7.2 Use of the certificate and the trusted user's public key

Bona fide third parties may only place their trust in certificates for the purposes set forth in this DPC, CP and the regulations.

Bona fide third parties can successfully perform public key operations by relying on the certificate issued by the chain of trust. Likewise, they must take the precaution and assume the responsibility of verifying the status of the certificate using the means established in this DPC.

4.8. Renewal of the certificate

4.8.1. Timing of Renewal

Certicámara shall notify its subscribers at least thirty (30) calendar days in advance of the termination of the validity of their digital certificate. This notification may be made by e-mail to the address provided by the subscriber or by any other suitable means of communication when Certicámara deems it appropriate.

However, it is not Certicámara's obligation to guarantee the effectiveness of the notification on the termination of the validity of its certificate or to confirm the receipt of the same, since it is an obligation of the Subscriber to know the validity of its digital certificate and to advance the pertinent procedures before Certicámara for the issuance of its new signature.

Renewal shall be understood as the issuance of a new digital certificate, which implies the registration of a new application, which will be subject to the acceptance of the Terms and Conditions of the digital signature certification service of Certicámara S.A., the Declarations and Commitments regarding the prevention of ML/FT/FPDAM and C/ST, by the applicant, the previous validation of identity and the generation of a new pair of keys.

4.8.2. Who may apply for renewal

Subscribers are authorized to request the renewal of a certificate when the service is about to expire and the subscriber wishes to continue using a digital certificate that accredits the conditions that were approved in the digital certificate.

4.8.3. Processing of Certificate Renewal Requests

The subscriber must once again complete the identity validation process to request the renewal of a certificate. For this reason, the application procedure for certificate renewal is the same as for first-time issuance. Except that you will not have to attach documents to the application unless they are no longer valid, if applicable.

4.8.4. Notification of issuance of new certificate to the subscriber

Certicámara will notify the Subscriber of the effective issuance of a new certificate by means of an e-mail to the address provided.

4.9. Certificate key renewal

Certicámara does not consider within the life cycle of its certificates the renewal of the key pair, in all cases the issuance of a certificate entails the generation of a new key pair.

4.10 Modification of the certificate

During the life cycle of a certificate, it is not foreseen to modify/update the fields contained in the certificate. If a change in the issued certificate data is required, it will be necessary to revoke the certificate and issue a new one with the corresponding modifications.

4.11 Revocation and suspension of certificates

The revocation of a digital certificate is the mechanism by which the issued certificate is disabled and its validity period is terminated, either by the end of its validity or upon the occurrence of any of the revocation events established in this Certification Practices Statement, causing the loss of confidence in it.

Additionally, Certicámara does not allow the status of suspended digital certificates.

4.11.1 Grounds for Revocation

Certicámara shall revoke the digital certificate in accordance with article 37 of Law 527 of 1999, when it becomes aware that any of the following events have occurred:

a) By compromise of security in any reason, manner, situation or circumstance.

b) Compromise or loss of the subscriber's private key for any reason or circumstance.

c) The private key has been exposed or is in danger of being misused.

d) By death of the subscriber.

e) By supervening incapacity of the subscriber.

f) By liquidation of the represented legal entity that appears in the digital certificate.

g) By update of the information contained in the digital certificate.

h) By the confirmation that any information or fact contained in the digital certificate is false, as well as the occurrence of new facts that cause that the original data does not correspond to reality.

i) For the compromise of the private key of Certicámara or of its security system in such a way that affects the reliability of the digital certificate, for any circumstance, including fortuitous ones.

j) By the cessation of activities of Certicámara, unless the digital certificates issued are transferred to another Certification Entity.

k) By court order or competent administrative entity.

l) Loss, disablement or compromise of the security of the physical support of the digital certificate that has been duly notified to Certicámara.

m) By the termination of the subscription contract, in accordance with the grounds established in the contract and in this Certification Practice Statement.

n) For any cause that reasonably leads to believe that the certification service has been compromised to the point that the reliability of the digital certificate is in doubt.

o) Due to improper handling by the subscriber of the digital certificate.

p) For non-compliance of the subscriber or the legal entity he/she represents or to which he/she is linked through the Digital Certification Service Contract provided by Certicámara.

q) For overdue portfolio report caused by non-payment of the services being provided by Certicámara.

r) For events in which the delivery of the certificate is not possible due to a cause associated with the subscriber.

s) For causes associated with Certicámara and/or the logistic operator.

t) For the concurrence of any other cause specified in this Certification Practices Statement.

u) Termination of the labor contract or contractual relationship of the subscriber with the entity for which the digital signature certificate was issued.

4.11.2 Who can request revocation?

The Subscriber may voluntarily, at any time, directly or through a third party, request Certicámara to revoke the issued digital certificate, in which case the digital certificate revocation procedure will be initiated.

Certicámara may process the revocation of a certificate if it has knowledge or suspicion of the compromise of the Subscriber's private key or any other determining fact that requires proceeding to revoke the certificate.

4.11.3 Revocation Request Procedure

Certicámara has provided the following means for the receipt of revocation requests:

- Telephonically by calling the hotline (601) 7442727 Monday through Friday from 7:00 a.m. to 6:00 p.m. and Saturdays from 8:00 a.m. to 1:00 p.m.
- Online revocation through Certicámara's WEB page by registering the revocation request at the following URL: https://solicitudes.certicamara.com/SSPS/solicitudes/RevocarCertificadoClienteCF.aspx

If Certicámara deems it necessary, it will carry out, personally or through third parties, the pertinent inquiries, verifications and steps to verify the existence of the revocation cause invoked. Such steps may include direct communication with the subscriber and the physical presence of the third party invoking the cause for revocation.

Certicámara will validate the identity of the subscriber who invokes the cause for revocation. If the person invoking such cause is not the subscriber or in case of being the subscriber cannot be satisfactorily identified, he/she may personally go to the offices of Certicámara during office hours from 08:00 a.m. to 05:00 p.m. on the day of the revocation. - 05:00 p.m. Monday through Friday, with proof of the existence of the respective cause for revocation in applicable cases, notwithstanding that Certicámara has the measures established for the security of the Digital Certification System. It is clarified that once the revocation request is received and the veracity of the request is verified, the certificate will be revoked, without grace periods for such revocations.

In the cases in which the revocation is requested due to the termination of the labor contract or contractual relationship of the subscriber with the entity for which the digital signature certificate was issued, Certicámara will request from the person in charge or responsible for the entity a certification stating the termination of the labor relationship.

If the cause is verified, Certicámara will incorporate the digital signature certificate in the Database of revoked digital certificates as revoked digital certificate. Otherwise, it will terminate the digital certificate revocation process. It is clarified that Certicámara does not offer the service of certificate suspension to subscribers.

4.11.4 Grace period for revocation requests

Certicámara must inform the subscriber within 24 hours of the cancellation of the service or revocation of its certificate(s), in accordance with current regulations.

4.11.5 Frequency of CRL issuance

The publication of the list of Revoked Certificates of the Subordinate CA Certicámara (CRL) and CA SUB CERTICÁMARA (CRL) is carried out with validity of three (3) days:

- Periodically
- Publication may be made no more than eight (8) hours after the last revocation, at any time of the day.

4.11.6 Availability of online status/revocation verification

The revoked certificate lists (CRL) and the online certificate status validation service (OCSP) shall be available for consultation 365 days a year, 24 hours a day, 7 days a week. This service will be provided with an availability agreement of 99.8%.

Certicámara has a history of revoked certificates since the beginning of the service.

4.11.7 Online revocation verification requirements

Online certificate status verification must be performed using the OCSP service in accordance with RFC 6960. Using that protocol, the current status of an electronic certificate is determined without requiring CRLs.

An OCSP client sends a request about the certificate status to the VA, which, after querying its Database, provides a response about the certificate status via HTTP using the addresses http://ocsp.certicamara.com, http://ocsp.certicamara.co and http://ocsp4096.certicamara.co

4.11.8 Suspension Circumstances

Certicámara does not consider within the life cycle of the certificates the temporary suspension of the same, in all cases a revoked certificate cannot be reactivated again.

4.12 Digital Signature Certificates replacements

Certicámara establishes that the replacement of a digital certificate consists in generating a new certificate as defined in the life cycle of this Certification Practices Statement, the Certification Policy, and the values established in these documents.

However, to make the replacement effective, it must be taken into account that the initial certificate acquired meets the following criteria:

- The validity of the digital certificate must be equal to or greater than one (1) year.
- Digital certificates that are less than ninety (90) days from their expiration date shall not be replaced.
- The same certification policy with which it was initially issued must be maintained.
- The digital signature certificate will be replaced for the missing time.

This new generation of the digital signature certificate will have a cost associated with its commercial value at the time of issuance, according to the rates stipulated in the Certification Policy. In the event that commercial agreements have been agreed with the client, the rates to be applied will be those established in that document.

For the management of the replacement of digital signature certificates, the following requirements must be met:

- The subscriber must generate the request in Certicámara's web page: https://web.certicamara.com/soporte_tecnico, under the replacement project.
- The generation of the new signature must be done according to the contents of section 4.2 of this Certification Practices Statement.
- The subscriber must revoke the digital signature certificate. To do so, there are two possibilities:

i. The holder of the digital signature certificate, or an authorized third party, shall send the corresponding form authorizing the revocation of the digital certificate to the e-mail revocaciones@certicamara.com. The form may be requested by contacting the customer service line provided by Certicámara (601) 7442727 option 2, option 1.

ii. Through the following link where, by accepting the terms and conditions, you can carry out the process personally

iii. https://solicitudes.certicamara.com/SSPS/solicitudes/RevocarCertificadoClienteCF.aspx.

Additionally, there are exceptional cases where commercial agreements establish the obligation of Certicámara to maintain custody and management of quotas.In this scenario there must be a formal communication from the supervisor and/or administrator of the contract requesting the replacement of certificates and justifying under any of the following grounds:

- Change of holder
- Change of position
- Change of certificate type (Physical/Digital).

Next, the contract holder will send this request to the operations area at revocaciones@certicamara.com, where the certificate to be replaced must be indicated, as well as the information corresponding to the respective revocation. Based on the information provided, the control of the entity's quotas will be carried out.

4.12.1 Grounds for Replenishment

For each of the reasons set forth below, an internal analysis will be carried out by this company and a determination will be made as to whether the reinstatement is appropriate, in accordance with the defined procedure.

Certicámara will perform the replacement of the digital signature certificate in accordance with the previous numeral, when any of the following causes are present:

i. Loss of the physical device.
ii. Exposure of the PIN (Password/Key) of the digital certificate.
iii. Change in the information of the digital certificate previously issued (change of identification number does not apply).
iv. Change in the company's corporate name, regardless of keeping the same NIT.
v. Error attributable to Certicámara.

Additionally, the reinstatement will be made when any of the following events have occurred, which are typified in article 37 of law 527 of 1999:

i. Death of the subscriber.
ii. Due to supervening incapacity of the subscriber.
iii. Due to update of the information contained in the digital certificate.
iv. Due to loss, disablement or compromise of the security of the physical support of the digital certificate that has been duly notified to Certicámara.

In the event that the replacement is due to an error attributable to Certicámara, it may use the information previously provided by the applicant for the issuance of the certificate, without

the need for the generation of a new application by the subscriber and under the same conditions initially agreed.

4.13 Operational characteristics

4.13.1 Operatives Characteristics

For the validation of digital certificates, several Validation Service Providers are available to provide information on the status of certificates issued by the certification hierarchy. This is an online validation service (Validation Authority, VA) that implements the Online Certificate Status Protocol following RFC 6960. Using this protocol, the current status of an electronic certificate is determined without requiring CRLs.

An OCSP client sends a request about the status of the certificate to the VA, which, after consulting its database, provides a response about the certificate status via HTTP through the addresses http://ocsp.Certicamara.com, http://ocsp.Certicamara.co and http://ocsp4096.certicamara.co

The CRL files corresponding to each CA will also be available published on the Certicámara website at the following URLs:

- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara.crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_4096.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_4096.crl?crl=cr

4.13.2 Service Availability

The certificate status checking service is available 24 hours a day, 365 days a year, with a minimum availability level of 99.8%.

4.13.3 Optional Functions

To make use of the Online Validation Service by querying the address http://ocsp.Certicamara.com, http://ocsp.Certicamara.co and http://ocsp4096.certicamara.co , it is the responsibility of the bona fide third party to have an OCSP Client compliant with RFC 6960.

4.14 End of subscription

Termination of a certificate subscription occurs in the following cases:

- Revocation of the certificate for any of the causes for revocation expressed in the following document.
- Expiration of the certificate's validity.

4.15 Custody and retrieval of keys

4.15.1 Key Custody and Recovery Policy and Practices

The root CA private key is escrowed by an HSM cryptographic device. For access to the private key repository, Shamir's (k, n) threshold limit scheme is used in both software and cryptographic devices.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1. Site Location and Construction

All critical operations of the Root CA and Subordinate CA are physically protected with all necessary security measures for the most critical elements and with 24/7 surveillance. These systems are separated from other Certicámara systems so that only authorized personnel can access them.

5.1.2. Physical Access

Certicámara has services and technologies that complement the physical access controls to both its racks and Datacenter, where normally a minimum of three (03) controls must be passed.

The Data Processing Centers of the root CA and the Subordinate CA meet the following physical requirements:

- Closed-circuit television in critical or restricted access areas.
- Access control based on biometrics, keys.
- Authorizations through systems.
- Fire protection and prevention systems: detectors, fire extinguishers, training of personnel to act in the event of fire, etc.
- Facilities are located away from smoke vents.
- Video and/or photographic captures

5.1.3. Power and air conditioning

The facilities where the equipment is located have the necessary power and ventilation conditions to avoid power failures or other electrical anomalies or anomalies in the electrical systems.

Equipment cabling is protected to prevent interception or damage, and special measures have been taken to prevent loss of information caused by interruptions in the flow of electrical supply, connecting the most critical components to UPS to ensure a continuous supply of electrical power, with sufficient power to maintain the electrical network during controlled system shutdown events and to protect equipment from electrical fluctuations that could damage it.

The air conditioning systems maintain the equipment rooms with the proper humidity and temperature conditions for the correct operation and maintenance of the equipment.

5.1.4. Exposure to water

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

5.1.5. Fire Prevention and Protection

The Root CA and Subordinate CA facilities have an intelligent detection and extinguishing system. It is made up of:

- Intelligent control panel.
- Extension nozzles on the roof.
- Fire detectors in the ceiling and false ceiling.
- Alarm system that activates the fire detectors.

5.1.6. Media Storage

Information related to the Root CA and Subordinate CA infrastructure is securely stored in fireproof cabinets and safes, depending on the classification of the information contained therein.

This information is housed in different locations, in order to minimize associated risks.

5.1.7. Waste disposal

All waste generated from the operation of digital certification services are treated in accordance with applicable regulations to contribute to the environment and ensure the security of information.

5.1.8. Offsite Backup

All backup copies are stored in off-site entities distant from the Root CA and Subordinate CA. These facilities are protected with security means and mechanisms, in accordance with good international security practices.

5.2 Procedural controls

5.2.1. Trust roles

The Root CA and Subordinate CA, have personnel that due to their responsibilities are subject to special control procedures because their activity is essential for the proper functioning of the digital certification authority Certicámara S.A. Thus, they are considered trusted roles:

RA Agent: They are responsible for the review and validation of the information contained in the documents submitted by the applicant for the issuance of a DCA service.

CA Agent: They are in charge of approving the approval, activation and revocation of a DCA service.

PKI/TSA Infrastructure Specialist: Responsible for the operation of the systems that make up the root CA and Subordinate CA system, hardware and base software.

System Auditor: The Administrative and Financial Manager is internally responsible for the audit management process, where guidelines are established to evaluate compliance with applicable requirements.

5.2.2. Number of people required per task

As a security measure, collaborators have been designated to the different roles, guaranteeing due segregation of duties, independence and impartiality in their actions within the accredited services.

5.2.3. Identification and authentication for each role

The collaborators in charge of each of the roles have the necessary permissions within the framework of their functions, which are authenticated through the use of multiple factors, based on something that is known (platform access credentials) and something that is held (One Time Password).

Authentication is complemented with the corresponding authorizations to access certain information assets of the Certicámara system.

5.2.4. Roles requiring segregation of duties

The functions of the personnel performing the roles corresponding to the CA (Certification Authority) and the RA (Registration Authority) are segregated, so as to ensure independence and impartiality in their activities.

Taking into account the functions performed by the Registration Authority (RA) and the Certification Authority (CA), and in accordance with the Specific Accreditation Criteria - CEA, these activities are carried out by the personnel directly linked to Certicámara S.A.

5.3 Personnel controls

5.3.1. Qualifications, experience, and authorization requirements

Certicámara's collaborators that perform activities in the provision of digital services have a reliability study process through which references, experience, background, home visit, qualifications, among others, are validated.

5.3.2. Background verification procedures

For background checks, Certicámara, through a specialized company, performs consultations in defined lists to establish the suitability of a collaborator.

5.3.3. Training requirements

Certicámara establishes an annual training plan for its collaborators aligned with the training needs identified within the framework of their functions, which may contemplate some of the following aspects:

- Legal aspects related to the provision of certification services.
- Information security and personal data protection.
- Characteristics of accredited services at the operational and technical levels.
- Operating and administration procedures.
- Business continuity
- Technological changes in the environment.
- Introduction of new tools.
- Modification of operating procedures

5.3.4. Sanctions for Unauthorized Actions

Certicámara has established the procedure to carry out investigations and take the disciplinary measures that apply if employees fail to comply with the guidelines issued by the organization. In any case, if Certicámara suspects that any employee is performing an unauthorized action, it will automatically suspend his or her access permission, with the possibility of dismissal from the organization.

5.3.5. Independent contractor requirements

Certicámara has the contracting supports and the fulfillment of the administrative and technical requirements requested for those independent contractors that provide data center services.

5.3.6. Documentation provided to personnel

Certicámara shall make available to all personnel the documentation related to the functions associated with their position, the policies and practices that govern such processes and security documentation.

5.4 Audit logging procedures (Logs)

Certicámara has a log analysis tool to monitor the transactional and security audit logs and issue automatic alerts in order to identify failures or risk events that require remediation in a timely manner. It also keeps records for a minimum period of three (3) years that have been generated in the systems during this period of time.

5.4.1. Types of events recorded

Certicámara contemplates the recording of the following events:

- Warning: Indicates that an action performed within the systems involved presents an abnormal situation but is not necessarily a failure.
- Informative: Indicates that an action performed within the systems involved in the provision of accredited services has been completed correctly.
- Error: Indicates that an action performed within the systems involved presents an unexpected behavior that results in the expected non-completion of the action.

5.4.2. Frequency of record processing

The frequency of record processing is carried out on a permanent basis, ensuring that the information derived from the actions within the information systems involved is safeguarded.

5.4.3. Audit log retention period

The retention period for the different audit records has been defined as 3 years, after which time, in accordance with the guidelines provided, they may be destroyed.

5.4.4. Protection of audit records

The records derived from the actions carried out in the information systems shall be safeguarded in one copy inside Certicámara's facilities and another outside, ensuring that a copy is always available for consultation of the information in case it is necessary.

5.4.5. Vulnerability Assessments

Security tests including risk analysis, vulnerability scanning and ethical hacking are performed at least once a year. These are contracted by a specialized third party that complies with the assurance requirements defined in the specific ONAC accreditation criteria and internal to the company.

5.5 Archiving of records

5.5.1. Types of archived records

For digital signature certificate services, the documentation shall be defined in the information system according to each type of policy. For the other accredited services, they shall be displayed in the respective certification policies.

5.5.2. Archive retention period

The document retention period shall be in accordance with Article 38 of Law 527 of 1999, Certicámara's document retention schedules and current regulations.

5.5.3. Protection of the archive

The security measures defined are designed to protect the archives from unauthorized access (internal or external), so that only certain people can consult, modify or delete the archives. Files are stored using physical and logical security measures to protect them.

5.5.4. File Backup Procedures

Copies of the files that make up the files to be retained are made in accordance with the defined backup policies. The copy is generated and stored in a secure site within the Subordinate CA's main data center, which complies with environmental and physical security conditions.

5.5.5. Procedures for obtaining and verifying archival information

Recorded events are protected using cryptographic techniques so that no one except the event viewing and management applications themselves can access them. Only authorized personnel have access to the physical archives of media and computer files, to carry out integrity or other checks.

5.6 Change of password

The keys of the certificates issued by the Root CA will cease to be valid at the same time as their self-signed certificate. Once expired, the Root CA will generate a new self-signed key pair to generate the new root certificate. Certicámara will notify the external auditor and/or accreditation entity established by the regulations in force at the time of the key change, in order to determine the technical, procedural and legal conditions applicable to this procedure prior to its execution, to ensure compliance with the rules applicable to the process from the point of view of security. For such purpose, Certicámara shall submit the document called Key Change Ceremony, which shall be drafted and adjusted for its presentation prior to the proposed date for the change of keys.

5.7 Commitment and disaster recovery

Certicámara has established and tested the Business Continuity and Contingency Plan (BCP) that defines the actions to be taken, resources to be used and personnel to be employed, in the event of a natural disaster or an intentional or accidental event that disables or degrades the resources and the digital signature certificate service accredited by ONAC, to ensure the continuity of the service.

The plan ensures that Certicámara can continue to provide the service in adverse situations, after identifying, assessing, managing and minimizing any type of risk.

Through the Business Impact Analysis (BIA), the respective preparation, attention and response to possible adverse situations that may arise, as well as the respective actions to be executed, have been carried out, having as a reference the reduction of the operational impacts to which Certicámara would have been exposed.

5.7.1. Incident Management Procedures and Commitments

Certicámara has defined the procedure for Incident Management to ensure the continuity of the operation, prevention and timely reaction to possible failures in the normal operation of

the services, guaranteeing a minimum of interruptions in the provision and availability of the platforms.

The business continuity plan ensures that Certicámara can continue providing the service in adverse situations, after identifying, evaluating, managing and minimizing any type of risk events, where at least the following are contemplated:

- When the security of the certification entity's private key has been compromised.
- When the security system of the certification entity has been breached.
- When there are failures in the certification entity's system that compromise the provision of the service.
- When the encryption systems become invalid because they do not offer the level of security contracted by the subscriber.

Certicámara will advocate for the follow-up of the recommendations given by: https://csrc.nist.gov/projects/hash-functions

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt3r1.pdf

5.7.2. Business Continuity Capabilities after a Disaster

Certicámara's business continuity capabilities are defined in the business continuity plan, where the necessary resources for its execution are established.

5.8 Cessation of activities

Pursuant to the provisions of Article 163 of Decree Law 019 of 2012, which amends Article

34 of Law 527 of 1999, the DCAs accredited by ONAC "may cease the exercise of activities, provided that they guarantee the continuity of the digital certification service to those who have already contracted it, directly or through third parties, without additional costs to the services already cancelled". Because of the above, Certicámara shall inform ONAC of the cessation of services, with 30 days' notice, as established in Chapter 48 of DURSCIT, Article 2.2.2.48.3.8. Cessation of activities.

Therefore, Certicámara has defined a business continuity and contingency plan for all services that are accredited, ensuring the continuity in high availability of the infrastructure provided and ensuring the proper cessation of its activities as DCA.

Certicámara will inform of the termination by sending an e-mail to all subscribers who have the accredited services in force and by means of two notices published in newspapers or media of wide national circulation, with an interval of 15 days, about:

I. The termination of its activity or activities and the precise date of cessation.
II. The legal consequences of the cessation with respect to the accredited services.
III. The possibility for a subscriber to obtain a refund equivalent to the value of the remaining term of the contracted service.
IV. The authorization issued by ONAC for the DCA to cease the service, and if applicable, the CRL operator responsible for the publication of the certificates issued by the DCA, until the last of them expires.
V. Any other obligation established by law

In any case, subscribers may request the revocation and reimbursement equivalent to the value of the remaining term of the services, if requested within two (2) months after the second publication.

The completion of the activity or activities shall be carried out in the manner and according to the schedule presented by Certicámara to the supervisory and control entity and approved by the latter.

6. TECHNICAL SECURITY CONTROLS

6.1 Generation and installation of key pairs

The Root CA generates the key pair (Public and Private) using a hardware cryptographic device (HSM) that complies with the requirements established in a standardized certification authority secure electronic signature device protection profile, in accordance with FIPS 140-2 Level 3 or higher security level, and the CA's key creation uses a pseudo- random number generation algorithm.

The key generation procedure for Subordinate CAs accredited to Certicámara is identical, in their own HSM.

6.1.1. Delivery of private key to the subscriber

The algorithm used for the generation of the subscriber's key pair is RSA not less than 4096 bits using the cryptographic hash function SHA256. Subscribers can use the following means to generate their digital certificates and guard them:

- USB hardware token devices to generate their private key, which comply with the FIPS 140-2 Level 3 standard.
- Virtual Token, using Certicámara's HSM (Hardware Security Module).
- PKCS#10, when the subscriber previously creates his own keys and requests Certicámara to sign the digital certificate, the request must guarantee:
  - Minimum key size 4096 bits.
  - The request must be sent in PKCS#10 format.

Risks to which the cryptographic devices used would be exposed:

- Fluctuations outside the normal environmental operating ranges, such as, for example: voltage, temperature
- Unauthorized attempts of physical access outside the manufacturer's datasheet

For the level of risks associated with cryptographic devices, please refer to NIST.FIPS.140-2.pdf

6.1.2. Delivery of public key to the certificate issuer

The public keys generated by the end entity under its responsibility are sent to Certicámara as part of a certificate request. CSR requested to be signed by the subordinate CA.

6.1.3. Delivery of the CA's public key to trusted parties

The public key of any Certicamera subscriber shall be permanently available in the active directory for consultation by trusted parties upon request.

6.1.4. Key sizes

- For Root CA certificates, RSA algorithm with 4096-bit size is used.
- For Subordinate CA certificates, RSA algorithm with size of 4096 bits is used.
- For End Entity certificates, RSA algorithm with minimum key size of 2048 bits is used.

6.1.5. Key usage purposes (according to X.509 v3 key usage field)

Only the private key and certificate may be used for authorized uses in this CPD and PC. Certicamera issues certificates with the private key usage fields limited to certificate signing and CRL signing.

The intended uses for CA certificate keys are:

- Certificate Signing
- Offline CRL signing
- Certificate revocation list (CRL) signing

The intended uses for end-entity certificate keys are:

- Digital Signature
- Non-repudiation
- Key encryption
- Data encryption
- Key agreement.
- Enhanced key usage:
- Subscriber authentication (OID 1.3.6.1.5.5.7.3.2)- Applies to all certificates.
- Secure mail (OID 1.3.6.1.5.5.7.3.4) – Applies to all certificates
- Server authentication (1.3.6.1.5.5.7.3.1) – Applies to Company / Entity Representation and Legal Entity certificates.

6.2 Private key protection and cryptographic module engineering

The Root CA's private key is protected by a security scheme generated by a cryptographic device. To keep the private keys of the self-signed certificate safe, the private key is never decrypted outside the HSM.

The backup copies maintain the secrecy of the private key in the same way that the original private key is safeguarded.

6.2.1. Cryptographic module standards and controls

The HSM used by the Root CA to generate its keys is FIPS 140-2 Level 3 certified.

The public key has been stored in signed electronic format, so that they are protected from electronic failures and/or power problems.

Therefore, the commissioning of a CA involves the following tasks:

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

6.2.2. Private key (K of N) multi-person control

The Root CA generates its key pair using a hardware security module (HSM). Authentication against the HSM requires at least 2 of 3 operators. This procedure follows the K of N scheme, with the non-persistent mode of the cryptographic device. In this mode it is necessary to guarantee the physical connection of the last set of cards in the HSM reader, to open the private key of the Root CA.

6.2.3. Custody of the private key

The private key of the Root CA and Subordinate CA is stored in a cryptographic device. This device complies with the requirements established in a standardized certification authority secure electronic signature device protection profile, in accordance with FIPS 140-2 Level 3 security.

The rest of the private keys of operators and administrators are contained in cryptographic smartcards held by the administrators of each entity, the private key of Certicámara is not held in trust by a third party.

6.2.4. Private key security copy

Private key backups are performed in accordance with the security guidelines and recommendations indicated by the PKI software manufacturer. The security guidelines describe the use of FIPS 140-2 level 3 compliant cryptographic devices, a set of cards that meet the k/n requirement for protection, and at least the collaboration of the PKI/TSA infrastructure specialist, cryptographic material custodian and personnel designated by the Operations and Technology Management are required.

6.2.5. Archiving of private keys

Backup copies of private keys will be kept in encrypted custody in the alternate computing center. Backup copies of private keys are kept in secure fireproof archives.

6.2.6. Storage of private keys in cryptographic module

The private keys are created within the cryptographic module at the time it is initialized, subsequently the private key generated within the HSM is exported in encrypted form.

6.2.7. Private Key Activation Method

The only activation method for the private key is the use of smart cards to distribute access to different people and roles. Explicitly the only combination to activate the private key requires two out of three HSM administrators, three out of eight HSM operators and an application OS administrator.

6.2.8. Private Key Deactivation Method

An OS administrator can proceed with the deactivation of the private key of the Root CA and Subordinate CA. After being activated by the combination described in the previous section, the operator can proceed to deactivation by stopping the CA application.

6.2.9. Private key destruction method

The Root CA and the Subordinate CA shall delete the private key when its term expires or has been revoked. The destruction shall be performed using the established commands to physically erase the portion of the HSM memory in which the key was recorded. The same will happen with your backup copies.

6.2.10. Cryptographic Module Qualification

The Root CA and Subordinate CA use commercially available hardware and software cryptographic modules developed by third parties. The Root CA and Subordinate CA only use FIPS 140-2 Level 3 certified cryptographic modules (nShield Edge, nShield Connect 500, nShield Connect 1500+, nShield Connect 6000+).

6.3 Other aspects of key pair management

6.3.1. Public key file

The public key of the Root CA and Subordinate CA is archived according to the standard PKCS#7 format for a period of 20 years.

6.3.2. Certificate operating periods and key pair usage periods

The Root CA key pair shall be valid until Saturday, May 24, 2031. On the other hand, the certificate operating periods shall be ten years.

The key pair of the subordinate CA will be valid until Saturday, May 24, 2031. On the other hand, the certificate operating periods shall be ten years.

6.4 Activation data

6.4.1. Generation and installation of activation data

The activation data of the Root CA and Subordinate CA must be generated and stored on smart cards. Their protection is ensured by a PIN in the possession of authorized personnel.

6.4.2. Activation data protection

Only authorized personnel possess the cryptographic cards capable of activating the CA's private keys, as well as the PINs required for their use.

The personal access key (PIN) is confidential, personal and non-transferable and is the parameter that protects the private keys allowing the use of the root CA and Subordinate CA certificates; therefore, security rules for its custody and use must be taken into account:

- The PIN must not be sent or communicated to any person.
- Operators and administrators should change the PIN when they suspect that it is known to someone else.
- It is recommended to change the PIN periodically.

6.5 Computer security controls

6.5.1. Specific technical requirements for computer security

For the respective provision of the service, a series of technical controls have been established to ensure its proper functioning and guarantee its adequate operation. Among the aspects that are considered are:

- Equipment configuration
- Configuration of the applications
- User configuration
- Application of profiles for network access.

6.5.2. IT security qualification

Certicámara as part of its organizational approach is currently certified under ISO/IEC 27001:2013 - Information Security Management System in accordance with the scope published within the respective certificate.

6.6 Technical life cycle controls

6.6.1. System Development Controls

Security requirements for system development for the Root CA and SUBORDINATE ENTITY are enforceable.

A security design analysis must be performed during the design and new requirements specification phases of any components to be used in the Root CA and Subordinate CA applications. This is to ensure that the systems involved are secure.

The technology infrastructure of the Root CA and Subordinate CA should be provided with clearly differentiated and independent development and production environments. Change control procedures should be used for new versions and upgrades.

6.6.2. Security Management Controls

Certicámara maintains an inventory of all IT assets and classifies them according to their protection needs; the guidelines for this will be dictated by the results of the risk analysis carried out.

The configuration of the systems must be audited periodically and the growing need for resources must be monitored according to demand.

6.6.3. Life cycle security controls

Throughout the lifecycle, security controls must be implemented to implement and audit each phase of the root CA and subordinate CA systems.

6.7 Network Security Controls

The technological infrastructure of the Root CA and Subordinate CA has a network with all the necessary security mechanisms to guarantee a reliable and complete service. Firewalls or encrypted data exchange between networks are used to ensure integrity. On the other hand, waiver and high availability technologies are used to guarantee a reliable and high-performance operation. In addition, the infrastructure must be periodically audited by people inside and outside Certicámara.

6.8 Time stamping

The synchronization of the clocks of the CA and the RA is based on the Legal Time of the Republic of Colombia, taken directly from the reference standards of the National Metrology Institute - INM, of Colombia, in accordance with the provisions of Article 14 of Decree 4175 of 2011, as amended by Decree 62 of 2021.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

Root CA and SUBORDINATE ENTITY certificates are issued in accordance with the following standards:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, mayo 2008.
- ITU-T Recommendation X.509 (2012): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.3 (2006-01): Qualified Certificate Profile, 2006
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (TS 101 862 prevailing in case of conflict)

7.1.1. Version number(s)

Certificates issued by Certicámara are compliant with the X.509 v3 standard.

7.1.2. Certificate extensions

The certificate extensions of the Root CA and Subordinate CA allow additional information to be encoded in the certificates.

The X.509 standard extensions define the following fields:

- SubjectKeyIdentifier
- AuthorityKeyIdentifier
- BasicConstraints. Marked as critical
- Certificate Policies. Marked as critical
- KeyUsage. Marked as critical
- CRLDistributionPoint. Marked as critical
- SubjectAlternativeName. Marked as critical
- AuthorityInformationAccess

The following are the fields of the certificates that are issued to subscribers:

- Date and time signed
- Document Name
- Subject
- Certificate Authority
- Certificate Serial
- Thumbprint
- Certificate valid from
- Certificate valid until

7.1.3. Algorithm object identifiers

- OID of the SHA256withRSAEncryption 1.2.840.113549.1.1.11 signature algorithm
- OID of the RSAEncryption 1.2.840.113549.1.1.1 public key algorithm

7.1.4. Name forms

Certificates issued by Certicamera have a DN, in X format. 500 format, the names of the issuer and certificate holder in the issuer (issuer) and subject (subject) fields.

7.1.5. Name restrictions

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

7.1.6. Certificate policy object identifier

The root CA has defined a policy for assigning OID's within its private numbering tree.

7.1.7. Policy Qualifier Syntax and Semantics

The syntax and semantics of its description can be found inside the generated digital certificates, within the certificate directives section, where a URL where the Certicámara's DPC is published is shown.

7.2 Certificate revocation list profile

7.2.1. Version Number(s)

The Subordinate CA issues the CRLs with X. 509 format.

7.2.2. CRLs and CRL entry extensions

The extensions of the CRLs issued by the Root CA, are those defined according to RFC 5280, i.e.:

- Authority Key Identifier
- CRL Number
- Issuing Distribution Point

7.3 OCSP Profile

The validity status of a particular certificate issued to a subscriber may be verified using the online OCSP certificate status protocol, which is implemented in accordance with RFC 6960.

7.3.1 Version number(s)

Version 1 of the OCSP protocol is used, as stated in RFC 6960.

7.3.2 OCSP extensions

According to the operation of the generation of digital certificates, the use of OCSP extensions is not established.

8. COMPLIANCE AUDIT AND OTHER EVALUATIONS

8.1 Frequency or circumstances of the evaluation

According to the definitions of the National Accreditation Body - ONAC in Colombia, an annual audit plan has been established, within which the different accredited services are evaluated.

The accreditation system of the Root CA and Subordinate CA shall be subject to a third- party audit on an annual basis, in accordance with the audit program defined by Certicámara. This ensures the adequacy of its functioning and operability with the stipulations included in this DPC.

Additionally, Certicámara may establish internal audits at its own discretion or at any time, due to a suspicion of non-compliance with any security measure or due to a compromise of the keys.

Each year an external audit will be conducted to assess the degree of compliance with the principles and criteria of Web Trust for AICPA/CICA Digital Certification Authorities.

8.2 Assessor's identity/qualifications

In the case of third-party audits, the auditing company must comply with the minimum assurance requirements established in the specific accreditation criteria published on ONAC's website and those defined in the internal processes for contracting third parties.

8.3 Relationship between the assessor and the entity being assessed

The relationship between the auditor and the audited entity shall be strictly limited to the processes and information required for the audit. Therefore, the auditee (root CA or subordinate entity) shall not have any current or planned financial, legal, or any other type of relationship that could result in a conflict of interest with the auditor. In the case of internal auditors, they may not have a functional relationship with the area being audited.

8.4 Subjects covered by the assessment

All technical, functional, and organizational requirements are subject to audit including:

- The DPC used.
- Information Security Policy.
- Administration of the Root CA and Subordinate CA.

- Confidentiality considerations.
- Physical Security.
- Backup Model.
- Business Continuity Plan.
- Operational Staffing.
- Specific ONAC accreditation criteria according to the current CEA.

8.5 Actions taken as a result of non-conformities

The identification of any nonconformity in audits will result in the implementation of the Corrective and Preventive Action Management process internally, in order to eliminate the root cause identified. In the case of a critical non-conformity, Certicámara may determine the temporary suspension of the operations of the Root CA or Subordinate CA until the deficiencies are corrected, revocation of the entity's certificate, personnel changes, etc.

8.6 Communication of results

All audit results are presented to the presiding committee, with the objective of determining the corrective and preventive actions considered pertinent.

9. OTHER LEGAL AND COMMERCIAL MATTERS

9.1 Fees

9.1.1. Fees for issuance or renewal of certificates

The fees established by Certicámara for each of the services that are accredited are defined in each of the certification policies published on the web page.

9.1.2. Fees for access to revocation or status information

Certicámara does not consider within its tariff policies the charge for access to certificate status validation services. There will be no charge for this service.

9.1.3. Refund Policy

Digital certificate subscribers may request a refund through the Certicámara S.A. website, section PQRSAF https://web.certicamara.com/soporte_tecnico in the following cases:

- Subscriber withdrawal: the right of the subscriber to return the product he/she purchased or the service he/she contracted, and request the refund of the money paid, without giving explanations, before 5 working days from the delivery of the good or the conclusion of the contract.
- Withdrawal of the acquisition process: The subscriber requests the refund when the digital certificate has not been issued. In these cases, we speak of a withdrawal from the acquisition process, since the good has not yet been delivered.
- Reimbursement for double payment, overpayment, erroneous payment: The subscriber pays twice for the same invoice or digital certificate or paid a little more than what was due or made an erroneous consignment.
- Tax refund: In this case the customer paid a value of some tax that should not be paid and therefore must proceed with the refund.
- Refund due to incompatibility: In these cases the client requests a refund because the digital certificate is not compatible with his equipment or system or simply the certificate was not the one he required.
- Refund for breach of the duty of information: Certicámara is obliged to provide information about its products that is complete, clear and true. Therefore, in case of failure to comply with the duty of information, Certicámara must proceed with the refund of the money regardless of the term in which it is presented.
- Request for reversal of payment in accordance with the grounds set forth in Decree 587 of 2016.

9.2 Financial Liability

9.2.1. Insurance coverage

In accordance with the provisions of numeral 5 of article 2.2.2.48.2.3 of Decree 1074 of 2015 (which compiles Decree 333 of 2014, article 7) and article 2.2.2.48.2.2. 5 of Decree 1074 of 2015 (compiling Decree 333 of 2014, article 9), Certicámara has taken out an insurance policy with an insurance company authorized in accordance with Colombian law, which covers contractual and extra-contractual damages of subscribers and third parties in good faith exempt from fault arising from errors and omissions, or acts of bad faith of the administrators, legal representatives or employees of Certicámara in the development of its activities.

b. The insured amount is 7,500 Current Minimum Monthly Wages per event.

c. The general conditions of the policy can be consulted at https://web.certicamara.com/marco_legal , where you will find the updated information of the policy.

9.3 Confidentiality of information

Certicámara undertakes to protect all data to which it has access as a consequence of its activity as a certification entity.

However, Certicámara reserves the right to disclose to employees and consultants, external or internal, confidential data necessary to carry out its activities. In this case, employees and/or consultants are informed of the confidentiality obligations.

These obligations do not apply if the information qualified as "confidential" is required by the Courts or competent administrative bodies or imposed by a law, in which case the confidential information given by the subscriber will be disclosed, in accordance with the regulations in force.

The confidential information of the subscriber of digital certification services may be disclosed at his request, in his capacity as owner of this information.

9.3.1. Scope of confidential information

Confidential information is considered to be:

- Documents that have information related to the administration, management and control of the PKI infrastructure.
- Business information supplied by its suppliers and other persons with whom Certicámara has a legally or conventionally established duty of secrecy.
- Information resulting from consultations made in credit bureaus or other private or public sector entities.
- Employment information containing data related to the subscriber's salary.
- All information that is sent to Certicámara and that has been labeled as "Confidential" by the sender.

9.3.2. Information outside the scope of confidential information

Non-confidential information is considered to be:

- Content of issued certificates
- List of Revoked Certificates (CRL)
- The public key of the Root CA and Subordinate CA
- The certification practices statement
- Organizational policies

9.3.3. Responsibility to protect confidential information

Certicámara undertakes to safeguard the confidentiality of the information and not to make it available or disclose it to unauthorized individuals.

Regarding the treatment of personal data, Certicámara applies the principle of confidentiality through which, for those personal data that are not of a public nature, the confidentiality of the information is guaranteed, making the provision or communication only in cases authorized by law.

9.3.4. Notice and Consent to Use Private Information

Certicámara has at the disposal of the applicant and subscriber, the policy of treatment of personal data in the web page https://web.certicamara.com/politicas.

In addition to the above, prior to the acquisition of digital certification services, Certicámara delivers the terms and conditions, which also refer to the existence of the policy and how to access it.

When applicable, Certicámara will generate privacy notices informing the owners, the treatment and purposes to which the data will be submitted, as well as the rights of the owner, to ensure compliance with the duty to inform the owner.

9.3.5. Disclosure by virtue of a judicial or administrative process

The information is not available or disclosed to unauthorized individuals, entities or processes. It may only be disclosed when required by a judicial or administrative authority, in the exercise of its functions.

In accordance with the provisions of Law 1581 of 2012, the authorization of the holder is not necessary when the information is required by a public or administrative entity in the exercise of its legal functions or by court order.

9.4 Intellectual Property Rights

The Subscriber shall respect and comply with the regulations on intellectual property, which includes both industrial property and copyrights. To this effect, it shall comply with the provisions of the Code of Commerce, Decision 486 of 2000, Decision 351 of 1993 and other complementary regulations on these matters.

By means of this provision it is established that all information contained in the Declaration of Certification Practices -DPC belongs solely and exclusively to the Sociedad Cameral de Certificación Digital Certicámara S.A., so that it reserves all rights related to the intellectual property of this document (DPC), including information, techniques, models, internal policies, processes and procedures, in accordance with national and international regulations related to the matter.

9.5 Obligations and Responsibilities of the Interveners

9.5.1. Obligations and duties of Certicámara

Certicámara has the following obligations in the provision of its services:

a) Implement and maintain the security systems that are reasonable in terms of the service provided and in general the infrastructure necessary for the provision of the Digital Certification service.

b) Comply with the Declaration of Certification Practices (DPC), Certification Policies (CP) and the agreements made with subscribers.

c) Inform the subscriber of the characteristics of the service, the limits of responsibility, and the obligations assumed by the subscriber as a participant in the digital certification process. Certicámara shall inform the subscriber or third parties that request it, about the time and computational resources required to validate the digital signature made with the signature certificates it issues to its subscribers.

d) Verify directly or through the Registration Entities duly accredited before Certicámara, the information defined in this Certification Practice Statement as verifiable for the issuance of digital certificates.

e) Refrain from accessing or storing the subscriber's private key.

f) Keep, by itself or through an intermediary, the custody of the physical support of the digital certificate until the effective delivery of the same to the subscriber (if applicable).

g) Allow and facilitate the performance of audits by the National Accreditation Body of Colombia.

h) Issue digital certificates in accordance with the provisions of the digital certificate issuance procedure section of this Certification Practice Statement, and the specifications agreed by the subscriber in the subscription contract.

i) Publish the digital certificates issued and keep the Register of Issued Certificates.

j) Inform the National Accreditation Body of Colombia the occurrence of any event established in the Certification Practices Statement, which compromises the provision of the service.

k) Inform the National Accreditation Body of Colombia of the introduction of new requirements or changes in the PKI infrastructure that may affect the provision of the service.

l) Notify the subscriber of any change in the status of its digital certificate, explaining the reasons for the decisions taken in accordance with the provisions of the Certification Practices Statement.

m) Maintain control and confidentiality of the private key and establish reasonable safeguards against disclosure or compromise.

n) Diligently seek the permanent and uninterrupted provision of digital certification services.

o) Allow access by subscribers, relying parties and third parties to this Certification Practices Statement and the repository of the Certification Entity.

p) Update the database of revoked digital certificates under the terms established in this Certification Practice Statement and make the notices and publications established by law in this document.

q) Revoke digital certificates as required in accordance with the provisions of section 4.7 of this Certification Practice Statement.

r) Inform the subscriber, within 24 hours, the revocation of its digital certificate(s), in accordance with current regulations.

s) Remove the administrators or representatives that are found to be in breach of the grounds established in article 29 c of Law 527 of 1999.

t) To have a hotline for subscribers and third parties, which allows for consultations and the prompt request for revocation of certificates by subscribers.

u) Provide the information required by the competent administrative or judicial entities in relation to the digital signatures and certificates issued and in general about any data message under its custody and administration.

v) Keep physically or electronically the documentation that supports the digital certificates issued, for the term provided by law for the traders' papers and take the necessary measures to guarantee the integrity and confidentiality that are proper to it.

w) Address requests, complaints and claims made by subscribers, in accordance with the provisions of this Declaration of Certification Practices.

x) Treat the information provided by the subscriber as established in the certificate request section of this Certification Practice Statement.

y) Comply with the Specific Accreditation Criteria CEA 3.0-7 published on the ONAC web page.

z) Warn about the security measures that must be observed by subscribers of digital signatures and certificates for the use of these mechanisms.

aa) Certicámara, without any discrimination whatsoever, will provide the digital certification service to any applicant that complies with the requirements established in this DPC and legal regulations in force; however, Certicámara may decline the digital certification request to the applicant or subscriber when there is evidence of participation in illicit activities.

bb) To comply with the provisions of the Statutory Law 1581 of 2012 on Personal Data Protection and its implementing regulations, the personal data provided will be treated in accordance with the procedures that Certicámara S.A. has defined for this purpose and with the purpose of issuing a Digital Certification service or services related to it.

cc) Notify the subscriber in advance about the outsourcing activities in order to give him/her the opportunity to object in accordance with the Colombian regulations in force, for this purpose Certicámara has in its web page a system for reception of Petitions, Complaints, Claims, Suggestions and Appeals PQRSA.

dd) The critical suppliers contracted for the provision of datacenter services comply with the minimum requirements established in the document Specific Criteria for Accreditation CEA 3.0-7 published on ONAC's web page. To this effect, compliance with the requirements described in the CEA 3.0-7 Specific Accreditation Criteria published by ONAC shall be extended to them when applicable.

ee) The others established by Law 527 of 1999 in its article 32 and Decree 1074 of 2015 (which compiles Decree 333 of 2014) in its article 2.2.2.48.3.6.

The fulfillment of all or part of the obligations or procedures for the issuance of digital certificates or the provision in general of the digital certification service may be performed directly by Certicámara or through its Registration Entities.

CERTICÁMARA HAS NO ADDITIONAL OBLIGATIONS TO THOSE FORESEEN IN THIS SECTION EXCEPT THOSE FORESEEN IN THE CURRENT REGULATIONS, NOR SHALL IT BE UNDERSTOOD THAT THERE ARE ADDITIONAL IMPLICIT OBLIGATIONS TO THOSE EXPRESSLY SET FORTH IN THIS CERTIFICATION PRACTICES STATEMENT.

9.5.2. Obligations and Duties of the Applicant

Applicants for Certicámara's certification services shall have the following obligations and responsibilities:

a) Provide the required information in accordance with the requested digital certification service.

9.5.3. Obligations and responsibilities of the Subscriber

The Subscriber has the following obligations towards Certicámara and third parties:

a) Use the private key and the digital certificate issued only for the purposes established and in accordance with the conditions established in the contract entered into with him/her individually and in this Certification Practice Statement and the corresponding certification policy. It will be the responsibility of the subscriber the improper use that he or third parties make of it.

b) Use the private key and the digital certificate to sign data messages, explaining to the relying parties under which capacity the subscriber is signing (either as a natural person or as a natural person linked to a specific capacity at the time of issuance of the digital certificate), provided that the information system of the relying party does not verify the capacity in which the subscriber is acting. The data message or

electronic document that the subscriber signs with its digital certificate will determine the context of the capacity in which the subscriber is signing, and whether or not the subscriber is using the capacity associated with the digital certificate (if applicable).

c) Respond for the custody of the private key and its physical support (if applicable) avoiding its loss, disclosure, modification or unauthorized use. In particular, the subscriber shall refrain, regardless of the circumstance, from noting on the physical support of the digital certificate the activation code or the private keys, nor in any other document that the subscriber keeps or carries with him/her or with the physical support.

d) Request the revocation of the digital certificate that has been delivered when any of the cases foreseen for the revocation of digital certificates is fulfilled.

e) Refrain in all circumstances from disclosing the private key or the activation code of the digital certificate, as well as refrain from delegating its use to third parties.

f) Ensure that all the information contained in the digital certificate is true and immediately notify Certicámara in case any incorrect or inaccurate information has been included or in case that due to any subsequent circumstance the information in the digital certificate does not correspond to reality. Likewise, it will have to communicate immediately the change or variation that has suffered any of the data provided to acquire the digital certificate, even if these were not included in the digital certificate itself.

g) Immediately inform Certicámara about any situation that may affect the trustworthiness of the digital certificate and initiate the procedure for revocation of the digital certificate when necessary. It shall immediately notify the loss, theft or forgery of the physical support and any attempt to perform these acts on it, as well as the knowledge by others of the activation code or private keys, requesting the revocation of the digital certificate in accordance with the procedure established in the Certification Practices Statement.

h) Destroy the physical support when required by Certicámara, when it has been replaced by another for the same purposes or when the period of the service purchased from the digital certificate with Certicámara ends, following in any case the instructions of Certicámara.

i) To return the physical support of the digital certificate when Certicámara requires it.

j) Respect the intellectual property rights (Industrial Property and Copyrights) of Certicámara and third parties in the application and use of the digital certificates. Certicámara will not include information in the digital certificate whose inclusion may

constitute in any way the violation of the intellectual or industrial property rights of Certicámara and third parties.

k) Any other that derives from the current regulations, the content of this Certification Practices Statement or the Certification Policy.

l) Refrain from monitoring, altering, reverse engineering or interfering in any other way with the provision of digital certification services.

m) Refrain from using the digital certificate in situations that may cause bad reputation and damage to Certicámara.

n) Refrain from using the name of the DCA and the certification mark or in all advertising material containing any reference to the digital certification service provided by Certicámara immediately after its cancellation or termination and take the actions required by the digital certification service and any other action required.

o) Comply with the manual for the use of the logo established by Certicámara.

p) Comply with the requirements established by the digital certification service in relation to the use of trademarks in the provision of services and consequently respect the trademark rights held by Certicámar.

The others established in article 39 of Law 527 of 1999.

THE SUBSCRIBER MAY USE ITS CERTIFICATE TO: (I) IDENTIFY ITSELF AS A NATURAL PERSON, OR (II) ASSOCIATE ITS PERSONAL IDENTIFICATION TO A SPECIFIC QUALITY VERIFIED BY CERTICÁMARA AT THE TIME OF ISSUANCE OF THE DIGITAL CERTIFICATE (IF APPLICABLE). THE USE OF THE DIGITAL CERTIFICATE IN EITHER CASE WILL DEPEND DIRECTLY ON THE CONTEXT IN WHICH THE DIGITAL CERTIFICATE IS BEING USED AND WHETHER OR NOT THE RELYING PARTY'S INFORMATION SYSTEM CAN VERIFY THE SUBSCRIBER'S IDENTIFICATION.

IT WILL BE THE ELECTRONIC DOCUMENT OR DATA MESSAGE THAT THE SUBSCRIBER SIGNS DIGITALLY, WHICH WILL PROVIDE THE CONTEXT WITHIN WHICH THE SUBSCRIBER MAKES USE OF THE CERTIFICATE AND WHETHER OR NOT THE SUBSCRIBER USES THE QUALITY ASSOCIATED WITH THE DIGITAL CERTIFICATE.

9.5.4. Obligations and responsibilities of the relying party

Certicámara's Digital Certification System comprises the use of a set of integrated elements around the provision of a service to both subscribers and those who use and trust the digital certificates issued by Certicámara. When a third party trusts a digital certificate, it is accepting to use such system in its entirety and therefore agrees to abide by the rules established for it, which are contained essentially but not exclusively in this Declaration of Certification Practices. This third party becomes an intervener of the Digital Certification System, as a relying party, and therefore assumes the obligations established below:

a) Verify the reliability of the digital signature and the digital certificate, checking especially that it is not found in the database of revoked digital certificates of Certicámara available on the website or in the offices of Certicámara. The trustworthiness of the digital signature and the digital certificate shall in any case comply with the provisions of the section on Trustworthiness of digital signatures and certificates.

b) Accept and acknowledge digital certificates only for the use that is permitted in accordance with the provisions of the Use of Digital Certificates section.

c) To know carefully and always comply with the Declaration of Certification Practices in the use of digital signatures and certificates of Certicámara. In particular, the relying party shall always be aware of and act in accordance with the limitations of liability and warranties provided by Certicámara.

d) Inform Certicámara of any irregularity or suspected irregularity in the use of the Digital Certification System.

e) Refrain from monitoring, altering, reverse engineering or interfering in any other way with the provision of digital certification services.

9.5.5. Contractor Obligations

If Certicámara externally contracts services or products related to the activities accredited in the scope, compliance with the requirements established in the CEA 3.0-7 shall be extended, based on the nature of the contracted service, this Certification Practices Statement and the requirements of the Colombian regulatory framework in force according to its contracted function for digital certificates.

Certicámara will determine whether the external approval entity provides the levels of compliance, as contractually established, without prejudice to the highest standards in force at the legal, technical, operational and procedural level for the approval process, which will be available for study and contrast in the management systems of Certicámara, which allow

to establish access according to their classification of confidentiality, and in any case will be available for the reception of third party audits and by the National Accreditation Agency.

9.6 Limits of Liability

a) The obligations listed in the section on Certicámara's obligations are of means and not of result. This means that Certicámara will use its knowledge and experience in the provision of the digital certification service and will be professionally liable for slight fault in its actions as a Digital Certification Authority. Certicámara cannot ensure that the certification activity will have a certain result. Certicámara will only be liable for those errors that could have been avoided by its professional diligence.

b) The damages produced or related to the non-performance or defective performance of the obligations of the subscriber, the relying party or both, shall be borne by them, as well as any damage caused by the improper use of the digital certificates or violations of the limitations of use established in the same, in the section of Use of digital certificates or in any other document that regulates the Digital Certification System. In addition to the above, in the case of subscribers will be taken into account what the current regulations establish in terms of liability of subscribers.

c) Certicámara shall not be liable for damages caused by the breach of its obligations due to force majeure, acts of God or, in general, any circumstance over which it cannot have reasonable control, including but not limited to the following: natural disasters, public disturbances, power and/or telephone outages, computer viruses, deficiencies in telecommunications services (Internet, communication channels, etc.) or the compromise of asymmetric keys resulting from unforeseeable technological risk.

d) Regardless of the cause or origin of its liability, Certicámara sets as maximum amount for the compensation of damages for the damages caused by a digital certificate issued, according to the provisions of the professional liability policy. Consequently, Certicámara will only indemnify the persons harmed by a digital certificate issued by Certicámara, regardless of the number of times it has been used or the number of persons harmed by such uses. In the event that there are several injured parties, the maximum amount of compensation shall be distributed pro rata among them. If, once the indemnity has been distributed, new injured parties should arise, they shall contact the persons already indemnified in order to obtain their indemnity on a pro rata basis.

e) Certicámara will only be liable for damages caused by the use of digital certification services within one year after the expiration or revocation of the digital certificate.

Certicámara does not offer any type of guarantee that is not expressly stipulated in this Declaration of Certification Practices, nor will it respond for any event that is not expressly contemplated in this section.

f) Shall be liable in accordance with the provisions of articles 16 and 19 of Decree 333 of 2014 compiled by Decree 1074 of 2015.

g) If the laws applicable to the digital certification service establish the impossibility of limiting liability in any of the aspects described herein or described in this Certification Practices Statement, these clauses shall be given the widest scope that the law allows to give them in terms of the limitation of Certicámara's liability.

9.7 Rights of the intervening parties

9.7.1. Rights of the applicant

Applicants for Certicámara's certification services shall have the following rights:

a) That their request be attended to in accordance with the times defined by the entity.

b) That the provisions of the certification policies be complied with.

c) Receive attention to solve doubts or concerns regarding the digital certification service.

9.7.2. Subscriber Rights

Subscribers to Certicámara's certification services shall have the following rights:

a) To be able to properly use the purchased digital certification service.

b) To inform the trusting third parties that Certicámara is their DCA providing the purchased service.

c) To request the revocation of the digital certification service when required.

d) To request the rectification and/or revocation of the information in accordance with the personal data treatment policy.

e) To receive support from or digital certification services in accordance with the terms and conditions established between the parties.

f) To retract the acquisition of certification services, provided that it complies with the requirements established in the law 1480 of 2011.

g) To revert the payment when it is one of the events determined in decree 587 of 2016.

9.8 Exclusion of warranties

Certicámara shall not be liable for:

a) The veracity of the information provided by the Subscriber or Applicant.

b) Computer Crimes suffered by the subscriber.

c) Fraudulent use of the certified services or CRLs.

d) Damages caused by misinterpretation of the Certification Practices Statement (DPC).

e) Failure to comply with the obligations of the subscriber or applicant.

f) For the content of messages or documents in which digital certification services are used.

g) Due to an act of God or force majeure.

h) Due to the use of the certificates when it exceeds the provisions of the regulations in force, in the DPC and PCs.

9.9 Contract minutes

The contract model used by Certicámara for the provision of the digital signature certificate service consists of two (2) documents, which are available in the following links:

- Términos y condiciones del servicio de certificación de firma digital Certicámara S.A.
- Condiciones generales de contratación del servicio de certificación de firma digital de Certicámara S.A.

On the other hand, the model contract used by Certicámara for the provision of the other accredited services, consists of two (2) documents, which are available at the following links:

- Términos y condiciones de productos, servicios y/o soluciones de Certicámara S.A.
- Condiciones generales de contratación de productos, servicios y/o soluciones de Certicámara S.A.

In case of particular commercial situations with the client, Certicámara and the client may enter into a contract detailing such situations.

9.10 Policy for handling other services

Not applicable.

9.11 Impartiality and non-discrimination

Certicámara recognizes the importance of safeguarding impartiality and independence, in order to prevent conflicts of interest in the internal and external organizational context. For this reason the organization, headed by the Executive Presidency, declares its commitment to ensure compliance with the requirements of independence, impartiality and integrity with respect to all its services, having as main mechanism to ensure impartiality the impartiality management process and the formation of the impartiality committee.

The policy is published in the following link: https://web.certicamara.com/politicas

Certicámara has identified, analyzed and evaluated the risks that may affect the objectivity and impartiality of the digital certification service. For this reason, Certicámara informs the actions taken in order to minimize any situation that may jeopardize the objectivity and impartiality of the provision of its services:

To prevent risks with misleading advertising, our web portal (https://web.certicamara.com/productos_y_servicios) is designed so that our customers and/or subscribers can clearly identify which are our products and/or services accredited by the National Accreditation Body (ONAC).

To prevent risks in the contracting of Datacenter services, our suppliers that provide this service are managed (selection, contracting and evaluation) according to what is established in our supplier management procedure in order to ensure compliance with the admissible technical requirements defined in the specific accreditation criteria.

The policies and procedures under which Certicámara operates, as well as the administration of these, are non-discriminatory. Certicámara does not use procedures that impede or inhibit applicants' access to our services.

Certicámara's digital certification services are accessible to all applicants whose applications are within the scope of its accreditation. This includes the application of the principle of technological neutrality which is recorded in the definitions and conventions of this document.

Access to Certicámara's digital certification services does not depend on any characteristic of the applicant or subscriber other than those defined in the Certification Policy (CP), nor on the membership of any association or group, nor does it depend on the number of certifications already issued. There are no undue conditions, financial or otherwise.

9.12 Policy on Requests, Complaints, Claims, Suggestions and Compliments

If you or any person has any request, complaint, claim, suggestion and/or congratulations regarding any of Certicámara's services or activities, you can come to our headquarters in Bogotá, generate your request through our website, contact our customer service line or write to our email.

- Address: Carrera 7 Nº 26-20 Pisos 18, 19 y 31
- Email: certicamararesponde@certicamara.com
- Telephone number (sales, customer service and technical support): (601) 7442727 Option 3
- National toll-free line 018000181531 - Not valid for cell phones
- PQRSAF System
- Responsible for attention: Business Manager
- Responsible for review and approval: Corporate Relationship Manager

The procedure for Petitions, Complaints, Claims, Requests and Compliments is framed as follows:

Certicámara provides technical support through:

- National Toll Free: 018000181531 - Not valid for cell phones.
- Bogotá Support Line: (601) 7442725 Option 1

The page www.certicamara.com provides:

- Installation instructions
- Technical support through virtual appointment scheduling
- Technical support via email: mesadeayuda@certicamara.com

If explanations are required on the application of the Certification Practice Statement (DPC) or any certification policy (CP) defined in this document for a specific digital certification service, please direct your inquiry to info@certicamara.com.

9.13 Dispute Resolution Provisions

All disputes that may arise between the parties in connection with the execution of the contract, during its execution or its interpretation, will be resolved between the Digital Certificate Holder and Certicámara S.A. In the first instance, by means of conciliation, transaction or amicable composition, for which the non-conforming party will send a written communication duly supported to the other PARTY, who will evaluate the reasons for non-

conformity and will send a response within five (5) working days from the date of receipt (it will be the responsibility of the party sending the communication to ensure that the other party receives the communication sent taking into account security parameters and integrity of the information).

If after the term indicated above, fifteen (15) days elapse and the dispute(s) persist(s), they shall be resolved by an Arbitration Tribunal regardless of the nationality of the holder of the Digital Certificate, which shall be subject to the rules in force on the matter and shall be governed, especially, by the following rules:

a) The Tribunal shall be composed of one (1) arbitrator appointed by THE PARTIES by mutual agreement. If this is not possible, the appointment shall be delegated to the Director of the Arbitration and Conciliation Center established by Certicámara S.A. At the time of accepting his appointment, the arbitrator shall state in writing to THE PARTIES his independence and impartiality to act as arbitrator of the controversy.

b) The arbitrator must be a Colombian lawyer, registered in the lists of arbitrators of the Arbitration and Conciliation Center.

c) The internal organization of the Tribunal shall be subject to the rules provided for such purpose by the Arbitration and Conciliation Center, in all matters not regulated in this clause.

d) The Tribunal shall operate in the city of Bogotá, at the Arbitration and Conciliation Center.

e) The Tribunal shall decide in law and its decision shall have the effect of res judicata of last instance and, consequently, shall be final and binding for THE PARTIES.

f) The costs incurred on the occasion of the convening of the Tribunal shall be borne by the losing PARTY.

g) The applicable regulations shall be those of Colombia.

9.14 Applicable Law

From Certicámara has identified the following regulations that are within the scope of the provision of accredited services in compliance with:

- Single Decree of the Commerce, Industry and Tourism Sector - DURSCIT, 1074 of 2015.
- Law 527 of 1999

- Decree 019 of 2012
- Decree 620 of 2020
- Law 2106 of 2019
- Law 1581 of 2012
- Law 1898 of 2018
- Decree 333 of 2014
- Law 1341 of 2009
- Decree 1595 of 2015

- **Activity 1.** Issuance of certificates in connection with digital signatures of natural or legal persons.
- **Activity 2.** Issuing certificates on verification regarding alteration between sending and receiving data message and electronic transferable documents.
- **Activity 3.** Issue certificates in relation to the person holding a right or obligation with respect to the documents set forth in subparagraphs f) and g) of Article 26 of Law 527 of 1999.
- **Activity 4.** Offer or facilitate the services for the generation of the data for the creation of certified digital signatures.
- **Activity 6.** Offer or facilitate the services of generation of creation data of electronic signatures.
- **Activity 9.** Any other activity related to the creation, use or use of digital and electronic signatures."

9.15 Certification Policies

The interrelation between this DPC and the Certification Policies applicable to the different types of certification services is based on the fact that:

This DPC is structured based on the recommendations of RFC3647 and establishes the practices adopted by Certicámara for the provision of services accredited by ONAC and contains detailed information on its security system, support, administration and issuance of certificates, as well as on the relationship of trust between the Applicant, Subscriber, Responsible, Suppliers, Bona Fide Third Parties and the DCA.

The Certification Policies establish the particular procedures and requirements applicable to the Certification services provided by Certicámara. Each of the Certification Policies defines the requirements for the service request, responsibilities, commercial conditions and in general the conditions for each of the certification services.

CERTIFICATION PRACTICE STATEMENT

Certicámara details the requirements applicable to each of the services in the following Certification Policies:

- PC Digital Certificates
- PC Time Stamping
- PC Associated Information Services

These are available at https://web.certicamara.com/marco_legal.

10. CHANGE CONTROL

Date	Reason for update
12/09/2019	The following adjustments are made to the document: • The names of the positions and areas are updated in accordance with the current organizational structure. • The URL's are updated. • In accordance with the new operating model, the Director of Product Management is responsible for keeping the CPD updated on the web page. Likewise, the Commercial and Marketing Manager and the Director of Product Management are responsible for reviewing and approving changes to the certification practices statement. • The responsibilities and trust roles defined by the organization for the administration and control of the PKI infrastructure are aligned. • In the "Vulnerability Analysis" section, it is clarified that they are managed by a third party that complies with the specific ONAC accreditation criteria through the Administrative and Financial Management. • In the "Auditors" section, it is clarified that, for third party audits, the auditing company must comply with

CERTIFICATION PRACTICE STATEMENT

Date	Reason for update
	the minimum assurance requirements established in the specific accreditation criteria published on ONAC's website. • The table of fees per type of certificate is updated. • The data of Certicámara's physical facilities are updated. • The log management performed by the organization for monitoring and control is updated at a general level. • The requirements for each type of certificate are aligned with those defined internally by the organization. • Change of code and version according to the document structure.
11/06/2020	The following adjustments are made to the document: • The positions responsible for making the adjustments, review and approval of the certification practice statements are updated, in accordance with the changes in the organizational structure. Also, the person responsible for its publication on the web page. • Roles requiring segregation of duties and independent contractor requirements are included.
30/06/2020	The following adjustments are made to the document: • Clarification that the certification policies (CP) are immersed in the chapters of this document of the Certification Practices Statement (DPC), with the objective of facilitating the management and consultation of the information for interested parties. • For the update and/or modification of the Certification Practices Statement (DPC), the procedure established

CERTIFICATION PRACTICE STATEMENT

Date	Reason for update
	by Certicámara will be followed, which includes a first stage of review of the changes and/or adjustments where the impacts are analyzed together with those involved in each management. Subsequently, they are submitted to the Executive President for approval.
02/09/2020	The following adjustments are made to the document: • Clarification on the mechanisms for the delivery of digital certificates, described in numeral 6.1.8. Generation of the subscribers' key pair. Based on the above, the Declaration of certification practices of Centralized Signature Services is deactivated, since it is unified with this document. • Requirements for the issuance request for each certification policy, regarding the subscriber's identification document.
22/10/2020	The document is updated in the following aspects: • Key words and their definition, for a better understanding of the document. • For Colombian citizens of legal age, it is required to attach a copy of the citizenship card in the application for all certification policies mentioned. • In numeral 1.2 "The Cameral Society of Digital Certification Certicámara S.A.", the identification data of the company and the person responsible for the Requests, Inquiries and Complaints of subscribers and users are included. • For modification/update of the information contained in the certificates, the wording is adjusted to provide clarity to the subscriber of the steps to be followed in this regard.

CERTIFICATION PRACTICE STATEMENT

Date	Reason for update
	• As part of numeral 10 of the "Digital Certificate Management Policies" issued by Certicámara, it is clarified that the certificates issued may have a maximum validity of 2 years in accordance with the provisions of CEA-4.1.10. • The following paragraph "Contract Model and Minutes" has been added.
27/10/2020	The document is updated in the following aspects: • Modification of the name of the building where Certicámara is located. • Inclusion of the procedure for the attention of PQRSAF. • Inclusion of the link to consult the certificate of existence and legal representation of the DCA and the DataCenter. • Inclusion of the identification information related to the DataCenter. • Adjustment of the link to the DCA accreditation certificate. • Reference documents and activities of certification bodies that are in the scope of service.
22/02/2021	The document is updated in the following aspects: • Change of the company name of Datcenter Bt Latam to SENCINET LATAM COLOMBIA S.A. • In the glossary, the definition of Registration Authority (RA) is included and the definition of Time Stamping is adjusted. • Redrafting of the business continuity plan for greater clarity.

CERTIFICATION PRACTICE STATEMENT

Date	Reason for update
	• Adjustment in the policies of the types of digital certificates. • Inclusion of Annex 1 where the information available in the different digital certificates is described. • Update of tariffs.
22/09/2021	The document is updated in the following aspects: • Code and contact number for administrative issues of Certicámara. • In numeral 1.5.1 Certification Authority Root CA and Subordinate Certification Authorities, the serial and hash of the certificate of the Root CA and the Subordinate CA respectively are included. • In numeral 4.1 Request for certificates, it is included that Certicámara will consult the necessary databases to comply with SAGRILAFT. • In numeral 4.6.1 Use of Root and Subordinate CA key, the uses of the key are updated according to those declared in the digital certificate. • Clarification "Certicámara annually to ensure the construction of the keys, will take the recommendations given by: https://csrc.nist.gov/projects/hash-functions ". • Update of tariff for digital certificates in physical token with validity of two (2) years. • Adjustment in the stages and channels of communication in the Procedure for handling Petitions, Complaints, Claims, Suggestions, Appeals and Compliments.

CERTIFICATION PRACTICE STATEMENT

Date	Reason for update
	• In Annex 1 - Digital Certificates, the OID's Email Address (E) is eliminated. • Updating of the names of responsible positions according to the new organizational structure. • Adjustment in the wording so that the information is clearer for the user and subscriber.
12/05/2022	The document is updated in the following aspects: • Redaction of the description of the Civil Service policy, in order to provide a better understanding of its application. • In the policy for natural persons, the guidelines for legal persons are incorporated in accordance with the accreditation of the service by ONAC. • Inclusion of the OIDs of the legal entity policy. • Updating of fees for 2022.
01/09/2022	• In the framework of compliance with the provisions of Chapter 48 of DURSCIT, Article 2.2.2.48.3.1. Certification Practices Statement (DPC) and the RFC 3647 standard, the paragraphs are aligned with the provisions of these documents and the wording is adjusted to provide greater clarity to the applicant and subscriber on the provisions, information, guidelines, controls and others applicable to the services accredited before the National Accreditation Body of Colombia ONAC. Based on the above, a transversal DPC and independent certification policies (CP) are defined for the services: digital signature certificate, time stamping and associated services, which are published on the website in the same section.

CERTIFICATION PRACTICE STATEMENT

Date	Reason for update
22/09/2022	In numeral 1.1 Identification of the digital certification entity, the positions responsible for: • Reception of requests, queries and complaints from subscribers and users. • Review and approval of responses to requests, inquiries and complaints from subscribers and users.
29/09/2022	In numeral 4.9.6 Availability of online status verification/revocation, it is included that Certicámara has the history of revoked certificates since the beginning of the service provision.
16/02/2023	Section 4.10 is included for the definition of the replacement of digital signature certificates, where it is clarified that a new certificate must be generated and the conditions that the subscriber must take into account for its management.
21/07/2023	The document is updated in the following aspects: • Inclusion of the numerals: 4.5 Withdrawal and 4.6 Non refund of money, in order to make known to applicants and subscribers the conditions to be taken into account for each of these issues. • Update of the URLs of the new 4026 distribution points for the list of revoked CRL certificates.
18/09/2023	The document is updated in the following aspects: • Inclusion of definitions: Declination of the application, denial of the application and recommendation for decision. • Updating of the concepts declination and denial of the application in the numeral "4.1 Application for the

CERTIFICATION PRACTICE STATEMENT

Date	Reason for update
	certificate". Likewise, the language of the documents submitted by the applicant is clarified. • In section "4.10.1 Grounds for reinstatement", the guidelines to be taken into account for the management of this type of requests are clarified. • Clarification in item "5.2.4 Roles that require separation of functions" regarding the functions performed by the Registration Authority (RA) and Certification Authority (CA) in accordance with the Specific Accreditation Criteria - CEA, are carried out by personnel directly linked to Certicámara S.A. • Inclusion in item "9.1.3 Refund Policy" of the authorized channel to request the refund and reversal of payment through the website of Certicámara S.A. PQRSAF section or payment reversal tab. • In the numeral "9.11 Impartiality and non-discrimination" clarity is given on the policies and procedures related to non-discrimination and the application of the principle of technological neutrality.
15/01/2024	The following changes are made to the document: • In the numeral *"1.3.5 Other participants, service providers"*, the providers for the provision of the Datacenter service are updated. • In item *"3.2 Identity validation mechanisms",* the identity verification from the web portal is included when the applicant submits its request. • Inclusion in section *"4.1 Certificate application"* of the full, unreserved and complete acceptance of the Terms and Conditions of the service, as well as the Declarations and Commitments regarding the prevention of money laundering, financing of terrorism,

CERTIFICATION PRACTICE STATEMENT

Date	Reason for update
	financing of the proliferation of weapons of mass destruction, corruption and transnational bribery. • Clarification in section *"4.8.1 Renewal times"* that the issuance of a new digital certificate implies prior acceptance of the Terms and Conditions of the service, the Declarations and Commitments regarding the prevention of money laundering, financing of terrorism financing, financing of the proliferation of weapons of mass destruction, corruption and transnational bribery and the validation of identity in the registration of a new application.
18/03/2024	The following changes are made to the document: • Elimination of the Certified Digitalization service for evidentiary purposes from the scope of accredited services. • In numeral 4.1 certificate request, it is clarified that identity validation is part of the requirements to be met by the subscriber. • Updating of links according to changes in the web page.
26/04/2024	• Clarification of the general contracting conditions for digital certification services in item 9.9 Contract minutes.
09/09/2024	The following changes are made to the document: • Updating of the delivery management times of digital certificates in physical media. • Clarification on the replacement in case of error attributable to Certicámara. • Adjustment of the channels of attention for technical support.

CERTIFICATION PRACTICE STATEMENT

Date	Reason for update
	• Update of the key length 4096 bits in the issuance of digital certificates. • Inclusion of the cause of revocation due to termination of the labor contract or contractual relationship of the subscriber. • Inclusion of policies: Digital certificate for natural person PKCS#10 and Digital certificate for legal person PKCS#10.