Código:	DYD-L-003
Fecha:	26/09/2025
Versión:	021
Etiquetado:	PÚBLICO

CERTIFICATION PRACTICE STATEMENT

Certification Practices Statement

Code: DYD-L-003

Date: September 2025

Version: 020

CERTIFICATION PRACTICE STATEMENT

Content

CERTIFICATION PRACTICE STATEMENT

1. INTRODUCTION

This Statement of Certification Practices (SCP) is the public declaration of the Open Digital Certification Entity, which establishes the rules and practices adopted by the Certification Authority for the provision of digital certification services. This is done in accordance with Law 527 of 1999 and its compiling and modifying decrees (Decree 1074 of 2015, Decree 620 of 2020), as well as with Law 2106 of 2019, Law 1581 of 2012, Law 1898 of 2018 (Article 13.10) and Decree Law 019 of 2012 (particularly the activities of Article 161).

This document details the practices for the accredited services offered by the Sociedad Cameral de Certificación Digital Certicámara S.A.: Digital signature certificate, Chronological Timestamp, Certified Biometric Fingerprint, Certified Electronic Mail, Digital Signature Generation, and Certified Electronic Signature Generation. The SCP is intended for natural and legal persons who request or use digital certification services, as well as for third parties who rely on their legal and evidentiary validity in the different contexts of their application.

This document has been structured in accordance with the RFC 3647 standard.

1.1 Identification of the Digital Certification Entity

Sociedad Cameral de Certificación Digital Certicámara S.A. (hereinafter, Certicámara) is a limited company constituted by the Chambers of Commerce of Bogotá, Medellín, Cali, Bucaramanga, Cúcuta, Aburrá Sur, and Confecámaras, in order to offer digital certification services. Certicámara, a subsidiary of the Bogotá Chamber of Commerce, operates as an Open Digital Certification Entity, acting as a trusted third party for the security of electronic products and services. Its main purpose is to provide entrepreneurs and Internet users in the country with the necessary tools to conduct electronic business with legal certainty.

Name	Sociedad Cameral de Certificación Digital Certicámara S.A.
NIT	830.084.433-7
Commercial registration	1079279
Certificate of existence and legal representation	https://web.certicamara.com/nosotros
Main domicile	Bogotá
Address	Carrera 7 N° 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	Directorate of Continuous Improvement
Responsible for receiving requests, queries and complaints from subscribers and users	Directorate of Continuous Improvement
Responsible for the review and approval of responses to requests, inquiries and complaints from subscribers and users	certicamararesponde@certicamara.com
PQRS Email	www.certicamara.com
WEB Address	16-ECD-002
Accreditation Certificate No.	https://onac.org.co/certificados/16-ECD-002.pdf

1.2 Document Name and Identification

Certicámara provides the following information for this document regarding its various services:

Name	Certification Practices Statement - DPC
Date of publication	26/09/2025
Version	021
Code	DYD-L-003
Location	https://web.certicamara.com/marco-normativo

Note: If you need to consult a previous version of this document, you must request it by sending an email to info@certicamara.com for your request to be addressed.

1.3 PKI Participants

1.3.1 Certification authorities

It is 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, or the relying third parties.

Certicámara has the following CA:

Root CA (AC Raíz): The Root CA is the original Certification Authority of the digital certification hierarchy. This Certicámara component is responsible for the issuance of digital certificates that accredit its issuance platform.

The structure of its data is:

- Root CA Key: 4096 bits
- Valid until May 24, 2031, 01:39:46 pm
- Version: V3
- Certificate Serial Number: Unique identifier of the certificate. Less than 32 hexadecimal characters.
- Certificate Signature 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 Of ed 25 57 44 9f f2 fd Oe 5e 14

Subordinate Certifiers

In the Colombian regulatory framework, these are derived from the Root CA hierarchy, where the Root CA is required to sign their certificate so that they in turn can issue certificates to final subscribers, continuing with the chain of trust from the Certicámara root point, as an Open Digital Certification Entity accredited by ONAC under Accreditation Certificate number 16-ECD-002. For all CAs belonging to Certicámara's public key infrastructure, what is expressed in the SCP is applicable and consistent with the general requirements established by the legal framework described in the section on normative references. The data structure of the certificate for subordinate authorities is:

- Root Certificate Field
- Root Certificate Value
- Root CA Key: 4096 bits
- Valid until May 24, 2031, 1:39:46 PM
- Version: V3
- Certificate Serial Number
- Unique certificate identifier. Less than 32 hexadecimal characters.
- Certificate Signature Algorithm: SHA256 with RSA Encryption

- 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

Timestamp Authority

The "Chronological Timestamp" is provided by Certicámara in a secure and appropriate electronic format defined so that it is incorporated into the data message generated, transmitted, or received by the subscriber, preventing its subsequent alteration. The "chronological timestamp" of a data message is unique to it and cannot be incorporated into a different data message or messages. The timestamp service is located at the following URL http://tsa.certicamara.com:9233/ donde el suscriptor deberá tener un usuario y contraseña para hacer consumo del servicio respectivo.

where the subscriber must have a username and password to consume the respective service. This is explained as follows: (i) A user wants to obtain a timestamp for an electronic document they own. (ii) A digital summary (technically a hash) is generated for the document on the device that requests the timestamp. (iii) This summary forms the request that is sent to the certification entity that provides the chronological timestamp service. (iv) The certification entity that provides the chronological timestamp service generates a timestamp (or chronological stamp) with this digital summary, the date and time obtained from a reliable source, and the digital signature. In this way, by chronologically stamping this summarized representation of the document, what is really being done is sealing the original document. (v) The timestamp is sent back to the user. And (vi) The certification entity that provides the chronological timestamp services keeps a record of the stamps issued for future verification. The structure of the Digital Timestamp Service TSA (Time Stamp Authority) is described in the RFC 3628 document and the TSP (Time-Stamp Protocol) in RFC 3161.

1.3.2 Registration Authorities

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

Certicámara's registration authority is composed of:

- **RA Software**: It facilitates the registration of requests and allows the management of the certification request lifecycle.
- **RA Agents**: RA users with privileges. They are responsible for reviewing and validating the information contained in the documents submitted by the applicant for the issuance of an ECD service.
- **RA Administrator**: The person responsible for administering and configuring the RA.

- **System Auditor**: This is the person in charge of auditing the compliance of the RA's procedures and systems, validating that what is established in the Statement of Certification Practices (SCP) and Certification Policies (CP) is met.

1.3.3 Subscribers

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

1.3.4 Relying Parties

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

1.3.5 Other Participants

a. Service Providers

The critical suppliers selected for the provision of the Datacenter service meet the minimum requirements established in the Specific Accreditation Criteria CEA 3.0-7 document, available on the ONAC website. Therefore, they will be required to comply with the detailed requirements in said document in the cases that apply.

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.Certicámara.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 uses of the certificate

The root digital certificate can only be used for the identification of the root certification authority itself and for the secure distribution of its public key. The use of certificates issued by the root CA will be limited to the signing of digital certificates and the signing of the corresponding revoked certificate lists.

General uses applicable to digital certificates issued by Certicámara:

a) The subscriber can only give digital certificates the uses that are specified in the contract they sign with Certicámara individually, those permitted in this Statement of Certification Practices, in the Certification Policies, and those permitted by virtue of Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014). The contract celebrated with the subscriber may limit the scope of the 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 given to it will be considered a violation of this Statement of Certification Practices and Certification Policies and will constitute a reason for the revocation of the digital certificate and the termination of the contract with the subscriber, without prejudice to the criminal or civil actions that may arise.

b) b) The subscriber considers and accepts that the products and services that are advertised are as they are offered individually, that digital certificates mainly certify the identity of the natural person who appears as the subscriber of the service, that there is no implicit information that implies additional services or benefits to those expressly mentioned, and that their use is their exclusive responsibility, taking into account the provisions of Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014).

c) c) The use of the digital certificate and the data messages that are digitally signed with it, including monetary electronic transactions, regardless of their amount, are the TOTAL responsibility of the corresponding subscriber and, therefore, Certicámara has no responsibility for the verification or public faith of the signed data messages, as it does not know or have a legal obligation to know the digitally signed messages or the amount of the transactions that are carried out with the digital certificate in third-party electronic transaction systems. In general, Certicámara, as an Open Digital Certification entity and a Trusted Third Party, does not compromise its responsibility for the use that the subscriber makes of the digital signature certificates, therefore, there are no applicable financial limits in this regard. To this end, the subscriber must comply with their duties provided in Law 527 of 1999 and Decree 1074 of 2015 (which compiles

Decree 333 of 2014), and must also assume the burden of responsibility that these regulations impose on them.

1.4.2 Prohibited uses of the certificate

a) Digital certificates may not be used under any circumstances for illicit purposes or operations under any legal regime in the world.
b) b) Any use of 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 Statement of certification practices and in the contracts signed between Certicámara and the Subscriber is strictly prohibited.
c) c) Any use of digital certificates whose purpose is to violate any intellectual property right of Certicámara or third parties is prohibited.
d) d) The physical medium of the digital certificate supplied by Certicámara (if applicable) can only be used within the context of the Digital Certification System. Information other than that expressly authorized by Certicámara may not be incorporated into the supplied physical medium, nor may it be used outside the Digital Certification System

1.5 Policy Administration

1.5.1 Organization that administers the document

All the information contained in this Statement of Certification Practices (SCP) and Certification Policies (CP) is the intellectual property of Certicámara, and its administration is carried out in accordance with the guidelines established internally.

1.5.2 Contact Person

Within Certicámara, it has been established that the contact person for matters related to this Statement of Certification Practices (SCP) and Certification Policies (CP) is the Product Director.

Name	Angela Vivina Leandro Hernandez
Position	Director of Continuous Improvement
Email	certicamararesponde@certicamara.com
Telephone	(601) 9157808
Address	Carrera 7 N° 26-20 Piso 18

1.5.3 Procedure for updating and approving the SCP

The updating of the Statement of Certification Practices will be carried out when required by legal, regulatory, and/or other requirements applicable to the accredited services. In this process, the heads of the various areas involved in providing the services within the scope will meet to evaluate the modifications to be made. The final approval of said changes is given by the President. The responsibility for managing the update of the SCP on the Certicámara website, specifically the link https://web.certicamara.com/marco-normativo, corresponds to the Director of Continuous Improvement.

1.6 Definitions and acronyms

- **Algorithm**: A prescribed set of well-defined, ordered, and finite instructions or rules that allows an activity to be carried out through successive steps that do not generate doubts for the person who must perform said activity. Given an initial state and following the successive steps, a final state is reached, and a solution is obtained.
- **Certification Authority (CA)**: A trusted entity, responsible for issuing and revoking certificates.
- **Time Stamp Authority (TSA)**: Time Stamp Authority.
- **Validation Authority (VA)**: A trusted entity that provides information on the validity of digital certificates.
- **Root CA**: First-level certification authority, the basis of trust.
- **Subordinate CA**: Second-level or multi-level certification authority.
- **Digital Certificate**: An electronic data message signed by the digital certification entity, which identifies both the certification entity that issues it and the subscriber and contains the latter's public key.
- **Client**: In digital certification services, the term client identifies the natural or legal person with whom the ECD establishes a commercial relationship.
- **Signature Creation Data (Private Key)**: These are unique numerical values that, used together with a known mathematical procedure, serve to generate the digital signature of a data message.
- **Signature Verification Data (Public Key)**: These are data, such as public cryptographic codes or keys, that are used to verify that a digital signature was generated with the subscriber's private key.
- **Statement of Certification Practices (SCP)**: A statement of certification practices. An official document presented by the Digital Certification Entity, in which it defines the rules and practices of the Certification Authority for the provision of digital certification services.
- **Service Request Refusal**: 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 opportunity for the user to remedy the situation.

- **Open Certification Entity**: One that offers services typical of ECDs to the general public, such that: their use is not limited to the exchange of messages between the entity and the subscriber, and they receive remuneration.
- **Digital Certification Entity (ECD)**: It is that person who, authorized in accordance with this law, is empowered to issue certificates in relation to the digital signatures of people, offer or facilitate the services of registration and chronological timestamping of the transmission and reception of data messages, as well as perform other functions related to communications based on digital signatures.
- **Chronological Timestamp (Time Stamping)**: A data message digitally signed and timestamped by a TSA that links another data message with a specific point in time, which allows establishing with evidence that this data existed at that time and that it did not undergo any modification from the moment the timestamp was made.
- **ETSI**: European Telecommunications Standards Institute.
- **FIPS**: Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in wider communities (ANSI, IEEE, ISO, etc.).
- **Digital Signature**: It will be understood as a numerical value that is attached to a data message and that, using a known mathematical procedure, linked to the initiator's key and the text of the message, allows determining that this value has been obtained exclusively with the initiator's key and that the initial message has not been modified after the transformation was performed.
- **Electronic Signature**: When any regulation requires the presence of a signature or establishes certain consequences in the absence of it, in relation to a data message, said requirement will be understood as satisfied if: a) A method has been used that allows the initiator of a data message to be identified and to indicate that the content has their approval . b) The method is both reliable and appropriate for the purpose for which the message was generated or communicated.
- **HASH Function**: It is an operation that is performed on a set of data of any size, so that the result obtained is another set of data of a fixed size, regardless of the original size, and that has the property of being uniquely associated with the initial data.
- **HSM**: Hardware Security Module.
- **LDAP**: Lightweight Directory Access Protocol.
- **Certificate Revocation List (CRL)**: It is that list of digital certificates that have been revoked by the Certification Authority (CA), which have not met their scheduled expiration date and which should no longer be trusted.
- **Log**: Event logging service of the information system, leaving the previous and current information, it identifies who and when the event was performed.

- **Service Request Denial**: A digital certification service will be denied for reasons unrelated to Certicámara S.A., and which are the user's responsibility, as long as they can be remedied by the latter.
- **Technological Neutrality**: Principle of non-discrimination between information recorded on paper and information communicated or archived 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 archive information electronically.
- **OID**: Unique object identifier (Object Identifier). OID, an acronym for the English term "Object Identifier", which consists of a unique identification number assigned based on 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 Infrastructure)**: It is the set of hardware, software, policies, procedures, and technological elements that, by using a pair of cryptographic keys, a private one that only the service subscriber possesses and a public one, which is included in the digital certificate.
- **Certificate Policies (CP)**: 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, regulatory, and common security requirements.
- **Recommendation for the Decision**: Communication issued by the Registration Authority (RA) to the Certification Authority (CA), to approve the request for service provision to the applicant by Certicámara S.A..
- **Revocation**: For this document, it is the process by which the issued digital certificate is disabled and its period of validity of use is terminated from the date of revocation. When any of the causes established in the statement of certification practices occurs.
- **Digital Certification Service**: A set of certification activities offered by the ECD to certify the origin and integrity of data messages, based on digital or electronic signatures, timestamping, as well as on the applicability of technical standards admitted and in force in public key infrastructure - PKI.
- **Online Certificate Status Service OCSP**: Real-time consultation activity with the ECD system, on the status of a digital certificate through the OCSP protocol.
- **Applicant**: A natural or legal person who, for the purpose of obtaining digital certification services from an ECD, demonstrates compliance with the requirements established in their SCP and CP, to access the digital certification service.
- **Subscriber**: A natural or legal person in whose name a digital certificate is issued.
- **Token**: A cryptographic hardware device supplied by an ECD, which contains the digital certificate and the subscriber's private key.
- **UpTime**: A commitment in terms of the percentage of available time of an information system, which the company providing it undertakes to offer its client per year.

- **Usability**: It is a term from English "Usability", 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 the list of revoked certificates CRL will be available for consultation 365 days a year, 24 hours a day, 7 days a week. This service will be provided with a 99.8% availability agreement, and in case of interruption due to force majeure, the service will be restored within the time established according to the availability percentage. For the PKI, an availability of 99.8% is established.

2.2 Publication of Certification Information

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

- WEB:
  Certicámara S.A. Root CA.
  http://www.certicamara.com/repositoriorevocaciones/ac_offline_raiz_certicamara_.cer

- Certicámara S.A. Subordinate CA.
  http://www.certicamara.com/repositoriorevocaciones/ac_online_subordinada_certicamara_.crt
  http://www.certicamara.com/repositoriorevocaciones/ac_online_subordinada4096_certicamara_.crt

b) For the certificate revocation list (CRL):

- WEB:
  - Certicámara S.A. Root CA
    http://www.certicamara.com/repositoriorevocaciones/ac_raiz_certicamara.crl

  - Certicámara S.A. Subordinate CA
    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 SCP:
- WEB: https://web.certicamara.com/marco-normativo

d) For OCSP certificate revocation status verification:
- **o** 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, an OCSP Client that complies with RFC 6960 must be available. If the user does not have this OCSP Client, they 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 certificate will be published before its effective date via the Certicámara website. The validity period is until Saturday, May 24, 2031, 13:39:46.

2.3.2 Certificate Revocation List (CRL)

The publication of the Certificate Revocation List of the Subordinate CA Certicámara S.A. (CRL) is carried out with a validity of three (3) days.

- The publication can be made a maximum of eight (8) hours after the last revocation, at any time of the day.

2.3.3 OCSP certificate revocation status

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

- Every time a digital certificate is revoked.

2.4 Access controls to repositories

Access to the information published by the Root CA will be for consultation only, and its modification will be restricted to authorized personnel. The updating of public information will be carried out exclusively by Certicámara personnel assigned to this function. In addition, consultation of the CRL, the issued certificates, the OCSP server, and the SCP in their previous and updated versions is guaranteed.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

All certificates have a section called Subject whose objective is to allow the identification of the certificate subscriber. 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 type of certificate are established in the certificate issuance policy. Each type of certificate will be identified by a unique OID (Object Identifier), included in the certificate as a policy identifier, within the certificate properties.

OID	Tipo de Política
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 anonymous or pseudonymous names to identify a natural or legal person. In the case of a legal entity or 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 be made up of first and last names as they appear on the recognized identification document. Exceptionally, contractions or abbreviations may be used provided there is prior, express, and written consent from the holder, and that documentary evidence of such authorization is kept.

3.1.4 Rules for interpreting various forms of names

The rules used for the interpretation of distinguished names in the 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 Uniqueness of names

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

3.1.6 Recognition, authentication, and function of trademarks

The ECD does not assume commitments in the issuance of certificates regarding the use by Subscribers of a commercial brand, so the ECD is not obliged to seek evidence of the possession of registered trademarks before the issuance of the certificates. A certificate applicant retains all rights they possess (if any) in any registered trademark, service mark, or trade name contained in any certificate request and distinguished name within any certificate issued to said certificate applicant

3.2 Initial Identity Validation

3.2.1 Method for proving private key possession

The certification system implemented and used by Certicámara for the administration of the lifecycle 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 it, made with the private key corresponding to the public key of the certificate.

3.2.2 Authentication of the organization or person's identity

In the process of authenticating the identity of the organization or person, the applicant will be obliged to provide the relevant documentation for each accredited service. Likewise, the applicant must provide Certicámara with information that is truthful, sufficient, and adequate in compliance with the established requirements.

3.2.3 Verification of representation powers

The verification of the applicant's powers of representation to Certicámara will be carried out by consulting the Unique Business and Social Registry (RUES) or by verifying the legal documents that, in accordance with Colombian legislation, accredit and authorize their role as legal representative.

3.2.4 Identity validation mechanisms

3.2.4.1 Identity Verification

Certicámara, as an Open Digital Certification Entity, will carry out identity verification through the defined mechanisms, using reliable sources and data provided by third parties with whom Certicámara has a current contract for this purpose.

3.2.4.2 Biometric Identity Verification

If required, Certicámara may carry out the validation of the applicant based on the biometric identification provided to ensure that the applicant is who they say they are.

3.2.5 Unverified subscriber information

Certicámara, in its capacity as an Open Digital Certification Entity, verifies the information provided by the applicant that can be supported with probative evidence. Regarding information that lacks documentary support, such as physical address, email, and similar data, the principle of good faith of the applicant will be applied at the time of its submission.

3.2.6 Interoperability criteria

Certicámara, in its capacity as an Open Digital Certification Entity, does not contemplate interoperability with other external ECDs. It only contemplates the issuance of digital certificates with its Subordinate. However, if the need arises, due to commercial and/or regulatory issues, to perform interoperability with another ECD, the different scenarios for its execution must be evaluated, guaranteeing the adequate provision of the service.

3.3 Identification and authentication for key renewal requests

Certicámara does not contemplate the renewal of digital certificates within its processes while maintaining the original key pair of the subscriber. If the renewal of a previously issued certificate is necessary, a new issuance request process must be carried out, which will include the generation of a new key pair.

4. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFECYCLE

4.1 Certificate Request

The request process can be carried out in one of the following ways:

1. In person by going to Certicámara's facilities.
2. Through the Contact Center.
3. Or by any other electronic means that Certicámara has available.

The requests received will be subject to review by the Registration Authority (RA), in accordance with the specific accreditation criteria established by ONAC and those defined internally by Certicámara. Said review will be carried out within a maximum period of two (2) business days, counted from the reception of all the required documents, the proof of payment, and the satisfactory validation of the applicant's identity. Once the review is completed, the requests will be sent to the Certification Authority (CA) for their issuance, which will be carried out within a maximum period of one (1) business day.

In accordance with Certicámara S.A.'s internal policies, all documentation provided by the applicant must be in Spanish. If a document is presented in another language, it must be accompanied by an official translation carried out by a translator endorsed by the Ministry of Foreign Affairs. The documentation will be kept according to Certicámara's document retention schedules. The applicant's information will not be made public without their explicit consent.

By using and electronically subscribing to the digital signature certificate of Certicámara S.A., the applicant fully and without reservations accepts the following documents, which are an integral part of this SCP and the service provision contract: the Terms and Conditions of the service, the Declarations and Commitments on the prevention of LA/FT/FPDAM AND C/ST, the Certification Policy (CP), the processing of personal data, and the organizational policies of Certicámara S.A., available on the Certicámara website.

The Terms and Conditions of the digital signature certification service are applicable from the moment the applicant expresses their interest in acquiring the certificate and remain in force during its validity, together with the general service contracting conditions.

Applicants must take into account the following before requesting any service from Certicámara S.A.:

a) **Reading of Documentation**: Having fully read the Terms and Conditions of the digital signature certification service, the Declarations and Commitments for the prevention of LA/FT/FPDAM AND C/ST, this Statement of Certification Practices (SCP), the Certification Policy (CP), and the personal data processing policy.

b) **Verification of Information**: Verifying the information mentioned by Certicámara S.A. to make an informed decision about the digital signature certificate request, in compliance with Law 527 of 1999, Decree 019 of 2012, Law 1341 of 2009, Law 1978 of 2019, Law 1581 of 2012, Decree 1074 of 2015, Decree 358 of 2020, Decree 1538 of 2020, and Decree 620 of 2020.

c) **Provision of information**: The client must provide updated and available contact information that allows them to be contacted to carry out the processes associated with the issuance of the digital signature, preventing these from having restriction configurations, security filters, or any other additional adjustment or authorization in their domains. The email address and mobile phone number linked to a device provided in the request will be the authorized communication channels for sending notifications associated with the process, therefore, by sending this data, the sending for this purpose is authorized.

d) **Password Assignment**: For the use of the digital certificate, it is necessary for the holder to assign a password. The implications in case of forgetting or losing it are detailed below:

- **Virtual Token**: Password resets may be requested through the contact center at no additional cost up to ten (10) times; after this number of requests, there will be an associated cost.
- **Physical Token**: Because Certicámara S.A. does not have mechanisms for its recovery, since it remains local, it will be essential to acquire a new certificate, which implies an associated cost.

The holder must remember and securely store the password. This password is the exclusive means of accessing the issued certificate.

e) **Technical and Security Knowledge**: Knowing the technological and security requirements for the use of the digital signature certificate. Being informed about the characteristics of the Certicámara S.A. certificate, its level of reliability, the limits of responsibility, the client's obligations, and the necessary security measures for its use.

f) **Right to Non-Provision of the Service**: Keep in mind that Certicámara S.A. may reserve the right not to issue a digital signature certificate due to technical conditions, without this generating any responsibility.

g) **Identity Validation by Certicámara S.A.**: Certicámara S.A., as an Open Digital Certification Entity, will previously carry out identity verification using reliable sources and data provided by third parties with a current contract for this purpose.

h) **Request for Additional Documents**: Certicámara reserves the right to request additional documents or copies of those required in the application form when it deems it necessary to verify the identity or any quality of the applicant. It may also waive the presentation of documents if the applicant's identity has been

sufficiently verified by other means. These additional documents may include (without limitation):

- Commercial references of the company.
- Personal references of the applicant.
- Bank certifications.
- Valid driver's license.
- Military card.
- Document of affiliation to the social security health regime.
- Document of affiliation to the professional risk administrator company.
- Other documents that allow verifying the identity or powers of the subscriber or the entity for the issuance of any type of certificate.

i) **Database Consultation**: Certicámara may consult identity information databases of public or private entities to carry out the necessary validations to issue the digital certificate.

j) **SAGRILAFT Compliance**: It will consult the necessary databases to comply with SAGRILAFT, subject to the applicant's acceptance of the Declarations and Commitments for the prevention of LA/FT/FPDAM AND C/ST, published on the Certicámara S.A. website.

k) **Certificate Validity**: Digital signature certificates will be issued with a maximum validity of two (2) years.

l) **Denial or Refusal of the Request**: Certicámara S.A. may deny the issuance of a digital certificate when it is not within the scope of the accreditation granted by ONAC, due to non-compliance with the law and/or when in its opinion it violates its good name as an ECD. In this case, there will be no opportunity for the user to remedy the situation. If Certicámara decides to deny or refuse the request, it will notify the applicant by email, indicating the reasons.

m) **Development for Mac OS**: Currently, Certicámara is developing the infrastructure for compatibility in the issuance of digital signature certificates for the Mac OS operating system.

4.1.1 Who can submit a certificate request?

A digital certificate request may be made by any natural person in full exercise of their legal capacity, as well as by legal persons through their legal representative, an attorney, an employee, or a duly authorized third party, provided that said capacity is accredited with the documents required by the Registration Authority (RA). In the case of minors, the digital signature request must be submitted by their representative, attaching the minor's identity document and the document that accredits the representation in accordance with current civil regulations.

4.2 Certificate Issuance

4.2.1 CA Actions during certificate issuance

Once the issuance request has been approved, the Certification Authority (CA) proceeds to generate the corresponding certificate, which is associated with a key pair and is digitally signed using the CA's certificate, which is part of the Certicámara trust chain. The issuance of certificates requires the authorization of the request by the Subordinate CA's system. After approval, the certificates are issued securely and made available to the subscriber.

In the issuance process, the Subordinate CA performs the following actions:

- It implements a certificate generation procedure that establishes a secure link between the certificate and the registration information, including the certified public key.
- It guarantees the protection of the confidentiality and integrity of the registration data.
- The validity of all certificates begins once the holder performs the download / activation of the digital signature. Under no circumstances will a certificate be issued with a validity period that precedes the current date.

4.2.2 Notification to the subscriber by the CA of certificate issuance

The subscriber will be notified of the successful issuance of their certificate through an email sent to their registered address.

4.3 Delivery of the digital certificate to subscribers via physical medium

4.3.1 Coverage

The delivery of digital certificates will be carried out in accordance with the coverage matrix of the delivery service of the logistics operator that has a current contract with Certicámara for this purpose, or by direct delivery by a Certicámara logistics team member. In both scenarios, the physical device will be delivered, and the link to the download instructions will be shared in the approval email sent to the holder.

4.3.2 Delivery requirements

The physical device will be delivered by the logistics operator to the reported address or may be picked up by the subscriber at Certicámara's facilities, in accordance with the information indicated in the application form. When the holder authorizes a third party

to collect the device at Certicámara's facilities, they must send an email to logistica@certicamara.com prior to the delivery.

The logistics operator's guide will serve as evidence of receipt of the physical device, and in the case of delivery at Certicámara's facilities, formal delivery documentation will be available.

4.3.3 Delivery management time - Physical Certificates

The estimated delivery times from the issuance of the certificate are:

- **Bogotá and nearby municipalities**: Approximately two (2) business days.
- **Department capitals**: Approximately two (2) to four (4) business days.
- **Other municipalities**: Approximately four (4) to five (5) business days.
- **Special municipalities or destinations**: Approximately six (6) to fifteen (15) business days.

In case of impossibility of delivery, a second attempt will be made. If this also fails, the logistics operator will return the digital certificate to Certicámara's facilities. If the delivery is not possible due to causes attributable to the subscriber, Certicámara or the logistics operator will contact them to coordinate the delivery. However, it is important to note that if a delivery or collection date cannot be coordinated within a period of three (3) months from the date of issuance, the item will be considered abandoned. In this case, Certicámara will proceed to block the download link. If, after this period, the holder requires the digital signature, they must start a new request process, which will generate a cost according to Certicámara's policies.

4.3.4 Download time

Once the digital signature request is approved, the holder will automatically receive an email with the download link, a detailed manual, and important recommendations. The download link will be active for thirty (30) calendar days. After this period, the system will block it for security reasons. To reactivate it, the holder must formally request it and will have two (2) additional months to download their signature. If, after this three (3) month period, they have not downloaded their signature, it will be understood that the item has been abandoned and Certicámara will proceed to definitively block the link. In such a case, if they wish to obtain the digital signature certificate, they must start a new request process, which will generate a cost according to Certicámara's rates

4.4 Certificate Acceptance

A confirmation from the subscriber is not required as acceptance of the received service. It is understood that the digital signature certificate service is accepted from the moment its issuance is requested. Consequently, if the information contained in the service activation communication does not conform to its current status or was not

provided correctly, the subscriber must inform Certicámara through any of the available service channels to carry out the relevant correction procedures if they apply

4.4.1 Publication of the certificate by the CA

The registration authority, through its server, will incorporate the public keys of the digital certificates issued by the subordinate certification authority into the LDAP (Lightweight Directory Access Protocol) directory structure of the PKI at the instant the certificate is issued. In case of any technical difficulty that hinders its publication, it will be carried out within the month following the date of issuance of the certificate, in accordance with the conclusions of the technical analysis that prevented its timely publication.

4.4.2 Notification of certificate issuance by the CA to other entities

Certicámara has an LDAP digital certificate repository, through which entities, government bodies, private sector companies, and other interested parties have the possibility of consulting the issuance of certificates. This repository is accessible at the following web address: https://ar.Certicámara.com:8443/Search/. The information is published in this repository once the certificate has been issued.

4.5 Withdrawal

In the event that the user has made the payment for one of the services offered by Certicámara, but has not completed the delivery of all the required documentary requirements, a period of ninety (90) calendar days is established from the date of the service request for said information to be duly supplied. If the applicant does not complete the required information within the stipulated period, it will be understood that there is a withdrawal from the acquisition of the service. Consequently, the values paid for the service will not be subject to a refund.

4.6 No refund of money

Certicámara will not be obliged to return the money to the applicant in any case, except when the law expressly requires it.

4.7 Use of key pairs and certificates

4.7.1 Generation and installation of key pairs

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

4.7.2 Use of the subscriber's certificate and private key

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

4.7.3 Use of the relying user's certificate and public key

Good faith third parties may only place their trust in the certificates for the purposes defined in this SCP, the CP, and current regulations. Said third parties may carry out public key operations satisfactorily by trusting the certificates issued by the trust chain. However, they must act with diligence and assume the responsibility of verifying the status of the certificates using the mechanisms detailed in this SCP..

4.8 Certificate Renewal

4.8.1 Renewal times

Certicámara will notify its subscribers of the expiration of their digital certificate's validity with a minimum of thirty (30) calendar days' notice. Said notification may be made via email to the address provided by the subscriber or through any other suitable communication means that Certicámara deems convenient. However, it is not an obligation for Certicámara to ensure the effectiveness of the notification about the end of the certificate's validity or to confirm its receipt. It is the subscriber's duty to know the expiration date of their digital certificate and to manage the pertinent procedures with Certicámara for the issuance of a new signature. Renewal will be understood as the issuance of a new digital certificate, which involves the registration of a renewed request, the applicant's acceptance of the Terms and Conditions of Certicámara S.A.'s digital signature certification service, the Declarations and Commitments regarding the prevention of LA/FT/FPDAM AND C/ST, the prior validation of identity, and the generation of a new key pair.

4.8.2 Who can request renewal?

Subscribers can request the renewal of their certificate when it is about to expire and they wish to continue using a digital certificate that accredits the same conditions approved in the current certificate.

4.8.3 Processing of certificate renewal requests

For the purpose of renewing a certificate, the subscriber must undergo the identity validation process again. Consequently, the request procedure for renewing a certificate is identical to the first-time issuance, with the exception that no documents will be required to be attached to the request, unless they have expired (if applicable).

4.8.4 Notification of new certificate issuance to the subscriber

The effective issuance of the new certificate will be communicated to the subscriber through an email sent to the address they have provided.

4.9 Certificate Key Renewal

Certicámara does not contemplate the renewal of the key pair within the lifecycle of its certificates. In all cases, the issuance of a certificate implies the generation of a new key pair.

4.10 Certificate Modification

During the validity of a certificate, the modification or updating of the information it contains is not allowed. If any data on the issued certificate needs to be changed, it will be necessary to revoke the current certificate and request the issuance of a new one with the correct data and pay the corresponding value.

4.11 Certificate Revocation

The revocation of a digital certificate constitutes the mechanism by which an issued certificate is disabled, ending its period of validity, either by the expiration of its term or upon the occurrence of any of the revocation events stipulated in this Statement of Certification Practices. It should be clarified that revocation has no associated cost. Certicámara does not handle the suspension status for its digital certificates.

4.11.1 Reasons for revocation

Certicámara revocará el certificado digital de conformidad con el artículo 37 de la Ley 527 de 1999, cuando tenga conocimiento de que se ha producido alguno de los siguientes hechos:

a) Certicámara will 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:

b) Due to a security compromise for any reason, mode, situation, or circumstance.

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

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

e) Due to the death of the subscriber.

f) Due to the subsequent incapacity of the subscriber.

g) Due to the liquidation of the represented legal person that appears on the digital certificate.

h) Due to the updating of the information contained in the digital certificate.Due to the confirmation that some information or fact contained in the digital certificate is false, as well as the occurrence of new facts that cause the original data not to conform to reality.

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

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

k) By judicial order or from a competent administrative entity.

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

m) Due to the termination of the subscription contract, in accordance with the causes established in the contract and in this Statement of Certification Practices.

n) For any reason that reasonably leads to the belief that the certification service has been compromised to the point where the reliability of the digital certificate is questioned.

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

p) Due to the non-compliance of the subscriber or the legal person they represent or are linked to through the Digital Certification service Contract provided by Certicámara.

q) Due to a past-due portfolio report caused by the non-payment of the services that Certicámara is providing.

r) Due to events in which the delivery of the certificate is not possible for a reason associated with the subscriber.

s) Due to causes associated with Certicámara and/or the logistics operator.

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

u) Due to the termination of the subscriber's labor or contractual relationship with the entity for which the digital signature certificate was issued.

4.11.2 Who can request revocation?

The subscriber is empowered to request the voluntary revocation of their digital certificate at any time. Said request may be submitted directly or through a duly authorized third party. The digital certificate revocation procedure will not generate any cost.

Certicámara may also process the revocation of a certificate if it becomes aware of or has a founded suspicion of a compromise of the subscriber's private key, or any other determining event that makes the revocation of the certificate imperative. In those cases where the revocation is attributable to reasons inherent to Certicámara, a new certificate will be issued to the subscriber under the same conditions and for the remaining term of validity. For this purpose, the documentation previously supplied will be used, in order not to affect the availability of the service.

4.11.3 Procedure for requesting revocation

Certicámara has provided the following means to receive revocation requests:

- **By phone**: By calling the service line (601) 7442727, from Monday to Friday from 7:00 a.m. to 6:00 p.m. and Saturdays from 8:00 a.m. to 1:00 p.m..
- **Online**: Through the Certicámara website, by registering the request at the following URL: https://ventadigital.certicamara.com/revocar-certificado

If it deems it necessary, Certicámara will carry out pertinent inquiries, verifications, and procedures, personally or through third parties, to verify the existence of the invoked revocation cause. These procedures may include direct communication with the subscriber and the physical presence of the third party who invokes the cause. Certicámara will validate the identity of the subscriber who invokes the revocation cause. If the person who presents said is not the subscriber or in case they are, they cannot be satisfactorily identified, they can go in person to Certicámara's offices during office hours from 08:00 a.m. to 05:00 p.m. from Monday to Friday, with proof of the existence of the respective revocation cause for the cases in which it applies, without prejudice to Certicámara providing the measures that are established for the security of the Digital Certification System. It is clarified that once the revocation request is received and the veracity of said request is verified, the certificate will be revoked, without grace periods for said revocations. In cases where revocation is requested due to the termination of the subscriber's labor or contractual relationship with the entity for which the digital signature certificate was issued, Certicámara will request a certification from the person in charge or responsible for the entity stating the end of the labor relationship. If the cause is proven, Certicámara will incorporate the digital signature certificate into the database of revoked digital certificates as a revoked digital certificate.

Otherwise, it will terminate the digital certificate revocation process. It is clarified that Certicámara does not offer the suspension service for certificates to subscribers.

4.11.4 Revocation request grace period

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

4.11.5 CRL issuance frequency

The publication of the Certificate Revocation List of the Subordinate CA Certicámara (CRL) and CA SUB CERTICÁMARA (CRL) is carried out with a validity of three (3) days:

- Periodically
- The publication can be carried out a maximum of eight (8) hours after the last revocation, at any time of the day.

4.11.6 Online status/revocation verification availability

The certificate revocation lists (CRL) and the online certificate status validation service (OCSP) will be available for consultation 365 days a year, 24 hours a day, 7 days a week. This service will be provided with a 99.8% availability agreement. Certicámara has the history of revoked certificates since the beginning of the service provision.

4.11.7 Online revocation verification requirements

The verification of the online certificate status must be carried out using the OCSP service in accordance with RFC 6960. By using this 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 consulting its database, provides a response about the certificate status via HTTP through the addresses http://ocsp.certicamara.com, http://ocsp.certicamara.co y http://ocsp4096.certicamara.co

4.11.8 Suspension circumstances

Certicámara does not consider the temporary suspension of certificates within their lifecycle; in all cases, a revoked certificate cannot be reactivated again.

4.12 Replacement of Digital Signature Certificates

erticámara establishes that the replacement of a digital certificate consists of generating a new certificate, in accordance with what is defined in the lifecycle of this Statement of Certification Practices, 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 conditions:

- The validity of the digital certificate must be equal to or greater than one (1) year.

- Replacements will not be made for digital certificates that are less than ninety (90) days from their expiration.
- The same certification policy with which it was initially issued must be maintained.
- The digital signature certificate will be replaced for the remaining time of its validity.

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

To manage the replacement of digital signature certificates, the following requirements must be met:

- The subscriber must generate the request on the Certicámara website: https://web.certicamara.com/soporte_tecnico, under the replacement project.
- The generation of the new signature must be done according to the content of numeral 4.2 of this Statement of Certification Practices.
- The subscriber must revoke the digital signature certificate. To do this, they will have two possibilities:

    i. The corresponding form must be sent—by the holder of the digital signature certificate, or an authorized third party—where they authorize the revocation of the digital Certificate to the email revocaciones@certicamara.com. The form can be requested by communicating with 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, the personal process can be carried out: https://ventadigital.certicamara.com/revocar-certificado

Additionally, there are exceptional cases, where commercial agreements establish Certicámara's obligation to maintain custody and manage quotas. In this scenario, a communication from the supervisor and/or contract administrator is required, in which the replacement of certificates is requested and justified under one of the following causes:

- 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 the email revocaciones@certicamara.com, where the certificate that must be the object of the replacement 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 Reasons for Replacement

For each of the reasons set forth below, an internal analysis will be carried out by this company and the validity of the replacement will be determined, in accordance with the defined procedure. Certicámara will carry out the replacement of the digital signature certificate in accordance with the previous numeral, when any of the following reasons occur:

a) Loss of the physical device.
b) Exposure of the PIN (Password/key) of the digital certificate.
c) Change in the information of the previously issued digital certificate (Does not apply to a change in identification number).
d) Change in the company's corporate name regardless of whether it keeps the same NIT.
e) Due to an error attributable to Certicámara

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

i. Due to the death of the subscriber.
ii. Due to the subsequent incapacity of the subscriber.
iii. Due to the updating of the information contained in the digital certificate.
iv. Due to the loss, uselessness, or compromise of the security of the physical medium 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 subscriber to generate a new request and under the same conditions initially agreed upon

4.13 Characteristics of certificates

4.13.1 Operational characteristics

For the validation of digital certificates, several Validation Service providers are available that 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. Through the use of this 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

consulting its database, provides a response about the certificate status via HTTP through the addresses http://ocsp.Certicamara.com, http://ocsp.Certicamara.co y http://ocsp4096.certicamara.co.

The corresponding CRL files for 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=crl

4.13.2 Service availability

The certificate status checking service is available 24 hours a day, 365 days a year, and the minimum availability level will be 99.8%

4.13.3 Optional functions

To use the online validation service by consulting the addresses http://ocsp.Certicamara.com; http://ocsp.Certicamara.co and http://ocsp4096.certicamara.co, it is the responsibility of the good faith third party to have an OCSP Client that complies with RFC 6960..

4.14 End of subscription

The end of a certificate subscription occurs in the following cases:

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

4.15 Key custody and recovery

4.15.1 Key custody and recovery policy and practices

The private key of the root CA is kept in custody by a cryptographic HSM device. To access the private key repository, the Shamir threshold scheme (k, n) is used both in software and in 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 the Subordinate CA are physically protected by the implementation of rigorous security measures and an uninterrupted surveillance scheme 24 hours a day, 7 days a week. Said systems operate independently of other Certicámara systems, restricting access exclusively to duly authorized personnel.

5.1.2 Physical access

Certicámara has services and technologies that complement the physical access controls to both its racks and its Datacenter, where they normally must pass at least three (03) controls. 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, extinguishers, personnel training to act in case of fire, etc..
- The facilities are located away from smoke outlets.
- Video and/or photographic captures.

5.1.3 Power and air conditioning

The facilities where the equipment is located comply with the power and ventilation conditions required to prevent interruptions in the electrical supply or other electrical anomalies. The equipment wiring is protected to avoid interceptions or physical damage. Additionally, specific measures have been adopted to mitigate the loss of information caused by the interruption of the electrical supply, by connecting the essential components to UPS systems that guarantee a continuous electrical supply with sufficient capacity to support the electrical network during controlled system shutdown procedures and to safeguard the equipment from electrical fluctuations that could compromise its integrity. The air conditioning systems maintain the spaces where the equipment is located with optimal humidity and temperature levels for its proper functioning and preservation.

5.1.4 Water exposures

The facilities of the Root CA and the Subordinate CA are protected to prevent exposure to water, through the implementation of humidity and flood detectors and other security mechanisms appropriate to the environment.

5.1.5 Fire prevention and protection

The installation of the Root CA and Subordinate CA has an intelligent detection and extinguishing system. It is made up of:

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

5.1.6 Media storage

The information related to the infrastructure of the root CA and Subordinate CA is stored securely in fireproof cabinets and safes, according to the classification of the information contained in them. This information is housed in sites with different locations, in order to minimize associated risks

5.1.7 Waste disposal

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

5.1.8 Off-site backup

All backups are stored in entities distant from the Root CA and Subordinate CA. These dependencies are protected with security means and mechanisms, adhering to good international security practices.

5.2 Procedural controls

5.2.1 Trusted roles

The Root CA and the Subordinate CA have personnel who, due to their essential responsibilities for the functioning of Certicámara S.A., are subjected to special control procedures and are considered trusted roles:

- **RA Agent**: Responsible for reviewing and validating the information in the applicant's documents for the issuance of ECD services.

- **CA Agent**: Responsible for the approval, activation, and revocation of ECD services.
- **PKI/TSA Infrastructure Specialist**: Responsible for the functioning of the systems (hardware and base software) of the root CA and Subordinate CA.
- **System Auditor**: The Director of Continuous Improvement is internally responsible for the audit management process, establishing the guidelines to evaluate compliance with the applicable requirements through a specialized third party.

5.2.2 Number of people required per task

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

5.2.3 Identification and authentication for each role

The collaborators assigned to each role have the necessary permissions for their functions, which are authenticated by personal and non-transferable access credentials to the platform. The authentication is complemented by the corresponding authorizations to access specific information assets of the Certicámara system.

5.2.4 Roles that require separation of duties

The responsibilities of the personnel who perform the roles corresponding to the Registration Authority (RA) and the Certification Authority (CA) are duly segregated, thus guaranteeing independence and impartiality in the performance of their functions. In consideration of the functions inherent to the Registration Authority (RA) and the Certification Authority (CA), and in accordance with the Specific Accreditation Criteria - CEA, these activities are carried out by personnel who maintain a direct employment relationship with Certicámara S.A..

5.3 Personnel controls

5.3.1 Qualifications, experience, and authorization requirements

Certicámara implements a reliability study process for collaborators who perform activities in the provision of digital services. This process includes the validation of references, work experience, background, home visit, and qualifications, among other evaluation criteria.

5.3.2 Background verification procedures

In the background verification process, Certicámara uses a specialized company to conduct consultations in defined lists, with the aim of determining the suitability of its collaborators.

5.3.3 Training requirements

Certicámara implements an annual training plan for its collaborators, designed based on the training needs identified within the framework of their responsibilities. This plan may include, among others, the following topics:

- Legal framework related to the provision of certification services.
- Information security and personal data protection.
- Operational and technical characteristics of accredited services.
- Operation and administration procedures.
- Business continuity.
- Technological evolution of the environment.
- Implementation of new tools.
- Modification of operating procedures.

5.3.4 Sanctions for unauthorized actions

Certicámara has established a procedure to carry out investigations and apply the corresponding disciplinary sanctions in case its collaborators contravene the guidelines given by the organization. In the event of Certicámara's suspicion that an employee is carrying out an unauthorized action, their access permission will be automatically suspended, with the possibility of the termination of their employment contract.

5.3.5 Independent contractor requirements

Certicámara keeps the contracting supports and the documentation that accredits the compliance with both administrative and technical requirements by the independent contractors that provide the data center service.

5.3.6 Documentation provided to personnel

Certicámara will make available to all personnel the documentation related to the functions associated with the position they hold, the policies and practices that govern said processes, and the security documentation.

5.4 Audit log procedures (Logs)

Certicámara has a log analysis tool, which allows monitoring transactional and security audit logs and in turn issues automatic alerts, in order to promptly identify failures or risk events that require remediation. Likewise, it keeps its log in custody 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 logged events

Certicámara contemplates the logging of the following events:

- **Warning:** Indicates that an action performed within the involved systems presents an abnormal situation, but that 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 involved systems presents unexpected behavior that results in the non-completion of the expected action.

5.4.2 Log processing frequency

The frequency of log processing is carried out permanently, ensuring that the information derived from the actions within the involved information systems is safeguarded.

5.4.3 Retention period for the audit log

It has been defined that the retention period for the different audit logs is three (3) years, a period after which, and in accordance with the guidelines given, they can be destroyed.

5.4.4 Audit log protection

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

5.4.5 Vulnerability assessments

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

5.5 Record archiving

5.5.1 Types of records archived

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

5.5.2 Archive retention period

The retention period of the documents will be in accordance with article 38 of law 527 of 1999, Certicámara's document retention schedules, and current regulations

5.5.3 Archive protection

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

5.5.4 Archive backup procedures

Copies of the files that make up the archives 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 archive information

The logged events are protected by cryptographic techniques, so that no one except the viewing and event management applications themselves can access them. Only authorized personnel have access to physical media archives and computer files, to carry out integrity verifications or others.

5.6 Key change

The keys of the certificates issued by the Root CA will cease to be valid at the same time as their self-signed certificate does. Once expired, the Root CA will generate a new key pair that it self-signs to generate the new root certificate. Certicámara will notify the external auditor and/or accreditation body established by current regulations at the time of making the key change, in order to determine the technical, procedural, and legal conditions that are applicable to this procedure before its execution, to guarantee that the applicable rules will be complied with from a security point of view. For this purpose, Certicámara will present the document called Key Change Ceremony, which will be drafted and adjusted for its presentation in advance of the proposed date for the key change.

5.7 Compromise and disaster recovery

Certicámara S.A. plans and prepares for Business Continuity to have the capacity to continue operating during emergency events or any event that causes an interruption or malfunction, for this purpose it identifies and manages the risks that could have an impact on business continuity and takes measures against their materialization, seeking to comply with the legal, regulatory, statutory, and contractual requirements of our

interested parties related to business continuity.

Certicámara S.A. establishes and applies guidelines, policies, and commitments, in order to respond quickly to an interruption or disruptive events, properly managing risks and carrying out tests that consider critical processes, suppliers, services, and activities.

5.7.1 Incident and compromise handling procedures

Certicámara has defined the incident management procedure that allows ensuring 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 to provide the service in adverse situations, after identifying, evaluating, managing, and minimizing any type of risk events, which include at a minimum the following:

- When the security of the certification entity's private key has been compromised.
- When the certification entity's security system has been breached.
- When failures occur in the certification entity's system that compromise the provision of the service.
- When the encryption systems lose validity by not offering the level of security contracted by the subscriber.

Certicámara will seek to follow 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

In accordance with the provisions of article 163 of Decree Law 019 of 2012, which modifies article 34 of Law 527 of 1999, ECDs accredited by ONAC "may cease their 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 paid for". Consequently, Certicámara will inform ONAC of the cessation of services, with 30 days' notice, as established in chapter 48 of the DURSCIT, Article 2.2.2.48.3.8. Therefore, Certicámara has defined a business continuity and contingency plan for all accredited services, ensuring the continuity in

high availability of the provided infrastructure and guaranteeing the adequate cessation of its activities as an ECD.

Certicámara will inform of the cessation by sending an email to all subscribers who have current accredited services and through two notices published in newspapers or media of wide national circulation, with an interval of 15 days, about:

- The termination of its activity or activities and the precise date of cessation.
- The legal consequences of the cessation with respect to the accredited services.
- The possibility for a subscriber to obtain a refund equivalent to the value of the remaining validity period of the contracted service.
- The authorization issued by ONAC for the ECD to cease the service, and if applicable, the CRL operator responsible for the publication of the certificates issued by the ECD, until the last of them expires.
- Any other obligation that the law establishes.

In any case, subscribers may request the revocation and the refund equivalent to the value of the remaining validity period of the services, if they request it within two (2) months following the second publication. The termination of the activity or activities will be done in the manner and following the schedule presented by Certicámara to the surveillance and control body and that it approves.

6. TECHNICAL SECURITY CONTROLS

6.1 Generation and installation of key pairs

The Root CA generates the key pair (Public and Private) using a cryptographic hardware device (HSM) that complies with the requirements established in a protection profile for a secure certification authority electronic signature device, in accordance with FIPS 140-2 Level 3 or a higher security level. The creation of the CA keys uses a pseudo-random number generation algorithm. The key generation procedure for the subordinate CAs accredited before Certicámara is identical, in their own HSM.

6.1.1 Private key delivery to the subscriber

The algorithm used for the generation of the key pair of the subscribers is RSA not less than 4096 bits using SHA256 as a cryptographic summary or hash function. Subscribers can use the following means to generate their digital certificates and keep them in custody:

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

The risks to which the cryptographic devices used would be exposed are:

- Fluctuations outside the normal environmental operating ranges, such as: voltage, temperature.
- Unauthorized physical access attempts outside the manufacturer's technical sheet.

To know the level of associated risks of cryptographic devices, you can consult the document NIST.FIPS.140-2.pdf

6.1.2 Public key delivery 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 that is requested to be signed by the subordinate CA.

6.1.3 Public key delivery of the CA to relying parties

The public key of any Certicámara subscriber will be permanently available in the active directory for consultation by relying parties who so require it.

6.1.4 Key sizes

- For Root CA certificates, the RSA algorithm with a size of 4096 bits is used.
- For Subordinate CA certificates, the RSA algorithm with a size of 4096 bits is used.
- For end entity certificates, the RSA algorithm with a minimum key size of 2048 bits is used.

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

The private key and the certificate can only be used for the uses authorized in this SCP and CP. Certicámara issues certificates with the private key usage fields limited to signing certificates and signing CRLs. The intended uses for the CA certificate keys are:

- Certificate Signing.
- Offline CRL Signing.
- Signing of the certificate revocation list (CRL).

The intended uses for the 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 email (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 Certificates of Representation of a Company / Entity and Legal Person.

6.2 Private key protection and cryptographic module engineering

The private key of the Root CA is protected by a security scheme generated by a cryptographic device. In order to maintain the custody of the private keys of the self-signed certificate, the private key is never decrypted outside the HSM. The backups maintain the secrecy of the private key in the same way that the original private key is kept in custody.

6.2.1 Cryptographic module standards and controls

The HSM that the Root CA uses to generate its keys is FIPS 140-2 Level 3 certified. The public key has been stored in a signed electronic format, so that it is protected from electronic failures and/or problems with electrical power. Therefore, the start-up 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.

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

The Root CA generates its key pair using a cryptographic hardware 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 Private key custody

The private key of the Root CA and Subordinate CA is housed in a cryptographic device. It complies with the requirements established in a protection profile for a secure certification authority electronic signature device, 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 Certicámara private key is not held in trust by a third party.

6.2.4 Private key backup

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

6.2.5 Private key archive

The backup copies of the private keys will be kept in custody in an encrypted form in the alternate data center. The backup copies of the private keys are made in secure fireproof files.

6.2.6 Private key storage in cryptographic module

The private keys are created inside the cryptographic module when it is initialized, and then the private key generated inside the HSM is exported in encrypted form.

6.2.7 Private key activation method

The only activation method for the private key consists of the use of smart cards to distribute access among 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 one Operating System administrator of the application.

6.2.8 Private key deactivation method

An operating system administrator can proceed with the deactivation of the private key of the Root CA and Subordinate CA. After having been activated by the combination described in the previous section, the operator can proceed with the deactivation by stopping the Certification Authority application.

6.2.9 Private key destruction method

The Root CA and the Subordinate CA will delete their private key when its validity period expires or it has been revoked. The destruction will be carried out using the commands established to physically erase the part of the HSM memory where the key was recorded. The same will happen with its 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 cryptographic modules with FIPS 140-2 Level 3 certification (nShield Edge, nShield Connect 500, nShield Connect 1500+, nShield Connect 6000+).

6.3 Other aspects of key pair management

6.3.1 Public key archive

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

6.3.2 Certificate operating periods and key pair usage periods

The key pair of the root CA will be valid until Saturday, May 24, 2031. On the other hand, the operating periods of the certificates will be ten years. The key pair of the subordinate CA will be valid until Saturday, May 24, 2031. On the other hand, the operating periods of the certificates will 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 guaranteed by a PIN in the possession of authorized personnel.

6.4.2 Protection of activation data

- Only authorized personnel possess the cryptographic cards capable of activating the CA's private keys, and they also know the PINs required for their use.
- The personal access key (PIN) is confidential, personal, and non-transferable. It is the parameter that protects the private keys, allowing the use of Root CA and Subordinate CA certificates. Therefore, certain security rules must be followed for its safekeeping and use:
- The PIN should not be sent or communicated to anyone.
- Operators and administrators should change the PIN when they suspect that someone else knows it.
- It is recommended that the PIN be changed periodically.

6.5 Information security controls

6.5.1 Specific technical requirements for information security

For the respective provision of the service, a series of technical controls have been established, which ensure its proper functioning. Among the aspects that are taken into account are:

- Equipment configuration.
- Application configuration.
- User configuration.

- Application of profiles for network access.
- Information about the security system for protecting information collected for the purpose of issuing certificates.

6.5.2 Information security qualification

Currently, Certicámara, as part of its organizational focus, is certified under the ISO/IEC 27001:2022 - Information Security Management System Standard in accordance with the scope defined in the certificate, which is available on the Certicámara website.

6.6 Technical lifecycle controls

6.6.1 System development controls

The security requirements for the development of systems for the root CA and the SUBORDINATE ENTITY are mandatory. A security design analysis must be performed during the design and specification phases of new requirements for any component that will be used in the root CA and Subordinate CA applications. This is in order to ensure that the involved systems are secure. The technological infrastructure of the root CA and Subordinate CA must have clearly differentiated and independent development and production environments. Change control procedures must be used for new versions and updates.

6.6.2 Security management controls

Certicámara maintains an inventory of all information 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 growth of resource needs must be monitored according to demand.

6.6.3 Lifecycle security controls

Throughout the lifecycle, security controls must be implemented that allow for the instrumentation and auditing of 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 integral service. Firewalls or encrypted data exchange between networks are used to guarantee integrity. On the other hand, redundancy and high availability technologies are used to guarantee reliable and high-performance operation. Additionally, the infrastructure must be audited periodically by internal and external Certicámara personnel.

6.8 Timestamping

The synchronization of the CA and RA clocks is carried out 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, modified by Decree 62 of 2021.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The certificates of the root CA and the SUBORDINATE ENTITY are issued in accordance with the normative or technical documents defined in the scope accredited by the ONAC, which is published at https://onac.org.co/directorio-de-acreditados/

7.1.1 Version number(s)

The certificates issued by Certicámara are in accordance with the X.509 v3 standard

7.1.2 Certificate extensions

The extensions of the certificates of the Root CA and Subordinate CA allow for encoding additional information in the certificates. The standard X.509 extensions define the following fields:

- SubjectKeyIdentifier
- Authority KeyIdentifier
- BasicConstraints. Marked as critical
- Certificate Policies. Marked as critical
- KeyUsage. Marked as critical
- CRLDistributionPoint. Marked as critical
- SubjectAlternativeName. Marked as critical
- AuthorityInformation Access

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

- Date and time of signing.
- Document name.
- Subject.
- Certifying Entity.
- Certificate Serial.
- Thumbprint.
- Certificate valid from.
- Certificate valid until.

7.1.3 Algorithm object identifiers

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

7.1.4 Name forms

The certificates issued by Certicámara have a DN, in X.500 format, the names of the issuer and certificate holder in the issuer and subject fields.

7.1.5 Name restrictions

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

7.1.6 Certificate policy object identifier

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

7.1.7 Syntax and semantics of policy qualifiers

The syntax and semantics of their description are found within the generated digital certificates, within the certificate directives section, where a URL is shown where Certicámara's SCP is published.

7.2 Certificate revocation list profile

7.2.1 Version number(s)

The Subordinate CA issues CRLs in X.509 format.

7.2.2 CRL and CRL entry extensions

The extensions of the CRLs issued by the Root CA are those defined in accordance with RFC 5280, that is:

- Authority Key Identifier.
- CRL Number.
- Issuing Distribution Point.

7.3 OCSP profile

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

7.3.1 Version number(s)

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

7.3.2 OCSP extensions

In accordance with the functioning of the generation of digital certificates, the use of OCSP extensions has not been established.

8. COMPLIANCE AUDIT AND OTHER EVALUATIONS

8.1 Frequency or circumstances of the evaluation

In accordance with the definitions of the National Accreditation Body of Colombia - ONAC, Certicámara has established an annual audit program for the evaluation of its various accredited services. The accreditation system of the root CA and the Subordinate CA will be subject to a third-party audit annually, in accordance with the audit program defined by Certicámara. This process guarantees the adequacy of their functioning and operation to the provisions contained in this SCP. Additionally, Certicámara reserves the right to carry out internal audits at its own discretion or at any time there is a suspicion of non-compliance with any security measure or a possible key compromise. Likewise, an external audit will be carried out annually to evaluate the level of conformity with the Webtrust principles and criteria for digital Certification Authorities of AICPA/CICA.

8.2 Identity/qualifications of the evaluator

In the case of the third-party audit, the auditing firm must comply with the minimum assurance requirements stipulated in the specific accreditation criteria that the ONAC has published on its website, in addition to those defined in Certicámara's internal procedures for contracting third parties.

8.3 Evaluator's relationship with the evaluated entity

The interaction between the auditor and the entity subject to audit will be strictly limited to the processes and information required for the performance of the audit. Consequently, the audited party (either the root CA or the subordinate entity) must not have any financial, legal, or any other relationship, whether current or projected, that could lead to a conflict of interest with the auditor. With respect to internal auditors, the absence of any functional relationship with the area subject to the audit will be required.

8.4 Actions taken as a result of a non-conformity

The identification of any non-conformity during the audits will activate the internal process of managing improvement actions, whose objective is the elimination of the detected root cause. In the event of a critical non-conformity, Certicámara will be empowered to determine the temporary suspension of the operations of the root CA or the Subordinate CA until the deficiencies are remedied as soon as possible.

8.5 Communication of results

All audit results are presented to the presidency committee in order to determine the corrective and improvement actions that should be implemented.

9. OTHER LEGAL AND COMMERCIAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Fees for accessing revocation or status information

Certicámara does not consider charging for access to revocation or status information related to the certificate in its pricing policies. Both consultation and revocation will have no cost

9.1.3 Refund policy

Subscribers can request a refund through the Certicámara S.A. PQRSAF section website https://web.certicamara.com/soporte/Sistema-de-PQRSAF in the following cases:

- **Withdrawal from the acquisition process**: A right exercised by the subscriber when the digital certificate has not been issued. In these cases, it is a withdrawal in the course of the acquisition process until before the download of the digital certificate or the delivery of the physical token. The subscriber or client user has a maximum period of ninety (90) days.
- **Subscriber's right of withdrawal**: This is applicable when exercised within 5 business days from the delivery of the item, the provision of the service, or the conclusion of the contract. The applicability of this will be evaluated in consideration of the specific characteristics of the product or service acquired. Subscribers who acquire digital signature certificates issued by Certicámara S.A. through non-traditional or distance mechanisms (including electronic, telephone, or virtual channels) may exercise their right of withdrawal within five (5) business days following the conclusion of the contract, provided that the service has not begun to be executed. Since digital signature certificates constitute personalized services, exclusively associated with the holder, and whose execution is perfected with the issuance or download of the certificate, the right of withdrawal will not proceed once the technical process of activating the certificate has begun. Therefore, the right of withdrawal will only be applicable if: i) It is exercised within the legal period of five (5) business days from contracting, and ii) The certificate has not been issued, downloaded, activated, or linked to the user.

- **Payment reversal**: A right exercised in cases of fraud, unsolicited operation, defective product, acquired product not being received, and non-conforming product, within 5 business days.
- **Refund for double payment, excess payment, wrong payment**: A request made by the subscriber when a payment is made twice on the same invoice or digital certificate, or when a little more than what was owed was paid, or a wrong deposit was made. The subscriber or client user has a maximum period of ninety (90) days.
- **Refund for Taxes**: In this case, the client paid a value for some tax that they should not have paid, and therefore, the refund must be processed. The subscriber or user has a maximum period of ninety (90) days.
- **Refund for incompatibility**: In these cases, the client requests a refund because the digital certificate is not compatible with their computer or their system. The subscriber or user has a maximum period of ninety (90) days as long as the digital signature has not been downloaded.
- **Refund for non-compliance with the duty to inform**: This occurs in cases where there are sanctions or fines for non-compliance with this duty, provided there is a judicial or administrative decision, in which cases the refund must be processed regardless of the time in which it occurs.

9.2 Financial responsibility

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 2.2.2.48.2.5 of Decree 1074 of 2015 (which compiles Decree 333 of 2014, article 9°), Certicámara has subscribed an insurance policy with an authorized insurance entity in accordance with Colombian legislation, which covers the contractual and non-contractual damages of subscribers and good faith third parties free of fault resulting from errors and omissions, or from bad faith acts of the administrators, legal representatives, or employees of Certicámara in the development of its activities.

b) The insured amount is 7,500 SMMLV per event.

c) The general conditions of the policy can be consulted on the website in the following section: https://web.certicamara.com/marco-normativo/poliza-de-garantias.

9.3 Confidentiality of Information

Certicámara is committed to protecting all data to which it has access as a result of its activity as a certification entity. However, Certicámara reserves the right to disclose to employees and consultants, external or internal, the confidential data necessary to carry out activities within Certicámara. In this case, employees and/or consultants are informed about the confidentiality obligations. These obligations do not apply if the information classified 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 current regulations. The confidential information of the digital certification services subscriber may be exposed at their request, in their capacity as the owner of this information. When the ECD is required, by law or authorization in contractual provisions, to disclose confidential information, the subscriber or the person involved must, unless prohibited by law, be notified of the information provided.

9.3.1 Scope of confidential information

The following is considered confidential information:

- Documents that contain information related to the administration, management, and control of the PKI infrastructure.
- Business information supplied by its suppliers and other people with whom Certicámara has a duty to keep secret established legally or conventionally.
- Information resulting from consultations made in risk centers or other private or public sector entities.
- Labor information that contains related subscriber data.
- All information that is sent to Certicámara and that has been labeled as "Confidential" by the sender.
- Information about the subscriber obtained from sources other than the subscriber (for example, from a complainant or regulators) must be treated as confidential, except when it is of a public nature.

9.3.2 nformation outside the scope of confidential information

The following is considered non-confidential information:

- Content of the issued certificates.
- Certificate Revocation List (CRL).
- The public key of the Root CA and Subordinate CA.
- The certification practice statement.
- Organizational policies.

9.3.3 Responsibility for protecting confidential information

As an accredited digital certification entity, Certicámara S.A. has established a commitment to safeguard the confidentiality, integrity, and availability of all the information it manages within the framework of certification services. This includes, but is not limited to, the personal information of subscribers, private keys, digital certificate data, and any other information that, due to its nature, must be treated with the utmost discretion. To guarantee the protection of this information, we are committed to:

- Implementing and maintaining strict information security policies and procedures that comply with national and international standards, including the requirements of the ONAC and current legislation on data protection.
- Continuously training all our staff on best practices in information security, the importance of confidentiality, and their individual responsibilities in data protection.
- Using robust and updated security technologies and systems, including data encryption, strict access controls, intrusion detection systems, and information backup and recovery mechanisms.
- Limiting access to confidential information only to authorized personnel who require such information to perform their duties. All access is monitored and recorded.
- Establishing confidentiality agreements with all our employees, contractors, and third parties who may have access to sensitive information.
- Managing the information of subscribers' private keys securely and responsibly, ensuring their protection against unauthorized access, disclosure, alteration, or destruction.
- Notifying the competent authorities and those affected in a timely manner about any security incident that compromises the confidentiality, integrity, or availability of the information, in accordance with applicable regulatory frameworks.
- Performing internal and external audits regularly to evaluate the effectiveness of our security controls and ensure continuous compliance with our policies and regulatory requirements.

The trust of our users is fundamental. Therefore, the protection of their confidential information is an essential pillar of our operations.

9.3.4 Personal Data Treatment

At Certicámara S.A., the processing of personal data is governed by the principles of legality, purpose, freedom, truthfulness or quality, transparency, access and restricted circulation, security, and confidentiality, in strict compliance with current Colombian legislation on data protection, including Law 1581 of 2012 and its regulatory decrees. To

guarantee the proper treatment of the personal data that Certicámara S.A. collects or has access to, it is committed to:

- Collecting personal data only when it is necessary and relevant for the provision of its digital certification services, identity verification, the issuance, renewal, suspension, or revocation of certificates, and the fulfillment of our legal and contractual obligations.
- Informing the data holders about the specific purpose for which their data will be collected and processed, obtaining their prior, express, and informed consent, unless the law requires or permits otherwise.
- Using personal data exclusively for the informed and authorized purposes, refraining from using them for purposes other than those established in its personal data processing policy, authorizations, or privacy notice provided at the time of collection.
- Guaranteeing the truthfulness, updating, and completeness of the information contained in our databases, implementing the necessary mechanisms for the holders to be able to update or rectify their data.
- Implementing rigorous technical, human, and administrative measures to safeguard the security of personal data, preventing its adulteration, loss, consultation, use, or unauthorized or fraudulent access.
- Allowing holders to access their personal data and information about its processing, as well as facilitating the exercise of their rights to know, update, rectify, and delete their data, and to revoke the authorization granted.
- Maintaining the confidentiality of personal data, even after the relationship with the holder has ended, except in cases where the information is required by a judicial or administrative authority in the exercise of its legal functions.
- Not transferring or communicating personal data to third parties without the express authorization of the holder, except in cases where the law permits or requires it for the fulfillment of a legal or contractual function.

Certicámara has the personal data processing policy available to the applicant and subscriber on the website, at the following online location, https://web.certicamara.com/politicas

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 can only be disclosed when a judicial or administrative authority, in the exercise of its functions, requires it. In accordance with the provisions of law 1581 of 2012, the holder's authorization is not necessary when the information is required by a public or administrative entity in the exercise of its legal functions or by judicial order.

9.4 Intellectual property rights

The subscriber must respect and comply with the regulations on intellectual property, which includes both industrial property and Copyright. To this end, they will comply with the provisions of the Commercial Code, 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 the information contained in the Statement of Certification Practices -SCP belongs solely and exclusively to the Sociedad Cameral de Certificación Digital Certicámara S.A., in such a way that it reserves all rights related to the intellectual property of this document (SCP), including the 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 depending on the service provided and in general the necessary infrastructure for the provision of the Digital Certification service.
b) Comply with the Statement of Certification Practices (SCP), Certification Policies (CP), and the agreements made with the subscribers.
c) Inform the subscriber of the characteristics of the service provision, the limits of responsibility, and the obligations they assume as an intervener in the digital certification process. In particular, Certicámara must inform the subscriber or third parties who request it, about the time and computer resources required to validate the digital signature that is 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 Statement of Certification Practices as verifiable for the issuance of digital certificates.
e) Refrain from accessing or storing the subscriber's private key.
f) Preserve by itself or through an interposed person the custody of the physical medium of the digital certificate until its effective delivery 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 section on the digital certificate issuance procedure of this Statement of Certification Practices, and the specifications agreed upon by the subscriber in the subscription contract.
i) Publish the issued digital certificates and keep the Register of Issued Certificates.

j) Inform the National Accreditation Body of Colombia of the occurrence of any event established in the Statement of Certification Practices that 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 their digital certificate, explaining the reasons for the decisions made in accordance with what is established in the Statement of Certification Practices.
m) Maintain control and confidentiality of its private key and establish reasonable security measures so that it is not disclosed or compromised.
n) Diligently seek the permanent and uninterrupted provision of digital certification services.
o) Allow access to subscribers, relying parties, and third parties to this Statement of Certification Practices and the repository of the Certification Entity.
p) Update the database of revoked digital certificates in the terms established in this Statement of Certification Practices and make the notices and publications that are established by law in it.
q) Revoke the digital certificates that are required in accordance with the provisions of section 4.7 of this Statement of Certification Practices.
r) Inform the subscriber, within the following 24 hours, of the revocation of their digital certificate in accordance with current regulations.
s) Remove administrators or representatives who are involved in the causes established in literal c of article 29 of Law 527 of 1999.
t) Have a telephone line available for subscribers and third parties, which allows for inquiries and the prompt request for revocation of certificates by subscribers.
u) Supply the information that is required by the competent administrative or judicial entities in relation to the digital signatures and certificates issued and in general about any data message that is under its custody and administration.
v) Keep the documentation that supports the issued digital certificates physically or electronically for the term provided by law for commercial papers and take the necessary measures to guarantee the integrity and confidentiality that are its own.
w) Address the petitions, complaints, and claims made by subscribers, in accordance with what is established in this Statement of Certification Practices.
x) Grant the information provided by the subscriber the treatment that is established in the section on certificate request of this Statement of Certification Practices.
y) Comply with the Specific Accreditation Criteria CEA 3.0-7 published on the ONAC WEB page.
z) Warn about the security measures that subscribers of digital signatures and certificates must observe for the use of these mechanisms.
aa) Certicámara, without any discrimination, will provide the digital certification service to any applicant who complies with the requirements established in this

SCP and current legal regulations. However, Certicámara may decline the digital certification request to the applicant or subscriber when participation in illicit activities is evidenced.

bb) Comply with the provisions of Statutory Law 1581 of 2012 on Personal Data Protection and its development 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 related services.

cc) Notify the subscriber in advance about subcontracting activities in order to give them the opportunity to object in accordance with current Colombian regulations. For this, Certicámara has a system for receiving Petitions, complaints, claims, suggestions, and appeals (PQRSA) on its website.

dd) The critical suppliers contracted for the provision of the datacenter service comply with the minimum requirements established in the Specific Accreditation Criteria CEA 3.0-7 document published on the ONAC WEB page. For this purpose, compliance with the requirements described in the Specific Accreditation Criteria CEA 3.0-7 published by the ONAC will be extended to them when it corresponds.

ee) The others established in article 32 of Law 527 of 1999 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 issuing digital certificates or the provision in general of the digital certification service may be carried out directly by Certicámara or through its Registration Entities. CERTICÁMARA HAS NO ADDITIONAL OBLIGATIONS TO THOSE PROVIDED IN THIS SECTION EXCEPT THOSE PROVIDED IN THE CURRENT REGULATIONS, NOR SHOULD IT BE UNDERSTOOD THAT THERE ARE ADDITIONAL IMPLICIT OBLIGATIONS TO THOSE EXPRESSLY ESTABLISHED IN THIS STATEMENT OF CERTIFICATION PRACTICES.

9.5.2 Obligations and duties of the applicant

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

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

9.5.3 Obligations and responsibilities of the subscriber

The subscriber has the following obligations to Certicámara and third parties:

a) Use the private key and the digital certificate issued only for the established purposes and in accordance with the conditions established in the contract celebrated with them individually and in this Statement of Certification Practices

and the corresponding certification policy. The subscriber will be responsible for the improper use that they 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 what capacity they are signing (either as a natural person or as a natural person linked to a specific quality at the time of the issuance of the digital certificate), as long as the information system of the relying party does not verify the quality in which the subscriber is acting. The data message or electronic document that the subscriber signs with their digital certificate will be the one that determines the context of the capacity in which the subscriber signs, and whether or not they are using the quality associated with the digital certificate (if applicable).

c) Be responsible for the custody of the private key and its physical medium (if applicable), preventing its loss, disclosure, modification, or unauthorized use. Especially, the subscriber must refrain, regardless of the circumstance, from writing the activation code or the private keys on the physical medium of the digital certificate, nor on any other document that the subscriber keeps or carries with them or with the physical medium.

d) Request the revocation of the digital certificate that has been delivered to them when any of the assumptions provided for the revocation of digital certificates are met.

e) Refrain in all circumstances from disclosing the private key or the activation code of the digital certificate, as well as refraining 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 for any subsequent circumstance the information of the digital certificate does not correspond to reality. Likewise, they must immediately communicate the change or variation that any of the data they provided to acquire the digital certificate has undergone, even if these were not included in the digital certificate itself.

g) Immediately inform Certicámara about any situation that may affect the reliability of the digital certificate, and initiate the digital certificate revocation procedure when necessary. In particular, they must immediately notify the loss, theft, or falsification of the physical medium and any attempt to carry out these acts on it, as well as the knowledge by other people of the activation code or the private keys, requesting the revocation of the digital certificate in accordance with the procedure established in the Statement of Certification Practices.

h) Destroy the physical medium when Certicámara requires it, when it has been replaced by another for the same purposes, or when the period of the acquired digital certificate service with Certicámara ends, following Certicámara's instructions in all cases.

i) Return the physical medium of the digital certificate when Certicámara requires it.

j) Respect the intellectual property rights (Industrial Property and Copyright) of Certicámara and third parties in the request and use of digital certificates. Certicámara will not include information in the digital certificate whose inclusion could in any way constitute the violation of the intellectual or industrial property rights of Certicámara and third parties.
k) Any other that derives from current regulations, the content of this Statement of Certification Practices, 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 a bad reputation and harm to Certicámara.
n) Refrain from using the name of the ECD and the certification mark or in all advertising material that contains any reference to the digital certification service provided by Certicámara immediately after its cancellation or termination and undertake the actions required by the digital certification service and any other measure that is required.
o) Comply with the logo use manual 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 that are held by Certicámara.
q) The others established in article 39 of Law 527 of 1999.

THE SUBSCRIBER MAY USE THEIR CERTIFICATE FOR: (I) IDENTIFYING THEMSELVES AS A NATURAL PERSON, OR (II) ASSOCIATING THEIR PERSONAL IDENTIFICATION WITH A SPECIFIC QUALITY VERIFIED BY CERTICÁMARA AT THE TIME OF ISSUANCE OF THE DIGITAL CERTIFICATE (IF APPLICABLE). THE USE OF THE DIGITAL CERTIFICATE IN ONE OR THE OTHER CASE WILL DEPEND DIRECTLY ON THE CONTEXT IN WHICH THE DIGITAL CERTIFICATE IS BEING USED AND ON WHETHER THE INFORMATION SYSTEM OF THE RELYING PARTY CAN OR CANNOT VERIFY THE IDENTIFICATION OF THE SUBSCRIBER. IT WILL BE THE ELECTRONIC DOCUMENT OR DATA MESSAGE THAT THE SUBSCRIBER DIGITALLY SIGNS THAT WILL OFFER THE CONTEXT WITHIN WHICH THE SUBSCRIBER USES THE CERTIFICATE AND WHETHER OR NOT THEY USE THE QUALITY ASSOCIATED WITH THE DIGITAL CERTIFICATE.

9.5.4 Obligations and responsibilities of the relying party

Certicámara's Digital Certification System includes the use of a set of elements integrated around the provision of a service to both subscribers and those who use and rely on the digital certificates issued by Certicámara. When a third person relies on a digital certificate, they are accepting to use said system in its entirety and therefore agree to be governed by the rules established for it, which are contained essentially but not exclusively in this Statement of Certification Practices. This third person becomes an intervener in the Digital Certification System, in the capacity of a relying party, and therefore assumes the obligations that are established below:

a) Verify the reliability of the digital signature and the digital certificate, especially checking that it is not in Certicámara's database of revoked digital certificates available on the website or in Certicámara's offices. The reliability of the digital signature and the digital certificate must in all cases adhere to what is established in the section on Reliability of signatures and digital certificates.

b) Accept and recognize the digital certificates only for the use that is permitted in accordance with what is established in the section on Use of digital certificates.

c) Know in detail and comply at all times with the Statement of Certification Practices in the use of Certicámara's digital signatures and certificates. In particular, the relying party must keep in mind and act at all times in accordance with the limitations of liability and guarantees that Certicámara offers.

d) Inform Certicámara of any irregularity or suspicion of the same that occurs 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 Obligations of contractors

In the event that Certicámara externally contracts services or products related to the accredited activities in the scope, the fulfillment of the requirements established in CEA 3.0-7 will be extended, based on the nature of the contracted service, this Statement of Certification Practices, and the requirements of the current Colombian regulatory framework according to their contracted function for digital certificates. Certicámara will determine if the external approval entity provides the levels of compliance, as established contractually, without prejudice to the norms of higher hierarchy in force at the legal, technical, operational, and procedural level for the approval process, which will be available for study and contrast in Certicámara's management systems, which allow for establishing access according to their confidentiality classification, and in any case will be available for the reception of third-party audits and by the National Accreditation Body.

9.6 Limits of liability

a) 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 respond professionally for slight fault in its actions as a Digital Certification Entity. Certicámara cannot ensure that the certification activity has a specific result. Certicámara will only be liable for those errors that, having occurred, could have been avoided by its professional diligence.

b) b) The damages produced or related to the non-execution or defective execution of the obligations of the subscriber, the relying party, or both, will be at their expense, as well as all damages caused by the improper use of digital certificates or violations of their use limitations established in it, in the section on 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, what the current regulations establish in terms of the responsibility of subscribers will be taken into account.

c) c) Certicámara will not be liable for damages caused by the non-compliance with its obligations due to cases of force majeure, unforeseeable circumstances, or, in general, any circumstance over which it cannot have reasonable control, including but not limited to the following: natural disasters, public order disturbances, power and/or telephone supply cuts, computer viruses, deficiencies in telecommunications services (Internet, communication channels, etc.), or the compromise of asymmetric keys derived from unforeseen technological risk.

d) d) Regardless of the cause or origin of its liability, Certicámara sets the maximum amount for the indemnification of damages for damages caused by a digital certificate issued, in accordance with what is established in the professional civil liability policy. Consequently, Certicámara will only indemnify the people harmed by a digital certificate issued by it, regardless of the number of times it has been used or the number of people harmed by said uses. In the event that there are several harmed parties, the maximum indemnifiable amount will be distributed pro rata among them. If, after the indemnification has been distributed, new harmed parties arise, they must go against the already indemnified people in order to obtain their indemnification pro rata.

e) e) Certicámara will only be liable for damages caused by the use of digital certification services within the year following the expiration or revocation of the digital certificate. Certicámara does not offer any type of guarantee that is not expressly stipulated in this Statement of Certification Practices, nor will it be liable for any event that is not expressly contemplated in this section.

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

g) g) In the event that the laws applicable to the digital certification service establish the impossibility of limiting liability in any of the aspects described here or that are described in this Statement of Certification Practices, these clauses will be given the greatest scope that the law allows them to have in terms of the limitation of Certicámara's liability.

9.7 Rights of the interveners

9.7.1 Rights of the applicant

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

a) To have their request attended to in accordance with the times defined by the entity.
b) To have what is established in the certification policies complied with.
c) To receive attention to resolve doubts or concerns regarding the digital certification service.

9.7.2 Rights of the subscriber

Subscribers of Certicámara's certification services will have the following rights:

a) To be able to use the acquired digital certification service properly.
b) To inform relying third parties that Certicámara is their ECD that provides the acquired 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 processing policy.
e) To receive support for the digital certification service(s) in accordance with the terms and conditions established between the parties.
f) To withdraw from the acquisition of certification services, as long as they comply with the requirements established in law 1480 of 2011.
g) To reverse the payment when it is one of the events determined in decree 587 of 2016.

9.8 Exclusion of guarantees

Certicámara will not be responsible for:

a) The veracity of the information provided by the subscriber or applicant.
b) Computer crimes suffered by the subscriber.
c) The fraudulent use of certified services or CRLs.
d) Damages and losses caused by the erroneous interpretation of the Statement of Certification Practices (SCP).
e) For the content of the messages or documents in which digital certification services are used.
f) For the non-compliance with the obligations of the subscriber or applicant.
g) For unforeseeable circumstances or force majeure.
h) For the use of certificates when it exceeds the provisions of current regulations, the SCP, and CPs.

9.9 Contract templates

The contract model that Certicámara uses for the provision of the digital signature certificate service is made up of two (2) documents, which are available at 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 contract model that Certicámara uses for the provision of the other accredited services is made up 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, a contract detailing these situations may be signed between Certicámara and the client.

9.10 Policy for handling other services

Does not apply.

9.11 Impartiality and non-discrimination

Certicámara recognizes the importance of safeguarding impartiality and independence to prevent both internal and external conflicts of interest. Therefore, the Presidency declares its commitment to guaranteeing compliance with the requirements of independence, impartiality, and integrity in all its services. The main mechanism to ensure impartiality is the impartiality management process and the formation of the impartiality committee. The impartiality policy is available at: https://web.certicamara.com/politicas

Certicámara has carried out an exhaustive process of identifying, analyzing, and evaluating the risks that could compromise the objectivity and impartiality in the provision of its digital certification service. Consequently, it reports on the actions implemented with the purpose of minimizing any circumstance that could jeopardize the objectivity and impartiality in the provision of its services:

- In order to prevent risks associated with misleading advertising, its website has been carefully designed to ensure that its clients and/or subscribers can clearly discern which of its products and/or services have the accreditation of the National Accreditation Body of Colombia (ONAC).
- To mitigate risks in the contracting of Datacenter services, the providers that supply this service are managed integrally (from selection and contracting to the evaluation of their performance) in strict observance of their supplier management procedure, thus ensuring compliance with the admissible technical requirements defined in the specific accreditation criteria.
- The policies and procedures that govern Certicámara's operation, as well as its administration, are applied in a non-discriminatory manner. Certicámara refrains from using procedures that may hinder or restrict the access of applicants to its services.

The digital certification services offered by Certicámara are accessible to all applicants whose requests fall within the scope of its accreditation, consistently applying the principle of technological neutrality, which is duly stated in the definitions and conventions of this document. Access to Certicámara's digital certification services is not conditioned by any particular characteristic of the applicant or subscriber other than those expressly defined in the Certification Policy (CP), nor by belonging to any association or group, nor by the number of certifications previously issued. There are no improper conditions, whether financial or of another nature.

9.12 Policy for Petitions, complaints, claims, suggestions, and felicitations

Certicámara establishes the guidelines, processes, and communication channels for the reception, management, monitoring, and timely response to Petitions, Complaints, Claims, Suggestions, and Felicitations submitted by clients, users, and other interested parties. In this way, the continuous improvement of services and products is guaranteed, as well as the satisfaction of all interest groups. For the above, the following channels have been made available to file a PQRSAF:

- **In person**: At our Bogotá headquarters, Carrera 7 N° 26-20 Floor 18.
- **Email**: certicamararesponde@certicamara.com.
- **Telephone line** (sales, customer service, and technical support): (601) 7442727.
- **PQRSAF System**: Available on the website.

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

9.13 Dispute resolution provisions

All differences that arise between the parties on the occasion of the celebration of the contract, during its execution or due to its interpretation, will be resolved between the Holder of the Digital Certificate and Certicámara S.A. in the first instance, by way of conciliation, transaction, or amicable composition. To do this, the non-conforming party will send a duly substantiated written communication to the other PARTY, who will evaluate the reasons for non-conformity and send a response within five (5) business days from the date of its receipt. (It will be the responsibility of the party that sends the communication to ensure that the other party receives the communication sent, taking into account security and information integrity parameters) .

If after the term indicated above, fifteen (15) days pass and the difference(s) persist, it (they) will be resolved by an Arbitration Tribunal regardless of the nationality of the Digital Certificate holder. The tribunal will be subject to the current regulations on the matter and will be governed especially by the following rules:

a) The Tribunal will be made up of one (1) arbitrator appointed by THE PARTIES by mutual agreement. If this is not possible, his appointment is delegated to the

Director of the Arbitration and Conciliation Center established by Certicámara S.A.. At the time of accepting their appointment, the arbitrator must state in writing to THE PARTIES their 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 will be subject to the rules provided for this purpose by the Arbitration and Conciliation Center, in what is not regulated in this clause.
d) The Tribunal will function in the city of Bogotá, at the Arbitration and Conciliation Center.
e) The Tribunal will decide in law and its ruling will have the effects of res judicata of last instance and, consequently, will be final and binding for THE PARTIES.
f) The costs caused by the convocation of the Tribunal will be borne by the defeated PARTY.
g) The applicable regulations will be Colombian.

9.14 Applicable law

From Certicámara, the following regulations have been identified 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 relation to the digital signatures of natural or legal persons.
- **Activity 2.** Issuing certificates on the verification regarding the alteration between the sending and receiving of the data message and transferable electronic documents.
- **Activity 3.** Issuing certificates in relation to the person who holds a right or obligation with respect to the documents listed in literals f) and g) of article 26 of Law 527 of 1999.
- **Activity 4.** Offering or facilitating the services of generating the creation data of certified digital signatures.

- **Activity 6.** Offering or facilitating the services of generating the creation data of electronic signatures.
- **Activity 9.** Any other activity related to the creation, use, or utilization of digital and electronic signatures.

9.15 Certification policies

The interrelation between this SCP and the Certification Policies applicable to the different types of certification services is based on the following:

- This SCP is structured based on the recommendations of RFC 3647 and establishes the practices adopted by Certicámara for the provision of services accredited by ONAC. It contains detailed information about its security, support, administration, and certificate issuance system, as well as the relationship of trust between the Applicant, Subscriber, Responsible Party, Providers, good faith Third Parties, and the ECD.
- The Certification Policies establish the particular procedures and requirements applicable to the Certification services provided by Certicámara.
- In each of the Certification Policies, the requirements for the service request, responsibilities, commercial conditions, and in general the particular conditions for each of the certification services are defined.

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

- PC Digital Signature Certificate.
- PC Chronological Timestamp.
- PC Associated Information Services.

Which are available at https://web.certicamara.com/marco-normativo

10. CHANGE CONTROL

Fecha	Razón de actualización
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.

CERTIFICATION PRACTICE STATEMENT

Fecha	Razón de actualización
	• 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 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.

CERTIFICATION PRACTICE STATEMENT

Fecha	Razón de actualización
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 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.

CERTIFICATION PRACTICE STATEMENT

Fecha	Razón de actualización
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. • 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.

Fecha	Razón de actualización
	• 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. • 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 ".

CERTIFICATION PRACTICE STATEMENT

Fecha	Razón de actualización
	• 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. • 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

CERTIFICATION PRACTICE STATEMENT

Fecha	Razón de actualización
	services, which are published on the website in the same section.
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 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.

Fecha	Razón de actualización
	• 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, 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.

CERTIFICATION PRACTICE STATEMENT

Fecha	Razón de actualización
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. • 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.
05/08/2025	The following changes have been made to the document: • Comprehensive wording adjustments to provide greater clarity and precision in the information. • Updates to the position and area responsible for PQRSAF support, as well as the procedure to be followed. • Adjustments to the approval procedure for changes to the CPD. • Adjustments to the download time conditions. • Inclusion of the fact that the digital certificate revocation procedure is free of charge. • Clarity of the conditions to be taken into account for reimbursement due to withdrawal.

CERTIFICATION PRACTICE STATEMENT

Fecha	Razón de actualización
	• Elimination of the national toll-free number. • Updates to links.
26/09/2025	The following changes have been made to the document: • Updated contact information in section 1.5.2. • Adjusted guidelines for resetting virtual token passwords, which are free of charge for up to ten requests.