Código:	DYD-L-007
Fecha:	26/09/2025
Versión:	011
Etiquetado:	PÚBLICO

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

Policy for Certification - Digital Signature Certificate

Code: DYD-L-007

Date: September 2025

Version: 010

certicámara.

Código:	DYD-L-007
Fecha:	26/09/2025
Versión:	011
Etiquetado:	PÚBLICO

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

Content

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

1. INTRODUCTION

This document presents a public statement of the open digital certification authority on the specific policies and procedures, rules and general conditions of the digital certificate service provided by the Digital Certification Chamber Certicámara S.A.

This certification policy (PC) has been structured in accordance with the recommendations of RFC 3647 and the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014 and the regulations that modify or complement them, in the Colombian territory.

The general conditions that have a transversal scope to the different digital certification services offered by Certicámara are described in the **Declaration of Certification Practices** (DPC) published on the website under the regulatory framework section.

1.1 *Name and identification of the document*

Certicámara for the provision of its digital signature certificate service, establishes the following information for the present document.

Name	Certification Policies - Digital signature certificate
Date of publication	26/09/2025
Version	011
Code	DYD-L-007
Location	https://web.certicamara.com/marco-normativo

1.2 *Scope*

This document sets the rules and guidelines to be followed by the Certicámara certifying entity to offer the Digital Signature Certificate service as established in the accreditation certificate issued by the National Accreditation Body of Colombia (ONAC) on its website https://onac.org.co/certificados/16-ECD- 002.pdf

1.3 Procedure for Updating or Approving the Policy

The Certification Policy will be updated when required by legal, regulatory, and/or other requirements applicable to the services within the scope of this document. 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. Final approval of these changes is given by the President.

The responsibility for managing the update of the CP on the Certicámara website, specifically at the link https://web.certicamara.com/marco-normativo, falls to the Director of Continuous Improvement

1.4 Publication Responsibilities

The Certification Entity is obligated to publish information related to its practices, its certificates, and the updated status of said certificates. Certicámara's publications of all information classified as public will be announced on its respective website as follows:

a) The Certificate Revocation List (CRL) is available in CRL V2 format in the root CA repository.
b) The Certification Policies of the root CA can be found in the updated version of this document.
c) The latest version of this document is public and available on the root CA's website at https://web.certicamara.com/marco-normativo.
d) The public keys of the certificates issued by the subordinate CA are available in the public LDAP repository, in X.509 v3 format, and at the address https://ar.certicamara.com:8443/Search/, where they can be consulted by a search parameter.
e) Certicámara's contact details are described on the website https://web.certicamara.com
f) The root CA's operation manuals and all information considered relevant to the certificates issued can be found at https://web.certicamara.com/soporte_tecnico.
g) The status of OCSP certificate revocation is available for consultation via the web at http://ocsp.certicamara.com, http://ocsp.certicamara.co y http://ocsp4096.certicamara.co.

2. IDENTIFICATION OF POLICIES

2.1 Criteria for Identifying Policies

Each certificate issued by Certicámara has an associated OID identifier in the extension, which is detailed in the certificate properties. Through this OID identifier, the issued certificate is linked to the corresponding Certification Policy, which confirms compliance with the described conditions.

2.2 OID of policies

Each type of certificate will be identified by a unique OID (Object Identifier), included in the certificate as a policy identifier, within the certificate's properties

OID	Type of policies
1.3.6.1.4.1.23267.50.1.1	Certificate of Membership to a Company / Entity in local and/or centralized devices.
1.3.6.1.4.1.23267.50.1.2	Certificate of Representation of a Company / Entity in local and/or centralized devices.
1.3.6.1.4.1.23267.50.1.3	Certificate of Public Official in local and/or centralized devices.
1.3.6.1.4.1.23267.50.1.4	Certificate of Professional Title Holder in local and/or centralized devices.
1.3.6.1.4.1.23267.50.1.5	Digital certificate for a natural/legal person in local and/or centralized devices.
1.3.6.1.4.1.23267.50.1.8.5	Digital certificate for a natural person PKCS10.
1.3.6.1.4.1.23267.50.1.8.4	Digital certificate for a legal person PKCS10.

2.3 Types of Certicámara ECD Certificates

To meet the different needs that arise in the context of the growing use of information and communication technologies, Certicámara generates various types of **digital certificates**, which are issued with a maximum validity of two (2) years, in accordance with the Specific Accreditation Criteria in force, which is in conformity with the Certificate Lifecycle section of this document.

2.3.1 Certificate of membership to a company / Entity in local and/or centralized devices.

It is issued to national or foreign natural persons who have been fully identified before Certicámara with valid and current identity document(s) issued by the competent authority of the Republic of Colombia, or with equivalent document(s) issued by the

competent authority of any Foreign State. It allows them to be identified as a natural person, linking them as belonging to a specific business organization or state entity, but without having the legal representation of the same or the power to legally compromise it.

The subscribers of this type of digital certificate are:

1) The natural person who can sufficiently prove, in the opinion of Certicámara, that a legal, labor, or any other relationship exists with the legal person or state entity that will appear on the digital certificate.

2) The legal person that appears on the digital certificate.

- Issuance requirements

  - The applicant must attach the following documents:

    1. Company/entity's Single Tax Registry (RUT): The subscriber will be responsible for updating the address, municipality, and department in the RUT. Individuals residing outside of Colombia who are not registered with the DIAN must attach the document that represents their tax resident status in their country. This document must be validated by the Directorate of Legal and Contractual Affairs, who will provide an opinion for issuing the document.
    2. Identification document of the signature holder: Colombian Citizenship Card, Passport for foreigners, Venezuelan Identity Document (Temporary Protection Permit (PPT), Colombian Alien Identification Card or Colombian Identity Card.
    3. Document proving the existence and legal representation of the company or entity: For companies or entities registered with the Chamber of Commerce, a Certificate of Existence and Legal Representation no older than 30 days is required, and for companies or entities not registered with the Chamber of Commerce, a Certificate issued by a regulatory body, such as the Financial Superintendency, the Superintendency of Industry and Commerce, the Ministry of Education, or mayor's offices, among others. For consortia and temporary unions, the document proving the existence and legal representation is the deed of consortium or temporary union.

  - The applicant must fill out the digital certification services form for the Certificate of Membership to a Company/Entity type, attaching the requested documents at the following link: https://ventadigital.certicamara.com
  - The applicant's identity must be validated according to the mechanisms provided by Certicámara at the time of the request.
  - The information published in the respective certificate includes:

1. Common Name (CN)	Subscriber's Name(s) and Last Name(s)
2. Serial Number	IDigital Certificate Identifier
3. Organization (O)	Social Reason of the Subscriber's Organization
4. 1.3.6.1.4.1.23267.2.1	Agreement Code
5. 1.3.6.1.4.1.23267.2.2	Subscriber's Identification Document Number
6. 1.3.6.1.4.1.23267.2.3	Organization's Identification Number
7. Title (T)	Name of the Subscriber's Position in the Organization
8. Organizational Unit (OU)	Agreement - Certificate Validity - Physical / Virtual Token
9. Street Address (STREET)	Organization's Address
10. Country (C)	Country of Certificate Issuance
11. State Or Province Name (S)	City/Municipality of the Subscriber's Organization
12. Locality (L)	Department of the Subscriber's Organization
13. Surname (SN)	Subscriber's Last Name(s)
14. Given Name (G)	Subscriber's First Name

2.3.2 Certificate of Representation of a Company / Entity in local and/or centralized devices.

It is issued to national or foreign natural persons who have been fully identified before Certicámara with valid and current identity document(s) issued by the competent authority of the Republic of Colombia, or with equivalent document(s) issued by the competent authority of any Foreign State, linking them in the capacity of legal representative of a legal person or State Entity.

The Certificates of Representation of a Company/Entity certify the identity of a natural person, linking them to the legal representation of a legal person or a State Entity.

The Certificates of Representation of a Company/Entity have as their subscriber both the natural person who acts on behalf and legal representation of a legal person, and the

represented legal person that also appears on the digital certificate.

- Issuance requirements

- The applicant must attach the following documents:

1. Company/entity's Single Tax Registry (RUT): The subscriber will be responsible for updating the address, municipality, and department in the RUT. Individuals residing outside of Colombia who are not registered with the DIAN must attach the document that represents their tax residence in their country. This document must be validated by the Directorate of Legal and Contractual Affairs, who will provide an opinion for issuing the document.
2. Identification document of the company owner: Colombian Citizenship Card, Passport for foreigners, Venezuelan Identity Document (Temporary Protection Permit (PPT), Colombian Foreigner's Identity Card, or Colombian Identity Card).
3. Document proving the existence and legal representation of the company or entity: For companies or entities registered with the Chamber of Commerce, a Certificate of Existence and Legal Representation no older than 30 days is required. For companies or entities not registered with the Chamber of Commerce, a Certificate issued by a regulatory body, such as the Financial Superintendency, the Superintendency of Industry and Commerce, the Ministry of Education, or municipal governments, among others. For consortia and temporary unions, the document proving the existence and legal representation is the consortium or temporary union deed.

- The applicant must fill out the digital certification services form for the Certificate of Representation of a Company/Entity type, attaching the requested documents at the following link: https://ventadigital.certicamara.com/

- The applicant's identity must be validated according to the mechanisms provided by Certicámara at the time of the request.
- The information published in the respective certificate includes:

1. Common Name (CN)	Subscriber's Name(s) and Last Name(s) (Legal Representative)
2. Serial Number	Unique Digital Certificate Identifier
3. Organization (O)	Company Name of the Organization to which the Subscriber belongs
4. 1.3.6.1.4.1.23267.2.1	Agreement Code

5. 1.3.6.1.4.1.23267.2.2	Subscriber's Identification Document Number
6. 1.3.6.1.4.1.23267.2.3	Organization Identification Number
7. Title (T)	Name of the Subscriber's Position in the Organization
8. Organizational Unit (OU)	Agreement - Certificate Validity - Physical / Virtual Token
9. Street Address (STREET)	Management of the Organization
10. Country (C)	Country of Certificate Issuance
11. State Or Province Name (S)	City / Municipality of Subscriber's Organization
12. Locality (L)	Underwriter Organization Department
13. Surname (SN)	Subscriber's Last Name(s)
14. Given Name (G)	First Subscriber Name

2.3.3 Certificate of Public Official in local and/or centralized devices.

It is issued to national or foreign natural persons who have been fully identified before Certicámara with valid and current identity document(s) issued by the competent authority of the Republic of Colombia, or with equivalent document(s) issued by the competent authority of any Foreign State. It allows them to be identified as a natural person and links them as a public official belonging to a state entity in the Republic of Colombia.

The subscribers of this type of digital certificate are natural persons who can sufficiently prove, in the opinion of Certicámara, that they have obtained an appointment as public officials, official workers, or are the legal holders of the position of notary, consul, judge of the republic, magistrate, registrar, public servant in the Republic of Colombia, and contractors designated or authorized by a public entity.

The Certificate of Public Official does not guarantee the quality, suitability, or effective fulfillment of the functions in charge of its holder. Certicámara does not guarantee that the subscriber of the Public Official certificate has been subject to disciplinary, administrative, criminal, or any other type of sanctions in the Republic of Colombia or abroad. For the issuance of a Public Official Certificate, Certicámara relies on the documentation exhibited and the declarations made by the subscriber at the time of requesting the service. As long as the law or applicable regulations do not establish otherwise, the request for a Public Official Certificate is not mandatory for Public Officials. The issuance of a Public Official Certificate does not limit the subscriber from requesting other digital certificates.

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

- Issuance requirements

- The applicant must attach the following documents:

1. Single Tax Registry (RUT) of the Notary Public or Urban Curator and/or the entity: It will be the subscriber's responsibility to update the address, municipality, and department in the RUT. Individuals residing outside of Colombia who are not registered with the DIAN must attach the document that represents their tax residence in their country. This document must be validated by the Directorate of Legal and Contractual Affairs, who will provide an opinion for issuing it.
2. Identification document of the signature holder: Colombian Citizenship Card, Passport for foreigners, Venezuelan Identity Document (Temporary Protection Permit (PPT), Colombian Alien Identification Card, or Colombian Identity Card).
3. Document linking the individual to the public entity: Some of the following documents that prove the relationship are: Possession Certificate (Article 2.2.5.1.8 of Decree 1083 of 2015), Employment Certificate, Certificates from the Registry Office for mayors, Contractor Service Provision Contract / SECOPII screenshot.

- The applicant must fill out the digital certification services form for the Certificate of Public Official type, attaching the requested documents at the following link: https://ventadigital.certicamara.com/
- The applicant's identity must be validated according to the mechanisms provided by Certicámara at the time of the request.
- The information published in the respective certificate includes:

1. Common Name (CN)	Subscriber's First Name(s) and Last Name(s)
2. Serial Number	Unique Digital Certificate Identifier
3. Organization (O)	Company Name of the Organization to which the Subscriber belongs
4. 1.3.6.1.4.1.23267.2.1	Agreement Code
5. 1.3.6.1.4.1.23267.2.2	Subscriber's Identification Document Number
6. 1.3.6.1.4.1.23267.2.3	Organization Identification Number
7. Title (T)	Name of the Subscriber's Position in the Organization
8. Organizational Unit (OU)	Agreement / Agreement - Certificate Validity - Physical / Virtual Token *(Depends on the agreement selected for the application)*
9. Street Address (STREET)	Management of the Organization
10. Country (C)	Country of Certificate Issuance

11. State Or Province Name (S)	City / Municipality of Subscriber's Organization
12. Locality (L)	Municipality / City of the Subscriber Organization
13. Surname (SN)	Subscriber's Last Name(s)
14. Given Name (G)	First Subscriber Name

2.3.4 Certificate of Professional Title Holder in local and/or centralized devices.

It is issued to national or foreign natural persons who have been fully identified before Certicámara with valid and current identity document(s) issued by the competent authority of the Republic of Colombia, or with equivalent document(s) issued by the competent authority of any Foreign State. It identifies them as a natural person, linking them to the obtaining of a professional title duly recognized in the Republic of Colombia or in a Foreign State, and who have obtained the corresponding registration, license, college, or professional card required for the exercise of their profession in the Republic of Colombia or in a Foreign State.

The subscribers of this type of digital certificate are natural persons who can sufficiently prove, in the opinion of Certicámara, that they have obtained a professional title duly recognized in the Republic of Colombia or in a Foreign State validated by the Ministry of National Education, and who have obtained the corresponding registration, license, college, or professional card required for the exercise of their profession in the Republic of Colombia or in a Foreign State.

- Issuance requirements

  - The applicant must attach the following documents:

1. Unique Tax Registry (RUT) of the professional and/or company/entity: It will be the subscriber's responsibility to update the address, municipality, and department in the RUT. Individuals residing outside of Colombia who are not registered with the DIAN must attach the document that represents their tax residence in their country. This document must be validated by the Directorate of Legal and Contractual Affairs, who will provide an opinion for issuing the document.
2. Identification document of the signature holder: Colombian Citizenship Card, Passport for foreigners, Venezuelan Identity Document (Temporary Protection Permit [PPT]), Colombian Alien Identification Card, or Colombian Identity Card.
3. Certificate of Qualified Professional: Applies to technicians, technologists, and university graduates. Law 30 of 1992, concept 059 881 of the Administrative Department of the Civil Service, such as: Professional Card, Diploma, degree certificate or professional registration, Professional Degree Certification. For professionals with a degree from another country, the document must be validated by the Ministry of National Education.

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

- The applicant must fill out the digital certification services form for the Certificate of Professional Title Holder type, attaching the requested documents at the following link: https://ventadigital.certicamara.com/

- The applicant's identity must be validated according to the mechanisms provided by Certicámara at the time of the request
- The information published in the respective certificate includes:

1. Common Name (CN)	Subscriber's First Name(s) and Last Name(s)
2. Serial Number	Unique Digital Certificate Identifier
3. Organization (O)	Company Name of the Organization to which the Subscriber belongs / Subscriber's First Name(s) and Last Name(s). *(Depends on the information entered in the application*)
4. 1.3.6.1.4.1.23267.2.1	Agreement Code
5. 1.3.6.1.4.1.23267.2.2	Subscriber's Identification Document Number
6. 1.3.6.1.4.1.23267.2.3	Organization ID Number / Subscriber ID Number with or without check digit*(Depends on the information entered in the application*)
7. Title (T)	Name of Subscriber's Profession
8. Organizational Unit (OU)	Agreement - Certificate Validity - Physical / Virtual Token
9. Street Address (STREET)	Organization's Address / Subscriber's Address*(Depends on information entered in application*)
10. Country (C)	Country of Certificate Issuance
11. State Or Province Name (S)	City / Municipality of the organization / Subscriber*(Depends on the information entered in the application*)
12. Locality (L)	Department of the Organization / Subscriber (*Depends on the information entered in the application*)
13. Surname (SN)	Subscriber's Last Name(s)
14. Given Name (G)	First Subscriber Name

2.3.5 Digital certificate for a natural person / legal person in local and/or centralized devices.

It is issued to national, foreign natural persons, or legal persons who have been fully identified before Certicámara with valid and current identity document(s) issued by the

competent authority of the Republic of Colombia, or with equivalent document(s) issued by the competent authority of any Foreign State.

The Certificates for a Natural Person / Legal Person have as their subscriber the natural person or legal person who, acting on their own behalf, can sufficiently prove, in the opinion of Certicámara, their identity through the exhibition of the documentation that proves it.

- Issuance requirements

  - The applicant must attach the following documents:
    1. Unique Tax Registry (RUT) of the natural or legal person or equivalent document certifying the address (Applies to natural persons): It will be the subscriber's responsibility to update the address information (address, municipality and department) in the RUT. Individuals domiciled outside of Colombia who are not registered with the DIAN must attach the document that acts as a tax resident in their country, which must be validated by the Directorate of Legal and Contractual Affairs, who will provide a concept for issuing it. An equivalent document certifying the address of the natural person, such as: Lease agreement, utility bill, residence certificate issued by the municipal authority, must be validated by the Directorate of Legal and Contractual Affairs, who will provide a concept for issuing it.
    2. Identification document of the signature holder: Colombian Citizenship Card, Passport for foreigners, Venezuelan Identity Document (Temporary Protection Permit (PPT), Colombian Alien Identification Card or Colombian Identity Card.
    3. Document that proves the existence and legal representation of the company or entity (Applies to Legal Entity): Certificate of existence and legal representation no older than thirty (30) days (Companies or entities registered in the Chamber of Commerce), Deed of consortium or temporary union formation (Consortiums and temporary unions) or certificate issued by the corresponding control body, for example: Financial Superintendence, Superintendence of Industry and Commerce, Superintendence of Surveillance, Superintendence of Health, Superintendence of Family Subsidy, Ministry of Education, Mayors' Offices, District Ombudsmen's Offices, Governors' Offices, Ecclesiastical entities, Indigenous territorial entities (Deed) (Companies or entities not registered in the Chamber of Commerce).

  - The applicant must fill out the digital certification services form for the Natural Person / Legal Person digital certificate type, attaching the requested documents at the following link: https://ventadigital.certicamara.com/
  - The applicant's identity must be validated according to the mechanisms provided by Certicámara at the time of the request.
    For legal and natural persons obligated to issue electronic invoices, Certicámara S.A. will provide a platform for the generation of the request, key

pairing, and other aspects related to the signature request. According to the above, the applicant will be responsible for the information contained in the Request when using their own tool to make the request. Certicámara, with its information systems, will validate that the information contained is identical to that provided in the digital certificate request.

- The information published in the respective certificate for a Natural Person Certificate includes:

1. Common Name (CN)	Subscriber's First Name(s) and Last Name(s)
2. Serial Number	Unique Digital Certificate Identifier
3. Organization (O)	Subscriber's First Name(s) and Last Name(s)
4. 1.3.6.1.4.1.23267.2.1	Agreement Code
5. 1.3.6.1.4.1.23267.2.2	Subscriber's Identification Document Number
6. 1.3.6.1.4.1.23267.2.3	Subscriber's ID Number (with or without verification digit) *(Depends on the information entered* in *the application*)
7. Title (T)	Natural Person
8. Organizational Unit (OU)	Agreement - Validity of the Certificate - Physical / Virtual Token
9. Street Address (STREET)	Subscriber's Address
10. Country (C)	Country of Certificate Issuance
11. State Or Province Name (S)	City / Municipality of Subscriber
12. Locality (L)	Subscriber's Department
13. Surname (SN)	Subscriber's Last Name(s)
14. Given Name (G)	First Subscriber Name

2.3.6 Digital certificate for a natural person / legal person PKCS#10.

It is issued to national, foreign natural persons, or legal persons who have been fully identified before Certicámara with valid and current identity document(s) issued by the competent authority of the Republic of Colombia, or with equivalent document(s) issued by the competent authority of any Foreign State.

The Certificates for a Natural Person / Legal Person have as their subscriber the natural person or legal person who, acting on their own behalf, can sufficiently prove, in the opinion

of Certicámara, their identity through the exhibition of the documentation that proves it.

- Issuance requirements

  - The applicant must attach the following documents:

    1. Unique Tax Registry (RUT) of the natural or legal person or equivalent document certifying the address (Applies to natural persons): It will be the subscriber's responsibility to update the address information (address, municipality and department) in the RUT. Individuals domiciled outside of Colombia who are not registered with the DIAN must attach the document that acts as a tax resident in their country, which must be validated by the Directorate of Legal and Contractual Affairs, who will provide a concept for issuing it. An equivalent document certifying the address of the natural person, such as: Lease agreement, utility bill, residence certificate issued by the municipal authority, must be validated by the Directorate of Legal and Contractual Affairs, who will provide a concept for issuing it.
    2. Identification document of the signature holder: Colombian Citizenship Card, Passport for foreigners, Venezuelan Identity Document (Temporary Protection Permit (PPT), Colombian Alien Identification Card or Colombian Identity Card.
    3. Documents with end customer (invoicing) data: This requirement applies when used for electronic invoicing.
    4. Document that proves the existence and legal representation of the company or entity (Applies to Legal Entity): Certificate of existence and legal representation no older than thirty (30) days (Companies or entities registered in the Chamber of Commerce), Deed of consortium or temporary union formation (Consortiums and temporary unions) or certificate issued by the corresponding control body, for example: Financial Superintendence, Superintendence of Industry and Commerce, Superintendence of Surveillance, Superintendence of Health, Superintendence of Family Subsidy, Ministry of Education, Mayors' Offices, District Ombudsmen's Offices, Governors' Offices, Ecclesiastical entities, Indigenous territorial entities (Deed) (Companies or entities not registered in the Chamber of Commerce).

  - The applicant must fill out the digital certification services form for the Natural Person / Legal Person digital certificate type, attaching the requested documents at the following link:https://ventadigital.certicamara.com/
  - The applicant's identity must be validated according to the mechanisms provided by Certicámara at the time of the request.
  - For legal and natural persons obligated to issue electronic invoices, Certicámara S.A. will provide a platform for the generation of the request, key pairing, and other aspects related to the signature request. According to the above, the applicant will be responsible for the information contained in the Request when using their own tool to make the request. Certicámara, with its

information systems, will validate that the information contained is identical to that provided in the digital certificate request.

- The information published in the respective certificate for a Natural Person / Legal Person PKCS#10 Certificate includes:

1. Common Name (CN)	Company name of the Organization
2. Serial Number	Unique Digital Certificate Identifier
3. Organization (O)	Company name of the Organization
4. 1.3.6.1.4.1.23267.2.2	Subscriber Identification Number
5. 1.3.6.1.4.1.23267.2.3	Organization Identification Number
6. Organizational Unit (OU)	Certificate Usage
7. Street Address (STREET)	Subscriber's Address
8. Country (C)	Country of Certificate Issuance
9. State Or Province Name (S)	City / Municipality of the Organization
10. Locality (L)	Subscriber's Department
11. Surname (SN)	Subscriber's Last Name(s)
12. Given Name (G)	First Subscriber Name

3. OPERATIONAL REQUERIMENT OF THE CERTIFICATE LIFECYCLE

3.1 Certificate request

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

1. In person at Certicámara's facilities.
2. Through the Contact Center.
3. Or by any other electronic means provided by Certicámara.

Received requests will be reviewed by the Registration Authority (RA), in accordance with the specific accreditation criteria established by ONAC and those defined internally by Certicámara. This review will be carried out within a maximum period of two (2) business days, counted from the reception of all 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 issuance, which will take place 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 submitted in another language, it must be accompanied by an official translation performed by a translator endorsed by the Ministry of Foreign Affairs. The documentation will be retained 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 Certicámara S.A.'s digital signature certificate, the applicant fully and unreservedly accepts the following documents, which are an integral part of this CPS 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 Certicámara S.A.'s organizational policies, 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, along with the general service contracting conditions.

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

a) **Reading 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 Certification Practice Statement (CPS), the Certification Policy (CP), and the personal data processing policy.

b) **Information Verification**: 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) **Information Provision**: 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, ensuring that these do not have 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, and therefore, by submitting this data, the sending of such notifications is authorized for this purpose.

d) **Password Assignment**: To use the digital certificate, the holder must 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**: Since Certicámara S.A. does not have mechanisms for its recovery, as 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 using the digital signature certificate. Being informed about the characteristics of Certicámara S.A.'s certificate, its level of reliability, the limits of responsibility, the client's obligations, and the necessary security measures for its use.

f) **Right to Refuse Service:** Be aware that Certicámara S.A. may reserve the right not to issue a digital signature certificate due to technical conditions, without this generating any liability.

g) **Identity Validation by Certicámara S.A.:** Certicámara S.A., as an Open Digital Certification Entity, will previously verify identity 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 submission 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 health social security 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 perform 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, stating the reasons.

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

3.1.1 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 this status is proven 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 proves the representation in accordance with current civil regulations

3.2 Certificate Issuance

3.2.1 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 downloads/activates the digital signature. Under no circumstances will a certificate be issued with a validity period that precedes the current date.

3.2.2 Notification to the subscriber by the CA of certificate issuance

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

3.2.3 Private key restoration

In the case of digital signature certificates on a virtual device, Certicámara has implemented secure mechanisms that allow the subscriber to manage the change or reset of their password, through the contact center, which does not generate an associated cost, up to a maximum of ten (10) requests, subsequently, this will have a cost. In the case of a digital signature certificate on a physical device, the subscriber may change it whenever required directly from the application, in case of loss or forgetting the password, they must carry out the process of acquiring a new signature.

3.3 Delivery of the digital certificate to subscribers via physical medium

3.3.1 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 through direct delivery by a Certicámara logistics team member. In both scenarios, the physical device will be delivered, and the link to the instructions for downloading will be shared in the approval email sent to the holder.

3.3.2 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 provided in the request form. When the holder authorizes a third party to collect the device at Certicámara's facilities, the holder must send an email to logistica@certicamara.com prior to delivery. The logistics operator's tracking number 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.

3.3.3 Delivery management time - Physical Certificates

In Bogotá and nearby municipalities, the delivery time from the issuance of the certificate to the delivery to the applicant will be approximately two (2) business days.

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 delivery is not possible due to reasons 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 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 the holder requires the digital signature after this period, they must initiate a new request process, which will generate a cost according to Certicámara's policies.

3.3.4 Download time

Once the signature certificate application has been approved, the holder will automatically receive an email with the download link, a detailed manual and important recommendations. They will have ninety (90) calendar days to complete this process. Otherwise, the asset will be deemed abandoned and Certicámara will permanently block the link. In this case, if you wish to obtain the signature certificate, you must initiate a new application process, which will incur a fee based on Certicámara's rates.

3.4 Certificate Acceptance

A confirmation from the subscriber is not required as an 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 applicable.

3.4.1 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 PKI's LDAP (Lightweight Directory Access Protocol) directory structure at the moment the certificate is issued. In case of any technical difficulty that hinders its publication, it will be carried out within one month following the date of issuance of the certificate, in accordance with the conclusions of the technical analysis that prevented its timely publication.

3.4.2 *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 can consult 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.

3.5 Use of key pairs and certificates

3.5.1 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 standardized protection profile for a secure certification authority electronic signature device, in accordance with FIPS 140-2 Level 3 or higher security level, and the creation of the CA keys uses a pseudo-random number generation algorithm.

3.5.2 Use of the subscriber's certificate and private key

The Identification of policies section of this document details the uses and purposes for each of the types of certificates issued by Certicámara.

3.5.3 *Use of the trusting user's certificate and public key*

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

3.5.4 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.

3.6 Certificate Renewal

3.6.1 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. This notification may be made via email to the address provided by the subscriber or through any other suitable communication means that Certicámara deems appropriate. However, it is not an obligation for Certicámara to ensure the effectiveness of the notification about the certificate's validity expiration 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.

3.6.2 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.

3.6.3 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).

3.6.4 Notification of new certificate issuance to the subscriber

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

3.7 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.

3.8 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.

3.9 Certificate Revocation and Suspension

The revocation of a digital certificate constitutes the mechanism by which an issued certificate is disabled, ending its period of validity, either due to the expiration of its term or

upon the occurrence of any of the revocation events stipulated in this Certification Practice Statement. It should be noted that revocation does not have any associated cost.

Certicámara does not handle the suspension status for its digital certificates.

3.9.1 Reasons for revocation

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:

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

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

c) The private key has been exposed or is at risk of misuse.

d) Due to the death of the subscriber.

e) Due to the subsequent incapacity of the subscriber.

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

g) Due to the updating of the information contained in the digital certificate.

h) 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 Certification Practice Statement.

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 of the digital certificate by the subscriber.

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) In cases where 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 Certification Practice Statement.

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

3.9.2 Who can request revocation?

The subscriber is empowered to voluntarily request the revocation of their digital certificate at any time. This request can 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 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 time of validity. For this purpose, the previously supplied documentation will be used, in order not to affect the availability of the service.

3.9.3 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 Certicámara's 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 it is not the subscriber or if they are but cannot be satisfactorily identified, they may 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 where it applies, without prejudice to Certicámara providing the measures established for the security of the Digital Certification System. It is clarified that once the revocation request is received and the veracity of 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 head or person 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 certificate suspension service to subscribers.

3.9.4 Revocation request grace period

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

3.9.5 CRL issuance frequency

The publication of the Certicámara Subordinate CA Certificate Revocation List (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.

3.9.6 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 minimum availability agreement of 99.8%. Certicámara has the history of revoked certificates from the beginning of the service provision.

3.9.7 Online revocation verification requirements

The online certificate status verification must be carried out using the OCSP service in accordance with 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 AV, 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

3.9.8 Suspension circumstances

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

3.10 Replacement of Digital Signature Certificates

Certicámara 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 Certification Practice Statement, the Certification Policy, and the values established in these documents.

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.

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 3.1 of this Certification Policy.
- 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, requesting the replacement of certificates and justifying it under one of the following reasons:

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

The contract holder will then send this request to the operations area at the email revocaciones@certicamara.com, where the certificate to be replaced must be indicated, as well as the corresponding revocation information. Based on the information provided, the entity's quotas will be controlled.

3.10.1 Reasons for Replacement

Certicámara will carry out the replacement of the digital signature certificate in accordance with the previous numeral, when any of the following reasons occur:

i. Loss of the physical device.
ii. Exposure of the PIN (Password/key) of the digital certificate.
iii. Change in the information of the previously issued digital certificate (Does not apply to a change in identification number).
iv. Change in the company's social reason regardless of whether it keeps the same NIT.
v. Due to an error attributable to Certicámara.

Additionally, 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 initially agreed conditions.

3.11 Certificate Characteristics

3.11.1 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 AV, 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?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_4096.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_409 6.crl?crl=crl

3.11.2 Service availability

The certificate status checking service is available 24 hours a day, 365 days a year. The

minimum availability level will be 99.8%.

3.11.3 Optional functions

To use the online validation service by consulting the addresses http://ocsp.certicamara.com 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.

3.12 End of subscription

The termination 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.

3.13 Key custody and recovery

3.13.1 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.

4. USES OF CERTIFICATES

4.1 Appropriate uses of the digital 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 the 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 may only give digital certificates the uses specified in the contract they sign with Certicámara individually, those permitted in this Certification Practice Statement, in the Certification Policies, and those permitted under Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014). The contract 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 Certification Practice Statement 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 announced 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 sole 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.

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) Any use of digital certificates whose purpose is contrary to Colombian legislation, international agreements signed by the Colombian State, supranational norms, good customs, sound commercial practices, and everything contained in this Certification practice statement and in the contracts signed between Certicámara and the Subscriber is strictly prohibited.
c) Any use of digital certificates whose purpose is to violate any intellectual property right of Certicámara or third parties is prohibited.
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.

4.3 Validity of certificates

Certicámara issues various types of digital certificates, which are issued with a maximum validity of two (2) years, which is equivalent to 730 days, in accordance with current regulations.

5. CHARACTERISTICS OF CERTIFICATES

5.1 Digital certificate on physical token

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

It corresponds to a physical device that is connected to the USB port of the computer, which contains the digital certificate and the pair of public and private keys. It is also protected by a fixed key to enforce its use. It is not required to have the equipment connected to the Internet service to use it. It is the customer's responsibility to safeguard the device delivered, as well as the management of the respective password.

Certicámara committed to the management of the environmental impact of physical storage devices delivered to customers, will make available to users:

1. A new physical token delivery option which has undergone a reconditioning process of physical and functional review of high standards.
2. A secure deletion process has been practiced to remove the previous digital certificate, in accordance with the application functionalities provided by the supplier.
3. This new process ensures that the physical token meets the appropriate usability and technological performance conditions.

i. *Technical aspects*

✔ Key length of 4096 bits.

✔ Certificate signature algorithm with RSA-SHA-2 256-2056 hash.

✔ Compatibility with API and standards (PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE MS minidriver, CNG).

✔ Memory capacity 80K. With retention of at least 10 years.

✔ Dimensions: 5110 - 16.4mm *8.5mm*40.2mm.

✔ Compatible with ISO 7816-1 and 4 specifications.

✔ Molded rigid plastic, anti-tamper closure.

✔ Windows (Server 2008/R2 Server 2012/R2, 7, 8 and 10).

✔ Linux.

✔ USB connector.

ii. *Care of the cryptographic device*

✔ Operating temperature 0 °C a 70 °C (32 °F a 158 °F)

✔ Storage temperature -40°C a 85 °C (-40°F a 185 °F)

✔ Humidity range 0- 100% sin condensación

✔ Water resistance certification IPX7 – IEC 60529

For the assignment of keys by the subscriber, the following recommendations and care for their protection must be taken into account:

✔ The password must be for personal use and should not be transferred to a third party.

✔ Store your password in a safe place, it is recommended to memorize it to prevent others from knowing it.

✔ Do not leave the device connected to the computer when not in use.

✔ Disconnect the device correctly.

✔ Avoid bumps and drops.

✔ Use the applications provided by Certicámara for the use of your certificate

iii. Associated risks

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

✔ Fluctuations outside the normal environmental operating ranges, such as: voltage and 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 NIST.FIPS.140-2.pdf

5.2 Certificate in virtual token

This corresponds to an infrastructure provided as a service in which the issued digital certificates, along with their key pair, are kept in custody in Certicámara's technological infrastructure. They are associated with a username and password given by the certificate holder. For its use, an active Internet connection must be available.

i. Characteristics

✔ rivate key of 4096 bits.

✔ Certificate signature algorithm with SHA256 hash.

✔ X.509 v3 certificates.

✔ Storage in an infrastructure that complies with FIPS 140-2 Level 3.

✔ Signature of files signed with the document's hash (does not require sending the document to protect its confidentiality).

- ✔ Network access to the domain *.certicamara.com through port 443.
- ✔ Signature component that allows the consumption of Certitoken.
- ✔ Minimum Java in Ver 7.
- ✔ Windows 7 or higher.
- ✔ Framework 4.0 or higher.

ii. Device care

Physical and technological care of the datacenter where the HSM is located, to ensure its proper functioning, where controls can be found for humidity, electricity, unauthorized access, fire detectors, biometric security for access to the rack and the datacenter area, among others.

For the assignment of keys by the subscriber, the following recommendations and care for their protection must be taken into account:

- ✔ The password must contain between eight (8) and twelve (12) alphanumeric characters, using uppercase and lowercase letters.
- ✔ The password must be for personal use and should not be transferred to a third party.
- ✔ Store your password in a safe place, it is recommended to memorize it to prevent others from knowing it.

iii. Associated risks

For the certificate in a virtual token, the risks to which it is exposed are those in which environmental aspects prevent the proper functioning of the datacenter where the HSM is installed. In logical matters, the associated risks are defined by cyber attacks that prevent the respective access and/or availability.

5.3 Digital certificate in PKCS#10

This corresponds to a standard for the generation of public and private keys from the signatory's infrastructure and under their responsibility, for the purpose of being certified by a digital certification entity.

i. Characteristics

- ✔ Public key of 4096 bits.
- ✔ Certificate signature algorithm with SHA256 hash.

✔ Public key signed in *.CER format in accordance with the Certicámara trust chain.

✔ Issuance using the PKCS#10 standard.

✔ Generate a Certificate Signing Request - CSR - in PKCS#10 format.

✔ Ability to receive and use the public key in .CER format.

ii. Device care

Physical and technological care of the datacenter where the HSM is located, to ensure its proper functioning, where controls can be found for humidity, electricity, unauthorized access, fire detectors, biometric security for access to the rack and the datacenter area, among others.

For the assignment of keys by the subscriber, the following recommendations and care for their protection must be taken into account:

✔ The password must contain between eight (8) and twelve (12) alphanumeric characters, using uppercase and lowercase letters.
✔ The password must be for personal use and should not be transferred to a third party.
✔ Store your password in a safe place, it is recommended to memorize it to prevent others from knowing it.

iii. Associated risks

For the certificate in PKCS#10, the risks to which it is exposed are those in which environmental aspects prevent the proper functioning of the datacenter where the HSM is installed. In logical matters, the associated risks are defined by cyber attacks that prevent the respective access and/or availability.

6. OBLIGATIONS AND RESPONSIBILITIES OF THE INTERVENERS

The obligations and responsibilities of the interveners are defined in the Certification Practice Statement document in numeral 9.5.

7. RIGHTS OF THE INTERVENERS

The rights of the interveners are defined in the Certification Practice Statement document in numeral 9.7.

8. RELIABILITY OF SIGNATURES AND DIGITAL CERTIFICATES

Certicámara's Digital Certification System is a system built based on the strict compliance with its policies and procedures. The trust it generates in its interveners depends directly on the compliance with them. All interveners must provide all the

collaboration within their reach for the generation of the trust inherent to the digital certification system, following the established policies and procedures at all times.

a. Reliability of digital signatures

The relying party, before being able to trust a digital signature certified by Certicámara, has the duty to strictly follow the indications specified below:

1. The relying party must determine the reliability of the digital certificate, in accordance with the stipulations in the following section.
2. The relying party must verify that the digital signature was created within the validity period of the digital certificate and that it has not been revoked.
3. The relying party must take into account all other policies and procedures that govern Certicámara's activity and that are specified in its Certification Practice Statement.

b. Reliability of the digital certificate

The relying party must follow the indications listed below if it intends to trust a digital certificate issued by Certicámara:

- The relying party must verify that the digital certificate has not expired, in accordance with the validity date that appears on it.
- The relying party must verify that the digital certificate is not in Certicámara's database of revoked digital certificates which is published on Certicámara's website. In any case, and without any exception, it is prohibited to determine the revocation status of a digital certificate based on information other than that of the database of revoked digital certificates.
- The reliability of the digital certificate depends on it being digitally signed by Certicámara. The relying party can verify Certicámara's digital signature by verifying it with the root certificate, which contains Certicámara's public key, which is available on Certicámara's website.

The use of a digital certificate by any intervener in the Digital Certification System is subject to the strict adherence to the rules contained in:

- The contract signed with each subscriber of the digital certification service, which contains the general conditions for contracting Certicámara S.A.'s digital certification services, whose clauses are found in the request form (https://ventadigital.certicamara.com/).
- This Certification Practice Statement in relation to digital signatures issued through its digital certificates. The relying party must take them into account whenever it intends to trust a digital certificate.

9. 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 perform 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 provided by the subscriber will be disclosed, in accordance with current regulations. The confidential information of the digital certification services subscriber may be disclosed at their request, in their capacity as the owner of this information.

9.1 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 persons with whom Certicámara has a duty of secrecy 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

9.2 Information 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 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 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.

9.4 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 so that the holders can 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 their 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 its website, at the following online location: https://web.certicamara.com/politicas

9.5 Disclosure by virtue of a judicial or administrative process

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.

10. FEES FOR THE DIGITAL CERTIFICATE ISSUANCE SERVICE

The value that CERTICÁMARA sets for the provision of Digital Signature Certificate Services is established in accordance with the contractual conditions agreed upon with the service applicants and will be adequately calculated and liquidated by CERTICÁMARA.

The fee for the provision of the Digital Signature Certificates service will be established based on the client's needs and in accordance with the volume of digital signature certificates that the client requires, with the following base public sale prices:

Producto	Artículo	Tipo	Precio
Digital Certificate Physical Token	Digital Certificate Natural Person, valid for one (1) year.	Unit	$ 336,000
	Digital Certificate Natural Person, valid for two (2) years.	Unit	$ 458,000

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

Producto	Artículo	Tipo	Precio
	Digital Certificate of Company Membership, valid for one (1) year.	Unit	$ 336,000
	Digital Certificate of Membership in a Company, valid for two (2) years.	Unit	$ 458,000
	Professional Digital Certificate, valid for one (1) year.	Unit	$ 336,000
	Professional Digital Certificate, valid for two (2) years.	Unit	$ 458,000
	Digital Certificate of Legal Representation, valid for one (1) year.	Unit	$ 336,000
	Digital Certificate of Legal Representation, valid for two (2) years.	Unit	$ 458,000
	Replenishment Validity (1) one year without a token	Unit	$ 336,000
	Replenishment Validity (2) two years without token	Unit	$ 458,000
Digital Certificate Physical Token (Reuse)	Digital Certificate Natural Person, validity (1) one year	Unit	$ 285,000
	Digital Certificate Natural Person, valid for (2) two years	Unit	$ 370,000
	Digital Certificate of Company Membership, valid for (1) one year	Unit	$ 285,000
	Digital Certificate Belonging to a Company, valid for (2) two years	Unit	$ 370,000
	Digital Certificate for Qualified Professional, valid for one year (1)	Unit	$ 285,000
	Digital Certificate of Qualified Professional, valid for (2) two years	Unit	$ 370,000
	Legal Representation Digital Certificate, valid for (1) one year	Unit	$ 285,000
	Digital Certificate of Legal Representation, valid for (2) two years	Unit	$ 370,000
	Digital Certificate Public Function, valid for one (1) year.	Unit	$ 256,000

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

Producto	Artículo	Tipo	Precio
Certitoken Digital Certificate	Digital Certificate Public Function, valid for two (2) years.	Unit	$ 331,000
	Digital Certificate Natural Person, valid for one (1) year.	Unit	$ 256,000
	Digital Certificate Natural Person, valid for two (2) years.	Unit	$ 331,000
	Digital Certificate of Company Membership, valid for one (1) year.	Unit	$ 256,000
	Digital Certificate of Membership in a Company, valid for two (2) years.	Unit	$ 331,000
	Professional Digital Certificate, valid for one (1) year.	Unit	$ 256,000
	Professional Digital Certificate, valid for two (2) years.	Unit	$ 331,000
	Digital Certificate of Legal Representation, valid for one (1) year.	Unit	$ 256,000
	Digital Certificate of Legal Representation, valid for two (2) years.	Unit	$ 331,000
	Replenishment Validity (1) one year	Unit	$ 256,000
	Replenishment Validity (2) two years	Unit	$ 331,000
PKCS#10 Digital Certificate	Digital Certificate Natural Person / Legal entity, valid for one (1) year.	Unit	$ 656,000
	Digital Certificate Natural Person / Legal entity, valid for two (2) years.	Unit	$ 953,000
	Replenishment Validity (1) one year	Unit	$ 656,000
	Replenishment Validity (2) two years	Unit	$ 953,000

- The price for the renewal of digital signature certificates corresponds to the same one mentioned in the table above.

- The prices established above do not include IVA.
- The indicated rates may vary according to special commercial agreements with entities and subscribers or due to the development of promotional campaigns.
- It is determined that the validity of a one-year certificate is 365 calendar days.

Applicants will have the possibility of obtaining the applicable rates through the following link https://ventadigital.certicamara.com/, where, depending on the data entered by the applicant and in accordance with the project and/or agreement they belong to, the respective rate will be liquidated.

11. MODELS AND MINUTES OF THE TERMS AND CONDITIONS DOCUMENTS

The model of terms and conditions for the subscription that Certicámara uses in the provision of the digital signature certificate service is available at the following link: https://ventadigital.certicamara.com/.

In case of particular commercial situations with the client, a contract detailing these situations may be signed between Certicámara and the client.

12. ASSOCIATED REGULATIONS

The digital signature certificates 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/

13. CHANGE CONTROL

Date	Reason for update
07/09/2022	• In compliance with the provisions of Chapter 48 of DURSCIT, Article 2.2.2.2.48.3.1. Declaration of Certification Practices (DPC) and the RFC 3647 standard, aligning the paragraphs with the provisions of these documents and creating this document to provide greater clarity to the applicant and subscriber on the provisions, information, guidelines, controls and other applicable for the digital signature certificate service. Taking into account the above, a new code and version of the document is assigned according to the organization's process structure.

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

Date	Reason for update
28/09/2022	o The following changes are made to the document: • Care for the protection of physical, virtual and PKCS#10 cryptographic devices. • Information published in the templates for each policy. • Information for private key restoration and key pair generation and installation.
31/10/2022	✔ Section 9.3 Security systems to protect information is included, where the procedures defined to protect the information gathered in the issuance of certificates are reported.
16/02/2023	The following changes are made to the document: ✔ Update of fees for 2023. ✔ Inclusion of item 3.10 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. ✔ The definition of Reuse as a means of delivery of physical tokens is included.
21/07/2023	The following adjustments are made to the document: ✔ Clarity that the information in the OID'S of address, city / municipality and department of all policies, will be the one reported in the RUT. ✔ Update of certificate fees: Physical Digital Token, Physical Digital Token (reuse) and Digital Certitoken. ✔ Update of the URLs of the new 4026 distribution points for the list of revoked CRL certificates.
18/09/2023	The following adjustments are made to the document: ✔ Updating of the channels for certificate request. ✔ In section *"2.3 Types of ECD Certicámara certificates"* the required documents by type of policy are specified. ✔ In the policy *"2.3.5 Digital Certificate Natural Person / Legal Person"* clarity is provided regarding the platform available for the generation of the request, key binding and other aspects related to the signature request. As well as the responsibility of the subscriber in the certificate issued under this modality. ✔ In the numeral *"3.1 Certificate request"* clarity is given regarding the temporary suspension of digital signature

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

Date	Reason for update
	certificates in Mac OS operating system.
15/01/2024	The following changes are made to the document: • In the numeral *"3.1 Certificate Application"* the full acceptance, without reservations and in its entirety of the Terms and Conditions of the service, 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 is included. Likewise, the identity validation that will be performed to the applicant during the application process. • Clarification in the numeral *"3.6.1 Times for renewal"* that the issuance of a new digital certificate implies prior acceptance of the Terms and Conditions of the service, of the Declarations and Commitments regarding the prevention of money laundering, financing of terrorism, financing of the proliferation of weapons of mass destruction, corruption and transnational bribery and the validation of identity in the registration of a new application. • Update of fees for the year 2024.
18/03/2024	The following adjustments are made to the document: • Elimination of the request requirement "Labor certificate when the technical contact is different from the legal representative (Applies Legal Person and when the use of the signature is different from electronic invoicing) PN requirements". • In numeral 3.1 certificate request, it is clarified that identity validation is part of the requirements to be met by the subscriber. • Updating of the links according to the changes in the web page. • Update of the regulations applied to each service.

POLICY FOR CERTIFICATION - DIGITAL SIGNATURE CERTIFICATE

Date	Reason for update
09/09/2024	The following adjustments are made to the document: • Update of the delivery management times of digital certificates in physical media. • Update of the key length 4096 bits in the issuance of digital certificates. • Inclusion of policies: Digital certificate for natural person PKCS#10 and Digital certificate for legal person PKCS#10.
05/08/2025	The following adjustments are made to the document: • Comprehensive editorial adjustments to provide greater clarity and precision in the information. • Adjustments to the approval procedure for changes to the DPC. • Adjustments to the download time conditions. • Inclusion of the free digital certificate revocation procedure. • Elimination of the national toll-free number. • Link updates. • Elimination of the national toll-free number. • Elimination of the "Subscriber Refund Policies" section, as these conditions are established in the Certification Practices Statement across all products. • Updates to rates.
26/09/2025	The following changes have been made to the document: • Clarification in the requirements section for each policy as to whether the RUT corresponds to a natural person or a legal entity. • Clarification of the documents equivalent to the RUT for applying for a natural person digital certificate. • Adjustment of the guidelines for resetting the virtual token password, which is free of charge for up to ten requests. • Clarification that the timeframe for downloading the digital certificate is ninety (90) calendar days.