certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certicámara.

Certification Policy - Digital Signature Certificate

certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

Table of Contents

1. INTRODUCTION **5**
1.1 Document Title and Identification 5
1.2 Scope 5
1.3 Policy Update and Approval Procedure 6
1.4 Publication Responsibilities 6
2. POLICY IDENTIFICATION **6**
2.1 Policy Identification Criteria 7
2.2 Policy OIDs 7
2.3 Certicámara CA Certificate Types 7
2.3.1 Company / Entity Affiliation Certificate on local and/or centralized devices. 7
2.3.2 Company / Entity Representation Certificate on local and/or centralized devices. 9
2.3.3 Public Office Holder Certificate on local and/or centralized devices. 10
2.3.4 Licensed Professional Certificate on local and/or centralized devices.. 12
2.3.5 Natural Person Digital Certificate on local and/or centralized devices. 13
2.3.6 Natural Person / Legal Entity Digital Certificate 15
3. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFECYCLE **16**
3.1 Certificate Application 16
3.1.1 ¿Who can submit a certificate application? 19
3.2 Certificate Issuance 19
3.2.1 CA Actions During Certificate Issuance 19
3.2.2 Notification to the Subscriber by the Issuing CA of Certificate Issuance 20
3.2.3 Private Key Restoration 20
3.3 Physical Delivery of the Digital Certificate to Subscribers 20
3.3.1 Coverage 20
3.3.2 Delivery Requirements 20
3.3.3 Delivery Management Time – Physical Certificates 21
3.3.4 Download Timeframe 21
3.4 Certificate Acceptance 21
3.4.1 Certificate Publication by the CA 21
3.4.2 Notification of Certificate Issuance by the CA to Other Entities 22
3.5 Use of Key Pairs and Certificates 22
3.5.1 Generation and Installation of Key Pairs 22
3.5.2 Use of Certificate and Private Key of the Subscriber 22
3.5.3 Use of the Certificate and Public Key of the Relying Party 22

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

3.5.4 Private Key Destruction Method 22
3.6 Certificate Renewal 23
3.6.1 Renewal Timeframes 23
3.6.2 ¿Who can request a renewal? 23
3.6.3 Processing of Certificate Renewal Applications 23
3.6.4 Notification of New Certificate Issuance to the Subscriber 23
3.7 Certificate Key Renewal 23
3.8 Certificate Modification 24
3.9 Certificate Revocation and Suspension 24
3.9.1 Grounds for Revocation 24
3.9.2 ¿Who can request a revocation? 25
3.9.3 Revocation Request Procedure 25
3.9.4 Grace Period for Revocation Requests 26
3.9.5 CRL Issuance Frequency 26
3.9.6 Online Status/Revocation Verification Availability 27
3.9.7 Online Revocation Verification Requirements 27
3.9.8 Suspension Circumstances 27
3.10 Replacement of Digital Signature Certificates 27
3.10.1 Grounds for Replacement 28
3.11 Certificate Characteristics 29
3.11.1 Operational Characteristics 29
3.11.2 Service Availability 29
3.12 End of Subscription 30
3.13 Key Escrow and Recovery 30
3.13.1 Key Escrow and Recovery Policy and Practices 30
4. CERTIFICATE USAGE 30
4.1 Appropriate Uses of the Digital Certificate 30
4.2 Prohibited Certificate Uses 31
4.3 Certificate Validity Period 31
5. CERTIFICATE CHARACTERISTICS 31
5.1 Physical Token Digital Certificate 31
5.2 Virtual Token Certificate 33
5.3 PKCS#10 Digital Certificate 34
6. OBLIGATIONS AND RESPONSIBILITIES OF PARTICIPANTS 35
7. RIGHTS OF PARTICIPANTS 35
8. RELIABILITY OF DIGITAL SIGNATURES AND CERTIFICATES 35

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

9. CONFIDENTIALITY OF INFORMATION **36**
9.1 Scope of Confidential Information 37
9.2 Information Outside the Scope of Confidential Information 37
9.3 Responsibility to Protect Confidential Information 37
9.4 Processing of Personal Data 38
9.5 Disclosure Pursuant to a Judicial or Administrative Process 39
10. DIGITAL CERTIFICATE ISSUANCE SERVICE FEES **39**
11. MODELS AND TEMPLATES FOR TERMS AND CONDITIONS DOCUMENTS **40**
12. APPLICABLE REGULATIONS **40**
13. REVISION HISTORY **40**

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

1. INTRODUCTION

This **Certification Policy (CP)** constitutes the public disclosure of the Open Digital Certification Entity, establishing the rules and practices adopted for the digital signature certificate services provided by Sociedad Cameral de Certificación Digital Certicámara S.A.

This **Certification Policy (CP)** has been prepared in accordance with the recommendations of international standards, such as RFC 3647. Additionally, it complies with current Colombian legislation, specifically Law 527 of 1999, Decree-Law 019 of 2012, Decree 333 of 2014, and any regulations that amend or supplement them.

The general terms and conditions applicable to all digital certification services provided by Certicámara are set forth in the **Certification Practice Statement (CPS)**. This CPS is available in the "regulatory framework" section of our website.

1.1 Document Title and Identification

For the provision of its digital signature certificate services, Certicámara establishes the following information for this document.

Nombre:	Certification Policy - Digital Signature Certificate
Fecha de publicación:	11/11/2026
Versión:	004
Código:	IDI-L-002
Ubicación:	https://web.certicamara.com/marco-normativo

1.2 Scope

This document establishes the standards and rules to be followed by the **Certicámara** Certification Authority to provide the Digital Signature Certificate service, as set forth in the accreditation certificate issued by the National Accreditation Body of Colombia (ONAC) on its website. https://onac.org.co/directorio3/index.php/acreditaciones/16-ECD-002

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

1.3 Policy Update and Approval Procedure

The Certification Policy shall be updated as required by legal, regulatory, or other applicable requirements governing the services within the scope of this document.

During this process, the managers of the various departments involved in providing the services within scope will meet to evaluate the proposed modifications. Final approval of these changes is granted by the President.

The Process Director is responsible for managing the update of the CP on the Certicámara website, specifically at the following link: https://web.certicamara.com/marco-normativo

1.4 Publication Responsibilities

The Certification Authority is obligated to publish information regarding its practices, certificates, and the updated status of those certificates. Publicly classified information published by Certicámara will be made available on its website as follows:

a) The Certificate Revocation List (CRL) is available in CRL V2 format within the root CA repository.
b) LaThe Certificate 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 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 https://ar.certicamara.com:8443/Search/, which can be queried using a search parameter.
e) Certicámara's contact details are provided on the website at https://web.certicamara.com
f) The root CA operation work instructions and all information deemed relevant to the issued certificates are available at https://web.certicamara.com/soporte/manuales-de-soporte-tecnico .
g) The OCSP certificate revocation status is available for online lookup at http://ocsp.certicamara.com, http://ocsp.certicamara.co y http://ocsp4096.certicamara.co.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

2. POLICY IDENTIFICATION

2.1 Policy Identification Criteria

Each certificate issued by Certicámara includes an associated Object Identifier (OID) within its extension, detailed under the certificate properties. This OID links the issued certificate to the corresponding Certification Policy, confirming compliance with the conditions described herein

2.2 Policy OIDs

Each certificate type is identified by a unique Object Identifier (OID), which is included in the certificate as a policy identifier within the certificate properties.

OID	Policy Type
1.3.6.1.4.1.23267.50.1.1	Company / Entity Affiliation Certificate on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.2	Company / Entity Representation Certificate on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.3	Public Office Holder Certificate on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.4	Licensed Professional Certificate on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.5	Natural Person Digital Certificate on local and/or centralized devices
1.3.6.1.4.1.23267.50.1.8.5	Natural Person Digital Certificate - PKCS10
1.3.6.1.4.1.23267.50.1.8.4	Legal Entity Digital Certificate - PKCS10

2.3 Certicámara CA Certificate Types

To meet the diverse needs arising from the increasing use of information and communication technologies, Certicámara issues various types of **digital certificates**. These certificates are issued with a maximum validity period of two (2) years, in accordance with the current Specific Accreditation Criteria and in compliance with the Certificate Lifecycle section of this document.

2.3.1 Company / Entity Affiliation Certificate on local and/or centralized devices.

This certificate is issued to national or foreign natural persons who have been fully identified by Certicámara using valid identity documents issued by the competent authority of the Republic of Colombia, or equivalent documents issued by the competent authority of a foreign state. It identifies the individual as a natural person and

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

establishes their affiliation with a specific business organization or government entity, without granting legal representation or the authority to legally bind the organization.

The subscribers of this type of digital certificate are:

1) The natural person who sufficiently demonstrates, to Certicámara's satisfaction, the existence of a legal, employment, or other relationship with the legal entity or government body to be named in the digital certificate.

2) The legal entity listed in the digital certificate.

Issuance Requirements

- Applicants must complete the form available on the website at https://ventadigital.certicamara.com. By submitting the required information, the user guarantees that it is **accurate, complete, and up to date**.

- For this certificate type, applicants must attach an employment certificate issued by the requesting company within the last 30 days. The certificate must be on the entity's letterhead, include the individual's full name, identification number, and job title, and be signed by the Human Resources department or the legal representative. In the case of a statutory auditor or proxy, a certificate of existence and legal representation issued within the last thirty (30) days showing the official appointment is acceptable.

- As part of the process, the applicant's identity must be verified using the mechanisms established by Certicámara at the time of application.

Note: The subscriber's residential information (address, municipality, and department) will not be subject to external verification. Under the principle of good faith, the data entered by the user in the application form will be deemed an official declaration.

Published information that will appear on the digital certificate:

1. Common Name (CN)	Subscriber's First and Last Name(s)
2. Serial Number	Digital Certificate Unique Identifier
3. Organization (O)	Corporate Name 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 Identification Number
7. Title (T)	Subscriber's Job Title within the Organization

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

8. Organizational Unit (OU)	Agreement - Certificate Validity – Physical / Virtual Token
9. Street Address (STREET)	Organization 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 Surname(s)
14. Given Name (G)	Subscriber's Given Name

2.3.2 Company / Entity Representation Certificate on local and/or centralized devices.

This certificate is issued to national or foreign natural persons who have been fully identified by Certicámara using valid identity documents issued by the competent authority of the Republic of Colombia, or equivalent documents issued by the competent authority of a foreign state, establishing their status as the legal representative of a legal entity or government body.

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

The subscribers of Company / Entity Representation Certificates are both the natural person acting on behalf of and as the legal representative of a legal entity, and the represented legal entity also listed in the digital certificate.

Issuance Requirements

- Applicants must complete the form available on the website at https://ventadigital.certicamara.com. By submitting the required information, the user guarantees that it is **accurate, complete, and up to date**.

- For this certificate type, the applicant must attach the document proving the existence and legal representation of the company or entity. For companies or entities registered with a Chamber of Commerce, a Certificate of Existence and Legal Representation issued within the last 30 days is required. For companies or entities not registered with a Chamber of Commerce, a certificate issued by a regulatory or supervisory body is required, such as the Financial Superintendency, the Superintendency of Industry and Commerce, the Ministry of Education, or Local Mayoral Offices, among others. For consortiums and temporary joint ventures, the document proving existence and legal representation is the consortium or temporary joint venture formation

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

agreement.

- Como parte del proceso, se debe **validar la identidad** del solicitante mediante los mecanismos dispuestos por Certicámara al momento de realizar la solicitud.

Note: The subscriber's residential information (address, municipality, and department) will not be subject to external verification. Under the principle of good faith, the data entered by the user in the application form will be deemed an official declaration..

Published information that will appear on the digital certificate:

1. Common Name (CN)	Subscriber's First and Last Name(s) (Legal Representative)
2. Serial Number	Digital Certificate Unique Identifier
3. Organization (O)	Corporate Name 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 Identification Number
7. Title (T)	Subscriber's Job Title within the Organization
8. Organizational Unit (OU)	Agreement - Certificate Validity – Physical / Virtual Token
9. Street Address (STREET)	Organization 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 Surname(s)
14. Given Name (G)	Subscriber's Given Name

2.3.3 Public Office Holder Certificate on local and/or centralized devices.

This certificate is issued to national or foreign natural persons who have been fully identified by Certicámara using valid and current identity documents issued by the competent authority of the Republic of Colombia, or equivalent documents issued by the competent authority of a foreign state. It identifies the individual as a natural person and establishes their status as a public official affiliated with a government entity in the Republic of Colombia.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

The subscribers of this type of digital certificate are natural persons who sufficiently demonstrate, to Certicámara's satisfaction, that they have been appointed as public officials, official workers, or legally hold office as a notary, consul, judge, magistrate, registrar, or public servant in the Republic of Colombia, as well as contractors designated or authorized by a public entity.

The Public Office Holder Certificate does not guarantee the performance, suitability, or effective fulfillment of the duties assigned to its holder. Certicámara does not guarantee that the subscriber of the Public Office Holder Certificate has not been subject to disciplinary, administrative, criminal, or any other type of sanctions in the Republic of Colombia or abroad. For the issuance of the Public Office Holder Certificate, Certicámara relies on the documentation provided and the declarations made by the subscriber at the time of the service request. Unless otherwise provided by law or applicable regulations, applying for the issuance of the Public Office Holder Certificate is voluntary for public office holders. The issuance of the Public Office Holder Certificate does not restrict the subscriber from applying for other digital certificates.

Issuance Requirements

- Applicants must complete the form available on the website at https://ventadigital.certicamara.com. By submitting the required information, the user guarantees that it is **accurate, complete, and up to date**.

- For this certificate type, the applicant must attach the document establishing their affiliation with the public entity. Acceptable proof of affiliation includes, but is not limited to: the formal act of assumption of office (Acta de posesión pursuant to Article 2.2.5.1.8 of Decree 1083 of 2015), an employment certificate, National Registry (Registraduría) certificates for mayors, or a service procurement contract for contractors (including SECOPII system screenshots).

- As part of the process, the applicant's identity must be verified using the mechanisms established by Certicámara at the time of application.

Note: The subscriber's residential information (address, municipality, and department) will not be subject to external verification. Under the principle of good faith, the data entered by the user in the application form will be deemed an official declaration.

Published information that will appear on the digital certificate:

1. Common Name (CN)	Subscriber's First and Last Name(s)
2. Serial Number	Digital Certificate Unique Identifier
3. Organization (O)	Corporate Name 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

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

6. 1.3.6.1.4.1.23267.2.3	Organization Identification Number
7. Title (T)	Subscriber's Job Title within 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)	Organization Address
10. Country (C)	Country of Certificate Issuance
11. State Or Province Name (S)	City / Municipality of the Subscriber's Organization
12. Locality (L)	Municipality / City of the Subscriber's Organization
13. Surname (SN)	Subscriber's Surname(s)
14. Given Name (G)	Subscriber's Given Name

2.3.4 Licensed Professional Certificate on local and/or centralized devices..

This certificate is issued to national or foreign natural persons who have been fully identified by Certicámara using valid and current identity documents issued by the competent authority of the Republic of Colombia, or equivalent documents issued by the competent authority of a foreign state. It identifies the individual as a natural person and links them to the attainment of a professional degree duly recognized in the Republic of Colombia or abroad, provided they have obtained the corresponding registration, license, professional membership, or professional card required to practice their profession in the Republic of Colombia or abroad.

The subscribers of this type of digital certificate are natural persons who can sufficiently demonstrate, to Certicámara's satisfaction, that they have obtained a professional degree duly recognized in the Republic of Colombia or a foreign degree validated by the Ministry of National Education, and that they have obtained the corresponding registration, license, professional membership, or professional card required to practice their profession in the Republic of Colombia or abroad.

Issuance Requirements

- The applicant must complete the form available on the website via the link https://ventadigital.certicamara.com. By entering the corresponding information, the user guarantees that it is **accurate, complete, and up to date**.

- When it is not possible to verify the profession through reliable sources, the applicant will be required to provide the Licensed Professional Certificate documentation. This requirement applies to technical, technological, and university levels (pursuant to Law 30 of 1992 and Opinion 059881 of the Administrative Department of the Public Function). Acceptable documents include: professional card, diploma, graduation certificate, professional

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

registration, or degree certificate. For degrees obtained abroad, the document must be duly validated by the Ministry of National Education.

- As part of the process, the applicant's identity must be verified using the mechanisms established by Certicámara at the time of application..

Note: The subscriber's residential information (address, municipality, and department) will not be subject to external verification. Under the principle of good faith, the data entered by the user in the application form will be deemed an official declaration.

Published information that will appear on the digital certificate:

1. Common Name (CN)	Subscriber's First and Last Name(s)
2. Serial Number	Digital Certificate Unique Identifier
3. Organization (O)	Corporate Name of the Subscriber's Organization / Subscriber's First 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 Identification Number / Subscriber's Identification Number with or without verification digit (Depends on the information entered in the application)
7. Title (T)	Subscriber's Profession
8. Organizational Unit (OU)	Agreement - Certificate Validity – Physical / Virtual Token
9. Street Address (STREET)	Organization Address / Subscriber's Address (Depends on the information entered in the 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 Surname(s)
14. Given Name (G)	Subscriber's Given Name

2.3.5 Natural Person Digital Certificate on local and/or centralized devices.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

This certificate is issued to national or foreign natural persons who have been fully identified by Certicámara using valid and current identity documents issued by the competent authority of the Republic of Colombia, or equivalent documents issued by the competent authority of a foreign state.

The subscribers of Natural Person Certificates are natural persons acting in their own name, proves their identity to Certicámara. This certificate can be used through a physical device (USB token) connected to the computer or through a virtual device (in the cloud) via an Internet connection.

Issuance Requirements

- The applicant must complete the form available on the website via the link https://ventadigital.certicamara.com. By entering the corresponding information, the user guarantees that it is **accurate, complete, and up to date**.

- As part of the process, the applicant's identity must be verified using the mechanisms established by Certicámara at the time of application.

Note: The subscriber's residential information (address, municipality, and department) will not be subject to external verification. Under the principle of good faith, the data entered by the user in the application form will be deemed an official declaration.

Published information that will appear on the digital certificate:

1. Common Name (CN)	Subscriber's First and Last Name(s)
2. Serial Number	Digital Certificate Unique Identifier
3. Organization (O)	Subscriber's First 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 Identification Document Number (with or without verification digit) (Depends on the information entered in the application)
7. Title (T)	Natural Person
8. Organizational Unit (OU)	Agreement - Certificate Validity – Physical / Virtual Token
9. Street Address (STREET)	Subscriber's Address
10. Country (C)	Country of Certificate Issuance

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

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

2.3.6 Natural Person / Legal Entity Digital Certificate

This certificate is issued to national or foreign natural persons or legal entities that have been fully identified by Certicámara using valid and current identity documents issued by the competent authority of the Republic of Colombia, or equivalent documents issued by the competent authority of a foreign state.

The subscribers of Natural Person / Legal Entity Certificates are natural persons or legal entities acting on their own behalf that sufficiently demonstrate their identity, to Certicámara's satisfaction, by presenting the required supporting documentation.

Issuance Requirements

- The applicant must complete the form available on the website via the link https://ventadigital.certicamara.com. By entering the corresponding information, the user guarantees that it is **accurate, complete, and up to date.**

- For this certificate type, the applicant must attach the document proving the existence and legal representation of the company or entity: For companies or entities registered with a Chamber of Commerce, a Certificate of Existence and Legal Representation issued within the last 30 days is required. For companies or entities not registered with a Chamber of Commerce, a certificate issued by a regulatory or supervisory body is required, such as the Financial Superintendency, the Superintendency of Industry and Commerce, the Ministry of Education, or Local Mayoral Offices, among others. For consortiums and temporary joint ventures, the document proving existence and legal representation is the consortium or temporary joint venture formation agreement.

- As part of the process, the applicant's identity must be verified using the mechanisms established by Certicámara at the time of application.

Note: The subscriber's residential information (address, municipality, and department) will not be subject to external verification. Under the principle of good faith, the data entered by the user in the application form will be deemed an official declaration.

Note: The PKCS#10 format is a standard request structure containing the formal request and the necessary keys to integrate and generate the digital signature

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

directly from the organization's or subscriber's own systems. This type of certificate is oriented towards entities or persons requiring management of the signature lifecycle within their own technological infrastructure. For its issuance, the client is responsible for guaranteeing the accuracy of the information entered, while Certicámara S.A. will verify that the provided data matches the submitted documentation exactly

Published information that will appear on the digital certificate:

1. Common Name (CN)	Corporate Name of the Organization
2. Serial Number	Digital Certificate Unique Identifier
3. Organization (O)	Corporate Name of the Organization
4. 1.3.6.1.4.1.23267.2.2	Subscriber's 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)	Organization's City / Municipality
10. Locality (L)	Subscriber's Department
11. Surname (SN)	Subscriber's Surname(s)
12. Given Name (G)	Subscriber's Given Name

3. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFECYCLE

3.1 Certificate Application

The application process may be carried out through any of the following channels:

1. In-person at Certicámara facilities.
2. Through the Contact Center.
3. Via any other electronic means provided by Certicámara.

Received applications shall 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 conducted within a maximum of two (2) business days from the receipt of all required documents, proof of payment, and the successful validation of the applicant's identity. Once the review is complete, applications will be forwarded to the

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

Certification Authority (CA) for issuance, which shall take place within a maximum of one (1) business day.

In accordance with the internal policies of Certicámara S.A., 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 certified by the Ministry of Foreign Affairs. Documentation will be retained in accordance with Certicámara's document retention schedules. The applicant's information will not be made public without their explicit consent.

By using and electronically subscribing to the Certicámara S.A. digital signature certificate, the applicant fully and unreservedly accepts the following documents, which form an integral part of this CPS and the service agreement: the Terms and Conditions of the service, the Declarations and Commitments regarding the Prevention of Money Laundering, Terrorist Financing, Proliferation of Weapons of Mass Destruction Financing, and Corruption/Smuggling (LA/FT/FPDAM and C/ST), the Certification Policy (CP), the personal data processing policy, and the organizational policies of Certicámara S.A., available on the Certicámara website.

The Terms and Conditions of the digital signature certification service apply from the moment the applicant expresses interest in acquiring the certificate and remain in effect throughout its validity period, along with the general contracting terms of the service.

Applicants must consider the following prior to 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 on 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) **Verification of Information:** Verifying the information provided by Certicámara S.A. to make an informed decision regarding the digital signature certificate application, in compliance with Law 527 of 1999, Decree 019 of 2012, Law 1341 of 2009, Law 1978 of 2019, Law 1581 of 2012, Decree 1074 of 2015, Decree 358 of 2020, Decree 1538 of 2020, and Decree 620 of 2020.

c) **Provision of Information:** The client must provide updated and available contact information to facilitate communication for processes associated with digital signature issuance, ensuring that these channels do not have restrictive configurations, security filters, or any other additional adjustments or authorizations in their domains. The email address and mobile phone number linked to a device provided in the application will be the authorized communication channels for sending notifications related to the process; therefore, submitting this data authorizes its use for this purpose.

d) **Password Assignment:** To use the digital certificate, the holder must assign a password. The implications of forgetting or losing the password are detailed below:

FOR EXCLUSIVE USE OF CERTICÁMARA S.A.

- **Virtual Token:** Password resetting can be performed through the website at https://ventadigital.certicamara.com/reset-password at no additional cost up to ten (10) times; subsequent requests will incur an associated fee.
- **Physical Token:** Because Certicámara S.A. does not possess mechanisms for password recovery due to its local storage, it will be indispensable to acquire a new certificate, which will incur an associated cost.

The holder must remember and securely safeguard the password. This password is the exclusive means to access the issued certificate.

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

f) **Right to Refuse Service:**Noting that Certicámara S.A. reserves the right to decline the issuance of a digital signature certificate due to technical conditions, without generating any liability.

g) **Identity Validation by Certicámara S.A.:** Certicámara S.A., as an Open Digital Certification Entity, will perform prior identity verification using reliable sources and data provided by third parties with active contracts 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 deemed necessary to verify the applicant's identity or status. 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 ID card.
- Health insurance regime affiliation document.
- Occupational risk insurance management company (ARL) affiliation document.
- Other documents that allow for the verification of the identity or authority of the subscriber or the entity for the issuance of any type of certificate

i) **Database Queries:** Certicámara may query identity databases of public or private entities to perform the necessary validations to issue the digital certificate.

j) **SAGRILAFT Compliance:** It will query the databases necessary to comply with SAGRILAFT, subject to the applicant's prior acceptance of the Declarations and

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A.

Commitments on 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 period of two (2) years.

l) **Denial or Decline of Application:** Certicámara S.A. may deny the issuance of a digital certificate if it falls outside the scope of the accreditation granted by ONAC, due to non-compliance with the law, and/or when, in its judgment, it compromises its reputation as a Certification Authority. In this case, there will be no opportunity for remediation by the user. If Certicámara decides to deny or decline the application, it will notify the applicant via email, stating the reasons.

m) **Mac OS Development:** Currently, Certicámara is 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 application?

The application for a digital certificate may be made by any natural person in full exercise of their legal capacity, as well as by legal entities through their legal representative, a proxy, an employee, or a duly authorized third party, provided that such capacity is proven with the documents required by the Registration Authority (RA). In the case of minors, the digital signature application must be presented by their legal representative, attaching the minor's identity document and the document proving 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 digitally signed using the CA's certificate, forming part of the Certicámara chain of trust.

The issuance of certificates requires authorization of the request by the Subordinate CA system. Upon approval, certificates are securely issued and made available to the subscriber.

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

- Implements a certificate generation procedure that establishes a secure link between the certificate and the registration information, including the certified public key.
- Guarantees the protection of the confidentiality and integrity of 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 preceding the current date.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

3.2.2 Notification to the Subscriber by the Issuing CA of Certificate Issuance

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

3.2.3 Private Key Restoration

For digital signature certificates on virtual devices, Certicámara has implemented secure mechanisms that allow the subscriber to manage the change or reset of their password through the contact center at no associated cost for up to a maximum of ten (10) requests; subsequent requests will incur a fee. For digital signature certificates on physical devices, the subscriber may change the password directly from the application whenever required; in the event of loss or a forgotten password, they must complete the process to acquire a new digital signature.

3.3 Physical Delivery of the Digital Certificate to Subscribers

3.3.1 Coverage

The delivery of digital certificates will be carried out in accordance with the service coverage matrix of the logistics operator that maintains an active contract with Certicámara for this purpose, or through direct delivery by a collaborator from Certicámara's logistics department. In both scenarios, the physical device will be delivered, and the approval email sent to the holder will contain the link to the download instructions.

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 facilities, as indicated in the application form. When the holder authorizes a third party to claim the device at the facilities, this person must physically present the Authorized Third Party form, which can be downloaded from the Certicámara website at the following link: https://web.certicamara.com/soporte/formatos

The form titled "Authorized Third Party" must be fully completed and signed by both parties. Additionally, photocopies of the identity documents of both the holder and the authorized third party must be presented.

The logistics operator's waybill will serve as evidence of acknowledgment of receipt of the physical device, and formal delivery documentation will be maintained for deliveries at Certicámara facilities.

3.3.3 Delivery Management Time – Physical Certificates

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

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

The estimated delivery times from certificate issuance are:

- **Bogotá and nearby municipalities:** Approximately two (2**) business days.**
- **Department capital cities:** 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.

If delivery is impossible, a second attempt will be made. If this also fails, the logistics operator will return the digital certificate to Certicámara facilities.

If delivery is not possible due to causes attributable to the subscriber, Certicámara or the logistics operator will contact them to coordinate delivery. However, it is important to note that if a delivery or collection date is not coordinated within ninety (90) calendar days from the issuance date, the asset will be deemed 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 application process, which will incur a cost according to Certicámara policies..

3.3.4 Download Timeframe

Once the signature certificate request is approved, the holder will automatically receive an email with the download link, a detailed manual, and important recommendations. The holder will have ninety (90) calendar days to complete this process; otherwise, the asset will be understood as abandoned, and Certicámara will definitively block the link. In such case, if they wish to obtain the signature certificate, they must initiate a new application process, which will incur a cost according to Certicámara rates.

3.4 Certificate Acceptance

Confirmation by the subscriber is not required as acceptance of the service received. The digital signature certificate service is understood to be accepted from the moment its issuance is requested. Consequently, if the information contained in the service activation communication does not match its current status or was not provided correctly, the subscriber must inform Certicámara through any of the available service channels to perform the relevant correction procedures, if applicable.

3.4.1 Certificate Publication by the CA

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

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 exact moment the certificate is issued.

In the event of a technical difficulty that hinders its publication, this will be carried out within the month following the certificate's issuance date, based on the findings of the technical analysis that prevented its timely publication..

3.4.2 *Notification of Certificate Issuance by the CA to Other Entities*

Certicámara maintains an LDAP digital certificate repository through which entities, government agencies, private sector companies, and other interested parties can query certificate issuance. This repository is accessible at the following web address: https://ar.certicamara.com:8443/Search/. 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 hardware security module (HSM) that complies with the requirements established in a standard secure electronic signature device protection profile for a certification authority, in accordance with FIPS 140-3 Level 3 or a higher security level, and the creation of CA keys uses a pseudo-random number generation algorithm.

3.5.2 Use of Certificate and Private Key of the Subscriber

The Policy Identification section of this document details the uses and purposes for each type of certificate issued by Certicámara.

3.5.3 *Use of the Certificate and Public Key of the Relying Party*

Relying parties acting in good faith may only place reliance on the certificates for the purposes defined in this CPS, the CP, and current regulations.

Such third parties may successfully perform public key operations by relying on the certificates issued by the chain of trust. However, they must act with diligence and assume the responsibility to verify the status of the certificates using the mechanisms detailed in this CPS.

3.5.4 Private Key Destruction Method

The RSE component of Certicámara's PKI infrastructure will delete the identity associated with the private key of the subscriber's certificate issued on a virtual token upon expiration of its validity period or if it has been revoked. The destruction will be

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

carried out using established commands to physically erase from the HSM memory the section where the key was recorded.

3.6 Certificate Renewal

3.6.1 Renewal Timeframes

Certicámara will notify its subscribers of the expiration of their digital certificate validity with a minimum notice of thirty (30) calendar days. This notification may be made via email to the address provided by the subscriber or through any other appropriate means of communication that Certicámara deems convenient.

However, Certicámara is under no obligation to ensure the effectiveness of the notification regarding the end of the certificate's validity or to confirm its receipt. It is the subscriber's duty to know the expiration date of their digital certificate and to manage the relevant procedures before Certicámara for the issuance of a new signature.

Renewal shall be understood as the issuance of a new digital certificate, which entails the registration of a renewed application, the acceptance by the applicant of the Terms and Conditions of the digital signature certification service of Certicámara S.A., 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 a renewal?

Subscribers may request the renewal of their certificate when it is close to expiring 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 Applications

For the purpose of renewing a certificate, the subscriber must undergo the identity validation process again. Consequently, the application procedure for the renewal of a certificate is identical to that of first-time issuance, with the exception that attaching documents to the application will not be required unless they have expired (if applicable).

3.6.4 Notification of New Certificate Issuance to the Subscriber

The successful 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.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

3.8 Certificate Modification

During the validity period of a certificate, the modification or update of the information it contains is not permitted. If it is necessary to change any data in the issued certificate, it will be required to revoke the current certificate, request the issuance of a new one with the correct data, and pay the corresponding fee.

3.9 Certificate Revocation and Suspension

The revocation of a digital certificate is the mechanism by which an issued certificate is invalidated, terminating its validity period, either due to its expiration or upon the occurrence of any of the revocation events stipulated in this Certification Practice Statement. It is clarified that revocation does not have any associated cost.

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

3.9.1 Grounds 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) Compromise of security 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 being misused.

d) Death of the subscriber.

e) Supervening incapacity of the subscriber.

f) Liquidation of the represented legal entity listed in the digital certificate.

g) Update of the information contained in the digital certificate.

h) Confirmation that any information or fact contained in the digital certificate is false, as well as the occurrence of new facts that cause the original data to no longer reflect reality.

i) Compromise of Certicámara's private key or its security system in a manner that affects the reliability of the digital certificate, due to any circumstance, including fortuitous events.

j) Cessation of operations by Certicámara, unless the issued digital certificates are transferred to another Certification Authority.

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

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

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

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

n) Any cause that reasonably leads to the belief that the certification service has been compromised to the extent that the reliability of the digital certificate is called into question.

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

p) Non-compliance by the subscriber or the legal entity they represent or to which they are linked through the Digital Certification Service Agreement provided by Certicámara.

q) Report of an overdue account balance caused by non-payment for the services provided by Certicámara.

r) Upon request for money refund by the subscriber, in accordance with the refund policies defined by Certicámara. .

s) For causes associated with Certicámara within the framework of regulatory or compliance requirements.

t) The occurrence of any other cause specified in this Certification Practice Statement.

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

3.9.2 ¿Who can request a revocation?

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

Certicámara may also process the revocation of a certificate if it obtains knowledge or reasonable suspicion of a compromise of the subscriber's private key, or any other decisive event that makes the revocation of the certificate imperative. In cases where 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 validity period. For this purpose, the previously submitted documentation will be used to avoid affecting service availability.

3.9.3 Revocation Request Procedure

Certicámara has established the following means to receive revocation requests:

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

- **Virtual:** Complete the application form available on the website: https://web.certicamara.com/soporte/formatos and subsequently file the request through the following link: https://pqr.certicámara.com/registrar. This mechanism applies when the digital certificate is associated with a legal entity or entity and the subscriber loses their relationship with said organization.
- **Online:** Through the Certicámara website, registering the request at the following URL: https://ventadigital.certicamara.com/revocar-certificado

If deemed necessary, Certicámara will conduct investigations, verifications, and relevant procedures, personally or through third parties, to verify the existence of the invoked ground for revocation. These actions may include direct communication with the subscriber and the physical presence of the third party invoking the ground.

Certicámara will validate the identity of the subscriber invoking the ground for revocation. If the person presenting the request is not the subscriber, or if they are but cannot be satisfactorily identified, they may appear in person at Certicámara offices during business hours (8:00 a.m. – 5:00 p.m., Monday through Friday) with proof of the existence of the respective ground for revocation where applicable, without prejudice to any measures Certicámara may establish 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 any grace periods for such revocations.

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

If the ground is verified, 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 a certificate suspension service to subscribers.

3.9.4 Grace Period for Revocation Requests

Certicámara must inform the subscriber within the following 24 hours regarding 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 Certificate Revocation List of the Subordinate CA Certicámara (CRL) and CA SUB CERTICÁMARA (CRL) is carried out with a validity of three (3) days::

- Periodically
- Publication may take place a maximum of eight (8) hours after the last revocation, at any time of the day.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

3.9.6 Online Status/Revocation Verification Availability

The Certificate Revocation Lists (CRL) and the Online Certificate Status Protocol (OCSP) validation service will be available for query 365 days a year, 24 hours a day, 7 days a week. This service will be provided with an availability service level agreement (SLA) of 99.8%.

Certicámara maintains the historical record of revoked certificates since the inception of the service provision.

3.9.7 Online Revocation Verification Requirements

Online certificate status verification must be performed 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 regarding the certificate status to the Validation Authority (VA), which, after querying its database, provides a response on the certificate status via HTTP through the addresses http://ocsp.certicamara.com, http://ocsp.certicamara.co and 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.

3.10 Replacement of Digital Signature Certificates

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

However, to make the replacement effective, it must be considered 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 performed for digital certificates that are less than ninety (90) calendar days from their expiration.
- The same certification policy under which it was initially issued must be maintained.

This new generation of the digital signature certificate will incur 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

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

negotiated 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://ventadigital.certicamara.com requesting the replacement of the digital certificate, taking into account the conditions mentioned in the preceding section.
- The subscriber must revoke the digital signature certificate, as defined in the Revocation Request Procedure section of this document.

Additionally, there are exceptional cases where, by commercial agreements, Certicámara is obligated to maintain custody and manage license quotas; in this scenario, a communication from the supervisor and/or contract administrator must be provided, requesting the replacement of certificates and justifying it under any of the following grounds:

- Change of holder
- Change of job title
- Change of certificate type (Physical/Digital)

Subsequently, the contract holder will send this request to the registration and usage department through the form available on the website: ttps://pqrf.certicamara.com/registrar, indicating the certificate to be replaced as well as the information corresponding to the respective revocation. Based on the provided information, the control of the entity's quotas will be carried out.

3.10.1 Grounds for Replacement

Certicámara will replace the digital signature certificate in accordance with the preceding section when any of the following grounds occur:

Loss of the physical device.

- Exposure of the PIN (Password/key) of the digital certificate.
- Change in the information of the previously issued digital certificate (does not apply to changes in the identification number).
- Change in the corporate name of the company, regardless of whether it retains the same tax identification number (NIT).
- Error attributable to Certicámara.

Additionally, replacement will proceed when any of the following events occur, which are codified in Article 37 of Law 527 of 1999:

I. Death of the subscriber.
II. Supervening incapacity of the subscriber.
III. Update of the information contained in the digital certificate.
IV. Loss, destruction, or compromise of the security of the physical medium

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

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 submitted by the applicant for the issuance of the certificate, without requiring the generation of a new request by the subscriber, and under the same conditions initially agreed upon.

3.11 Certificate Characteristics

3.11.1 Operational Characteristics

For the validation of digital certificates, several Validation Service Providers are available, providing 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 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 regarding the certificate status to the VA, which, after querying its database, provides a response on the certificate status via HTTP through the addresses http://ocsp.certicamara.com, http://ocsp.certicamara.co y http://ocsp4096.certicamara.co

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

- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_2014.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_2014.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_4096.crl?crl=crl
- https://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_409 6.crl?crl=crl

3.11.2 Service Availability

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

3.11.3 Optional Functions

To make use of the online validation service by querying the addresses

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

http://ocsp.certicamara.com and http://ocsp4096.certicamara.co, it is the responsibility of the relying party acting in good faith 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 causes of revocation specified in this document.
- Expiration of the certificate's validity period.

3.13 Key Escrow and Recovery

3.13.1 Key Escrow and Recovery Policy and Practices

The private key of the Root CA is escrowed by a hardware cryptographic device (HSM). Access to the private key repository utilizes Shamir's threshold scheme (k, n) both in software and cryptographic devices.

4. CERTIFICATE USAGE

4.1 Appropriate Uses of the Digital Certificate

The root digital certificate may only be used to identify the root certification authority itself and to securely distribute its public key. The use of certificates issued by the root CA shall be limited to signing digital certificates and signing the corresponding certificate revocation lists (CRLs).

General uses applicable to digital certificates issued by Certicámara:

a) **Subscribers** may only use digital certificates for the specific purposes set forth in their individual agreement executed with Certicámara, those permitted under this **Certification Practice Statement (CPS) and the Certification Policies (CP)**, and those authorized under Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014). The agreement executed with the subscriber may limit the scope of use based on the environment in which the digital certificate is utilized or the specific characteristics of the project being developed. Any other use shall be deemed a violation of this **Certification Practice Statement** and **the Certification Policies**, constituting grounds for the revocation of the **digital certificate** and the termination of the **subscriber** agreement, without prejudice to any applicable civil or criminal legal actions.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

b) The subscriber acknowledges and accepts that the advertised products and services are provided "as is" on an individual basis, that digital certificates primarily certify the identity of the natural person appearing as the service subscriber, and that there is no implied information regarding additional services or benefits beyond those expressly stated. Furthermore, the use of these certificates is the subscriber's sole responsibility, taking into account the provisions of Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014).
c) The use of the digital certificate and any data messages digitally signed with it—including electronic monetary transactions, regardless of the amount—are the SOLE responsibility of the respective subscriber. Consequently, Certicámara assumes no liability for the verification or public certification of signed data messages, as it does not know, nor does it have any legal obligation to know, the content of digitally signed messages or the transaction amounts processed using the digital certificate within third-party electronic transaction systems. In general, Certicámara, as an Open Digital Certification Entity and Trusted Third Party, does not assume liability for the subscriber's use of digital signature certificates; therefore, no financial limits are applicable in this regard. To this end, the subscriber shall fulfill their duties and bear the full burden of liability imposed under Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014).

4.2 Prohibited Certificate Uses

a) Under no circumstances may digital certificates be used for illicit purposes or operations under any legal jurisdiction worldwide.
b) Any use of digital certificates that violates Colombian legislation, international treaties ratified by the Colombian State, supranational regulations, public decency, sound commercial practices, or any provision contained within this Certification Practice Statement and the agreements executed between Certicámara and the Subscriber is strictly prohibited.
c) Any use of digital certificates intended to infringe upon the intellectual property rights of Certicámara or any third party is prohibited.
d) The physical medium of the digital certificate provided by Certicámara (if applicable) may only be used within the context of the Digital Certification System. No information other than that expressly authorized by Certicámara may be embedded into the provided physical medium, nor may it be used outside the Digital Certification System.

4.3 Certificate Validity Period

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

5. CERTIFICATE CHARACTERISTICS

5.1 Physical Token Digital Certificate

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

This refers to a physical device that connects to a computer's USB port, containing the digital certificate and the public and private key pair. It is protected by a fixed password required for its operation. An active internet connection is not required to use the device. The client is solely responsible for safeguarding the delivered device and managing its corresponding password.

In line with its commitment to managing the environmental impact of physical storage devices delivered to clients, Certicámara offers users:

1. A refurbished physical token option that has undergone a rigorous physical and functional inspection meeting high quality standards.
2. A secure erasure process performed to delete any previous digital certificate, in accordance with the application features provided by the vendor.
3. An updated process ensuring that the physical token complies with all applicable usability and technical operational standards.

i. Technical Specifications

✔ 4096-bit private key length.
✔ Certificate signing algorithm with RSA-SHA-2 256 -2056 hash.
✔ Compatibility with APIs and standards (PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, MS minidriver, CNG).
✔ 80K memory capacity with a minimum data retention of 10 years.
✔ Dimensions: 5110 - 16.4mm * 8.5mm * 40.2mm.
✔ Compliant with ISO 7816-1 and 4 specifications.
✔ Rigid molded plastic with a tamper-evident enclosure.
✔ Windows (Server 2008/R2, Server 2012/R2, 7, 8, and 10).
✔ Linux.
✔ USB connector.

ii. Cryptographic Device Care

✔ Operating temperature: 0°C to 70°C (32°F to 158°F).
✔ Storage temperature: -40°C to 85°C (-40°F to 185°F).
✔ Humidity range: 0% to 100% non-condensing.
✔ IPX7 waterproof rating – IEC 60529.

When setting passwords, subscribers should observe the following security recommendations and protection guidelines:

✔ The password must be strictly for personal use and must not be shared with any third party.

✔ Store your password securely; it is highly recommended to memorize it to prevent disclosure.

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

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

✔ Always disconnect the device using the proper safe-removal procedure.
✔ Avoid impacts and drops.
✔ Use only the official applications provided by Certicámara to operate the certificate.

iii. Associated Risks

The cryptographic devices used may be exposed to the following risks:

✔ Environmental fluctuations outside normal operating ranges, such as voltage and temperature anomalies.
✔Unauthorized physical access attempts exceeding the manufacturer's technical specifications.

For detailed information on cryptographic device risk levels, please refer to the NIST.FIPS.140-3.pdf document.

5.2 Virtual Token Certificate

This refers to a cloud-based infrastructure provided as a service, where issued digital certificates and their corresponding key pairs are securely hosted within Certicámara's technological infrastructure. These certificates are linked to a username and password created by the certificate holder. An active internet connection is required to use this service.

i. Características

✔ 4096-bit private key.
✔ Certificate signing algorithm with SHA256 hash.
✔ X.509 v3 certificates.
✔ Storage within infrastructure compliant with FIPS 140-2 Level 3.
✔ File signing via document hash encryption (does not require transmitting the original document, ensuring strict confidentiality).
✔ Network access to the *.certicamara.com domain via port 443.
✔ Signing component that enables Certitoken consumption.
✔ Minimum Java Version 7.
✔ Windows 7 or higher.
✔ Framework 4.0 or higher.
✔ RSE: Two-factor authentication

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

ii. ***Device Care***

Physical and technical maintenance of the data center housing the HSM to ensure its proper operation. This includes humidity controls, power redundancy, unauthorized access prevention, fire detection systems, biometric security for rack access, and data center perimeter security, among others.

When setting passwords, subscribers should observe the following security recommendations and protection guidelines:

✔ The password must contain between eight (8) and twelve (12) alphanumeric characters, including both uppercase and lowercase letters.

✔ The password must be strictly for personal use and must not be shared with any third party.

✔ Store your password securely; it is highly recommended to memorize it to prevent disclosure.

iii. ***Associated Risks***

For virtual token certificates, the associated environmental risks are those that could disrupt the proper operation of the data center where the HSM is installed.

In terms of logical security, risks are defined by cyberattacks that could compromise system access and/or availability.

5.3 PKCS#10 Digital Certificate

This refers to a standard for generating public and private keys within the signer's own infrastructure and under their sole responsibility, with the purpose of having them certified by a digital certification authority.

i. *Characteristics*

✔ 4096-bit public key.
✔ Certificate signing algorithm with SHA256 hash.
✔ Signed public key in *.CER format, compliant with the Certicámara chain of trust.
✔ Issuance utilizing the PKCS#10 standard.
✔ Generation of a Certificate Signing Request (CSR) in PKCS#10 format.
✔ Capability to receive and utilize the public key in .CER format.

ii. *Device care*

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

Physical and technical maintenance of the data center housing the HSM to ensure its proper operation. This includes humidity controls, power redundancy, unauthorized access prevention, fire detection systems, biometric security for rack access, and data center perimeter security, among others.

When setting passwords, subscribers should observe the following security recommendations and protection guidelines:

- ✔ The password must contain between eight (8) and twelve (12) alphanumeric characters, including both uppercase and lowercase letters.
- ✔ The password must be strictly for personal use and must not be shared with any third party.
- ✔ Store your password securely; it is highly recommended to memorize it to prevent disclosure.

iii. Associated Risks

For PKCS#10 certificates, the associated environmental risks are those that could disrupt the proper operation of the data center where the HSM is installed.

In terms of logical security, risks are defined by cyberattacks that could compromise system access and/or availability.

6. OBLIGATIONS AND RESPONSIBILITIES OF PARTICIPANTS

The obligations and responsibilities of the participants are defined in section 9.5 of the Certification Practice Statement document.

7. RIGHTS OF PARTICIPANTS

The rights of the participants are defined in section 9.7 of the Certification Practice Statement document.

8. RELIABILITY OF DIGITAL SIGNATURES AND CERTIFICATES

Certicámara's Digital Certification System is built upon strict compliance with its policies and procedures. The trust it engenders among its participants directly depends on adherence to these standards. All participants must extend all cooperation within their power to foster the trust inherent in the digital certification system, complying with the established policies and procedures at all times.

a. Reliability of Digital Signatures

Before relying on a digital signature certified by Certicámara, the relying party has a duty to strictly follow the instructions specified below:

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

1. The relying party must determine the reliability of the digital certificate in accordance with the provisions of 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 the certificate has not been revoked.
3. The relying party must take into account all other policies and procedures governing Certicámara's activities as specified in its Certification Practice Statement.

b. Reliability of the Digital Certificate

The relying party must follow the guidelines listed below if they intend to rely on a digital certificate issued by Certicámara:

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

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

- The agreement executed with each subscriber of the digital certification service, which contains the general terms and conditions for contracting Certicámara S.A.'s digital certification services, the clauses of which are available in the application form (https://ventadigital.certicamara.com/).

- This Certification Practice Statement regarding digital signatures issued through its digital certificates. The relying party must take these provisions into account whenever they intend to rely on a digital certificate.

9. CONFIDENTIALITY OF INFORMATION

Certicámara is committed to protecting all data to which it has access as a result of its operations as a certification authority.

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

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

These obligations do not apply if the information classified as "confidential" is requested by competent courts or administrative bodies, or if its disclosure is mandated by law. In such events, the confidential information provided by the subscriber will be disclosed in compliance with current regulations.

The confidential information of the digital certification services subscriber may be disclosed upon their request, in their capacity as the owner thereof.

9.1 Scope of Confidential Information

The following is considered confidential information:

- Documents containing information related to the administration, management, and control of the PKI infrastructure.
- Business information provided by vendors and other entities with whom Certicámara has a legal or contractual duty of nondisclosure.
- Information resulting from inquiries made to credit bureaus or other private or public sector entities.
- Employment information containing relevant data of the subscriber.
- All information submitted to Certicámara 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 issued certificates
- Certificate Revocation Lists (CRLs)
- The public keys of the Root CA and Subordinate CA
- The Certification Practice Statement (CPS)
- Organizational policies

9.3 Responsibility to Protect Confidential Information

As an accredited open digital certification authority, Certicámara S.A. is committed to safeguarding the confidentiality, integrity, and availability of all information managed within the framework of its certification services. This includes, but is not limited to, the personal information of subscribers, private keys, digital certificate data, and any other information that, by its nature, must be treated with the utmost discretion.

To ensure the protection of this information, we pledge to:

- Implement and maintain strict information security policies and procedures that comply with national and international standards, including ONAC requirements and current data protection legislation.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A

- Continuously train all personnel on information security best practices, the importance of confidentiality, and their individual responsibilities regarding data protection.
- Utilize robust and updated security technologies and systems, including data encryption, strict access controls, intrusion detection systems, and data backup and recovery mechanisms.
- Limit access to confidential information solely to authorized personnel who require such information to perform their duties. All access is monitored and logged.
- Establish non-disclosure agreements with all employees, contractors, and third parties who may have access to sensitive information.
- Securely and responsibly manage subscribers' private key information, ensuring its protection against unauthorized access, disclosure, alteration, or destruction.
- Timely notify competent authorities and affected parties of any security incident that compromises the confidentiality, integrity, or availability of information, in accordance with applicable regulatory frameworks.
- Conduct regular internal and external audits to evaluate the effectiveness of our security controls and ensure ongoing 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 Processing of Personal Data

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

To guarantee the proper processing of the personal data that Certicámara S.A. collects or has access to, it pledges to:

- Collect personal data only when necessary and relevant for the provision of its digital certification services, identity verification, and the issuance, renewal, suspension, or revocation of certificates, as well as for compliance with our legal and contractual obligations.
- Inform data subjects of the specific purpose for which their data will be collected and processed, obtaining their prior, express, and informed consent, unless otherwise required or permitted by law.
- Use personal data exclusively for the disclosed and authorized purposes, refraining from utilizing it for purposes other than those established in its personal data processing policy, authorizations, or privacy notice provided at the time of collection.
- Guarantee the accuracy, update, and completeness of the information residing in our databases, implementing the necessary mechanisms for data subjects to update or rectify their data.

FOR THE EXCLUSIVE USE OF CERTICAMARA S.A.

- Implement rigorous technical, human, and administrative measures to safeguard the security of personal data, preventing its alteration, loss, unauthorized or fraudulent consultation, use, or access.
- Permit data subjects to access their personal data and information regarding its processing, as well as facilitate the exercise of their rights to know, update, rectify, and delete their data, and to revoke the granted authorization.
- Maintain the confidentiality of personal data even after the relationship with the data subject has ended, except in cases where the information is required by a judicial or administrative authority in the exercise of its legal functions.
- Not transfer or communicate personal data to third parties without the express authorization of the data subject, except in cases permitted or required by law for the fulfillment of a legal or contractual function.

Certicámara makes its personal data processing policy available to applicants and subscribers on its website at the following online location: https://web.certicamara.com/politicas

9.5 Disclosure Pursuant to a Judicial or Administrative Process

Information is neither available nor disclosed to unauthorized individuals, entities, or processes. It may only be disclosed upon a formal requirement from a judicial or administrative authority acting in the exercise of its duties.

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

10. DIGITAL CERTIFICATE ISSUANCE SERVICE FEES

The fees established by CERTICÁMARA for the provision of digital signature certificate services are determined in accordance with the contractual terms agreed upon with the service applicants and will be properly calculated and settled by CERTICÁMARA.

Fees for the provision of the digital signature certificate service will be established based on the client's needs and the volume of digital signature certificates required, utilizing the following base retail prices:

Device Type	Policy	Quantity	Fee		Renewal/Replacement Fee	
			1 year	2 year	1 year	2 year
Virtual Token (Certitoken)	Company/Entity Affiliation Company/Entity Representative Public Official	Unit	$233.500	$310.500	$233.500	$310.500

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

Physical Token	Qualified Professional Natural Person	Unit	$313.500	$441.500	$313.500	$441.500
Physical Token (Reuse)		Unit	$273.500	$362.500	$273.500	$362.500
PKCS# 10	Natural Person / Legal Entity	Unit	$625.500	$932.500	$625.500	$932.500

- The renewal fees for digital signature certificates are identical to those specified in the table above.
- The aforementioned prices do not include Value Added Tax (VAT).
- The specified rates may vary based on special commercial agreements executed with entities and subscribers, or due to promotional campaigns.
- The validity period for a one-year certificate is defined as 365 calendar days.

Applicants will be able to access the applicable fees 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 to which they belong, the respective fee will be calculated.

11. MODELS AND TEMPLATES FOR TERMS AND CONDITIONS DOCUMENTS

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

In the event of specific commercial arrangements with a client, a dedicated agreement detailing such circumstances may be executed between Certicámara and the client.

12. APPLICABLE REGULATIONS

Digital signature certificates are issued in compliance with the regulatory or technical documents defined within the scope of accreditation granted by ONAC, which is published at https://onac.org.co/directorio-de-acreditados/

13. REVISION HISTORY

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

Date	Reason for Update
07/09/2022	• Within the framework of compliance with the provisions of Chapter 48 of the DURSCIT, Article 2.2.2.48.3.1 (Certification Practice Statement - CPS), and in alignment with the RFC 3647 standard, the sections herein are aligned with the requirements established in these documents. This document has been created to provide greater clarity to applicants and subscribers regarding the provisions, information, guidelines, controls, and other terms applicable to the digital signature certificate service. In light of the foregoing, a new document code and version have been assigned in accordance with the organization's process structure.
28/09/2022	✔ The following changes have been made to the document: • Care guidelines for the protection of physical, virtual, and PKCS#10 cryptographic devices. • Information published in the templates for each policy. • Information regarding private key restoration and the generation and installation of the key
31/10/2022	✔ Section 9.3 (Security Systems to Protect Information) has been included, outlining the established procedures for safeguarding the information collected during certificate issuance.
16/02/2023	The following changes have been made to the document: • Update of the fees for the year 2023. • Inclusion of section 3.10 (Replacement of Digital Signature Certificates), clarifying the mandatory requirement to generate a new certificate and detailing the conditions that the subscriber must consider for its management. • Incorporation of the definition of Physical Token (Reuse) as a delivery method. • Update of policy names in accordance with ONAC accreditation.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

Date	Reason for Update
21/07/2023	The following adjustments have been made to the document: • Clarification that the address, city/municipality, and department information contained in the OIDs for all policies must match the data reported in the Single Tax Registry (RUT). • Update of the fees for the following certificates: Physical Digital Token, Physical Digital Token (Reuse), and Digital Certitoken. • Update of the URLs for the new 4026 distribution points for the Certificate Revocation List (CRL).
18/09/2023	The following adjustments have been made to the document: • Update of the certificate application channels. • Section 2.3 ("Certicámara ECD Certificate Types") specifies the required documentation for each policy type. • Within policy 2.3.5 ("Natural Person / Legal Entity Digital Certificate"), clarification is provided regarding the designated platform for request generation, key pairing, and other aspects concerning the signature request, along with the subscriber's liability for certificates issued under this modality. • Section 3.1 ("Certificate Application") provides clarification regarding the temporary suspension of digital signature certificates on the macOS operating system.
15/01/2024	The following changes have been made to the document: • Section 3.1 ("Certificate Application") has been updated to include the full, unconditional, and complete acceptance of the service's Terms and Conditions, as well as the Declarations and Commitments regarding the prevention of money laundering, terrorist financing, the financing of the proliferation of weapons of mass destruction, corruption, and transnational bribery. Furthermore, it details the identity verification process to be conducted on the applicant during the application stage. • Clarification in section 3.6.1 ("Renewal Timelines") stating that the issuance of a new digital certificate requires the prior acceptance of the service's Terms and Conditions, the Declarations and Commitments regarding the prevention of money laundering, terrorist financing, the financing of the proliferation of weapons of mass destruction, corruption, and transnational bribery, and the completion of identity verification when registering a new application.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

Date	Reason for Update
	• Update of the fees for the year 2024.
18/03/2024	The following adjustments have been made to the document: • Removal of the application requirement for an "Employment certificate when the technical contact is different from the legal representative (Applies to Legal Entities and when signature use is other than electronic invoicing) Natural Person requirements". • In section 3.1 ("Certificate Application"), it is clarified that identity verification forms part of the requirements that the subscriber must fulfill. • Update of hyperlinks to reflect changes on the website. • Update of the regulations applicable to the service..
09/09/2024	The following adjustments have been made to the document: • Update of the delivery processing timelines for digital certificates on physical media. • Update to a 4096-bit key length for the issuance of digital certificates. • Inclusion of the following policies: Natural Person PKCS#10 Digital Certificate and Legal Entity PKCS#10 Digital Certificate.
05/08/2025	The following changes have been made to the document: • Comprehensive editorial adjustments to enhance the clarity and precision of the information. • Update to the approval process for amendments to the CPS. • Revision of the download timeframe terms and conditions. • Inclusion clarifying that the digital certificate revocation procedure incurs no cost. • Removal of the national toll-free hotline. • Update of links. • Removal of the national toll-free hotline. • Removal of the "Subscriber Refund Policies" section, given that these conditions are comprehensively established for all products within the overarching Certification Practice Statement. • Update of fees..

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A

certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

Date	Reason for Update
26/09/2025	The following changes have been made to the document: • Clarification within the requirements section of each policy specifying whether the Single Tax Registry (RUT) must belong to a natural person or a legal entity. • Clarification regarding the documents accepted as equivalent to the RUT for natural person digital certificate applications. • Adjustment of the guidelines for resetting virtual token passwords, specifying that this process incurs no cost for up to ten (10) requests. • Clarification that the designated timeframe for downloading the digital certificate is ninety (90) calendar days.
20/04/2026	The following changes have been made to the document: • Comprehensive update of customer service channels. • Update of responsible roles in accordance with changes in the organizational structure. • Modification of the description and requirements for the Natural Person Digital Certificate policy on local and/or centralized devices. • Update of the requirements for delivering physical tokens to third parties. • Change of the document code and version in accordance with process modifications..
01/06/2026	The following changes have been made to the document: • Comprehensive update of links in accordance with website modifications. • Adjustment of issuance requirements for each of the policies. • Update of the method for resetting virtual token passwords. • Clarification of the channels available to request revocation. • Update of fees.
21/09/2026	The following changes are made to the document: • Clarity on the use of natural person certificates in local and centralized devices, and Natural Person / Legal Entity Digital Certificate, to provide greater clarity to the applicant. • Adjustment of technical regulations for FIPS 140-3 certificates throughout the entire document.

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A.

certicámara.

Code:	IDI-L-002
Date:	11/11/2026
Version:	004
Labeling:	PÚBLIC

CERTIFICATION POLICY – DIGITAL SIGNATURE CERTIFICATE

Date	Reason for Update
	• Adjustment of revocation grounds in accordance with the operational model. • As part of the technical features for virtual token certificates, "RSE: Two-factor authentication" is included.
11/11/2026	The following changes are made to the document: • In Section 3.5.4, "Private Key Destruction Method," the method used for the destruction of keys for digital certificates issued on a physical token is adjusted."

FOR THE EXCLUSIVE USE OF CERTICÁMARA S.A