certicámara.
Validez y seguridad jurídica electrónica

Certification Policy - Digital Signature Certificate

Code: DYD-L-007
Date: july 2023
Version: 005

CERTIFICATION POLICY - DIGITAL SIGNATURE CERTIFICATE

Content

CERTIFICATION POLICY - DIGITAL SIGNATURE CERTIFICATE

1. INTRODUCTION

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

This certification policy (PC) has been structured in accordance with the recommendations of RFC 3628, RFC 3161 and the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014 and the regulations that modify or complement them, in the Colombian territory.

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

1.1 Name and identification of the document

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

Name	Certification Policies - Digital signature certificate
Date of publication	21/07/2023
Version	005
Code	DYD-L-007
Location	https://web.certicamara.com/marco_legal

1.2 Scope

This document establishes the standards and rules to be followed by the Certicámara Certification Body to offer the digital signature certificate service as established in the accreditation certificate issued by the National Accreditation Body ONAC on its website https://onac.org.co/certificados/16-ECD-002.pdf.

1.3 Procedure for updating or approving the policy

The update of the certification policy - Digital Signature Certificate of the Digital Signature Certificate service, shall be performed every time it is required by legal, regulatory and/or applicable issues to the accredited services.

To this end, the CPD and CP change committee will meet to evaluate the changes and/or modifications to be made, which will be approved by the Executive President.

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

1.4 Publishing responsibilities

It is the obligation of the Certification Entity to publish information about its practices, its certificates and the updated status of such certificates. The publications made by Certicámara of any information classified as public, will be announced on its respective web page as follows:

a) The list of Revoked Certificates (CRL) is available in CRL V2 format in the root CA repository.
b) The 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 is available on the Root CA website https://web.certicamara.com/marco_legal.
d) The public keys of the certificates issued by the subordinate CA are available in the public LDAP repository, in X.509 v3 format and at the address https://ar.certicamara.com:8443/Search/, which can be consulted by a search parameter.
e) Certicámara's contact information at https://web.certicamara.com/.
f) The Root CA's operating instructions and all information considered relevant to the certificates issued can be found at https://web.certicamara.com/soporte_tecnico.
g) OCSP certificate revocation status is available for consultation via the web at http://ocsp.certicamara.com and http://ocsp.certicamara.co.

2. POLICY IDENTIFICATION

2.1 Policy identification criteria

Each of the certificates issued by Certicámara has an OID identifier related to the extension, which is detailed in the certificate properties. This OID identifier links the issued certificate with the corresponding Certification Policy, which confirms compliance with the conditions described above.

2.2 Policy OID

Each certificate type shall be identified by a unique OID (Object Identifier), 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	Belonging to a Company / Entity
1.3.6.1.4.1.23267.50.1.2	Company / Entity Representation
1.3.6.1.4.1.23267.50.1.3	Head of Civil Service
1.3.6.1.4.1.23267.50.1.4	Qualified Professional
1.3.6.1.4.1.23267.50.1.5	Natural Person
1.3.6.1.4.1.23267.50.1.2	Legal Entity

2.3 Types of ECD Certicámara certificates

Seeking to meet the different needs that arise in the context of the growing use of information and communications technologies, Certicámara generates various types of digital certificates, which are issued with a maximum validity of two (2) years, in accordance with the provisions of the Specific Criteria for Accreditation in force, which is in accordance with the section on Life Cycle of the certificates of this document.

2.3.1 Company / Entity Representation Certificate - Local and/or centralized devices.

It is issued to national or foreign individuals who have been fully identified before Certicámara with valid and current identity document(s) issued by the competent authority of the Republic of Colombia, or with equivalent document(s) issued by the competent authority of any Foreign State, being linked with the quality of legal representative of a legal person or State Entity.
The Company/Entity Representation Certificates certify the identity of a natural person linking it with the legal representation of a legal person, a State Entity, or as a natural person trader in the scope of its professional or mercantile activity.
The Company/Entity Representation Certificates have as subscriber both the natural person acting on behalf and legal representation of a legal entity, and the represented legal entity that also appears in the digital certificate.

- Issuance requirements

  - The applicant must fill out the Digital Certification Services Provision Form for the type Company/Entity Representation Certificate, attaching the requested documents found in the link: https://solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso.aspx
  - The applicant's identity has been validated in accordance with the initial validation of the subscriber's identity.
  - The information published in the respective certificate includes:

Common Name (CN)	Subscriber's Name(s) and Last Name(s) (Legal Representative)
Serial Number	Unique Digital Certificate Identifier
3. Organization (O)	Company Name of the Organization to which the Subscriber belongs
4. 1.3.6.1.4.1.23267.2.1	Agreement Code
5. 1.3.6.1.4.1.23267.2.2	Subscriber's Identification Document Number
6. 1.3.6.1.4.1.23267.2.3	Organization Identification Number
7. Title (T)	Name of the Subscriber's Position in the Organization
8. Organizational Unit (OU)	Agreement - Certificate Validity - Physical / Virtual Token
9. Street Address (STREET)	Management of the Organization (as reported in the RUT)
10. Country (C)	Country of Certificate Issuance
11. State Or Province Name (S)	City / Municipality of Subscriber's Organization (as reported in the RUT)
12. Locality (L)	Underwriter Organization Department (as reported in the RUT)
13. Surname (SN)	Subscriber's Last Name(s)
14. Given Name (G)	First Subscriber Name

2.3.2 Company / Entity Membership Certificate - Local and/or centralized devices.

It is issued to national or foreign natural persons who have been fully identified before Certicámara with valid and current identity document(s) issued by the competent authority of the Republic of Colombia, or with equivalent document(s) issued by the competent authority of any foreign state, and allows identifying them as natural persons, linking them as belonging to a certain business organization or state entity, but without having the legal representation of the same or the power to legally bind them.

The subscribers of this type of digital certificates are: 1) The natural person who can sufficiently prove, in the opinion of Certicámara, that there is a legal, labor or any other kind of relationship with the legal person or entity of the State that will appear in the digital certificate. 2) The legal entity that appears in the digital certificate.

- Issuance requirements

- The applicant must fill out the Digital Certification Service Provision Form for the type Certificate of Membership in a Company/Entity, attaching the documents requested at the next link: https://solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso .asp x
- The applicant's identity has been validated in accordance with the initial validation of the subscriber's identity.
- The information published in the respective certificate includes:

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

2.3.3 Qualified Professional Certificate - Local and/or centralized devices.

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

CERTIFICATION POLICY - DIGITAL SIGNATURE CERTIFICATE

The **subscribers** of this type of **digital certificates** are the natural persons who can sufficiently prove, in the opinion of Certicámara, that they have obtained a professional degree duly recognized in the Republic of Colombia or in a foreign state, and that they have obtained the corresponding registration, license, professional license or professional card required for the exercise of their profession in the Republic of Colombia or in a foreign state.

- Issuance requirements

- The applicant must fill out the Digital Certification Services Provision Form for the Qualified Professional Certificate type, attaching the following documents documents requested at the next link: https://solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso.aspx
- The applicant's identity has been validated in accordance with the initial validation of the subscriber's identity.
- The information published in the respective certificate includes:

Common Name (CN)	Subscriber's First Name(s) and Last Name(s)
Serial Number	Unique Digital Certificate Identifier
3. Organization (O)	Company Name of the Organization to which the Subscriber belongs / Subscriber's First Name(s) and Last Name(s). *(Depends on the information entered in the application*)
4. 1.3.6.1.4.1.23267.2.1	Agreement Code
5. 1.3.6.1.4.1.23267.2.2	Subscriber's Identification Document Number
6. 1.3.6.1.4.1.23267.2.3	Organization ID Number / Subscriber ID Number with or without check digit*(Depends on the information entered in the application*)
7. Title (T)	Name of Subscriber's Profession
8. Organizational Unit (OU)	Agreement - Certificate Validity - Physical / Virtual Token
9. Street Address (STREET)	Organization's Address / Subscriber's Address*(Depends on information entered in application*) (as reported in the RUT)
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*) (as reported in the RUT)
12. Locality (L)	Department of the Organization / Subscriber (*Depends on the information entered in the application*) (as reported in the RUT)
13. Surname (SN)	Subscriber's Last Name(s)

14. Given Name (G)	First Subscriber Name

2.3.4 Civil Service Holder Certificate - Local and/or centralized devices.

It is issued to national or foreign natural persons who have been fully identified before Certicámara with valid and current identity document(s) issued by the competent authority of the Republic of Colombia, or with equivalent document(s) issued by the competent authority of any foreign state, allowing identification as a natural person and linking him/her as a public official belonging to a state entity in the Republic of Colombia.

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

The Certificate of Public Function Holder does not guarantee the quality, suitability, or effective fulfillment of the functions of its holder. Certicámara does not guarantee that the subscriber of the Public Function Holder certificate has been subject to disciplinary, administrative, criminal or any other kind of sanctions in the Republic of Colombia or abroad. For the issuance of the Certificate of Public Function Holder, Certicámara relies on the documentation exhibited and the declarations made by the subscriber at the time of requesting the service. As long as the law or applicable regulations do not provide otherwise, the application for the Issuance of the Civil Service Certificate is not mandatory for the Civil Service Holders. The issuance of the Public Function Certificate does not limit the subscriber to apply for other digital certificates.

- Issuance requirements

- The applicant must fill out the Digital Certification Services Provision Form for the type Public Function Holder Certificate attaching the requested documents in the following link: https://solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso.aspx
- The applicant's identity has been validated in accordance with the initial validation of the subscriber's identity.
- The information published in the respective certificate includes:

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

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

2.3.5 Digital Certificate Natural Person / Legal Entity - Local and/or centralized devices.

It is issued to nationals, foreigners or legal entities that have been fully identified before Certicámara with valid and current identity document(s) issued by the competent authority of the Republic of Colombia, or with equivalent document(s) issued by the competent authority of any foreign state.

The Natural Person / Legal Entity Certificates have as subscriber the natural person or legal entity that, acting in its own name, can sufficiently prove, in Certicámara's opinion, its identity through the exhibition of the documentation that proves it.

- Issuance requirements

  - The applicant must fill out the Digital Certification Services Provision Form for the type Digital Certificate for Natural Person / Legal Entity attaching the requested documents in the following link: https: //solicitudes.certicamara.com/SSPS/Solicitudes/RecomendacionesUso.asp x
  - The applicant's identity has been validated in accordance with the provisions of numeral 3.1.6 - Initial validation of the subscriber's identity.
  - The information published in the respective certificate includes the following information for the Certificate of Natural Person

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

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

- The information published in the respective certificate includes the following information for the Certificate of Legal Entity

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

12. Given Name (G)	First Subscriber Name

3. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFE CYCLE

3.1 Certificate application

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

1. In person at Certicámara's facilities.
2. Virtual a through from the next link: https://solicitudes.Certicámara.com/ssps/Solicitudes/AceptoLosTerminos.aspx ,
3. For the Contact Center.
4. Or by any other electronic means available to Certicámara.

The applications will be reviewed by the RA (registration authority) according to the specific accreditation criteria of ONAC and those defined by Certicámara, for confirm its veracity and integrity. This review will be executed in a maximum of two (02) working days from the completion of the documents, together with the payment support attached by the applicant. Subsequently, the requests will be escalated to the CA (certification authority) for issuance, which has a maximum time of one business day.

The documentation submitted by the applicant will be stored in accordance with the document retention tables generated by Certicámara. The applicant's information will not be published by Certicámara unless explicit consent is given.

Applicants who make use of the system for requesting products and services subscribe electronically through acceptance of terms, the conditions of service, specified in this CPD, CP and in the contract for the provision of digital certification services.

Applicants should consider the following points before requesting the service(s) from Certicámara:

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

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

- Affiliation document to the professional risk management company.
- Other documents that allow verifying the identity or powers of the subscriber or the entity, for the issuance of any of the types of certificates issued by Certicámara.

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

c) It will consult the databases necessary to comply with SAGRILAFT.

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

e) It reserves the right to deny the issuance of a digital certificate to an applicant, when in its judgment it is detrimental to the good name of ECD, according to the applicant's background or activities, without being held liable for this reason.

f) If Certicámara decides to reject the request for the issuance of the digital signature certificate, it will notify the applicant in writing, by e-mail, indicating the reasons that justify it.

- Who can submit an application for a certificate?

The application for a certificate may be made by any person of legal age who is capable of assuming the obligations and responsibilities inherent to the type of certificate requested.

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

3.2 Issuance of certificates

3.2.1 CA actions during certificate issuance

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

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

In the issuance of certificates, the Subordinate CA:

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

3.2.2 Notification to the subscriber by the CA of certificate issuance

The subscriber will know about the effective issuance of the certificate by means of a notification sent to his registered e-mail address.

3.2.3 Restoration of the private key

In the case of digital signature certificates in a virtual environment, Certicámara has implemented secure mechanisms that allow the subscriber to manage the change of his/her password without the knowledge of the password by the subscriber. In the case of a digital signature certificate in a physical medium, the subscriber will not be able to restore his private key, but will be able to change it when required.

3.3 Delivery of the digital certificate to subscribers by physical means

3.3.1 Coverage

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

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

3.3.2 Delivery requirements

The delivery is made in any of the event's prior identification of the applicant; if it is impossible to deliver the digital certificate personally, the applicant must authorize a third party to receive it through a power of attorney signed by the applicant, attaching a copy of the identification document of the applicant and the authorized third party. The logistic operator's guide will serve as evidence of the acknowledgement of receipt of the digital

signature certificate. In the events that the contracting entity has a coordinator in charge of the administration of the digital certificates, he/she may receive and distribute the certificates after validation by Certicámara.

3.3.3 Delivery management time - Physical Certificates

In urban areas and major cities, the delivery time from the issuance of the certificate to the delivery to the applicant will be approximately two (2) business days; if it is impossible to locate the applicant or authorized third party, the delivery time may be five (5) business days.

At national level and intermediate cities, the delivery time from the issuance of the certificate to the delivery to the applicant will be approximately three (3) working days; if it is impossible to locate the applicant or authorized third party, such term may be eight (8) working days.

For special destinations, the delivery time from the issuance of the certificate to the delivery to the applicant will be approximately four (4) working days; if it is impossible to locate the applicant or authorized third party, this term may be nine (9) working days.

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

3.3.4 Download Time - Virtual Certificate

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

In the events in which the download of the certificate is not possible due to a cause associated to the subscriber, Certicámara will contact the applicant to coordinate the download process. If no response is received with the download date of the digital signature certificate, Certicámara will block the download link and will only be reactivated upon request of the client for a period of three (3) months from the date of issuance. Once this term has expired and the subscriber has not made any statement, it will be understood that he/she has abandoned the property and Certicámara will proceed with the revocation. If the applicant requires the issuance of a digital signature certificate, he/she must initiate the application process as established by Certicámara.

3.4 Acceptance of the certificate

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

3.4.1 Publication of the certificate by the CA

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

In the event of any technical inconvenience that prevents its publication, this will occur within the month following the issuance of the certificate in accordance with the result of the technical analysis that has prevented its immediate publication.

3.4.2 Notification of certificate issuance by the CA to other entities

Certicámara has a repository of LDAP digital certificates, in which entities, government agencies, private companies and other interested parties may consult the issuance of certificates. It is available at the following URL: https://ar.Certicámara.com:8443/Search/ . The publication in this repository is done 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 cryptographic device (HSM) that complies with the requirements set forth in a standardized certificate authority's electronic signature secure device protection profile, in accordance with FIPS 140-2 Level 3 or higher security level, and the CA's key creation uses a pseudo-random number generation algorithm. The Root CA generates the key pair (Public and Private) using a hardware cryptographic device (HSM) that meets the requirements of a standardized certificate authority's electronic signature secure device protection profile, in accordance with FIPS 140-2 Level 3 or higher security level, and the CA's key creation uses a pseudo-random number generation algorithm.

3.5.2 Use of certificate and subscriber's private key

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

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

Bona fide third parties may only rely on certificates for what is established in the CPD, CP and regulations.

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

3.5.4 Private key destruction method

The Root CA and the Subordinate CA will delete its private key when its term expires or has been revoked. The destruction will be performed using the commands set to physically erase from the HSM memory the part in which the key was recorded. The same will be true for your backups.

3.6 Certificate renewal

3.6.1 Time for renewal

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

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

Renewal shall be understood as the issuance of a new digital certificate, which implies the registration of a new application, which will be subject to identity validation by the registration authority, and the generation of a new key pair.

3.6.2 Who can apply for renewal

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

3.6.3 Processing of certificate renewal applications

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

3.6.4 Notification of issuance of new certificate to subscriber

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

3.7 Certificate key renewal

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

3.8 Modification of the certificate

During the life cycle of a certificate, there are no plans to modify/update the fields contained in the certificate. If a change in the issued certificate data is required, it will be necessary to revoke the certificate and issue a new one with the corresponding modifications.

3.9 Revocation and suspension of certificates

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

Additionally, Certicámara does not allow suspended status on digital certificates.

3.9.1 Grounds for revocation

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

a) For compromise of safety in any reason, manner, situation or circumstance.

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

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

d) By death of the subscriber.

e) By supervening incapacity of the subscriber.

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

g) For updating the information contained in the digital certificate.

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

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

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

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

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

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

n) For any because that reasonably leads to believe that the certification service has been compromised to the extent that the trustworthiness of the digital certificate is in doubt.

o) For improper handling by the subscriber of the digital certificate.

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

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

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

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

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

3.9.2 Who can request revocation?

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

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

3.9.3 Revocation request procedure

The subscriber in case of requiring the revocation of its digital signature certificate for any of the reasons described above, may use the following means for the reception of its request:

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

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

Certicámara will validate the identity of the subscriber who invokes the cause for revocation. If the person submitting the said statement is not the subscriber, or if he/she is the subscriber, he/she cannot identify him/herself satisfactorily, he/she must go in person to Certicámara's offices during office hours at 08:00 a.m. - 05:00 p.m. Monday through Friday, with proof of the existence of the respective cause for revocation in applicable cases, without prejudice that Certicámara has the measures established for the security of the Digital Certification System. It is clarified that once the revocation request is received and the veracity of such request is verified, the certificate will be revoked, with no grace periods for such revocations.

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

3.9.4 Grace period of the revocation request

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

3.9.5 Frequency of CRL issuance

The list of Revoked Certificates of the Subordinate CA Certicámara (CRL) and CA SUB CERTICÁMARA (CRL) is published for three (3) days:

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

3.9.6 On-line status check/revocation available

The Certificate Revocation List (CRL) and the Online Certificate Status Validation Service (OCSP) will be available for consultation 365 days a year, 24 hours a day, 7 days a week. This service will be provided with a 99.8% availability agreement.

3.9.7 Online revocation verification requirements

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

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

3.9.8 Circumstances of suspension

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

3.10 Digital Signature Certificates replacements

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

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

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

- Digital certificates that are less than ninety (90) days from their expiration date shall not be replaced.
- The same certification policy with which it was initially issued must be maintained.

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

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

- The subscriber must generate the request in Certicámara's web page: https://web.certicamara.com/soporte_tecnico, under the replacement project.
- The generation of the new signature must be done according to the contents of section 4.2 of this Certification Practices Statement.
- The subscriber must revoke the digital signature certificate. To do so, there are two possibilities:
  i. The holder of the digital signature certificate, or an authorized third party, shall send the corresponding form authorizing the revocation of the digital certificate to the e-mail revocaciones@certicamara.com. The form may be requested by contacting the customer service line provided by Certicámara (601) 7442727 option 2, option 1.
  ii. Through the following link where, by accepting the terms and conditions, you can carry out the process personally https://solicitudes.certicamara.com/SSPS/solicitudes/RevocarCertificadoClienteCF.aspx.

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

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

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

3.10.1 Grounds for Replenishment

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

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

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

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

3.11 Characteristics of the certificates

3.11.1 Operational characteristics

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

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

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

- http://www.Certicámara.com/repositoriorevocaciones/ac_subordinada_Certicámara.crl?crl=crl
- http://www.Certicámara.com/repositoriorevocaciones/ac_subordinada_Certicámara_con_extension_critica.crl?crl=crl
- http://www.Certicámara.com/repositoriorevocaciones/ac_subordinada_Certicámara_2014.crl?crl=crl
- http://www.Certicámara.com/repositoriorevocaciones/ac_subordinada_Certicámara_con_extension_critica_2014.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_con_extension_critica_4096.crl?crl=crl
- http://www.certicamara.com/repositoriorevocaciones/ac_subordinada_certicamara_4096.crl?crl=crl

3.11.2 Service availability

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

Optional functions

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

3.12 End of subscription

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

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

3.13 Custody and recovery of keys

3.13.1 Key custody and retrieval policy and practices

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

4. USES OF CERTIFICATES

4.1 General uses of digital certificates

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

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

3. The use of the digital certificate and the data messages that are digitally signed with it, including electronic monetary transactions, regardless of their amount, are the TOTAL responsibility of the corresponding subscriber and, therefore, Certicámara has no responsibility whatsoever for the verification or public faith of the signed data messages, since it does not know and has no legal obligation to know the digitally signed messages or the amount of transactions that are made with the digital certificate in third party electronic transaction systems.Certicámara has no responsibility for the verification or public faith of the signed data messages, since it does not know and has no legal obligation to know the digitally signed messages or the amount of the transactions that are made with the digital certificate in electronic transaction systems of third parties. In general, Certicámara as an Open Digital Certification Entity and Trusted Third Party does not commit its responsibility in the use made by the subscriber of the digital signature certificates, therefore, there are no financial limits applicable in this regard. For such purpose, the subscriber shall comply with its duties under

Law 527 of 1999 and Decree 1074 of 2015 (which compiles Decree 333 of 2014), as well as shall meet the burden of responsibility imposed by such regulations.

4.2 Prohibitions on the use of certificates

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

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

c) The use of digital certificates and the Digital Certification System as a control system for high-risk activities or for fail-safe systems, including but not limited to the following, is prohibited:

- Navigation systems for land, air or sea transportation.
- Air traffic control systems.
- Weapons control systems.

d) Digital certificates may not be used in any system whose failure could cause death or injury to persons or cause serious damage to the environment.

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

4.3 Validity of certificates

Certicámara issues different types of digital certificates, which are issued with a maximum validity of 2 years, equivalent to 730 days, in accordance with the provisions of the CEA in force.

5. CHARACTERISTICS OF THE CERTIFICATES

5.1 Digital certificate on physical token

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

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

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

5.1.1 Technical Aspects

- ✓ Private key length of 2048 bits.
- ✓ Certificate signing algorithm with RSA-SHA-2 hash 256 -2056
- ✓ API and standards support (PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, MS minidriver, CNG)
- ✓ Memory capacity 80K. With retention of at least 10 years.
- ✓ Dimensions: 5110 - 16.4mm*8.5mm*40.2mm.
- ✓ Compatible with ISO 7816-1 and 4 specifications.
- ✓ Molded rigid plastic, tamper-evident closure.
- ✓ Windows (Server 2008/R2, Server 2012/R2, 7, 8 and 10).
- ✓ Linux.
- ✓ Mac OS (Gemalto only)
- ✓ USB connector.

5.1.2 Care of the cryptographic device

- ✓ 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- 100% without condensation
- ✓ IPX7 water resistance certification - IEC 60529

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

- ✓ The password must be for personal use and must not be transferred to a

third party.
- ✓ Store your password in safe places, it is recommended to memorize it to prevent others from knowing it.
- ✓ Do not leave the device connected to the equipment when not in use.
- ✓ Correctly disconnect the device
- ✓ Avoid bumps and falls.
- ✓ Use the applications provided by Certicámara for the use of your certificate.

5.1.3 Associated risks

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

- ✓ Fluctuations source de the ranges operation environmental standards, such as voltage and temperature.
- ✓ Attempts to physically access outside of the unauthorized manufacturer's datasheet

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

5.2 Virtual token certificate

It corresponds to an infrastructure available as a service in which the digital certificates issued along with its key pair are stored in the technological infrastructure of Certicámara, which are associated with a username and password given to the certificate holder. An active Internet connection is required for its use.

5.2.1 Features

- ✓ 2048-bit private key.
- ✓ Certificate signing algorithm with SHA256 hash.
- ✓ X.509 v3 certificates.
- ✓ FIPS 140-2 Level 3 compliant infrastructure storage.
- ✓ Signature of files signed with the hash of the document (does not require sending the document to protect its confidentiality).
- ✓ Network access to the domain *.certicamara.com on port 443.
- ✓ Signature component that allows the consumption of Certitoken
- ✓ Java minimum in See 7
- ✓ Windows 7 or higher
- ✓ Framework 4.0 or higher

- ✓ Access to URLs
  - https://certitoken.certicamara.com/certificate/list
  - https://certitoken.certicamara.com/sign

5.2.2 Care of the device

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

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

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

5.2.3 Associated risks

For the virtual token certificate, the risks to which it is exposed are those in which environmental aspects prevent the proper functioning of the datacenter where the HSM is installed.

In logical issues, the associated risks are defined by cyber-attacks that prevent access and/or availability.

5.3 Digital certificate in PKCS#10

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

5.3.1 Features

- ✓ 2048-bit public key.
- ✓ Certificate signing algorithm with SHA256 hash.
- ✓ Public key signed in *.CER format according to Certicámara's chain of

trust.

- ✓ Emission using the PKCS#10 standard.
- ✓ Generate a Certificate Signing Request - CSR – in PKCS#10 format.
- ✓ Ability to receive and use the public key in CER format.

5.3.2 Care of the device

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

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

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

5.3.3 Associated risks

For the PKCS#10 certificate, the risks to which it is exposed are those in which environmental aspects prevent the proper functioning of the datacenter where the HSM is installed.

In logical issues, the associated risks are defined by cyber-attacks that prevent access and/or the respective availability

6. OBLIGATIONS AND RESPONSIBILITIES OF THE PARTICIPANTS

The obligations and responsibilities of the participants are defined in the Certification Practices Statement document in numeral 9.5.

7. RIGHTS OF THE INTERVENING PARTIES

The rights of the participants are defined in the Declaration of Certification Practices document in paragraph 9.6.

8. RELIABILITY OF DIGITAL SIGNATURES AND CERTIFICATES.

Certicámara's Digital Certification System is a system built on strict compliance with its policies and procedures. The confidence it generates in its participants depends directly on their compliance. All the participants must provide all the cooperation within their reach for the generation of trust in the digital certification system, following at all times the established policies and procedures.

8.1 Reliability of digital signatures

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

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

8.2 Trustworthiness of the digital certificate

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

- The relying party must verify that the digital certificate has not expired, in accordance with the effective date shown on the certificate.
- The relying party must verify that the digital certificate is not in Certicámara's database of revoked digital certificates published on Certicámara's website. In any case, and without any exception, it is prohibited to determine the revocation status of a digital certificate based on information other than that in the database of revoked digital certificates.
- The reliability of the digital certificate depends on it being digitally signed by Certicámara. The relying party can verify Certicámara's digital signature by checking it against the root certificate, containing Certicámara's public key, which is available on Certicámara's 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 contract signed with each subscriber of the digital certification service, which contains the general conditions of contracting the digital certification services of Certicámara S.A., the clauses of which can be found in the application form (https://solicitudes.certicamara.com/ssps/Solicitudes/AceptoLosTerminos.aspx).
- This Certification Practices Statement in relation to digital signatures issued through its digital certificates. The relying party must take them into account whenever it intends to rely on a digital certificate.

9. CONFIDENTIALITY OF INFORMATION

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

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

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

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

9.1 Scope of confidential information

It is considered confidential information:

- Documents containing information related to the administration, management and control of the PKI infrastructure.
- The business information provided by its suppliers and other persons with whom Certicámara has a duty of secrecy established by law or convention.
- Information resulting from queries made to credit bureaus or other private or public sector entities.
- Employment information containing data related to the subscriber's salary.
- All information that is submitted to Certicámara and that has been labeled as "Confidential" by the sender.

9.2 Information outside the scope of confidential information

It is considered non-confidential information:

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

Note. All personal data of the subscriber related to the registration of certificates are treated in accordance with the Personal Data Protection Policy defined by Certicámara for this purpose and in compliance with the Statutory Law 1581 of 2012 "Protection of Personal Data", being such policy published on the website of Certicámara S.A.

9.3 Sistemas de seguridad para proteger la información

CERTICAMARA has security systems that protecting the information that is collected in order to issue the certificates, which are developed through guidelines for the management of information assets that bind all those responsible for the administration of these data, from each of their roles. In the same way, CERTICAMARA has a procedure for labeling and proper handling of information, whose main objective is to establish the step-by-step that must be followed to label the information and thus ensure that it receives an appropriate level of protection, according to their level of importance.

Likewise, CERTICAMARA has an information security management system certified under the ISO/IEC 27001:2013 standard and with a robust infrastructure that guarantees the protection of information.

10. DIGITAL CERTIFICATE ISSUANCE SERVICE FEES

The value set by CERTICÁMARA for the provision of digital signature certificate services is established in accordance with the contractual conditions agreed with the service applicants and will be properly calculated and settled by CERTICÁMARA.

The fee for the provision of digital signature certificate services will be established based on the client's needs and according to the volume of digital signature certificates that the client requires, having as base public sale prices of:

Producto	Artículo	Tipo	PVP 2023
Digital	Digital Certificate Natural Person, valid for one (1)	Unidad	$

CERTIFICATION POLICY - DIGITAL SIGNATURE CERTIFICATE

Producto	Artículo	Tipo	PVP 2023
Certificate Physical Token	year.		270,000.00
	Digital Certificate Natural Person, valid for two (2) years.	Unidad	$ 370,000.00
	Digital Certificate of Company Membership, valid for one (1) year.	Unidad	$ 270,000.00
	Digital Certificate of Membership in a Company, valid for two (2) years.	Unidad	$ 370,000.00
	Professional Digital Certificate, valid for one (1) year.	Unidad	$ 270,000.00
	Professional Digital Certificate, valid for two (2) years.	Unidad	$ 370,000.00
	Digital Certificate of Legal Representation, valid for one (1) year.	Unidad	$ 270,000.00
	Digital Certificate of Legal Representation, valid for two (2) years.	Unidad	$ 370,000.00
	Replenishment Validity (1) one year without a token	Unidad	$ 270,000.00
	Replenishment Validity (2) two years without token	Unidad	$ 370,000.00
Digital Certificate Physical Token (Reuse)	Digital Certificate Natural Person, validity (1) one year	Unidad	$ 270,000.00
	Digital Certificate Natural Person, valid for (2) two years	Unidad	$ 300,000.00
	Digital Certificate of Company Membership, valid for (1) one year	Unidad	$ 230,000.00
	Digital Certificate Belonging to a Company, valid for (2) two years	Unidad	$ 300,000.00
	Digital Certificate for Qualified Professional, valid for one year (1)	Unidad	$ 230,000.00
	Digital Certificate of Qualified Professional, valid for (2) two years	Unidad	$ 300,000.00
	Legal Representation Digital Certificate, valid for (1) one year	Unidad	$ 230,000.00
	Digital Certificate of Legal Representation, valid for (2) two years	Unidad	$ 300,000.00
Certitoken Digital Certificate	Digital Certificate Public Function, valid for one (1) year.	Unidad	$ 200,000
	Digital Certificate Public Function, valid for two (2) years.	Unidad	$ 270,000
	Digital Certificate Natural Person, valid for one (1) year.	Unidad	$ 200,000
	Digital Certificate Natural Person, valid for two (2) years.	Unidad	$ 270,000
	Digital Certificate of Company Membership, valid for one (1) year.	Unidad	$ 200,000

CERTIFICATION POLICY - DIGITAL SIGNATURE CERTIFICATE

Producto	Artículo	Tipo	PVP 2023
	Digital Certificate of Membership in a Company, valid for two (2) years.	Unidad	$ 270,000
	Professional Digital Certificate, valid for one (1) year.	Unidad	$ 200,000
	Professional Digital Certificate, valid for two (2) years.	Unidad	$ 270,000
	Digital Certificate of Legal Representation, valid for one (1) year.	Unidad	$ 200,000
	Digital Certificate of Legal Representation, valid for two (2) years.	Unidad	$ 270,000
	Replenishment Validity (1) one year	Unidad	$ 200,000
	Replenishment Validity (2) two years	Unidad	$ 270,000
PKCS#10 Digital Certificate	Digital Certificate Public Function, valid for one (1) year.	Unidad	$ 515,000
	Digital Certificate Public Function, valid for two (2) years.	Unidad	$ 870,000
	Digital Certificate Natural Person, valid for one (1) year.	Unidad	$ 515,000
	Digital Certificate Natural Person, valid for two (2) years.	Unidad	$ 870,000
	Digital Certificate of Company Membership, valid for one (1) year.	Unidad	$ 515,000
	Digital Certificate of Membership in a Company, valid for two (2) years.	Unidad	$ 870,000
	Professional Digital Certificate, valid for one (1) year.	Unidad	$ 515,000
	Professional Digital Certificate, valid for two (2) years.	Unidad	$ 870,000
	Digital Certificate of Legal Representation, valid for one (1) year.	Unidad	$ 515,000
	Digital Certificate of Legal Representation, valid for two (2) years.	Unidad	$ 870,000
	Replenishment Validity (1) one year	Unidad	$ 515,000
	Replenishment Validity (2) two years	Unidad	$ 870,000

- The price for the renewal of digital signature certificates corresponds to the same mentioned in the previous table.
- The above prices do not include VAT.
- The indicated rates may vary according to special commercial agreements with entities and subscribers or due to the development of promotional campaigns.
- It is determined that the validity of a one-year certificate is 365 calendar days.

Applicants will be able to obtain the applicable rates through the following link https://solicitudes.certicamara.com/ssps/Solicitudes/AceptoLosTerminos.aspx, where depending on the data entered by the applicant and according to the project and/or agreement to which they belong, the respective rate will be settled.

For this purpose, you may enter through Certicámara's web pagewww.certicamara.com to the Product and Service Request System to generate the request form and the corresponding Order Form and start the acquisition process.

10.1 Subscriber Refund Policies

Digital certificate subscribers may request a refund in the following cases:

- **When a deposit is made for an amount greater than the established amount:** in this case the Administrative and Financial Management performs the necessary validations to confirm the additional payment, in the event that the validation is successful, the respective reimbursement will be made to the entity or person who made the request.
- **When a digital certificate that does not apply to the subscriber is requested:** the Operations Department verifies the digital certificates issued to the subscriber and if the result of this validation confirms that the digital signature certificate is not required, authorizes the Administrative and Financial Management to proceed with the refund.

11. MODELS AND MINUTES OF TERMS AND CONDITIONS DOCUMENTS

The model of terms and conditions for the subscription used by Certicámara in the provision of the digital signature certificate service is available at the following link:

https://solicitudes.certicamara.com/ssps/Solicitudes/AceptoLosTerminos.aspx.

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

12. ASSOCIATED REGULATIONS

- RSA 2048, Final Entity / RSA 4096, Root CA.
- FIPS PUB 180-4 Secure Hash Standard (SHS) 2015-08 - SHA 256
- RFC 5280: mayo 2008 - Perfil de certificado de infraestructura de clave pública X.509 de Internet y lista de revocación de certificados (CRL).
- RFC 4523: junio 2006 - Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates.

- RFC 3647: noviembre 2003 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- ETSI TS 102 042 February 2013
- FIPS 140-2 Nivel 3 Mayo 2001
- ITU-T-X509: October 2019 - Information technology - Open Systems Interconnection - The Directory: Frameworks for public key certificates and attributes;

13. CHANGE CONTROL

Date:	Reason for update
07/09/2022	✓ In compliance with the provisions of Chapter 48 of DURSCIT, Article 2.2.2.2.48.3.1. Declaration of Certification Practices (DPC) and the RFC 3647 standard, aligning the paragraphs with the provisions of these documents and creating this document to provide greater clarity to the applicant and subscriber on the provisions, information, guidelines, controls and other applicable for the digital signature certificate service. Taking into account the above, a new code and version of the document is assigned according to the organization's process structure.
28/09/2022	✓ The following changes are made to the document: ○ Care for the protection of physical, virtual and PKCS#10 cryptographic devices. ○ Information published in the templates for each policy. ○ Information for private key restoration and key pair generation and installation.
31/10/2022	✓ Section 9.3 Security systems to protect information is included, where the procedures defined to protect the information gathered in the issuance of certificates are reported.
16/02/2023	The following changes are made to the document: ✓ Update of fees for 2023. ✓ Inclusion of item 3.10 Replacement of Digital Signature Certificates, where it is clarified that a new certificate must be generated and the conditions that the subscriber must take into account for its management. ✓ The definition of Reuse as a means of delivery of physical tokens is included.

CERTIFICATION POLICY - DIGITAL SIGNATURE CERTIFICATE

21/07/2023	The following adjustments are made to the document: ✓ Clarity that the information in the OID'S of address, city / municipality and department of all policies, will be the one reported in the RUT. ✓ Update of certificate fees: Physical Digital Token, Physical Digital Token (reuse) and Digital Certitoken. ✓ Update of the URLs of the new 4026 distribution points for the list of revoked CRL certificates.