Official Translator: José Fernando Jaramillo Sanint. Address: Calle 70A #23B – 34 Manizales - Caldas
Phone : (606) 8792900 Mobile: (310) 404-0972 - (300) 339-46-01 Email: traducciones@121.com.co

GSE

CERTIFICATE POLICIES FOR DIGITAL CERTIFICATES
Standard

Code	Name	Version	Information classification
POP-PL-55	Certificate Policies for Digital Certificate Service	18	Public

Document Title	Certificate Policies for Digital Certificate Service
Version	18
Working Group	Management Committee
Document status	Final
Date of issue	15/02/2010
Effective date	09/12/2025
OID (Object Identifier)	1.3.6.1.4.1.31136.1.4.18
Policy Location	https://gse.com.co/documentos/calidad/politicas/Politica_de_certificado_para_certificados_digitales_V18.pdf
Prepared	Operations Coordinator
Reviewed by	Integrated Management System
Approved	Management Committee
Change control	

Version	Date	Change/Modification
1	01/11/2016	Initial document in accordance with the development of the ONAC audit action plan.
2	05/10/2017	Updated information regarding the ECD GSE headquarters.
3	03/04/2018	Update in accordance with ONAC audit recommendations.
4	27/11/2018	Version 3 was changed to Version 4 on 11/26/2018. This update includes charges, fees, website access paths, title change, inclusion of the open certification authority's liability limits, service validity, obligations of the CCE, RA, EE, subscriber, responsible parties, bona fide third parties, the entity, and obligations of other participants.
5	12/04/2019	The section on EE obligations was eliminated, the responsibilities of the subscriber and responsible party were unified, the specifications for MAC use are described in the section on Supported Operating Systems, it was clarified that, for the use of centralized signature, the acquisition of a technological platform with additional costs is necessary, and the obligations of the subscribers were updated according to the type of service
6	07/06/2019	5.10.3 The subscriber's obligations and rights were clarified
7	31/03/2020	The CPs are adjusted to the changes generated by the new platforms, the Objective and Scope and policy administration sections are added, the price list is adjusted, the links are modified to point to the new routes, and the version of the ETSY and ITU-509 standards is updated.
8	14/08/2020	The contact person in section 4.1 was updated. A note was added to section 7.5: if the subscriber has a valid certificate, they may submit the digitally signed application, which will replace the documents initially requested. For the public service certificate, if the employment certificate is unavailable, the appointment document, appointment letter, or service contract may be attached. For the professional certificate, the RUT (Taxpayer Identification Number) is required (if applicable), the professional registration application is replaced with the diploma application, and the graduation certificate must be authenticated. The data from the ECD and CA(Paynet) were included with links to consult the Certificate of Existence and Legal Representation online.
9	12/02/2021	The links were updated to point to the new routes. The following sections were updated: • 7.6. Specific requirement for processing the certificate
10	16/07/2021	The following sections were updated: 3.1. Summary, PKI infrastructure service provider, CERL query URL, and contact phone numbers. 5.3. Policy OID. 7. ECD digital certificate requirements. 7.7. Specific certificate processing requirements. 8.1.1 The image of the cryptographic devices was modified The following numbers were included: 7.6 Prohibitions on the Use of Certificates 8.1.2 Security commitments

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

		8.1.3 Cryptographic device care 8.1.4 Associated risks. 7.9.3. Technical Characteristics of Digital Certificates 10. Protection of personal information 11. Impartiality and non-discrimination The OID and the policy consultation link are updated.
11	27/10/2021	• Section 7.7 Specific Requirements for Processing the Certificate was modified, including in the final Note section a clarification about the updated RUT from the DIAN which must have the QR code. • The OID and PC link were adjusted
12	31/05/2022	According to the new version of the CEA, the following adjustments were made: • 4.4 Petitions, Complaints, Claims and Requests: The term Appeal was removed. • 5.2 Certificate Content: The centralized signature certificate was removed. • 6. Types of Certificates: The purpose of the legal entity certificate was modified. • 7.4. Uses of certificates: The attribute of the legal entity certificate was modified. • 7.7. Technical requirements for processing the certificate: The description of the application documentation for the electronic invoicing certificate and the legal entity certificate was modified. • 7.9. Activities and technical references: The activities and regulatory documents for each type of certificate were modified in accordance with the ONAC accreditation certificate. • 9.1.6. Obligations of other participants in the ECD: Item r) was modified, leaving only CEA and eliminating the 4.1-10. • The OID and the Policy query link were adjusted. • The quality code was included in the document header • Section 3.1 Summary was modified to include the chapters of the duran cit. • The ECD address was modified in sections 3.1 and 4.4. • The address of Paynet SAS was modified in section 3.1.
13	23/09/2022	• The ITU X509 of 2016 was modified to ITU X509 October 2019 in the standards of each accredited service in section 7.9, and the ITU-TX.500 October 2019 and FIPS PUB 186-4 July 2013 standards were eliminated. • Section 9.1.1 was modified to include items o) through y). • Items 13 through 16 were included. • Section 7.7 of the legal representative was modified by including a paragraph in the requested documentation. • The OID and the Policy query link were adjusted • The entire order of the document was modified in accordance with the numerals of RFC 3647. • Paynet SAS was removed as the CA authority since the PKI was moved to the GSE ECD.
14	16/05/2023	• Section 1.3.8.4 was adjusted, the person responsible for complaints, claims, and requests (PQRS) was changed to Customer Service. • The Operations Director was changed to Operations Manager • The data for the main and alternate data centers was modified, leaving Hostdime and Claro. • The OID and the Policy consultation link have been updated • Section 1.9.1 was adjusted to the type of digital certificate (Person) for the requested registration. • Section 1.3.8.1 Changes in the Management Committee was modified: The management committee regulations are cited. • Section 1.9.1 Certificate Application was modified • 1.14.11.2 Obligations of the RA: Subparagraphs C and AND
15	23/10/2023	• Section 6, Certificate Profile, was modified: The OID and the link were updated.Policy consultation
16	08/07/2024	• The numbering and order are updated according to section 6, Scheme of a set

JOSE F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

		of provisions of RFC 3647 • The OID and the Policy consultation link have been updated • Features of cryptographic devices: Includes FIPS 140-2 Level 3 or higher. • Technical characteristics of digital certificates: Key generation is maintained.
17	22/10/2025	It conforms to HSM: FIPS 140-2 Level 3 or higher (Centralized Signature). The document template was adjusted.
18	09/12/2025	The position of Operations Manager is adjusted to Operations Coordinator 1.3.1 Certification Authority (CA). The information associated with the data centers is updated

table of Contents

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

1. INTRODUCTION

This document specifies the Certificate Policies for Digital Certificates (hereinafter referred to as CPs) for the various certificates issued by the ECD GSE. The purpose of the CPs is to define the requirements necessary for issuing the different ECD GSE certificates.

Insofar as the ECD GSE DPC establishes all the generic requirements regarding the security system, support, administration and issuance of ECD GSE Certificates, the policies will only refer to the specific requirements of each type of certificate, referring in the rest of the terms to what is established in the DPC.

In this way, the different ECD GSE certificates must comply with the generic requirements and security levels detailed in the DPC and the specific requirements for each one defined in this document.

ECD GSE must inform Subscribers and/or Responsible Parties of the existence of this document which answers the CPs of the different certificates issued by ECD GSE.

This document applies to issuing certificates in relation to the electronic or digital signatures of natural or legal persons, issuing certificates on the verification regarding the alteration between the sending and receiving of the data message and of transferable electronic documents, issuing certificates in relation to the person who has a right or obligation with respect to the documents stated in the subparagraphs f) and g) of article 26 of Law 527 of 1999

1.1 General Description

The Policy for Digital Certificates, hereinafter referred to as the Policy, is a document prepared by Gestión de Seguridad Electrónica SA (hereinafter referred to as GSE) which, acting as a Digital Certification Entity, contains the rules and procedures that the Digital Certification Entity (hereinafter referred to as GSE) as a Digital Certification Service Provider (PSC) applies as a guideline to provide the Service in accordance with the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014, chapters 47 and 48 of title 2 of part 2 of book 2 of the Single Decree of the Commerce, Industry and Tourism Sector - DURSCIT and the regulations that modify or complement them, in the territory of Colombia.

DATA OF THE ENTITY PROVIDING DIGITAL CERTIFICATION SERVICES:

Company Name:	ELECTRONIC SECURITY MANAGEMENT SA
Initials:	GSE SA
Tax Identification Number:	900.204.272 - 8
Commercial Registry No: Certificate of Existence and Legal Representative:	01779392 of February 28, 2008 https://gse.com.co/documentos/marco-regulatorio/Certificado-de-Existencia-y-Representante-Legal-GSE.pdf
Commercial registry status:	Active
Company address and correspondence:	77th Street No. 7 - 44 Office 701
City / Country:	Bogotá DC, Colombia
Phone:	+57 (601) 4050082
Email:	info@gse.com.co
Web page:	www.gse.com.co

1.2. Name and identification of the document Policy Identification Criteria (OID)

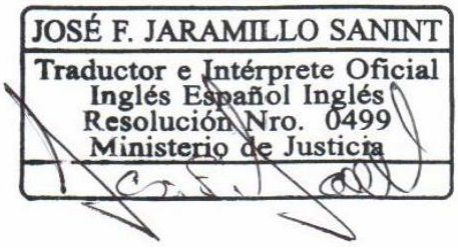
The way to identify the different types of ECD GSE digital certificates is through object identifiers (OIDs). A specific OID allows applications to clearly distinguish the certificate being presented.

The PC identifier is made up of a series of numbers separated by periods, each with a specific meaning.

Starting from the OID, the generic ECD GSE certificate is distinguished, and in turn, starting from this ECD GSE certificate, different subtypes are defined based on some specific characteristics, such as:

The content of the certificates, distinguishing:

These are signature certificates, which are further classified into other subtypes depending on whether or not they contain an attribute.The attribute constitutes the specific characteristic of the natural person holding the digital certificate that appears contained in the certificate and that can be of different types:



- Company Membership
- Company Representation
- of Public Service
- of a Qualified Professional
- of Natural Person
- of Legal Entity
- Electronic Invoice

Whoever generates the digital certificate keys, distinguishing between the certificate holder or the ECD GSE itself.
The procedure for updating the information contained in the certificates must be carried out in accordance with the DPC "Certificate Renewal with Key Change." To renew digital certificates, the procedure for requesting a new certificate must be followed. The subscriber must access the GSE products and services application web portal and initiate the certificate renewal request process in the same way as when the certificate was initially requested. Their information will be validated again to update data if necessary.

OID of Policies
The following table shows the different certificates issued by the ECD GSE, and the OIDs of their corresponding CPs, based on the different variables defined in the previous section:

OID	DESCRIPTION
1.3.6.1.4.1.31136.1.4.18	Certificate Policy for Digital Certificates

Policies assigned to this document.
This document specifically addresses the PC requirements for the following certificates and their different subtypes: . GSE-PE

- GSE-RE
- GSE-FP . GSE-PT
- GSE-PN
- GSE-PJ . GSE-FE

1.3. PKI Participants.

1.3.1. Certification Authority (CA).
It is that legal entity, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, authorized by the Colombian government or the National Accreditation Body in Colombia to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014 and the regulations that modify or complement them, is the origin of the digital certification hierarchy that allows it to provide services related to communications based on public key infrastructures.

Hierarchy of the CAs.
The GSE certification hierarchy is comprised of the following Certification Authorities (CAs):

GSE SA CERTIFICATION HIERARCHY			
GSE Root Authority		GSE ECDSA Root	GSE Root Electronic Signature
Subordinate Authority 01 GSE		GSE ECDSA Subordinate	GSE Intermediate Electronic Signature

GSE has two data centers: the (Active) data center with Sencinet Latam Colombia SA ICD Nimbus, located at Carrera 106 No. 15A25 Manzana 4 Lote 38 Zona Franca, Bogotá, Colombia, and the (Active) data center with Claro located at Autopista Medellin Km 7.5 Celta Trade Park - Datacenter Triara, Cota, Cundinamarca, Colombia.

1.3.2. Registration Authority (RA).
This is the GSE area responsible for verifying the validity of the information provided by the applicant for a digital certification service. This is done by verifying the identity of the subscriber or the entity responsible for the digital certification services. The RA (Registration Authority) decides on the issuance or activation of the digital certification service. To this end, it has defined the criteria and methods for evaluating applications.
Under this DPC, the RA figure is part of the ECD itself and may act as a Subordinate of ECD GSE.
GSE does not under any circumstances delegate the functions of Registration Authority (RA).

1.3.3. Subscribers.
Subscriber is the natural person to whom the digital certification services are issued or activated and therefore acts as subscriber or responsible for it, trusting in it, with knowledge and full acceptance of the rights and duties established and published in this DPC.

The Subscriber status will differ depending on the services provided by the ECD GSE as established in the Certificate Policies for digital certificates.

1.3.4. Relying Parties (Trusted Third Parties).

The responsible party is the natural person to whom the digital certification services of a legal entity are activated and therefore acts as the responsible party, trusting in him, with knowledge and full acceptance of the rights and duties established and published in this DPC.

The role of the responsible party will differ depending on the services provided by the ECD GSE as established in Annex 1 of this DPC.

Precautions that third parties should observe:

1. Verify the scope of the certificate in the associated certification policy.
2. Consult the regulations associated with digital certification services
3. Verify the ECD's accreditation status with ONAC.
4. Verify that the digital signature was generated correctly.
5. Verify the origin of the certificate (Certification chain)
6. Verify its conformity with the content of the certificate.
7. Verify the integrity of a digitally signed document.

Applicant.

The term Applicant shall refer to the natural or legal person interested in the digital certification services issued under this DPC. This may coincide with the role of the Subscriber.

Entity to which the subscriber or responsible party is linked.

In this case, the legal entity or organization to which the subscriber or responsible party is closely related through the accredited link in the digital certification service.

1.3.5. Other participants.

Management Committee.

The Management Committee is an internal body of ECD GSE, which is formed in accordance with the management committee regulations who have the responsibility of approving the DPC as an initial document, as well as authorizing the changes or modifications required on the approved DPC and authorizing its publication.

Service providers.

Service providers are third parties that provide infrastructure or technological services to ECD GSE, when GSE so requires, and guarantee the continuity of service to subscribers, entities for the entire time that the digital certification services have been contracted.

Reciprocal Digital Certification Entities.

In accordance with the provisions of Article 43 of Law 527 of 1999, digital signature certificates issued by foreign certification entities may be recognized under the same terms and conditions required by law for the issuance of certificates by national certification entities, provided that such certificates are recognized by an authorized certification entity that guarantees, in the same way as it does with its own certificates, the regularity of the certificate details, as well as its validity and validity.

Currently, ECD GSE does not have any reciprocity agreements in place.

Petitions, Complaints, Claims and Requests.

Requests, complaints, claims and inquiries regarding services provided by ECD GSE or subcontracted entities, and explanations regarding this Certification Policy, are received and handled directly by GSE as ECD and will be resolved by the relevant and impartial persons or by committees with the necessary technical competence. The following channels are available for serving subscribers, responsible parties and third parties.

Phone: +57 (1) 4050082
Email: pqrs@gse.com.co
Address: 77th Street No. 7 - 44 Office 701
Website: www.gse.com.co
Responsible: Customer service

Once a case is presented, it is forwarded along with the relevant information to the Customer Service process, following the established internal procedure for investigating and managing such cases. Similarly, the department responsible for taking corrective or preventive actions is identified, in which case the corresponding action procedure must be followed. Once the investigation is generated, the response is evaluated in order to subsequently make the decision that resolves the PQRS and its final communication to the subscriber, responsible party or interested party.

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

1.4. Use of the Certificate.

Based on the generic definitions established in the DPC relating to the uses of the certificate, the scope of application of each type of certificate is established below in order to delimit responsibilities, commitments or rights on the part of the Subscriber and/or Responsible, and where appropriate, also on the part of the Entity to the extent that it can be deduced from the very nature of the attribute of the certificate.

TYPE OF DIGITAL CERTIFICATE	SCOPE, USES AND APPLICATIONS
Company Membership	The subscriber and/or responsible party may carry out business procedures without implying representation. The company may establish usage limitations.
Company Representation	The subscriber and/or responsible party may carry out business procedures on behalf of the company. The company may establish usage limitations.
Public Service	Performance of procedures by the subscriber and/or responsible party in the exercise of their functions as a public official. The Public Administration may establish limitations on use.
Qualified Professional	Carrying out procedures by the subscriber and/or responsible party in the exercise of their functions as a registered professional.
Natural person	The subscriber and/or responsible party will carry out the procedures in their capacity as a citizen. There is no affiliation with any entity.
Electronic Invoice	Implementation by the subscriber and/or person responsible for billing and/or electronic payroll

TYPE OF DIGITAL CERTIFICATE	SCOPE, USES AND APPLICATIONS
Legal Entity	Performing business procedures by an application running on a machine in automatic and/or unattended signing processes on behalf of a legal entity of public or private law that require guaranteeing the authenticity and integrity of the data sent or stored digitally and that will be represented by a person responsible for the issued certificate. The use of this certificate is permitted within unattended platforms once the risk management study regarding the handling of cryptographic keys has been completed.

1.4.1. Appropriate use of certificates
In accordance with the provisions of the Certification Practice Statement

1.4.2. Prohibited use of certificates
The performance of unauthorized operations according to this Policy, by third parties or subscribers of the service, will exempt ECD GSE from any liability for this prohibited use.

- The certificate may not be used to sign other certificates or revocation lists (CRLs).
- It is prohibited to use the certificate for purposes other than those stipulated in the "Use of the Certificate" and "Limits of Liability of the Open Digital Certification Authority" sections of this Policy.
- Alterations to certificates are not permitted and the certificate must be used exactly as supplied by the ECD GSE.
- The use of certificates in control systems or fault-intolerant systems that could cause personal or environmental damage is prohibited.
- Any action that violates the provisions, obligations and requirements stipulated in this Policy is considered prohibited.
- It is not possible for the ECD GSE to issue any assessment on the content of the documents signed by the subscriber, therefore the responsibility for the content of the message is the sole responsibility of the signatory.

- It is not possible for the ECD GSE to recover encrypted data in case of loss of the subscriber's private key because the CA, for security reasons, does not keep a copy of the subscribers' private keys; therefore, it is the subscriber's responsibility to use data encryption.
- Illicit purposes or operations under any legal regime in the world.

Validity of certificates
Certificates issued by the ECD GSE have a maximum validity of twenty-four (24) months.

Types of ECD GSE certificates
The different types of certificates issued by ECD GSE are classified according to the "content" criterion and the fields defined in them and established in the technical profiles defined in Annex 1 of the DPC.
Based on this criterion, certain information that constitutes the subject of the certificate is guaranteed. Therefore, the digital certificates defined under this policy are as follows:

TYPE OF DIGITAL CERTIFICATE	OBJECT
Company Membership	This certificate guarantees the identity of the individual holder and their affiliation with a specific legal entity by virtue of their position within that entity. This certificate does not, in itself, grant the holder any greater powers than those they possess through their regular duties.
Company Representation	It is issued to a natural person representing a specific legal entity. The certificate holder is identified not only as a natural person belonging to a company, but also as its legal representative.
Public Service	This certificate guarantees the identity of the individual holder and their affiliation with a Public Administration by virtue of their position as a public official. This certificate does not, in itself, grant the holder any greater powers than those they possess through the performance of their regular duties.
Qualified Professional	This certificate guarantees the identity of the individual holder and their status as a qualified professional. This certificate does not, in itself, grant the holder any greater powers than those they possess by virtue of their regular professional activities.
Natural person	It only guarantees the identity of the natural person.
Electronic Invoice	Exclusive certificate for electronic invoicing, addressing the needs of companies and/or individuals seeking the security of the certificate for issuing electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment receipts, adjustment notes of the electronic payroll payment receipt document and other documents resulting from the processes of the unattended platforms of the technology providers approved by the DIAN, the DIAN's free invoicing system and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Legal Entity	Performing business procedures by an application running on a machine in automatic and unattended signing processes on behalf of a legal entity of public or private law that require guaranteeing the authenticity and integrity of the data sent or stored digitally and that will be represented by a person responsible for the issued certificate.

1.5. Policy Administration.
The administration of the Certification Policies (CP) will be the responsibility of the Operations process:
1.5.1. Organization that manages the document:
In accordance with the provisions of the Certification Practice Statement
1.5.2. Contact (ECD Manager):

Contact position:	Operations Coordinator
Contact phone numbers:	4050082

1.5.3. Person who determines the suitability of the DPC for the policy
In accordance with the provisions of the Certification Practice Statement

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

1.5.4. DPC approval procedures.
Policies must be approved in all cases by the Management Committee.

Publishing responsibilities
Once the policy changes have been made and approved, it is the responsibility of the Operations Coordinator and/or the Integrated Management System Process to request the responsible process to update the policies on the WEB portals to their latest version.
1.6. Definitions and Acronyms Definitions
The following terms are commonly used and required for understanding this Policy.
Certification Authority (CA): In English "Certification Authority" (CA): Certification Authority, root entity and public key infrastructure certification service provider.
Registration Authority (RA): In English "Registration Authority" (RA): It is the entity responsible for certifying the validity of the information provided by the applicant for a digital certificate, through the verification of their identity and registration.
Time Stamping Authority (TSA): Acronym for "Time Stamping Authority": Certification entity providing time stamping services
Secure Data Archiving: This is the service GSE offers its clients through a technological platform. Essentially, it consists of a secure and encrypted storage space accessed with credentials or a digital certificate. Documentation stored on this platform will have evidentiary value as long as it is digitally signed.
Digital certificate: A document electronically signed by a certification service provider that links signature verification data to a signatory and confirms their identity. This is the definition in Law 527/1999, which in this document is extended to cases where the signature verification data is linked to a computer component.
Specific Accreditation Criteria (CEA): Requirements that must be met to obtain Accreditation as a Digital Certification Entity - ECD, before the National Accreditation Body of Colombia - ONAC; that is, to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 019 of 2012, chapters 47 and 48 of title 2 of part 2 of book 2 of the Single Decree of the Commerce, Industry and Tourism Sector - DURSCIT and the regulations that modify or complement them.
Personal Access Key (PIN): Acronym for "Personal Identification Number": Sequence of characters that allow access to the digital certificate.
Private key compromise: compromise is understood as the theft, loss, destruction or disclosure of the private key that may put at risk the use of the certificate by unauthorized third parties or the certification system.
Certified email: A service that ensures the sending, receiving, and verification of electronic communications, guaranteeing at all times the characteristics of fidelity, authorship, traceability, and non-repudiation.
Certification Practice Statement (CPS): A statement by the certification body regarding the policies and procedures it applies to the provision of its services.
Time Stamping: According to numeral 7 of Article 3 of Decree 333 of 2014, it is defined as: Data message with a specific moment or period of time, which allows establishing with proof that this data existed at a moment or period of time and that it did not undergo any modification from the moment the stamping was made.
Certification Entity: It is that legal person, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, authorized by the Colombian government (National Accreditation Body in Colombia) to issue certificates in relation to the digital signatures of the clients who acquire them, offer or facilitate the services of registration and time stamping of the transmission and reception of data messages, as well as fulfill other functions related to communications based on digital signatures.
Open Certification Authority: This is a Certification Authority that offers services typical of certification authorities, such as:
1. Its use is not limited to the exchange of messages between the entity and the subscriber, or
2. He receives remuneration for these.

Closed certification authority: An entity that offers services typical of certification authorities only for the exchange of messages between the entity and the subscriber, without requiring remuneration for it.
Public Key Infrastructure (PKI): A PKI is a combination of hardware and software, security policies and procedures that allows users of a basically insecure public network such as the Internet to exchange data messages securely using a pair of cryptographic keys (one private and one public) that are obtained and shared through a trusted authority.
Initiator: Person who, acting on their own behalf, or on whose behalf someone has acted, sends or generates a data message.
Trust hierarchy: A set of certification authorities that maintain trust relationships whereby a higher-level CDA guarantees the reliability of one or more lower-level CDAs.
Certificate Revocation List (CRL): English acronym for "Certificate Revocation List": A list that includes only revoked certificates that have not yet expired.

Public and Private Keys: The asymmetric cryptography on which PKI is based. It uses a pair of keys where encryption is done with one key and decryption is only possible with the other, and vice versa. One of these keys is called the public key and is included in the digital certificate, while the other is called the private key and is known only to the subscriber or certificate holder.
Private Key (Private Key): Numerical value or values that, used together with a known mathematical procedure, serve to generate the digital signature of a data message.
Public key (Public Key): Numerical value or values that are used to verify that a digital signature was generated with the private key of the person acting as the initiator.
Cryptographic Hardware Security Module: Acronym for "Hardware Security Module", hardware module used to perform cryptographic functions and store keys in secure mode.
Certification Policy (CP): It is a set of rules that define the characteristics of the different types of certificates and their use.
Certification Service Provider (CSP): A natural or legal person who issues digital certificates and provides other services related to digital signatures.
Online Certificate Status Protocol (OCSP): A protocol that allows you to verify the status of a digital certificate online.
Repository: an information system used to store and retrieve certificates and other related information.

Revocation: Process by which a digital certificate is disabled and loses validity.
Applicant: Any natural or legal person who requests the issuance or renewal of a digital certificate.
Subscriber and/or responsible party: Natural or legal person to whom digital certification services are issued or activated and therefore acts as subscriber or responsible party thereof
Third party acting in good faith: A person or entity other than the subscriber and/or responsible party who decides to accept and rely on a digital certificate issued by ECD GSE. TSA GSE: This refers to the term used by ECD GSE, in the provision of its Time Stamping service, as a Time Stamping Authority.
Acronyms
CA: Certification Authority
CPS: Certification Practice Statement
CRL: Certificate Revocation List
CSP: Certification Service Provider
DNS: Domain Name System
FIPS: Federal Information Processing Standard
HTTP: The Hypertext Transfer Protocol (HTTP) is the protocol used in every transaction on the World Wide Web (WWW). HTTP defines the syntax and semantics used by the software elements of the web architecture (clients, servers, proxies) to communicate. It is a transaction-oriented protocol and follows a request-response pattern between a client and a server.
HTTPS: Hypertext Transfer Protocol Secure (in Spanish: Protocolo seguro de transferencia de hipertexto), better known by its acronym HTTPS, is a network protocol based on the HTTP protocol, intended for the secure transfer of hypertext data; that is, it is the secure version of HTTP.
IEC: International Electrotechnical Commission
IETF: Internet Engineering Task Force (Internet Standards Organization) IP: Internet Protocol
ISO: International Organization for Standardization
OCSP: Online Certificate Status Protocol.
OID: Object identifier (Unique object identifier)
PIN: Personal Identification Number
PUK: Personal Unlocking Key
PKCS: Public Key Cryptography Standards. PKI standards developed by RSA Laboratories and internationally accepted. PKI: Public Key Infrastructure. PKIX: Public Key Infrastructure (X.509). RA: Registration Authority
RFC: Request For Comments (Standard issued by the IETF) URL: Uniform Resource Locator

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.

2.1. Repositories.

In accordance with the provisions of the Certification Practice Statement

2.2. Publication of information on certification.

In accordance with the provisions of the Certification Practice Statement

2.3. Publication schedule or frequency.

In accordance with the provisions of the Certification Practice Statement

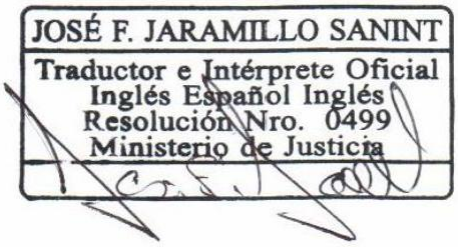
2.4. Access controls to repositories.

In accordance with the provisions of the Certification Practice Statement

3. IDENTIFICATION AND AUTHENTICATION.

3.1. Names.

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.



In accordance with the provisions of the Certification Practice Statement
3.2. Initial identity validation.
In accordance with the provisions of the Certification Practice Statement
3.3. Identification and Authentication for key renewal.
In accordance with the provisions of the Certification Practice Statement
3.4. Identification and authentication for the revocation request.
In accordance with the provisions of the Certification Practice Statement

4. OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF CERTIFICATES.

4.1. Certificate application.
Anyone requiring the provision of the digital certification service may do so using the channels, means or mechanisms provided by GSE, in which the necessary information to manage the request for the required digital certification service will be obtained, accepting the ECD terms and conditions document.

TYPE OF DIGITAL CERTIFICATE	RECORD: INFORMATION REQUESTED
The following information will be required for all types of certificates: • Completed application form. • Acceptance of terms and conditions. • Document and/or information that certifies the applicant's identification	
Company Membership	• Document of Existence and Legal Representation of the Company with validity of no more than thirty (30) days. • Employment certificate of the applicant including the position on institutional paper (no older than thirty (30) days). • Single Taxpayer Registry - RUT
Company Representation	• Document of Existence and Legal Representation of the Company with validity of no more than thirty (30) days. • Single Taxpayer Registry - RUT In the event that the application is delegated by the Legal Representative and/or Alternate to a third party, the delegation letter for the application of the digital certificate must be attached.
Public Service	• To confirm the applicant's relationship with the Company, one of the following documents will be requested: 0 Record of possession. 0 Appointment resolution or decree. 0 Service provision contract. 0 Employment certificate of the applicant including the position on institutional paper (no older than thirty (30) days from the filing of the application).
Qualified Professional	• Single Taxpayer Registry - RUT • Applicant's address information • Professional card and/or equivalent document. • Degree diploma (optional)
Natural person	• Applicant's address information In the event that the request for the digital certification service is generated from a trusted source or third party, such as the National Civil Registry, no additional information and/or documentation will be requested as long as the information is signed by the same entity and a contract, agreement, accord, alliance, and/or any other means of direct and/or indirect contractual and/or commercial relationship remains in place.
Electronic Invoice	Natural person • Applicant's address information. In the event that the application is delegated by the Legal Representative and/or Alternate to a third party, the delegation letter for the application of the digital certificate must be attached. Legal Entity • Single Taxpayer Registry - RUT Document of Existence and Legal Representation of the Company with validity of no more than thirty (30) days.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

	If the applicant does not have the document of existence and legal representation and is a public or state entity, the information and/or equivalent documents will be requested in which the creation of the entity can be validated in accordance with current regulations and the respective administrative act (law, decree, resolution, among others). In the event that the application is delegated by the Legal Representative and/or Alternate to a third party, the delegation letter for the application of the digital certificate must be attached. • Document of Existence and Legal Representation of the Company with validity of no more than thirty (30) days. • Single Taxpayer Registry - RUT
Legal Entity	If the applicant does not have the document of existence and legal representation and is a public or state entity, information and/or equivalent documents will be requested to validate the entity's creation in accordance with current regulations and the respective administrative act (law, decree, resolution, among others). If the application is delegated by the Legal Representative and/or Alternate to a third party, a letter of delegation for the digital certificate application must be attached.

Grades:

- Documents, when applicable, will be received scanned or in electronic original, preserving legibility for the use of the information.
- The Single Taxpayer Registry (RUT) document, when applicable, will be requested in the updated DIAN format that includes a QR code.
- If the applicant does not have a Single Taxpayer Registry - RUT (when applicable), they must submit a document where the address information is registered, issued by a third party that verifies it, or the address information will be consulted by the ECD GSE using data services from external sources.
- For certificate types where the Document of Existence and Legal Representation is requested, said document will be valid for a period of no more than thirty (30) days from the filing of the application.
- For certificate types where the Document of Existence and Legal Representation of the Company is requested, in cases where required, an equivalent document will be valid where the existence and legal representation of the company can be validated; if applicable, the duly authenticated document will be requested.
- For all documents received authenticated, the authentication must be valid for no more than sixty (60) days from the date of filing the application.
- In cases where applications for digital certificates are submitted with additional and/or equivalent documents to the documentation and/or information requested, the documents mentioned in the Documentary Annex for Validation of Applications published on the website in the Support-Guides and Manuals-Validation of Applications section will be taken into account for the review of the applications.

The ECD-GSE has a security management system to protect the information collected for the purpose of issuing certificates, which is established in the DPC under "Computer Security Controls".

ECD GSE does not prevent or inhibit applicants' access to services as an ECD; therefore, a digital certificate can be requested regardless of the size of the applicant or subscriber, the type of relationship with ECD GSE, or membership with any association or group. It also does not depend on the number of digital certificates already issued or any other factor that discriminates against access to the service provided by ECD GSE.

Generic Requirements

It is the set of detailed information in the DPC about its security system, support, administration and issuance of Certificates, as well as about the relationship of trust between the Applicant, Subscriber and/or Responsible, the Entity that receives or Third Party in good faith and the ECD constitutes the generic requirements for the issuance of ECD GSE certificates.

However, due to the specific characteristics of the different certificates, these requirements sometimes have their own particularities for each type of digital certificate. These particularities are defined as specific requirements and are outlined in the following section.

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

Specific Requirements

Based on the generic definitions established in the DPC relating to the figures of Subscriber and/or Responsible and Entity, the details of the natural or legal persons who perform these functions for each type of certificate are established below, as well as the attribute or link between these two figures that delimit the requirements, review of the application and decision in accordance with the scope of accreditation granted by ONAC.

TYPE OF DIGITAL CERTIFICATE	SUBSCRIBER / RESPONSIBLE	ATTRIBUTE	ENTITY
Company Membership	Natural person who belongs to the company and who is the holder of the certificate.	Link to belonging to a company	Company to which the Subscriber is linked
Company Representation	Natural person who legally represents the company and who holds the certificate	Linking legal representation to company	Company represented by the Subscriber
Public Service	Natural person belonging to a Public Administration and holding the certificate	Civil service affiliation with a Public Administration	Public Administration to which the Subscriber is linked
Qualified Professional	Natural person who practices a profession titled and who holds the certificate	Practice of a regulated profession and affiliation with the Professional Association	Professional Association to which it is linked Subscriber
Natural person	Natural person holding the certificate	Not applicable	Not applicable
Electronic Invoice	It only guarantees the identity of subscriber and/or responsible party	Linkage for the realization of electronic invoicing and/or payroll	Subscriber and/or responsible party requiring perform electronic invoicing and/or payroll
Legal Entity	Responsible for the certificate that is on file name of a Legal Entity	Linking of legal representation to company	Company represented by the Subscriber and/or responsible party.

4.2. Certificate application processing.
In accordance with the provisions of the Certification Practice Statement
4.3. Issuance of the Certificate.
In accordance with the provisions of the Certification Practice Statement
4.4. Acceptance of the Certificate.
In accordance with the provisions of the Certification Practice Statement
4.5. Use of key pairs and certificates.
In accordance with the provisions of the Certification Practice Statement
4.6. Certificate Renewal.
In accordance with the provisions of the Certification Practice Statement
4.7. Re-use of certificate key.
In accordance with the provisions of the Certification Practice Statement
4.8. Certificate Modification.
In accordance with the provisions of the Certification Practice Statement
4.9. Revocation and Suspension of the Certificate.
In accordance with the provisions of the Certification Practice Statement
4.10. Certificate Status Services.
In accordance with the provisions of the Certification Practice Statement
4.11. End of Subscription.
In accordance with the provisions of the Certification Practice Statement
4.12. Key Custody and Recovery.
In accordance with the provisions of the Certification Practice Statement
5. FACILITIES, MANAGEMENT AND OPERATIONAL CONTROLS.
5.1. Physical Security Controls.
In accordance with the provisions of the Certification Practice Statement
5.2. Procedural Controls.
In accordance with the provisions of the Certification Practice Statement
5.3. Personnel controls.

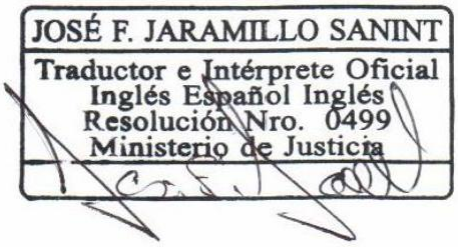
This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

In accordance with the provisions of the Certification Practice Statement
5.4. Audit Recording Procedures.
In accordance with the provisions of the Certification Practice Statement
5.5. Records Archive.
In accordance with the provisions of the Certification Practice Statement
5.6. Key Change.
In accordance with the provisions of the Certification Practice Statement
5.7. Commitment and Disaster Recovery.
In accordance with the provisions of the Certification Practice Statement
5.8. Termination of the CA or the RA.
In accordance with the provisions of the Certification Practice Statement
6. TECHNICAL SECURITY CONTROLS.
6.1. Generation and Installation of Key Pairs.
In accordance with the provisions of the Certification Practice Statement
6.2. Private key protection and cryptographic module engineering controls.
In accordance with the provisions of the Certification Practice Statement
6.3. Other Aspects of Key Pair Management.
In accordance with the provisions of the Certification Practice Statement
6.4. Activation Data.
In accordance with the provisions of the Certification Practice Statement
6.5. Information Security Controls.
In accordance with the provisions of the Certification Practice Statement
6.6. Technical Lifecycle Controls.
In accordance with the provisions of the Certification Practice Statement
6.7. Network Security Controls.
In accordance with the provisions of the Certification Practice Statement
6.8. Time Stamping.
In accordance with the provisions of the Certification Practice Statement
7. CERTIFICATE, CRL AND OCSP PROFILES.
7.1. Certificate Profile.
In accordance with the provisions of the Certification Practice Statement
7.2. CRL profile.
In accordance with the provisions of the Certification Practice Statement
7.3. OCSP profile.
In accordance with the provisions of the Certification Practice Statement

8. COMPLIANCE AUDIT AND OTHER EVALUATIONS.
8.1. Frequency or Circumstances of the Evaluation.
In accordance with the provisions of the Certification Practice Statement
8.2. Evaluator identity and qualifications.
In accordance with the provisions of the Certification Practice Statement
8.3. Relationship of the evaluator with the entity being evaluated.
In accordance with the provisions of the Certification Practice Statement
8.4. Topics subject to evaluation.
In accordance with the provisions of the Certification Practice Statement
8.5. Actions taken as a result of the deficiency.
In accordance with the provisions of the Certification Practice Statement
8.6. Communication of Results.
In accordance with the provisions of the Certification Practice Statement
9. OTHERS COMMERCIAL AND LEGAL MATTERS.
9.1. Fees.
In accordance with the provisions of the Certification Practice Statement
9.2. Financial Responsibility.
In accordance with the provisions of the Certification Practice Statement
9.3. Confidentiality of Commercial Information.
In accordance with the provisions of the Certification Practice Statement
9.4. Privacy of Personal Information.
In accordance with the provisions of the Certification Practice Statement

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.



9.5. Intellectual Property Rights.
In accordance with the provisions of the Certification Practice Statement
9.6. Representations and Guarantees.
In accordance with the provisions of the Certification Practice Statement
9.7. Warranty Disclaimers.
Not Applicable
9.8. Limitations of Liability.
The limitations of the Open Certification Authority's liability are comprehensively defined in the Liability Limitations section of the DPC, but based on the specific uses of each certificate established in the preceding section. ECD GSE assumes no other commitments or provides any other guarantees, nor does it assume any other liability to certificate holders or trusted third parties, except as provided by the provisions of this PC.
The ECD GSE will decline a request for a digital certification service if it is not within the scope of the accreditation granted to it by ONAC.

TYPE OF DIGITAL CERTIFICATE	LIMITATION OF LIABILITY OF THE CERTIFICATION ENTITY
Company affiliation, company representation, public service, qualified professional, qualified professional, natural person, electronic invoice, legal entity	Digital certificates issued by ECD GSE may only be used for the purposes for which they were issued and specified in the DPC and specifically in the section Use of certificate. Uses not defined in the DPC and PC are considered improper, and consequently, for legal purposes, the ECD GSE is exempt from all responsibility for the use of certificates in operations that are outside the limits and conditions established for the use of digital certificates according to the DPC, PC and in accordance with the provisions of the section Limits of Responsibility of the open certification entity.

9.9. Compensation.
Not Applicable
9.10. Duration and Termination.
In accordance with the provisions of the Certification Practice Statement
9.11. Individual notifications and communications to participants.
In accordance with the provisions of the Certification Practice Statement
9.11.1. Obligations of the ECD GSE
ECD GSE, as a certification service provider, is obligated under current regulations, as set out in the Certificate Policies and in the
DPC to:
1. Respect the provisions of current regulations, the DPC and the Certificate Policies.
2. Publish the DPC and each of the Certificate Policies on the GSE website.
3. Inform ONAC about the modifications to the DPC and the Certificate Policies.
4. Maintain the DPC and Certificate Policies with their latest version published on the GSE website.
5. Protect and safeguard your private key securely and responsibly.
6. Issue certificates in accordance with the Certificate Policies and the standards defined in the DPC.
7. Generate certificates consistent with the information provided by the applicant or subscriber.
8. Retain information on digital certificates issued in accordance with current regulations.
9. Issue certificates whose minimum content is in accordance with current regulations for the different types of certificates.
10. Publish the status of issued digital certificates in an open access repository.
11. Do not keep a copy of the applicant's or subscriber's private key.
12. Revoke digital certificates as provided in the Digital Certificate Revocation Policy.
13. Update and publish the CRL revoked digital certificate list with the latest revoked certificates.
14. Notify the Applicant, Subscriber or Entity of the revocation of the digital certificate within 24 hours of the revocation of the digital certificate in accordance with the digital certificate revocation policy.
15. Inform subscribers of the approaching expiration of their digital certificate.
16. Having qualified personnel with the knowledge and experience necessary to provide the certification service offered by the ECD GSE.
17. Provide the applicant with the following information on the ECD GSE website, free of charge and with open access:

- The Certification Policies and Statement of Practice and all updates thereto.

- Subscriber obligations and how the data must be kept safe
- Procedure for requesting the issuance of a certificate.

- The procedure for revoking your certificate.
- Mechanisms to guarantee the reliability of the electronic signature over time.
- The conditions and limits of the use of the certificate

18. To verify, either personally or through a different person acting on their behalf, the identity and any other circumstances of the applicants or data of the certificates, which are relevant for the purposes of the verification procedure prior to their issuance.
19. Report to the Superintendency of Industry and Commerce and to ONAC, immediately, the occurrence of any event that compromises or may compromise the provision of the service.
20. Report promptly any modification or update of services included in the scope of your accreditation, in accordance with the procedures, rules and requirements of the ONAC accreditation service.
21. Update contact information whenever there is a change or modification to the data provided.
22. To train and warn users about the safety measures they must observe and about the logistics required for the use of the service delivery mechanisms.
2.3. To guarantee the protection, integrity, confidentiality and security of the information provided by the subscriber by keeping the documentation that supports the certificates issued.
24. To guarantee the conditions of integrity, availability, confidentiality and security, in accordance with current national and international technical standards and with the specific accreditation criteria established for this purpose by ONAC.
25. List the accredited services on the ECD GSE website.

9.11.2. Obligations of the RA

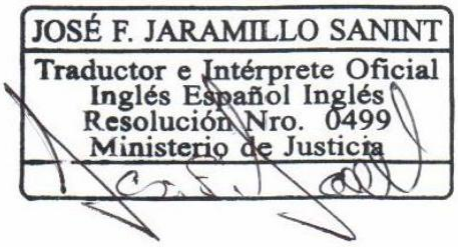
The ECD GSE RA is authorized to perform the identification and registration work, therefore, it is obligated under the terms defined in the Certification Practice Statement to:

1. To know and comply with the provisions of the DPC and the Certificate Policy corresponding to each type of certificate.
2. Safeguard and protect your private key.
3. Review and/or verify the initial validation records of the identity of Applicants, Responsible Parties or Subscribers of digital certificates.
4. Verify the accuracy and authenticity of the information provided by the Applicant using the protocols described in the DPC
5. To archive and safeguard the information and/or documentation provided by the applicant or subscriber for the issuance of the digital certificate, for the time established by current legislation.
6. Respect the provisions of the contracts signed between ECD GSE and the subscriber.
7. Identify and inform the ECD GSE of the reasons for revocation provided by applicants regarding current digital certificates.

9.11.3. Obligations (Duties and Rights) of the Subscriber and/or Responsible Party

The Subscriber and/or Responsible Party of a digital certificate is obliged to comply with the provisions of current regulations and the provisions of the DPC, such as:

1. Use your digital certificate according to the terms of the DPC.
2. Verify within the next business day that the digital certificate information is correct. If any inconsistencies are found, notify the ECD.
3. Refrain from: lending, transferring, writing, publishing the password for using your digital certificate and take all necessary, reasonable and timely measures to prevent it from being used by third parties.
4. Do not transfer, share, or lend the cryptographic device to third parties.
5. Provide all the information required in the Application Form to facilitate your timely and full identification.
6. Request the revocation of the Digital Certificate upon change of name and/or surnames.
7. Request the revocation of the Digital Certificate when the Subscriber has changed their nationality.
8. Comply with what was accepted and signed in the terms and conditions document or the digital certificate manager.
9. Provide the required information accurately and truthfully.
10. Report any changes to the data initially provided for the issuance of the digital certificate during its validity period.
11. Safeguard and protect your private key responsibly.
12. Use the certificate in accordance with the provisions of this PC for each type of certificate.



13. As a subscriber or responsible party, you must immediately request the revocation of your digital certificate when you become aware that there is a cause defined in the section "Circumstances for the revocation of a DPC certificate".
14. Do not use the private key or the digital certificate once it has expired or has been revoked.
15. Inform trusted third parties of the need to verify the validity of the digital certificates they are using at any given time.
16. Informing a third party in good faith to verify the status of a certificate provides the Certificate Revocation List (CRL), published periodically by ECD GSE.
17. Do not use your digital certificate in a way that violates the law or causes a bad reputation for the ECD.
18. Do not make any statement related to your digital certification in the ECD GSE that may be considered misleading or unauthorized, in accordance with the provisions of the DPC and PC.
19. Once the digital certification service has expired or been revoked, the subscriber must immediately stop using it in all advertising material that contains any reference to the service.
20. When referring to the digital certification service provided by ECD GSE in media such as documents, brochures or advertising, the subscriber must state that it complies with the requirements specified in the DPC CPs, indicating the version.
21. The subscriber may use the conformity marks and information related to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, as long as they comply with the requirements in the preceding paragraph.

On the other hand, it has the following rights:

1. Receive the digital certificate within the timeframes established in the DPC.
2. The subscriber may use the conformity marks and information related to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, as long as they comply with the requirements in the preceding paragraph.
3. Request information regarding applications in process.
4. Request revocation of the digital certificate by providing the necessary documentation.

5. Receive the digital certificate in accordance with the scope granted by ONAC to GSE.

9.11.4. Obligations of Third Parties in Good Faith

Third parties acting in good faith, as parties relying on digital certificates issued by ECD GSE, are obliged to:

1. To know the provisions regarding Digital Certification in the current regulations.
2. Know the provisions of the DPC and PC.
3. Verify the status of the certificates before performing operations with digital certificates.
4. Check the Certificate Revocation List (CRL) before performing operations with digital certificates.
5. To know and accept the conditions regarding guarantees, uses and responsibilities when carrying out operations with digital certificates.

9.11.5. Obligations of the Entity (Client)

The client entity is responsible for requesting the services for its employees, and the subscribers are the people who use the service.

As established in the Certificate Policies, in the case of certificates where the Subscriber or Responsible Party's relationship with the same is accredited, the Entity will be obligated to:

1. Request the RA GSE to suspend/revoke the certificate when said link ceases or is modified.
2. All those obligations related to the person responsible for the digital certification service.
3. When referring to the digital certification service provided by ECD GSE in media such as documents, brochures or advertising, the entity must state that it complies with the requirements specified in the DPC CPs.
4. The entity may use the conformity marks and information related to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, as long as it complies with the requirements in the preceding paragraph.

9.11.6. Obligations of other participants in the ECD

The Management Committee and the Integrated Management System process, as internal bodies of ECD GSE, are obliged to:

1. Review the consistency of the DPC with current regulations.
2. Approve and decide on changes to be made to digital certification services, due to regulatory decisions or requests from subscribers or managers.
3. Approve the notification of any changes to subscribers and/or responsible parties, analyzing their legal, technical, or commercial impact.
4. Review and take action on any comments made by Subscribers and/or Responsible Parties when a change to the digital certification service is made.

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

5. Report action plans to ONAC and SIC on any change that has an impact on the PKI infrastructure and that affects digital certification services, in accordance with RAC-3.0-01.
6. Authorize the required changes or modifications to the DPC.
7. Authorize the publication of the DPC on the ECD GSE website.
8. Approve changes or modifications to the ECD GSE Security Policies.
9. Ensure the integrity and availability of the information published on the ECD GSE website.
10. Ensure the existence of controls over the technological infrastructure of the ECD GSE.
11. Request the revocation of a certificate if you have knowledge or suspicion of the compromise of the subscriber's private key, entity or any other fact that tends to the misuse of the subscriber's private key, entity or the ECD itself.
12. To recognize and take appropriate action when security incidents occur.
13. Perform a review of the DPC at a maximum frequency of one year to verify that the lengths of the keys and periods of the certificates being used are adequate.
14. Review, approve and authorize changes to digital certification services accredited by the competent body.
15. Review, approve and authorize the ownership and use of symbols, certificates and any other mechanism that ECD GSE requires to indicate that the digital certification service is accredited.
16. Ensure that the accreditation conditions granted by the competent body are maintained.
17. Ensure the proper use in documents or any other advertising of the symbols, certificates, and any other mechanism that indicates that ECD GSE has an accredited certification service and complies with the provisions of ONAC's Accreditation Rules RAC-3.0-01 and RAC-3.0-03.
18. Ensure that critical suppliers and reciprocal ECDs, if any, are kept informed of the obligation to comply with the CEA requirements, in the relevant sections.
19. The Integrated Management System process will implement preventive and corrective action plans to respond to any risk that compromises the impartiality and non-discrimination of the ECD, whether it arises fromthe actions of any person, body, organization, activities, their relationships, or the relationships of their staff or themselves. For this purpose, it uses the ISO 31000 standard for identifying risks that could compromise the impartiality of the ECD.
20. Ensure that all ECD staff and committees (internal or external) that may have influence on certification activities act with impartiality and non-discrimination, especially those arising from commercial, financial or other pressures that compromise their impartiality.
21. Document and demonstrate the commitment to impartiality and non-discrimination.
22. Ensure that the administrative, management, and technical staff of the PKI and the ECD associated with consulting activities maintain complete independence and autonomy from the staff involved in the review and decision-making process regarding the certification of the ECD itself.

2.3. Ensure that critical suppliers such as reciprocal ECD and data centers that meet ECD accreditation requirements are kept informed as support for their contracting and compliance with the requested administrative and technical requirements.

9.12. Amendments.

In accordance with the provisions of the Certification Practice Statement

9.13. Provisions on dispute resolution.

In accordance with the provisions of the Certification Practice Statement

9.14. Applicable legislation.

In accordance with the provisions of the Certification Practice Statement

9.15. Compliance with applicable legislation

In accordance with the provisions of the Certification Practice Statement

9.16. Various provisions.

In accordance with the provisions of the Certification Practice Statement

9.17. Other Provisions.

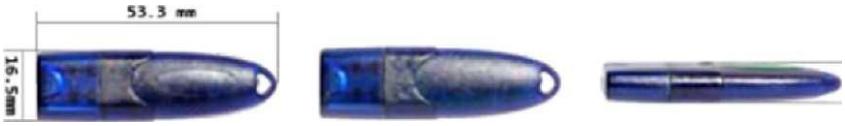
In accordance with the provisions of the Certification Practice Statement

10. CHARACTERISTICS OF CRYPTOGRAPHIC DEVICES

For the issuance and storage of digital certificates, GSE uses FIPS 140-2 level 3 or higher certified cryptographic devices, which provides greater physical and logical security to the device, protecting its contents.

10.1.Digital Certificate in Token

JOSÉ F. JARAMILLO SANINT
Traductor e Intérprete Oficial
Inglés Español Inglés
Resolución Nro. 0499
Ministerio de Justicia

70.2. 

Front Back

Characteristics

FEATURE	TECHNICAL SPECIFICATION
Supported Operating Systems	32-bit and 64-bit Windows XP SP3, Vista, 7, 8,10. MacOS. Server2003, Server2008, Server2008 R2, Server 2012 R2.
Standard	X.509 Oct 2019, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID
Cryptographic Functions	Key pair generation, digital signature and verification, data encryption and decryption
Algorithm Support	RSA 512/1024/2048, DES, 3DES, SHA-1, SHA-256/384/512, AES 128/192/256
Processor	16 bit smart card chip (Common Criteria EAL 5+ certified)
Memory	64KB (EEPROM)
Connectivity	USB 2.0 full speed token, Type A connector
Device Lock	It will be locked after the third attempt to use it with an incorrect password.
Operating Temperature	0°C ~70°C (32°F ~ 158°F)
Humidity	0% ~ 100% non-condensing
Storage Temperature	-20°C ~85°C (-4°F ~ 185°F)
Net Weight	8.1 gr
Dimensions	54.5x17x8.5 mm

10.3. Segurity commitments

Due to circumstances that affect the security of the cryptographic device:

- Compromise or suspected compromise of the security of the cryptographic device.
- Loss or damage to the cryptographic device.
- Unauthorized access, by a third party, to the activation data of the Signer or the certificate holder

10.4. Cryptographic device care

- Keep it in a dry place away from ambient and/or temperature variations.
- Do not expose it to magnetic fields.
- Prevent it from being hit or subjected to physical stress.
- Do not attempt to open it, remove the plastic protection or circuit board, as this will cause it to malfunction.
- Do not put it in water or other liquids.
- Notify the ECD - GSE in case of theft, robbery, loss and/or fraud of the token in order to revoke the digital certificate.

70.5. Associated Risks

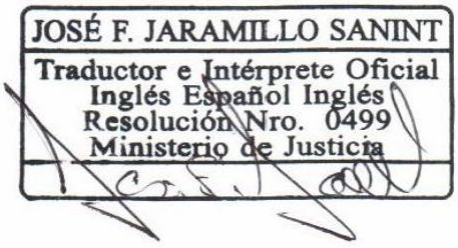
Cryptographic devices supported by the ECD-GSE may present the following risks:

- Loss of the device.
- Key commitment.
- Damage due to improper handling.
- Damage due to lack of care of the device in the face of environmental conditions.
- Damage due to voltage variation.

To mitigate the associated risks, the following should be taken into account:

- The digital signature certificate is personal and non-transferable; the PIN is confidential.
- It is recommended to change the PIN periodically.
- Entering the PIN incorrectly more than three (3) times will lock the device.
- Cryptographic devices must be kept in suitable environmental conditions.

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. January 29th, 2026.



• In case of compromise or loss of the private key, you must request the revocation of the digital certificate.

10.6. Digital Certificate in HSM - Hardware Security Module (Centralized Signature)

FEATURE	TECHNICAL SPECIFICATION
Supported Operating Systems	32-bit and 64-bit Windows XP SP3, Vista, 7, 8,10. Server2003, Server2008, Server2008 R2, Server 2012 R2.
Standard	X.509 Oct 2019, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID
Cryptographic Functions	Key pair generation, digital signature and verification, data encryption and decryption
Connectivity	Web, with Username/Password
Session Lock	The session is blocked from the user's IP address after the third login attempt with an incorrect password.

10.7. Technical Characteristics of Digital Certificates

FEATURE	TECHNICAL SPECIFICATION
Signature Algorithm	SHA256 Hash Function with RSA Encryption. SHA384 Hash Function with ECDSA Encryption Function RSA with key length 4096 for CA ROOT RSA with key length 4096 for CA SUBORDINATE RSA with subscriber/responsible key length of 2048. ECDSA with key length 384 for CA ROOT ECDSA with key length 384 for SUBORDINATE CA ECDSA with subscriber/responsible key length of 256.
Content of the Digital Certificate	RFC 5280 - Internet X.509 Public Key Infrastructure Certify and CRL Profile. May 2008. ITU-T-X509 October 2019 ETSI TS 102 042 - Policy requirements for certification authorities issuing public key.
Certificate lifecycle	RFC 3647 - Internet X.509 Public Key Infrastructure Certify Policy and Certification Practices Framework.
Key generation	FIPS 140-2 Level 3 Token HSM FIPS 140-2 Level 3 or higher (Centralized Signature)
Certification activities article 161 of decree law 0019 of 2012	1. Issuing certificates related to the electronic or digital signatures of individuals natural or legal persons. 2. Issue certificates verifying the alteration between the shipment and reception of data messages and transferable electronic documents. 3. To issue certificates in relation to the person who has a right or obligation with with respect to the documents mentioned in subparagraphs f) and g) of Article 26 of Law 527 of 1999

10.8. FEES FOR THE ISSUANCE OF DIGITAL CERTIFICATES

In accordance with the provisions of the Certification Practice Statement

10.9. IMPARTIALITY AND NON-DISCRIMINATION

In accordance with the provisions of the Certification Practice Statement

10.10. MODELS AND MINUTES OF TERMS AND CONDITIONS DOCUMENTS

In accordance with what is stated in Annex 2 of the DPC.

10.11. PROFILE OF CERTIFICATES

Consult Annex 1 of the DPC Technical Profile Matrix of the Certificates

OID (Object Identifier)	1.3.6.1.4.1.31136.1.4.18
PC Location	https://gse.com.co/documentos/calidad/politicas/Politica_de_certificado_para_certificados_digitales_V18.pdf