Official Translator: José Fernando Jaramillo Sanint. Address: Calle 70A No. 23B-25 Manizales Colombia
Tel: (57) (6) 8874503 Mobile: (310) 404-0972 - (300) 339-46-01 Email: traducciones@121.com.co

CERTIFICATE POLICIES FOR DIGITAL CERTIFICATES

Code	Name	Version	Classification of the information
POP-PL-55	**Certificate Policies for Digital Certificate Service**	16	Public

Document Title	**Certificate Policies for Digital Certificate Service**
Version	16
Working Group	Management Committee
Document status	final
Issue date	02/15/2010
Effective Date	08/07/2024
OID (Object Identifier)	1.3.6.1.4.1.31136.1.4.16
Location of the Policy	https://ase.com.co/documentos/calidad/politicas/Certificate policy for daily certificates V16.pdf
Prepared	Operations Manager
Reviewed	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	ECD GSE Headquarters Information Update.
3	03/04/2018	Updated in accordance with ONAC audit recommendations.
4	11/27/2018	Change from V3 to V4 11/26/2018 update charges, fees, access routes to the website, title change, inclusion of the liability limits of the open certification entity, validity of the services, obligations of the ECD, the RA, the EE, the subscriber, those responsible, third parties in good faith, the entity and obligations of other participants

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. August 30th, 2024

5	12/04/2019	The EE obligations section was eliminated, the responsibilities of the subscriber and the responsible party were unified, the specifications for the use of MAC are described in the section on Supported Operating Systems, the clarification was made 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 Subscriber obligations and rights were clarified
7	03/31/2020	The PCs are adjusted to the changes generated by the new platforms, the Objective and Scope numerals and administration of the policies 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	08/14/2020	The contact person in section 4.1 was updated. A note was added to section 7.5, in case the subscriber has a valid certificate, he/she may submit the digitally signed application and said application will replace the documents initially requested. For the public function type certificate, in case of not having the labor certificate, the possession certificate, appointment certificate or service provision contract can be attached. For the professional type certificate, the RUT is requested (if applicable), the professional registration application is changed for the diploma and the degree certificate must be authenticated.
9	12/02/2021	ECD and CA (Pay net) data were included with links to consult in Online the Certificate of Existence and Legal Representation. Links have been updated to point to the new routes. The following numerals were updated: • 7.6. Specific requirement for processing the certificate
10	07/16/2021	The following sections have been updated: 3.1. Summary, PKI infrastructure service provider, CERL query URL and contact telephone numbers. 5.3. OID of the Policies 7. Requirements for ECD digital certificates 7.7. Specific requirements for certificate processing 8.1.1 modified the image of the cryptographic devices The numerals were included: 7.6 Prohibitions on the Use of Certificates 8.1.2 Security commitments 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 policy consultation link have been updated.
11	10/27/2021	• modify section 7.7 Specific Requirements for Processing the Certificate by including in the final section of the Note a clarification on the updated RUT of the DIAN which must have the QR code. • adjust the OID and the PC link
12	05/31/2022	According to the new version of the CEA, the following adjustments were made: • 4.4 Petitions, Complaints, Claims and Requests: The term Appeal was eliminated. • 5.2 Certificate Content: The centralized signing certificate has been removed. • 6. Types of Certificates: modify the object of the legal entity certificate. • 7.4. Uses of certificates: modify the attribute of the legal entity certificate. • 7.7. Technical requirements for processing the certificate: modify the description of the application documentation for the electronic invoicing certificate and the legal entity certificate. • 7.9. Activities and technical references: The activities and regulatory documents for each type of certificate were modified in accordance with the accreditation certificate with ONAC. • 9.1.6. Obligations of other ECD participants: I modify item r) leaving only CEA, eliminating 4.1-10. • adjust the OID and the Policy query link. • The quality code was included in the document header
13	09/23/2022	• The was modified numeral 3.1 Summary including the chapters of the durscit. • The ECD address was modified in sections 3.1 and 4.4.

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. August 30th, 2024

		• modify the address of Paynet SAS in section 3.1. • modify the ITU X509 of 2016 to the ITU X509 of October 2019 in the standards of each accredited service in section 7.9, just as the ITU standards -TX.500 of October 2019 and FIPS PUB 186-4 of July 2013 were eliminated. • modify numeral 9.1.1 including items o) to y). • Numbers 13 to 16 were included. • modify numeral 7.7 of legal representative by including a paragraph in the requested documentation. • adjust the OID and the Policy consultation link
14	05/16/2023	• modify the entire order of the document according to the numerals of the RFC 3647. • It was eliminated Paynet SAS as the CA authority since the PKI was moved to the ECD of GSE. • Section 1.3.8.4 was adjusted, the person responsible for PQRS becoming Customer Service. • change the Director of Operations to the Operations Manager • The data of the main and alternate datacenter leaving Hostdime and Claro. • The OID and the Policy consultation link have been updated • Adjust numeral 1.9.1 in the type of digital certificate (Person) of the requested registration.
15	10/23/2023	• modify numeral 1.3.8.1 changes in the Management Committee: The management committee regulations are cited. • modify numeral 1.9.1 Certificate request • 1.14.11.2 RA Obligations: Literals C and E are updated • modified numeral 6 Profile of the certificates: The OID and the consultation link of the Policy were updated
16	08/07/2024	• The numbering and order are updated according to numeral 6 Diagram of a set of provisions of RFC 3647 • The OID and the Policy consultation link have been 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. August 30th, 2024

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. August 30th, 2024

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 PC) for the different certificates issued by the ECD GSE.
The purpose of the PC is to define those requirements that are necessary for the issuance of the different ECD GSE certificates.
To the extent that the ECD GSE CPS establishes all the generic requirements regarding the security system, support, administration and issuance of ECD GSE Certificates, the policies will refer only to the specific requirements of each type of certificate, referring in all other terms to what is established in the CPS.
In this way, the different certificates of the ECD GSE must comply with the generic requirements and security levels detailed in the CPD and the specific requirements for each one defined in this document.
ECD GSE must inform Subscribers and/or Controllers of the existence of this document, which provides answers to the PCs of the various certificates issued by ECD GSE.
This document applies to issue certificates in relation to electronic or digital signatures of natural or legal persons, issue certificates on the verification regarding the alteration between the sending and receiving of the data message and transferable electronic documents, issue certificates in relation to the person who has a right or obligation with respect to the documents stated in literals f) and g) of article 26 of Law 527 of 1999.

1.1 General Description

Policy for Digital Certificate, hereinafter Policy, is a document prepared by Gestión de Seguridad Electronica SA (hereinafter GSE) which, acting as a Digital Certification Entity, contains the rules and procedures that the Digital Certification Entity (hereinafter 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 CERTIFICATION SERVICE PROVIDER ENTITY

Company Name:	GESTION DE SEGURIDAD ELECTRONICA SA
Initials:	GSE SA
Tax Identification Number:	900.204.272 - 8
Commercial Register No:	01779392 of February 28, 2008
Certificate of Existence and Legal Representative:	https://gse.com.co/documentos/marco-regulatorio/Certificado-de-existentia-y-Representante-Legal-GSE.pdf
Status of the commercial register:	Asset
Business address and correspondence:	77th Street No. 7 - 44 Office 701
City / Country:	Bogota DC, Colombia
Phone:	+57 (601) 4050082
Email: Website:	info@gse.com.co 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 from each other by periods and each one has a specific meaning.
Based on the OID, the generic ECD GSE certificate is distinguished, and in turn, based on this ECD GSE certificate, different subtypes are defined based on some specific characteristics, such as:

The content of the certificates, distinguishing:
If they are signing certificates, they are in turn 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 can be of different types:

- of Company Belonging
- Company Representation
- of Civil Service
- of Qualified Professional
- of Natural Person
- of Legal Entity
- Electronic Invoice

Whoever generates the keys for the digital certificate, distinguishing between the person holding the certificate or the ECD GSE itself.

The procedure to update the information contained in the certificates must be carried out in accordance with the provisions of the DPC "Certificate renewal with key change". To renew digital certificates, the procedure to request a

new certificate must be executed. The subscriber must access the GSE product and service request web portal and start the certificate renewal request process in the same way as when requesting the certificate for the first time. Your information will be validated again in order to update data if required.

OID of Policies

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

OID	DESCRIPTION
1.3.6.1.4.1.31136.1.4.16	Certificate Policy for Digital Certificates

Policies assigned to this document.

This specific document responds to the PCs of the following certificates and tr different subtypes: . GSE-PE

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

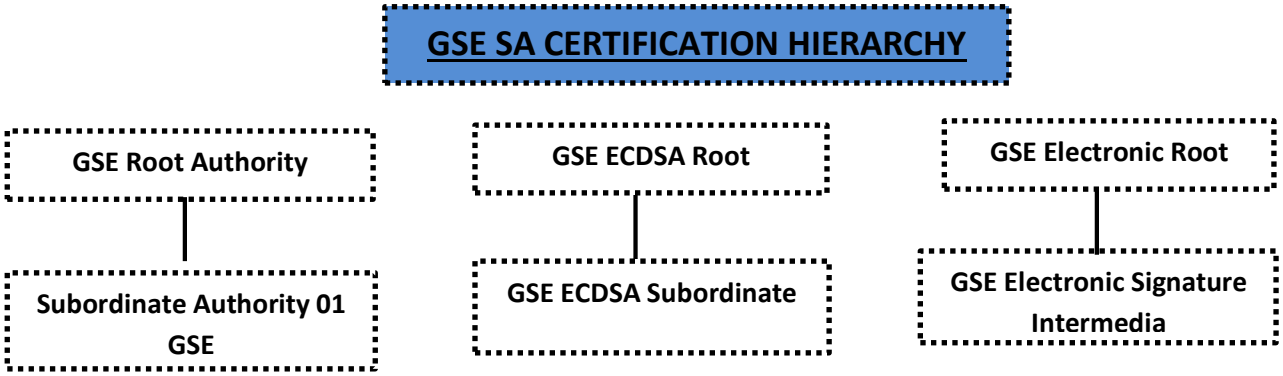
1.3. PKI Participants.

1.3.1. Certification Authority (CA).

It is a 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 CAs.

The GSE certification hierarchy is composed of the following Certification Authorities (CA):



GSE has two datacenters (one main and one alternate), the main datacenter with Hostdime is located in Verganzo, Zona Franca de Tocancipá Int 9, Km 1.5 via Briceño-Zipaquirá, Tocancipá, Cundinamarca, Colombia and the alternate datacenter with Claro is located on 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 certifying the validity of the information provided by the applicant for a digital certification service, by verifying the subscriber entity or entity responsible for the digital certification services. The RA decides on the issuance or activation of the digital certification service. To do this, it has defined the criteria and methods for evaluating applications.
Under this CPD, 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 person responsible for the same, trusting in it, with knowledge and full acceptance of the rights and duties established and published in this CPS.
The Subscriber figure will be different depending on the services provided by the ECD GSE as established in the Certificate Policies for digital certificates.

1.3.4. Trusted Parts.

The controller is the natural person to whom the digital certification services of a legal entity are activated and therefore acts as the controller of this legal entity, trusting in it, with knowledge and full acceptance of the rights and duties established and published in this CPS.
The person responsible will be different depending on the services provided by the ECD GSE as established in Annex 1 of this CPS.

Precautions to be observed by third parties:

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

Applicant.

The Applicant shall be understood as the natural or legal person interested in the digital certification services issued under this CPS. This may coincide with the figure of the Subscriber.
Entity to which the subscriber or responsible party is linked.
Where applicable, the legal person or organization to which the subscriber or controller 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 regulations of the management committee, who are responsible for approving the CPS as an initial document, as well as authorizing the changes or modifications required on the approved CPS and authorizing its publication.
Service providers.
Service providers are third parties that provide infrastructure or technological services to ECD GSE, when so required by GSE and guarantee the continuity of service to subscribers, entities during the entire time in which 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 when 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 details of the certificate, as well as its validity and validity.

Currently ECD GSE does not have any reciprocity agreements in force.

Petitions, Complaints, Claims and Requests.
Requests, complaints, claims and applications regarding the services provided by ECD GSE or subcontracted entities, explanations regarding this Certification Policy; are received and attended to directly by GSE as ECD and will be resolved by the relevant and impartial persons or by the committees that have the necessary technical competence, for which the following channels are available for the attention of subscribers, those responsible and third parties.

Phone:	+57 (1) 4050082
Email:	pqrs@gse.com.co
Address:	Calle 77 No. 7 – 44 office 701
Website:	www.gse.com.co
Responsible:	Customer service

Once the case has been submitted, it is transmitted with the information concerning the Customer Service process according to the internal procedure established for the investigation and management of these. Likewise, it is determined which area is responsible for taking corrective or preventive actions, in which case the action procedure must be applied.
Once the investigation is generated, the response is evaluated to subsequently make the decision that resolves the PQRS and its final communication to the subscriber, responsible party or interested party.

1.4. Use of the Certificate.

Based on the generic definitions established in the CPS 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 Controller, and where applicable, 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	Carrying out business procedures by the subscriber and/or controller without representation. The company may establish usage limitations.
Company Representation	Carrying out business procedures by the subscriber and/or responsible party on behalf of and representing the company. The company may establish usage limitations.
Civil Service	Carrying out procedures by the subscriber and/or responsible party in the exercise of tr functions as a public official. The Public Administration may establish usage limitations.
Qualified Professional	Completion of procedures by the subscriber and/or responsible party in the exercise of tr functions as a registered professional.
Natural person	Procedures carried out by the subscriber and/or responsible party in tr capacity as citizens. There is no connection with any entity.
Electronic Invoice	Completion by the subscriber and/or person responsible for billing and/or electronic

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

1.4.1. Proper use of certificates

In accordance with the Certification Practices Statement

1.4.2. Prohibited use of certificates

Any unauthorized transactions under this Policy by third parties or subscribers to the service will exempt ECD GSE from any liability for such prohibited use.

• The use of the certificate to sign other certificates or revocation lists (CRLs) is not permitted.
• It is prohibited to use the certificate for purposes other than those stipulated in the "Use of the Certificate" and "Limits of Responsibility of the Open Digital Certification Entity" section of this Policy.
• Alterations to certificates are not permitted and the certificate must be used as supplied by the ECD GSE.
• The use of certificates in control systems or fault-intolerant systems that may 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 the event of loss of the subscriber's private key because the CA does not keep a copy of the subscribers' private key for security reasons, therefore it is the subscriber's responsibility to use data encryption.
• Illegal purposes or operations under which 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" criteria and the fields defined therein and established in the technical profiles defined in Annex 1 of the CPD.
Under this criterion, one or another information that constitutes the subject of the certificate is guaranteed.
Thus, the digital certificates defined under this policy are the following:

TYPE OF DIGITAL CERTIFICATE	OBJECT
Company Membership	It guarantees the identity of the natural person who holds the certificate, as well as his or her connection to a specific legal entity by virtue of the position he or she holds therein.

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

TYPE OF DIGITAL CERTIFICATE	OBJECT
	This certificate will not in itself grant its holder greater powers than those he or she possesses through the performance of his or her usual activity.
Company Representation	It is issued to a natural person representing a specific legal entity. The certificate holder identifies himself not only as a natural person belonging to a company, but also adds his qualification as a legal representative of the company.
Civil Service	It guarantees the identity of the natural person who holds the certificate, as well as his or her connection to a Public Administration by virtue of his or her rank as a public official. This certificate will not in itself grant its holder greater powers than those he or she possesses through the performance of his or her usual activity.
Qualified Professional	It guarantees the identity of the natural person who holds the certificate, as well as his status as a qualified professional. This certificate will not in itself grant its holder greater powers than those he possesses through the performance of his usual activity in the field of his profession.
Natural person	It only guarantees the identity of the natural person.
Electronic Invoice	Exclusive certificate for electronic invoicing, meeting the needs of companies and/or individuals seeking the security of a certificate for issuing electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment documents, adjustment notes for electronic payroll payment document and other documents resulting from the processes of the unattended platforms of the technological providers approved by the DIAN, the DIAN free billing system and the RADIAN platform, in compliance with the technical annexes issued by said entity.
legal person	Carrying out business procedures by an application running on a machine in automatic and unattended signature processes on behalf of a public or private legal entity that requires guaranteeing the authenticity and integrity of the data sent or stored digitally and that will be represented by a person responsible for the certificate issued.

1.5. Policy Administration.

The administration of the Certification Policies (PC) will be in charge of the Operations process:

1.5.1. Organization administering the document:

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

In accordance with the Certification Practices Statement

1.5.2. Contact (ECD Manager):

Contact position:	Operations Manager
Contact telephone numbers:	4050082
Email:	info@gse.com.co

1.5.3. Person who determines the suitability of the DPC for the policy

In accordance with the Certification Practices Statement

1.5.4. CPD approval procedures.

Policies must be approved in all cases by the Management Committee.

Publication responsibilities

Once the policy changes have been made and approved, it is the responsibility of the Operations Manager and/or the Integrated Management System Process to request the process in charge to update the policies on the WEB portals in tr 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 entity providing public key infrastructure certification services.

Registration Authority (RA): This is the entity responsible for certifying the validity of the information provided by the applicant for a digital certificate, by verifying tr identity and registration.

Time Stamping Authority (TSA): Acronym for "Time Stamping Authority": Certification entity providing time stamping services

Reliable data archiving: This is the service that GSE offers its clients through a technological platform. Essentially, it consists of a secure and encrypted storage space that is accessed with credentials or a digital certificate. The documentation stored on this platform will have probative 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 his or her identity. This is the definition of Law 527/1999, which in this document is extended to cases in which the linking of signature verification data is made 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 Code (PIN): Acronym for "Personal Identification Number": Sequence of characters that allow access to the digital certificate.

Compromise of the private key: Compromise means the theft, loss, destruction or disclosure of the private key that may jeopardize the use of the certificate by unauthorized third parties or the certification system.

Certified email: Service that ensures the sending, receiving and checking of electronic communications, ensuring at all times the characteristics of fidelity, authorship, traceability and non-repudiation of the same.

Certification Practice Statement (CPS): A statement by the certification body regarding the policies and procedures it applies to the provision of its services.

Chronological stamp: 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 stamp was made.
Certification Entity: A legal entity, 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 clients who acquire them, to offer or facilitate the services of registration and time stamping of the transmission and reception of data messages, as well as to fulfill other functions related to communications based on digital signatures.
Open Certification Entity: It is a Certification Entity that offers services typical of certification entities, such as:
1. Its use is not limited to the exchange of messages between the entity and the subscriber, or
2. Receive remuneration for these.

Closed certification authority: Entity that offers services typical of certification authorities only for the exchange of messages between the entity and the subscriber, without requiring remuneration for this.
Public Key Infrastructure (PKI): Acronym for "Public Key Infrastructure": A PKI is a combination of hardware and software, security policies and procedures that allows users of a fundamentally insecure public network such as the Internet to exchange data messages in a secure manner using a pair of cryptographic keys (one private and one public) that are obtained and shared through a trusted authority.
Originator: A person who, acting on his or her 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 ECD guarantees the trustworthiness of one or more lower-level ECDs.
Certificate Revocation List (CRL): Acronym in English for "Certificate Revocation List": List that exclusively contains revoked certificates that have not expired.
Public Key and Private Key: The asymmetric cryptography on which PKI is based. It uses a pair of keys in which one can encrypt and only the other can decrypt, and vice versa. One of these keys is called public and is included in the digital certificate, while the other is called private and is known only to the subscriber or person responsible for the certificate.
Private key (Private key): Numeric value or values that, used in conjunction with a known mathematical procedure, serve to generate the digital signature of a data message.
Public key (Public key): Numeric value or values that are used to verify that a digital signature was generated with the private key of the person acting as initiator.
Hardware Security Cryptographic 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 tr use.
Certification Service Provider (CSP): A natural or legal person that issues digital certificates and provides other services related to digital signatures.
Online Certificate Status Protocol (OCSP): Protocol that allows the online verification of the status of a digital certificate
Repository: Information system used to store and retrieve certificates and other information related to them.
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 for the same.
Bona fide third party: Person or entity other than the subscriber and/or controller who decides to accept and trust a digital certificate issued by ECD GSE.
TSA GSE: Corresponds to the term used by ECD GSE, in the provision of its Time Stamping service, as a Time Stamping Authority.

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. August 30th, 2024

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: Hyper Text 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 the request-response scheme between a client and a server.
HTTPS: Hypertext Transfer Protocol Secure (in Spanish: Hypertext Transfer Protocol Secure), 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 Electro technical Commission
IETF: Internet Engineering Task Force 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 accepted internationally.
PKI: Public Key Infrastructure
PKIX: Public Key Infrastructure (X.509)
RA: Registrar 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 Certification Practices Statement

2.2. Publication of certification information.

In accordance with the Certification Practices Statement

2.3. Term or frequency of publication.

In accordance with the Certification Practices Statement

2.4. Access controls to repositories.

In accordance with the Certification Practices Statement

3. IDENTIFICATION AND AUTHENTICATION.

3.1. Names.

In accordance with the Certification Practices Statement

3.2. Initial identity validation.

In accordance with the Certification Practices Statement

3.3. Identification and Authentication for key renewal.

In accordance with the Certification Practices Statement

3.4. Identification and authentication for the revocation request.

In accordance with the Certification Practices Statement

4. OPERATIONAL REQUIREMENTS OF THE LIFE CYCLE OF THE CERTIFICATES.

4.1. Certificate request.

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

TYPE OF DIGITAL CERTIFICATE	REGISTRATION: REQUESTED INFORMATION
For all types of certificates the following information will be requested: • Completed application form. • Acceptance of terms and conditions. • Document and/or information certifying the applicant's identification	
Company Membership	• Document of Existence and Legal Representation of the Company with validity no greater than thirty (30) days. • Applicant's employment certificate including the position on institutional paper (no more than thirty (30) days old. • Single Tax Registry - RUT
Company Representation	• Document of Existence and Legal Representation of the Company with validity no greater than thirty (30) days. • Single Tax Registry - RUT In the event that the request is delegated by the Legal and/or Alternate Representative to a third party, the delegation letter must be attached for the request for the digital certificate.
Civil Service	• To confirm the applicant's relationship information with the Company, one of the following documents will be requested: 0 Deed of possession. 0 Appointment resolution or decree. 0 Service provision contract. 0 Employment certificate of the applicant including the position on institutional paper (no more than thirty (30) days from the filing of the application). • Single Tax Registry - RUT
Qualified Professional	• Applicant's address information • Professional Card and/or equivalent document. • Degree Diploma (optional)
Natural person	• Applicant's address information In the event that the service request is

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

TYPE OF DIGITAL CERTIFICATE	REGISTRATION: REQUESTED INFORMATION
	If the digital certification is generated from a reliable source or third party, for example 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 there is a contract, agreement, partnership, and/or any means of contractual and/or commercial relationship, direct and/or indirect.
Electronic Invoice	Natural person • Applicant's address information. In the event that the request is delegated by the Legal Representative and/or Alternate to a third party, the delegation letter must be attached for the request for the digital certificate.
	Artificial person • Single Tax Registry - RUT Document of Existence and Legal Representation of the Company with validity of no more than thirty (30) days. 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 request is delegated by the Legal Representative and/or Alternate to a third party, the delegation letter must be attached for the request for the digital certificate.
legal person	• Document of Existence and Legal Representation of the Company with validity no greater than thirty (30) days. • Single Tax Registry - RUT 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 request is delegated by the Legal Representative and/or Alternate to a third party, the delegation letter must be attached for the request for the digital certificate.
Notes: • Documents, where applicable, will be received in scanned or electronic original form, preserving legibility for the use of the information. • The Single Registry document	

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. August 30th, 2024

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

TYPE OF DIGITAL CERTIFICATE	REGISTRATION: REQUESTED INFORMATION
Tax - RUT when applicable, will be requested in the updated DIAN format that includes a QR code. • In the event that the applicant does not have a Single Tax Registry - RUT (when applicable), he/she must present a document where the address information is registered that is issued by a third party that verifies it or the address information will be consulted by the ECD GSE consuming data service from external sources. • For the types of certificate 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 the types of certificates where the Document of Existence and Legal Representation of the Company is requested, in the cases where it is required, an equivalent document where the existence and legal representation of the company can be validated will be valid; if applicable, the duly authenticated document will be requested. • For any document received authenticated, the authentication must be valid for no more than sixty (60) days from the filing of the application. • In cases where applications for digital certificates are submitted with additional documents and/or documents equivalent 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 CPS under "Computer security controls".
ECD GSE does not prevent or inhibit applicants from accessing services such as ECD, therefore a digital certificate can be requested regardless of the size of the applicant or subscriber, the type of relationship existing with ECD GSE, or membership with any association or group, nor does it depend on the number of digital certificates already issued or any other factor that discriminates access to the request for 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 the relationship of trust between the Applicant, Subscriber and/or Responsible Party, the receiving Entity or Third Party in good faith and the ECD, which 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 specific characteristics for each type of digital certificate. These characteristics are defined as specific requirements and are defined in the following section.

Specific Requirements

Based on the generic definitions established in the CPS regarding the figures of Subscriber and/or Responsible Party 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 / CONTROLLER	ATTRIBUTE	ENTITY
Company Membership	Natural person who belongs to the company and who is the holder of the certificate.	Linking company membership	Company to which the Subscriber is linked
Company Representation	Natural person who legally represents the company and who is the holder of the certificate	Linking legal representation to company	Company that the Subscriber represents
Civil Service	Natural person who belongs to a Public Administration and who is the holder of the certificate	Civil service link with respect to a Public Administration	Public Administration to which the Subscriber is linked
Qualified Professional	Natural person who exercises a qualified profession and who is the holder of the certificate	Practice of a professional association and connection with the Professional Association	Professional Association to which the Subscriber is linked
Natural person	Natural person holding the certificate	Not applicable	Not applicable
Electronic Invoice	It only guarantees the identity of the subscriber and/or responsible party	Linking for electronic billing and/or payroll	Subscriber and/or responsible party who requires electronic billing and/or payroll
Artificial person	Person responsible for the certificate that is issued on behalf of a Legal Entity	Linking legal representation to company	Company that the Subscriber and/or responsible party represents.

4.2. Processing certificate request.

In accordance with the Certification Practices Statement

4.3. Issuance of the Certificate.

In accordance with the Certification Practices Statement

4.4. Acceptance of the Certificate.

In accordance with the Certification Practices Statement

4.5. Using key pairs and certificates.

In accordance with the Certification Practices Statement

4.6. Certificate Renewal.

In accordance with the Certification Practices Statement

4.7. Re-use of certificate key.

In accordance with the Certification Practices Statement

4.8. Certificate Modification.

In accordance with the Certification Practices Statement

4.9. Revocation and Suspension of the Certificate.

In accordance with the Certification Practices Statement

4.10. Certificate Status Services.

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. August 30th, 2024

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

In accordance with the Certification Practices Statement

4.11. End of Subscription.
In accordance with the Certification Practices Statement

4.12. Key Custody and Recovery.
In accordance with the Certification Practices Statement

5. FACILITIES, MANAGEMENT AND CONTROLS OPERATIONAL.

5.1. Physical Security Controls.
In accordance with the Certification Practices Statement

5.2. Procedural Controls.
In accordance with the Certification Practices Statement

5.3. Personnel controls.
In accordance with the Certification Practices Statement

5.4. Audit Log Procedures.
In accordance with the Certification Practices Statement

5.5. Records Archive.
In accordance with the Certification Practices Statement

5.6. Change of Keys.
In accordance with the Certification Practices Statement

5.7. Disaster Engagement and Recovery.
In accordance with the Certification Practices Statement

5.8. Termination of CA or RA.
In accordance with the Certification Practices Statement

6. TECHNICAL SAFETY CONTROLS.

6.1. Generation and Installation of Key Pairs.
In accordance with the Certification Practices Statement

6.2. Private Key protection and engineering controls of cryptographic modules.
In accordance with the Certification Practices Statement

6.3. Other Aspects of Key Pair Management.
In accordance with the Certification Practices Statement

6.4. Activation Data.
In accordance with the Certification Practices Statement

6.5. Computer Security Controls.
In accordance with the Certification Practices Statement

6.6. Life Cycle Technical Controls.
In accordance with the Certification Practices Statement

6.7. Network Security Controls.
In accordance with the Certification Practices Statement

6.8. Chronological Print.
In accordance with the Certification Practices Statement

7. CERTIFICATE, CRL AND OCSP PROFILES.

7.1. Certificate Profile.
In accordance with the Certification Practices Statement

7.2. CRL Profile.
In accordance with the Certification Practices Statement

7.3. OCSP Profile.
In accordance with the Certification Practices Statement

8. COMPLIANCE AUDIT AND OTHER EVALUATIONS.

8.1. Frequency or Circumstances of the Evaluation.
In accordance with the Certification Practices Statement

8.2. Identity and qualifications of the evaluator.
In accordance with the Certification Practices Statement

8.3. Relationship of the evaluator with the entity evaluated.
In accordance with the Certification Practices Statement

8.4. Topics to be evaluated.
In accordance with the Certification Practices Statement

8.5. Actions taken as a result of the deficiency.
In accordance with the Certification Practices Statement

8.6. Communication of Results.
In accordance with the Certification Practices Statement

9. OTHER COMMERCIAL AND LEGAL MATTERS.

9.1. Fee.
In accordance with the Certification Practices Statement

9.2. Financial Responsibility.

In accordance with the Certification Practices Statement

9.3. Confidentiality of Commercial Information.

In accordance with the Certification Practices Statement

9.4. Privacy of Personal Information.

In accordance with the Certification Practices Statement

9.5. Intellectual Property Rights.

In accordance with the Certification Practices Statement

9.6. Representations and Warranties.

In accordance with the Certification Practices Statement

9.7. Disclaimer of Warranties.

Not Applicable

9.8. Limitations of Liability.

The Open Certification Authority's Liability Limitations are comprehensively defined in the section Limits of Liability of the CPD, but based on the specific uses of each of the certificates established in the previous section. ECD GSE does not assume any other commitment or provide any other guarantee, nor does it assume any other liability to certificate holders or trusted third parties except as established by the provisions of this CP.
The ECD GSE will decline a request for a digital certification service if it is not within the scope of the accreditation granted by ONAC.

TYPE OF DIGITAL CERTIFICATE	LIMITATION OF LIABILITY OF THE CERTIFICATION ENTITY
Belonging to a company, 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 CPS and specifically in the section Use of certificate. Any uses that are not defined in the DPC and the 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, the PC and in accordance with the provisions of the Limits of Responsibility of the open certification entity.

9.9. Compensation.

Not Applicable

9.10. Duration and Termination.

In accordance with the Certification Practices Statement

9.11. Individual notifications and communications to participants.

In accordance with the Certification Practices Statement

9.11.1. Obligations of the ECD GSE

ECD GSE as a certification services provider is obliged according to current regulations, in the provisions of the Certificate Policies and the CPS to:
1. Comply with the provisions of current regulations, the CPD and the Certificate Policies.

2. Publish the CPD and each of the Certificate Policies on the GSE website.
3. Inform ONAC about changes to the CPS and Certificate Policies.
4. Maintain the CPD and Certificate Policies with latest version published on the GSE website.
5. Safely and responsibly protect and store your private key.
6. Issue certificates in accordance with the Certificate Policies and standards defined in the CPD.
7. Generate certificates consistent with the information provided by the applicant or subscriber.
8. Maintain information on digital certificates issued in accordance with current regulations.
9. Issue certificates whose minimum content complies with current regulations for the different types of certificates.
10. Publish the status of issued digital certificates in a freely accessible repository.
11. Do not keep a copy of the private key of the requester or subscriber.
12. Revoke digital certificates as provided in the Digital Certificate Revocation Policy.
13. Update and publish the CRL digital certificate revocation 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 proximity of the expiration of digital certificate.
16. Have 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 free of charge and with open access on the ECD GSE website:

- The Certification Policies and Practices Statement and all updates thereto.
- Obligations of the subscriber and the way in which the data must be kept
- 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 by itself or through a different person acting on its behalf and on its account, the identity and any other circumstances of the applicants or of the data of the certificates, which are relevant for the purposes of the verification procedure prior to issuance.
19. Inform the Superintendency of Industry and Commerce and the ONAC immediately of any event that compromises or may compromise the provision of the service.
20. To promptly report any modification or update of services included in the scope of its accreditation, in accordance with the terms established by 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. Train and warn users about the security measures they must observe and about the logistics required to use the service provision mechanisms.
23. Guarantee the protection, integrity, confidentiality and security of the information provided by the subscriber by keeping the documentation supporting the certificates issued.
24. 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 the ONAC.
25. Provide the accredited services on the ECD GSE website.

9.11.2. Obligations of the RA

The RA of the ECD GSE is authorized to carry out the identification and registration work, therefore, it is obliged in the terms defined in the Certification Practices Statement to:

1. Know and comply with the provisions of the CPS 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 the Applicants, Controllers or Subscribers of digital certificates.
4. Verify the accuracy and authenticity of the information provided by the Applicant using the protocols described in the CPS
5. 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. Comply with 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 Controller

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 in accordance with the terms of the DPC.
2. Check within the next business day that the information on the digital certificate is correct. If you find any inconsistencies, notify the ECD.
3. Refrain from: lending, transferring, writing, publishing the password for using your digital certificate and take all necessary, reasonable and appropriate 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 revocation of the Digital Certificate due to a change of name and/or surname.
7. Request the revocation of the Digital Certificate when the Subscriber has changed his/her nationality.
8. Comply with what is accepted and signed in the terms and conditions document or the person responsible for digital certificates.
9. Provide accurately and truthfully city the required information.
10. Report any changes to the data initially provided for issuing the certificate during the validity of the digital certificate.
11. Responsibly safeguard and protect your private key.
12. Use the certificate in accordance with the provisions of this PC for each type of certificate.
13. As a subscriber or responsible party, request the immediate revocation of your digital certificate when you become aware that there is a reason defined in 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 check the validity of the digital certificates that you are using at any given time.
16. Informing the third party in good faith to verify the status of a certificate has the list of revoked certificates CRL, published periodically by ECD GSE.
17. Do not use your digital certification in a way that contravenes the law or brings the ECD into disrepute.
18. Do not make any statement relating to your digital certification in the ECD GSE that may be considered misleading or unauthorized, as provided for by the CPD 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 report that it complies with the requirements specified in the DPC PCs, indicating the version.
21. The subscriber may use the conformity marks and information related to the digital certification service provided by ECD GSE in communication media, such as documents, brochures or advertising, provided that the requirements of the previous paragraph are met.

On the other hand, you have the following rights:

1. Receive the digital certificate within the time 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 communication media, such as documents, brochures or advertising, provided that the requirements of the previous paragraph are met.
3. Request information regarding applications in process.
4. Request revocation of the digital certificate by providing the necessary documentation.
5. Receive the digital certificate according to the Scope granted by ONAC to GSE.

9.11.4. Obligations of Third Parties in Good Faith

Third parties acting in good faith in capacity as parties trusting the digital certificates issued by ECD GSE are obliged to:

1. Know the provisions regarding Digital Certification in current regulations.
2. Know the provisions of the DPC and PC.
3. Check the status of certificates before performing operations with digital certificates.
4. Check the Certificate Revocation List (CRL) before performing operations with digital certificates.
5. 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 services for its employees and the subscribers are the people who use the service.

In accordance with the provisions of the Certificate Policies, in the case of certificates where the link between the Subscriber or Responsible Party and the same is accredited, it will be the obligation of the Entity:

1. Request the RA GSE to suspend/revoke the certificate when said relationship ceases or changes.
2. All obligations linked 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 report that it complies with the requirements specified in the CP of the DPC.
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 set out in the following: wanted in the previous literal.

9.11.6. Obligations of other ECD participants

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

1. Review the consistency of the CPD 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 controllers.
3. Approve notification of any changes to subscribers and/or controllers, analyzing tr legal, technical or commercial impact.
4. Review and take action on any comments made by subscribers and/or managers when a change to the digital certification service is made and.

5. Inform ONAC and SIC of action plans regarding any change that impacts the PKI infrastructure and affects digital certification services, in accordance with RAC-3.0-01.
6. Authorize the required changes or modifications to the CPD.
7. Authorize the publication of the CPD 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 Web page of lto ECD GSE.
10. Ensure that controls are in place over the ECD GSE's technological infrastructure.
11. Request the revocation of a certificate if you have knowledge or suspicion of the compromise of the subscriber's or entity's private key or any other fact that tends to the improper use of the subscriber's or entity's private key or the ECD itself.
12. Be aware of and take appropriate action when security incidents occur.
13. Carry out a review of the CPS at least once a year to verify that the key lengths and periods of the certificates being used are appropriate.
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 required by ECD GSE to indicate that the digital certification service is accredited.
16. Ensure that the conditions of accreditation granted by the competent body are maintained.
17. Ensure the proper use in documents or in any other advertising of symbols, certificates, and any other mechanism that indicates that ECD GSE has an accredited certification service and complies with the provisions of ONAC Accreditation Rules RAC-3.0-01 and RAC-3.0-03.
18. Ensure that critical suppliers and reciprocal ECD, if any, are kept informed of the obligation to comply with the CEA requirements, in the corresponding sections.
19. The Integrated Management System process will execute preventive and corrective action plans to respond to any risk that compromises the impartiality and non-discrimination of the ECD, whether it arises from the actions of any person, body, organization, activities, its relationships or the relationships of its staff or itself. For this purpose, it uses the ISO 31000 standard for the identification of risks that compromise the impartiality of the ECD.
20. Ensure that all ECD staff and committees (whether internal or external) that may have influence on certification activities act impartially and without discrimination, especially those arising from commercial, financial or other pressures that compromise tr impartiality.
21. Document and demonstrate 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 with respect to the staff involved in the review and decision-making process regarding the certification of the same ECD.
23. Ensure that critical suppliers such as the ECD are kept informed reciprocal and datacenter that meet the accreditation requirements for ECD as support for hiring and compliance with the requested administrative and technical requirements.

9.12. Amendments.

In accordance with the Certification Practices Statement

9.13. Dispute resolution provisions.

In accordance with the Certification Practices Statement

9.14. Applicable legislation.

In accordance with the Certification Practices Statement

9.15. Compliance with applicable legislation

In accordance with the Certification Practices Statement

9.16. Miscellaneous provisions.

In accordance with the Certification Practices Statement

9.17. Other Provisions.

In accordance with the Certification Practices Statement

CHARACTERISTICS OF CRYPTOGRAPHIC DEVICES

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

Digital Certificate in Token

Characteristics

CHARACTERISTIC	TECHNICAL SPECIFICATION
Supported Operating Systems	32bit and 64bit 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 blocked on 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

Security 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 unusability due to damage to the cryptographic device.
- Unauthorized access, by a third party, to the activation data of the Signatory or the person responsible for the certificationified

Care of the cryptographic device

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. August 30th, 2024

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

- Keep it in a dry place and away from environmental and/or temperature variations.
- Do not expose to magnetic fields.
- Prevent him from being hit or subjected to any physical effort.
- 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.

Associated risks

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

- Lost device.
- Key commitment.
- Damage due to improper handling.
- Damage due to failure to take care of the device in the face of environmental conditions.
- Damage due to voltage variation.

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

- The digital signature certificate is personal and non-transferable, the PIN is confidential.
- It is recommended to change your PIN periodically.
- Do not enter the PIN incorrectly more than three (3) times, it will lock the device.
- Cryptographic devices must be kept in suitable environmental conditions.
- In case of commitment orloss of the private key must request the revocation of the digital certificate.

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

CHARACTERISTIC	TECHNICAL SPECIFICATION
Supported Operating Systems	32bit and 64bit . 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 after the third access attempt with an incorrect password

Technical Characteristics of Digital Certificates

CHARACTERISTIC	TECHNICAL SPECIFICATION
Signature Algorithm	SHA256 Hash Function with RSA Encryption. SHA384 Hash Function with ECDSA Encryption Function
	RSA with key length of 4096 for ROOT CA RSA with key length of 4096 for SUBORDINATED AC RSA with subscriber/manager key length of 2048.

	ECDSA with key length of 384 for ROOT CA ECDSA with key length of 384 for SUBORDINATE CA ECDSA with subscriber/controller key length of 256.
Content of the Digital Certificate	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. May 2008. ITU-T-X509 October 2019 ETSI TS 102 042 - Policy requirements for certification authorities issuing public key.
Certificate life cycle	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
Key generation	FIPS 140-2 Level 3 Token HSM FIPS 140-2 Level 3 (Centralized Signature)
Certification activities article 161 of decree law 0019 of 2012	1. Issue certificates in relation to electronic or digital signatures of natural or legal persons. 2. Issue certificates on verification regarding the alteration between the sending and receiving of the message, data and electronic transferable documents. 3. Issue certificates in relation to the person who has a right or obligation with respect to the documents stated in paragraphs f) and g) of article 26 of Law 527 of 1999

DIGITAL CERTIFICATE ISSUANCE SERVICE RATES

In accordance with the Certification Practices Statement

IMPARTIALITY AND NON-DISCRIMINATION

In accordance with the Certification Practices Statement

MODELS AND MINUTES OF THE TERMS AND CONDITIONS DOCUMENTS

In accordance with the provisions of Annex 2 of the CPD.

CERTIFICATE PROFILE

See Annex 1 of the DPC Technical Profile Matrix of Certificates

OID (Object Identifier)	1 1.3.6.1.4.1.31136.1.4.16
PC Location	https://qse.com.co/documentos/calidad/politicas/Certificate policy for digital certificates V16.pdf