Document Title	**CPS, certificate practice statement, certification practice statement**
Version	15
Working Group	Board of Management
Document status	Final
Date of issue	01/11/2016
Effective Start Date	16/05/2023
OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.1.15
LOCATION OF THE	https://gse.com.co/documents/quality/DPC/Declaracion_de_Practicas_de_Certificacion_V15.pdf
Prepared by	Operations Manager
Reviewed by	Integrated Management System
Approved	Board of Management

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* July 06,*2023

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

CHANGE CONTROL

Version	Date	Change/Modification
1	01-11-2016	Initial document
2	04-10-2017	• Update of contact details of the ECD and Logo • Updating Enrollment Entities • Updating contact details Certification service providers • Information regarding the General Manager of GSE. TSA GSE data update.
3	03/04/2018	Update information and adjustments in relation to CEA-4.1-10 in accordance with the review of the requirements matrices.
4	27/11/2018	It was changed from V3 to V4 on 27/11/2018 Update of table of contents, information and adjustments in relation to new charges, rates, routes of access to the website, correction of the subordinate, the established and tested phrase is included, numeral 8.7.4 is extended naming the technological mechanisms used for data protection, all the certification policies, change of terms and update of the legal representative were related.
5	12/04/2019	The EE numeral was deleted, it was clarified that, for the use of the centralized signature certificate, it is necessary to acquire a technological platform with additional costs. The clarification is made in section 1.6.2 of the requirements and restrictions of the RA and of Criteria and methods of evaluation of the Applications. RA Roles Updated
6	07/06/2019	Clarification of the scope of accreditation under CPD 1.1 Summary 4.1 Request for the certificate, the procedure of how to access the service is clarified. 4.1.1 Clarification of non-discrimination when accessing the service. 8.9.3 Clarification of rights of the subscriber or responsible
7	31/03/2020	The CPD is adjusted to the changes generated by the new platforms, the objective and scope numbers are added, the price list is adjusted, the links are modified to point to the new routes, the change of the Legal Representation is made and the services accredited by ONAC are more specifically related.
8	14/08/2020	Everything related to the Digital Signature Generation service is eliminated, another condition is added in section 5.2.2 Authentication of the identity of an entity, for the renewal of digital signature certificates and the services used for identity validation are mentioned.

Version	Date	Change/Modification
9	12/02/2021	The link to consult online the Certificate of Existence and Legal Representation for the ECD and the current CA (Paynet SAS) was included. The detailed information of the current CA (Paynet SAS) and historical CA (Indenova) was included in accordance with the provisions of item 1 of numeral 10.7 of CEA 4.1-10. The data center information was modified in accordance with the provisions of the ONAC accreditation certificate. The paragraph on the renewal of digital certificates in 5.2.2 and 5.2.3 was deleted. The following numerals were updated: • 6.4.2 Approval or rejection of certificate applications • 6.4.3 Deadline for processing certificate requests • 7.10.1 Trust Roles • 8.1.4 Delivery of the ECD public key to accepting third parties Updated links to point to new routes
10	16/07/2021	The numbers have been updated: 3.6.1 Certification Authority (CA), data provider datacenter. 4.1 Repositories Paragraph 6.5.6 was updated. 6.5.7 Deadline for processing certificate applications 6.8.2 Use of the private key and certificate by bona fide third parties 6.12 Revocation and suspension of certificates 6.12.3 Request for revocation procedure 6.13.1Description of the content of the certificates Subordinated Authority 01 GSE 6.13.1.8 Object identifiers (OIDS) of algorithms 6.14.1.3 CRL Availability 6.14.1.7 OCSP Availability 6.14.3 Optional Features 7.10.1 Trust Roles 8.1.4 Delivery of the ECD public key to accepting third parties 8.1.5 Key size 8.1.6 Public Key Generation Parameters and Quality Verification 8.2.4 Backup of the private key 8.2.5 Private Key File 8.2.6 Transferring the private key from the cryptographic module 8.2.7 Storing private keys in a cryptographic module

Version	Date	Change/Modification
		8.5.3 Actions in the event of an information security event or incident 10. DESCRIPTION OF PRODUCTS and SERVICES, Archiving Service, Registration, Conservation, Custody and Annotation for Electronic Documents 11.7.1 Personal Data Processing Policy 11.3 Impartiality and Non-Discrimination 14. ANNEX 1 DPC MATRIX TECHNICAL PROFILE DIGITAL CERTIFICATES 15. ANNEX 2 TERMS AND CONDITIONS OID and query links are updated from: • Statement of Certification Practices • Certificate Policies for Digital Certificates • Certificate Policies for Chronological Stamping Service • Certificate Policies for Archiving, Registration, Conservation, Custody and Annotation of Transferable Electronic Documents and Data Messages. • Certificate Policies for Certified Email Service
11	5/10/2021	• The numbers were updated including electronic signature: 6.1 Application for the certificate 6.5 Initial validation of identity 6.5.1 Method for proving possession of the private key Description of Products and Services 11.1.1 Fees for issuing or renewing certificates 11.9.3 Obligations of the Subscriber and/or Responsible. • The following numerals were included with reference to electronic signature: 5.1.1.1.1 Electronic Signature 5.1.1.2.2 ECD GSE Subscriber Certificates (Matrix Technical Profile of Electronic Signature Certificates) Certification policies 16 Annex 3 DPC matrix technical profile certificates electronic signature • A clarifying note of the validation of the OCSP was included in sections 4.1, 4.3, 6.12.9, 6.12.10, 6.14.3. • Paragraph 6.12.3 Revocation request procedure was updated by adding a new online revocation channel.

Version	Date	Change/Modification
		• Paragraph 8.3.2 was updated giving clarity of the validity period of the root and subordinate keys of the RSA and ECDSA algorithm • OID and query links are updated
12	27/10/2021	• The number 6.5 of Identity Validation has been modified • Updated the OIDS and the link of the Digital Certificate PC • The OID and the DPC link were updated with this new version.
13	31/05/2022	According to the new version of CEA, adjustments were made to the following numerals: • 3.1 Summary: 4.1-10 was deleted leaving only CEA. • 3.2. Petition, Complaint, Claim and Applications: The appeal term was removed. • 3.6 PKI Participants: Indenova is deleted as CA. • 5.1.1.1 – 5.1.1.2 Types of Names: The root and subordinate certificates of Indenova are eliminated and those related to elliptic curve are included. • 6.5 Initial Identity Validation: A final paragraph on confrontational consumption was included in the services. • 6.13.1 Description of the contents of the certificates: The subject's alternative name field was included. • 6.13.1.7 3 purposes were removed from the key. • 7.10.1 Trust Roles: The roles of RA Agents, RA Administrator, and RA Auditor were changed: • 7.16 Cessation of an ECD: Amended as required in the new CEA. • 9.2 Auditor Identity/Qualification: Assurance requirements have been modified. • 10. Description of products and services: The centralized signature certificate was deleted, the Archive service name was modified and the electronic signature generation service was modified in accordance with the accreditation certificate. • 11.4. Exemption for limits of liability was modified. • 11.9.6 Obligation of other participants: Item r) was modified by eliminating 4.1-10 leaving only CEA. • 15. The name of the annex on terms and conditions was amended. • 16. This item of the technical annex to the electronic signature certificate is included.

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* July 06,*2023

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

Version	Date	Change/Modification
		• Updated the OIDS and the link of the Digital Certificate PC • The OID and the DPC link were updated with this new version. • The quality code was included in the document header.
14	23/09/2022	• 3.1 Summary: The chapters of the Durscit were included. • The direction of the ECD was changed in items 3.1, 3.2, 3.6.2 and 3.7.1. • The Paynet SAS address was changed in items 3.6.1 and 3.6.7.2. • Paragraph 3.6.4 was amended by changing the responsible party to a third party in good faith • Section 3.6.4.1 Precautions to be observed by third parties • Paragraph 6.4.1 Performing the identification and authentication functions has been modified • Paragraph 6.5.1 Method to demonstrate the possession of the private key was modified giving clarity in case the applicants generate the pair of keys in their own infrastructure. • Paragraph 6.5.5 Interoperability criteria has been amended • Paragraph 6.12.7 Frequency of updating the CRLs was modified according to the percentage of availability established in the new CEA. • RFC 2560 was amended by RFC 6960 in 6.12.10 Online Revocation Check Requirements, 6.14.1.4 OCSP Profile and 6.14.1.5 Version Number. • Paragraph 7.7 is amended. Storage system making it clear that servers are in cloud environments. • Paragraph 7.4 is amended. Exposure to water clarifying that it refers to PKI datacenters. • Paragraph 7.16 was amended. Cessation of an ECD including a paragraph on the Cessation of Activities Safety Plan. • 11.4 Limits of liability were modified including Liability for the veracity of the Subscriber's information, Liability for availability of the service, Liability for the functionality of the service in the Subscriber's infrastructure, Liability for computer crimes.

Version	Date	Change/Modification
		• The number 11.9.1 Obligations of the ECD GSE including the items o) to y) was modified. • Paragraphs 12.3 Notification and communication, 12.5 Prevention and Resolution of disputes, 12.6 Applicable law and 12.7 Compliance with applicable law were included. • Updated the OIDS and the link of the Digital Certificate PC • The OID and the DPC link were updated with this new version.
15	16/05/2023	• The entire order of the document was modified in accordance with RFC 3647. • Paynet SAS was removed as the CA authority as the PKI was moved to the GSE ECD. • Changed to Director of Operations by Operations Manager • The data of the main and alternate datacenters were modified, leaving Hostdime and Claro. • The OIDs and the Policy link have been updated. • The OID and the DPC link were updated with this new version.

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* July 06,2023**

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

1. CONTENTS OF THE DECLARATION OF CERTIFICATION PRACTICES.

1.1. INTRODUCTION.

1.1.1. Overview

The Declaration of Certification Practices (DPC)- Global Certification Authority Root GSE (hereinafter DPC) is a document prepared by **Gestión de Seguridad Electrónica S.A. (hereinafter GSE)** that acting as a Digital Certification Entity, contains the rules, statements on the policies and procedures that the **Digital Certification Entity (hereinafter ECD GSE)** as a Digital **Certification Service Provider (PSC)** applies as a guideline 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, in the territory of Colombia.

The CPD agrees with the following guidelines:

i. Specific Accreditation Criteria for Digital Certification Entities (hereinafter CEA) that must be met to obtain Accreditation as a Digital Certification Entity - ECD, before the National Accreditation Body of Colombia – ONAC;
ii. The DPC is organized under the structure defined in document RFC3647 Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework of the IETF working group - The Internet Engineering Task Force, (which replaces RFC2527) http://www.ietf.org/rfc/rfc3647.txt?number=3647.
iii. ETSI EN 319 411-1 V1.2.0 (2017-08).
iv. Chapters 47 and 48 of Title 2 of Part 2 of Book 2 of the Single Decree of the Trade, Industry and Tourism Sector – DURSCIT

The updating and/or modification of the DPC will be carried out through the procedure established by GSE of documented information, any change or adaptation on the document must be reviewed, analyzed and approved by the Management Committee.

This document applies to products and services accredited by the National Accreditation Agency of Colombia - ONAC.

ELECTRONIC SECURITY MANAGEMENT DATA S.A.:

Business Name:	GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.
Acronym:	GSE S.A.

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* July 06,*2023

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

Tax Identification Number (TIN)	900.204.272 – 8
Trade Registration No.	01779392 of 28 February 2008
Certificate of Existence and Legal Representative:	https://gse.com.co/documents/regulatory-framework/Certificate-of-Existence-and-Representative-Legal-GSE.pdf
Status of the commercial register:	Asset
Company address and correspondence:	Calle 77 No. 7 – 44 Office 701
City/ Country:	Bogotá D.C., Colombia
Phone:	+57 (1) 4050082
Fax:	+57 (1) 4050082
E-MAIL:	info@gse.com.co
Website:	www.gse.com.co

1.1.2. Name and identification of the document.

The **DPC** for **ECD GSE** will be called “Declaration of Certification Practices (DPC)” The version changes according to the modifications on the same document.

GSE is a registered company (Registered Private Enterprise) with the international organization IANA (Internet Assigned Numbers Authority), with the private code No 31136 under the branch 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprise). The above information can be consulted at the URL, searching by code 31136 http://www.iana.org/assignments/enterprise-numbers

The hierarchy of OIDs was established by ECD GSE from the root 1.3.6.1.4.1.31136 defined by the IANA and conforms to the following parameters:

OID HIERARCHY	DESCRIPTION	NAME
1	ISO format	Unvarying
3	Organization	Unvarying
6	Public	Unvarying
1	Internet	Unvarying
4.1 (31136)	Organization Id	Not varied, as defined by the IANA
1	Type of document	It changes depending on whether they are policies, procedures, manuals among others
1	Document Number	This is the number assigned to the

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* July 06,*2023

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

		document among your group
14	Document version	It is modified according to each version of the document

In accordance with this hierarchy, this CPD has been identified with the OID: **1.3.6.1.4.1.31136.1.1.15**

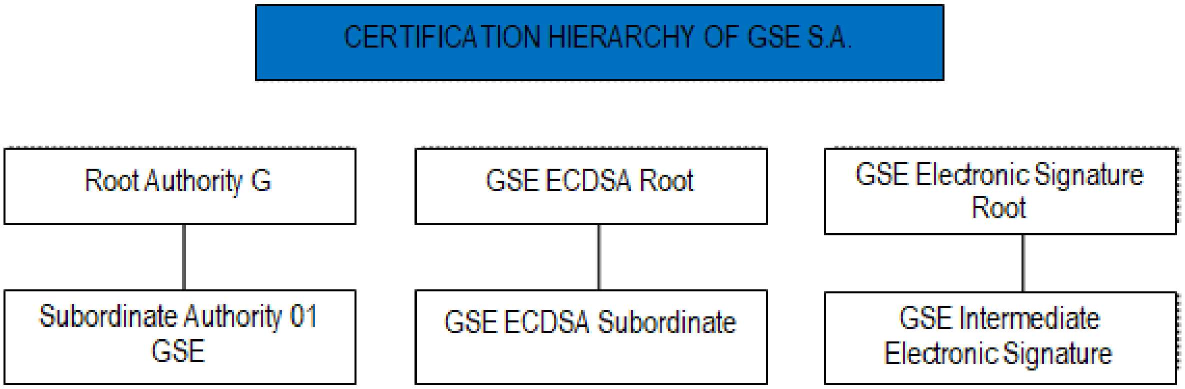
1.1.3. PKI Participants.

1.1.3.1. Certification Authority (CA).

It is that legal person, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, empowered 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.

1.1.3.2. Hierarchy of CAs.

The GSE certification hierarchy is composed of the following Certifying Authorities (CAs):


CERTIFICATION HIERARCHY OF GSE S.A.
Root Authority G
Subordinate Authority 01 GSE
GSE ECDSA Root
GSE ECDSA Subordinate
GSE Electronic Signature Root
GSE Intermediate Electronic Signature

GSE has two datacenters (one main and one alternate), the main datacenter with Hostdime is located on the Verganzo sidewalk, Zona Franca de Tocancipá Int 9, Km 1.5 via Briceño-Zipaquirá, Tocancipá, Cundinamarca, Colombia and the alternate datacenter with Claro is located on the Medellin Km 7.5 Celta Trade Park – Datacenter Triara, Cota, Cundinamarca, Colombia.

1.1.3.3. Registration Authority (RA).

It is the GSE area responsible for certifying the validity of the information provided by the applicant for a digital certification service, by verifying the entity of the subscriber or responsible for the digital certification services, in the RA it is decided 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 GSE ECD Subordinate.

Under no circumstances does GSE delegate the functions of Registry Authority (RA).

1.1.3.4. Subscriber and/or responsible.

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

The figure of Subscriber will be different depending on the services provided by the ECD GSE as established in the Certificate Policies for digital certificates.

1.1.3.5. bona fide third party

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

The person in charge will be different depending on the services provided by the ECD GSE as established in Annex 1 of this CPD.

1.1.3.6. Precautions to be observed by third parties:

a) Verify the scope of the certificate in the associated certification policy.
b) Consult the regulations associated with digital certification services
c) Verify the ECD's accreditation status with ONAC.
d) Verify that the digital signature was generated correctly.
e) Verify Certificate Source (Certification String)
f) Verify its conformity with the content of the certificate.
g) Verify the integrity of a digitally signed document.

1.1.3.7. Applicant.

Applicant shall mean the natural or legal person interested in the digital certification services issued under this DPC. It can match the Subscriber figure.

1.1.3.8. Entity to which the subscriber or responsible is linked.

Where applicable, the legal person or organisation to which the subscriber or controller is closely related through accredited linking in the digital certification service.

1.1.3.9. Other participants.

1.1.3.10.Board of Management

The Management Committee is an internal body of ECD GSE, made up of the Director General and Directors who have responsibility for the approval of the DPC as an initial document, as well as authorizing the changes or modifications required on the approved DPC and authorizing its publication.

1.1.3.11. SERVICE PROVIDERS

Service providers are third parties that provide infrastructure or technological services to ECD GSE, when GSE requires it and guarantees the continuity of the service to subscribers, entities throughout the time in which the digital certification services have been contracted.

1.1.3.12.Reciprocal Digital Certification Entities.

In accordance with the provisions of article 43 of Law 527 of 1999, certificates of digital signatures 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 details of the certificate, as well as its validity and validity.
ECD GSE does not currently have reciprocity agreements in place.

1.1.3.13.Petitions, Complaints, Complaints and Requests.

Requests, complaints, claims and requests about the services provided by ECD GSE or subcontracted entities, explanations about this DPC and its policies; are received and addressed 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, managers and third parties.

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* July 06,*2023

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

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 is presented, it is transmitted with the information concerning the Customer Service process according to the internal procedure established for the investigation and management of these. Similarly, 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, manager or interested party.

1.1.4. Certificate Usage

1.1.4.1. List of types of uses for which certificates are supported.

Appropriate uses of Certificates issued by ECD GSE are specified in Certificate Policies for Digital Certificates.

Certificates issued under this DPC may be used for the following purposes:

- **Identification of the Subscriber:** The Subscriber of the Digital Certificate can authenticate, in front of another party, his identity, demonstrating the association of his private key with the respective public key, contained in the Digital Certificate.
- **Integrity:** The use of the Digital Certificate to apply digital signatures guarantees that the signed document is intact, that is, it guarantees that the document was not altered or modified after being signed by the Subscriber. It is hereby certified that the message received by the entrusting Recipient or Destination is the same as that issued by the Subscriber.
- **Non-repudiation:** The use of this Digital Certificate also guarantees that the person who digitally signs the document cannot repudiate it, that is, the Subscriber who has signed it cannot deny the authorship or integrity of it.

The public key contained in a Digital Certificate can be used to encrypt data messages, such that only the holder of the private key can decrypt said data message and access the information. If the private key used to decrypt is lost or destroyed, the information that has been encrypted cannot be decrypted. The subscriber, responsible and third parties in good faith, recognize and accept the risks of using digital certificates to perform encryption processes and in particular the use of keys to encrypt data messages is the sole responsibility of the subscriber or responsible in the event of a loss or destruction of the key.

The ECD GSE assumes no responsibility for the use of digital certificates for encryption processes.

Each certification policy is identified by a unique object identifier (OID) that also includes the version number.

Any other use that is not described in this DPC will be considered a violation of this DPC and will constitute a cause for immediate revocation of the digital certification service and termination of the contract with the subscriber and/or responsible, without prejudice to the criminal or civil actions that may be taken by the ECD GSE.

1.1.4.2. List of application types where certificate issuance is prohibited or non-functional.

Certificates may only be used for the uses for which they have been issued and specified in this DPC and specifically in the Certificate Policies for Digital Certificates.

Uses that are not defined in this DPC and therefore for legal purposes, ECD GSE is exempt from any liability for the use of certificates in operations that are outside the limits and conditions established for the use of Digital Certificates under this DPC, including but not limited to the following prohibited uses:

- Unlawful purposes or operations under any legal regime in the world.
- Any practice contrary to Colombian law.
- Any practice contrary to international conventions signed by the Colombian state.
- Any practice contrary to supranational norms.
- Any practice contrary to good customs and commercial practices.
- Any use in systems whose failure may cause:
  - Death
  - Injury to persons
  - Damage to the environment
- As a control system for high-risk activities such as:
  - Maritime navigation systems
  - Land transport navigation systems
  - Air navigation systems
  - Air traffic control systems

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 **July 06,2023**

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

- Weapon control systems

1.1.5. POLICY ADMINISTRATION

1.1.5.1. Document management organization.

The DPC and certification policies are the responsibility and property of GSE and therefore act as its administrator.

1.1.5.2. Responsible for ECD:

Name: Álvaro de Borja Carreras Amorós
Position: Legal Representative
Address: Calle 77 # 7-44 Office 701
Address: Bogotá D.C., Colombia.
Phone: +57 (1) 4050082
Email: info@gse.com.co

1.1.5.3. Responsible for PC and DPC Upgrade.

Area in charge: Operations Manager
Address: Calle 77 # 7-44 Office 701
Address: Bogotá D.C., Colombia.
Phone: +57 (1) 4050082
Email: info@gse.com.co

1.1.5.4. DPC approval procedures.

The Management Committee is the internal GSE body responsible for reviewing, approving and authorising the publication of the CPD on the website http://www.gse.com.co

1.1.6. DEFINITIONS AND ACRONYMS

1.1.6.1. Definitions

The following terms are commonly used and required for the understanding of this DPC:

Certification Authority (CA): Certification Authority, root entity and provider of public key infrastructure certification services.

Registration Authority (RA): It is the entity in charge of certifying the validity of the information provided by the applicant of a digital certificate, by verifying his identity and his registration.

Time Stamping Authority (TSA): Certification body providing chronological stamping services

Reliable data archiving: It is the service that GSE offers to its customers through a technological platform. Essentially, it consists of a secure, 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 signed electronically by a certification service provider that links signature verification data to a signatory and confirms their identity. This is the definition of Law 527/1999 which in this document extends to cases where the linking of signature verification data is done 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 Identification Number (PIN): Sequence of characters that allow access to the digital certificate.

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

Certified email: Service that allows to ensure the sending, receipt and verification of electronic communications, ensuring at all times the characteristics of fidelity, authorship, traceability and non-repudiation of the same.

Declaration of Certification Practice (DPC): In English "Certification Practice Statement" (CPS): manifestation of the certification entity on the policies and procedures it applies for the provision of its 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 **July 06,*2023***

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

Chronological stamping: According to numeral 7 of Article 3 of Decree 333 of 2014, it is defined as: Data message with a specific time or period of time, which allows to establish with a proof that these data existed at a time or period of time and that they did not undergo any modification from the moment the stamping was carried out.

Certification Entity: It is that legal entity, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, empowered by the Colombian government (National Accreditation Body in Colombia) to issue certificates in relation to the digital signatures of customers who acquire them, offer or facilitate the registration and chronological stamping services of the transmission and reception of data messages, as well as fulfill other functions related to communications based on digital signatures.

Open Certification Entity: It is a Certification Entity that offers services of the certification entities, such that:

a. Its use is not limited to the exchange of messages between the entity and the subscriber, or

b. They get paid for them.

Closed certification entity: Entity that offers services of certification entities 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 in a secure manner using a pair of cryptographic keys (a private one and a public one) that are obtained and shared through a trusted authority.

Initiator: A person who, acting on his or her own behalf, or on whose behalf a data message has been acted, sends or generates a data message.

Trust hierarchy: A set of certification authorities that maintain trust relationships by which a higher-level ECD ensures the reliability of one or more lower-level ECDs.

Certificate Revocation List (CRL): A list of 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 it is encrypted with one and can only be deciphered with the other 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 by the subscriber or responsible for the certificate.

Private key: A numeric value or values used in conjunction with a known mathematical procedure to generate the digital signature of a data message.

Public Key: A numeric value or values used to verify that a digital signature was generated with the private key of the originator.

Cryptographic Hardware Security Module: Abbreviation for "Hardware Security Module", hardware module used to perform cryptographic functions and store keys in secure mode.

Certification Policy (PC): 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 in connection with digital signatures.

Online Certificate Status Protocol (OCSP): A protocol for verifying the status of a digital certificate online.
Repository: information system used to store and retrieve certificates and other information related to them.

Revocation: The 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: Natural or legal person to whom the digital certification services are issued or activated and therefore acts as subscriber or responsible for it

Third party in good faith: Person or entity different from the subscriber and/or responsible 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 Chronological Stamping service, as Chronological Stamping Authority.

1.1.6.2. Acronyms

CA: Certification Authority
CA Sub: Subordinate Certification Authority
CP: Certificate Policy

DPC: Certificate Practice Statement
CRL: Certificate Revocation List
CSP: Certification Service Provider
DNS: Domain Name System.
FIPS 140-2: Federal Information Processing Standard.
The HyperText Transfer Protocol (HTTP) is the protocol used in every Web transaction (WWW). C. HTTP defines the syntax and semantics that web architecture software elements (clients, servers, proxies) use to communicate B. It is a transaction-oriented protocol and follows the request-response method between a client and a server
HTTPS: 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.
HSM: Cryptographic Security Module (Hardware Security Module)
IEC: International Electrotechnical Commission
IETF: Internet Engineering Task Force
IP: Internet Protocol.
ISO: International Organization for Standardization
LDAP: Lightweight Directory Access Protocol.
OCSP: Online Certificate Status Protocol.
OID: 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: Registration Authority
RFC: Request For Comments (Standard issued by the IETF)
URL: Uniform Resource Locator
VA: Validation Authority

1.1.6.3. Standards and standardization bodies.

CEN: Comité Europeo de Normalización
CWA: CEN Workshop Agreement
ETSI: European Telecommunications Standard Inst
FIPS 140-2: Federal Information Processing Standard.
IETF: Internet Engineer Task Force
PKIX: IETF Working Group on PKI
PKCS: Public Key Cryptography Standards

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* July 06,2023**

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

RFC: Request For Comments

1.2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.

1.2.1. PKI Repositories.

- **ECD GSE Root Certificates**
  https://certs2.gse.com.co/CA_ROOT.crt
  https://certs2.gse.com.co/CA_ECROOT.crt
  https://certs2.gse.com.co/CA_FEROOT.crt

- **List of Revoked ECD GSE Root Certificates (CRL)**
  https://crl2.gse.com.co/CA_ROOT.crl
  https://crl2.gse.com.co/CA_ECROOT.crl
  https://crl2.gse.com.co/CA_FEROOT.crl

- **ECD GSE Subordinate Certificates**
  https://certs2.gse.com.co/CA_SUB01.crt
  https://certs2.gse.com.co/CA_ECSUB01.crt
  https://certs2.gse.com.co/CA_FESUB01.crt

- **List of ECD GSE Subordinated Revoked Certificates (CRL)**
  https://crl2.gse.com.co/CA_SUB01.crl
  https://crl2.gse.com.co/CA_ECSUB01.crl
  https://crl2.gse.com.co/CA_FESUB01.crl

- **Online Validation of Digital Certificates**
  https://ocsp2.gse.com.co

Note: Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such as OPENSSL.
This GSE ECD repository does not contain any confidential or private information.

GSE ECD repositories are referenced by URL. Any changes to the URLs will be notified to all entities that may be affected.

The IP addresses corresponding to each URL may be multiple and dynamic, and may be modified without prior notice by ECD GSE.

1.2.2. Publication of certification information.

The List of Revoked Certificates published on the GSE website is digitally signed by the GSE ECD.

The status information of the current digital certificates is available for consultation on the website and with the OCSP protocol.

1.2.3. Time or frequency of publication.

root certificate
The root certificate will be published and remain on the ECD GSE website for as long as digital certification services are being provided.

Subordinate Certificate
The Subordinate's certificate will be published and will remain on the ECD GSE website for as long as digital certification services are being provided.

List of Revoked Certificates (CRL)
ECD GSE will publish on the website the list of certificates revoked at events and with the frequency defined in the *Frequency of issuance section of the CRLs.*

Declaration of Certification Practices (DPC)- Global Certification Authority Root GSE

With the authorization of the Management Committee, the validation by the Audit firm, the issuance of the audit compliance report and finally with the express accreditation of the ONAC, the version finally approved for the provision of the digital certification service will be published and subsequent publications will be subject to the modifications that take place with the approval of the Management Committee. The changes generated in each new version will be reported to ONAC and published on the ECD GSE website together with the new version. The Annual Audit will validate these changes and issue the compliance report.

Online Validation of Digital Certificates
ECD GSE will publish the certificates issued in a repository in X.509 format which can be consulted at https://ocsp2.gse.com.co

Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such as OPENSSL.

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* July 06,2023**

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

1.2.4. Repository access controls.

The consultation of the repositories available on the aforementioned GSE website is freely accessible to the general public. The integrity and availability of the published information is the responsibility of ECD GSE, which has the necessary resources and procedures to restrict access to the repositories for purposes other than consultation.

1.3. IDENTIFICATION AND AUTHENTICATION

1.3.1. Names.

1.3.1.1. Types of certificate names from root to final entity, according to ISO/IEC 9595 (X.500).

The guidance document that ECD GSE uses for the unique identification of subscribers or those responsible for issued certificates is defined in the *Distinguished Name* (DN) structure of ISO/IEC 9595 (X.500).

The certificates issued by ECD GSE contain the distinguished name (*DN*) X.500 of the issuer and the recipient of the certificate in the *issuer name* and *subject name* fields respectively.

1.3.1.1.1. Root certificates of the ECD GSE.

The DN of the ‘issuer name’ of the root certificate has the following fields and fixed values:
C co
O = GSE
OU = PKI
CN = GSE Root Authority
E = info@gse.com.co

The following fields are included in the subject name DN:
C co
O = GSE
OU = PKI
CN = GSE Root Authority
E = info@gse.com.co

1.3.1.1.1.1. Elliptic curve (ECDSA).

The DN of the ‘issuer name’ of the root certificate has the following fields and fixed values:
C co
Capital District
BOGOTA D.C.

O = GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.
OU = GSE CA ROOT R2
SERIALNUMBER = 900204278
CN = GSE ECDSA ROOT
E = info@gse.com.co
STREET = www.gse.com.co

The following fields are included in the subject name DN:
C co
Capital District
BOGOTA D.C.
O = GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.
OU = GSE CA ROOT R2
SERIALNUMBER = 900204278
CN = GSE ECDSA ROOT
E = info@gse.com.co
STREET = www.gse.com.co

1.3.1.1.1.2. Electronic signature

STREET=www.gse.com.co,
E=info@gse.com.co,
CN=GSE ROOT ELECTRONIC SIGNATURE,
SN=900204272,
OU=GSE ELECTRONIC SIGNATURE R1,
O=GESTIÓN DE SEGURIDAD ELECTRONICA S.A,
L=BOGOTA D.C.,
ST= CAPITAL DISTRICT,
C co

1.3.1.1.2. Certificates of Subordinates.

The DN of the 'issuer name' of the certificates of the subordinates of ECD GSE, have the following characteristics:
C co
O = GSE
OU = PKI
CN = GSE Root Authority
E = info@gse.com.co

The following fields are included in the subject name DN:
C co

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* July 06,2023**

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

BOGOTA D.C.
O = GSE
OU = PKI
CN = Subordinated Authority 01 GSE
E = info@gse.com.co

1.3.1.1.2.1. Elliptic curve (ECDSA).

The DN of the ‘issuer name’ of the certificates of the subordinates of ECD GSE, have the following characteristics:
C co
Capital District
BOGOTA D.C.
O = GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.
OU = GSE CA ROOT R2
SERIALNUMBER = 900204278
CN = GSE ECDSA ROOT
E = info@gse.com.co
STREET = www.gse.com.co

The following fields are included in the subject name DN:
C co
Capital District
BOGOTA D.C.
O = GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.
OU = GSE ECDSA R2 SUB1
SERIALNUMBER = 900204278
CN = GSE ECDSA SUBORDINATE
E = info@gse.com.co
STREET = www.gse.com.co

1.3.1.1.2.2. ECD GSE Subscriber Certificates (Matrix Technical Certificate Profile).

The DN of the ‘issuer name’ of the ECD GSE subscriber certificates have the following general characteristics:
C co
BOGOTA D.C.
O = GSE
OU = PKI
CN = Subordinated Authority 01 GSE
E = info@gse.com.co

In the DN of the 'subject name' is determined by ANNEX 1 DPC MATRIX TECHNICAL PROFILE DIGITAL CERTIFICATES

1.3.1.1.2.3. ECD GSE Subscriber Certificates (Matrix Technical Profile of Electronic Signature Certificates).

STREET=www.gse.com.co,
E=info@gse.com.co,
CN=GSE INTERMEDIATE ELECTRONIC SIGNATURE,
SN=900204272,
OU=GSE ELECTRONIC SIGNATURE R1,
O=GESTIÓN DE SEGURIDAD ELECTRONICA S.A,
L=BOGOTA D.C.,
ST= CAPITAL DISTRICT,
C co

1.3.1.2. Significant/ Distinctive Names.

The distinctive names (DNs) of certificates issued by ECD GSE are unique and allow a link to be established between the public key and the subscriber identification number. Because the same person or entity can request multiple certificates on their behalf, these will be differentiated by the use of a unique value in the DN field.

1.3.1.3. Anonymous/pseudo-anonymous identification of subscribers.

Aliases may not be used in the fields of subscriber or responsible since the certificate must contain the real name, acronym or denomination of the applicant for the certificate.

1.3.1.4. Rule of Interpretation of Name Forms.

The rule used to interpret the distinctive names of the issuer and the subscribers or digital certificate holders issuing ECD GSE is the ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

1.3.1.5. Unique Names.

The DN of issued digital certificates is unique to each subscriber.

1.3.1.6. Recognition, authentication and role of recognized brands.

Recognition, authentication and role of ECD GSE recognized trademarks is not required to collect or request evidence in connection with the possession or subscription or liability of trademarks or other distinctive signs prior to the issuance of digital certificates. This policy extends to the use and use of domain names

1.3.2. Initial identity validation.

The ECD GSE reserves the right to decline acceptance of an application or the maintenance of a contract for certification when in its opinion there are reasons that may jeopardize the credibility, commercial value, legal or moral suitability of the ECD, as well as the demonstrated participation of the applicant in illegal activities, or similar issues related to it, will be sufficient reason to reject the application.

The applicant's data: type of identification, identification number, names, surnames, nit (applies to company), company name (applies to company), address data: department, municipality, address and email are reviewed and/or validated together with the application form and the documentation provided for each type of digital certificate.

Identity validation is performed in a manner analogous to face-to-face validation by consuming some(s) of the widely used services in accordance with the requested digital certificate service, for this purpose listed below:

- National Identification Archive - National Civil Registry Office.
- Muisca (Single Model of Income, Service and Automated Control) of the Dian (National Tax and Customs Directorate).
- Compare.
- Single Business and Social Registry (For Legal Entity).

The Single Tax Registration – RUT document will be requested in the updated Dian format that includes QR code.

These services are related in the Procedure for issuing digital certificates.

For digital certification services: (Chronological Stamping, Certified Email, Generation of Certified Electronic Signatures, Archiving and Retention of Transferable Electronic Documents and Data Messages the Confronta identity validation service will not be consumed, but the other validation mechanisms.

The ECD GSE reserves the right to request additional documents, in original or copy; in order to verify the identity of the applicant, it may also exempt the presentation of any document when the identity of the applicant has been sufficiently verified by the ECD GSE through other means.

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 **July 06,2023**

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

In the case of electronic signature certificates, the identity of the subscriber is not validated but a verification of the data recorded at the time of the signature request by sending an OTP code to the registered email.

1.3.2.1. Mechanism to prove possession of the private key.

To guarantee the issuance, possession and control of the private key by the subscriber and/or responsible, it is delivered directly from a secure cryptographic token device in which the subscriber and/or responsible generates the pair of keys and transmits through a secure channel the file in PKCS#10 format where it proves that it is in possession of the private key.

In the event that the certificate is centralized, the generation of the key pair is carried out on an HSM device owned by ECD GSE and the subscriber and/or responsible for a set of credentials (user and password) is delivered for the exclusive use thereof.

Since electronic signature certificates are ephemeral and are used only for the generation of the signature, the credentials for use of these certificates are not delivered to the subscriber and instead are automatically and randomly generated by the platform and discarded once the electronic signature is generated.

By virtue of the provisions of ONAC in CEA 3.0-07, in the event that the pair of keys are generated by the applicant in its own infrastructure, for example, for the use of the certificate on unattended platforms, the applicant must accept and comply with the requirements set forth in the document Annex 1 of Terms and Conditions numeral 6 literal m), if these were generated by software and by devices that comply with Annex F of the CEA, if they were generated by hardware.

1.3.2.2. Requirements for the identification and authentication of the identity of an organization (Legal Entity).

To ensure the identity of a legal person, the RA GSE requires the presentation of the official document proving the legal existence of the same and its legal representative or proxies who will be the only people who can request the digital certificate in the name of said organization. In the event that the request is made by a third party, the proof of delegation of the process must be delivered scanned to the attorney-in-fact. The documents will be received scanned, preserving the legibility for the use of the information.

Notwithstanding the foregoing, ECD GSE reserves the right to issue certificates when in its opinion the credibility, commercial value or legal or moral suitability of the Digital Certification Entity may be put at risk.

1.3.2.3. Requirements for the Identification and Authentication of the Identity of an Individual (Natural Person).

To ensure the identity of a natural person, the RA GSE requires the presentation of the identity document of the scanned applicant and verifies its existence and correspondence against its own or third-party databases, whether official or private. When the service is requested by a minor, his identity will be secured with the authenticated identity document (identity card) and document supporting the link of the applicant and the minor. In the event that the request is made by a third party, the proof of delegation of the process must be delivered scanned to the attorney-in-fact. The documents will be received scanned, preserving the legibility for the use of the information.

Notwithstanding the foregoing, ECD GSE reserves the right to issue certificates when in its opinion the credibility, commercial value or legal or moral suitability of the Digital Certification Entity may be put at risk.

1.3.2.4. Unverified subscriber information.

Under no circumstances shall ECD GSE omit the verification work that leads to the identification of the applicant and that results in the request and requirement of the aforementioned documents for organizations and individuals.

1.3.2.5. Interoperability criteria.

ECD GSE will only issue digital certificates to Subordinated ECDs, where the decision to issue or activate the digital certification service is made by the ECD GSE through the recommendation based on the review and recommendation of the GSE RA.

1.3.3. Identification and Authentication for key renewal.

1.3.3.1. Identification and authentication requirements for routine key generation.

ECD GSE performs in all events the authentication process of the applicant even in those of renewal and based on this it issues the digital certificates. Only those applications digitally signed by the subscriber, the renewal of the digital certificate will be made without going through a new identification and authentication process always guaranteeing documentary validation.

1.3.3.2. Post-revocation identification and authentication requirements.

The process of replenishing a digital signature certificate as a result of revocation for the different reasons defined in this DPC, requires a verification process for that request (Replenishment).

1.3.4. Identification and authentication in revocation requests.

ECD GSE, responds to requests for revocation in accordance with the grounds for revocation specified in the section *Circumstances for the revocation of a certificate of this DPC* and authenticates the identity of the person requesting the revocation of the certificate. In accordance with the provisions of the revocation procedure.

1.4. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFE CYCLE.

1.4.1. Application for a certificate

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 document terms and conditions of the ECD and providing them together with the documentation required to authenticate the information provided. Once the information has been completed and confirmed by the applicant, the application form is sent to the Registration Authority who will be responsible for reviewing the supplied information application and approving it in accordance with compliance with the requirements of the Certification Policies.

The request for a digital certification service must be filed through the electronic channels provided for this purpose by ECD GSE.

Users who request our Digital Certification services accept the terms and conditions of service specified in this DPC.

The applicant provides the necessary documents scanned or in electronic original, preserving the legibility for the use of the information and the procedures established by ECD GSE, for obtaining its digital certificate.

ECD GSE reserves the right to request additional documents to those required, in original or copy; in order to verify the identity of the applicant, it may also exempt from the presentation of any document when the identity of the applicant has been sufficiently verified by ECD GSE through other means or mechanisms available. The documentation provided will be reviewed in accordance with the Criteria and Methods of Evaluation of Applications established by GSE.

The applicant accepts that the ECD GSE has the discretionary right to reject an application for a digital certificate when in its opinion the credibility, commercial value, good name of

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* July 06,*2023

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

GSE, legal or moral suitability of the entire digital certification system may be put at risk, notifying the applicant of non-approval.

For the application for an electronic signature certificate, the Electronic Signature Procedure (PTI-PD-20) has been established.

1.4.1.1. Who can apply for a certificate?

Any natural or legal person legally empowered and duly identified can process the application for the issuance of a digital certificate.

1.4.1.2. Application, registration and liability process.

The GSE RA, having previously complied with the requirements for authentication and verification of the applicant's data, shall approve and digitally sign the certificate of issuance of the digital certificates. All related information will be recorded in the RA GSE system.

1.4.2. Processing of certificate request.

1.4.2.1. Procedure for processing the request/ identification and authentication.

The functions of authentication and verification of the identity of the applicant are carried out by the RA of GSE, in charge of giving the recommendation for the decision on the digital certification based on the review of the application, who checks whether the information provided is authentic and meets the requirements defined for each type of certificate in accordance with this CPD.

The documentation that the GSE RA must review to give the recommendation for decision making for the correct issuance of each type of certificate is defined in the Certificate Policies for Digital Certificates.

1.4.2.2. Criteria for acceptance or rejection of the applicationd.

If, once the identity of the applicant has been verified, the information provided complies with the requirements established by this CPD, the application is approved. If full identification of the identity of the applicant is not possible or there is no full authenticity of the information provided, the application is denied and the certificate is not issued. ECD GSE assumes no responsibility for the consequences that may arise from the non-approval of the issuance of a digital certificate and this is accepted and recognized by the applicant who has been denied the issuance of the respective certificate.

Likewise, ECD GSE reserves the right not to issue certificates despite the fact that the identification of the applicant or the information provided by the latter has been fully

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* July 06,*2023

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

authenticated, when the issuance of a particular certificate for reasons of legal order or commercial convenience, good name or reputation of GSE may endanger the digital certification system.

If after the filing of an application and the process did not approve the review of the application or the applicant did not perform the identity validation, after fifteen (15) days without the novelty being corrected, the RA of the ECD GSE will have the alternative of rejecting the application and the applicant will be notified to file a new application.

For which ECD GSE will notify the applicant of the approval or rejection of the application.

1.4.2.3. Deadline for processing certificate requests

The deadline for processing a request by the GSE RA is one (1) to five (5) business days from the moment the requested documentation and information is received and the applicant has approved the identity validation.

The delivery time of the digital certificate issued on a cryptographic device depends on the place of destination, not to exceed eight (8) business days for delivery.

1.4.3. Issuance of the Certificate.

1.4.3.1. Actions of the ECD GSE during the issuance of certificates.

The final step in the process of issuing digital certificates is the issuance of the certificate by ECD GSE and its safe delivery to the subscriber and/or responsible.

The GSE RA generates the formal documentation of the digital certification, when the decision to grant the digital certificate has been made.

The process of issuing digital certificates securely links the registration information and the generated public key.

1.4.3.2. Notification mechanisms authorized by subscribers.

By email, the subscriber is notified of the issuance of his digital certificate and therefore the subscriber accepts and acknowledges that once he receives the aforementioned email, it will be understood that the certificate has been issued. It will be understood that the email where the issuance of a certificate is notified has been received, when said email enters the information system designated by the applicant, this is in the email address that the subscriber reported in the application form. In the event that the subscriber requests that the issuance of the signature be on a cryptographic device, it will be understood as delivered once the delivery letter and/or the shipping guide is signed to the logistics operator or courier.

The publication of a certificate in the certificate repository constitutes proof and a public notification of its issuance.

1.4.4. Acceptance of the Certificate.

1.4.4.1. Mechanism of acceptance of the certificate by the subscriber.

Confirmation by the subscriber or responsible person is not required as acceptance of the certificate received. It is considered that a certificate is accepted by the subscriber or responsible from the moment he requests its issuance, therefore, if the information contained in the certificate issued does not correspond to the current state of it or was not supplied correctly, it is the responsibility of the subscriber to request its revocation.

1.4.5. For keys and use of certificate.

1.4.5.1. Responsibilities of the Subscriber with regard to the use of the private key.

The subscriber or responsible for the digital certificate and the associated private key, accepts the conditions of use established in this DPC for the sole fact of having requested the issuance of the certificate and may only use them for the uses explicitly mentioned and authorized in this DPC and in accordance with the provisions of the "Key Usage" fields of the certificates. Therefore, certificates issued and the private key must not be used in other activities that are outside the aforementioned uses. Once the validity of the certificate has expired, the subscriber or responsible party is obliged not to continue using the private key associated with it. Based on the above, from now on the subscriber accepts and acknowledges, that in this sense he will be solely responsible for any loss or damage caused to third parties by the use of the private key once the validity of the certificate has expired. ECD GSE assumes no responsibility for unauthorized uses.

1.4.5.2. Responsibilities of the trusted third party related to the use of the subscriber's private key.

The subscriber to whom a certificate has been issued undertakes that each time he makes use of the certificate for third parties must inform them that it is necessary that they consult the status of the certificate in the repository of revoked certificates, as well as in that of issued in order to verify its validity and that it is being applied within its permitted uses established in this DPC.

In this regard, you should:

- Check that the associated certificate does not breach the effective start and end dates.
- Check that the certificate associated with the private key is not revoked.
- Check that the ***fingerprint*** of the certificate of the root ECD and that of the certificate of the subordinate of ECD GSE coincide with that published by GSE on its website.

1.4.5.2.1. Root ECD certificate fingerprint:

SHA 256
Fingerprint=7C:1C:A5:51:31:2E:A0:2E:F1:D6:3A:4F:56:54:D0:3F:D0:4F:6F:32:7C:8E:2E:03:52:1A:22:69:7A:B7:98:43

SHA256
Fingerprint=9F:BF:5F:E1:A3:34:49:35:44:6A:95:EB:45:D3:DD:F3:49:36:18:41:21:71:71:65:F0:B8:42:11:85:0D:E6:F3

SHA256
Fingerprint=3F:CE:D4:24:F2:D5:70:53:6E:DA:65:2D:D7:C9:D3:6D:58:5A:10:ED:BB:58:85:1C:F8:2C:91:12:03:41:5C:0C

1.4.5.2.2. Fingerprint of the certificate of the subordinate of ECD GSE Subordinate Certificate 001:

SHA-256
Fingerprint=70:99:01:C9:1D:8F:B2:92:DB:81:B7:04:8B:0B:06:E5:A2:AA:14:59:7D:CA:C4:DF:BE:6B:DD:90:49:D8:E2:01

SHA256
Fingerprint=8C:8B:17:8E:AA:D2:E9:AD:BF:2D:28:1E:91:53:3F:96:BF:7C:BE:1B:2D:8A:89:A0:D8:AE:FD:19:40:D0:35:88

SHA256
Fingerprint=6C:91:FA:BA:42:7F:0D:93:CB:B4:EB:09:4A:3F:5E:4A:64:D8:F2:5F:B8:7B:AA:75:D8:26:8D:BF:79:8E:CC:95

1.4.6. Renewal of Certificate without Change of Keys.

ECD GSE, does not meet requirements for renewal of a certificate without changing keys.

1.4.6.1. Circumstances for renewal of certificates without change of keys.

It does not apply because certificates are not issued without changing keys.

1.4.6.2. Who can apply for a renewal without changing keys?

It does not apply because certificates are not issued without changing keys.

1.4.6.3. Procedures for the application for renewal of certificates without change of keys.

It does not apply because certificates are not issued without changing keys.

1.4.6.4. Notification to the subscriber or person responsible for issuing a new certificate without changing keys.

It does not apply because certificates are not issued without changing keys.

1.4.6.5. Form in which the renewal of a certificate without change of keys is accepted.

It does not apply because certificates are not issued without changing keys.

1.4.6.6. Publication of the certificate renewed by the ECD without change of keys.

It does not apply because certificates are not issued without changing keys.

1.4.6.7. Notification of the issuance of a certificate renewed by the ECD to other entities.

It does not apply because certificates are not issued without changing keys.

1.4.7. Renewal of Certificate with Change of Keys.

For ECD GSE, a requirement to renew a certificate with a change of keys is a normal requirement to request a digital certificate as if it were a new one and therefore implies the change of keys and this is recognized and accepted by the applicant.

1.4.7.1. Circumstances for renewal of a certificate.

A digital certificate may be renewed at the request of the subscriber or responsible for upcoming loss of validity or revocation in accordance with the causes mentioned in this DPC or when required by the subscriber.

1.4.7.2. Who can apply for a renewal of a certificate?

For certificates of natural persons, the subscriber may request renewal of the certificate. For legal persons, the renewal of the digital certificate can be requested by the legal representative, alternates or responsible parties.

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 **July 06,*2023***

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

1.4.7.3. Procedure for renewal of a digital certificate.

The procedure for renewing digital certificates is the same as the procedure for applying for a new certificate. The subscriber must access the GSE product and service application web portal and initiate the certificate renewal application process in the same way as they did when they first applied for the certificate. Your information will again be validated in order to update data if required.

1.4.7.4. Notification of renewal of the certificate to the subscriber.

By email, the subscriber is notified of the issuance of his digital certificate and therefore the subscriber accepts and acknowledges that once he receives the aforementioned email, it will be understood that the certificate has been issued. It will be understood that the email where the issuance of a certificate is notified has been received, when said email enters the information system designated by the applicant, this is in the email address that the subscriber reported in the application form. In the event that the subscriber requests that the issuance of the signature be on a cryptographic device, it will be understood as delivered once the delivery letter is signed to the logistics operator.

1.4.7.5. Acceptance of certificate renewal.

No confirmation is required from the subscriber or responsible party as acceptance of the certificate renewal received. It is considered that a renewed certificate is accepted by the subscriber or responsible from the moment it requests its issuance, therefore, if the information contained in the certificate issued does not correspond to the current status of the same or was not supplied correctly, its revocation must be requested by the applicant or responsible and the latter accepts it.

1.4.7.6. Publication of the certificate

It does not apply because ECD GSE does not publish the certificates.

1.4.7.7. Notification of issuance of certificates to other entities

There are no external entities to which the issuance of a renewed certificate is required to be notified.

1.4.8. Modification of Certificate.

The digital certificates issued by ECD GSE cannot be modified, i.e. they do not apply amendments. Consequently, the subscriber must request the issuance of a new digital certificate. In this event a new certificate will be issued to the subscriber; the cost of this modification will be borne entirely by the subscriber according to the rates reported by ECD GSE or according to the conditions defined at the contractual level.

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* July 06,*2023

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

1.4.8.1. Circumstances for modifying a certificate.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.4.8.2. Who can request an amendment?

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.4.8.3. Procedures for the application for modification of a certificate.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.4.8.4. Notification to the subscriber or responsible for issuing a new certificate.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.4.8.5. Form in which the modification of a certificate is accepted.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.4.8.6. Publication of the certificate as amended by the ECD.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.4.8.7. Notification of the issuance of a certificate by the ECD to other entities

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.4.9. Certificate Revocation/Suspension

1.4.9.1. Circumstances under which a certificate may be revoked.

The subscriber or responsible person may voluntarily request the revocation of his digital certificate at any time as described in article 37 of Law 527 of 1999, but is obliged to request the revocation of his digital certificate under the following situations:

a. For loss or deactivation of the private key or digital certificate.
b. The private key has been exposed or is in danger of being misused.
c. Changes in the circumstances under which ECD GSE authorised the issuance of the digital certificate.
d. If during the period of validity part or all of the information contained in the digital certificate loses relevance or validity.

If the subscriber or responsible person does not request the revocation of the certificate in the event of the above situations, he will be responsible for the losses or damages incurred by third parties in good faith exempt from fault who relied on the content of the certificate.

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* July 06,*2023

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

The subscriber or responsible party acknowledges and accepts that the certificates must be revoked when GSE knows or has indications or confirmation of the occurrence of any of the following circumstances:

a. At the request of the subscriber, responsible or a third party on their behalf and representation.
b. By death of the subscriber or responsible.
c. For confirmation or evidence that any information or fact contained in the digital certificate is false.
d. The private key of the certification body or its security system has been compromised in a material way that affects the reliability of the certificate.
e. By judicial order or competent administrative entity.
f. For compromise of security in any reason, mode, situation or circumstance.
g. Due to supervening incapacity of the subscriber or responsible party.
h. By liquidation of the represented legal person that appears on the digital certificate.
i. Due to the occurrence of new facts that cause the original data to not correspond to reality.
j. For loss or deactivation of the cryptographic device that has been delivered by ECD GSE.
k. For the termination of the subscription contract, in accordance with the grounds established in the contract.
l. For any reason that reasonably leads to believe that the certification service has been compromised to the extent that the reliability of the digital certificate is called into question.
m. For the improper handling by the subscriber of the digital certificate.
n. For the breach of the subscriber or the legal entity it represents or to which it is linked through the terms and conditions document or responsible for digital certificates of the ECD GSE.
o. Knowledge of events that modify the initial status of the data provided, among others: termination of the Legal Representation, termination of the employment relationship, liquidation or termination of legal status, termination of public office or change to a different one.
p. At any time that falsehood is evidenced in the data provided by the applicant, subscriber or responsible.
q. For non-compliance by the ECD GSE, the subscriber or responsible for the obligations established in the DPC.
r. For non-payment of the securities for the certification services, agreed between the applicant and ECD GSE.

However, the above causes, ECD GSE, may also revoke certificates when in its opinion the credibility, reliability, commercial value, good name of the ECD GSE, legal or moral suitability of the entire certification system may be put at risk.

1.4.9.2. Who can request the revocation of a certificate

The subscriber or responsible party, a bona fide third party or any interested person when it has demonstrable evidence of knowledge of facts and grounds for revocation mentioned in the section ***Circumstances for the revocation of a certificate*** of this DPC and that compromise the private key.

A bona fide third party or any interested person who has demonstrable evidence that a digital certificate has been used for purposes other than those set forth in the ***Appropriate Uses of Certificate*** section of this DPC.

Any interested person who has demonstrable proof that the certificate is not in the possession of the subscriber or responsible.

The CA IT team as the maximum control body that is assigned the management of the security of the technological infrastructure of ECD GSE, is able to request the revocation of a certificate if it had the knowledge or suspicion of the compromise of the private key of the subscriber, responsible or any other fact according to the circumstances for the revocation of a certificate.

1.4.9.3. Procedure for requesting revocation of a certificate.

Interested persons will have the opportunity to request the revocation of a digital certificate whose causes are specified in this DPC may do so under the following procedures:

- In the offices of GSE.
  During business hours, written requests for revocation of digital certificates signed by subscribers and/or those responsible for providing the original identification document are received.

- Online revocation request:
  The subscriber and/or responsible person, may carry out the process of revocation of the digital certificate through the web portal of GSE S.A., https://gse.com.co/consultas-en-linea/ - Request its revocation, when filing the request the current digital certificates will be displayed, the certificate to be revoked must be selected and your registered email, you will receive a notification with the security code to complete the filing of the online revocation request, the subscriber and/or responsible person must select the reason for the revocation, enter the

security code, accept the Terms and Conditions and revoke your digital certificate; once the request ends, the selected certificate will be automatically revoked and the confirmation of revocation will be sent to the registered email. Another means arranged to carry out the revocation of the digital certificate by the subscriber and/or responsible through the tool from where the request for the issuance of the digital certificate was filed.

- Email Revocation Service
  By means of our email revocations@gse.co m.co, subscribers and/or managers can request the revocation of digital certificates according to the grounds for revocation mentioned in the section Circumstances for the revocation of a certificate of this DPC, sending a digitally signed revocation request letter or email with the subscriber's data and grounds for revocation.

  Note: The ECD – GSE makes available a guide template to make the revocation request letter which is available on the website https://gse.com.co/guias-y-manuales, option Revocations and root and subordinate certificates

  The ECD through the IT area and the personnel designated to carry out the certification activities in accordance with the digital certificate revocation procedure will perform the verification of the revocation request.

1.4.9.4. Grace period to request revocation of a certificate.

After validating the authenticity of a request for revocation, ECD GSE will proceed immediately with the revocation requested, within the office hours of the latter. Consequently, there is no grace period that allows the applicant to cancel the application. If it was an erroneous request, the subscriber or responsible person must request a new certificate, since the revoked certificate lost its validity immediately the revocation request was validated and ECD GSE will not be able to reactivate it.

The procedure used by ECD GSE to verify the authenticity of a revocation request made by a specific person is to verify the request in accordance with the previous section.

Once the revocation of the certificate has been requested, if it is evidenced that said certificate is used linked to the private key, the subscriber or responsible party relieves ECD GSE of all legal responsibility, since it acknowledges and accepts that the control, custody and confidentiality of the private key is the sole responsibility of the latter.

1.4.9.5. Time within which the ECD must process the revocation request.

The request for revocation of a digital certificate must be addressed with the utmost urgency, without its revocation taking more than three (3) business days once the request is reviewed.

Once the formalities foreseen for the revocation have been completed and if for any reason, the revocation of a certificate is not made effective in the terms established by this DPC, ECD GSE as a certification service provider will be liable for the damages caused to subscribers or third parties in good faith derived from errors and omissions, in bad faith of the administrators, legal representatives or employees of ECD GSE in the development of the activities for which it has authorization and for this it has civil liability insurance in accordance with *Article 9°. Guarantees, of Decree 333 of 2014.* ECD GSE does not assume any other commitment or provide any other guarantee, nor does it assume any other responsibility before subscriber or certificate holders or trusted third parties except as established by the provisions of this DPC.

1.4.9.6. Validation mechanisms by the third party in good faith.

It is the responsibility of the subscriber or person responsible for a digital certificate and he/she accepts and acknowledges this, informing third parties in good faith of the need to check the validity of the digital certificates on which he/she is using at any given time. The subscriber or responsible party shall also inform the third party in good faith that, in order to carry out such consultation, it has the list of certificates revoked CRL, published periodically by ECD GSE.

1.4.9.7. Frequency of emission of CRLs.

The GSE ECD will generate and publish a new CRL every twenty-four (24) hours in its repository with an online consultation availability of 7x24x365, 99.8% uptime per year.

1.4.9.8. Maximum latency of CRLs.

The time between generation and publication of the CRL is minimal because publication is automatic.

1.4.9.9. Availability of online status check/ revocation.

ECD GSE will publish both the CRL and the status of the revoked certificates in repositories of free access and easy consultation, with availability 7X24 during all days of the year. ECD GSE offers an online consultation service based on the OCSP protocol at https://ocsp2.gse.com.co.

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* July 06,*2023

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

Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such as OPENSSL.

1.4.9.10. Online revocation verification requirements.

To obtain information on the revocation status of a certificate at any given time, you can consult online at https://ocsp2.gse.com.co for which you must have software that is capable of operating with the RFC6960 protocol. Most browsers offer this service.

Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such as OPENSSL.

1.4.9.11. Notice of revocation of a certificate.

Within 24 hours of the revocation of a certificate, ECD GSE informs the subscriber or responsible, by email, the revocation of his digital certificate and therefore the applicant accepts and acknowledges that once he receives the aforementioned email it will be understood that his request was met. It will be understood that the email has been received where the revocation of a certificate is notified when said mail enters the information system designated by the applicant, that is, in the email address that appears in the application form.

The publication of a revoked certificate in the CRL constitutes proof and a public notification of its revocation.

1.4.9.12. Other available forms of disclosure of revocation information.

ECD GSE will maintain a historical file of up to three (3) years of the CRLs generated and that will be available to subscribers by written request addressed to ECD GSE.

1.4.9.13. Special requirements for renewal of compromised keys.

If the revocation of a digital certificate was requested due to compromise (loss, destruction, theft, disclosure) of the private key, the subscriber may request a new digital certificate for a period equal to or longer than that initially requested by submitting a renewal request in relation to the compromised digital certificate. The responsibility for the custody of the key is the subscriber or responsible party and the latter accepts and acknowledges it, therefore, it is he who assumes the cost of the renewal in accordance with the current rates set for the renewal of digital certificates.

1.4.9.14. Circumstances for suspension

ECD GSE does not have the digital certificate suspension service, only revocation.

1.4.9.14.1. Who Can Request Suspension

It does not apply because ECD GSE does not have the digital certificate suspension service, only revocation.

1.4.9.14.2. Suspension request procedure

It does not apply because ECD GSE does not have the digital certificate suspension service, only revocation.

1.4.9.14.3. Limits of the suspension period

It does not apply because ECD GSE does not have the digital certificate suspension service, only revocation.

1.4.10. Certificate State Services.

1.4.10.1. CRL Profile.

CRLs issued by ECD GSE comply with RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2” and contain the following basic elements:

1.4.10.1.1. Version number

The CRLsissued by ECD GSE comply with the current X.509 standard.

1.4.10.1.2. CRL and CRL extensions.

Information on the reason for revocation of a certificate will be included in the CRL, using the extensions of the CRL and more specifically in the reasonCode field.

1.4.10.2. Availability CRL.

As indicated in numeral 6.12.9 Online revocation/availability of status verification.

1.4.10.3. OCSP profile.

The OCSP service complies with the provisions of RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

1.4.10.3.1. Version number

It complies with OCSP Version 1 of RFC6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

1.4.10.3.2. OCSP Extensions.

Not applicable

1.4.10.4. Service availability OCSP.

As indicated in numeral 6.12.9 Online revocation/availability of status verification.

1.4.10.4.1. Operational characteristics.

To consult the status of certificates issued by ECD GSE, an online consultation service based on the OCSP protocol is available at https://ocsp2.gse.com.co. The subscriber or responsible for sending a request for consultation on the status of the certificate through the OCSP protocol, which, once consulted the database, is served by a response via HTTP or query via CRL.

1.4.10.4.2. Optional features

To obtain the information of the certificate status at any given time, the online consultation can be made at the address https://ocsp2.gse.com.co, for which you must have a software that is capable of operating with the OCSP protocol. Most browsers offer this service or query the CRL published on the portal https://crl2.gse.com.co.

Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such as OPENSSL.

1.4.11. End of subscription:

ECD GSE terminates the validity of a digital certificate issued in the following circumstances:

- Loss of validity due to revocation of the digital certificate.
- Expiration of the period for which a subscriber contracted the validity of the certificate.

1.4.12. Key Custody and Recovery.

1.4.12.1. Storage of the subscriber's private key.

The subscriber's private key can only be stored on a hardware cryptographic device (token or HSM). The cryptographic devices in hardware used by ECD GSE comply with the certifications as a cryptographic chip: security level CC EAL5+ PP 9806, BSI-PP-002-2001, FIPS 140-2 LEVEL 3 and the OS certifications of the cryptographic chip: security level CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3) – BSI -DSZ-CC-0422-2008 and support the standards PKCS#11, Microsoft CAPI, PC/SC, X.509 current certified storage, SSL v3, IPsec/IKE.

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 **July 06,*2023***

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

The ECD GSE publishes in the Digital Certificate Policies for Digital Certificates the characteristics of the cryptographic devices it offers to subscribers who request it for the creation and storage of their private keys.

1.4.12.1.1. Storage of the private key to a person in charge.

The subscriber's private key can only be stored on a hardware cryptographic device (token or HSM).

The cryptographic device in hardware used by ECD GSE is a cryptographic card or USB token that meets the minimum requirements of current regulations and the guarantees of the European Common Criteria certification as a "secure signature creation device".

These secure cryptographic signature creation devices comply with the certifications as cryptographic chip: CC EAL5+ PP 9806 security level, BSI-PP-002-2001, FIPS 140-2 LEVEL 3 and cryptographic chip OS certifications: CC EAL4+ BSI-PP-0006-2002 security level (CWA 14169 SSCD Type-3) – BSI -DSZ-CC-0422-2008 and support the standards PKCS#11, Microsoft CAPI, PC/SC, X.509 in force, SSL v3, IPsec/IKE.

The ECD GSE publishes in the Digital Certificate policies for Digital Certificates the characteristics of the cryptographic devices it offers to subscribers who request it for the creation and storage of their private keys.

1.4.12.2. Key Custody and Recovery Policies.

The generation of the private key is stored on a secure device (hardware), from which it cannot be exported. Consequently, retrieval of the subscriber's private key is not possible. The responsibility for the custody of the private key lies with the subscriber and the latter accepts and acknowledges it.

1.4.12.3. Session Key Custody and Recovery Policies.

The retrieval of the subscriber's session key or pin is not possible since the sole responsible for assigning it and the latter declares and accepts it. The responsibility for the custody of the session key or pin is the subscriber who agrees not to keep digital records, written or in any other format and who is obliged to memorize it, so its forgetting requires the request for revocation of the certificate and the request for a new one on behalf of the subscriber.

1.5. FACILITIES, ADMINISTRATION AND OPERATIONAL CONTROLS.

1.5.1. PHYSICAL SECURITY CONTROLS

1.5.1.1. Physical location of the ECD.

ECD GSE has security measures for access control to the building where its infrastructure is located, the digital certification services regulated and provided through this DPC are carried out through a service provider. Only access to the rack that houses the servers through which the communication services of the ECD GSE of previously identified and authorized people who carry the visitor card in a visible place is allowed.

The GSE ECD Technology Infrastructure Provider ensures that PKI servers are in continuous operation virtually in the Amazon cloud.

This provider has procedures to carry out the operations of administration of the communications infrastructure of the ECD GSE and to which only authorized personnel have access.

The restricted area of the communications center meets the following requirements:

a. Only authorized persons are admitted.
b. Critical communication equipment is properly protected in racks.
c. It has no windows to the outside of the building.
d. It is monitored through a 24-hour closed-circuit television, with cameras both inside and outside the computer center.
e. It has physical access control.
f. Fire protection and prevention systems: smoke detectors, fire extinguishing system.
g. It has personnel trained to act in the face of catastrophic events.
h. It has a physical intrusion detection system.
i. The wiring is properly protected against damage, attempts to sabotage or interception by means of gutters.

1.5.1.2. access control mechanisms

There are several levels of security that restrict access to the communications infrastructure through which ECD GSE provides its services and each of them have physical access control systems. The facilities have a closed-circuit television service and surveillance personnel. There are restricted areas within the facilities that due to the type of communications equipment considered critical and sensitive operations that are managed have access allowed only to certain people.

1.5.1.3. Energy and air conditioning.

The communications center has an air conditioning system and has an adequate supply of electricity with protection against voltage drops and other electrical fluctuations that could eventually significantly affect the equipment and cause serious damage. In addition, there is a backup system that guarantees that there is no interruption in the service with sufficient autonomy to guarantee continuity in the service. In the event of a failure in the backup system, there is sufficient time to perform a controlled shutdown.

1.5.1.4. Water exposure.

The data centers where the PKI services are housed have insulation from possible water sources and have flood detection sensors connected to the general alarm system.

1.5.1.5. Prevention and protection against fire.

The communications centre has a fire detection system and a fire suppression system. There is a wiring system that protects the internal networks.

1.5.1.6. Backup system.

There are procedures for taking backups, restoring and testing databases for accredited services.

Missionary servers are located in cloud environments, however, on-premises servers are backed up and stored on a local NAS server with their respective contingency.

1.5.1.7. Disposal of materials.

Any paper document that contains sensitive information of the entity and that has fulfilled its useful life must be physically destroyed to ensure the impossibility of retrieval of information. If the document or information is stored on a magnetic medium, the device must be formatted, permanently deleted or physically destroyed in extreme cases such as damage to storage devices or non-reusable devices, always ensuring that it is not possible to recover the information by any means known or not known at the moment.

1.5.1.8. Off-site backup.

ECD GSE will maintain a backup copy of the databases on Amazon that will be taken to replication should it be required for restoration.

1.5.1.9. Physical controls of the technological infrastructure through which ECD GSE provides its services

The technological infrastructure services through which ECD GSE provides its services.

1.5.2. Procedural Controls

1.5.2.1. ECD Trust Roles.

The RA has defined the following roles, which may not be performed by the same person within the area:

- **RA Agents:** Persons responsible for daily operations such as: review and approval of applications addressing all activities related to digital certification services provided by the ECD GSE through the RA, the roles and responsibilities of the RA agents are defined in accordance with the Profiles and Functions of the ECD GSE.

- **RA Administrator:** The person responsible for managing and configuring the RA.

- **RA Auditor:** A trained and impartial person in charge of evaluating compliance with the requirements of the RA, auditing the information systems of the RA clarifying that their role is different from that of the internal auditor of the management systems.

1.5.2.2. Number of people required in each role.

One person is required for each of the above roles. The ECD ensures at least the collaboration of two people to perform the tasks that affect the cryptographic key management of the ECD itself.

1.5.2.3. Identification and authentication of each role.

RA Agents and RA Administrator are authenticated by digital certificates issued by ECD GSE.

Each person only controls the assets needed for their role, thus ensuring that no person accesses unallocated resources.

Access to resources is done depending on the asset through login/ password, digital certificates.

1.5.2.4. Roles that require segregation of duties.

The role of RA Administrator, RA Agents and RA Auditor are independent.

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 **July 06,2023**

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

1.5.3. Personnel controls.

1.5.3.1. Requirements on qualification, experience and professional knowledge.

A staff selection process has been defined that is based on the profile of each of the positions involved in the process of issuing digital certificates. The candidate for a position must have the training, experience, knowledge and skills defined in the Profile and Position Functions document.

1.5.3.2. Background check procedure.

Candidates for positions in the certification cycle must present their current background certificate, as established in the internal human talent processes of the ECD GSE.

1.5.3.3. Training requirements.

The training requirements for each of the positions mentioned are found in the Position Profile and Functions that is disclosed to the person selected to hold the position as part of their induction. The highlights that are part of the training are:

- Knowledge of the Declaration of Certification Practices.
- Knowledge of current regulations and related to open certification entities and the services they provide.
- Knowledge of the Security Policies and acceptance of a confidentiality agreement on the information handled under the position.
- Knowledge of the operation of software and hardware for each specific role.
- Knowledge of security procedures for each specific role.
- Knowledge of the operation and administration procedures for each specific role.

1.5.3.4. Training update requirements.

The annual training program includes an update on Information Security for the members of the Digital Certificate Issuance Cycle.

1.5.3.5. Frequency and sequence of rotation of tasks.

There is no rotation of tasks in the positions mentioned.

1.5.3.6. Penalties for unauthorized actions.

It is classified as a serious offense to carry out unauthorized actions and people will be sanctioned in accordance with the disciplinary process.

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 **July 06,2023**

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

1.5.3.7. Controls for third party contracting.

Among the contracting requirements of third parties is knowledge of the Security Policies and a confidentiality clause on the information that is provided or known for reasons of the contractual link with GSE.

1.5.3.8. Documentation provided to staff during induction and reinduction.

The documentation mentioned in the paragraph **Training Requirements** is published for easy reference and is part of the induction of personnel.

1.5.4. Audit Record Procedures.

Security audit procedures are executed internally or by third-party audit vendors.

1.5.4.1. Type of events recorded.

The most sensitive activities of the certification cycle require the control and monitoring of events that may occur during its operation. According to their level of criticality, events are classified into:

- Informational: An action ended successfully
- Brand Type: Start and end of a session
- Warning: Presence of an abnormal event but not a fault
- Error: An operation generated a predictable failure
- Fatal error: An operation generated an unpredictable failure

1.5.4.2. Logs processing frequency.

Audit records are reviewed using manual and/or automatic procedures.

The review of the logs is carried out once a week or when a security alert is detected or there are indications of an unusual operation of the systems.

1.5.4.3. Period of retention of audit records.

The audit records are kept for three (3) years after the last modification of the file, with that it is guaranteed to be able to review the problems presented with those that have been presented in the history. Once the 3 years have elapsed and with the authorization of the GSE Management Committee, you can proceed to destroy them, however, if the records are being used in judicial proceedings, their retention will be indefinitely.

1.5.4.4. Protection of audit records.

Information system audit logs are likewise retained by keeping one copy on-site and one copy off-site.

1.5.4.5. Procedure for backing up audit logs.

Audit log backups are replicated to a centralized log site

1.5.4.6. Audit log collection system (internal or external).

The audit information collection system is based on the automatic records of the applications that support the certification cycle including the application logs, security logs and system logs. Which are stored in CloudWatch and databases for monitoring

1.5.4.7. Notification to the person responsible for the security incident.

In the opinion of the Information Security Officer, the subject will be notified of a security incident detected through the audit logs in order to have a formal answer about what happened.

1.5.4.8. Vulnerability scan.

In addition to periodic logs reviews, ECD GSE carries out sporadic or suspicious activity reviews in accordance with established internal procedures. Likewise, it reviews the results obtained from the Ethical Hacking and the activities described for the correction of findings

1.5.5. FILE OF REGISTERS:

The file registration and event registration is executed by the NOC SOC of GSE.

1.5.5.1. Types of records to be archivedor.

A file of records of the most relevant events on the operations carried out during the process of issuing digital certificates is maintained.

1.5.5.2. Retention period.

The retention period of this type of documentation is 3 years and/or indefinite if there are open court proceedings

1.5.5.3. File protection.

The files generated are kept in custody with strict security measures to preserve their state and integrity.

1.5.5.4. File Backup Procedures s.

Backup copies of the Log Files are made according to established procedures for backup and recovery of backups of the rest of the information systems.

1.5.5.5. Requirements for time stamping of records.

Servers are kept up to date with UTC Time (Coordinated Universal Time). They are synchronized using the Network Time Protocol (NTP). Since in accordance with the provisions of numeral 14 of article 6 of Decree number 4175 of 2011, the National Institute of Metrology IMC, is the official body that maintains, coordinates and disseminates the legal time of the Republic of Colombia, adopted by Decree 2707 of 1982, the synchronization will be carried out with the NTP server of the INM.

1.5.5.6. File collection system (internal or external).

Both external and internal audit information is stored and stored on a site external to the ECD GSE facilities once it has been digitized. Digitized audit files are accessed only by authorized personnel using visualization tools. Amazon maintains the CloudWatch database service.

1.5.5.7. Procedures for obtaining and verifying file information.

The log files are accessed only by authorized personnel through visualization and event management tools for the purpose of verifying their integrity or for audits in the event of security incidents.

1.5.6. Change of Keys.

1.5.6.1. GSE ECD Root Key Change.

The GSE ECD Root key change procedure is the equivalent of generating a new digital certificate. Certificates issued by subordinates with the previous key must be revoked or the infrastructure must be maintained until the expiration of the last issued certificate. If you choose to revoke the certificates and issue new ones, these will have no cost to the subscriber or responsible.

Before the use of the ECD GSE private key expires a change of keys will be made. The previous root CA and its private key will only be used for the signature of the CRL as long as there are active certificates issued by the subordinates of the previous CA. A root CA will be generated with a new private key and a new DN. The public key will be published in the same repository with a new name than the difference from the previous one.

1.5.6.2. Change of keys of the GSE ECD Subordinate.

The key change procedure of a GSE ECD subordinate is the equivalent of generating a new digital certificate. Certificates issued with the previous key of the subordinate must be revoked or the infrastructure must be maintained until the expiration of the last issued certificate. If you choose to revoke the certificates and issue new ones, these will have no cost to the subscriber or responsible.

Before the use of the private key of the subordinate ECD GSE expires a change of keys will be made. The former ECD subordinate and her private key will only be used for the signature of the CRL as long as there are active certificates issued by the former ECD subordinate. A subordinate ECD GSE will be generated with a new private key and a new DN. The public key will be published in the same repository with a new name than the difference from the previous one.

1.5.7. Commitment and Disaster Recovery.

1.5.7.1. Incident Management Procedures.

ECD GSE has established and tested an **Information Security Incident Procedure** for both RA and CA that sets out the actions to take in the event of a vulnerability or security incident. Once the procedures for re-establishing the systems have been satisfactorily implemented, the public will be served.

1.5.7.2. Recovery procedure in case of alteration of technological resources.

Upon suspicion of alteration of hardware, software, or data resources, the operation of the ECD will be stopped until the security of the environment is restored. To avoid a recurrence of the incident, the cause of the disturbance must be identified. In the event of an occurrence of this fact ECD GSE will inform ONAC giving explanation and justification.

1.5.7.3. Recovery procedure against the compromise of the private key of the ECD.

ECD GSE has established and tested a Business Continuity Plan of the CA that defines the actions to follow in case of a vulnerability of the private key of the root of ECD GSE or one of its subordinates. In these cases, the compromised private keys of the ECD GSE and the certificates signed under its hierarchy must be immediately revoked. A new private key must be generated and at the request of the subscribers and/or managers, new certificates must be issued, in addition, this plan will be executed under the following scenarios:

a. When the certification body's security system has been breached.
b. When there are failures in the system of the certification entity that compromise the provision of the service.

c. When the encryption systems lose validity for not offering the level of security contracted by the subscriber.
d. When any other information security event or incident occurs.

In case of ECD commitment:

a) Apply incident containment to prevent recurrence
b) It will inform all Subscribers, Managers, relying Third Parties and other CAs with whom it has agreements or other type of engagement relationship.
c) It will indicate that certificates and revocation status information signed using this key are invalid.
d) Inform ONAC and customers.

1.5.7.4. Capacity to recover in the event of a natural disaster or catastrophe.

ECD GSE in the event of a natural disaster or other type of catastrophe, is able to recover the most critical services of the business, described in the RA and CA Business Continuity Plan document, within forty-eight (48) hours after the occurrence of the event or within the RTO of the process. The restoration of other services such as the issuance of digital certificates will be done within five (5) days after the occurrence of the event or according to the RPO specified in the Business Continuity Plan document.

1.5.8. Cessation of CA or RA.

1.5.8.1. Procedure in case of cessation of CA and RA

In accordance with the provisions of Article 34 of Law 527 of 1999, as amended by Article 163 of Decree Law 019 of 2012 and in accordance with Decree 333 of 2014, open digital certification entities must inform ONAC and the Superintendency of Industry and Commerce of the cessation of activities at least 30 days in advance.

The ECD - GSE will inform all subscribers and/or managers through two notices published in newspapers or media of wide national circulation, with an interval of 15 days, about:

a. The termination of the activity or activities and the precise date of cessation.
b. The legal consequences of termination in respect of accredited services
c. The possibility for a subscriber to obtain the refund equivalent to the value of the remaining effective time on the contracted service.
d. The authorization issued by the Superintendency of Industry and Commerce so that the ECD can cease service, and if applicable, the operator of the CRL responsible for

the publication of the certificates issued by the ECD - GSE until the last of them expires.

ECD GSE will inform the name of the entity that will guarantee the continuity of the service for those who have contracted, directly or through third parties services of ECD GSE, without additional costs, if they do not accept the continuation of the service through the third party, the subscriber and/or responsible may request the revocation and reimbursement equivalent to the value of the remaining validity time of the digital certification service, if they request it within two (2) months following the second publication on the website and notices.

The ECD GSE has a safety plan in case of cessation of activities which includes the guidelines and activities for the execution of this.

1.6. Technical Security Controls

1.6.1. Generation and Installation of Key Pairs.

1.6.1.1. Generation of the key pair of the Root ECD.

The generation of the Root ECD key pair was carried out on the platform service provider's premises with the strictest security measures and under the key generation ceremony protocol established for this type of event and in the presence of a GSE ECD delegate. For the storage of the private key, a FIPS 140-2 level 3 approved cryptographic device was used.

1.6.1.2. Generation of the key pair of the ECD GSE subordinates.

The generation of the key pair of the ECD GSE subordinates was carried out at the premises of the ECD GSE service provider under the key generation ceremony protocol. For the storage of the subordinate private key, a FIPS 140-2 Level 3 approved cryptographic device is used.

1.6.1.3. Generation of the key pair of the subscribers or managers of ECD GSE.

The generation of the key pair of the GSE ECD subscribers is carried out at the premises of the GSE ECD service provider. For the storage of the subscriber's private key, a FIPS 140-2 Level 3 approved cryptographic device is used.

1.6.1.4. Delivery of the private key to the subscribers.

The private key is delivered to the subscriber and/or responsible in his cryptographic device and it is not possible to extract it. There is therefore no private key copy of the subscriber.

1.6.1.4.1. Delivery of the public key to the issuer of the certificate.

The public key is sent to the GSE ECD as part of the request for the digital certificate in PKCS#10 format.

1.6.1.4.2. Delivery of the ECD public key to accepting third parties.

The public key of the Root ECD and the Subordinate ECD is included in your digital certificate.

The certificates of the Root ECD can be consulted by trusted third parties in the repositories listed in section 4.1Repositories, GSE ECD Root Certificates.

The certificates of the Subordinated ECD can be consulted by trusted third parties in the repositories listed in section 4.1 Repositories, Subordinated ECD GSE Certificates.

1.6.1.5. Size of the keys.

For RSA, the following key sizes are defined:

- ECD Root of ECD GSE is 4096 bits.
- Subordinates of ECD GSE is 4096 bits.
- Certificates issued by ECD GSE to end users is 2048 bits.

When trying to derive the private key, from the 2048-bit public key contained in the end-user certificates, the problem lies in finding the prime factors of two large numbers, since there would be 2^{2047} possibilities for each number. It is estimated that decrypting a 2048-bit public key would require processing work on the order of 3 x$^{10-20}$ MIPS-years*.

MIPS-Year: A unit used to measure the processing power of a computer running for one year. It is equivalent to the number of millions of instructions that a computer can process per second for a year.

For ECDSA the following key sizes are defined:

- ECD Root of ECD GSE is 384 bits.
- Subordinates of ECD GSE is 384 bits.
- Certificates issued by ECD GSE to end users is 256 bits.

For elliptic curve a specific and published base point G is chosen for use with the curve E(q) and then a random integer k is chosen as the private key. The corresponding public key would be P=k*G and is disclosed. The discrete algorithm problem says that it is a problem of exponential complexity to obtain k from P. It is estimated that 2.4x10^{26} MIPS-years are required to derive a 256-bit elliptic curve public key.

1.6.1.6. Public key generation parameters.

The public key of the Root ECD is encoded according to RFC 5280 and PKCS#11. The signature algorithm used in the generation of the keys is the RSA or EC.

The public key of ECD GSE subordinates is encoded according to RFC 5280 and PKCS#11. The signature algorithm used in the generation of the keys is the RSA or EC.

The public key of end-user certificates is encoded according to RFC 5280 and PKCS#11. The signature algorithm used in the generation of the keys is the RSA or EC.

1.6.1.7. Permitted uses of the key.

The permitted uses of the key for each type of certificate are established by the Certificate Policies for digital certificates and in the policies defined for each type of certificate issued by ECD GSE.

All digital certificates issued by ECD GSE contain the '*Key Usage'* extension defined by the X.509 v3 standard, which is rated as critical.

KEY USE CERTIFICATE TYPE
Digital Signature Certificate
Certificate of Authentication Non Repudiation

1.6.2. Private Key Protection and Cryptographic Module Engineering Controls.

1.6.2.1. Standards for use of cryptographic modules.

Cryptographic modules used in the creation of keys used by ECD Root Certification Authority ECD GSE meet the requirements established in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher level of security.

1.6.2.2. Multiperson control (n of m) of the private key.

The private keys of the ECD GSE Root and the private keys of the subordinates of ECD GSE are under multi-person control. The method of activation of the private keys is through the initialization of the ECD GSE software by means of a combination of keys held by several people

1.6.2.3. Safekeeping of the ECD private key.

GSE ECD private keys are stored on cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level.

The technical data of the device are as follows:

- **SafeNet Luna SA**

The private key of the digital end-user certificates is under the sole control and custody of the subscriber or responsible. Under no circumstances does ECD GSE keep a copy of the private key of the subscriber or certificate managed by the responsible since it is generated by the same subscriber or responsible and it is not possible to access it by ECD GSE.

1.6.2.4. Backup copy of the private key.

The private keys of the GSE ECD are stored in cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher level of security. (see 8.2.3 Safekeeping of the private key**).**

The backup copies of the private keys of the ECD GSE are stored on external devices cryptographically protected by a dual control and are only recoverable within a device equal to the one they were generated.

1.6.2.5. Private key file.

GSE ECD private keys are stored in cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher level of security. (see 8.2.3 Safekeeping of the private key**).**

They are located in a cryptographic backup box in a place other than the place where the HSMs are located.

1.6.2.6. Transfer of private keys.

GSE ECD private keys are stored on cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level. (See 8.2.3 Custody of the private key).

The process of downloading the private keys is performed according to the procedure of the cryptographic device and they are stored securely protected by cryptographic keys.

1.6.2.7. Private key storage.

The private keys of the GSE ECD are generated and stored in cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher level of security. (See 8.2.3 Custody of the private key).

Cryptographic keys may be loaded onto an equal performance cryptographic device from the backup copies by a process requiring the participation of at least two operators.

1.6.2.8. Method of activation of the private key.

Private keys, from the Root GSE ECD and Subordinate ECDs, are under multi-person control. The method of activation of the private key is by initializing the ECD GSE software by means of a combination of keys held by several operators.

Multi-person control is required for activation of the ECD private key. At least 2 people are required to activate the keys.

1.6.2.9. Method of deactivating the private key.

The deactivation of the private key is done by disabling the software or turning off the ECD server. It is activated again through the use of multi-person control, following the procedures set by the manufacturer of the cryptographic module.

1.6.2.10. Method for destroying the private key.

The method used in case the destruction of the private key is required is by erasing the keys stored in the cryptographic devices as described in the device manufacturer's manual and physically destroying the access cards held by the operators in case it is required.

1.6.2.11. Technical characteristics of the cryptographic modules used.

The cryptographic devices used by ECD GSE comply with the provisions of Annex F: Cryptographic Devices, of the CEA.

1.6.2.12. Evaluation of the cryptographic module.

The cryptographic device is monitored by its own software to foresee possible failures.

1.6.2.13. Evaluation of the encryption system.

ECD GSE welcomes the recommendations for the use of cryptographic algorithms and key lengths that are published by NIST (National Institute of Standards and Technology) and by ONAC, if any circumstance materializes in which the algorithms used for signature and encryption by ECD GSE are compromised at all levels, ECD GSE will immediately

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* July 06,*2023

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

take the measures and recommendations imparted by this entity or by ONAC to maintain the security of the signature during the remainder of its life cycle.

1.6.3. Other Aspects of Key Pair Management.

1.6.3.1. Public key file.

ECD GSE will maintain controls for the archiving of your own public key.

1.6.3.2. Operational periods of the certificates and period of use of the pair of keys.

The period of use of the pair of keys is determined by the following validity of each certificate:

RSA algorithm

The validity period of the RSA digital certificate and the root key pair is thirty (30) years.

The validity period of the RSA digital certificate and the pair of keys of the subordinate is ten (10) years.

ECDSA algorithm:

The validity period of the ECDSA digital certificate and the Root key pair is twenty-five (25) years.

The validity period of the ECDSA digital certificate and the pair of keys of the subordinate is ten (10) years.

1.6.4. Activation Data.

1.6.4.1. Generation and installation of activation data.

For the operation of the GSE ECD, passwords are created for the operators of the cryptographic device and that will serve together with a pin for the activation of the private keys.

The activation data of the private key is divided into passwords guarded by a multi-person system where 4 people share the access code of said cards.

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 **July 06,*2023***

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

1.6.4.2. Protection of activation data.

Knowledge of activation data is personal and non-transferable. Each of the interveners is responsible for their custody and must handle it as confidential information.

1.6.4.3. Other aspects of the activation data.

The activation key is confidential, personal and non-transferable and therefore the security rules for its custody and use must be taken into account.

1.6.4.4. Computer Security Controls.

The equipment used is initially configured with the appropriate safety profiles by the systems personnel, in the following aspects:

- Operating system security settings.
- Application security settings.
- Control of access to devices.
- Closing system vulnerabilities.
- Hardenization of systems according to good practices.
- Network configuration at the security level (Internal Network, Administrative Network, among others)
- Configuration of Users and Permissions.
- Log event settings.
- Backup and recovery plan.
- Antivirus configuration
- Network traffic requirements configured in the firewall.

1.6.4.5. Specific technical safety requirements.

ECD GSE has a technological infrastructure duly monitored and equipped with security elements required to guarantee the availability established in the CEA and trust in the services offered to its subscribers, entities and trusted third parties.

Information related to Information Security is considered confidential and therefore can only be provided to those control entities that require your knowledge.

1.6.4.6. Computer security assessment.

The security of end-user equipment is managed from ECD GSE and is supported with a risk analysis in such a way that the security measures implemented are responses to the probability and impact produced by a group of defined threats that can take advantage of security breaches.

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 **July 06,*2023***

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

Additionally, periodic security tests (ethical hacking) are carried out, so that possible vulnerabilities of the systems are identified and that contribute to the closure of these.

1.6.4.7. Actions in the event of an information security event or incident.

The Information Security Management System implemented by ECD GSE has established an incident management procedure for both the CA and the RA that specifies the actions to be executed, components or resources to be used and how personnel should react in the event of an intentional or accidental event that disables or degrades the resources and digital certification services of ECD GSE.

a. **Detection and reporting of the incident:** Security incidents must be reported through the email seguridad.informacion@gse.com.co, which is managed by the Information Security Officer of the ECD GSE
Incidents may be detected through monitoring systems, intrusion detection systems, system logs, notice by staff or by subscribers and/or managers.
b. **Analysis and evaluation of the incident:** Once the incident is detected, the response procedure is determined and the responsible persons are contacted to evaluate and document the actions to be taken according to the severity of the incident. An investigation is carried out to determine the scope of the incident, that is, to find out how far the attack has gone and the maximum possible information about the incident.
c. **Control of damage caused by an incident:** React quickly to contain the incident and prevent it from spreading by taking measures such as blocking access to the system.
d. **Investigation and evidence collection:** Review audit records to keep track of what happened.
e. **Recovery and counter-incident measures:** Restore the system to its correct functioning and document the procedure and ways to prevent the recurrence of the incident.
f. **Subsequent analysis of the incident to improve the procedure:** Perform an analysis of everything that happened, detect the cause of the incident, correct the cause for the future, analyze the response and correct errors in the response.

1.6.5. Life Cycle Safety Controls.

1.6.5.1. System development controls.

ECD GSE complies with established change control procedures for new software developments and updates.

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* July 06,*2023

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

1.6.5.2. Security management controls.

ECD GSE maintains control over the inventories of the assets used in its certification process. There is a classification of these according to their level of risk.
ECD GSE periodically monitors its technical capacity in order to guarantee an infrastructure with the minimum availability requested in the CEA.

1.6.5.3. Life Cycle Safety Controls.

ECD GSE has the appropriate security controls throughout the life cycle of the systems that have some impact on the security of the issued digital certificates.

1.6.6. Network Security Controls.

ECD GSE has a network infrastructure duly monitored and equipped with security elements required to ensure the availability and trust in the services offered to its subscribers, entities and third parties in good faith.

Information related to Information Security is considered confidential and therefore can only be provided to those control entities that require your knowledge.

1.6.7. Timestamping.

ECD GSE has the chronological stamping service, which is described in the corresponding Certificate Policies for Chronological Stamping Service, published on the portalhttp://www.gse.co m.co.

1.7. CERTIFICATE PROFILES CERTIFICATE PROFILES, CRL AND OCSP.

1.7.1. Certificate Profile.

Certificates comply with the current X.509 standard and for authentication infrastructure it is based on RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Content of the certificates. A certificate issued by ECD GSE, in addition to being digitally signed by ECD GSE, shall contain at least the following:

1. Name, address and address of the subscriber or manager.
2. Identification of the subscriber or responsible named in the certificate.
3. The name, address, and location of the ECD.
4. The public key of the certificate.

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* July 06,*2023

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

5. The methodology for verifying the subscriber's digital signature imposed on the data message.
6. The serial number (unique) of the certificate.
7. Date of issue and expiry of the certificate.

Field	Value or restrictions RSA	Value or restrictions ECDSA
Version	3 (0x2)	3 (0x2)
Serial Number	Unique identifier issued by ECD GSE	Unique identifier issued by ECD GSE
Signature algorithm	SHA256withRSAEncryption	SHA384withECDSA

Issuer	See “Rules for the Interpretation of Various Forms of Name.”
	
	For ECD GSE as issuer it is specified:
	E=info@gse.com.co,
	CN= Subordinated Authority 01 GSE,
	OU=PKI,
	O=GSE,
	L=Bogota D.C.,
	C co
		See “Rules for the Interpretation of Various Forms of Name.”
		For ECD GSE as issuer it is specified:
		STREET=www.gse.com.co,
		E=info@gse.com.co,
		CN=GSE ECDSA SUBORDINATE,
		SN=900204278,
		OU=GSE ECDSA R2 SUB1,
		O=GESTIÓN DE SEGURIDAD ELECTRONICA S.A,
		L=Bogota D.C.,
		S= Capital District,
		C co

Valid from	Specifies the date and time from which the certificate is valid.	Specifies the date and time from which the certificate is valid.
Valid until	Specifies the date and time from which the certificate ceases to be valid.	Specifies the date and time from which the certificate ceases to be valid.
Party	In accordance with the policy of Annex 1 and the *“Rules for the Interpretation of Various Forms of Name”.*	In accordance with the policy of Annex 1 and the *“Rules for the Interpretation of Various Forms of Name”.*
Subject Public Key	Encoded in accordance with RFC 5280. The certificates issued by ECD GSE have a length of 2048 bits and RSA algorithm.	Encoded in accordance with RFC 5280. The certificates issued by ECD GSE have a length of 256 bits and EC algorithm.
Authority Key Identifier	It is used to identify the root certificate in the certification hierarchy. Normally it refers to the “Subject Key Identifier” field of ECD GSE as a digital certification issuing entity.	It is used to identify the root certificate in the certification hierarchy. Normally it refers to the “Subject Key Identifier” field of ECD GSE as a digital certification issuing entity.
Subject Key Identifier	It is used to identify a certificate that contains a certain public key.	It is used to identify a certificate that contains a certain public key.

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* July 06,2023**

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

Field	Value or restrictions RSA	Value or restrictions ECDSA
Certificate Directives	Describes the policies applicable to the certificate, specifies the OID and the URL where the certification policies are available.	Describes the policies applicable to the certificate, specifies the OID and the URL where the certification policies are available.
Using the key	Specifies the permitted uses of the key. It is a CRITICAL FIELD.	Specifies the permitted uses of the key. It is a CRITICAL FIELD.
CRL Distribution Point	It is used to indicate the addresses where the ECD GSE CRL is published. In the Root ECD certificate, this attribute is not specified.	It is used to indicate the addresses where the ECD GSE CRL is published. In the Root ECD certificate, this attribute is not specified.
Access to Authority information	It is used to indicate the addresses where the GSE ECD root certificate is located. In addition, to indicate the address to access the OCSP service. In the GSE ECD root certificate, this attribute is not specified.	It is used to indicate the addresses where the GSE ECD root certificate is located. In addition, to indicate the address to access the OCSP service. In the GSE ECD root certificate, this attribute is not specified.
Subject Alternate Name	It is used to indicate the email address and additionally to indicate the accreditation code assigned by the ONAC. Name RFC822=correo@empresa.com URL= https://gse.com.co/documents/certifications/accreditation/16-ECD-001.pdf	It is used to indicate the email address and additionally to indicate the accreditation code assigned by the ONAC. Name RFC822=correo@empresa.com URL= https://gse.com.co/documents/certifications/accreditation/16-ECD-001.pdf
Extended Key Uses	Other purposes in addition to the use of the key are specified.	Other purposes in addition to the use of the key are specified.
Basic constraints	The PathLenConstraint extension indicates the number of sub-levels that are supported in the certificate path. There is no restriction for ECD GSE, therefore it is zero.	The PathLenConstraint extension indicates the number of sub-levels that are supported in the certificate path. There is no restriction for ECD GSE, therefore it is zero.

1.7.1.1. Version number

Certificates issued by ECD GSE comply with the current X.509 standard.

1.7.1.2. Extensions of the certificate.

Annex 1 of this DPC describes in detail the certificates issued by GSE.

1.7.1.3. Key Usage.

Key usage is a critical extension that indicates the use of the certificate in accordance with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

1.7.1.4. Extension of certificate policy.

The "certificatepolicies" extension of the current X.509 is the object identifier of this DPC according to the object identifier section of the Certification Policy of this DPC. Extension is not considered critical.

1.7.1.5. Alternative name of the subject.

The extension “subjectAltName” is optional and the use of this extension is “Not critical”.

1.7.1.6. Basic restrictions.

For the case of GSE ECD in the “PathLenConstraint” field of the subordinates certificate has a value of 0, to indicate that the GSE ECD does not allow more sub-levels in the route of the certificate. It is a critical field.

1.7.1.7. Extended use of the key.

This extension allows defining other additional purposes of the key. It is considered non-critical. The most common purposes are:

OID	Description	Certificate types
1.3.6.1.5.5.7.3.4	Mail Protection	Digital signature of natural person and Electronic Agent
1.3.6.1.5.5.7.3.8	Time Stamping	Time Stamping
1.3.6.1.5.5.7.3.34	TLS Web Server Authentication	All Certificate Types

1.7.1.8. Object identifiers (OIDS) of algorithms.

The object identifier of the signature algorithm is: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption

The public key algorithm object identifier is: 1.2.840.113549.1.1.1 rsaEncryption
The object identifier of the signature algorithm is:
1.2.840.10045.4.3.3 SHA384WITHECDSA.

The public key algorithm object identifier is: 1.2.840.10045.2.1 id-ecPublicKey

1.7.1.9. Name formats.

In accordance with what is specified in the **Types of names** section of this DPC.

1.7.1.10. Restrictions on Names.

Names must be written in capital letters and without tildes.

The country code is assigned according to the ISO 3166-1 standard “Codes for the representation of the names of countries and their subdivisions. Part 1: Country Codes ”. In the case of Colombia it is “CO”.

1.7.1.11. Object identifier of the Certification Policy.

The object identifier of the Certificate Policy corresponding to each type of certificate is a subclass of the class defined in the numeral **Name of the document and identification** of this DPC, as established in the Certificate Policies for digital certificates.

1.7.1.12. Use of the Policy Constrains extension.

It is not stipulated.

1.7.1.13. Syntax and Semantics of Policy Qualifiers

The policy qualifier is defined in the “Certificate Policies” extension and contains a reference to the URL where the DPC is published.

1.7.1.14. Semantic treatment for the Certificate Policies extension.

It is not stipulated.

1.7.2. CRL Profile.

CRLs issued by ECD GSE comply with RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2” and contain the following basic elements.

1.7.3. OCSP profile.

The OCSP service complies with the provisions of RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

1.8. COMPLIANCE AUDIT AND OTHER EVALUATION.

1.8.1. Frequency or Circumstances of Controls.

Compliance with controls ensuring security in the issuance of digital certificates shall be assessed by means of an annual audit carried out by an external audit firm.

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* July 06,*2023

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

1.8.2. Identity/qualification of the Auditor.

In accordance with Decree 333 of 2014 and specifically in **Article 14. Audits.** Certification entities must comply with the third party audit in the terms provided for in the Specific Accreditation Criteria established by ONAC.

Assurance requirements: Audit firm legally incorporated in Colombia whose corporate purpose includes: systems audit services, information security and PKI public key infrastructure. The competences of the audit group must be demonstrated with respect to the specific accreditation criteria, the requirements of the international standard ISO/IEC 27001 in terms of information security, in relation to the service ISO 9001 or ISO/IEC 20000-1, in case the auditor does not have competence in PKI, must be in the company of a technical expert knowledgeable in the management related to PKI public key infrastructure. The audit staff must have a current professional card in Engineering.

1.8.3. Relationship between the Auditor and the Audited Entity.

The only relationship established between the auditor and the audited entity is that of auditor and auditee. The audit firm exercises its absolute independence in the performance of its audit activities and there is no conflict of interest as the relationship is clearly contractual.

1.8.4. Aspects Covered by Controls.

The aspects covered by the audit control frame the scope accredited by ONAC for the ECD, in accordance with the provisions of the numeral REQUIREMENTS OF THE MANAGEMENT SYSTEM – Third Party Audit of the CEA document established by ONAC the deliverable is the compliance report, it is not allowed with exception or reasonableness.

1.8.5. Actions to Take as a Result of Detection of Deficiencies.

The deficiencies detected during the audit process must be remedied through corrective or improvement actions, procedures and implementation of the controls required to address the findings.

1.8.6. Comunicación de Resultados.

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* July 06,*2023

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

Upon completion of the audit, the audit firm must submit the audit report to ECD GSE and, if required, ECD GSE must establish corrective and improvement actions. The final report must be sent to ONAC.

1.9. OTHER COMMERCIAL AND LEGAL MATTERS.

1.9.1. Fees.

Not applicable

1.9.2. Financial responsibility.

1.9.2.1. Other assets.

ECD GSE has sufficient economic and financial capacity to provide the authorised services and to be responsible for its duties as a certification body. ECD GSE as a certification service provider will be liable for damages caused to subscribers, entities or third parties in good faith derived from errors and omissions, in bad faith of the administrators, legal representatives or employees of ECD GSE in the development of the activities for which it has authorization and for this it has civil liability insurance in accordance with that of Article 9°. Guarantees, of Decree 333 of 2014. ECD GSE does not assume any other commitment or provide any other guarantee, nor does it assume any other responsibility before the subscriber and/or responsible for certificates or trusted third parties except as established by the provisions of this DPC.

1.9.2.2. Insurance or guarantee of coverage for subscribers, managers and third parties in good faith.

Pursuant to Article 9. Guarantees, of Decree 333 of 2014, ECD GSE has acquired an insurance issued by an insurance entity authorized to operate in Colombia, which covers all contractual and non-contractual damages of the subscribers, managers and third parties in good faith exempt from fault derived from errors and omissions, or acts of bad faith of the administrators, legal representatives or employees of ECD GSE in the development of the activities for which it has authorization.

1.9.3. Confidentiality of Commercial Information.

1.9.3.1. Responsibility to protect confidential information.

ECD GSE is committed to protecting all data to which it has access as a result of its activity as an ECD.

All non-public information is considered confidential and therefore of restricted access, except in those cases provided for by law such as courts or competent administrative bodies or imposed by law, confidential information is not disseminated without the express written consent of the subscriber or the entity that has granted it the character of confidentiality.

However, it reserves the right to disclose to employees and consultants, external or internal, the confidential data necessary to carry out its activities as ECD obliging all personnel to sign a confidentiality agreement within the framework of the contractual obligations contracted with ECD GSE.

1.9.3.2. Confidential Information

The following information is considered confidential:

a. Private key of the Certification Authority and/or ECD
b. Subscriber or Entity Private Key
c. Information provided by the subscriber or entity and that is not necessary to validate the trust of the subscriber or entity
d. Information about the applicant, subscriber and/or controller obtained from different sources (e.g., from a claimant or regulators)
e. Transaction registries
f. Audit logs
g. Safety policies
h. Business Continuity Planning
i. All information that is classified as "Confidential" in the documents delivered by ECD GSE

1.9.3.3. Non-confidential information.

All non-confidential information is considered public and therefore freely accessible to third parties:

a. The one contained in this Declaration of Certification Practices and its annexes.
b. The one contained in the repository on the status of the certificates.
c. The list of revoked certificates.
d. All information that is classified as "PUBLIC" in the documents delivered by ECD GSE.

1.9.3.4. Duty to protect confidential information.

ECD GSE maintains security measures to protect all confidential information supplied to ECD GSE directly or through the channels established for this purpose from its receipt to

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* July 06,2023**

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

its storage and custody, where they will rest for 10 years. ECD GSE has an Integrated Management System that includes an Information Security System. This allows us to ensure that the information of our subscribers will not be compromised or disclosed to third parties unless formally requested by a competent authority that requires it.

1.9.4. the privacy of Personal Information.

1.9.4.1. Personal Data Treatment Policy

The ECD GSE has as its Personal Data Processing Policy in accordance with the provisions of Law 1581 of 2012, which can be consulted on our website https://gse.com.co/Politicas in the Personal Data Processing Policy section, as well as the authorization for the processing of personal data.

1.9.4.2. Information treated as private.

The personal information provided by the subscriber or responsible and that is required for the approval of the digital certificate is considered private information.

1.9.4.3. Information not classified as private.

They are those personal data that the rules and the Constitution have expressly determined as public for whose collection and processing the authorization of the owner of the information is not necessary.

1.9.4.4. Responsibility for the protection of personal data.

ECD GSE is responsible and has the appropriate technological resources to help ensure the proper custody and conservation of personal data collected by the channels used by the company, in compliance with Law 527 of 1999 "Article 32. Duties of certification bodies. The certification entities will have, among others, the following duties: Guarantee the protection, confidentiality and due use of the information provided by the subscriber, responsible and entity.

GSE ECD makes use of technological mechanisms such as the active directory where the access control policy is instrumentalized and a centralized repository where the information is protected by a firewall that prevents intrusions within the network for office equipment, and by digital certificates for access to the production servers of the ECD

1.9.4.5. Notification and consent to use personal data.

Personal data may not be communicated to third parties, without the due notification and consent of its owner, in accordance with the data protection law.

1.9.4.6. Disclosure in the context of an administrative or judicial process.

Personal data may be communicated when required by one of the public or administrative entities in the exercise of its legal functions or by judicial order without the due notification and consent of its owner, in accordance with the data protection law.

1.9.4.7. Other Circumstances of Disclosure.

ECD GSE has as its privacy policy what is strictly established in the right to data protection law: "Private information, will be that which for dealing with personal information or not, and that for being in a private area, can only be obtained or offered to third parties authorized by the Subscriber or responsible or by law".

1.9.4.8. Security system to protect information.

Regarding the system that houses the information provided by the subscriber or responsible for the certification service, the following validations are carried out:

a. The infrastructure provider must have the good practices of the following Standards:

i. ISO 27001
ii. ISO 9001

b. Penetration testing and scanning of network vulnerabilities, carried out by a company specialized in Ethical Hacking.

1.9.5. 7. Intellectual Property Rights

In Colombia, copyright protection includes all literary, artistic or scientific works that can be reproduced or disseminated through any means. Consequently, ECD GSE reserves all rights related to intellectual property and prohibits without its express authorization the reproduction, disclosure, public communication and transformation of information, techniques, models, internal policies, processes, procedures or any of the elements contained in this CPD, in accordance with national and international regulations related to intellectual property.

1.9.6. Representations and Warranties.

The ECD GSE will have at all times a liability insurance in accordance with the provisions of decree 333 of 2014 with a coverage of 7500 minimum legal monthly salaries per event.

The ECD GSE will act in the coverage of its responsibilities by itself or through the insurer, satisfying the requirements of certificate applicants, subscribers/managers and third parties who rely on certificates.

The responsibilities of the ECD GSE include those established by this CPD, as well as those that result from application as a result of the Colombian and International Regulations.

ECD GSE will be responsible for the damage caused to the Subscriber, Entity or any person who in good faith trusts in the certificate, provided that there is wilful misconduct or gross negligence, regarding:

- The accuracy of all the information contained in the certificate at the date of its issuance.
- The guarantee that, at the time of delivery of the certificate, works in the possession of the Subscriber, the private key corresponding to the public key given or identified in the certificate.
- Ensuring that the public and private keys work together and complement each other.
- The correspondence between the requested certificate and the delivered certificate.
- Any liability established by current legislation.

1.9.7. Warranty Waivers.

Not Applicable

1.9.8. Limitations of Liability

1.9.8.1. Responsibility for the veracity of Subscriber information.

The Subscriber assumes all risks for damages that may arise from conduct such as providing false information, impersonating third parties, validating documents or incomplete or outdated information.

1.9.8.2. Responsibility for availability of the service.

The Subscriber undertakes to act diligently to minimize the chances of failures or interruptions that may occur within his organization. Failures caused by the inability or insufficiency of the Subscriber's equipment, or by their lack of knowledge regarding the use of the service, will not be in any case attributable to ECD GSE and may not be required on their part to remedy any damage.

1.9.8.3. Responsibility for the functionality of the service in the Subscriber's infrastructure.

The Subscriber shall be solely responsible for the provision and payment of the costs necessary to ensure the compatibility of the service (digital signature certificate), in front of its equipment, including all hardware, software, electrical components and other physical or logical components required to access and use the same, including but not limited to telecommunications services, Internet access and connection, links, browsers, or other programs, equipment and services required to access and use the service.

1.9.8.4. Responsibility for cybercrime.

In the event that the Subscriber is the victim of any of the behaviors classified as a crime, by Law 1273 of 2009 (Computer Crimes Law), in its information systems, in its applications and technological infrastructure, in the execution of electronic transactions or in the access and use of the service, phishing attacks, impersonations of identity, due to negligence in the handling and confidentiality of the digital certificate, he will be solely responsible and will remedy the damages that may arise, provided that it is his obligation to adopt the security measures, policies, cultural campaigns, legal instruments and other mechanisms to safeguard the confidentiality and proper use of his digital certificate.

1.9.8.5. Disclaimers of warranties.

ECD GSE will not be liable in any case when faced with any of these circumstances:

- State of War, natural disasters, terrorism, strikes or any other case of Force Majeure.
- For the use of certificates as long as it exceeds the provisions of current regulations and this DPC and its Annexes.
- For the improper or fraudulent use of certificates or CRLs issued by the Certification Authority.
- For the use of the information contained in the Certificate or in the CRL.
- For the breach of the obligations established for the Subscriber, Entities, Managers or Third Parties that rely on current regulations, this DPC and its Annexes.
- For the damage caused in the period of verification of the causes of revocation /suspension.
- For the content of digitally signed or encrypted messages or documents.
- For the non-recovery of documents encrypted with the public key of the Subscriber or Entity.

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 **July 06,*2023***

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

- Fraud in the documentation submitted by the applicant.

1.9.9. Compensation.

Not applicable

1.9.10. Term; Termination.

1.9.10.1. Commencement of validity of the DPC and PC.

The CPD and PC enter into force from the moment they are published on the ECD GSE website, from that moment the previous version of the document is repealed and the new version replaces the previous version in its entirety.

ECD GSE keeps in the repository the previous versions of the DPC and PC.

1.9.10.2. Effects of termination and commencement of validity of the DPC and PC.

For digital certificates that have been issued under an old version of the DPC or PC, the new version of the DPC or PC applies in everything that does not oppose the declarations of the previous version.

1.9.10.3. Notification and communication

ECD GSE notifies the changes in this declaration of certification practices by publishing on the website the new version once it is authorized by the Management Committee and the respective change control will be recorded therein.

1.9.10.4. Change procedure in the DPC and PC.

1.9.10.4.1. Changes affecting DPC and PC.

Any changes affecting the DPC and PC of the ECD GSE will follow the following procedure:

a. The Management Committee will approve the changes it deems pertinent on the DPC and the PCs.
b. The updated DPC and PC is published on the ECD GSE website once authorized by the Management Committee.

1.9.10.4.2. Circumstances under which the OID must be changed.

In the following cases the ECD GSE will make adjustments to the identification of OID:

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* July 06,*2023

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

a. The authorization of a new certification hierarchy, event in which the OIDS must be defined according to the structure.
b. In the event that the changes of the DPC and PC that affect the acceptability of the digital certification services proceed to make the adjustment of OID.
   This type of modification will be communicated to the users of the certificates corresponding to the PC or DPC.

1.9.11. Individual Notices and Communication with Participants.

1.9.11.1. Obligations of the ECD GSE.

ECD GSE as a certification service provider is obliged according to current regulations and in the provisions of the Certification Policies and in this DPC to:

a) Respect the provisions of current regulations, this DPC and the PC Certification Policies.
b) Publish this DPC and each of the Certification Policies on the GSE website.
c) Inform ONAC about the modifications of the DPC and the Certification Policies.
d) Maintain the DPC with its latest version published on the GSE website.
e) Securely and responsibly protect and safeguard your private key.
f) Issue certificates in accordance with the Certification Policies and the standards defined in this DPC.
g) Generate certificates consistent with the information provided by the applicant or subscriber.
h) Keep information about digital certificates issued in accordance with current regulations.
i) Issue certificates whose minimum content is in accordance with the regulations in force for the different types of certificates.
j) Publish the status of issued digital certificates to an open access repository.
k) Do not keep a copy of the applicant's or subscriber's private key.
l) Revoke digital certificates as provided in the Digital Certificate Revocation Policy.
m) Update and publish the list of CRL revoked digital certificates with the latest revoked certificates.
n) Notify the Applicant, Subscriber or Entity of the revocation of the digital certificate within 24 hours of the revocation of the certificate in accordance with the digital certificate revocation policy.
o) Inform subscribers of the upcoming expiration of their digital certificate.
p) Have qualified personnel, with the knowledge and experience necessary for the provision of the certification service offered by the ECD GSE.

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* July 06,*2023

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

q) Provide the applicant on the website of the ECD GSE the following information free of charge and free access complying with the parameters and characteristics of current regulations without inducing error:
- The Certification Policies and Statement of Practices 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.
- The conditions and limits of the use of the certificate

r) Verify, by himself or through a different person acting on his 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 issue.

s) Inform the Superintendency of Industry and Commerce and the ONAC, immediately, of the occurrence of any event that compromises or may compromise the provision of the service.

t) Timely report the modification or update of services included in the scope of accreditation, in the terms established by the procedures, rules and requirements of the ONAC accreditation service

u) Update the contact information whenever there is a change or modification in the data provided.

v) Train and warn its users about the security measures that they must observe and about the logistics that are required for the use of the mechanisms of the provision of the service.

w) Guarantee the protection, integrity, confidentiality and security of the information provided by the subscriber by preserving the documentation that supports the certificates issued.

x) 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.

y) Provide the accredited services on the ECD GSE website.

1.9.11.2. Obligations of the RA.

The RA of the ECD GSE is responsible for carrying out the identification and registration work, therefore, the RA is obliged in the terms defined in this Declaration of Certification Practices to:

a) Know and comply with the provisions of this DPC and the Certification Policies corresponding to each type of certificate.

b) Keep and protect your private key.

c) Verify the identity of applicants, managers or subscribers of digital certificates.

d) Verify the accuracy and authenticity of the information provided by the Applicant.

e) Archive and keep the documentation provided by the applicant or subscriber for the issuance of the digital certificate, for the time established by current legislation.
f) Respect the provisions of the contracts signed between ECD GSE and the subscriber.
g) Identify and inform the ECD GSE of the causes of revocation provided by the applicants on the current digital certificates.

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

The Subscriber as a subscriber or responsible for a digital certificate is obliged to comply with the provisions of current regulations and the provisions of this DPC such as:

a) Use your digital certificate or electronic signature certificate under the terms of this DPC.
b) Verify within the next business day that the digital certificate information is correct. In case of finding inconsistencies, notify the ECD.
c) Refrain from: lending, assigning, writing, publishing the password to use your digital certificate and take all necessary, reasonable and timely measures to prevent it from being used by third parties.
d) Do not transfer, share or lend the cryptographic device to third parties.
e) Provide all the information required in the application form for digital certificates to facilitate their timely and full identification.
f) Request the revocation of the digital certificate before the change of name and/or surname.
g) Request the revocation of the digital certificate when the Subscriber has changed their nationality.
h) Comply with what is accepted and/or signed in the document terms and conditions.
i) Accurately and truthfully provide the required information.
j) Report during the validity of the digital certificate any change in the data initially provided for the issuance of the certificate.
k) Responsibly guard and protect your private key.
l) Use the certificate of conformity with the PCs established in this CPD for each of the types of certificate.
m) Request as subscriber and/or immediately responsible for the revocation of your digital certificate when you have knowledge that there is a reason defined in numeral *Circumstances for the revocation of a certificate* of this DPC.
n) Do not use the private key or the digital certificate once its validity has expired or is revoked.
o) Inform trusted third parties of the need to check the validity of the digital certificates you are using at any given time.

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 **July 06,*2023***

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

p) Inform the third party in good faith of the status of a revoked digital certificate for which the list of revoked certificates CRL is available, published periodically by ECD GSE.
q) Do not use your digital certification in a way that contravenes the law or creates a bad reputation for ECD.
r) Do not make any statement related to your digital certification in the ECD GSE that you may consider misleading or unauthorized, as provided by this DPC and PC.
s) 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.
t) The subscriber when referring to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, must report that it complies with the requirements specified in the PCs of this DPC, indicating the version.
u) The subscriber may use the conformity marks and the information related to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, as soon as it complies with the requirements in the previous paragraph.

On the other hand, you have the following rights:

a) Receive the digital certificate in the times established in the DPC.
b) Request information regarding pending applications.
c) Request revocation of the digital certificate by providing the necessary documentation.

d) Receive the digital certificate according to the scope granted by ONAC to GSE.

1.9.11.4. Obligations of Third Parties in good faith.

Third Parties in good faith as a party relying on digital certificates issued by ECD GSE are under an obligation to:

a) Know the provisions on Digital Certification in current regulations.
b) Know the provisions of the DPC.
c) Check the status of digital certificates before performing operations with digital certificates.
d) Check the list of CRL revoked certificates before performing operations with digital certificates.
e) Know and accept the conditions on guarantees, uses and responsibilities when carrying out operations with digital certificates.

1.9.11.5. Obligations of the Entity (Client).

In accordance with the provisions of the PCs listed in this document, in the case of certificates proving the linkage of the subscriber and/or responsible with it, it will be the obligation of the Entity:

a) Request the GSE ECD RA to suspend/revoke the digital certificate when this linkage ceases or is modified.
b) All those obligations linked to the person responsible for the digital certification service.
c) The entity when referring to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, must report that it complies with the requirements specified in the PCs related in this CPD.
d) 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 soon as it complies with the requirements in the previous paragraph.

1.9.11.6. Obligations of other ECD participants.

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

a) Review the consistency of the CPD with current regulations.
b) Approve and decide the changes to be made on certification services, by regulatory decisions or by requests from subscribers or managers.
c) Approve the notification of any change to subscribers and/or managers analyzing its legal, technical or commercial impact.
d) Review and take action on any comments made by subscribers or managers when a change to the certification service is made.
e) Inform the action plans to ONAC about any changes that have an impact on the PKI infrastructure and that affect the digital certification services, in accordance with RAC-3.0-01.
f) Authorize the changes or modifications required on the DPC.
g) Authorise the publication of the CPD on the ECD GSE website.
h) Approve changes or modifications to the ECD GSE Security Policies.
i) Ensure the integrity and availability of the information published on the ECD GSE website.
j) Ensure the existence of controls over the technological infrastructure of the ECD GSE.
k) Request the revocation of a digital certificate if you have knowledge or suspicion of the compromise of the private key of the subscriber, entity or any other fact that leads to the improper use of the private key of the subscriber, entity or the ECD itself.
l) Know and take relevant actions when security incidents occur.

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* July 06,*2023

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

m) Carry out a review of the DPC with a maximum annual frequency to verify that the lengths of the keys and periods of the certificates being used are adequate.
n) Review, approve and authorize changes to certification services accredited by the competent body.
o) 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.
p) Ensure that the accreditation conditions granted by the competent body are maintained.
q) Ensure proper use in documents or in any other publicity than symbols, certificates, and any other mechanism indicating that ECD GSE has an accredited certification service and complies with the provisions of the ONAC Accreditation Rules.
r) Ensure that their critical suppliers and reciprocal ECD, if any, are kept informed of the obligation to comply with the requirements of the CEA, in the corresponding numerals.
s) The Integrated Management System will execute corrective action plans and improvement actions to respond to any risk that compromises the impartiality of the ECD, whether derived from the actions of any person, organism, organization, activities, their relationships or the relationships of their personnel or themselves, for which it uses the ISO 31000 standard for the identification of risks that compromise the impartiality and non-discrimination of the ECD, delivering to the Management Committee the mechanism that eliminates or minimizes such risk, continuously.
t) Ensure that all ECD staff and committees (whether internal or external) that may have an influence on certification activities act with impartiality and non-discrimination, especially those arising from commercial, financial or other pressures that compromise their impartiality.
u) Document and demonstrate the commitment to impartiality and non-discrimination.
v) Ensure that the administrative, management, technical staff of the PKI, of the ECD associated with the consulting activities, maintain complete independence and autonomy with respect to the staff of the review process and decision making on the certification of this ECD.
w) Ensure to keep your critical suppliers informed such as the reciprocal ECD and datacenter that meet the accreditation requirements for ECD as support for their contracting and compliance with the requested requirements both administrative and technical.

1.9.12. Amendments.

The digital certificates issued by ECD GSE cannot be modified, i.e. they do not apply amendments. Consequently, the subscriber must request the issuance of a new digital certificate. In this event a new certificate will be issued to the subscriber; the cost of this modification will be borne entirely by the subscriber according to the rates reported by ECD GSE or according to the conditions defined at the contractual level.

1.9.12.1. Circumstances for modifying a certificate.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.9.12.2. Who can request an amendment?

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.9.12.3. Procedures for the application for modification of a certificate.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.9.12.4. Notification to the subscriber or responsible for issuing a new certificate.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.9.12.5. Form in which the modification of a certificate is accepted.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.9.12.6. Publication of the certificate as amended by the ECD.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.9.12.7. Notification of the issuance of a certificate by the ECD to other entities.

It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.9.13. Dispute Resolution Procedures.

If for any reason a difference arises between the Parties (subscriber/responsible and ECD GSE) on the occasion of:

i. The provision of the digital certification services described in this DPC.
ii. During the execution of the contracted services.
iii. For the interpretation of the contract, DPC and any other document delivered by ECD GSE.

The interested party shall notify the other party via certified email of the existence of such difference, with full and duly substantiated information of the difference, so that within fifteen (15) business days following such notification, the Parties seek to reach a direct settlement between them as a first instance.

At the end of said period the difference(s) persists, the Parties will be free to go before the ordinary Colombian justice to assert their rights or demands, which will be subject to the regulations in force on the matter, the costs that are caused on the occasion of the call will be fully borne by the expired Party.

In accordance with the provisions of Annex 2 - Terms and Conditions of the DPC.

1.9.14. Applicable Law.

The operation and operations carried out by the ECD GSE, as well as this Declaration of Certification Practices and the Certification Policies applicable to each type of certificate are subject to the regulations that apply to them and in particular to:

a. (e-Commerce) Defines and regulates access to and use of data messages, e-commerce and digital signatures, establishes certification authorities and contains other provisions.
b. Decree 333 of 2014, which regulates article 160 of Decree-Law 19 of 2012 regarding the characteristics and requirements of certification entities, and what is related to digital certificates.
c. Chapters 47 and 48 of Title 2 of Part 2 of Book 2 of the Single Decree of the Trade, Industry and Tourism Sector – DURSCIT.

1.9.15. Compliance with Applicable law.

ECD GSE states compliance with Law 527 of 1999 and that the Declaration of Certification Practices is satisfactory in accordance with the requirements established by the National Accreditation Agency of Colombia.

1.9.16. Miscellaneous provisions

Not applicable

1.9.17. OTHER PROVISIONS

1.9.17.1. Assignment.

Not Applicable

1.9.17.2. Divisibility.

In accordance with the provisions of Annex 2 - Terms and Conditions of the DPC.

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* July 06,2023**

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

1.10. CHANGES AFFECTING DIGITAL CERTIFICATION SERVICES.

ECD GSE may make adjustments or changes to digital certification services at the following events:

a. Due to regulatory changes in the legislation for ECD.
b. At the request of ONAC.
c. At the request of the Superintendence of Industry and Commerce of Colombia - SIC.
d. Technological changes affecting digital certification services.
e. At the request of subscribers or managers, subject to approval by the Management Committee.
   For which the Subscriber or responsible party must send a communication addressed to the ECD GSE Management Committee about the requested change, acceptance or rejection will be at the discretion of the Management Committee.

1.10.1. Procedure for Changes.

1.10.1.1. Changes that do not require notification.

a. When the changes made do not affect the functioning of the services provided to the subscribers or current managers, it will be the task of the Management Committee to define the level of impact of the changes.
b. To the extent that the changes imply typographical or editing corrections in the content of the services provided.

1.10.1.2. Changes that require notification

a. When the changes made affect the functioning of the services provided to the subscribers or current managers, it will be the task of the Management Committee to define the level of impact of the changes.
b. When the changes involve updating contact details with the ECD GSE.

1.10.1.3. Mechanism and notification period

ECD GSE will notify by email and/or web portal, subscribers, managers, ONAC and SIC with detailed technical information and modifications to contracts, about the change made to digital certification services, when:

a. The Management Committee and the Integrated Management System process of the ECD GSE consider that changes to digital certification services affect the operation and acceptability of these.

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* July 06,2023**

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

b. The changes introduce new requirements for the provision of digital certification services due to technological updates or regulatory changes that affect the services.

Subscribers and/or managers of the digital certification services affected by the changes made may submit their comments or rejection of the provision of the ECD GSE service in communication addressed to the Management Committee within thirty (30) days of notification, after thirty (30) days the conditions will be understood as accepted by the subscribers or managers.

1.11. DESCRIPTION OF PRODUCTS AND SERVICES

TYPE OF DIGITAL CERTIFICATE	OBJECT
Belonging to a company	It guarantees the identity of the natural person holding the certificate, as well as its link to a specific legal entity by virtue of the position held in it. This certificate will not by itself grant greater powers to its holder than those it possesses for the performance of its usual activity.
Company Representation	It is issued in favor of a natural person representing a certain legal entity. The holder of the certificate identifies himself not only as a natural person belonging to a company, but also adds his qualification as its legal representative.
Staff case	It guarantees the identity of the natural person holding the certificate, as well as their link to a Public Administration by virtue of the rank as a public official. This certificate will not by itself grant greater powers to its holder than those it possesses for the performance of its usual activity.
Qualified Professional	It guarantees the identity of the natural person holding the certificate, as well as his status as a qualified professional. This certificate will not by itself grant greater powers to its holder than those it possesses for the performance of its usual activity in the scope of its profession.
Natural Person	It only guarantees the identity of the natural person.
Electronic invoice for natural person	Exclusive certificate for electronic invoicing meeting the need of natural persons seeking the security of the certificate for the issuance of electronic invoices. Exclusive certificate for the digital signature of electronic invoices,

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* July 06,2023**

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

TYPE OF DIGITAL CERTIFICATE	OBJECT
	credit notes, debit notes, electronic payroll payment supports, adjustment notes of the electronic payroll payment support document and other documents resulting from the processes of the unattended platforms of the technological suppliers approved by the Dian, the free billing system of the Dian and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Electronic Invoice for Legal Entity	Exclusive certificate for electronic invoicing meeting the need of companies seeking the security of the certificate for the issuance of electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment supports, adjustment notes of the electronic payroll payment support document and other documents resulting from the processes of the unattended platforms of the technological suppliers approved by the Dian, the free billing system of the Dian and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Legal Entity	Carrying out business procedures by an application running on a machine in automatic signature processes and unattended on behalf of a legal person under public or private law that require guaranteeing the authenticity and integrity of the data sent or stored digitally together with the establishment of secure communication channels between customers, and that will be represented by a natural person (Responsible), holder of the certificate issued under this policy and called Responsible.
Generation of Certified Electronic Signatures	Exclusive certificate for the generation of certified electronic signatures.
Email Service	The certified email service allows to ensure the sending, receipt and verification of electronic communications, ensuring at all times the characteristics of fidelity, authorship, traceability and non-repudiation of the same.
Chronological Stamping Service (TSA)	Data message that links to another data message with a specific time or period of time, which allows establishing with a test that these data existed at that time or period of time and that they did not undergo any modification from the moment in which the stamping was carried out.

TYPE OF DIGITAL CERTIFICATE	OBJECT
Archiving and Retention Service of Transferable Electronic Documents and Data Message	Service consists of a secure and encrypted storage space that you access with credentials or a digital certificate. The documentation stored on this platform will have probative value as long as it is digitally signed.

Note: For the verification of the process of generation of each service refer to the corresponding procedures

1.12. FEES

1.12.1. Fees for issuing or renewing certificates.

Product Detail	Delivery time	Policy Period	Price without VAT	VAT	Total
Natural Person Certificate	Normal	1	$191,597	$36,403	$228,000
Natural Person Certificate	Normal	2	$277,310	$52,689	$329,999
Certificate Belonging to a company	Normal	1	$191,597	$36,403	$228,000
Certificate Belonging to a company	Normal	2	$277,310	$52,689	$329,999
Graduate Professional Certificate	Normal	1	$191,597	$36,403	$228,000
Graduate Professional Certificate	Normal	2	$277,310	$52,689	$329,999
Legal Representative Certificate	Normal	1	$191,597	$36,403	$228,000
Legal Representative Certificate	Normal	2	$277,310	$52,689	$329,999
Public Function Certificate	Normal	1	$191,597	$36,403	$228,000
Public Function Certificate	Normal	2	$277,310	$43,907	$274,999
CERTIFICATE OF GOOD STANDING	Normal	1	$504,202	$95,798	$ 600,000
CERTIFICATE OF GOOD STANDING	Normal	2	$857,143	$162,857	$1,020,000

These prices are calculated over a period of one and two years. The figures indicated here for each type of certificate may vary according to special commercial agreements that can be reached with subscribers, entities or applicants, in the development of promotional campaigns advanced by GSE.

For the case of electronic signature certificate there is no cost because it is included in the packages for the generation of certified electronic signatures.

*The ECD GSE makes available the issuance of digital certificates with validity in days or months not exceeding 24 months, the sale prices of these certificates will be agreed with the client after negotiation.

*For the issuance of digital certificates with elliptic curve algorithm, the same prices defined in the tariff table will apply.

1.12.2. Fees for access to certificates.

Access to the consultation of the status of the issued certificates is free and free of charge and therefore does not apply a fee.

1.12.3. Revocation fees or access to status information.

The request for revocation of a certificate is free of charge. Access to the status information of the issued certificates is free and free of charge and therefore does not charge a fee.

1.12.4. Fees for other services.

Once other services are offered by GSE, they are published on the PCs of the services on the GSE website.

1.12.5. Returns Policy.

Please note the Returns Policy published on the GSE website (https://gse.com.co/We/policies).

1.13. IMPARTIALITY AND NON-DISCRIMINATION

ECD GSE, at the head of the Management Committee and its collaborators are committed to safeguarding impartiality and independence in digital certification processes and services, in order to prevent conflicts of interest within the company, with relevant and external stakeholders, acting within the legal framework Law 527 of 1999, Decrees 019 of 2012, 333 of 2014 and 1471 of 2014, and the specific accreditation criteria of the National Accreditation Agency of Colombia (ONAC), so the following compliance mechanisms are established:

- The Management Committee and the collaborators of GSE declare that they do not participate directly or indirectly in services or activities, which may endanger free competition, responsibility, transparency.
- The collaborators will use the lifting of preventive and corrective actions to respond to any risk that compromises the impartiality of the company.
- The collaborators who are part of the accredited digital certification services will not be able to provide consulting services, nor involve the development team to provide technical support service to the subscriber or client.
- GSE is responsible for impartiality in the conduct of its activities and does not allow commercial, financial or other pressures to compromise its impartiality.
- GSE will not issue digital signature certificates to a natural or legal person who has relations with groups outside the law or who carry out illicit activities.
- GSE may decline acceptance of an application or maintenance of a contract for certification where there are substantiated, demonstrated or undue reasons on the part of the applicant and/or subscriber.
- GSE offers access to a digital certification service that does not depend on the size of the applicant or subscriber or the membership of any association or group, nor should it depend on the number of certifications already issued.

Note: Any case that puts at risk the impartiality of the ECD GSE as an ECD or its personnel, body or organization, will be brought to the attention of the Integrated Management System Process.

In accordance with the provisions of the Impartiality and Non-discrimination Policy of the ECD of GSE, which is located at the following link: https://gse.com.co/politicas.

1.14. Certification policies

The interrelationship between this DPC and the Certification Policies of the different certificates is fundamental. And this, insofar as:

- **The DPC** is the set of practices adopted by ECD GSE for the provision of services accredited by ONAC and contains detailed information on its security system, support, administration and issuance of certificates, as well as on the relationship of trust between Applicant, Subscriber, Responsible, Entity, bona fide Third Party and the ECD.

- **Certification policies** constitute the set of rules that define the characteristics of the different ECD GSE certificates and the applicability of these certificates for certain applications that require the same safety requirements and forms of use.

In short, the policy defines "**what**" requirements are necessary for the issuance of the different ECD GSE certificates while the DPC tells us "**how**" the security requirements imposed by the policy are met.

For this reason, the following Certificate Policies are listed:

- Certificate Policies for Digital Certificates:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.4.14
LOCATION OF THE	https://gse.com.co/documents/quality/policies/Politica_de_certificado_para_certificados_digitales_V14

- Certificate Policies for Chronological Stamping Service:

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.2.13
PC Location	https://gse.com.co/documents/quality/policies/Politica_de_Certificado_para_Servicio_de_Estampado_Cronologico_V13.pdf

- Certificate Policies for File Service and Retention of Electronic Transferable Documents and Data Messages:

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.3.13
PC Location	https://gse.com.co/documentos/calidad/politicas/Politica_de_Certificado_para_Servicio_de_Archivo_Confiable_de_Datos_V13.pdf

- Certificate Policies for Certified Email Service:

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.5.13
PC Location	https://gse.com.co/documents/quality/policies/Politica_Certificado_para_Servicio_de_Correo_Electronico_Certificado_V13.pdf

- Certified Electronic Signature Generation Policies:

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.6.5
PC Location	https://gse.com.co/documents/quality/policies/Politica_de_Generacion_de_Firmas_Electronicas_Certificadas_V5.pdf

1.15. ANNEX 1 DPC MATRIX TECHNICAL PROFILE DIGITAL CERTIFICATES.

1.16. ANNEX 2 DPC MODELS AND MINUTES OF THE TERMS AND CONDITIONS DOCUMENTS.

1.17. ANNEX 3 DPC MATRIX TECHNICAL PROFILE CERTIFICATES ELECTRONIC SIGNATURE.

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* July 06,*2023

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