GESTIÓN DE SEGURIDAD ELECTRÓNICA	CERTIFICATE POLICIES FOR DIGITAL CERTIFICATES	Code	POP-DT-5
		Version	14
		Implementation	16/05/2023
		Information Classification	Public

Document Title	**Certificate Policies for Digital Certificate Service**
Version	14
Working Group	Board of Management
Document status	Final
Date of issue	15/02/2010
Effective Start Date	16/05/2023
OID (Object Identifier)	1.3.6.1.4.1.31136.1.4.14
Policy Location	https://gse.com.co/documentos/calidad/politicas/Politicas_de_Certificado_para_Certificados_Digitales_V14.pdf
Prepared by	Operations Manager
Reviewed by	Integrated Management System
Approved	Board of Management

Change Control

Version	Date	Change/Modification
1	01-11-2016	Initial document in accordance with the development of the ONAC audit action plan.
2	5-10-2017	Update of information regarding the headquarters of ECD GSE.
3	03-04-2018	Update according to recommendations of the ONAC audit.
4	27-11-2018	It is changed from V3 to V4 26/11/2018 update charges, rates, routes of access to the website, change of title, inclusion of the limits of responsibility of the open certification entity, validity of the services, obligations of the ECD, the RA, the EE, the subscriber, those responsible, bona fide third parties, the entity and obligations of other participants
5	12-04-2019	The number of the obligations of the EE was eliminated, the responsibilities of the subscriber and responsible were unified, the specifications for MAC use were described in the number of supported Operating Systems, the clarification was made that, for centralized signature use, the acquisition of a technological platform is necessary with additional costs, and the obligations of the subscribers were updated according to the type of service.
6	07-06-2019	5.10.3 The obligations and rights of the subscriber were clarified
7	31/03/2020	The PC is adjusted to the changes generated by the new platforms, the Objective and Scope and administration of the policies are added, the price list is adjusted, the links are modified to point to the new routes and the version of the ETSY AND ITU-509 standards is updated.
8	14/08/2020	The contact person was updated in section 4.1. A note was added to section 7.5, in the event that the subscriber has a valid certificate, the digitally signed application may be filed and said application will replace the initially requested documents. For the public function type certificate, in case of not having the labor certificate, the act of possession, appointment act or service provision contract can be attached. For the certified professional type certificate, the RUT is requested (if applicable), the application for professional registration is changed to the diploma and that the degree certificate must be authenticated.
9	12/02/2021	The data of the ECD and CA(Paynet) were included with the links to consult the Certificate of Existence and Legal Representation online. The links have been updated to point to the new routes. The following numerals were updated: • 7.6. Specific requirement for processing 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

Version	Date	Change/Modification
10	16/07/2021	The numbers have been updated: 3.1. Overview, PKI Infrastructure Service Provider, CERL Query Url and Contact Phones. 5.3. OID of Policies 7. GSE ECD Digital Certificate Requirements 7.7. Specific requirements for processing the certificate 7.9. Activities and technical references of certificates, normative or technical documents Annexes CEA-4.1-10, EC384, EC256 were included in all digital certification services. 8.1.1 The image of the cryptographic devices was modified The numerals were included: 7.6 Prohibitions on the Use of Certificates 8.1.2 Safety Commitments 8.1.3 Cryptographic Device Care 8.1.4 Associated risks. 7.9.3. Technical Characteristics of Digital Certificates protection of personal data Fairness & Non-Discrimination The OID and the policy consultation link are updated.
11	27/10/2021	• Paragraph 7.7 Specific Requirements Processing of the Certificate was modified by including in the final section of the Note a clarification on the updated RUT of the Dian which must have the QR code. • Adjusted PC OID and link
12	31/05/2022	According to the new version of the CEA the following adjustments were made: • 4.4 Petitions, Complaints, Complaints and Applications: The term Appeal has been deleted. • 5.2 Content of the Certificates: The centralized signature certificate was deleted. • 6. Types of Certificates: The purpose of the legal entity certificate was modified. • 7.4. Uses of certificates: The attribute of the legal entity certificate was modified. • 7.7. Technical requirements for processing the certificate: The description of the application documentation of the electronic invoicing certificate and the legal entity certificate has been modified. • 7.9. Activities and technical references: The activities and regulatory documents of each of the types of certificates were modified in accordance with the accreditation certificate with ONAC.

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

GESTIÓN DE SEGURIDAD ELECTRÓNICA	CERTIFICATE POLICIES FOR DIGITAL CERTIFICATES	Code	POP-DT-5
		Version	14
		Implementation	16/05/2023
		Information Classification	Public

Version	Date	Change/Modification
		• 9.1.6. Obligations of other participants of the ECD: Item r) was modified leaving only CEA eliminating 4.1-10. • The OID and the consultation link of the Policy were adjusted. • The quality code was included in the header of the document.
13	23/09/2022	• Numeral 3.1 Abstract was modified including the chapters of the durscit. • The direction of the ECD was modified in sections 3.1 and 4.4. • The Paynet SAS address was modified in section 3.1. • The ITU X509 of 2016 was modified to the ITU X509 October 2019 in the standards of each service accredited in numeral 7.9 as well as the ITU -T-X.500 October 2019 and FIPS PUB 186-4 July 2013 standards were eliminated • Numeral 9.1.1 was modified including items o) to y). • Numerals 13 to 16 were included. • Paragraph 7.7 of the legal representative was modified by including a paragraph in the requested documentation. • The OID and the consultation link of the Policy were adjusted.
14	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. • Updated the OID and the consultation link of the Policy

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

CONTENTS

1. INTRODUCTION 9
1.1. Abstract 10
1.2. Name and identification of the document. 11
1.2.1. Policy Identification Criterion (OID) 11
1.2.2. The content of the certificates, distinguishing: 11
1.2.3. Coordination of national policy 12
1.2.4. Policies assigned to this document. 12
1.3. PKI Participants. 12
1.3.1. Certifying Authority (........ 12
1.3.2. Hierarchy of CAs. 13
1.3.3. Registration Authority (RA). 13
1.3.4. Subscriber and/or responsible. 14
1.3.5. bona fide third party 14
1.3.5.1. Precautions to be observed by third parties: 14
1.3.6. Applicant. 14
1.3.7. Entity to which the subscriber or responsible is linked. 14
1.3.8. Other participants. 14
1.3.8.1. Board of Management. 14
1.3.8.2. Service providers. 15
1.3.8.3. Reciprocal Digital Certification Entities. 15
1.3.8.4. Petitions, Complaints, Complaints and Requests. 15
1.4. Certificate Usage 16
1.4.1. Prohibitions on the use of certificates 16
1.4.2. Validity of certificates 17
1.4.3. Types of ECD GSE Certificates 17

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

1.5. POLICY ADMINISTRATION 18
1.5.1. Contact person: 19
1.5.2. Policy Approval Procedure 19
1.5.3. Publication Responsibilities 19
1.6. DEFINITIONS AND ACRONYMS 19
1.6.1. Definitions 19
1.6.2. Abbreviations 22
1.7. PUBLICATION AND REPOSITORY RESPONSIBILITIES. 23
1.7.1. PKI Repositories. 23
1.7.2. Publication of certification information. 23
1.7.3. Time or frequency of publication. 23
1.7.4. Repository access controls 23
1.8. IDENTIFICATION AND AUTHENTICATION 23
1.8.1. Names 23
1.8.2. Initial identity validation 24
1.8.3. Identification and Authentication for key renewal. 24
1.8.4. Identification and authentication in revocation requests 24
1.9. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFE CYCLE. 24
1.9.1. Application for a certificate 24
1.9.1.1. Generic requirements 27
1.9.1.2. Specific Requirements 27
1.9.2. Processing of certificate request. 28
1.9.3. Issuance of the Certificate. 29
1.9.4. Acceptance of the Certificate. 29
1.9.5. For keys and use of certificate. 29
1.9.6. Renewal of Certificate without Change of Keys. 29
1.9.7. Renewal of Certificate with Change of Keys 29
1.9.8. Modification of Certificate. 29

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

1.9.9. Certificate Revocation/Suspension 29
1.9.10. Certificate State Services. 29
1.9.11. End of subscription: 29
1.9.12. Key Custody and Recovery. 29
1.10. FACILITIES, ADMINISTRATION AND OPERATIONAL CONTROLS. 30
1.10.1. PHYSICAL SECURITY CONTROLS 30
1.10.2. Procedural Controls 30
1.10.3. Personnel controls 30
1.10.4. Audit Record Procedures. 30
1.10.5. FILE OF REGISTERS: 30
1.10.6. Change of Keys. 30
1.10.7. Commitment and Disaster Recovery. 30
1.10.8. Cessation of CA or RA. 30
1.11. Technical Security Controls 30
1.11.1. Generation and Installation of Key Pairs. 30
1.11.2. Private Key Protection and Cryptographic Module Engineering Controls. 31
1.11.3. Other Aspects of Key Pair Management. 31
1.11.4. Activation Data. 31
1.11.5. Life Cycle Safety Controls. 31
1.11.6. Network Security Controls. 31
1.11.7. Timestamping 31
1.12. CERTIFICATE PROFILES CERTIFICATE PROFILES, CRL AND OCSP. 31
1.12.1. Certificate Profile. 31
1.12.2. CRL Profile. 31
1.12.3. OCSP profile 31
1.13. COMPLIANCE AUDIT AND OTHER EVALUATION. 31
1.13.1. Frequency or Circumstances of Controls. 32
1.13.2. Identity/qualification of the Auditor. 32

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

1.13.3. Relationship between the Auditor and the Audited Entity. 32
1.13.4. Aspects Covered by Controls. 32
1.13.5. Actions to Take as a Result of Detection of Deficiencies. 32
1.13.6. Comunicación de Resultados. 32
1.14. OTHER COMMERCIAL AND LEGAL MATTERS. 32
1.14.1. Fees. 32
1.14.2. Financial responsibility. 32
1.14.3. Confidentiality of Commercial Information. 32
1.14.4. the privacy of Personal Information. 32
1.14.5. 7. Intellectual Property Rights 33
1.14.6. Representations and Warranties. 33
1.14.7. Warranty Waivers. 33
1.14.8. Limitations of Liability 33
1.14.9. Compensation. 34
1.14.10. Term; Termination. 34
1.14.11. Individual Notices and Communication with Participants. 34
1.14.11.1. Obligations of the ECD GSE 34
1.14.11.2. Obligations of the RA 35
1.14.11.3. Obligations (Duties and Rights) of the Subscriber and/or Responsible 36
1.14.11.4. Obligations of bona fide Third Parties 37
1.14.11.5. Obligations of the Entity (Client) 38
1.14.11.6. Obligations of other ECD participants 38
1.14.12. Amendments. 40
1.14.13. Dispute Resolution Procedures. 40
1.14.14. Applicable Law. 40
1.14.15. OTHER PROVISIONS 40
2. CHARACTERISTICS OF CRYPTOGRAPHIC DEVICES 40
2.1. Digital Certificate in Token 40

2.1.1. Features........ 40

2.1.2. - security commitment........ 41

2.1.3. Cryptographic Device Care........ 42

2.1.4. Associated risks........ 42

2.2. Digital Certificate in HSM – Hardware Security Module (Centralized Signature)........ 43

2.2.1. Technical Characteristics of Digital Certificates........ 43

3. RATES OF THE DIGITAL CERTIFICATE ISSUING SERVICE........ 44

3.1. Fees for issuing or renewing certificates........ 44

4. IMPARTIALITY AND NON-DISCRIMINATION........¡Error! Marcador no definido.

5. MODELS AND MINUTES OF THE TERMS AND CONDITIONS DOCUMENTS........ 46

6. CERTIFICATE PROFILE........ 46

1. INTRODUCTION

This document specifies the Certificate Policies for Digital Certificates (hereinafter PC) for the different certificates issued by the ECD GSE.

The purpose of the PC is to define those requirements that are necessary for the issuance of the different ECD GSE certificates.

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

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

ECD GSE must inform the Subscribers and/or Managers of the existence of this document where a response is given to the PCs of the different certificates issued by ECD GSE.

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

1.1. Abstract

Policy for Certificate of Digital Certificates, hereinafter **Policy** is a document prepared by **Gestión de Seguridad Electrónica S.A. (hereinafter GSE)** which, acting as a Digital Certification Entity, contains the standards, procedures that the **Digital Certification Entity (hereinafter GSE)** as **Provider of Digital Certification Services (PSC)** applies as a guideline to provide the Service in accordance with the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014, Chapters 47 and 48 of Title 2 of Part 2 of Book 2 of the Single Decree of the Commerce, Industry and Tourism Sector – DURSCIT and the regulations that modify or complement them, in the territory of Colombia.

DATA OF THE ENTITY PROVIDING DIGITAL CERTIFICATION SERVICES:

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

1.2. Name and identification of the document.

1.2.1. Policy Identification Criterion (OID)

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

The PC identifier is composed of a series of numbers separated from each other by points and with a specific meaning of each of them.

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

1.2.2. The content of the certificates, distinguishing:

If they are signature certificates they, in turn, are classified into other subtypes depending on whether or not they contain attribute.

The attribute constitutes the specific characteristic of the natural person holding the digital certificate that is contained in the certificate and that can be of different types:

- belonging to a Company
- company Representation
- civil Service
- a Graduate Professional
- persona Natural's
- Type of Legal Person:
- electronic Invoice

Who generates the keys of the digital certificate, distinguishing between the person holding the certificate or the ECD GSE itself.

The procedure to perform the update of the information contained in the certificates must be executed in accordance with the provisions of the DPC "Renewal of the certificate with change of keys", to perform the renewal of digital certificates the procedure of requesting a new certificate must be executed. 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.

1.2.3. Coordination of national policy

The following table shows the different certificates issued by the ECD GSE, and the OIDS of their corresponding PC, depending on the different variables defined in the previous section:

OID	DESCRIPTION
1.3.6.1.4.1.31136.1.4.14	Certificate Policy for Digital Certificates

1.2.4. Policies assigned to this document.

This document specifically responds to the PCs of the following certificates and their different subtypes:

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

1.3. PKI Participants.

1.3.1. Certifying Authority (

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

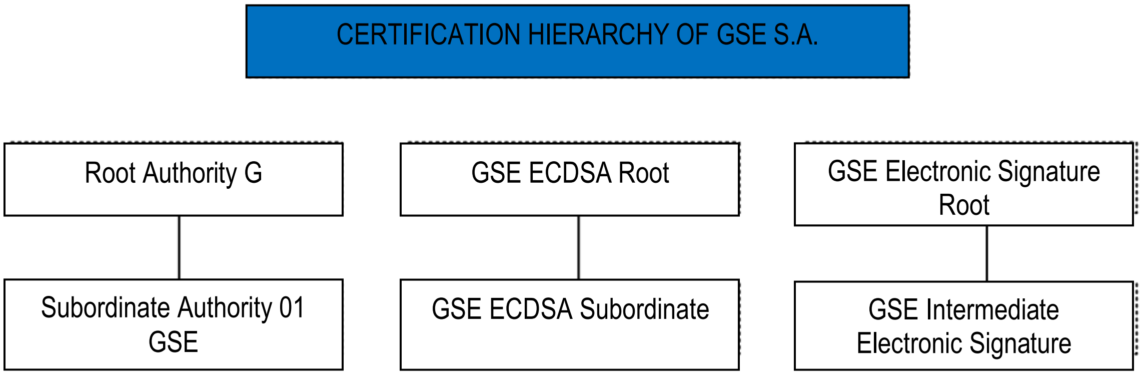
This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
***This document is an accurate translation of the original* July 06,2023**

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

hierarchy that allows it to provide services related to communications based on public key infrastructures.

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.

1.3.3. 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).

1.3.4. 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.

1.3.5. 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.

1.3.5.1. 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.

1.3.6. 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.

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

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

1.3.8. Other participants.

1.3.8.1. 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.

1.3.8.2. 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.

1.3.8.3. 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.

1.3.8.4. Petitions, Complaints, Complaints and Requests.

Requests, complaints, claims and requests about the services provided by ECD GSE or subcontracted entities, explanations about this Certification Policy; 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.

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.

1.4. Certificate Usage

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

TYPE OF DIGITAL CERTIFICATE	SCOPE USES AND APPLICATIONS
Belonging to a company	Carrying out business procedures by the subscriber and/or manager without involving representation. The Company may place limitations on use.
Company Representation	Carrying out business procedures by the subscriber and/or manager on behalf of the company. The Company may place limitations on use.
Staff case	Performing procedures by the subscriber and/or responsible in the exercise of his functions as a public official. The Public Administration may establish limitations of use.
Qualified Professional	Performing procedures by the subscriber and/or responsible in the exercise of their functions as a registered professional.
Natural Person	Performing procedures by the subscriber and/or responsible in his/her capacity as a citizen. There is no connection with any entity.
Electronic Invoice	Performed by the subscriber and/or person in charge of billing and/or electronic appointment
Legal Entity	Carrying out business procedures by an application running on a machine in automatic signature processes and/or 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 and that will be represented by a person responsible for the certificate issued. The use of this certificate is allowed within unattended platforms once the study of risk management with respect to the handling of cryptographic keys has been completed.

1.4.1. Prohibitions on the use of certificates

The performance of operations not authorized under this Policy, by third parties or subscribers of the service will exempt ECD GSE from any responsibility for this prohibited use.

- The use of the certificate to sign other certificates or revocation lists (CRLs) is not allowed
- It is forbidden to use the certificate for uses other than those stipulated in the section "Use of the Certificate" and "Limits of Liability of the Open Digital Certification Entity" of this Policy.
- Alterations on certificates are not allowed and the certificate must be used as supplied by the ECD GSE.
- The use of certificates in control systems or systems intolerant to failures that may cause personal or environmental damage is prohibited.
- Any action that violates the provisions, obligations and requirements stipulated in this Policy is prohibited.
- It is not possible for the ECD GSE to issue any assessment on the content of the documents signed by the subscriber, therefore the responsibility for the content of the message is the sole responsibility of the signatory.
- It is not possible for the ECD GSE to recover the encrypted data in case of loss of the subscriber's private key because the CA for security does not keep a copy of the subscribers' private key, therefore it is the subscriber's responsibility to use data encryption.
- Unlawful purposes or operations under any legal regime in the world.

1.4.2. Validity of certificates

Certificates issued by the ECD GSE are valid for a maximum of twenty-four (24) months.

1.4.3. Types of ECD GSE Certificates

The different types of certificates issued by ECD GSE are classified according to the criterion of "content" and the fields defined therein and established in the technical profiles defined in Annex 1 of the CPD.

By virtue of this criterion, one or other information constituting the subject-matter of the certificate is guaranteed.

Thus, the digital certificates defined under this policy are as follows:

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	Exclusive certificate for electronic invoicing meeting the need of companies and/or natural persons 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 and that will be represented by a person responsible for the certificate issued.

1.5. POLICY ADMINISTRATION

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

1.5.1. Contact person:

Contact's Position	Operations Manager
Contact phone numbers:	4050082
E-MAIL:	info@gse.com.co

1.5.2. Policy Approval Procedure

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

1.5.3. Publication Responsibilities

Once the policy changes have been made and approved, it is the responsibility of the Operations Manager and/or the Integrated Management System Process to request the process in charge of updating the policies in their latest version on the WEB portals.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

The following terms are commonly used and required for the understanding of this Policy.

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.

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

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.

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.

1.6.2. Abbreviations

CA: Certification Authority
CPS: Certification 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.
IEC: International Electrotechnical Commission

IETF: Internet Engineering Task Force
IP: Internet Protocol.
ISO: International Organization for Standardization
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

1.7. PUBLICATION AND REPOSITORY RESPONSIBILITIES.

1.7.1. PKI Repositories.

In accordance with the provisions of the Declaration of Certification Practices

1.7.2. Publication of certification information.

In accordance with the provisions of the Declaration of Certification Practices

1.7.3. Time or frequency of publication.

In accordance with the provisions of the Declaration of Certification Practices

1.7.4. Repository access controls.

In accordance with the provisions of the Declaration of Certification Practices

1.8. IDENTIFICATION AND AUTHENTICATION

1.8.1. Names.

In accordance with the provisions of the Declaration of Certification Practices

1.8.2. Initial identity validation.

In accordance with the provisions of the Declaration of Certification Practices

1.8.3. Identification and Authentication for key renewal.

In accordance with the provisions of the Declaration of Certification Practices

1.8.4. Identification and authentication in revocation requests.

In accordance with the provisions of the Declaration of Certification Practices

1.9. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFE CYCLE.

1.9.1. 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.

TYPE OF DIGITAL CERTIFICATE	REGISTRATION: DOCUMENTATION REQUESTED
For all types of certificates, the following information will be requested: • Completed application form. • Acceptance of terms and conditions • General data: Name, address and address of the subscriber and additional information according to the type of digital certificate.	
Company Membership	• Document of Existence and Legal Representation of the Company with validity no greater than thirty (30) days. • Labor certificate of the applicant including the position on institutional paper (no more than thirty (30) days). • Applicant Identification Document • RUT tax registration
Company Representation	• Document of Existence and Legal Representation of the Company with validity no greater than thirty (30) days. • Applicant Identification Document • RUT tax registration

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	REGISTRATION: DOCUMENTATION REQUESTED
	In the event that the request is delegated by the Legal Representative and/or Alternate to a third party, you must attach the letter of delegation for the request of the digital certificate.
Staff case	• To confirm the applicant's relationship information with the Company, one of the following documents will be requested: ➢ ACT OF POSSESSION ➢ Appointment resolution or decree. ➢ Contract for services ➢ Labor certificate of the applicant including the position on institutional paper (no more than thirty (30) days from the filing of the application). • Applicant Identification Document • RUT tax registration
Qualified Professional	• Professional Card and/or equivalent document. • Degree Diploma (optional) • Applicant Identification Document • RUT tax registration
Natural Person	• In the event that the applicant does not have a Single Tax Registry – RUT • You must present a document that records the address information that is issued by a third party that verifies it. • Applicant Identification Document • RUT tax registration
Electronic Invoice	Natural Person • RUT tax registration • In the event that the applicant does not have a Single Tax Registry – RUT must present a document recording the address information that is issued by a third party who verifies it. • Applicant Identification Document In the event that the request is delegated by the Legal Representative and/or Alternate to a third party, you must attach the letter of delegation for the request of the digital certificate.
	Legal Entity • RUT tax registration • Document of Existence and Legal Representation of the Company with validity no greater than thirty (30) days. • Applicant Identification Document If the applicant does not have the document of existence and legal representation and is a public or state entity, the equivalent document or documents in which the creation of the entity can be validated in accordance with current regulations and

TYPE OF DIGITAL CERTIFICATE	REGISTRATION: DOCUMENTATION REQUESTED
	the respective administrative act (law, decree, resolution, among others) will be requested. In the event that the request is delegated by the Legal Representative and/or Alternate to a third party, you must attach the letter of delegation for the request of the digital certificate.
Legal Entity	• Document of Existence and Legal Representation of the Company with validity no greater than thirty (30) days. • Applicant Identification Document • RUT tax registration If the applicant does not have the document of existence and legal representation and is a public or state entity, the equivalent document or documents in which the creation of the entity can be validated in accordance with current regulations and the respective administrative act (law, decree, resolution, among others) will be requested. In the event that the request is delegated by the Legal Representative and/or Alternate to a third party, you must attach the letter of delegation for the request of the digital certificate.

Notes:

- The documents will be received scanned or in electronic original, preserving the legibility for the use of the information.
- The Single Tax Registration – RUT document will be requested in the updated Dian format that includes QR code.
- The applicant's address information: country, department, municipality and address, will be verified in the documents: Document of Existence and Legal Representation or Single Tax Registry – RUT.
- For the types of certificate where the Existence and Legal Representation Document is requested, said document will be valid for no more than thirty (30) days from the filing of the request.
- For the types of certificates where the Document of Existence and Legal Representation of the Company is requested, in the cases that are required, an equivalent document will be valid where the existence and legal representation of the company can be validated, if applicable, the document will be duly authenticated.
- For the types of certificates where the Single Tax Registration – RUT of the applicant is requested, in the cases that are required, an equivalent document will be valid where the applicant's data and the applicant's address data can be validated, if applicable, the document will be requested duly authenticated.
- Any document that is received authenticated, the authentication must have a validity no greater than sixty (60) days from the filing of the request.

TYPE OF DIGITAL CERTIFICATE	REGISTRATION: DOCUMENTATION REQUESTED
• In cases where applications for digital certificates are submitted with additional documents and/or equivalent to the requested documentation, the documents mentioned in the Documentary Annex of Validation of Applications published on the website in the Support-Guides and Manuals-Validation of Applications section will be taken into account for the review of the applications.	

The ECD-GSE has a security management system to protect the information that is collected in order to issue the certificates which is established in the DPC in "Computer Security Controls".

ECD GSE does not prevent or inhibit applicants' access to services as ECD, therefore a digital certificate can be requested regardless of the size of the applicant or subscriber, the type of existing link with ECD GSE, or membership with any association or group, nor does it depend on the number of digital certificates already issued or any other that discriminates access to the request for the service provided by ECD GSE.

1.9.1.1. Generic requirements

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

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

1.9.1.2. Specific Requirements

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

TYPE OF DIGITAL CERTIFICATE	SUBSCRIBER / RESPONSIBLE	ATTRIBUTE	ENTITY

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	SUBSCRIBER / RESPONSIBLE	ATTRIBUTE	ENTITY
Belonging to a company	Natural person who belongs to the company and who is the holder of the certificate.	Linkage of membership in a company	Company to which the Subscriber is linked
Company Representation	Natural person who legally represents the company and who is the holder of the certificate	Linkage of legal representation to company	Company represented by Subscriber
Staff case	Natural person who belongs to a Public Administration and who is the holder of the certificate	Functional link with respect to a Public Administration	Public Administration to which the Subscriber is linked
Qualified Professional	Natural person who exercises a profession entitled and who is the holder of the certificate	Exercise of a collegiate profession and link with the Professional Association	Professional Association to which the Subscriber is linked
Natural Person	Natural person holding the certificate	Not applicable	Not applicable
Electronic Invoice	Guarantees only the identity of the subscriber and/or responsible	Linking for the realization of invoicing and/or electronic payroll	Subscriber and/or responsible that requires billing and/or electronic appointment
Legal Entity	Responsible for the certificate acting on behalf of a Legal Entity	Linkage of legal representation to company	Company represented by the Subscriber and/or responsible.

1.9.2. Processing of certificate request.

In accordance with the provisions of the Declaration of Certification Practices

1.9.3. Issuance of the Certificate.

In accordance with the provisions of the Declaration of Certification Practices

1.9.4. Acceptance of the Certificate.

In accordance with the provisions of the Declaration of Certification Practices

1.9.5. For keys and use of certificate.

In accordance with the provisions of the Declaration of Certification Practices

1.9.6. Renewal of Certificate without Change of Keys.

In accordance with the provisions of the Declaration of Certification Practices

1.9.7. Renewal of Certificate with Change of Keys.

In accordance with the provisions of the Declaration of Certification Practices

1.9.8. Modification of Certificate.

In accordance with the provisions of the Declaration of Certification Practices

1.9.9. Certificate Revocation/Suspension

In accordance with the provisions of the Declaration of Certification Practices

1.9.10. Certificate State Services.

In accordance with the provisions of the Declaration of Certification Practices

1.9.11. End of subscription:

In accordance with the provisions of the Declaration of Certification Practices

1.9.12. Key Custody and Recovery.

In accordance with the provisions of the Declaration of Certification Practices

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

1.10. FACILITIES, ADMINISTRATION AND OPERATIONAL CONTROLS.

1.10.1. PHYSICAL SECURITY CONTROLS

In accordance with the provisions of the Declaration of Certification Practices

1.10.2. Procedural Controls

In accordance with the provisions of the Declaration of Certification Practices

1.10.3. Personnel controls.

In accordance with the provisions of the Declaration of Certification Practices

1.10.4. Audit Record Procedures.

In accordance with the provisions of the Declaration of Certification Practices

1.10.5. FILE OF REGISTERS:

In accordance with the provisions of the Declaration of Certification Practices

1.10.6. Change of Keys.

In accordance with the provisions of the Declaration of Certification Practices

1.10.7. Commitment and Disaster Recovery.

In accordance with the provisions of the Declaration of Certification Practices

1.10.8. Cessation of CA or RA.

In accordance with the provisions of the Declaration of Certification Practices

1.11. Technical Security Controls

1.11.1. Generation and Installation of Key Pairs.

In accordance with the provisions of the Declaration of Certification Practices

1.11.2. Private Key Protection and Cryptographic Module Engineering Controls.

In accordance with the provisions of the Declaration of Certification Practices

1.11.3. Other Aspects of Key Pair Management.

In accordance with the provisions of the Declaration of Certification Practices

1.11.4. Activation Data.

In accordance with the provisions of the Declaration of Certification Practices

1.11.5. Life Cycle Safety Controls.

In accordance with the provisions of the Declaration of Certification Practices

1.11.6. Network Security Controls.

In accordance with the provisions of the Declaration of Certification Practices

1.11.7. Timestamping.

In accordance with the provisions of the Declaration of Certification Practices

1.12. CERTIFICATE PROFILES CERTIFICATE PROFILES, CRL AND OCSP.

1.12.1. Certificate Profile.

In accordance with the provisions of the Declaration of Certification Practices

1.12.2. CRL Profile.

In accordance with the provisions of the Declaration of Certification Practices

1.12.3. OCSP profile.

In accordance with the provisions of the Declaration of Certification Practices

1.13. COMPLIANCE AUDIT AND OTHER EVALUATION.

1.13.1. Frequency or Circumstances of Controls.

In accordance with the provisions of the Declaration of Certification Practices

1.13.2. Identity/qualification of the Auditor.

In accordance with the provisions of the Declaration of Certification Practices

1.13.3. Relationship between the Auditor and the Audited Entity.

In accordance with the provisions of the Declaration of Certification Practices

1.13.4. Aspects Covered by Controls.

In accordance with the provisions of the Declaration of Certification Practices

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

In accordance with the provisions of the Declaration of Certification Practices

1.13.6. Comunicación de Resultados.

In accordance with the provisions of the Declaration of Certification Practices

1.14. OTHER COMMERCIAL AND LEGAL MATTERS.

1.14.1. Fees.

In accordance with the provisions of the Declaration of Certification Practices

1.14.2. Financial responsibility.

In accordance with the provisions of the Declaration of Certification Practices

1.14.3. Confidentiality of Commercial Information.

In accordance with the provisions of the Declaration of Certification Practices

1.14.4. the privacy of Personal Information.

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

In accordance with the provisions of the Declaration of Certification Practices

1.14.5. 7. Intellectual Property Rights

In accordance with the provisions of the Declaration of Certification Practices

1.14.6. Representations and Warranties.

In accordance with the provisions of the Declaration of Certification Practices

1.14.7. Warranty Waivers.

Not Applicable

1.14.8. Limitations of Liability

The limitations of Liability of the Open Certification Entity are defined comprehensively in the Limits of Liability of the DPC, but starting from the specific uses of each of the certificates established in the previous numeral. ECD GSE does not assume any other commitment or provide any other guarantee, nor does it assume any other responsibility towards certificate holders or trusted third parties except as established by the provisions of this PC.

The ECD GSE will decline an application for a digital certification service, if it is not within the scope of the accreditation granted to it by ONAC.

TYPE OF DIGITAL CERTIFICATE	LIMIT OF LIABILITY OF THE CERTIFICATION BODY
Belonging to a company	Digital certificates issued by ECD GSE may only be used for the uses for which they have been issued and specified in the DPC and specifically in the paragraph Use of certificate. Those uses that are not defined in the DPC and in the PCs are considered improper and consequently for legal purposes, the ECD GSE is exempt from all responsibility for the use of the certificates in operations that are outside the limits and conditions established for the use of digital certificates according to the DPC, the PCs and in accordance with the provisions of the numeral Limits of Liability of the open certification entity.
Company Representation	
Staff case	
Qualified Professional	
Natural Person	
Electronic Invoice	
Legal Entity	

1.14.9. Compensation.

Not Applicable

1.14.10. Term; Termination.

In accordance with the provisions of the Declaration of Certification Practices

1.14.11. Individual Notices and Communication with Participants.

In accordance with the provisions of the Declaration of Certification Practices

1.14.11.1. Obligations of the ECD GSE

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

a) Respect the provisions of current regulations, the DPC and the Certificate Policies.
b) Publish the DPC and each of the Certificate Policies on the GSE website.
c) Inform ONAC about the modifications of the DPC and the Certificate Policies.
d) Maintain the DPC and Certificate Policies with their latest version published on the GSE website.
e) Securely and responsibly protect and safeguard your private key.
f) Issue certificates in accordance with the Certificate Policies and the standards defined in the 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 digital 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.

q) Provide the applicant on the ECD GSE website with the following information free of charge and free access:
- 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.
- Mechanisms to ensure the reliability of the electronic signature over time.
- 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 Superintendence 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 their accreditation, in the terms established by the procedures, rules and requirements of the accreditation service of the ONAC

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.

1.14.11.2. Obligations of the RA

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

a) Know and comply with the provisions of the DPC and the Certificate Policy corresponding to each type of 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

b) Keep and protect your private key.
c) Review the initial validation records of 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 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.

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

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

a) Use your digital certificate under the terms of the 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 to facilitate its timely and full identification.
f) Request the revocation of the Digital Certificate upon 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 signed in the document terms and conditions or responsible for digital certificates.
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 in accordance with the provisions of this PC for each of the types of certificate.
m) Request as a subscriber 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 the DPC.

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

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.
p) Inform the third party in good faith to verify the status of a certificate has the list of certificates revoked CRL, 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) Failure to make any statement related to your digital certification in the ECD GSE may be considered misleading or unauthorized, as provided by the 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 the 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) 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.
c) Request information regarding pending applications.
d) Request revocation of the digital certificate by providing the necessary documentation.
e) Receive the digital certificate according to the scope granted by ONAC to GSE.

1.14.11.4. Obligations of bona fide Third Parties

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 and PC.
c) Check the status of certificates before performing operations with digital certificates.
d) Check the CRL Revoked Certificate List before performing operations with digital certificates.
e) Know and accept the conditions on guarantees, uses and responsibilities when carrying out operations with digital certificates.

1.14.11.5. Obligations of the Entity (Client)

The client entity is in charge of requesting the services for its officials and the subscribers are the people who make use of the service.

In accordance with the provisions of the Certificate Policies, in the case of certificates proving the connection of the Subscriber or Responsible with the same, it will be the obligation of the Entity:

a) Request the RA GSE to suspend/revoke the certificate when said 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 of the 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.

1.14.11.6. Obligations of other ECD participants

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

a) Review the consistency of the CPD with current regulations.
b) Approve and decide on the changes to be made to digital 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 and/or managers when a change to the digital certification service is made.

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
***This document is an accurate translation of the original* July 06,2023**

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

e) Inform the action plans to ONAC and SIC about any changes that have an impact on PKI infrastructure and that affect digital certification services, in accordance with RAC-3.0-01.
f) Authorize the changes or modifications required on the DPC.
g) Authorize 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 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.
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 digital 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 RAC-3.0-01 and RAC-3.0-03.
r) Ensure that their critical suppliers and reciprocal ECD are kept informed, if any, of the obligation to comply with the requirements of the CEA, in the corresponding numerals.
s) The Integrated Management System process will execute preventive and corrective action plans to respond to any risk that compromises the impartiality and non-discrimination of the ECD, whether arising from the actions of any person, agency, organization, activities, their relationships or the relationships of their staff or themselves. To this end, it uses the ISO 31000 standard for the identification of risks that compromise the impartiality of the ECD.
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, compromise their impartiality.

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

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 the same 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.

1.14.12. Amendments.

In accordance with the provisions of the Declaration of Certification Practices

1.14.13. Dispute Resolution Procedures.

In accordance with the provisions of the Declaration of Certification Practices

1.14.14. Applicable Law.

In accordance with the provisions of the Declaration of Certification Practices

1.14.15. OTHER PROVISIONS

In accordance with the provisions of the Declaration of Certification Practices

2. CHARACTERISTICS OF CRYPTOGRAPHIC DEVICES

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

2.1. Digital Certificate in Token

2.1.1. Features

CHARACTERISTIC	TECHNICAL SPECIFICATION
Supported Operating systems	● **32bit and 64bit** ● **Windows (XP, Vista, 7, 8, 10) Mac OS Server2003, Server2008, Server2008 R2, Server 2012 R2.**
Standard	**X.509 Oct 2019, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID**
Mcrypt Encryption Functions	**Key Pair Generation** **Digital signature and verification** **Data encryption and decryption**
Algorithm Support	**RSA 512/1024/2048, DES, 3DES, SHA-1, SHA-256/384/512, AES 128/192/256**
Processor	**16-bit smart card chip (Common Criteria EAL 5+ certificate)**
Memory	**64KB (EEPROM)**
Connectivity	**USB 2.0 Total Speed Token, Type A Connector**
Device Lockout	**Third use attempt with incorrect key will be blocked**
Operating Temperature	**0°C ~ 70°C** **(32°F ~ 158°F)**
Moisture	**0% ~ 100% non-condensing**
Storage Temperature	**-20°C ~ 85°C** **(-4°F ~ 185°F)**
Net weight	**8.1 gr**
Dimensions	**54.5x17x8.5 mm**

2.1.2. - security commitment

For circumstances affecting the security of the cryptographic device:

- Compromise or suspicion of compromising the security of the cryptographic device.
- Loss or disablement due to damage of the cryptographic device.

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

- Unauthorized access, by a third party, to the activation data of the Signer or the certificate holder

2.1.3. *Cryptographic Device Care*

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

2.1.4. *Associated risks*

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

- Device loss.
- Key compromise.
- Damage due to improper handling.
- Damage due to the carelessness of the device in the face of environmental conditions.
- Damage due to voltage variation.

In order to mitigate the associated risks, the following should be taken into account:

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

2.2. Digital Certificate in HSM – Hardware Security Module (Centralized Signature)

CHARACTERISTIC	TECHNICAL SPECIFICATION
Supported Operating systems	32bit and 64bit • Windows (XP, Vista, 7, 8, 10) • Server2003, Server2008, Server2008 R2, Server 2012 R2.
Standard	• X.509 Oct 2019, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID
Mcrypt Encryption Functions	• Key Pair Generation • Digital signature and verification • Data encryption and decryption
Connectivity	• Website, with User/Password
Session Locking	• The session is blocked from the user's IP, on the third access attempt with incorrect password

2.2.1. Technical Characteristics of Digital Certificates

CHARACTERISTIC	TECHNICAL SPECIFICATION
Signature algorithm	*Hash function* SHA256 with RSA Encryption. *Hash function* SHA384 with ECDSA
	ENCRYPTION FUNCTION RSA with 4096 key length for ROOT CA RSA with key length of 4096 for SUBORDINATE CA RSA with 2048 subscriber / responsible key length. ECDSA with 384 key length for ROOT CA ECDSA with key length of 384 for SUBORDINATE CA ECDSA with key length of 256 subscribers / responsible.
Content of the Digital Certificate	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. May 2008 ITU-T-X509 October 2019 ETSI TS 102 042 - Policy requirements for certification authorities issuing public key.
Certificate Lifecycle	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

Key Generation	FIPS 140-2 Token Level 3 HSM FIPS 140-2 Level 3 (Centralized Signature)
Certification activities Article 161 of Decree Law 0019 of 2012	1. Issue certificates in relation to electronic or digital signatures of natural or legal persons. 2. Issue certificates on verification regarding the alteration between sending and receiving the data message and transferable electronic documents. 3. Issue certificates in relation to the person who possesses a right or obligation with respect to the documents listed in paragraphs f) and g) of article 26 of Law 527 of 1999

3. RATES OF THE DIGITAL CERTIFICATE ISSUING SERVICE

3.1. Fees for issuing or renewing certificates

Product Detail Digital Certificates	Delivery time	Policy Period	Price excluding VAT:	VAT	Total
Natural Person	Normal	1	$191,597	$36,403	$228,000
Natural Person	Normal	2	$277,310	$52,689	$329,999
Belonging to Company	Normal	1	$191,597	$36,403	$228,000
Belonging to Company	Normal	2	$277,310	$52,689	$329,999
Qualified Professional	Normal	1	$191,597	$36,403	$228,000
Qualified Professional	Normal	2	$277,310	$52,689	$329,999
Company Representative	Normal	1	$191,597	$36,403	$228,000
Company Representative	Normal	2	$277,310	$52,689	$329,999
Commission of the	Normal	1	$191,597	$36,403	$228,000
Commission of the	Normal	2	$277,310	$43,907	$274,999
Legal Entity	Normal	1	$504,202	$95,798	$ 600,000
Legal Entity	Normal	2	$857,143	$162,857	$1,020,000
Electronic Invoicing	Normal	1	$195,357	$37,117	$232,474
Electronic Invoicing	Normal	2	$275,523	52349	$327,872

*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.

*In order to use the centralized signature certificate, it is necessary to use a technological platform.

*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.

4. 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.

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

- 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.

5. MODELS AND MINUTES OF THE TERMS AND CONDITIONS DOCUMENTS

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

6. CERTIFICATE PROFILE

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

OID (Object Identifier)	1.3.6.1.4.1.31136.1.4.14
PC Location	https://gse.com.co/documentos/calidad/politicas/Politicas_de_Certificado_para_Certificados_Digitales_V14.pdf