CERTIFICATE POLICIES FOR DIGITAL CERTIFICATE SERVICES

Code	POP-DT-5
Version	12
Implementation	31/05/2022
Information Classification	Public

Document Title	**Certificate Policies for Digital Certificate Services**
Version	12
Working Group	Management Committee
Document status	Final
Date of issue	15/02/2010
Effective date	31/05/2022
OID (Object Identifier)	1.3.6.1.4.1.31136.1.4.12
Policy Location	https://gse.com.co/documentos/calidad/politicas/Certificate_Policies_for_Digital_Certificate_Services_V12.pdf
Prepared by	Chief Operating Officer
Reviewed	Integrated Management System
Approved	Management Committee

Change Control

Version	Date	Change/Modification
1	01-11-2016	Initial document in accordance with the development of the ONAC audit action plan.
2	05-10-2017	Update of information regarding ECD GSE headquarters.
3	03-04-2018	Updating in accordance with ONAC audit recommendations.
4	27-11-2018	Changed from V3 to V4 11/26/2018 update charges, fees, website access routes, title change, inclusion of open certification authority liability limits, term of services, obligations of the ECD, RA, EE, subscriber, responsible parties, bona fide third parties, entity and obligations of other participants
5	12-04-2019	The section on the obligations of the EE was eliminated, the responsibilities of the subscriber and the responsible party were unified, the specifications for the use of MAC were described in the section on Supported Operating Systems, and it was clarified that for the use of a centralized signature it is necessary to acquire a technological platform 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's are 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 so that they 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 item 4.1. A note was added to item 7.5, in case the subscriber has a valid certificate, he/she may submit the request digitally signed and such request will replace the documents initially requested. For the civil service type certificate, if the subscriber does not have the labor certificate, the possession certificate, appointment certificate or service contract may be attached. For the professional degree type certificate, the RUT is requested (if applicable), the request for professional registration is replaced by the diploma and the degree certificate must be authenticated.
9	12/02/2021	The ECD and CA(Paynet) data 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 items were updated: • 7.6. Specific requirement for certificate processing.
10	16/07/2021	The numbers have been updated: 3.1. Summary, PKI infrastructure service provider, CERL query url and contact phone numbers. 5.3. OID of the Policies 7. ECD GSE digital certificate requirements 7.7. Specific requirements for certificate processing

Version	Date	Change/Modification
		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 Image of cryptographic devices modified The numerals were included: 7.6 Prohibitions on Use of Certificates 8.1.2 Safety commitments 8.1.3 Care of the cryptographic device 8.1.4 Associated risks. 7.9.3. Technical Characteristics of Digital Certificates 10. Protection of personal information 11. Fairness and non-discrimination The OID and the policy consultation link are updated.
11	27/10/2021	• Section 7.7 Specific Requirements for Certificate Processing was modified to include in the final section of the Note a clarification on the updated RUT of the DIAN which must have the QR code. • OID and PC link adjusted
12	31/05/2022	According to the new version of the CEA, the following adjustments were made: • 4.4 Petitions, Complaints, Claims and Requests: The term Appeal was eliminated. • 5.2 Certificate Content: The centralized signature certificate has been eliminated. • 6. Types of Certificates: The purpose of the legal entity certificate has been modified. • 7.4. Uses of the certificates: The attribute of the legal entity certificate has been modified. • 7.7. Technical requirements for certificate processing: The description of the application documentation for the electronic invoicing certificate and the legal entity certificate has been modified. • 7.9. Activities and technical references: The activities and normative documents for each type of certificate were modified in accordance with the accreditation certificate with ONAC. • 9.1.6. Obligations of other DCE participants: Item r) was modified leaving only CEA, eliminating 4.1-10. • The OID and the link to consult the Policy have been adjusted. • The quality code was included in the document header.

TABLE OF CONTENTS

1. OBJECTIVE 6

2. SCOPE 6

3. INTRODUCTION 6

3.1. Summary 6

3.2. Definitions and acronyms 8

3.2.1 Definitions 8

3.2.2 Acronyms 10

4. POLICY MANAGEMENT 11

4.1 Contact person: 11

4.2 Policy approval procedure 11

4.3 Publication responsibilities 12

4.4 Petitions, Complaints, Claims and Requests 12

5. POLICY IDENTIFICATION 12

5.1. Policy Identification Criteria (OID) 12

5.2. The content of the certificates, distinguishing: 13

5.3. Policy OID 13

5.4. POLICIES ASSIGNED TO THIS DOCUMENT. 13

6. TYPES OF ECD GSE CERTIFICATES 14

7. REQUIREMENTS FOR ECD GSE DIGITAL CERTIFICATES 15

7.1. Generic Requirements 15

7.2. Specific Requirements 15

7.3. Specific Requirements: PKI Participants 15

7.4. Uses of the Certificates 16

7.5. Limits of Responsibility of the Open Certification Entity 17

7.6. Prohibitions on the Use of the Certificates 18

7.7. Specific Requirements Certificate Processing 18

7.8. Specific Requirement: Validity of the Certificates 20

7.9. Activities and Technical References of the Certificates 21

8. CHARACTERISTICS OF CRYPTOGRAPHIC DEVICES 25

8.1. Digital Certificate in Token 25

8.1.1 Features 25
8.1.2 Security commitments 26
8.1.3 Care of the cryptographic device 26
8.1.4 Associated risks 27
8.2. Digital Certificate in HSM - Hardware Security Module (Centralized Signature) 27
8.2.1. Technical Characteristics of Digital Certificates 28
Signature Algorithm 28
Content of the Digital Certificate 28
Life cycle of certificates 28
Key generation 28
Certification activities article 161 of the decree law 0019 of 2012 28
9. OBLIGATIONS 28
9.1.1. ECD GSE obligations 28
9.1.2. RA obligations 29
9.1.3. Obligations (Duties and Rights) of the Subscriber and/or Responsible Party 29
9.1.4. Obligations of Bona Fide Third Parties 31
9.1.5. Obligations of the Entity (Client) 31
9.1.6. Obligations of other DCE participants 31
10. PROTECTION OF PERSONAL INFORMATION 33
10.1. Personal Data Processing Policy 33
11. IMPARTIALITY AND NONDISCRIMINATION 33
12. DIGITAL CERTIFICATE ISSUANCE SERVICE FEES 34
12.1.1. Fees for issuance or renewal of certificates 34
13. MODELS AND MINUTES OF THE TERMS AND CONDITIONS DOCUMENTS .. 35
14. PROFILE OF THE CERTIFICATES 35

1. OBJECTIVE

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

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

In the event of any discrepancy between the terms of the CP and the CPS, the provisions of the CP shall be deemed to prevail over any conflicting terms set forth in the CPS.

2. SCOPE

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

3. INTRODUCTION

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

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

ECD GSE shall inform the Subscribers and/or Responsible Parties of the existence of this document where the CPs of the different certificates issued by ECD GSE are answered.

3.1. Summary

Policy for Digital Certificates Certificate, hereinafter **Policy** is a document prepared by **Gestión de Seguridad Electrónica S.A. (hereinafter GSE), acting as a Digital Certification Entity. (hereinafter GSE)** which, acting as a Digital Certification Entity, contains the rules, procedures that the **Digital Certification Entity (hereinafter GSE)** as a **Digital Certification Service Provider (PSC)** applies as guidelines 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 and the regulations that modify or complement them, in the territory of Colombia.

GESTIÓN DE SEGURIDAD ELECTRÓNICA SA DATA:

Company name:	GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.
Acronym:	GSE S.A.
Tax Identification Number:	900.204.272 - 8
Commercial Registry No:	01779392 of February 28, 2008
Certificate of Existence and Legal Representative:	https://gse.com.co/documentos/marco-regulatorio/Certificado-de-Existencia-y-Representante-Legal-GSE.pdf
Status of the commercial registry:	Active
Social address and correspondence:	Street 73 No. 7 - 31 Floor 3 Tower B Building el Camino
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

GSE has as its infrastructure service provider PKI - CA:

Company name:	PAYNET S.A.S
Acronym:	PAYNET
Tax Identification Number:	901.043.004-2
Commercial Registry No:	02766647 dated January 13, 2017.
Certificate of Existence and Legal Representative:	https://www.paynet.com.co/wp-content/uploads/Certificado-de-Existencia-y-Representante-Legal-Paynet.pdf
Status of the commercial registry:	Active
Social address and correspondence:	St 73 No. 7 - 31 Of 302
City / Country:	Bogotá D.C., Colombia
Phone 1:	+57 (1) 4053224
Fax:	+57 (1) 4053224
E-mail:	representante.legal@paynet.com.co
Website:	www.paynet.com.co

Reciprocal Digital Certification Entities

In accordance with the provisions of Article 43 of Law 527 of 1999, the 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 domestic 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 any reciprocity agreements in force.

3.2. Definitions and acronyms

3.2.1 Definitions

The following terms are commonly used and required for the understanding of this Policy. **Certification** Authority **(CA)**: Certification Authority, root entity and certification services 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 its identity and registration.

Time Stamping Authority **(TSA):** Certification body that provides time stamping services.

Reliable data archiving: This is the service that GSE offers its clients through a technological platform. In essence, it consists of a secure and encrypted storage space that can be accessed with credentials or a digital certificate. The documentation stored in 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 the signatory's identity. This is the definition of Law 527/1999, which in this document is extended to cases in which the linking of signature verification data is made to a computer component.

Specific Accreditation Criteria (CEA): Requirements that must be met to obtain the Accreditation as Digital Certification Entity - ECD, before the National Accreditation Body of Colombia - ONAC; i.e. 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.

Compromise of the private key: compromise 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 e-mail: Service that ensures the sending, reception and verification of electronic communications, ensuring at all times the characteristics of fidelity, authorship, traceability and non-repudiation of the same.

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

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

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 services of registration and time stamping of the transmission and reception of data messages, as well as fulfill other functions related to communications based on digital signatures.

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

a. Its use is not limited to the exchange of messages between the entity and the subscriber; or
b. He receives remuneration for them.

Closed Certification Entity: Entity that offers certification entity services 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 (one private and one public) that are obtained and shared through a trusted authority.

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

Trust hierarchy: A set of certification authorities that maintain trust relationships whereby a higher-level CCD guarantees the trustworthiness of one or more lower-level CCDs.

Certificate Revocation List **(CRL):** List **of** revoked certificates that have not expired.

Public Key and Private Key: The asymmetric cryptography on which PKI is based. It uses a pair of keys in which it is encrypted with one and can only be decrypted 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 person responsible for the certificate.

Private key (Private key): Numerical value or values that, used in conjunction with a known mathematical procedure, serve to generate the digital signature of a data message.

Public key (Public key): Numeric value or values that are used to verify that a digital signature was generated with the private key of the initiator.

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

Certification Policy (CP): A set of rules that define the characteristics of the different types of certificates and their use.

Certification Service Provider **(**CSP): Natural or legal person that issues digital certificates and provides other services related to digital signatures.

Online Certificate Status Protocol (OCSP): Protocol that allows online verification of the status of a digital certificate.

Repository: information system used to store and retrieve certificates and other related information.

Revocation: Process by which a digital certificate is disabled and loses validity.

Applicant: Any natural or legal person requesting the issuance or renewal of a Digital Certificate.

Subscriber and/or responsible party: Natural or legal person to whom the digital certification services are issued or activated and therefore acts as subscriber or responsible party thereof.

Bona fide third party: Person or entity other than the subscriber and/or responsible party who decides to accept and trust a digital certificate issued by ECD GSE.

TSA GSE: Corresponds to the term used by ECD GSE, in the provision of its Time Stamping service, as Time Stamping Authority.

3.2.2 Acronyms

CA: Certification Authority

CPS: Certification Practice Statement
CRL: Certificate Revocation List
CSP: Certification Service Provider
DNS: Domain Name System
FIPS: Federal Information Processing Standard
HTTP: The HyperText Transfer Protocol (HTTP) is the protocol used in every transaction on the World Wide Web (WWW). HTTP defines the syntax and semantics used by the software elements of the web architecture (clients, servers, proxies) to communicate. It is a transaction-oriented protocol and follows the request-response scheme 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, i.e. it is the secure version of HTTP.
IEC: International Electrotechnical Commission
IETF: Internet Engineering Task Force (Internet Standardization Body)
IP: Internet Protocol
ISO: International Organization for Standardization
OCSP: Online Certificate Status Protocol.
OID: Object identifier (Unique Object Identifier)
PIN: Personal Identification Number
PUK: Personal Unlocking Key
PKCS: Public Key Cryptography Standards. PKI standards developed by RSA Laboratories and accepted internationally.
PKI: Public Key Infrastructure
PKIX: Public Key Infrastructure (X.509)
RA: Registration Authority
RFC: Request For Comments (Standard issued by the IETF)
URL: Uniform Resource Locator

4. POLICY MANAGEMENT

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

4.1 Contact person:

Contact name:	Victor Armando Ibañez Palacios
Contact position:	Chief Operating Officer
Contact telephone numbers:	4050082 - 3232085097
E-mail:	victor.ibanez@gse.com.co info@gse.com.co

4.2 Policy Approval Procedure

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

4.3 Publishing responsibilities

Once the changes to the policies have been made and approved, it is the responsibility of the Operations Director and/or the Integrated Management System Process to request the process in charge to update the latest version of the policies on the web portals.

4.4 Petitions, Complaints, Grievances, Claims 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 handled 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 to subscribers, responsible and third parties.

Phone:	+57 (1) 4050082
E-mail:	pqrs@gse.com.co
Address:	Street 73 No. 7 - 31 Piso 3 Tower B Building el Camino
Website:	www.gse.com.co
Responsible:	Integrated Management System

Once the case is presented, it is transmitted with the information concerning the Integrated Management System process according to the internal procedure established for the investigation and management of these. Likewise, it is determined which area is responsible for taking corrective or preventive actions, in which case the action procedure must be applied.

Once the investigation has been generated, the response is evaluated and a decision is made to resolve the PQRS and its final communication to the subscriber, responsible party or interested party.

5. POLICY IDENTIFICATION

5.1. Policy Identification Criteria (OID)

The way to identify the different types of ECD GSE digital certificates is through object identifiers (OID's). A specific 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 dots and with a specific meaning for 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:

5.2. The content of the certificates, distinguishing:

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

The attribute is the specific characteristic of the natural person who holds the digital certificate that appears in the certificate and that can be of different types:

- of Company Membership
- Representation Company
- of Civil Service
- of Graduate Professional
- of Natural Person
- of Legal Entity
- of Electronic Invoice

Whoever generates the digital certificate keys, distinguishing between the certificate holder or the ECD GSE itself.

The procedure to update the information contained in the certificates must be executed in accordance with the provisions of the CPS "Certificate Renewal with change of keys", to perform the renewal of digital certificates, the procedure for requesting a new certificate must be executed. The subscriber must access the GSE products and services request web portal and start the certificate renewal request process in the same way as when he/she requested the certificate for the first time. Your information will be re-validated in order to update data if required.

5.3. Policy OID

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

OID	DESCRIPTION
1.3.6.1.4.1.31136.1.4.12	Certificate Policy for Digital Certificates

5.4. POLICIES ASSIGNED TO THIS DOCUMENT.

This document specifically provides answers to the CPs of the following certificates and their different subtypes:

- GSE-PE
- GSE-RE

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

6. TYPES OF ECD GSE CERTIFICATES

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

By virtue of this criterion, one or another information that constitutes the object of the certificate is guaranteed.

Thus, the digital certificates defined under this policy are the following:

TYPE OF DIGITAL CERTIFICATE	OBJECT
Company Membership	It guarantees the identity of the natural person who holds the certificate, as well as its link to a certain legal entity by virtue of the position he/she holds in it. This certificate will not grant by itself greater powers to its holder than those he/she possesses by virtue of the performance of his/her usual activity.
Company Representation	It is issued in favor of a natural person representing a specific legal entity. The certificate holder identifies himself not only as a natural person belonging to a company, but also adds his qualification as its legal representative.
Civil Service	It guarantees the identity of the natural person who holds the certificate, as well as his or her link to a Public Administration by virtue of his or her rank as a public official. This certificate shall not in itself grant greater powers to its holder than those he/she possesses by virtue of the performance of his/her usual activity.
Qualified Professional	It guarantees the identity of the natural person who holds the certificate, as well as his status as a qualified professional. This certificate shall not in itself grant greater powers to its holder than those he/she possesses for the performance of his/her usual activity within the scope of his/her profession.
Natural Person	It guarantees only the identity of the natural person.
Electronic Invoice	Exclusive certificate for electronic invoicing to meet the needs of companies and/or individuals 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, electronic payroll payment support document adjustment notes and other documents resulting from the processes of the unattended platforms of the technological suppliers approved

	by the DIAN, the DIAN's free invoicing system and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Legal Entity	Carrying out business procedures by an application running on a machine in automatic and unattended signature processes on behalf of a legal entity of public or private law that requires to guarantee the authenticity and integrity of the data sent or stored digitally and that will be represented by a person responsible for the certificate issued.

7. REQUIREMENTS FOR ECD GSE DIGITAL CERTIFICATES

ECD GSE does not prevent or inhibit the access of applicants to services as ECD, therefore a digital certificate can be requested regardless of the size of the applicant or subscriber, the type of existing linkage with ECD GSE, nor the 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 application for the service provided by ECD GSE.

7.1. Generic Requirements

The set of information detailed in the CPS on its security system, support, administration and issuance of Certificates, as well as on the trust relationship between the Subscriber and/or Responsible Party, the Applicant, the Receiving Entity or Bona Fide Third Party and the ECD constitute the generic requirements for the issuance of ECD GSE certificates.

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

7.2. Specific Requirements

Depending on the purpose of the different certificates, specific requirements are given regarding the following aspects:

Participating PKI (See Participating PKI): Depending on the different certificates will vary the Subscriber, Responsible, the Entity and the linkage (attribute) between these two figures.

Certificate Uses (See Certificate Uses): Depending on the different certificates, the use or scope of application will vary.

Processing of the Certificate (See Processing of the Certificate): Depending on the different certificates, the documentation accrediting their content varies.

7.3. Specific Requirements: PKI Participants

Based on the generic definitions established in the CPS regarding the figures of Subscriber and/or Responsible and Entity, the following is a detail of the natural or legal persons that 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
Company Membership	Natural person who belongs to the company and who is the certificate holder.	Company affiliation	Company with which the Subscriber is associated
Company Representation	Natural person who legally represents the company and who is the certificate holder.	Binding of legal representation to company	Company represented by the Subscriber
Civil Service	Natural person who belongs to a Public Administration and who is the certificate holder.	Civil servant relationship with a Public Administration	Public Administration to which the Subscriber is connected
Qualified Professional	Natural person practicing a licensed profession and holding a certificate	Practice of a registered profession and association with the Professional Association	Professional Association with which the Subscriber is affiliated
Natural Person	Natural person certificate holder	Not applicable	Not applicable
Electronic Invoice	Guarantees only the identity of the subscriber and/or person in charge.	Linking for electronic invoicing and/or electronic payroll	Subscriber and/or responsible party that requires electronic invoicing and/or electronic payroll
Legal Entity	Responsible for the certificate on behalf of a Legal Entity	Binding of legal representation to company	Company represented by the Subscriber and/or responsible party.

7.4. Uses of the Certificate s

Based on the generic definitions established in the CPS regarding 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

Party, and if applicable, also on the part of the Entity insofar as it can be deduced from the nature of the certificate attribute.

TYPE OF DIGITAL CERTIFICATE	SCOPE OF USES AND APPLICATIONS
Company Membership	Performance of business procedures by the subscriber and/or person in charge without implying representation. The company may establish limitations of use.
Company Representation	The subscriber and/or the person responsible for the subscriber's and/or the person in charge's name and on behalf of the company. The company may establish limitations of use.
Civil Service	Performance of procedures by the subscriber and/or person in charge in the exercise of his/her functions as a public official. The Public Administration may establish limitations of use.
Qualified Professional	Performance of procedures by the subscriber and/or person in charge in the exercise of his/her functions as a professional.
Natural Person	Performance of procedures by the subscriber and/or person in charge as a citizen. There is no connection with any entity.
Electronic Invoice	Subscriber and/or person responsible for electronic invoicing and/or electronic payroll
Legal Entity	Carrying out business procedures by an application running on a machine in automatic and/or unattended signature processes on behalf of a legal entity under public or private law that requires to guarantee 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 risk management study regarding the handling of cryptographic keys has been completed.

7.5. Limits of Responsibility of the Open Certification Entity

The limitations of liability of the Open Certification Entity are defined comprehensively in the disclaimer of liability section of the CPS, but based on the specific uses of each of the certificates established in the previous section. ECD GSE does not assume any other commitment or provide any other guarantee, nor does it assume any other liability to certificate holders or trusted third parties except as established by the provisions of this CP.

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

TYPE OF DIGITAL CERTIFICATE	LIMIT OF LIABILITY OF THE CERTIFICATION BODY
Company Membership	The digital certificates issued by ECD GSE can only be used for the purposes for which they have been issued and specified in the CPS and specifically in the numeral Use of certificate. Those uses that are not defined in the CPS and the CP are considered improper and consequently for legal purposes, ECD GSE is exempted from
Company Representation	
Civil Service	

TYPE OF DIGITAL CERTIFICATE	LIMIT OF LIABILITY OF THE CERTIFICATION BODY
Qualified Professional	any liability for the use of certificates in operations that are outside the limits and conditions established for the use of digital certificates according to the CPS, the CP and in accordance with the provisions of the Exemption from liability of the open certification entity.
Natural Person	
Electronic Invoice	
Legal Entity	

7.6. Prohibitions on the Use of Certificates

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

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

7.7. Specific Requirements Certificate Processing

Based on the operational requirements for the lifetime of the certificates established in the CPS regarding the processing of the certificate, the following establishes the documentation and accreditation standards necessary for the authentication of the data contained in each certificate:

- Law 527 of 1999, CHAPTER III Certificates.
- Law 527 of 1999, CHAPTER IV Subscribers of digital signatures, ARTICLE 39.

TYPE OF DIGITAL CERTIFICATE	REGISTRATION: DOCUMENTATION REQUESTED
The following documents will be requested for all types of certificates: • On-line application form completed. • Acceptance of terms and conditions. • Applicant's identification document • Sole Tax Registry - RUT	
Company Membership	• Document of Existence and Legal Representation of the Company valid for no more than thirty (30) days. • Applicant's labor certificate including position on institutional paper (not older than thirty (30) days).
Company Representation	• Document of Existence and Legal Representation of the Company valid for no more than thirty (30) days.
Civil Service	• To confirm the applicant's relationship with the Company, one of the following documents will be requested: ➢ Minutes of possession. ➢ Appointment resolution or decree. ➢ Service contract. ➢ Applicant's labor certificate including the position in institutional paper (no more than thirty (30) days from the filing of the application).
Qualified Professional	• Professional card and/or equivalent document. • Degree diploma (optional)
Natural Person	• In the event that the applicant does not have a Unique Tax Registration Number - RUT must present a document recording the address information that is issued by a third party verifier.
Electronic Invoice	Natural Person • In the event that the applicant does not have a Unique Tax Registration Number - RUT must present a document recording the address information that is issued by a third party verifier. In the case that the request is delegated by the Legal Representative and/or alternate to a third party, the letter of delegation for the request of the digital certificate must be attached.
	Legal Entity • Document of Existence and Legal Representation of the Company valid for no more than thirty (30) days. If the applicant does not have the document of existence and legal representation and is a public or state entity, the equivalent document(s) will be requested to validate the creation of the entity in accordance with the regulations in force and the respective administrative act (law, decree, resolution, among others). In the event that the request is delegated by the Legal Representative and/or alternate to a third party, the letter of delegation for the request of the digital certificate must be attached.

TYPE OF DIGITAL CERTIFICATE	REGISTRATION: DOCUMENTATION REQUESTED
Legal Entity	• Document of Existence and Legal Representation of the Company valid for no more than thirty (30) days s. If the applicant does not have the document of existence and legal representation and is a public or state entity, the equivalent document(s) will be requested to validate the creation of the entity in accordance with the regulations in force and the respective administrative act (law, decree, resolution, among others). In the event that the request is delegated by the Legal Representative and/or alternate to a third party, the letter of delegation for the request of the digital certificate must be attached.

Notes:

- The documents will be received scanned or in electronic original, preserving legibility for the use of the information.
- The document Registro Único Tributario - RUT will be requested in the updated DIAN format that includes a QR code.
- The applicant's domicile information: country, department, municipality and address will be reviewed in the documents: Document of Existence and Legal Representation or Registro Único Tributario - RUT.
- For the types of certificates where the Document of Existence and Legal Representation is requested, such document shall be valid for a period not exceeding thirty (30) days from the filing of the application.
- For the types of certificates where the Document of Existence and Legal Representation of the Company is requested, in those cases where it is required, an equivalent document will be valid where the existence and legal representation of the company can be validated, if applicable, the duly authenticated document will be requested.
- For the types of certificates where the applicant's RUT (Registro Único Tributario) is requested, in those cases where it is required, an equivalent document will be valid where the applicant's data and address data can be validated, if applicable, the document will be requested duly authenticated.
- All documents that are received authenticated, the authentication must be valid for no more than sixty (60) days from the filing of the request.
- In the cases that applications for digital certificates are submitted with additional and/or equivalent documents to the requested documentation, the documents mentioned in the Documentary Annex of Application Validation published in the web page in the section Support-Guides and Manuals-Application Validation will be taken into account for the review of the applications.

The procedure to process a digital certificate revocation request will be carried out under the provisions of the CPS in "Revocation and suspension of certificates".

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

7.8. Specific Requirement: Validity of the Certificates

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

7.9. Certificate Activities and Technical References

DIGITAL CERTIFICATION SERVICES	CERTIFICATION ACTIVITIES Article 161 of Decree Law 0019 of 2012 (2)	NORMATIVE OR TECHNICAL DOCUMENTS CEA Annexes
DIGITAL CERTIFICATES FOR COMPANY MEMBERSHIP	1. Issue certificates in connection with electronic or digital signatures of natural or legal persons. 2. Issue certificates on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents. 3. Issue certificates in relation to the person who has a right or obligation with respect to the documents set forth in paragraphs f) and g) of Article 26 of Law 527 of 1999.	RSA 2048 RSA 4096 SHA-256 Minimum key size 2048 bits August 2002 RFC 5280 May 2008 ITU-T-X509 October 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 November 2003 RFC 6960 June 2013 FIPS 140-2 Level 3 May 2001 (RSA - local devices) FIPS 140-2 Level 3 May 2001 (RSA - centralized)
		In centralized devices with Algorithm ECDSA ECDSA P-256 ECDSA P-384 RFC 5280 May 2008 RFC 3279 April 2002 RFC 5480 March 2009 ITU -T- X.509 v3 October 2016 ITU -T-X.500 October 2019 RFC 3647 November 2003 RFC 6960 June 2013 RFC 5758 January 2010 FIPS PUB 186-4 July 2013 SEC 2: Recommended Elliptic Curve Domain Parameters January 2010 FIPS 140-2 Level 3 May 2001 (ECDSA - Centralized)
DIGITAL CERTIFICATES FOR COMPANY REPRESENTATION .	1. Issue certificates in connection with electronic or digital signatures of natural or legal persons. 2. Issue certificates on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents. 3. Issue certificates in relation to the person who has a right or obligation with respect to the documents set forth in paragraphs f) and g) of Article 26 of Law 527 of 1999.	On Local or Centralized devices with RSA Algorithm RSA 2048 RSA 4096 SHA-256 Minimum key size 2048 bits August 2002 RFC 5280 May 2008 ITU-T-X509 October 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 November 2003 RFC 6960 June 2013 FIPS 140-2 Level 3 May 2001 (RSA - local devices) FIPS 140-2 Level 3 May 2001 (RSA - centralized)
		In centralized devices with Algorithm ECDSA ECDSA P-256 ECDSA P-384 RFC 5280 May 2008 RFC 3279 April 2002 RFC 5480 March 2009 ITU -T- X.509 v3 October 2016 ITU -T-X.500 October 2019

DIGITAL CERTIFICATION SERVICES	CERTIFICATION ACTIVITIES Article 161 of Decree Law 0019 of 2012 (2)	NORMATIVE OR TECHNICAL DOCUMENTS CEA Annexes
		RFC 3647 November 2003 RFC 6960 June 2013 RFC 5758 January 2010 FIPS PUB 186-4 July 2013 SEC 2: Recommended Elliptic Curve Domain Parameters January 2010 FIPS 140-2 Level 3 May 2001 (ECDSA - Centralized)
DIGITAL CERTIFICATES OF PUBLIC FUNCTION	1. Issue certificates in connection with electronic or digital signatures of natural or legal persons. 2. Issue certificates on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents. 3. Issue certificates in relation to the person who has a right or obligation with respect to the documents set forth in paragraphs f) and g) of Article 26 of Law 527 of 1999.	On Local or Centralized devices with RSA Algorithm RSA 2048 RSA 4096 SHA-256 Minimum key size 2048 bits August 2002 RFC 5280 May 2008 ITU-T-X509 October 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 November 2003 RFC 6960 June 2013 FIPS 140-2 Level 3 May 2001 (RSA - local devices) FIPS 140-2 Level 3 May 2001 (RSA - centralized)
		In centralized devices with Algorithm ECDSA ECDSA P-256 ECDSA P-384 RFC 5280 May 2008 RFC 3279 April 2002 RFC 5480 March 2009 ITU -T- X.509 v3 October 2016 ITU -T-X.500 October 2019 RFC 3647 November 2003 RFC 6960 June 2013 RFC 5758 January 2010 FIPS PUB 186-4 July 2013 SEC 2: Recommended Elliptic Curve Domain Parameters January 2010 FIPS 140-2 Level 3 May 2001 (ECDSA - Centralized)
DIGITAL CERTIFICATES OF QUALIFIED PROFESSIONAL	1. Issue certificates in connection with electronic or digital signatures of natural or legal persons. 2. Issue certificates on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents. 3. Issue certificates in relation to the person who has a right or obligation with respect to the documents set forth in paragraphs f) and g) of Article 26 of Law 527 of 1999.	On Local or Centralized devices with RSA Algorithm RSA 2048 RSA 4096 SHA-256 Minimum key size 2048 bits August 2002 RFC 5280 May 2008 ITU-T-X509 October 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 November 2003 RFC 6960 June 2013 FIPS 140-2 Level 3 May 2001 (RSA - Local Devices)

DIGITAL CERTIFICATION SERVICES	CERTIFICATION ACTIVITIES Article 161 of Decree Law 0019 of 2012 (2)	NORMATIVE OR TECHNICAL DOCUMENTS CEA Annexes
		FIPS 140-2 Level 3 May 2001 (RSA - centralized)
		In centralized devices with Algorithm ECDSA ECDSA P-256 ECDSA P-384 RFC 5280 May 2008 RFC 3279 April 2002 RFC 5480 March 2009 ITU -T- X.509 v3 October 2016 ITU -T-X.500 October 2019 RFC 3647 November 2003 RFC 6960 June 2013 RFC 5758 January 2010 FIPS PUB 186-4 July 2013 SEC 2: Recommended Elliptic Curve Domain Parameters January 2010 FIPS 140-2 Level 3 May 2001 (ECDSA - Centralized)
DIGITAL CERTIFICATES FOR NATURAL PERSONS	1. Issue certificates in connection with electronic or digital signatures of natural or legal persons. 2. Issue certificates on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents. 3. Issue certificates in relation to the person who has a right or obligation with respect to the documents set forth in paragraphs f) and g) of Article 26 of Law 527 of 1999.	On Local or Centralized devices with RSA Algorithm RSA 2048 RSA 4096 SHA-256 Minimum key size 2048 bits August 2002 RFC 5280 May 2008 ITU-T-X509 October 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 November 2003 RFC 6960 June 2013 FIPS 140-2 Level 3 May 2001 (RSA - Local Devices) FIPS 140-2 Level 3 May 2001 (RSA - centralized)
		In centralized devices with Algorithm ECDSA ECDSA P-256 ECDSA P-384 RFC 5280 May 2008 RFC 3279 April 2002 RFC 5480 March 2009 ITU -T- X.509 v3 October 2016 ITU -T-X.500 October 2019 RFC 3647 November 2003 RFC 6960 June 2013 RFC 5758 January 2010 FIPS PUB 186-4 July 2013 SEC 2: Recommended Elliptic Curve Domain Parameters January 2010 FIPS 140-2 Level 3 May 2001 (ECDSA - Centralized)
DIGITAL CERTIFICATES FOR ELECTRONIC INVOICING	1. Issue certificates in connection with electronic or digital signatures of natural or legal persons.	On Local or Centralized devices with RSA Algorithm RSA 2048

DIGITAL CERTIFICATION SERVICES	CERTIFICATION ACTIVITIES Article 161 of Decree Law 0019 of 2012 (2)	NORMATIVE OR TECHNICAL DOCUMENTS CEA Annexes
.	2. Issue certificates on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents. 3. Issue certificates in relation to the person who has a right or obligation with respect to the documents set forth in paragraphs f) and g) of Article 26 of Law 527 of 1999.	RSA 4096 SHA-256 Minimum key size 2048 bits August 2002 RFC 5280 May 2008 ITU-T-X509 October 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 November 2003 RFC 6960 June 2013 FIPS 140-2 Level 3 May 2001 (RSA - local devices) FIPS 140-2 Level 3 May 2001 (RSA - centralized)
		In centralized devices with Algorithm ECDSA ECDSA P-256 ECDSA P-384 RFC 5280 May 2008 RFC 3279 April 2002 RFC 5480 March 2009 ITU -T- X.509 v3 October 2016 ITU -T-X.500 October 2019 RFC 3647 November 2003 RFC 6960 June 2013 RFC 5758 January 2010 FIPS PUB 186-4 July 2013 SEC 2: Recommended Elliptic Curve Domain Parameters January 2010 FIPS 140-2 Level 3 May 2001 (ECDSA - Centralized)
DIGITAL CERTIFICATES FOR LEGAL ENTITIES	1. Issue certificates in connection with electronic or digital signatures of natural or legal persons. 2. Issue certificates on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents. 3. To issue certificates in relation to the person who has a right or obligation with respect to the documents set forth in paragraphs f) and g) of Article 26 of Law 527 of 1999.	On Local or Centralized devices with RSA Algorithm RSA 2048 RSA 4096 SHA-256 Minimum key size 2048 bits August 2002 RFC 5280 May 2008 ITU-T-X509 October 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 November 2003 RFC 6960 June 2013 FIPS 140-2 Level 3 May 2001 (RSA - Local Devices) FIPS 140-2 Level 3 May 2001 (RSA - centralized)
		In centralized devices with Algorithm ECDSA ECDSA P-256 ECDSA P-384 RFC 5280 May 2008 RFC 3279 April 2002 RFC 5480 March 2009 ITU -T- X.509 v3 October 2016 ITU -T-X.500 October 2019 RFC 3647 November 2003 RFC 6960 June 2013 RFC 5758 January 2010 FIPS PUB 186-4 July 2013

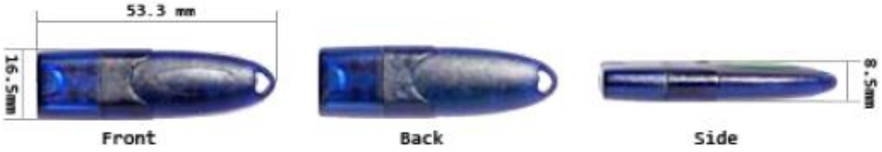
DIGITAL CERTIFICATION SERVICES	CERTIFICATION ACTIVITIES Article 161 of Decree Law 0019 of 2012 (2)	NORMATIVE OR TECHNICAL DOCUMENTS CEA Annexes
		SEC 2: Recommended Elliptic Curve Domain Parameters January 2010 FIPS 140-2 Level 3 May 2001 (ECDSA - Centralized)

8. 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.

8.1. Digital Certificate in Token

8.1.1 Features



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

8.1.2 Security commitments

Due to circumstances affecting the security of the cryptographic device:

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

8.1.3 Care of the cryptographic device

- Keep it in a dry place and away from ambient and/or temperature variations.
- Do not expose to magnetic fields.
- Avoid being hit or subjected to any physical effort.
- Do not attempt to open it, remove the plastic protection or circuit board, as this will cause it to malfunction.
- Do not put it in water or other liquids.

- Notify the ECD - GSE in case of theft, robbery, loss and/or fraud of the token in order to revoke the digital certificate.

8.1.4 Associated risks

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

- Loss of the device.
- Key commitment.
- Damage due to improper handling.
- Damage due to the device not being protected from environmental conditions.
- Damage due to voltage variation.

To mitigate the associated risks 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.
- Failure to enter the PIN incorrectly more than three (3) times will lock the device.
- Cryptographic devices must be kept in suitable environmental conditions.
- In case of compromise or loss of the private key, you must request the revocation of the digital certificate.

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

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

8.2.1. Technical Characteristics of Digital Certificates

FEATURE	TECHNICAL SPECIFICATION
Signature Algorithm	SHA256 *Hash function* with RSA Encryption. SHA384 *Hash function* with ECDSA
	Encryption Function • RSA with a key length of 4096 for CA RAIZ • RSA with key length of 4096 for SUBORDINATE CA • RSA with subscriber/responsible key length of 2048. • ECDSA with a key length of 384 for CA RAIZ • ECDSA with key length of 384 for CA SUBORDINATE • ECDSA with subscriber/responsible key length of 256.
Content of the Digital Certificate	• RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. May 2008. • ITU-T-X509 October 2016 • ETSI TS 102 042 - Policy requirements for certification authorities issuing public key.
Life cycle of certificates	• RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
Key generation	• FIPS 140-2 Level 3 token • HSM FIPS 140-2 Level 3 (Centralized Signature)
Certification activities article 161 of decree law 0019 of 2012	1. Issue certificates in connection with electronic or digital signatures of natural or legal persons. 2. Issue certificates on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents. 3. To issue certificates in relation to the person who has a right or obligation with respect to the documents set forth in paragraphs f) and g) of Article 26 of Law 527 of 1999.

9. OBLIGATIONS

9.1.1. Obligations of the ECD GSE

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

a) Respect the provisions of current regulations, the CPS and the Certificate Policies.
b) Publish the CPS and each of the Certificate Policies on the GSE website.
c) Inform ONAC of modifications to the CPS and Certificate Policies.
d) Maintain the CPS and Certificate Policies with their latest version published on the GSE website.
e) Protect and safeguard your private key in a secure and responsible manner.

f) Issue certificates in accordance with the Certificate Policies and standards defined in the CPS.
g) Generate certificates consistent with the information provided by the applicant or subscriber.
h) Keep the information on 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 digital certificates issued in an open access repository.
k) Failure to maintain 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 revoked digital certificates CRL with the latest revoked certificates.
n) Notify the Applicant, Subscriber or Entity of the revocation of the digital certificate within 24 hours after the revocation of the digital certificate in accordance with the digital certificate revocation policy.

9.1.2. Obligations of the RA

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

a) Know and comply with the provisions of the CPS and the Certificate Policy corresponding to each type of certificate.
b) Custody and protection of your private key.
c) To verify the identity of the Applicants, Responsible or Subscribers of digital certificates.
d) Verify the accuracy and authenticity of the information provided by the Applicant.
e) File and keep custody of the documentation provided by the applicant or subscriber, during the time established by the legislation in force.
f) Respect the provisions of the contracts signed between ECD GSE and the subscriber.
g) Identify and report to the ECD GSE the causes of revocation provided by the applicants on the digital certificates in force.

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

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

a) Use your digital certificate according to the terms of the CPS.
b) Verify within the next business day that the digital certificate information is correct. In case of inconsistencies, notify the ECD.

c) Refrain from: lending, transferring, writing, publishing the password for use of its digital certificate and take all necessary, reasonable and appropriate 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 Digital Certificate Application Form to facilitate its timely and full identification.
f) To request the revocation of the Digital Certificate upon change of name and/or surname.
g) To request the revocation of the Digital Certificate when the Subscriber has changed its nationality.
h) Comply with the accepted and signed in the terms and conditions document or responsible for digital certificates.
i) Provide accurate and truthful information as required.
j) To inform during the validity of the digital certificate any change in the data initially provided for the issuance of the certificate.
k) Responsible custody and protection of your private key.
l) Use the certificate in accordance with what is established in this CP for each type of certificate.
m) Request as subscriber or responsible immediately the revocation of its digital certificate when it has knowledge that there is a cause defined in numeral *Circumstances for the revocation of a certificate of* the DPC.
n) Not to make use of the private key or the digital certificate once its validity has expired or it has been revoked.
o) Inform trusted third parties of the need to check the validity of the digital certificates they are using at any given time.
p) Inform the bona fide third party to verify the status of a certificate has the list of revoked certificates CRL, published periodically by ECD GSE.
q) Not to use its digital certification in a way that contravenes the law or brings ECD into disrepute.
r) Not to make any statement related to its digital certification in the ECD GSE may consider misleading or unauthorized, as provided by the CPS and CP.
s) Once the digital certification service has expired or been revoked, the subscriber must immediately stop using it in all advertising material containing 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 inform that it complies with the requirements specified in the CPS CPs, indicating the version.

On the other hand, you have the following rights:

a) Receive the digital certificate within the times established in the CPS.
b) The subscriber may use the marks of conformity and information related to the digital certification service provided by ECD GSE in communication media, such as documents, brochures or advertising, as long as it complies with the requirements of the previous paragraph.

c) Request information regarding applications in process.
d) Request revocation of the digital certificate by providing the necessary documentation.
e) Receive the digital certificate in accordance with the scope granted by ONAC to GSE.

9.1.4. Obligations of Bona Fide Third Parties

Bona fide Third Parties in their capacity as a party relying on digital certificates issued by ECD GSE are under the obligation to:

a) To know the provisions on Digital Certification in the current regulations.
b) To be familiar with the provisions of the CPS and CP.
c) Verify the status of the certificates before performing operations with digital certificates.
d) Verify the CRL Revoked Certificate List before performing operations with digital certificates.
e) To know and accept the conditions about guarantees, uses and responsibilities when performing operations with digital certificates.

9.1.5. Obligations of the Entity (Client)

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

As established in the Certificate Policies, in the case of certificates where the relationship of the Subscriber or Responsible Party with the same is accredited, it shall be the obligation of the Entity:

a) Apply to the RA GSE for the suspension/revocation of the certificate when such linkage ceases or is modified.
b) All those obligations related to the person in charge of the digital certification service.
c) The entity when referring to the digital certification service provided by ECD GSE in communication media, such as documents, brochures or advertising, must inform that it complies with the requirements specified in the CPS CPs.
d) The entity may use the marks of conformity and information related to the digital certification service provided by ECD GSE in communication media, such as documents, brochures or advertising, as long as it complies with the requirements of the previous paragraph.

9.1.6. Obligations of other DCE participants

The Management Committee and the Integrated Management System process as internal bodies of ECD GSE are obliged to:
a) Review the consistency of the CPS with current regulations.
b) Approve and decide on the changes to be made to the digital certification services, due to regulatory decisions or requests from subscribers or responsible parties.

c) Approve the notification of any change to subscribers and/or responsible parties analyzing its legal, technical or commercial impact.
d) Review and take action on any comments made by subscribers or responsible parties when a change in the digital certification service is made.
e) Report action plans to ONAC and SIC on all changes that have an impact on the PKI infrastructure and affect digital certification services, in accordance with RAC-3.0-01.
f) Authorize the required changes or modifications to the CPS.
g) Authorize the publication of the CPS 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 ECD GSE's technological infrastructure.
k) Request the revocation of a certificate if it has knowledge or suspicion of the compromise of the private key of the subscriber, entity or any other fact that tends to misuse the private key of the subscriber, entity or the ECD itself.
l) Be aware of and take appropriate action when security incidents occur.
m) Perform a review of the CPS at least once a year 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 the proper use in documents or in any other publicity that the 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 its critical suppliers and reciprocal ECD, if any, are kept informed of the obligation to comply with the CEA requirements, in the corresponding numbers.
s) The Integrated Management System process will implement preventive and corrective action plans to respond to any risk that compromises ECD's impartiality and non-discrimination, whether arising from the actions of any person, body, organization, activities, its relationships or the relationships of its personnel or itself. It uses the ISO 31000 standard to identify 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 that may compromise their impartiality.
u) Document and demonstrate commitment to fairness and non-discrimination.
v) Ensure that the administrative, management and technical personnel of the PKI, of the ECD associated with the consulting activities, maintain complete independence and autonomy with respect to the personnel of the review process and decision making on the certification of the ECD itself.

w) Ensure that critical suppliers such as the ECD reciprocal and datacenter that comply with the ECD accreditation requirements are kept informed in order to support their contracting and compliance with the administrative and technical requirements requested.

10. PROTECTION OF PERSONAL INFORMATION

10.1. Personal Data Processing Policy

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

11. IMPARTIALITY AND NON-DISCRIMINATION

ECD GSE, headed by 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 stakeholders and external parties, 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 Body of Colombia (ONAC), so the following compliance mechanisms are established:

- The Management Committee and the employees of GSE declare that they do not participate directly or indirectly in services or activities that could jeopardize free competition, accountability and transparency.
- Employees will use preventive and corrective actions to respond to any risk that compromises the company's impartiality.
- The collaborators that are part of the accredited digital certification services may not provide consulting services, nor involve the development team to provide technical support services to the subscriber or customer.
- 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 natural or legal persons related to groups outside the law or that develop illegal activities.
- GSE may decline to accept an application or maintain a contract for certification when there are substantiated, demonstrated or improper 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 digital certifications already issued.

Note: Any case that jeopardizes the impartiality of ECD GSE as an ECD or of its staff, body or organization shall be brought to the attention of the Integrated Management System Process.

In accordance with the provisions of the GSE ECD Fairness and Non-Discrimination Policy, which can be found on the GSE website in the Fairness and Non-Discrimination Policy section at the following url: https://gse.com.co/politicas/.

12. DIGITAL CERTIFICATE ISSUANCE SERVICE FEES

12.1.1. Certificate issuance or renewal fees

Product detail Digital Certificates	Delivery time	Validity	Price excluding VAT	VAT	Total
Natural Person	Normal	1	$ 191.597	$ 36.403	$ 228.000
Natural Person	Normal		$ 277.310	$ 52.689	$ 329.999
Belonging to Company	Normal	1	$ 191.597	$ 36.403	$ 228.000
Belonging to Company	Normal		$ 277.310	$ 52.689	$ 329.999
Qualified Professional	Normal	1	$ 191.597	$ 36.403	$ 228.000
Qualified Professional	Normal		$ 277.310	$ 52.689	$ 329.999
Company Representative	Normal	1	$ 191.597	$ 36.403	$ 228.000
Company Representative	Normal		$ 277.310	$ 52.689	$ 329.999
Public Function	Normal	1	$ 191.597	$ 36.403	$ 228.000
Public Function	Normal		$ 277.310	$ 43.907	$ 274.999
Legal Entity	Normal	1	$ 504.202	$ 95.798	$ 600.000
Legal Entity	Normal		$ 857.143	$ 162.857	$ 1.020.000
Electronic Invoicing	Normal	1	$195.357	$37.117	$232.474
Electronic Invoicing	Normal		$275.523	$52.349	$327.872

*These prices do not include V.A.T. and are calculated on a one-year term. The figures indicated here for each type of certificate may vary according to special commercial agreements that may be reached with subscribers, entities or applicants, in the development of promotional campaigns carried out by GSE.

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

*The ECD GSE makes available the issuance of digital certificates with validity in days or months without exceeding 24 months, the sale prices of these certificates will be agreed with the customer after negotiation.

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

13. MODELS AND MINUTES OF TERMS AND CONDITIONS DOCUMENTS

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

14. CERTIFICATE PROFILE

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

OID (Object Identifier)	1.3.6.1.4.1.31136.1.4.12
Location of the PC	https://gse.com.co/documentos/calidad/politicas/Certificate_Policies_for_Digital_Certificate_Services_V12.pdf