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

CERTIFICATION PRACTICE STATEMENT

Code	Name	Version	Classification of information
POP-DT-58	Certification Practices Statement	17	Public

Document Title	**Certification Practices Statement**
Version	17
Working Group	Management Committee
Document status	final
Issue date	01/11/2016
Effective Date	08/07/2024
OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.1.17
DPC Location	https://ase.com.co/documentos/calidad/DPC/Declaration of Certification Practices V17.pdf
Prepared	Operations Manager
Reviewed	Integrated Management System
Approved	Management Committee

Change Control

Version	Date	Change/Modification
1	01-11-2016	Initial document
2	04-10-2017	• ECD Contact Information and Logo Update • Updating Enrollment Entities • Update contact information Certification service providers • Information regarding the General Director of GSE. TSA GSE data update.
3	03-04-2018	Update information and adjustments in relation to CEA-4.1-10 in accordance with the review of the requirements matrices.
4	27-11-2018	Changed from V3 to V4 on 11/27/2018. Update of the table of contents, information and adjustments regarding new charges, rates, access routes to the website, correction of the subordinate clause, the phrase established and tested is included, numeral 8.7.4 is expanded by naming the technological mechanisms used for data protection, all certification policies are listed, terms are changed and the legal representative is updated.
5	12-04-2019	The EE section was removed, and it was clarified that, in order to use the centralized signature certificate, it is necessary to acquire a technological platform with additional costs. The clarification is made in section 1.6.2 of the requirements and restrictions of the RA.

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. August 30th, 2024

		and Criteria and methods for evaluating applications. RA roles have been updated
6	07/06/2019	Clarification of the scope of accreditation under the CPD 1.1 Summary 4.1 Application for the certificate, the procedure for accessing the service is clarified. 4.1.1 Clarification of non-discrimination when accessing the service. 8.9.3 Clarification of rights of the subscriber or controller
7	03/31/2020	The DPC is adjusted to the changes generated by the new platforms, the objective and scope numerals are added, the price list is adjusted, the links are modified to point to the new routes, the Legal Representative is changed and the services accredited by ONAC are listed in a more specific manner.
8	08/14/2020	Everything related to the Digital Signature Generation service is eliminated, another condition is added in section 5.2.2 Authentication of the identity of an entity, for the renewal of digital signature certificates and the services used for identity validation are mentioned.
9	12/02/2021	The link to consult the Certificate of Existence and Legal Representation for the ECD and the current CA (Paynet SAS) online has been included. Detailed information on the current CA (Paynet SAS) and the historical CA (Indenova) has been included in accordance with the provisions of item 1 of section 10.7 of CEA 4.1-10. The information on the data centers has been modified in accordance with the provisions of the ONAC accreditation certificate. The paragraph on the renewal of digital certificates in sections 5.2.2 and 5.2.3 has been removed. The following sections have been updated: • 6.4.2 Approval or rejection of certificate requests • 6.4.3 Deadline for processing certificate requests • 7.10.1 Trusted Roles • 8.1.4 Delivery of the ECD public key to accepting third parties Links have been updated to point to the new routes
10	07/16/2021	The following numerals were updated: 3.6.1 Authority Certification (CA), data center provider data. 4.1 Repositories Section 6.5.6 was updated. 6.5.7 Deadline for processing requests for certificate 6.8.2 Use of the private key and certificate by bona fide third parties 6.12 Revocation and suspension of certificates 6.12.3 Revocation request procedure 6.13.1 Description of the content of the certificates Subordinate Authority 01 GSE 6.13.1.8 Object identifiers (OID) of the algorithms 6.14.1.3 CRL Availability 6.14.1.7 OCSP Availability 6.14.3 Optional Features 7.10.1 Trusted Roles 8.1.4 Delivery of the ECD public key to third party acceptors 8.1.5 Key size 8.1.6 Key generation parameters public and quality verification 8.2.4 Backup of the private key 8.2.5 Private key file 8.2.6 Transferring the private key from the

		cryptographic module 8.2.7 Storing private keys in a cryptographic module 8.5.3 Actions in the event of an event or information security incident 10. DESCRIPTION OF PRODUCTS AND SERVICES, Archive Service, Registry, Conservation, Custody and Annotation for the Electronic Documents 11.7.1 Data Processing Policy Personal 11.3 Impartiality and Non-Discrimination 14. ANNEX 1 DPC TECHNICAL PROFILE MATRIX DIGITAL CERTIFICATES 15. ANNEX 2 TERMS AND CONDITIONS OID and query links have been updated for: • Certification Practices Statement • Certificate Policies for Digital Certificates • Certificate Policies for Time Stamping Service • Certificate Policies for Archiving, Registration, Conservation, Custody and Annotation Service of Transferable Electronic Documents and Data Messages. • Certificate Policies for Certified Email Service
11	10/5/2021	• The numerals were updated including electronic signature: 6.1 Request for certificate 6.5 Initial identity validation 6.5.1 Method to prove possession of the private key 10 Description of Products and Services 11.1.1 Fees for issuing or renewing certificates 11.9.3 Obligations of the Subscriber and/or Responsible Party. • The following numerals were included referring to electronic signature: 5.1.1.1.1 Electronic Signature 5.1.1.2.2 ECD GSE Subscriber Certificates (Technical profile matrix for electronic signature certificates) 13 Certification Policies 16 Annex 3 DPC technical profile matrix electronic signature certificates • include an explanatory note on the validation of the OCSP in sections 4.1, 4.3, 6.12.9, 6.12.10, 6.14.3. • Section 6.12.3 Revocation request procedure was updated by adding a new online revocation channel. • Section 8.3.2 was updated to clarify the period of Validate the root and subordinate keys of the RSA and ECDSA algorithm • OID and query links are updated
12	10/27/2021	• modify numeral 6.5 of Identity Validation • The OID and the PC link for Digital Certificates have been updated • The OID and DPC link have been updated with this new version.
13	05/31/2022	According to the new version of CEA, adjustments were made to the following sections: • 3.1 Summary: It I remove the 4.1-10 leaving only CEA. • 3.2. Petition, complaint, claimand requests: The term appeal was removed. • 3.6 PKI Participants: Eliminated as CA Indenova. • 5.1.1.1 - 5.1.1.2 Name Types: Root and subordinate certificates are removed from Indenova and those related to the elliptic curve are included. • 6.5 Initial Identity Validation: It is include a final paragraph on the consumption of confrontation in services.

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. August 30th, 2024

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

		• 6.13.1 Description of the content of the certificates: I include the subject's alternative name field. • 6.13.1.7 Removed 3 key purposes. • 7.10.1 Trusted Roles: The roles of RA Agents, RA Administrator, and RA Auditor have been modified: • 7.16 Termination of an ECD: modified according to what is required in the new CEA. • 9.2 Auditor identity/qualification: Assurance requirements have been modified. • 10. Description of products and services: The centralized signature certificate was eliminated, the name of the Archive service was modified, and the electronic signature generation service was modified in accordance with the accreditation certificate. • 11.4. It modify exemption by limits of liability. • 11.9.6 Obligation of other participants: modify item r) by eliminating 4.1-10, leaving only CEA. • 15. It I modify the name of the annex on terms and conditions. • 16. It I include this item from the technical annex of the electronic signature certificate. • The OID and the PC link for Digital Certificates have been updated • The OID and DPC link have been updated with this new version. • include the quality code in the header of the document.
14	09/23/2022	• 3.1 Summary: The chapters of the Durscit. • The address of the ECD was modified in the items 3.1, 3.2, 3.6.2 and 3.7.1. •modify the address of Paynet SAS in items 3.6.1 and 3.6.7.2. • modify numeral 3.6.4 changing the responsible party to a third party in good faith • include numeral 3.6.4.1 Precautions that third parties must observe • modify numeral 6.4.1 Performance of identification and authentication functions • modify section 6.5.1 Method to demonstrate possession of the private key, providing clarity in case the applicants generate the key pair in tr own infrastructure. • modify section 6.5.5 Criteria for interoperability • modify section 6.12.7 Frequency of updating CRLs according to the availability percentage established in the new CEA. • modify RFC 2560 to RFC 6960 in sections 6.12.10 Online revocation checking requirements, 6.14.1.4 OCSP profile and 6.14.1.5 Version number. • modify numeral 7.7. Storage system making it clear that the servers are in cloud environments. • modify numeral 7.4. Exposure to water, clarifying that it refers to data centers. of the PKI. •Modify section 7.16. Cessation of an ECD by including a paragraph on the safety plan for the cessation of activities. • modify section 11.4 Limits of liability including Liability for the veracity of the Subscriber's information, Liability for the availability of the service, Liability for the functionality of the service in the Subscriber's infrastructure, Liability for computer crimes. • modify numeral 11.9.1 Obligations of
		the ECD GSE including items o) to y).

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

		• Sections 12.3 Notice and Communication, 12.5 Dispute Prevention and Resolution, 12.6 Applicable Law, and 12.7 Compliance with Applicable Law were included. • The OID and the PC link for Digital Certificates have been updated • The OID and DPC link have been updated with this new version.
15	05/10/2023	• modify the entire order of the document according to the numerals of RFC 3647. • It was eliminated Pay net SAS as the CA authority since the PKI was moved to the GSE ECD. • change the Director of Operations to the Operations Manager • The data of the main and alternate datacenter leaving Hostdime and Claro.
16	10/24/2024	• Section 1.1.6.2 Acronyms is modified: The acronym RNEC is included • Section 1.3.1.3 is modified. It includes: pseudonymous and pseudoanonymous, the nicknames are expanded. • Section 1.3.2 is modified: Section information is updated. • Section 1.3.2.3 is modified: Information on requirements for the identification and authentication of an individual's identity is included. • Section 1.3.2.4 is modified. The information in the section is updated. • Section 1.3.2.5 is modified. The word recommendation is eliminated. • Section 1.3.3.1 is modified. Identification and authentication requirements for routine key generation are adjusted. • Section 1.4.1 is modified. The ECD and information from fully reliable databases are included. • Section 1.4.2.1 is modified. The word information is included. • Number 1.4.3.2 is modified. The words defined and authorized are included. • Section 1.4.4.1 is modified. The word inform and/or is included. • Number 1.4.7.2 is modified: The term duly authorized and/or proxies is included • Number 1.4.7.3 is modified. The means or mechanisms for collecting ECD information are updated. • Number 1.4.7.4 is modified. The means to notify the subscriber are updated. • Number 1.4.9.3 is modified. Online revocation request information is updated. • Number 1.4.9.11 is modified. The means to notify the subscriber are updated. • Number 1.4.12.3 is modified. The service desk is included for cases of forgetting PIN • Number 1.5.2.2 is modified. The information of the people required by role is adjusted. • Number 1.5.7.2 is modified. GSE is included. • Number 1.5.7.3 is modified. GSE is included. • Number 1.7.1 is modified. Number information is updated. • Number 1.9.3.4 is modified. Information relating to the TRD is updated. • Section 1.9.4.1 is modified. Rules related to the processing of personal data are included. • Number 1.9.4.5 is modified. The wording of the number is adjusted. • Number 1.9.4.6 is modified. The wording of the number is adjusted. • Number 1.9.11.2 is modified. Literal c is adjusted. • Number 1.14 is modified OID is updated and

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. August 30th, 2024

		Location of the Certificate Policy for Digital Certificates
17	08/07/2024	• Section 1.1 is modified and the telephone code is updated. • Section 1.1 is modified and eliminates the fax • OIDs of the entire document are updated • The numbering and order are updated according to numeral 6 Outline of a set of provisions of RFC 3647 • IT process name is updated by technology • Section 3.2 Initial identity validation is modified (Information verification method is included) • Section 3.2 is modified. Information on verification mechanisms is adjusted. • Section 4.1 Certificate request is modified: procedure code is updated • Section 4.10.2 is modified. Information on service availability is included and related numbering is adjusted. • Section 4.12 is modified. The text "storage of the private key to a responsible person" is eliminated since it was repeated.

Table of Contents

Table of Contents

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. August 30th, 2024

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

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. August 30th, 2024

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

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. August 30th, 2024

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. August 30th, 2024

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original. August 30th, 2024

1. INTRODUCTION.

1.1 General Description

The Certification Practice Statement (CPS) - Global Certification Authority Root GSE (hereinafter CPS) is a document prepared by Gestión de Seguridad Electrónica SA (hereinafter GSE) which, acting as a Digital Certification Entity, contains the standards, statements on policies and procedures that the Digital Certification Entity (hereinafter ECD GSE) as a Digital Certification Services Provider (PSC) applies as a guideline to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014 and the regulations that modify or complement them, in the territory of Colombia.

The DPC complies with the following guidelines:

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

The update and/or modification of the CPS will be carried out through the procedure established by GSE for documented information. Any change or adjustment to the document must be reviewed, analyzed and approved by the Management Committee.

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

ELECTRONIC SECURITY MANAGEMENT DATA SA:

Company Name:	GESTION DE SEGUIRDAD ELECTRONICA SA
Initials:	GSE SA
Tax Identification Number:	900.204.272-8
Commercial Register No: Certificate of Existence and Legal Representative:	01779392 of February 28, 2008 https://gse.com.co/documentos/marco-regulatorio/Certificado-de-existencia-v-Representante-Legal-GSE.pdf
Status of the commercial register:	Asset
Business address and correspondence:	77th Street No. 7 - 44 Office 701
City / Country:	Bogota DC, Colombia
Phone:	+57 (601) 4050082
Email:	info@gse.com.co
Web page:	www.gse.com.co

1.2 Name and identification of the document.

The CPS for ECD GSE will be called "Certification Practice Statement (CPS)". The version changes according to the modifications on the same document.

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

The OID hierarchy was established by ECD GSE starting from the root 1.3.6.1.4.1.31136 defined by the IANA and is in accordance with the following parameters

OID HIERARCHY	DESCRIPTION	NAME
1	ISO format	It doesn't vary
3	Organization	It doesn't vary
6	Public	It doesn't vary

1	Internet	It doesn't vary
4.1 (31136)	Organization Identification	Does not vary, defined by IANA
1	Document type	It changes depending on whether they are policies, procedures, manuals, among others.
1	Document number	This is the number assigned to the document among its group
17	Document version	It is modified according to each version of the document

In accordance with this hierarchy, this DPC has been identified with the OID: 1.3.6.1.4.1.31136.1.1.17

1.3 PKI Participants.

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

GSE SA CERTIFICATION HIERARCHY		
GSE Root Authority	GSE ECDSA Root	GSE Root Electronic Signature
Subordinate Authority 01 GSE	GSE ECDSA Subordinated	GSE Electronic Signature Intermedia

GSE has two datacenters (one main and one alternate), the main datacenter with Hostdime is located in Verganzo, Zona Franca de Tocancipá Int 9, Km 1.5 via Briceño-Zipaquirá, Tocancipá, Cundinamarca, Colombia and the alternate datacenter with Claro is located on Autopista Medellin Km 7.5 Celta Trade Park - Datacenter Triara, Cota, Cundinamarca, Colombia.
1. PUBLICATION AND REPOSITORY RESPONSIBILITIES. a. PKI Repositories.

- ECD GSE Root Certificates https://certs2.gse.com.co/CA ROOT.crt https://certs2.gse.com.co/CA ECROOT.crt https://certs2.gse.com.co/CA FEROOT .crt
- GSE ECD Root Certificates Revoked List (CRL) https://crl2.gse.com.co/CAROOT.crl https://crl2.gse.com.co/CA ECROOT.crl https://crl2.gse.com.co/CA FEROOT.crl
- Subordinate Certificates ECD GSE https://certs2.gse.com.co/CA SUB01.crt https://certs2.gse.com.co/CA ECSUB01.crt https://certs2.gse.com.co/CA FESUB01 .crt
- List of ECD GSE Subordinate Revoked Certificates (CRL) https://crl2.gse.com.co/CA SUB01.crl https://crl2.gse.com.co/CA ECSUB01.crl https://crl2.gse. com.co/CA FESUB01.crl
- Online Validation of Digital Certificates https://ocsp2.gse.com.co

Note: Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is capable of understanding the responses generated by the service, such as OPENSSL.
This ECD GSE repository does not contain any confidential or proprietary information.
The GSE ECD repositories are referenced by URL. Any changes to URLs will be notified to all potentially affected entities.
The IP addresses corresponding to each URL may be multiple and dynamic, and may be modified without prior notice by
ECD GSE.

1.3.2 Registration Authority (RA).
This is the GSE area responsible for certifying the validity of the information provided by the applicant for a digital certification service, by verifying the subscriber entity or entity responsible for the digital certification services. The RA decides on the issuance or activation of the digital certification service. To do this, it has defined the criteria and methods for evaluating applications.

Under this CPS, the RA figure is part of the ECD itself and may act as a Subordinate of ECD GSE. GSE does not under any circumstances delegate the functions of Registration Authority (RA).

1.3.3 Subscribers

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

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

1.3.4 Trusted parties.

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

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

Precautions to be observed by third parties:

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

The Applicant shall be understood as the natural or legal person interested in the digital certification services issued under this CPS. This may coincide with the figure of the Subscriber.

Entity to which the subscriber or responsible party is linked.

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

1.3.5 Other participants. Management Committee.

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

Service providers.

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

Reciprocal Digital Certification Entities.

In accordance with the provisions of Article 43 of Law 527 of 1999, digital signature certificates issued by foreign certification entities may be recognized under the same terms and conditions 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 manner as it does with its own certificates, the regularity of the details of the certificate, as well as its validity and validity.

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

Petitions, Complaints, Claims and Requests.

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

Phone: +57 (601) 4050082
Email: pqrs@gse.com.co
Address: Calle 77 No. 7 - 44 Office 701
Website: www.gse.com.co
Responsible: Customer Service

Once the case has been submitted, it is transmitted with the information concerning the Customer Service process according to the internal procedure established for the investigation and management of these. Likewise, it is

determined which area is responsible for taking corrective or preventive actions, in which case the action procedure must be applied.
Once the investigation is generated, the response is evaluated to subsequently make the decision that resolves the PQRS and its final communication to the subscriber, responsible party or interested party.

1.4 Use of the certificate.

1.4.1 Appropriate use of certificates
The appropriate uses of Certificates issued by ECD GSE are specified in Certificate Policies for Digital Certificates.
Certificates issued under this CPS may be used for the following purposes:

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

The public key contained in a Digital Certificate can be used to encrypt data messages, such that only the holder of the private key can decrypt said data message and access the information. If the private key used to decrypt is lost or destroyed, the information that has been encrypted cannot be decrypted. The subscriber, those responsible and third parties acting in good faith, recognize and accept the risks involved in using digital certificates to perform encryption processes and in particular the use of keys to encrypt data messages is the exclusive responsibility of the subscriber or those responsible in the event of a loss or destruction of the key.
ECD GSE assumes no responsibility for the use of digital certificates for encryption processes.
Each certification policy is identified by a unique object identifier (OID) that also includes the version number.
Any other use not described in this CPS will be considered a violation of this CPS and will constitute a cause for immediate revocation of the digital certification service and termination of the contract with the subscriber and/or responsible party, without prejudice to any criminal or civil actions that may be taken by the ECD GSE.

1.4.2 Prohibited use of certificates
Certificates may only be used for the purposes for which they have been issued and specified in this CPS and specifically in the Certificate Policies for Digital Certificates.
Improper uses are considered those that are not defined in this CPS and consequently for legal purposes, ECD GSE is exempt from all responsibility for the use of certificates in operations that are outside the limits and conditions established for the use of Digital Certificates according to this CPS, which include, but are not limited to, the following prohibited uses:

- Illegal purposes or operations under any legal regime in the world.
- Any practice contrary to Colombian legislation.
- Any practice contrary to international agreements signed by the Colombian state.
- Any practice contrary to supranational regulations.
- Any practice contrary to good customs and business practices.
- Any use on systems whose failure may cause:
  - Death
  - Injuries to persons
  - Damage to the environment
- As a control system for high-risk activities such as:
  - Maritime navigation systems
  - Land transportation navigation systems
  - Air navigation systems
  - Air traffic control systems
  - Weapons control systems

1.5 Policy administration.

1.5.1 Organization that administers the document.

The CPD and certification policies are the responsibility and property of GSE and therefore acts as its administrator.

1.5.2 Contact (ECD Manager):

Name: Álvaro de Borja Carreras Amorós
Position: Legal Representative
Address: Calle 77 # 7-44 Office 701
Address: Bogotá DC, Colombia.
Phone: +57 (601) 4050082
Email: info@gse.com.co
Note:

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

Area in charge: Operations Manager
Address: Calle 77 # 7-44 Office 701
Address: Bogotá DC, Colombia.
Phone: +57 (601) 4050082
Email: info@gse.com.co

1.5.4 CPD approval procedures.

The Management Committee is the internal body of GSE responsible for the review, approval and authorization of the publication of the DPC on the website http://www.gse.com.co

1.6 Definitions and acronyms.

Definitions.
The following terms are commonly used and required for understanding this DPC:
Certification Authority (CA): In English "Certification Authority" (CA): Certification Authority, root entity and entity providing public key infrastructure certification services.
Registration Authority (RA): This is the entity responsible for certifying the validity of the information provided by the applicant for a digital certificate, by verifying tr identity and registration.
Time Stamping Authority (TSA): Acronym for "Time Stamping Authority": Certification entity providing time stamping services
Reliable data archiving: This is the service that GSE offers its clients through a technological platform. Essentially, it consists of a secure and encrypted storage space that is accessed with credentials or a digital certificate. The documentation stored on this platform will have probative value as long as it is digitally signed.
Digital certificate: A document electronically signed by a certification service provider that links signature verification data to a signatory and confirms his or her identity. This is the definition of Law 527/1999, which in this document is extended to cases in which the linking of signature verification data is made to a computer component.
Specific Accreditation Criteria (CEA): Requirements that must be met to obtain Accreditation as a Digital Certification Entity - ECD, before the National Accreditation Body of Colombia - ONAC; that is, to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 019 of 2012, Chapters 47 and 48 of Title 2 of Part 2 of Book 2 of the Single Decree of the Commerce, Industry and Tourism Sector - DURSCIT and the regulations that modify or complement them.
Personal Access Code (PIN): Acronym for "Personal Identification Number": Sequence of characters that allow access to the digital certificate.
Compromise of the private key: Compromise means the theft, loss, destruction or disclosure of the private key that may jeopardize the use of the certificate by unauthorized third parties or the certification system.
Certified email: Service that ensures the sending, receiving and checking of electronic communications, ensuring at all times the characteristics of fidelity, authorship, traceability and non-repudiation of the same.
Certification Practice Statement (CPS): A statement by the certification body regarding the policies and procedures it applies to the provision of its services.
Chronological stamp: According to numeral 7 of Article 3 of Decree 333 of 2014, it is defined as: Data message with a specific moment or period of time, which allows establishing with proof that this data existed at a moment or period of time and that it did not undergo any modification from the moment the stamp was made.
Certification Entity: A legal entity, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, authorized by the Colombian government (National Accreditation Body in Colombia) to issue certificates in relation to the digital

signatures of clients who acquire them, to offer or facilitate the services of registration and time stamping of the transmission and reception of data messages, as well as to fulfill other functions related to communications based on digital signatures.

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

1. Its use is not limited to the exchange of messages between the entity and the subscriber, or
2. Receive remuneration for these.

Closed certification authority: Entity that offers services typical of certification authorities only for the exchange of messages between the entity and the subscriber, without requiring remuneration for this.

Public Key Infrastructure (PKI): Acronym for "Public Key Infrastructure": A PKI is a combination of hardware and software, security policies and procedures that allows users of a fundamentally insecure public network such as the Internet to exchange data messages in a secure manner using a pair of cryptographic keys (one private and one public) that are obtained and shared through a trusted authority.

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

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

Certificate Revocation List (CRL): Acronym in English for "Certificate Revocation List": List that exclusively contains revoked certificates that have not expired.

Public Key and Private Key: The asymmetric cryptography on which PKI is based. It uses a pair of keys in which one can encrypt and only the other can decrypt, and vice versa. One of these keys is called public and is included in the digital certificate, while the other is called private and is known only to the subscriber or person responsible for the certificate.

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

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

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

Certification Policy (CP): It is a set of rules that define the characteristics of the different types of certificates and tr use.

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

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

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

Pseudonym: Hides his real name with a false name.

Pseudoanonymous: Intentionally using a false name

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

Applicant: Any natural or legal person who requests the issuance or renewal of a digital Certificate.

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

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

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

Acronyms.

CA: Certification Authority

CA Sub: Subordinate Certification Authority CP: Certification Policy CPD: Certification Practice Statement CRL: Certificate Revocation List

CSP: Certification Service Provider

DNS: Domain Name System

FIPS: Federal Information Processing Standard

HTTP: 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 (in Spanish: Hypertext Transfer Protocol Secure), better known by its acronym HTTPS, is a network protocol based on the HTTP protocol, intended for the secure transfer of hypertext data, that is, it is the secure version of HTTP.
HSM: Hardware Security Module IEC: International Electrotechnical Commission IETF: Internet Engineering Task Force
IP: Internet Protocol
ISO: International Organization for Standardization
LDAP: Lightweight Directory Access Protocol
OCSP: Online Certificate Status Protocol.
OID: Object identifier (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
RNEC: National Civil Registry
RFC: Request For Comments (Standard issued by the IETF)
URL: Uniform Resource Locator
VA: Validation Authority

Standards and standardization bodies.
CEN: European Committee for Standardization CWA: CEN Workshop Agreement ETSI: European Telecommunications Standard Inst FIPS: Federal Information Processing Standard IETF: Internet Engineer Task Force PKIX: IETF PKI Working Group PKCS: Public Key Cryptography Standards RFC: Request For Comments

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.
2.1 Repositories.

- ECD GSE Root Certificates
https://certs2.gse.com.co/CA ROOT.crt https://certs2.gse.com.co/CA ECROOT.crt https://certs2.gse.com.co/CA FEROOT.crt
- ECD GSE Root Certificates Revoked List (CRL) https://crl2.gse.com.co/CA_ROOT.crl
https://crl2.gse.com.co/CA ECROOT.crl https://crl2.gse.com.co/CA FEROOT.crl
- ECD GSE Subordinate Certificates https://certs2.gse.com.co/CA_SUB01.crt
https://certs2.gse.com.co/CA ECSUB01.crt https://certs2.gse.com.co/CA FESUB01.crt
- List of ECD GSE Subordinate Revoked Certificates (CRL) https://crl2.gse.com.co/CA SUB01.crl
https://crl2.gse.com.co/CA ECSUB01.crl https://crl2.gse. com.co/CA FESUB01.crl
- Online Validation of Digital Certificates https://ocsp2.gse.com.co

Note: Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is capable of understanding the responses generated by the service, such as OPENSSL.
This ECD GSE repository does not contain any confidential or proprietary information.
The GSE ECD repositories are referenced by URL. Any changes to URLs will be notified to all potentially affected entities.
The IP addresses corresponding to each URL may be multiple and dynamic, and may be modified without prior notice by
ECD GSE.
2.2 Publication of certification information.
The Revoked Certificate List published on the GSE website is digitally signed by the GSE ECD.
Information on the status of current digital certificates is available for consultation on the Web page and with the protocol
OCSP.
23 Term or frequency of publication.
Root Certificate
The root certificate will be published and remain on the ECD GSE website for as long as digital certification services are being provided.
Subordinate Certificate

The Subordinate's certificate will be published and remain on the ECD GSE website for the entire time that digital certification services are being provided.
Certificate Revocation List (CRL)
ECD GSE will publish on the Web page the list of certificates revoked in the events and with the periodicity defined in the section Frequency of issuance of CRLs.
Certification Practice Statement (CPS) - Global Certification Authority Root GSE
With the authorization of the Management Committee, validation by the Audit firm, issuance of the audit compliance report and finally with the express accreditation of the ONAC, the version finally approved for the provision of the digital certification service will be published and subsequent publications will be subject to the modifications that may take place with the approval of the Management Committee. The changes generated in each new version will be reported to ONAC and published on the ECD GSE website along with the new version. The annual Audit will validate these changes and issue the compliance report.
Online validation of digital certificates
ECD GSE will publish the issued certificates in a repository in X.509 format which can be consulted at the address https://ocsp2.gse.com.co
Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is capable of understanding the responses generated by the service, such as OPENSSL.

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

3. IDENTIFICATION AND AUTHENTICATION.

3.1 Names.

3.1.1 Types of names.
The guide document that ECD GSE uses for the unique identification of subscribers or those responsible for issued certificates is defined in the Distinguished Name (DN) structure of the ISO/IEC 9595 (X.500) standard.
Certificates issued by ECD GSE contain the X.500 distinguished name (DN) of the certificate issuer and recipient in the issuer name and subject name fields respectively.
ECD GSE Root Certificates.
The DN of the 'issuer name' of the root certificate, has the following fields and fixed values: C = CO O = GSE
OU = PKI
CN = GSE Root Authority E = info@gse.com.co
The DN of the 'subject name' includes the following fields: C = CO O = GSE
OU = PKI
CN = GSE Root Authority E = info@gse.com.co
Elliptic Curve (ECDSA).
The DN of the 'issuer name' of the root certificate, has the following fields and fixed values: C = CO
S = Capital District L = Bogota DC
O = GESTION DE SEGUIRDAD ELECTRONICA SA OU = GSE CA ROOT R2
SERIALNUMBER = 900204278
CN = GSE ECDSA RAIZ E = info@gse.com.co STREET = www.gse.com.co
The following fields are included in the 'subject name' DN: C = CO

S = Capital District L = Bogota DC
O = GESTION DE SEGUIRDAD ELECTRONICA SA
OU = GSE CA ROOT R2 SERIALNUMBER = 900204278
CN = GSE ECDSA RAIZ E = info@gse.com.co STREET = www.gse.com.co
Electronic Signature.
STREET=www.gse.com.co,
E= info@gse.com.co
CN = GSE ROOT ELECTRONIC SIGNATURE,

SN=900204272,
OU = GSE ELECTRONIC SIGNATURE R1,
O = GESTION DE SEGUIRDAD ELECTRONICA SA,
L=BOGOTA DC,
ST=CAPITAL DISTRICT,
C=CO
Certificates of Subordinates.
The DN of the 'issuer name' of the certificates of the ECD GSE subordinates have the following characteristics: C = CO O = GSE
OU = PKI
CN = GSE Root Authority E = info@gse.com.co
The following fields are included in the 'subject name' DN: C = CO
L = Bogota DC O = GSE
OU = PKI
CN = Subordinate Authority 01 GSE E = info@gse.com.co
Elliptic Curve (ECDSA).
The DN of the 'issuer name' of the certificates of the ECD GSE subordinates have the following characteristics: C = CO
S = Capital District L = Bogota DC
O = GESTION DE SEGUIRDAD ELECTRONICA SA
OU = GSE CA ROOT R2 SERIALNUMBER = 900204278
CN = GSE ECDSA RAIZ E = info@gse.com.co STREET = www.gse.com.co
The following fields are included in the 'subject name' DN: C = CO
S = Capital District L = Bogota DC
O = GESTION DE SEGUIRDAD ELECTRONICA SA OU = GSE ECDSA R2 SUB1
SERIALNUMBER = 900204278

CN = GSE ECDSA SUBORDINADA E = info(g)ase.com.co STREET = www.gse.com.co
ECD GSE Subscriber Certificates (Technical Profile Matrix for Certificates).
The DN of the 'issuer name' of the ECD GSE subscriber certificates, have the following general characteristics: C = CO
L = Bogota DC O = GSE OU = PKI
CN = Subordinate Authority 01 GSE E = info(g)ase.com.co
The DN of the 'subject name' is determined by ANNEX 1 DPC MATRIX TECHNICAL PROFILE DIGITAL CERTIFICATES
ECD GSE subscriber certificates (Technical profile matrix for electronic signature certificates).
STREET-www.gse.com.co, E=info(g)gse.com.co.
CN = GSE INTERMEDIATE ELECTRONIC SIGNATURE, SN = 900204272,
OU = GSE ELECTRONIC SIGNATURE R1,
0 = GESTION DE SEGUIRDAD ELECTRONICA SA,
L=BOGOTA DC,
ST=CAPITAL DISTRICT,
C=CO

3.1.2 Need for names to make sense.

Distinguished names (DNs) of certificates issued by ECD GSE are unique and allow a link to be established between the public key and the subscriber's identification number. Because the same person or entity can request several certificates in tr name, they will be differentiated by the use of a unique value in the DN field.

3.1.3 Anonymity or pseudonymity of subscribers.

Aliases, nicknames, nicknames, diminutives, and/or similar may not be used in the subscriber or responsible party fields, since the certificate must include the true name, company name, acronym, or denomination of the certificate applicant.

3.1.4 Rules for interpreting the different forms of the name.

The rule used to interpret the distinguished names of the issuer and the subscribers or those responsible for digital certificates issued by ECD GSE is the ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

3.1.5 Singularity of Names.

The DN of the issued digital certificates is unique for each subscriber.

3.1.6 Recognition, authentication and role of trademarks.

Recognition, authentication and role of recognized trademarks ECD GSE is not obliged to collect or request evidence in relation to the ownership or subscription or responsibility of registered trademarks or other distinctive signs prior to the issuance of digital certificates. This policy extends to the use and employment of domain names

3.2 Initial identity validation.
The ECD GSE will receive requests to certify the unequivocal identification of the subscriber's identity (natural or legal person), the veracity and authenticity of the information through any of its own identification systems, or if it belongs to a third party, provided that there is a contract, agreement, arrangement, alliance, and/or any means of contractual and/or commercial relationship, directly and/or indirectly, among others, with which the information is verified in a manner analogous to in-person validation by consuming one(s) of the widely used services in accordance with the requested digital certificate service, listed for this purpose below:

- National Identification Archive -National Civil Registry Office.
- Muisca - Single Model of Income, Service and Automated Control - and/or databases of the DIAN (National Tax and Customs Directorate).
- Confront.
- Single Business and Social Registry and/or databases of the Chambers of Commerce (For Legal Entities).

- Colombian Immigration (for foreigners).
- Databases available to theNational Civil Registry Office that allows for the unequivocal identification of the applicant. In accordance with the current regulations issued by the Entity.
- Selfie against identification document (hologram citizenship cards, physical digital and foreign identity cards)

The ECD GSE reserves the right to decline to accept an application or maintain a contract for certification when, in its judgment, there are reasons that may jeopardize the credibility, commercial value, legal or moral suitability of the ECD. Likewise, the demonstrated participation of the applicant in illegal activities, or similar issues related to the same, will be sufficient reason to reject the application.
The applicant's data: type of identification, identification number, first name, last name, NIT (applicable for companies), company name (applicable for companies) and email are reviewed and/or validated together with the application form, the information and/or documentation provided for each type of digital certificate.
The Single Tax Registry - RUT document will be requested in the updated DIAN format that includes a QR code (if applicable). These services are listed in the Procedure for issuing digital certificates.
For digital certification services: Chronological Stamping, Certified Electronic Mail, Generation of Certified Electronic Signatures, Archiving and Conservation of Transferable Electronic Documents and Data Messages, the identity validation service will not be consumed, but the verification mechanisms that apply to confirm the veracity and authenticity of the information will be, such as:

- National Identification Archive -National Civil Registry Office.
- Muisca - Single Model of Income, Service and Automated Control - and/or databases of the DIAN (National Tax and Customs Directorate).
- Single Business and Social Registry and/or databases of the Chambers of Commerce (For Legal Entities).
- Colombian Immigration (for foreigners).

The ECD GSE reserves the right to request additional documents, in original or copy; in order to verify the identity of the applicant, it may also exempt the presentation of any document when the identity of the applicant has been sufficiently verified by the ECD GSE through other means, if the request for a digital certificate of a natural person is made directly and/or indirectly from the platforms of the National Registry of Civil Status - RNEC after verification by said entity and its functions described in Decree 1010 of 2000:
(...)
ARTICLE 2. Purpose. The purpose of the National Civil Registry is to register the civil life and identify Colombians and to organize electoral processes and mechanisms for citizen participation, in order to support the administration of justice and the democratic strengthening of the country.
(...)
ARTICLE 5. Functions. The following are the functions of the National Civil Registry:
19. Issue and prepare Colombian citizenship cards in optimal conditions of security, presentation and quality, and adopt a unique identification system for first-time applications, duplicates and corrections.
20. To handle everything related to the management of information, databases, the National Identification Archive and the documents necessary for the technical process of citizen identification, as well as to inform and issue certifications for the procedures where appropriate.

24. Respond to requests for the issuance of citizenship cards at Colombian consulates abroad so that those who are authorized can exercise tr political rights as Colombian citizens and provide information about the process.
This means that if the request for a digital certificate for an applicant (citizen) is made from the RNEC as the main source of information in Colombia, it is ensured that the applicant had a prior validation of his or her identity and address data to carry out the process of issuing the citizenship card, the ECD GSE will receive the information from said source, the veracity and authenticity are ensured by carrying out the unequivocal identification of the subscriber, the ECD GSE will keep the records of the request ensuring the Digital Certification Life Cycle process.
In the case of electronic signature certificates, the identity of the applicant is not validated, but rather a verification of the data registered at the time of the signature request is carried out by sending an OTP code to the registered email address.

3.2.1 Method to prove possession of the private key.
To guarantee the issuance, possession and control of the private key by the subscriber and/or responsible party, a secure cryptographic token device is delivered directly in which the subscriber and/or responsible party generates the key pair and transmits, via a secure channel, the file in PKCS#10 format where he/she demonstrates that he/she is in possession of the private key.
In the event that the certificate is centralized, the generation of the key pair is carried out on an HSM device owned by the ECD GSE and the subscriber and/or person responsible is given a set of credentials (username and password) for tr exclusive use.
Since electronic signature certificates are ephemeral and are used only for generating the signature, the credentials for using these certificates are not delivered to the subscriber and are instead generated automatically and randomly by the platform and discarded once the electronic signature is generated.

Pursuant to the provisions of ONAC in CEA 3.0-07, in the case in which the key pair is generated by the applicant in its own infrastructure, for example, for the use of the certificate in unattended platforms, the applicant must accept and comply with the requirements set forth in document Annex 1 of Terms and Conditions, numeral 6, literal m), if they were generated by software and by devices that comply with Annex F of the CEA, if they were generated by hardware.
3.2.2 Authentication of the organization's identity.
To ensure the identity of a legal entity, the RA GSE requires the delivery of the information of the legal entity and/or presentation of the official document that proves the legal existence of the same and its legal representative or agents, who will be the only people who can request the digital certificate in the name of said organization. In the case that the request is made by a third party, the proof of delegation of the process to the agent must be delivered scanned. The documents will be received scanned, preserving the legibility for the use of the information.
Notwithstanding the foregoing, ECD GSE reserves the right to issue certificates when, in its judgment, the credibility, commercial value or legal or moral suitability of the Digital Certification Entity may be put at risk.
3.2.3 Authentication of individual identity.
In order to ensure the identity of a natural person, the RA GSE requires the registration of information that proves the identity of the applicant and/or the presentation of the applicant's digital identity document and verifies its existence and correspondence against its own and/or third-party databases, whether official and/or private through contracts, agreements, accords, alliances, and/or any type of contractual and/or commercial relationship, whether direct and/or indirect. When the service is requested by a minor, his/her identity will be ensured with the authenticated identity document (identity card) and a document that supports the link between the applicant and the minor. In the event that the request is made by a third party, the proof of delegation of the process must be delivered scanned to the representative. The documents will be received scanned, preserving the legibility for the use of the information.
Notwithstanding the foregoing, ECD GSE reserves the right to issue certificates when, in its judgment, the credibility, commercial value or legal or moral suitability of the Digital Certification Entity may be put at risk.
3.2.4 Unverified subscriber information.
Under no circumstances will ECD GSE omit the verification tasks that lead to the identification of the applicant and that translate into the request and requirement of the information and/or documents mentioned for organizations and individuals.
In the specific case of address data, the good faith of the information provided by the applicant is presumed, and therefore no verification of the same is carried out.
3.2.5 Validation of authority.
GSE uses a reliable method of communication with the Applicant or its representative.

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

The Applicants' authority to request Certificates on behalf of an organization is verified during the validation of the Applicant's identity.
GSE may permit Applicants to specify in writing the persons who may apply for Certificates on tr behalf. Where such specification has been made, GSE will not accept applications for Certificates that fall outside this specification but will, upon written request, provide the Applicant company with a list of its authorized Certificate applicants.

3.2.6 Interoperability criteria.
ECD GSE will only issue digital certificates to Subordinate ECDs, where the decision to issue or activate the digital certification service is made by ECD GSE through a recommendation based on the review of the application by the GSE RA.

3.3 Identification and Authentication for key renewal.
3.3.1 Identification and authentication for key reuse routine.
The ECD GSE does not consider the process of reusing the public and private keys of the certificate for the renewal of digital certificates.
If a renewal of an issued certificate is requested, the issuance request process must be completed in the same way as a new certificate, which will be generated from a new key pair.
ECD GSE carries out the authentication process of the applicant in all events, including renewal events, and based on this, issues the digital certificates. The foregoing, through any identification system as long as there is a contract, agreement, accord, alliance, and/or any type of contractual and/or commercial relationship, directly and/or indirectly, among others, with the National Registry of Civil Status, confronta, credit bureau databases or government data sources. Only those requests digitally signed by the subscriber will have tr digital certificate renewed without going through a new identification and authentication process, always guaranteeing documentary validation.
3.3.2 Identification and authentication for key reuse routine after revocation.
GSE does not consider the process of reusing the public and private keys of the certificate for the renewal of digital certificates, when tr revocation has been requested.

If the revocation of an issued certificate is requested and then the certificate is requested again with the same data as the revoked certificate, the issuance request process must be completed in the same way as a new certificate, which will be generated from a new pair of keys.
The process of replacing a digital signature certificate as a result of revocation for the different reasons defined in this CPD requires a verification process for that request (Replacement).

3.4 Identification and authentication for the revocation request.
ECD GSE handles revocation requests in accordance with the grounds for revocation specified in the Circumstances for revoking a certificate section of this CPD and authenticates the identity of the person requesting certificate revocation in accordance with the revocation procedure.

4. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFE CYCLE.

4.1 Request for certificate.
Any person requiring the provision of the digital certification service may do so using the channels, means or mechanisms provided by ECD GSE, where the necessary information will be obtained to manage the request for the required digital certification service. Once the terms and conditions have been accepted and the request has been submitted, the information is sent to the Registration Authority, which will be responsible for reviewing the request to ensure the unequivocal identification of the subscriber's identity (Natural or Legal Person), the veracity and authenticity of the information that allows a recommendation to be made for decision-making in compliance with the requirements set out in the Certification Policies.
The applicant provides the necessary information and/or documents as applicable, delivering them in scanned form or in electronic original, preserving the readability for the use of the information. The information can also be obtained through fully reliable databases, in accordance with those already mentioned in previous sections, thereby fulfilling the procedures established by the ECD GSE for obtaining the digital certificate.

The GSE ECD reserves the right to request additional information and/or documents to those required, in original or copy; in order to verify the identity of the applicant, it may also exempt the submission of any document when the identity of the applicant has been sufficiently verified by the GSE ECD through other means or mechanisms provided.
The information and/or documentation provided will be reviewed in accordance with the Criteria and Methods for Evaluation of Applications established by GSE.
The applicant accepts that the GSE ECD has the discretionary right to reject a digital certificate application when, in its opinion, the credibility, commercial value, good name of GSE, legal or moral suitability of the entire digital certification system may be jeopardized, notifying the applicant of the non-approval.
For the request for an electronic signature certificate, the Electronic Signature Procedure (PCO-PD-17) has been established.

4.1.1 Who can request a certificate.

Any natural or legal person legally authorized and duly identified may process the request for the issuance of a digital certificate.

4.1.2 Application, registration and liability process.

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

4.2 Processing certificate request.

4.2.1 Procedure for processing the request/identification and authentication.

The functions of authentication and verification of the applicant's identity are performed by the GSE RA, responsible for giving the recommendation for the decision on the digital certification based on the review of the application, who verifies whether the information provided is authentic and complies with the requirements defined for each type of certificate in accordance with this CPS.
The information and/or documentation that the GSE RA must review to make a recommendation for the decision-making process for the correct issuance of each type of certificate is defined in the Certificate Policies for Digital Certificates.

4.2.2 Criteria for accepting or rejecting the application.

If, once the identity of the applicant has been verified, the information provided complies with the requirements established by this CPS, the application is approved. If the full identification of the identity of the applicant is not possible or the information provided is not fully authentic, the application is denied and the certificate is not issued.
ECD GSE assumes no responsibility for the consequences that may arise from the non-approval of the issuance of a digital certificate, and this is accepted and recognized by the applicant to whom the issuance of the respective certificate has been denied.
Likewise, ECD GSE reserves the right not to issue certificates even if the applicant's identification or the information provided by the applicant has been fully authenticated, when the issuance of a particular certificate for reasons of legal order or commercial convenience, good name or reputation of GSE may jeopardize the digital certification system.

If after filing an application and the process did not approve the application review or the applicant did not perform the identity validation, after fifteen (15) days without correcting the novelty, the RA of the ECD GSE will have as an alternative to reject the application and the applicant will be notified to process a new application.
For this purpose, ECD GSE will notify the applicant of the approval or rejection of the application. 4.2.3 Deadline for processing certificate applications
The time frame for processing a request by the GSE RA is one (1) to five (5) business days from the moment the requested information and/or documentation is received and the applicant has approved the initial identity validation.
The delivery time of the digital certificate issued on a cryptographic device depends on the place of destination, without exceeding eight (8) business days for delivery.

4.3 Issuance of the Certificate.

4.3.1 ECD GSE actions during certificate issuance.

The final step in the process of issuing digital certificates is the issuance of the certificate by ECD GSE and its secure delivery to the subscriber and/or controller.
The GSE RA generates the formal documentation of the digital certification, when the decision to grant the digital certificate has been made.
The process of issuing digital certificates securely links registration information and the generated public key.

4.3.2 Notification mechanisms authorized by subscribers.
By email or other defined and authorized means, the subscriber is notified of the issuance of his/her digital certificate and therefore the subscriber accepts and acknowledges that once he/she receives the notification, it will be understood that the certificate has been issued. It will be understood that the notification informing the issuance of a certificate has been received when there was no news when delivering the notification, it will be said that it was not delivered satisfactorily. In the case in which the subscriber requested that the issuance of the digital certificate be in a cryptographic device, it will be understood as delivered once the shipping record is available: delivery letter and/or the shipping guide to the logistics operator or courier and/or confirms in the issuance notification that he/she has received the cryptographic device.
Publishing a certificate in the certificate repository constitutes proof and public notification of its issuance.

4.4 Acceptance of the Certificate.

4.4.1 Mechanism for acceptance of the certificate by the subscriber.
No confirmation is required from the subscriber or responsible party as acceptance of the certificate received. A certificate is considered to be accepted by the subscriber or responsible party from the moment it is requested to be issued. Therefore, if the information contained in the issued certificate does not correspond to the current status of the certificate or was not supplied correctly, it is the subscriber's responsibility to inform this and/or request its revocation.

4..4.2 Publication of the certificate by the CA
GSE publishes all root and subordinate CA certificates in its repository and has a mechanism for the subscriber to consult the end-entity certificates as the person responsible for the digital certificate. On the website: https://gse.com.co/consultas-en-linea/

4.4.3 Notification of the issuance of certificates by the ECD GSE to other entities.
See section 4.4.2. above.

4.5 Using key pairs and certificates.
4.5.1 Subscriber's Responsibilities Regarding the Use of the Private Key and Certificate.
The subscriber or person responsible for the digital certificate and the associated private key accepts the conditions of use established in this CPS by the mere fact of having requested the issuance of the certificate and may only use them for the uses explicitly mentioned and authorized in this CPS and in accordance with what is established in the "Key Usage" fields of the certificates. Consequently, the issued certificates and the private key must not be used in other activities that are outside the mentioned uses. Once the validity of the certificate has expired, the subscriber or person responsible is obliged to stop using the private key associated with it. Based on the above, the subscriber hereby accepts and acknowledges that in this sense he/she will be the only person responsible for any loss or damage caused to third parties by the use of the private key once the validity of the certificate has expired. ECD GSE does not assume any type of responsibility for unauthorized uses.
4.5.2 Trusted Third Party Responsibilities Related to the Use of the Subscriber's Private Key and Certificate.
The subscriber to whom a certificate has been issued is obliged to inform third parties that it is necessary for them to check the status of the certificate in the certificate revocation list every time they use the certificate for third parties.

certificates, as well as those issued in order to verify tr validity and that they are being applied within tr permitted uses established in this CPS.
In this regard, you should:
- Check that the associated certificate does not violate the start and end dates of validity.
- Check that the certificate associated with the private key is not revoked.
- Check that the fingerprint {The fingerprint of the root ECD certificate and the fingerprint of the ECD GSE subordinate certificate match the one published by GSE on its website.

Fingerprint of the root ECD certificate:
SHA 256 Fingerprint=7C:lC:A5:5l:3l:2E:A0:2E:Fl:D6:3A:4F:56:54:D0:3F:D0:4F:6F:32:7C:8E:2E: 03:52:lA:22:69:7A:B7:98:43
SHA256

Fingerprint=9F:BF:5F:El:A3:34:49:35:44:6A:95:EB:45:D3:DD:F3:49:36:l8:4l:2l:7l:7l:65: F0:B8:42:ll:85:0D:E6:F3 SHA256
Fingerprint=3F:CE:D4:24:F2:D5:70:53:6E:DA:65:2D:D7:C9:D3:6D: 58:5A:l0:ED:BB:58:85:lC:F8:2C:9l:l2:03:4l:5C:0C
Fingerprint of the certificate of the subordinate of ECD GSE Subordinate Certificate OOV-SHA 256
Fingerprint=70:99:0l:C9:lD:8F:B2:92:DB:8l:B7:04:8B:0B:06:E5:A2:AA:l4:59:7D:CA:C4:DF: BE:6B:DD:90:49:D8:E2:01
SHA256 Fingerprint=8C:8B:l7:8E:AA:D2:E9:AD:BF:2D:28:lE:9l:53:3F:96:
BF:7C:BE:lB:2D:8A:89:A0:D8:AE:FD:l9:40:D0:35:88 SHA256
Fingerprint=6C:9l:FA:BA:42:7F:0D:93:CB:B4:EB:09:4A:3F:5E:4A:64:D8:F2:5F:B8:7B:AA:75: D8:26:8D:BF:79:8E:CC:95

4.6 Certificate renewal

The ECD GSE does not handle certificate renewal requests without changing keys.

4.6.1 Circumstances for certificate renewal.

Not applicable since certificates are not issued without changing keys.

4.6.2 Who can request a renewal without changing keys.

Not applicable since certificates are not issued without changing keys.

4.6.3 Procedures for requesting certificate renewal.

Not applicable since certificates are not issued without changing keys.

4.6.4 Notification to the subscriber or person responsible for the issuance of a new certificate without changing keys.

Not applicable since certificates are not issued without changing keys.

4.6.5 Form in which the renewal of a certificate is accepted.

Not applicable since certificates are not issued without changing keys.

4.6.6 Publication of the certificate renewed by the ECD.

Not applicable since certificates are not issued without changing keys.

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

Not applicable since certificates are not issued without changing keys.

4.7 Re-use of certificate key

For the ECD GSE, a request for renewal of a certificate with a change of keys is a normal procedure for requesting a digital certificate as if it were a new one and therefore involves the generation of new keys, as recognized and accepted by the applicant.

In conclusion, GSE treats all requests for re-issuance and/or renewal of certificates as requests for issuance of a new certificate, taking into account that it does not reuse keys in any case.

4.7.1 Circumstance for re-using certificate keys.

A new digital certificate may be generated at the request of the subscriber and/or responsible party due to expiration of validity or revocation of the current certificate in accordance with the reasons mentioned in this CPS or when required by the subscriber.

Not applicable. See section 4.7

4.7.2 Who can request certification of a new public key.

For certificates issued by natural persons, the subscriber may request renewal of the certificate. For legal persons, the legal representative, duly authorized alternates or representatives may request renewal of the digital certificate.

Not applicable. See section 4.7

4.7.3 Processing certificate key reuse requests.

The procedure for renewing digital certificates is the same as the procedure for requesting a new certificate. The subscriber must access the means or mechanisms for this purpose to submit the request to the ECD GSE and start the process of requesting a new digital certificate in the same way as when submitting the request for the digital certificate for the first time. Your request will be validated again in order to update data if required.

Not applicable. See section 4.7

4.7.4 Notification to the subscriber of the issuance of a new certificate.

By email or other means for this purpose, the subscriber is notified of the issuance of his/her digital certificate and consequently the subscriber accepts and acknowledges that once he/she receives said notification, the subscriber will be deemed to have accepted the terms and conditions of the ECD GSE that the certificate has been issued. In the event that the subscriber requests that the issuance of the digital certificate be on a cryptographic device, it will be deemed to have been delivered once the delivery record is available: delivery letter and/or the shipping guide to the logistics operator or courier and/or confirms in the issuance notification that he/she has received the cryptographic device.

Not applicable. See section 4.7

4.7.5 Conduct that constitutes acceptance of a certificate with re-use of the key.

No confirmation is required from the subscriber or responsible party as acceptance of the renewal of a certificate received. A renewed certificate is considered to be accepted by the subscriber or responsible party from the moment it is requested to be issued. Therefore, if the information contained in the issued certificate does not correspond to the current status of the same or was not supplied correctly, its revocation must be requested by the applicant or responsible party and he/she will accept it.

Not applicable. See section 4.7

4.7.6 Publication of the certificate with key reuse by the CA

Not applicable as ECD GSE does not reuse certificate keys. Not applicable. See section 4.7

4.7.7 Notification of the issuance of certificates by the CA to other entities

There are no external entities that need to be notified of the issuance of a renewed certificate. Not applicable. See section 4.7

4.8 Certificate Modification.

Digital certificates issued by ECD GSE cannot be modified, i.e. amendments are not applicable. Consequently, the subscriber must request the issuance of a new digital certificate. In this event, a new certificate will be issued to the subscriber; the cost of this modification will be fully borne by the subscriber according to the rates informed by ECD GSE or according to the conditions defined at the contractual level.

4.8.1 Circumstance for modifying the certificate.

Not applicable since digital certificates issued by ECD GSE cannot be modified.

4.8.2 Who can request a certificate modification?

Not applicable since digital certificates issued by ECD GSE cannot be modified.

4.8.3 Processing requests for certificate modifications.

Not applicable since digital certificates issued by ECD GSE cannot be modified.

4.8.4 Notification to the subscriber of the issuance of a new certificate

Not applicable since digital certificates issued by ECD GSE cannot be modified.

4.8.5 Conduct that constitutes acceptance of a modified certificate.

Not applicable since digital certificates issued by ECD GSE cannot be modified.

4.8.6 Publication of the modified certificate by the CA.

Not applicable since digital certificates issued by ECD GSE cannot be modified.

4.8.7 Notification of the issuance of certificates by the CA to other entities.

Not applicable since digital certificates issued by ECD GSE cannot be modified.

4.9 Revocation and Suspension of the Certificate.

4.9.1 Circumstances for revocation.

The subscriber or responsible party may voluntarily request the revocation of his/her digital certificate at any time in accordance with the provisions of Article 37 of Law 527 of 1999, but is required to request the revocation of his/her digital certificate under the following situations:

1. Due to loss or unusability of the private key or digital certificate.
2. The private key has been exposed or is at risk of being misused.
3. Changes in the circumstances under which ECD GSE authorized the issuance of the digital certificate.
4. If during the period of validity part or all of the information contained in the digital certificate loses currency or validity.

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

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

1. At the request of the subscriber, the person responsible or a third party on tr behalf and representing them.
2. Due to death of the subscriber or responsible party.
3. For confirmation or evidence that some information or fact contained in the digital certificate is false.

4. The private key of the certification authority or its security system has been compromised in a way that materially affects the reliability of the certificate.
5. By order of a court or competent administrative entity.
6. Due to compromised security for any reason, mode, situation or circumstance.
7. Due to sudden incapacity of the subscriber or responsible party.
8. Due to liquidation of the legal entity represented as stated in the digital certificate.
9. Due to the occurrence of new events that cause the original data to not correspond to reality.

IT. Due to loss or disablement of the cryptographic device that has been delivered by ECD GSE.
Ll. By termination of the subscription contract, in accordance with the causes established in the contract.
L2. For any reason that reasonably leads to believe that the certification service has been compromised to the point that the reliability of the digital certificate is called into question.
L3. Due to improper handling of the digital certificate by the subscriber.
L4. Due to non-compliance by the subscriber or the legal entity that he represents or to which he is linked through the terms and conditions document or the person responsible for digital certificates of the ECD GSE.
L5. Knowledge of events that modify the initial state of the data supplied, among others: termination of the Legal representation, termination of employment, liquidation or extinction of legal status, cessation of public office or change to a different one.
L6. At any time when falsity is evident in the data provided by the applicant, subscriber or controller.
L7. Due to failure by the ECD GSE, the subscriber or the person responsible for the obligations established in the CPS.
L8. For failure to pay the amounts for certification services agreed between the applicant and ECD GSE.
However, for the above reasons, ECD GSE may also revoke certificates when, in its opinion, the credibility, reliability, commercial value, good name of ECD GSE, legal or moral suitability of the entire certification system may be put at risk.

4.9.2 Who can request the revocation of a certificate

The subscriber or responsible party, a third party in good faith or any interested person when they have demonstrable knowledge of the facts and grounds for revocation mentioned in the section Circumstances for the revocation of a certificate of this CPS and which compromise the private key.
A third party in good faith or any interested person who has demonstrable evidence that a digital certificate has been used for purposes other than those set out in the section Appropriate uses of the certificate of this CPS.
Any interested person who has demonstrable evidence that the certificate is not in the possession of the subscriber or responsible party.
The CA Technology team, as the highest control entity that is responsible for the administration of the security of the technological infrastructure of the ECD GSE, is able to request the revocation of a certificate if it has knowledge or suspicion of the compromise of the private key of the subscriber, responsible party or any other fact in accordance with the circumstances for the revocation of a certificate.

4.9.3 Procedure for requesting revocation of a certificate.

The subscriber and/or responsible party, a third party in good faith or any person will have the opportunity to request the revocation of a digital certificate whose causes are specified in this CPS. They may do so under the following procedures:

• At GSE offices.

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

• Online revocation request:

The subscriber and/or person responsible may carry out the digital certificate revocation process through the GSE SA web portal, https://gse.com.co/consultas-en-linea/ - Request its revocation, when completing the request, the current digital certificates will be displayed, the certificate to be revoked must be selected and your registered email, you will receive a notification with the security code to complete the completion of the online revocation request, the subscriber and/or person responsible must select the reason for the revocation, enter the security code, accept the Terms and Conditions and send the request to revoke your digital certificate; once the request is complete, your digital certificate will be revoked and the revocation notification will be sent to the registered email.
Other means available to revoke the digital certificate by the subscriber and/or responsible party and/or third party in good faith may be through the tool(s) and/or application(s) from which the request for the issuance of the digital certificate of authorized third parties was submitted.

• Revocation Service via Email

Through our email address revocaciones@gse.com.co , subscribers and/or those responsible may request the revocation of digital certificates in accordance with the reasons for revocation mentioned in the section Circumstances for the revocation of a certificate of this DPC, by sending a signed digital revocation request letter or email with the subscriber's details and reason for revocation, Digital Certification Service Revocation Form.
Note: The ECD - GSE provides a guide template to prepare the revocation request letter which is available on the website https://ase.com.co/auias-y-manuales. Revocations and Root and Subordinate Certificates option
The ECD, through the Technology area and the personnel designated to develop certification activities in accordance with the digital certificate revocation procedure, will verify the revocation request.

4.9.4 Grace period to request revocation of a certificate.

Upon review of a revocation request, the ECD GSE will proceed immediately with the requested revocation, within its office hours. Consequently, there is no grace period that allows the applicant to cancel the request. If it was an erroneous request, the subscriber or responsible party must request a new certificate, since the revoked certificate lost its validity immediately after the revocation request was validated and the ECD GSE will not be able to reactivate it.
The procedure used by the ECD GSE to verify a revocation request made by a specific person is to review the request in accordance with the previous section.
Once the certificate revocation has been requested, if it is evident that said certificate is used in connection with the private key, the subscriber or responsible party releases the ECD GSE from all legal responsibility, since they recognize and accept that the control, custody and confidentiality of the private key is tr exclusive responsibility.

4.9.5 Time within which the CA must process the revocation request.

The request for revocation of a digital certificate must be attended to with the highest priority, without its revocation taking more than three (3) business days once the request has been reviewed.
Once the formalities provided for revocation have been completed and if for any reason the revocation of a certificate is not made effective under the terms established by this CPS, ECD GSE as a certification services provider and responsible for the CA, will be liable for any damages caused to subscribers or third parties in good faith arising from errors and omissions, bad faith of the administrators, legal representatives or employees of ECD GSE in the development of the activities for which it is authorized and for which it has civil liability insurance in accordance with Article 9. Guarantees, of Decree 333 of 2014. ECD GSE does not assume any other commitment or provide any other guarantee, nor does it assume any other responsibility to the subscriber and/or those responsible for the certificate or trusted third parties except as established by the provisions of this CPS.

4.9.6 Revocation verification requirement for the partiesconfident.

It is the responsibility of the subscriber and/or person responsible for a digital certificate, and he/she accepts and acknowledges this, to inform third parties in good faith of the need to check the validity of the digital certificates that he/she is using at any given time. The subscriber and/or person responsible shall also inform the third party in good faith that, in order to carry out such a query, he/she has the list of revoked certificates CRL, published periodically by the ECD GSE.
Relying parties must confirm the validity of each certificate in the certification chain by checking the corresponding CRL or OCSP responder before trusting a certificate issued by the ECD GSE CA.

4.9.7 Frequency of broadcast of theCRLs.

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

4.9.8 Maximum latency of theCRLs.

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

4.9.9 Online revocation/status check availability

ECD GSE will publish both the CRL and the status of revoked certificates in freely accessible and easily consulted repositories, available 24/7, every day of the year. ECD GSE offers an online consultation service based on the OCSP protocol at https://ocsp2.ase.com.co.
Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is capable of understanding the responses generated by the service, such as OPENSSL.

4.9.10 Online revocation checking requirements.

To obtain information on the revocation status of a certificate at any given time, you can perform an online query at https://ocsp2.gse.com.co. To do so, you must have software that is capable of operating with the RFC6960 protocol. Most browsers offer this service.
Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is capable of understanding the responses generated by the service, such as OPENSSL.

4.9.11 Other forms of revocation notices available.
Within 24 hours of the revocation of a certificate, the ECD GSE informs the subscriber and/or responsible party by email or other means of notification of the revocation of tr digital certificate and, consequently, the applicant accepts and acknowledges that once they receive the notification, it will be understood that tr request has been attended to. It will be understood that the information notifying the revocation of a certificate has been received when said notification is entered into the information system designated by the applicant.
Publication of a revoked certificate on the CRL constitutes proof and public notification of its revocation.
The ECD GSE will maintain a historical archive of up to three (3) years of the CRLs generated and which will be available to subscribers upon written request addressed to the ECD GSE.
4.9.12 Special requirements for renewal of compromised keys.
If a digital certificate has been requested to be revoked due to compromise (loss, destruction, theft, disclosure) of the private key, the subscriber may request a new digital certificate for a period equal to or greater than that initially requested by submitting a renewal request in relation to the compromised digital certificate. The responsibility for the custody of the key rests with the subscriber or responsible party and he or she accepts and acknowledges this, therefore, he or she assumes the cost of the renewal in accordance with the current rates set for the renewal of digital certificates.
In the event that the subscriber's private key is compromised, the subscriber shall immediately notify the GSE ECD of the private key compromise event. The GSE ECD shall revoke the certificate in question and the same shall be displayed in the next CRL published at the next update to inform the using parties that the certificate is no longer trusted.
The subscriber is responsible for investigating the circumstances of such engagement.
4.9.13 Circumstances for suspension
ECD GSE does not offer a digital certificate suspension service, only revocation.
4.9.14 Who can request the suspension
Not applicable because ECD GSE does not have a digital certificate suspension service, only revocation.
4.9.15 Suspension application procedure
Not applicable because ECD GSE does not have a digital certificate suspension service, only revocation.
4.9.16 Suspension period limits
Not applicable because ECD GSE does not have a digital certificate suspension service, only revocation.

4.10 Certificate Status Services.
4.10.1 Operational characteristics
To query the status of certificates issued by ECD GSE, an online query service based on the OCSP protocol is available at https://ocsp2.ase.com.co. The subscriber or person responsible for sending a query request on the status of the certificate through the OCSP protocol, which, once the database has been consulted, is attended to by a response via http or a query via CRL.
CRLs issued by the ECD GSE comply with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" and contain the following basic elements:
Revocation entries for a CRL or OCSP response are not deleted until after the expiration date of the revoked certificate.
4.10.2 Service availability
The GSE ECD operates and maintains its CRL and OCSP capability with sufficient resources to provide a response time of ten seconds or less under normal operating conditions.
Certificate status services are available 24 hours a day, 7 days a week unless otherwise unavailable.

temporarily due to maintenance tasks but always guaranteeing online consultation availability 7x24x365, 99.8% uptime per year
Version number.
CRLs issued by ECD GSE comply with the current X.509 standard. CRLs and CRL extensions.
Information about the reason for revocation of a certificate will be included in the CRL, using the CRL extensions and more specifically in the revocation reason field (reasonCode).
CRL Availability.
As indicated in section 4.9.9 Availability of online verification of revocation/OCSP Profile status.
The OCSP service complies with RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".
Version number.

Compliant with OCSP Version 1 of RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP". OCSP Extensions. Not applicable
OCSP service availability
As indicated in section 4.9.9 Availability of online revocation/status verification 4.10.3 Optional features.
To obtain information on the certificate status at any given time, you can perform an online query at https://ocsp2.gse.com.co. To do so, you must have software that is capable of operating with the OCSP protocol. Most browsers offer this service or a query to the CRL published on the portal https://crl2.ase.com.co.
Online validation of digital certificates using OCSP must be performed with a tool that implements the OCSP protocol and is capable of understanding the responses generated by the service, such as OPENSSL.

4.11 End of Subscription.

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

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

4.12 Custody and Recovery of Keys

4.12.1 Key safekeeping and recovery policy and practices.

The subscriber's private key can only be stored on a hardware cryptographic device (token or HSM).
The hardware cryptographic devices used by ECD GSE comply with the certifications as cryptographic chip: security level CC EAL5+ PP 9806, BSI-PP-002-2001, FIPS 140-2 LEVEL 3 and the SO certifications of the cryptographic chip: security level CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3) - BSI -DSZ-CC-0422-2008 and support the standards PKCS#11, Microsoft CAPI, PC/SC, X.509 current certificate storage, SSL v3, IPsec/IKE.
The ECD GSE publishes in the Digital Certificate Policies for Digital Certificates the characteristics of the cryptographic devices that it offers to subscribers who request it for the creation and storage of tr private keys.
Key custody and recovery policies.
The private key generation is stored on a secure device (hardware) from which it cannot be exported. Consequently, the subscriber's private key cannot be recovered. The subscriber is responsible for the custody of the private key and is accepted and acknowledged by the subscriber.

4.12.2 Session key encapsulation and recovery policy and practices.

The recovery of the subscriber's session key or PIN is not possible since the only person responsible for assigning it and this is declared and accepted by the subscriber. The responsibility for the custody of the session key or PIN is of the subscriber who agrees not to keep digital records, written or in any other format and who is obliged to protect access to the PIN, so if the PIN is forgotten, a case will be filed at the ECD - GSE service desk to verify the request and if necessary by the subscriber, he may file the request for revocation of the digital certificate through the channels provided for this purpose and will manage the request for a new digital certificate.

5. FACILITIES, MANAGEMENT AND OPERATIONAL CONTROLS.

5.1 Physical Security Controls.

The GSE ECD CA infrastructure is located in and managed from secure facilities. Detailed security procedures are in place and followed to prohibit unauthorized access and entry to areas of the facility where CA systems reside.

5.1.1 Physical location of the ECD construction.

The ECD GSE has security measures in place to control access to the building where its infrastructure is located. The digital certification services regulated and provided through this CPD are carried out through a service provider. Access to the rack that houses the servers through which the ECD GSE communication services are managed is only permitted to previously identified and authorized persons who carry a visitor's card in a visible place.
The ECD GSE ensures that PKI servers are in continuous operation virtually in the Amazon cloud.
This provider has procedures to carry out the administration operations of the communications infrastructure of the ECD GSE and where only authorized personnel have access.
The restricted area of the communications center meets the following requirements:

1. Only authorized persons are allowed to enter.
2. Critical communication equipment is properly protected in racks.
3. It does not have windows facing the outside of the building.

4. It is monitored through a closed circuit television 24 hours a day, with cameras both inside and outside the computing center.
5. It has physical access control.
6. Fire protection and prevention systems: smoke detectors, fire extinguishing system.
7. It has personnel trained to respond to catastrophic events.
8. It has a physical intruder detection system.
9. The wiring is properly protected against damage, sabotage attempts or interception by means of conduits

5.1.2 Physical access control mechanisms.
There are several levels of security that restrict access to the communications infrastructure through which ECD GSE provides its services, and each of them has physical access control systems. The facilities have a closed-circuit television service and security personnel. There are restricted areas within the facilities that, due to the type of communications equipment considered critical and sensitive operations handled, are only allowed access to certain people.
5.1.3 Energy and air conditioning.
The communications center has an air conditioning system and an adequate power supply with protection against voltage drops and other electrical fluctuations that could eventually significantly affect the equipment and cause serious damage. Additionally, there is a backup system that guarantees that there is no interruption in the service with sufficient autonomy to guarantee continuity in the service. In the event of a failure in the backup system, there is sufficient time to perform a controlled shutdown.
5.1.4 Exposure to water.
The data centers where PKI services are hosted are isolated from possible sources of water and have flood detection sensors connected to the general alarm system.
5.1.5 Fire prevention and protection.
The communications centre has a fire detection system and a fire extinguishing system. There is a cabling system that protects the internal networks.
5.1.6 Backup System - Media Storage.
Backup, restoration and testing procedures are in place for databases for accredited services.
Mission servers are located in cloud environments, however, on-premises servers are backed up and stored on a local NAS server with its respective contingency.
5.1.7 Waste disposal
Any paper document containing sensitive information about the entity that has reached the end of its useful life must be physically destroyed to ensure that the information cannot be recovered. If the document or information is stored on magnetic media, it must be formatted, permanently erased or the device must be physically destroyed in extreme cases such as damage to storage devices or non-reusable devices, always ensuring that the information cannot be recovered by any means, whether known or unknown at the moment.
5.1.8 Offsite backup.
ECD GSE will maintain a backup copy of the databases on Amazon that will be taken to the replica in case it is required for restoration.

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

5.2 Procedural Controls.
5.2.1 ECD Trust Roles.
The RA has defined the following roles, which cannot be performed by the same person within the area:
- RA Agents: Individuals responsible for daily operations such as: review and approval of applications, attending to all activities related to the digital certification services provided by the ECD GSE through the RA, the functions and responsibilities of the RA agents are defined in accordance with the Profiles and Functions of the ECD GSE.
- RA Administrator: The person responsible for managing and configuring the RA.
- RA Auditor: Trained and impartial person in charge of evaluating compliance with the RA requirements, auditing the RA information systems, clarifying that his/her role is different from that of the internal auditor of the management systems.

5.2.2 Number of people required in each role.
For each of the roles mentioned above, the ECD will guarantee the collaborators to carry out the tasks that affect the management of the ECD's own cryptographic keys.

5.2.3 Identification and authentication of each role.
RA Agents and RA Administrators are authenticated using digital certificates issued by ECD GSE.
Each person only controls the assets necessary for tr role, ensuring that no one person accesses unassigned resources.
Access to resources is carried out depending on the asset through login/password or digital certificates.
5.2.4 Roles that require segregation of duties.
The roles of RA Administrator, RA Agents and RA Auditor are independent.

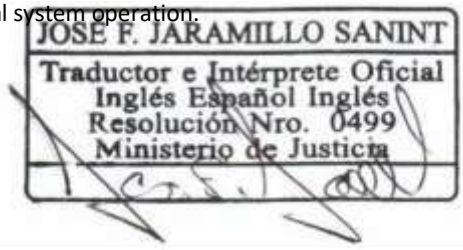
5.3 Personnel controls.
5.3.1 Requirements regarding qualifications, experience and qualification requirements.
A staff selection process has been defined based on the profile of each of the positions involved in the process of issuing digital certificates and the procedures for digital certification services. Candidates for a position must have the training, experience, knowledge and skills defined in the document Job Profile and Duties.
5.3.2 Background check procedure.
Candidates for positions in the certification cycle must present tr current certificate of criminal record, as established in the internal human talent processes of the ECD GSE.
5.3.3 Training requirements.
The training requirements for each of the positions mentioned are found in the Job Profile and Duties which is made known to the person selected to fill the position as part of tr induction. The most important aspects that are part of the training are:
- Knowledge of the Certification Practices Statement.
- Knowledge of current regulations related to open certification entities and the services they provide.
- Knowledge of Security Policies and acceptance of a confidentiality agreement regarding the information handled by virtue of the position.
- Knowledge of software and hardware operation for each specific role.
- Knowledge of security procedures for each specific role.
- Knowledge of operating and administration procedures for each specific role.

5.3.4 Training requirements and frequency of updating.
The annual training program includes an update on Information Security for members of the Digital Certificate Issuance Cycle.
5.3.5 Frequency and sequence of task rotation.
There is no job rotation in the positions mentioned.
5.3.6 Penalties for unauthorized actions.
Performing unauthorized actions is considered a serious offense and individuals will be sanctioned in accordance with a reprimand and/or disciplinary process.

5.3.7 Controls for contracting third parties.
Among the requirements for contracting third parties is knowledge of the Security Policies and a confidentiality clause on the information that is provided or known for reasons of the contractual relationship with GSE.
5.3.8 Documentation provided to staff.
The documentation mentioned in the Training Requirements section is published for easy consultation and is part of the staff induction.

5.4 Audit Log Procedures.
Security audit procedures are performed internally or by third-party audit providers.
5.4.1 Type of events recorded.
The most sensitive activities in the certification cycle require the control and monitoring of events that may occur during tr operation. According to tr level of criticality, events are classified as:
- News: An action ended successfully
- Type of mark: Start and end of a session
- Warning: Presence of an abnormal event but not a fault
- Error: An operation generated a predictable failure
- Fatal error: An operation generated an unpredictable failure

5.4.2 Processing frequency ofLogs.
Audit records are reviewed using manual and/or automated procedures.
Logs are reviewed once a week or when a security alert is detected or there are signs of unusual system operation.



5.4.3 Audit log retention period.

Audit records are kept for three (3) years after the last modification of the file, thus ensuring that the problems presented can be reviewed with those that have been presented in the history. Once the 3 years have passed and with authorization from the GSE Management Committee, they can be destroyed; however, if the records are being used in judicial proceedings, they will be retained for an indefinite period.

5.4.4 Protecting audit logs.

Information system audit logs are maintained in the same manner by keeping one copy on-site and one copy off-site.

5.4.5 Audit log backup procedure.

Audit log backups are replicated to a centralized log site

5.4.6 Audit log collection system (internal or external)

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

5.4.7 Notification to the person responsible for the security incident.

At the discretion of the Information Security Officer, the subject of a security incident detected through audit logs will be notified in order to obtain a formal response regarding what happened.

5.4.8 Vulnerability analysis.

In addition to periodic log reviews, ECD GSE occasionally reviews logs or in response to suspicious activities in accordance with established internal procedures. It also reviews the results obtained from Ethical Hacking and the activities described to correct findings.

5.5 Records Archive.

The archiving and event logging is performed by the ECD GSE NOC SOC.

5.5.1 Types of records to be archived.

A record file is kept of the most relevant events regarding the operations carried out during the process of issuing digital certificates.

5.5.2 Retention period for archiving

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

5.5.3 File protection

The generated files are kept under strict security measures to preserve tr status and integrity.

5.5.4 File Backup Procedures

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

5.5.5 Requirements for time stamping records.

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

5.5.6 File collection system (internal or external).

Audit information, both external and internal, is stored and maintained at a site outside ECD GSE's facilities once it has been digitized. Digitized audit files are only accessed by authorized personnel using viewing tools. At Amazon, they are maintained in the CloudWatch database service.

5.5.7 Procedures for obtaining and verifying file information.

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

5.6 Change of Keys.

ECD GSE root key change.

The procedure for changing the ECD GSE Root keys is the equivalent of generating a new digital certificate. The certificates issued by the subordinates with the previous key must be revoked or the infrastructure must be maintained until the expiration of the last certificate issued. If the decision is made to revoke the certificates and issue new ones, these will not incur any cost for the subscriber or responsible party.

Before the use of the ECD GSE private key expires, a key change will be performed. The old root CA and its private key will only be used for CRL signing as long as there are active certificates issued by the old CA's subordinates. A new root CA will be generated with a new private key and a new DN. The public key will be published in the same repository with a new name that differentiates it from the old one.
Change of keys of the ECD GSE Subordinate.
The procedure for changing the keys of a GSE ECD subordinate is the equivalent of generating a new digital certificate. Certificates issued with the previous key of the subordinate must be revoked or the infrastructure must be maintained until the expiration of the last certificate issued. If the decision is made to revoke the certificates and issue new ones, these will not incur any cost for the subscriber or responsible party.
Before the use of the ECD GSE slave's private key expires, a key exchange will be performed. The previous ECD slave and its private key will only be used for CRL signing as long as there are active certificates issued by the previous ECD slave. A new ECD GSE slave will be generated with a new private key and a new DN. The public key will be published in the same repository with a new name that differentiates it from the previous one.
5.7 Disaster Engagement and Recovery.

5.7.1 Incident management procedures and engagements
The GSE ECD has an established and tested Information Security Incident Procedure that establishes the actions to be taken in the event of a vulnerability or security incident. Once the procedures for restoring the systems have been satisfactorily executed, service will be provided to the public.
5.7.2 Procedure in case of damage to computer resources, software and/or data.
If there is a suspicion of alteration of the hardware, software or data resources, the operation of the ECD GSE will be stopped until the security of the environment is restored. To avoid a repeat incident, the cause of the alteration must be identified. If this occurs, ECD GSE will inform ONAC, giving an explanation and justification.
5.7.3 Recovery procedure in the event of ECD private key compromise.
The GSE ECD has established and tested a Business Continuity Plan that defines the actions to be taken in the event of a vulnerability of the private key of the GSE ECD root or one of its subordinates. In these cases, the compromised private keys of the GSE ECD and the certificates signed under its hierarchy must be immediately revoked. A new private key must be generated and new certificates must be issued at the request of the subscribers and/or those responsible.
Additionally, this plan will be executed under the following scenarios:
1. When the security system of the certification authority has been breached.
2. When failures occur in the certification entity's system that compromise the provision of the service.
3. When encryption systems lose validity because they do not offer the level of security contracted by the subscriber.

4. When any other information security event or incident occurs. In the event of a GSE ECD compromise:
1. Apply incident containment to prevent reoccurrence
2. You will inform all Subscribers, Controllers, Relying Third Parties and other CAs with whom you have agreements or other relationships of the engagement.
3. It will indicate that certificates and revocation status information signed using this key are invalid.
4. ONAC will inform customers.

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

5.8 Termination of the CA or RA.
Procedure in case of termination of the CA and the RA
In accordance with the provisions of Article 34 of Law 527 of 1999, amended by Article 163 of Decree Law 019 of 2012 and in accordance with Decree 333 of 2014, open digital certification entities must inform ONAC and the Superintendency of Industry and Commerce of the cessation of activities at least 30 days in advance.
The ECD - GSE will inform all subscribers and/or responsible parties through two notices published in newspapers or media of wide national circulation, with an interval of 15 days, about:

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

- The termination of the activity or activities and the precise date of cessation.
- The legal consequences of cessation with respect to accredited services
- The possibility for a subscriber to obtain a refund equivalent to the value of the remaining validity time on the contracted service.
- The authorization issued by the Superintendency of Industry and Commerce so that the ECD can cease the service, and if applicable, the CRL operator responsible for the publication of the certificates issued by the ECD - GSE until the last of them expires.

The ECD GSE will inform the name of the entity that will guarantee the continuity of the service for those who have contracted, directly or through third parties, services from the ECD GSE, without additional costs. If the continuation of the service through the third party is not accepted, the subscriber and/or responsible party may request the revocation and reimbursement equivalent to the value of the remaining validity time of the digital certification service, if requested within two (2) months following the second publication on the website and notices.
The ECD GSE has a safety plan in case of cessation of activities, which includes the guidelines and activities for its execution.

6. TECHNICAL SAFETY CONTROLS.

6.1 Generation and Installation of Key Pairs.

6.1.1 Generating the key pair

From the Root ECD.
The generation of the ECD Root key pair was carried out at the platform service provider's facilities with the strictest security measures and under the key generation ceremony protocol established for this type of event and in the presence of an ECD delegate. A FIPS 140-2 level 3 approved cryptographic device was used to store the private key.
From the subordinates of ECD GSE.
The generation of the ECD GSE subordinate key pair was carried out at the ECD GSE service provider's facilities under the key generation ceremony protocol. A FIPS 140-2 level 3 certified cryptographic device is used to store the subordinate private key.
From subscribers or those responsible for ECD GSE.
The generation of the key pair for ECD GSE subscribers is carried out at the ECD GSE service provider's facilities. A FIPS 140-2 level 3 certified cryptographic device is used to store the subscriber's private key.

6.1.2 Delivery of the private key to subscribers.

The private key is delivered to the subscriber and/or responsible party in tr cryptographic device and cannot be extracted. Therefore, there is no copy of the subscriber's private key.

6.1.3 Delivery of the public key to the certificate issuer.

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

6.1.4 Delivery of the CA's public key to the partiesconfident.

The public key of the Root ECD and the Subordinate ECD is included in tr digital certificate.
The Root ECD certificates can be consulted by trusted third parties in the repositories listed in section
4.1 Repositories, ECD GSE Root Certificates.
The certificates of the Subordinate ECD can be consulted by trusted third parties in the repositories listed in section 4.1 Repositories, Subordinate ECD GSE Certificates.

6.1.5 Key Size.

The following key sizes are defined for RSA:

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

When trying to derive the private key from the 2048-bit public key contained in the end-user certificates, the problem lies in finding the prime factors of two large numbers, since there would be 22047 possibilities for each number. It is estimated that decrypting a 2048-bit public key would require processing work in the order of 3 X 1020 MIPS-year*

- MIPS-year: Unit used to measure the processing capacity of a computer operating for one year. It is equivalent to the number of millions of instructions that a computer is capable of processing per second for one year.

The following key sizes have been defined for ECDSA:

- ECD Root of ECD GSE is 384 bits.
- Subordinate ECD GSE is 384 bits.

- Certificates issued by ECD GSE to end users are 256-bit.

For elliptic curve, a specific published base point G is chosen for use with the curve E(q) and then a random integer k is chosen as the private key. The corresponding public key would be P=k*G and is made public. The discrete algorithm problem says that it is an exponential complexity problem to derive k from P. It is estimated that it takes 2.4x1026 MIPS-years to derive a 256-bit elliptic curve public key.

6.1.6 Public key generation parameters and quality control.

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

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

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

6.1.7 Key usage purposes (according to the X.509 v3 key usage field).

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

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

CERTIFICATE TYPE KEY USAGE

Digital Signature Certificate Signature Non Repudiation Authentication Certificate

6.2 Private key protection and engineering controls of cryptographic modules.

6.2.1 Standards and controls for the use of cryptographic modules.

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

6.2.2 Controlmulti-person (n of m) of the private key.

The private keys of the ECD GSE Root and the private keys of the ECD GSE Subordinates are under multi-person control. The method of activating the private keys is by initializing the ECD GSE software using a combination of keys held by multiple people.

6.2.3 Custody of the ECD private key.

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

The technical data of the device are as follows:

• SafeNet Luna SA

The private key of the end-user digital certificates is under the exclusive control and custody of the subscriber or controller. Under no circumstances does ECD GSE keep a copy of the subscriber's private key or certificate managed by the controller, since it is generated by the subscriber or controller and cannot be accessed by ECD GSE.

6.2.4 Backup copy of the private key.

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

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

6.2.5 Private key file.

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

These are located in a cryptographic backup box in a different location from where the HSMs are located.

6.2.6 Transfer of private keys to or from a cryptographic module.

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

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

6.2.7 Storing the private key in the cryptographic module.

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

Cryptographic keys can be loaded into a similarly performing cryptographic device from backup copies through a process that requires the involvement of at least two operators.

6.2.8 Private key activation method.

The private keys of the GSE Root ECD and the Subordinate ECDs are under multi-person control. The method of activating the private key is by initializing the GSE ECD software through a combination of keys held by multiple operators.

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

6.2.9 Private key deactivation method.

The private key is deactivated by deactivating the software or shutting down the ECD server. It is reactivated by using multi-person control, following the procedures set by the manufacturer of the cryptographic module.

6.2.10 Method to destroy the private key.

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

6.2.11 Cryptographic module classification.

The cryptographic devices used by ECD GSE comply with what is indicated in Annex F: Cryptographic Devices, of the CEA.

Evaluation of the cryptographic module.

The cryptographic device is monitored by its own software to prevent possible failures. Evaluation of the encryption system.

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

will immediately take the measures and recommendations issued by this entity or by ONAC to maintain the security of the firm during the remainder of its life cycle.

6.3 Other Aspects of Key Pair Management.

6.3.1 Public key file.

ECD GSE will maintain controls over the archiving of its own public key.

6.3.2 Operating periods of certificates and period of use of the key pair.

The period of use of the key pair is determined by the following validity of each certificate: RSA Algorithm:

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

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

ECDSA algorithm:

The validity period of the ECDSA digital certificate and the Root key pair is twenty-five (25) years. The validity period of the ECDSA digital certificate and the Subordinate key pair is ten (10) years.

6.4 Activation Data.

6.4.1 Generation and installation of activation data.

For the operation of the ECD GSE, passwords are created for the operators of the cryptographic device and will be used together with a PIN to activate the private keys.

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

6.4.2 Protection of activation data.

Knowledge of the activation data is personal and non-transferable. Each party involved is responsible for its safekeeping and must treat it as confidential information.

6.4.3 Other aspects of activation data.

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

6.5 Computer Security Controls.

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

- Operating system security settings.
- Application security settings.
- Access control to devices.
- Closing system vulnerabilities.
- Hardening systems according to good practices.
- Network configuration at security level (Internal Network, Administrative Network, among others)
- User and Permissions Configuration.
- Log Event Configuration.
- Plan ofbackup and recovery.
- Antivirus settings.
- Network traffic requirements configured on the firewall.

6.5.1 Specific technical requirements for computer security.
ECD GSE has a technological infrastructure that is duly monitored and equipped with the security elements required to guarantee the availability established in the CEA and confidence in the services offered to its subscribers, entities and trusted third parties.
Information related to Information Security is considered confidential and therefore can only be provided to those control entities that require its knowledge.
6.5.2 Computer security classification.
The security of end-user equipment is managed from ECD GSE and is supported by a risk analysis so that the security measures implemented are responses to the probability and impact produced by a group of defined threats that can take advantage of security breaches.

In addition, security tests (ethical hacking) are carried out periodically to identify possible system vulnerabilities and help close them.
Actions in the event of an information security event or incident.
The Information Security Management System implemented by ECD GSE has established an incident management procedure that specifies the actions to be executed, components or resources to be used and how personnel should react in the event of an intentional or accidental event that disables or degrades the resources and digital certification services of ECD GSE.
1. Incident detection and reporting: Security incidents must be reported via email.
seguridad.informaciontaase.com.co. which is managed by the ECD GSE Information Security Officer
Incidents may be detected through monitoring systems, intrusion detection systems, system logs, notification by staff or by subscribers and/or managers.
1. Incident analysis and evaluation: Once the incident has been detected, the response procedure is determined and the responsible persons are contacted to evaluate and document the actions to be taken according to the severity of the incident. An investigation is carried out to determine the scope of the incident, that is, to find out how far the attack went and to obtain as much information as possible about the incident.
2. Incident damage control: React quickly to contain the incident and prevent it from spreading by taking measures such as blocking access to the system.
3. Investigation and evidence gathering: Review audit logs to track what happened.
4. Recovery and incident countermeasures: Restore the system to its correct operation and document the procedure and ways to prevent the incident from occurring again.
5. Post-incident analysis to improve the procedure: Perform an analysis of everything that happened, detect the cause of the incident, correct the cause for the future, analyze the response and correct errors in the response.

6.6 Life Cycle Technical Controls.
6.6.1 Systems development controls.
The GSE ECD complies with established change control procedures for new software developments and updates.
6.6.2 Security management controls.
ECD GSE maintains control over the inventories of assets used in its certification process. These are classified according to tr risk level.
ECD GSE periodically monitors its technical capacity in order to guarantee an infrastructure with the minimum availability requested in the CEA.
6.6.3 Lifecycle security controls.

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

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

6.7 Network Security Controls.

ECD GSE has a network infrastructure that is duly monitored and equipped with the security elements required to guarantee the availability and confidence in the services offered to its subscribers, entities and bona fide third parties. Information related to Information Security is considered confidential and therefore can only be provided to those control entities that require its knowledge.

6.8 Chronological Print.

ECD GSE has a time stamping service, which is described in the corresponding Certificate Policies for Time Stamping Service, published on the portal http://www.ase.com.co.

7. CERTIFICATE, CRL AND OCSP PROFILES.

7.1 Certificate Profile.

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

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

1. Name, address and domicile of the subscriber.
2. A unique ID of the subscriber named in the certificate.
3. The name and place where the CA carries out activities

Field	RSA Value or Restrictions	ECDSA value or restrictions
Version	3 (0x2)	3 (0x2)
Serial Number	Unique identifier issued by ECD GSE	Unique identifier issued by ECD GSE
Signature Algorithm	SHA256withRSAEncryption	SHA384withECDSA
Transmitter	See section "Rules for the interpretation of various forms of name". For ECD GSE as issuer, the following is specified: E=info@gse.com.co, CN=Subordinate Authority 01 GSE, OU = PKI, 0=GSE, L=Bogota DC, C=CO	See section "Rules for the interpretation of various forms of name". For ECD GSE as issuer, the following is specified: STREET=www.gse.com.co, E=info@gse.com.co, CN=GSE ECDSA SUBORDINATED, SN = 900204278, OU=GSE ECDSA R2 SUB1, 0=GESTION DE SEGUIRDAD ELECTRONICA SA, L=Bogota DC, S=Capital District, C=CO
Valid from	Specifies the date and time from which the certificate is valid.	Specifies the date and time from which the certificate is valid.
Valid until	Specifies the date and time after which the certificate becomes invalid.	Specifies the date and time after which the certificate becomes invalid.
Subject	In accordance with the policy in Annex 1 and the "Rules for the interpretation of various forms of name".	In accordance with the policy in Annex 1 and the "Rules for the interpretation of various forms of name".
Public key of the Subject	Encoded according to RFC 5280. Certificates issued by ECD GSE are 2048 bits long and RSA algorithm.	Encoded according to RFC 5280. Certificates issued by ECD GSE are 256 bits long and use the EC algorithm.
Authority Key Identifier	It is used to identify the root certificate in the certification hierarchy. It usually references the ECD GSE "Subject Key Identifier" field as the digital certification authority.	It is used to identify the root certificate in the certification hierarchy. It usually references the ECD GSE "Subject Key Identifier" field as the digital certification authority.

Subject key identifier	It is used to identify a certificate that contains a certain public key.	It is used to identify a certificate that contains a certain public key.
Certificate Guidelines	Describes the policies applicable to the certificate, specifies the OID and the URL where the certification policies are available.	Describes the policies applicable to the certificate, specifies the OID and the URL where the certification policies are available.
Using the key	Specifies the permitted uses of the key. This is a CRITICAL FIELD.	Specifies the permitted uses of the key. This is a CRITICAL FIELD.
CRL Distribution Point	It is used to indicate the addresses where the ECD GSE CRL is published. In the Root ECD certificate, this attribute is not specified.	It is used to indicate the addresses where the ECD GSE CRL is published. In the Root ECD certificate, this attribute is not specified.
Access to information from the Authority	It is used to indicate the addresses where the ECD GSE root certificate is located. Also, to indicate the address to access the OCSP service. In the ECD GSE root certificate, this attribute is not specified.	It is used to indicate the addresses where the ECD GSE root certificate is located. Also, to indicate the address to access the OCSP service. In the ECD GSE root certificate, this attribute is not specified.
Alternative name of the subject	It is used to indicate the email address and additionally to indicate the accreditation code assigned by the ONAC. Name RFC822=email@company.com URL= https://ase.com.co/documentos/certifications/accreditation/16-ECD-001.pdf	It is used to indicate the email address and additionally to indicate the accreditation code assigned by the ONAC. Name RFC822=email@company.com URL= https://ase.com.co/documentos/certifications/accreditation/16-ECD-001.pdf
Extended uses of the key	Additional purposes for using the key are specified.	Additional purposes for using the key are specified.
Basic restrictions	The "PathLenConstraint" extension indicates the number of sub-levels that are allowed in the certificate path. There is no restriction for ECD GSE, so it is zero.	The "PathLenConstraint" extension indicates the number of sub-levels that are allowed in the certificate path. There is no restriction for ECD GSE, so it is zero.

7.1.1 Version numbers.

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

7.1.2 Certificate extensions.

The certificates issued by GSE are described in detail in Annex 1 of this CPS. Key Usage.

The "key usage" is a critical extension that indicates the use of the certificate according to RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

Certificate Policy Extension.

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

Alternative name of the subject.

The "subjectAltName" extension is optional and the use of this extension is "Not critical". Basic restrictions.

In the case of ECD GSE, the "PathLenConstraint" field of the certificate of the subordinates has a value of 0, to indicate that the ECD GSE does not allow more sub-levels in the certificate path. This is a critical field.

Extended use of the key.

This extension allows you to define additional purposes for the key. It is considered non-critical. The most common purposes are:

OID	Description	Types of Certificates
1.3.6.1.5.5.7.3.4	Mail protection	Digital Signature of a Natural Person and Electronic Agent
1.3.6.1.5.5.7.3.8	Time stamping	Time stamping
1.3.6.1.5.5.7.3.34	TLS Web Server Authentication	All types of certificate

7.1.3 Algorithmic object identifiers.

The object identifier of the signature algorithm is:

1.2.840.113549.1.1.11 SHA256 with RSA Encryption

The object identifier of the public key algorithm is:

1.2.840.113549.1.1.1 rsaEncryption
The object identifier of the signature algorithm is:
1.2.840.10045.4.3.3 SHA384WITHECDSA.
The object identifier of the public key algorithm is:
1.2.840.10045.2.1 ecPublicKey-id
7.1.4 Forms of names.
In accordance with the specifications in the Types of names section of this DPC.
7.1.5 Naming restrictions.
Names must be written in capital letters and without accents.
The country code is assigned according to the ISO 3166-1 standard "Codes for the representation of the names of countries and tr subdivisions - Part 1: Country codes". For Colombia it is "CO".
7.1.6 Certification Policy object identifier.
The object identifier of the Certificate Policy corresponding to each type of certificate is a subclass of the class defined in the Document Name and Identification section of this CPD, as established in the Certificate Policies for digital certificates.
7.1.7 Using the extensionPolicy Constraints.
Not stipulated.
7.1.8 Syntax and semantics of thePolicy Qualifiers
The policy qualifier is defined in the "Certificate Policies" extension and contains a reference to the URL where the DPC is published.
7.1.9 Semantic treatment for the extensionCertificate Policies.
Not stipulated.

7.2 CRL Profile.

CRLs issued by ECD GSE comply with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" and contain the following basic elements.
7.2.1 Version number(s)
CRLs issued by ECD GSE comply with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" and contain the following basic elements:
7.2.2 CRL and CRL Entry Extensions
Information about the reason for revocation of a certificate will be included in the CRL, using the CRL extensions and more specifically in the revocation reason field (reasonCode).

7.3 OCSP Profile.
The OCSP service complies with RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".
7.3.1 Version number(s)
Complies with OCSP Version 1 of RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" and RFC6019 "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments".
7.3.2 OCSP Extensions
The singleExtensions of an OCSP response DO NOT CONTAIN the CRL entry extension reasonCode (OID 2.5.29.21).

8. COMPLIANCE AUDIT AND OTHER EVALUATIONS.
8.1 Frequency or Circumstances of the Evaluation.
Compliance with controls that guarantee security in the issuance of digital certificates will be assessed through an annual audit conducted by an external audit firm.
8.2 Identity and qualifications of the evaluator.
In accordance with Decree 333 of 2014 and specifically in Article 14. Audits. Certification entities must comply with third-party audits under the terms set forth in the Specific Accreditation Criteria established by ONAC.
Assurance requirements: Legally incorporated auditing firm in Colombia whose corporate purpose includes: systems auditing services, information security and public key infrastructure (PKI). The auditing group's competencies must be demonstrated with respect to the specific accreditation criteria, the requirements of the international standard ISO/IEC 27001 regarding information security, in relation to the ISO 9001 or ISO/IEC 20000-1 service. In the event that the auditor does not have competency in PKI, he/she must be accompanied by a technical expert familiar with the

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

management related to public key infrastructure (PKI). The auditing staff must have a valid professional engineering card.

8.3 Relationship of the evaluator with the entity evaluated.

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

8.4 Topics to be evaluated.

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

8.5 Actions taken as a result of the deficiency.

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

8.6 Communication of Results.

Once the audit is completed, the auditing firm must submit the audit report to ECD GSE and, if required, ECD GSE must establish corrective and improvement actions. The final report must be submitted to ONAC.

9. OTHER COMMERCIAL AND LEGAL MATTERS.

9.1 Fees.

Not Applicable.

9.1.1 Fees for issuing or renewing certificates

GSE charges fees for the issuance and renewal of certificates. GSE may modify its fees in accordance with the applicable customer agreement. See fee table in section 9.17.

9.1.2 Access fees to certificates

Unless specified in the applicable legal agreements or CP of a third party partner, GSE may charge a reasonable fee for access to its certificate databases.

9.1.3 Rates for access to information on revocation or status

GSE does not charge fees for certificate revocation or for checking the validity status of an issued certificate using a CRL. GSE may charge a fee for providing certificate status information through OCSP.

9.1.4 Fees for other services

Without stipulation.

9.1.5 Refund Policy

As set forth in the applicable customer agreement with GSE.

9.2 Financial Responsibility.

9.2.1 Insurance or coverage guarantee for subscribers, responsible parties and bona fide third parties.

In compliance with Article 9. Guarantees, of Decree 333 of 2014, ECD GSE has acquired insurance issued by an insurance company authorized to operate in Colombia, which covers all contractual and non-contractual damages of subscribers, responsible parties and third parties in good faith without fault arising from errors and omissions, or acts of bad faith by the directors, legal representatives or employees of ECD GSE in the development of the activities for which it is authorized.

9.2.2 Other assets.

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

9.2.3 Insurance or guarantee coverage for end entities

Without stipulation.

9.3 Confidentiality of Commercial Information.

9.3.1 Scope of confidential information.
ECD GSE is committed to protecting all data to which it has access as a result of its activity as an ECD.
All non-public information is considered confidential and therefore restricted access, except in those cases provided for by law such as courts or competent administrative bodies or imposed by law. Confidential information is not disclosed without the express written consent of the subscriber or the entity that has granted it confidentiality.
However, it reserves the right to disclose to employees and consultants, external or internal, the confidential data necessary to carry out its activities as an ECD, requiring all staff to sign a confidentiality agreement within the framework of the contractual obligations entered into with ECD GSE.
Confidential information.
The following information is considered confidential:

1. Private key of the Certification Authority and/or ECD
2. Private key of the subscriber or entity
3. Information provided by the subscriber or entity and not necessary to validate the subscriber's or entity's trust
4. Information about the applicant, subscriber and/or controller obtained from different sources (for example, from a complainant or regulators)
5. Transaction records
6. Audit logs
7. Security Policies
8. Business Continuity Plan
9. All information that is classified as "Confidential" in the documents delivered by ECD GSE

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

1. The one contained in this Certification Practices Statement and its annexes.
2. The one contained in the repository on the status of the certificates.
3. The list of revoked certificates.
4. All information that is classified as "PUBLIC" in the documents delivered by ECD GSE.

9.3.3 Duty to protect confidential information.
ECD GSE maintains security measures to protect all confidential information provided to ECD GSE directly or through the channels established for this purpose from receipt to storage and custody, where it will remain in accordance with the TRD. ECD GSE has an Integrated Management System that includes an Information Security System. This allows us to ensure that our subscribers' information will not be compromised or disclosed to third parties unless there is a formal request from a competent authority that requires it.

9.4 Privacy of Personal Information.
9.4.1 Privacy Plan - Personal Data Processing Policy.
The ECD GSE has a Personal Data Processing Policy in accordance with the provisions of Law 1581 of 2012, Decree 1377 of 2013, and other regulations that add, modify, complement, or replace it, which can be consulted on our website https://ase.com.co/Politicas in the Personal Data Processing Policy section, and you can also consult the authorization for the processing of personal data.
9.4.2 Information treated as private.
The personal information provided by the subscriber or controller and required for the approval of the digital certificate is considered private information.
9.4.3 Information that is not considered private.
These are personal data that the regulations and the Constitution have expressly determined as public, the collection and processing of which does not require the authorization of the owner of the information.
9.4.4 Responsibility to protect private information.
ECD GSE is responsible and has the appropriate technological resources to help ensure the proper custody and conservation of personal data collected through the channels used by the company, in compliance with Law 527 of 1999 "Article 32. Duties of certification entities. Certification entities shall have, among others, the following duties: Guarantee the protection, confidentiality and proper use of the information provided by the subscriber, responsible party and entity."

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

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

9.4.5 Notice and consent to use private information.

Personal data may not be disclosed to third parties without due notification and consent of the owner, in accordance with the applicable regulations on the protection of personal data.

9.4.6 Disclosure pursuant to a judicial or administrative procedure.

Personal data may be disclosed when required by one of the public or administrative entities in the exercise of its legal functions or by court order without due notification and consent of its owner, in accordance with current personal data protection regulations.

9.4.7 Other circumstances of disclosure of information.

ECD GSE's privacy policy is strictly established by the data protection law: "Private information will be that which, whether it concerns personal information or not, and which, because it is in a private sphere, can only be obtained or offered to third parties authorized by the Subscriber or responsible party or by law."

• Security system to protect information.

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

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

to. ISO 27001

b. ISO 9001

2. Penetration testing and vulnerability scanning on the network, carried out by a company specialized in Ethical Hacking.

9.5 Intellectual Property Rights.

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

9.6 Representations and Warranties.

The ECD GSE will always have civil liability insurance in accordance with the provisions of decree 333 of 2014 with coverage of 7,500 legal monthly minimum wages per event.

The ECD GSE will act to cover its responsibilities on its own or through the insurance entity, satisfying the requirements of the certificate applicants, the subscribers/responsible parties and the third parties who trust in the certificates.

The responsibilities of the ECD GSE include those established by this CPS, as well as those that are applicable as a consequence of Colombian and International Regulations.

ECD GSE shall be liable for any damage caused to the Subscriber, Entity or any person who in good faith relies on the certificate, provided that there is fraud or gross negligence, with respect to:

- The accuracy of all information contained in the certificate at the date of issue.
- The guarantee that, at the time of delivery of the certificate, the Subscriber has in his possession the private key corresponding to the public key given or identified in the certificate.
- The guarantee that the public and private keys work together and complementarily.
- The correspondence between the requested certificate and the certificate delivered.
- Any liability established by current legislation.

9.6.1 CA Representations and Warranties

Except as expressly provided in this CPS or in a separate agreement with a Subscriber, GSE makes no representations regarding its products or services. GSE represents, to the extent specified in this CPS, that: GSE complies, in all material respects, with the CP, this CPS and all applicable laws, GSE regularly publishes and updates the CRL and the database for generating OCSP responses.

9.6.2 RA Representations and Warranties

The RA states that:

1. RA certificate issuance and management services are in line with the GSE PC and this DPC,
2. The information provided by the RA does not contain any false or misleading information,
3. Translations performed by the RA are an exact translation of the original information, and

4. All certificates requested by the RA comply with the requirements of this CPS. The GSE agreement with the RA may contain additional statements.
The Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber's Representations and Warranties
Prior to being issued and receiving a Certificate, Subscriber shall be solely responsible for any misrepresentations made to third parties and for all transactions in which Subscriber's Private Key is used, whether or not such use was authorized. Subscribers are required to notify GSE if a change occurs that may affect the status of the Certificate or application.
Subscribers undertake to comply with the commitments and guarantees of this CPS and the following points:
1. In case of generating requests in PKCS#10 format, you must securely generate your Private keys and protect your Private keys from any compromise,
2. Provide accurate and complete information when communicating with GSE,
3. Confirm the accuracy of the certificate data before using it,
4. Immediately if applicable:

(Yo) request revocation of a Certificate, cease using it and its associated Private key, and notify GSE if misuse or compromise of the Private key associated with the public key included in the certificate occurs or is suspected, and
(ii) request revocation of the Certificate, and stop using it, if any information in the Certificate is or becomes incorrect or inaccurate,

5. Ensure that individuals using certificates on behalf of an organization have received appropriate security training related to the Certificate,
6. Use the Certificate only for authorized and legal purposes, in accordance with the purpose of the Certificate, this CPS, any applicable CP, and the applicable Subscriber Agreement.
7. Use the Certificate only for authorized and legal purposes, consistent with the Certificate's purpose, this CPS, any applicable PC, and the applicable Subscriber Agreement, including installing Certificates only on authorized servers with the Subscriber's consent, and
8. Immediately cease using the certificate and associated private key upon certificate expiration. Subscription agreements may include additional representations and warranties.
9.6.4 Representations and warranties of the partyConfident
Each Relying Party represents that, before relying on a Certificate issued by GSE:
1. Gained sufficient knowledge on the use of Digital Certificates and PKI,
2. You have reviewed the limitations applicable to the use of Certificates and agree to GSE's limitations of liability relating to the use of Certificates,
3. You have read, understand and agree to the Part AgreementConfident of GSE and this DPC,
4. You have verified both the subscriber certificates issued by GSE and the certificates in the certification chain using the appropriate CRL or OCSP,
5. You will not use a certificate issued by GSE if the certificate has expired or been revoked, and
6. You will take all reasonable steps to minimize the risk associated with relying on a digital signature, including relying only on a certificate issued by GSE after considering:

to) applicable law and legal requirements for the identification of the parties, the protection of confidentiality or privacy of information, and the applicability of the transaction;
b) the intended use of the Certificate as listed in the certificate or in this CPS,
c) the data listed in the Certificate
d) the economic value of the transaction or communication
and) the potential loss or damage that would be caused by a misidentification or a loss of confidentiality or privacy of the information in the request, transaction or communication,
F) the Relying Party's prior track record with the subscriber,
g) the relying party's business knowledge, including experience with computerized business methods, and
h) any other indication of reliability or unreliability in relation to the subscriber and/or the application, communication or transaction.
Any unauthorized reliance on a Certificate is at the relying party's own risk. Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and warranties of other participants
Not Applicable
9.7 Disclaimer of Warranties.
Not Applicable
9.8 Limitations of Liability.
Responsibility for the veracity of the Subscriber's information.
The Subscriber assumes all risks for damages that may arise from conduct such as providing false information, impersonating third parties, validating incomplete or outdated documents or information.
Responsibility for service availability.
The Subscriber undertakes to act diligently to reduce to a minimum the possibility of failures or interruptions that may occur within its organization. Failures caused by the incapacity or inadequacy of the Subscriber's equipment, or by its lack of knowledge regarding the use of the service, shall in no case be attributable to ECD GSE and no compensation for any damages may be required from it.
Responsibility for the functionality of the service on the Subscriber's infrastructure.
The Subscriber shall be solely responsible for the provision and payment of the costs necessary to ensure the compatibility of the service (digital signature certificate) with its equipment, including all hardware, software, electrical components and other physical or logical components required to access and use it, including, but not limited to, telecommunications services, Internet access and connection, links, browsers, or other programs, equipment and services required to access and use the service.
Responsibility for computer crimes.

In the event that the Subscriber is the victim of any of the conduct classified as a crime by Law 1273 of 2009 (Computer Crimes Law) in its information systems, in its applications and technological infrastructure, in the execution of electronic transactions or in access to and use of the service, phishing attacks, identity theft, due to negligence in the management and confidentiality of the digital certificate, the Subscriber will be solely responsible and will remedy any damages that may arise, since it is its obligation to adopt security measures, policies, cultural campaigns, legal instruments and other mechanisms to safeguard the confidentiality and proper use of its digital certificate.
Disclaimers of warranties.
ECD GSE will not be liable under any circumstances when faced with any of these circumstances:

- State of war, natural disasters, terrorism, strikes or any other case of Force Majeure.
- For the use of certificates provided that it exceeds the provisions of current regulations and this CPS and its Annexes.
- For improper or fraudulent use of certificates orCRLs issued by the Certification Authority.
- For the use of the information contained in the Certificate or in the CRL.
- For failure to comply with the obligations established for the Subscriber, Entities, Controllers or Third Parties that rely on current regulations, this CPS and its Annexes.
- For the damage caused during the period of verification of the causes of revocation/suspension.
- For the content of digitally signed or encrypted messages or documents.
- Due to the non-recovery of documents encrypted with the public key of the Subscriber or Entity.
- Fraud in the documentation submitted by the applicant.

9.9 Compensation.
Not Applicable.
9.10 Duration and Termination.

9.10.1 Duration.
The CPD and PC enter into force from the moment they are published on the ECD GSE website, from that moment the previous version of the document is repealed and the new version completely replaces the previous version.
ECD GSE keeps previous versions of the DPC and PC in the repository.
9.10.2 Termination.
For digital certificates that have been issued under an older version of the DPC or PC, the new version of the DPC or PC applies in everything that does not contradict the statements of the previous version.
9.10.3 Effect of termination, notification and communication.

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

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

9.10.4 Procedure for Changing the DPC and PC Changes that affect the DPC and PC.

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

1. The Management Committee will approve any changes it deems appropriate to the CPD and PC.
2. The updated CPD and PC are posted on the GSE ECD website once approved by the Management Committee.

Circumstances under which the OID must be changed.

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

1. The authorization of a new certification hierarchy, event in which the OIDs must be defined according to the structure.
2. In the event of changes to the DPC and PC that affect the acceptability of digital certification services, the OID adjustment is carried out.

These types of modifications will be communicated to the users of the certificates corresponding to the PC or DPC.

9.11 Individual notifications and communications to participants.

9.11.1 Obligations of the ECD GSE.

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

1. Comply with the provisions of current regulations, this CPD and the PC Certification Policies.
2. Publish this CPD and each of the Certification Policies on the GSE Website.
3. Inform ONAC about changes to the CPD and Certification Policies.
4. Maintain the CPD with its latest version published on the GSE website.
5. Safely and responsibly protect and store your private key.
6. Issue certificates in accordance with the Certification Policies and the standards defined in this CPS.
7. Generate certificates consistent with the information provided by the applicant or subscriber.
8. Maintain information on digital certificates issued in accordance with current regulations.
9. Issue certificates whose minimum content complies with current regulations for the different types of certificates.

LO. Publish the status of issued digital certificates in a freely accessible repository. Ll. Do not keep a copy of the private key of the applicant or subscriber.

L2. Revoke digital certificates as provided in the Digital Certificate Revocation Policy.

L3. Update and publish the list of revoked digital certificates CRL with the latest revoked certificates.

L4. Notify the Applicant, Subscriber or Entity of the revocation of the digital certificate within 24 hours of the revocation of the certificate in accordance with the digital certificate revocation policy.

L5. Inform subscribers of the proximity of the expiration of tr digital certificate.

L6. Have qualified personnel with the knowledge and experience necessary to provide the certification service offered by the ECD GSE.

L7. Provide the applicant with the following information free of charge and with open access on the ECD GSE website, complying with the parameters and characteristics of current regulations without misleading:

- The Certification Practices Statement, its Annexes, the Certificate Policies and all updates to the aforementioned documents.
- Obligations of the subscriber and the manner in which data must be safeguarded.
- Procedure for requesting the issuance of a certificate.
- The procedure for revoking your certificate.
- The conditions and limits of the use of the certificate

L8. Verify, either by itself or through a different person acting on its behalf and on its account, the identity and any other circumstances of the applicants or of the data of the certificates, which are relevant for the purposes of the verification procedure prior to tr issue.

L9. Immediately inform the Superintendency of Industry and Commerce and the ONAC of any event that compromises or may compromise the provision of the service.

20. To promptly report any modification or update of services included in the scope of accreditation, in accordance with the terms established by the procedures, rules and requirements of the ONAC accreditation service.

21. Update contact information whenever there is a change or modification to the data provided.

22. Train and warn users about the security measures they must observe and about the logistics required to use the service provision mechanisms.
23. Guarantee the protection, integrity, confidentiality and security of the information provided by the subscriber by keeping the documentation supporting the certificates issued.
24. Guarantee the conditions of integrity, availability, confidentiality and security, in accordance with current national and international technical standards and with the specific accreditation criteria thatfor this purpose, the ONAC establishes.
25. Provide the accredited services on the ECD GSE website.

9.11.2 Obligations of the RA.

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

1. Know and comply with the provisions of this CPS and the Certification Policies corresponding to each type of certificate.
2. Safeguard and protect your private key.
3. Review and/or verify the initial validation records of the identity of the Applicants, Controllers or Subscribers of digital certificates.
4. Verify the accuracy and authenticity of the information provided by the Applicant.
5. Archive and safeguard the information and/or documentation provided by the applicant or subscriber for the issuance of the digital certificate, for the time established by current legislation.
6. Respect the provisions of signed contractsbetween ECD GSE and the subscriber.
7. Identify and inform the ECD GSE of the reasons for revocation provided by applicants regarding current digital certificates.

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

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

1. Use your digital certificate or electronic signature certificate in accordance with the terms of this CPS.
2. Check within the next business day that the information on the digital certificate is correct. If you find any inconsistencies, notify the ECD.
3. Refrain from: lending, transferring, writing, publishing the password for using your digital certificate and take all necessary, reasonable and appropriate measures to prevent it from being used by third parties.
4. Do not transfer, share or lend the cryptographic device to third parties.
5. Provide all the information required in the application form or using the channels, means or mechanisms provided by GSE for the request of digital certificates to facilitate tr timely and full identification.
6. Request revocation of the digital certificate due to a change of name and/or surname.
7. Request revocation of the digital certificate when the Subscriber has changed nationality.
8. Comply with what is accepted and/or signed in the terms and conditions document.
9. Provide the required information accurately and truthfully.
10. Report any changes to the data initially provided for issuing the certificate during the validity of the digital certificate.
11. Responsibly safeguard and protect your private key.
12. Use the certificate of compliance with the PC established in this CPS for each of the types of certificate.
13. As a subscriber and/or responsible party, request the immediate revocation of your digital certificate when you become aware that there is a cause defined in section Circumstances for the revocation of a certificate of this document.

DPC.

14. Do not use the private key or the digital certificate once it has expired or has been revoked.
15. Inform trusted third parties of the need to check the validity of the digital certificates that you are using at any given time.
16. Inform the third party in good faith of the status of a revoked digital certificate for which the list of revoked certificates CRL is available, published periodically by ECD GSE.
17. Do not use your digital certification in a way that contravenes the law or brings the ECD into disrepute.
18. Not to make any statements relating to your digital certification in the GSE ECD that you consider misleading or unauthorized, as provided for in this CPS and PC.

19. Once the digital certification service has expired or been revoked, the subscriber must immediately stop using it in all advertising material that contains any reference to the service.
20. When referring to the digital certification service provided by ECD GSE in media such as documents, brochures or advertising, the subscriber must report that it complies with the requirements specified in the PC of this DPC, indicating the version.
21. The subscriber may use the conformity marks and information related to the digital certification service provided by ECD GSE in communication media, such as documents, brochures or advertising, provided that the requirements of the previous paragraph are met.

On the other hand, you have the following rights:

1. Receive the digital certificate within the time established in the DPC.
2. Request information regarding applications in process.
3. Request revocation of the digital certificate by providing the necessary documentation.
4. Receive the digital certificate in accordance with the scope granted by ONAC to GSE.

9.11.4 Obligations of Third Parties in Good Faith.

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

1. Know the provisions regarding Digital Certification in current regulations.
2. Know the provisions of the DPC.
3. Check the status of digital certificates before performing operations with digital certificates.
4. Check the certificate revocation list (CRL) before performing operations with digital certificates.

5. Know and accept the conditions regarding guarantees, uses and responsibilities when carrying out operations with digital certificates.

9.11.5 Obligations of the Entity (Client).

As established in the PCs listed in this document, in the case of certificates where the link between the subscriber and/or responsible party is accredited, it will be the obligation of the Entity:

1. Request the RA of the ECD GSE to suspend/revoke the digital certificate when said link ceases or changes.
2. All obligations linked to the person responsible for the digital certification service.
3. When referring to the digital certification service provided by ECD GSE in media such as documents, brochures or advertising, the entity must report that it complies with the requirements specified in the CPs listed in this CPS.
4. The entity may use the conformity marks and information related to the digital certification service provided by ECD GSE in communication media, such as documents, brochures or advertising, provided that it complies with the requirements in the previous paragraph.

9.11.6 Obligations of other ECD participants.

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

1. Review the consistency of the CPD with current regulations.
2. Approve and decide on changes to be made to certification services, due to regulatory decisions or requests from subscribers or those responsible.
3. Approve notification of any changes to subscribers and/or controllers, analyzing tr legal, technical or commercial impact.
4. Review and take action on any comments made by subscribers or managers when a change to the certification service is made.
5. Inform ONAC of action plans regarding any change that impacts the PKI infrastructure and affects digital certification services, in accordance with the current RAC-3.0-01.
6. Authorize the required changes or modifications to the CPD.
7. Authorize the publication of the CPD on the ECD GSE website.
8. Approve changes or modifications to the ECD GSE Security Policies.
9. Ensure the integrity and availability of information published on the ECD GSE website.

10. Ensure that controls are in place over the ECD GSE's technological infrastructure.

11. Request the revocation of a digital certificate if you have knowledge or suspicion of the compromise of the private key of the subscriber, entity or any other fact that tends to the improper use of the private key of the subscriber, entity or of the own
ECD.
12. Be aware of and take appropriate action when security incidents occur.
13. Carry out a review of the CPS at least once a year to verify that the key lengths and periods of the certificates being used are appropriate.
14. Review, approve and authorize changes to the certification services accredited by the competent body.
15. Review, approve and authorize the ownership and use of symbols, certificates and any other mechanism required by ECD GSE to indicate that the digital certification service is accredited.
16. Ensure that the accreditation conditions granted by the competent body are maintained.
17. Ensure the proper use in documents or in any other advertising of symbols, certificates, and any other mechanism that indicates that ECD GSE has an accredited certification service and complies with the provisions of the ONAC Accreditation Rules.
18. Ensure that critical suppliers and reciprocal ECD, if any, are kept informed of the obligation to comply with the CEA requirements, in the corresponding sections.
19. The Integrated Management System will execute corrective action plans and improvement actions to respond to any risk that compromises the impartiality of the ECD, whether it arises from the actions of any person, body, organization, activities, its relationships or the relationships of its staff or itself, for which it uses the ISO 31000 standard for the identification of risks that compromise the impartiality and non-discrimination of the ECD, providing the Management Committee with the mechanism that eliminates or minimizes such risk, on an ongoing basis.
20. Ensure that all ECD staff and committees (whether internal or external) that may have influence on certification activities act with impartiality and non-discrimination, especially those arising from commercial, financial or other pressures that compromise tr impartiality.
21. Document and demonstrate commitment to impartiality and non-discrimination.
22. Ensure that the administrative, management, and technical staff of the PKI and the ECD associated with consulting activities maintain complete independence and autonomy from the staff of the review and decision-making process on the

certification of this ECD.
23. Ensure that critical suppliers such as the reciprocal ECD and datacenter are kept informed that they meet the accreditation requirements for ECD as support for tr contracting and compliance with the requested administrative and technical requirements.

9.12 Amendments.
Digital certificates issued by ECD GSE cannot be modified, i.e. amendments are not applicable. Consequently, the subscriber must request the issuance of a new digital certificate. In this event, a new certificate will be issued to the subscriber; the cost of this modification will be fully borne by the subscriber according to the rates informed by ECD GSE or according to the conditions defined at the contractual level.
9.12.1 Procedure for amendment.
Not applicable since digital certificates issued by ECD GSE cannot be modified.
9.12.2 Mechanism and notification period.
Not applicable since digital certificates issued by ECD GSE cannot be modified.
9.12.3 Circumstances under which an OID should be modified.
Not applicable since digital certificates issued by ECD GSE cannot be modified.
9.12.4 Notification to the subscriber or person responsible for issuing a new certificate.
Not applicable since digital certificates issued by ECD GSE cannot be modified.
9.12.5 Form in which the modification of a certificate is accepted.
Not applicable since digital certificates issued by ECD GSE cannot be modified.
9.12.6 Publication of the certificate modified by the ECD.
Not applicable since digital certificates issued by ECD GSE cannot be modified.
9.12.7 Notification of the issuance of a certificate by the ECD to other entities.
Not applicable since digital certificates issued by ECD GSE cannot be modified.

9.13 Dispute resolution provisions.

If for any reason any dispute arises between the Parties (subscriber/controller and ECD GSE) on the occasion of:

1. The provision of digital certification services described in this CPS.
2. During the execution of the contracted services.
3. For the interpretation of the contract, DPC and any other document delivered by ECD GSE.

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

Once this period has ended, if the difference(s) persist, the Parties will be free to resort to the ordinary Colombian courts to assert tr rights or demands, which will be subject to the current regulations on the matter; the costs incurred on the occasion of the call will be fully borne by the losing Party.

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

9.14 Applicable legislation.

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

1. Law 527 of 1999, which defines and regulates access to and use of data messages, electronic commerce and digital signatures, establishes certification entities and dictates other provisions.
2. Decree 333 of 2014, which regulates article 160 of Decree-Law 019 of 2012 regarding the characteristics and requirements of certification entities, and matters related to digital certificates.
3. Chapters 47 and 48 of Title 2 of Part 2 of Book 2 of the Single Decree of the Trade, Industry and Tourism Sector -

DURSCIT.

9.15 Compliance with applicable legislation.

The ECD GSE declares compliance with Law 527 of 1999 and its associated decrees, additionally that the Certification Practices Declaration is satisfactory in accordance with the requirements established by the National Accreditation Body of Colombia.

9.16 Miscellaneous provisions.

9.16.1 Full agreement

The GSE ECD contractually obligates each RA to comply with this CPS and applicable industry guidelines. The GSE ECD also requires that each party using its products and services enter into an agreement defining the terms associated with the product or service. If an agreement contains provisions that differ from this CPS, this CPS shall prevail. Third parties may not rely on such an agreement or take action to enforce it if such agreement is contrary to this CPS.

9.16.2 Assignment

Entities operating under this CPS may not assign tr rights or obligations without the prior written consent of the ECD GSE.

9.16.3 Divisibility

If any provision of this CPD is declared invalid or unenforceable by a court or tribunal of competent jurisdiction, the remainder of this CPD will continue to be valid and enforceable.

9.16.4 Execution (attorney fees and waiver of rights)

ECD GSE may seek indemnification and attorneys' fees from any party for damages, losses and expenses related to such party's conduct.

ECD GSE's failure to enforce any provision of this CPS does not waive its right to enforce the same provision at a later time or its right to enforce any other provision of this CPS.

To be effective, resignations must be in writing and signed by the ECD GSE.

9.16.5 Force Majeure

ECD GSE shall not be liable for any delay or failure to perform any obligation under this CPS to the extent the delay or failure is caused by an event beyond ECD GSE's reasonable control.

The operation of the Internet is beyond the reasonable control of the ECD GSE.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements will include a force majeure clause protecting ECD GSE.

9.17 Other Provisions.

CHANGES AFFECTING DIGITAL CERTIFICATION SERVICES.

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

1. Due to regulatory changes in ECD legislation.

2. At the request of ONAC.
3. At the request of the Superintendency of Industry and Commerce of Colombia - SIC.
4. Technological changes that affect digital certification services.
5. At the request of subscribers or those responsible, with prior approval from the Management Committee.

For this, the Subscriber or responsible party must send a communication to the ECD GSE Management Committee regarding the requested change; acceptance or rejection will be at the discretion of the Management Committee.
Procedure for Changes.
Changes that do not require notification.

1. When the changes made do not affect the operation of the services provided tocurrent subscribers or those responsible, it will be the job of the Management Committee to define the level of impact of the changes.
2. When the changes involve typographical or editing corrections in the content of the services provided.

Changes requiring notification

1. When the changes made affect the operation of the services provided tocurrent subscribers or those responsible, it will be the job of the Management Committee to define the level of impact of the changes.
2. When changes involve updating contact information with the ECD GSE.

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

1. The Management Committee and the ECD GSE Integrated Management System process consider that changes to digital certification services affect tr operation and acceptability.
2. The changes introduce new requirements for the provision of digital certification services due to technological updates or regulatory changes that affect the services.

Subscribers and/or those responsible for the digital certification services affected by the changes made may present tr comments or rejection of the provision of the ECD GSE service in a communication addressed to the Management Committee within thirty (30) days following notification. After thirty (30) days, the conditions will be understood as accepted by the subscribers or those responsible.

DESCRIPTION OF PRODUCTS AND SERVICES

Note: To verify the generation process of each service, refer to the corresponding procedures.

TYPE OF DIGITAL CERTIFICATE	OBJECT
Company Membership	It guarantees the identity of the natural person who holds the certificate, as well as his or her connection to a specific legal entity by virtue of the position he or she holds therein. This certificate will not, in itself, grant its holder greater powers than those he or she possesses through the performance of his or her usual activity.
Company Representation	It is issued to a natural person representing a specific legal entity. The certificate holder identifies himself not only as a natural person belonging to a company, but also adds his qualification as a legal representative of the company.
Civil Service	It guarantees the identity of the natural person who holds the certificate, as well as his or her connection to a Public Administration by virtue of his or her rank as a public official. This certificate will not in itself grant its holder greater powers than those he or she possesses through the performance of his or her usual activity.
Qualified Professional	It guarantees the identity of the natural person who holds the certificate, as well as his status as a qualified professional. This certificate will not in itself grant its holder greater powers than those he possesses through the performance of his usual activity in the field of his profession.
Natural person	It only guarantees the identity of the natural person.
Electronic invoice for natural persons	Exclusive certificate for electronic invoicing, addressing the needs of individuals seeking the security of a certificate for issuing electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment documents, adjustment notes for electronic payroll payment document support documents, and other documents resulting from the processes of the unattended platforms of the technological providers approved by the DIAN, the DIAN

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

	free invoicing system, and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Electronic invoice for legal entities	Exclusive certificate for electronic invoicing, meeting the needs of companies seeking the security of a certificate for issuing electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment documents, adjustment notes for electronic payroll payment document and other documents resulting from the processes of the unattended platforms of the technological providers approved by the DIAN, the DIAN free billing system and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Artificial person	Carrying out business procedures by an application running on a machine in automatic and unattended signature processes on behalf of a public or private legal entity that requires guaranteeing the authenticity and integrity of the data sent or stored digitally together with the establishment of secure communication channels between clients, and which will be represented by a natural person (Controller), holder of the certificate issued under this policy and called Controller.
Generation of Certified Electronic Signatures	Exclusive certificate for the generation of certified electronic signatures.
Certified Email Service	The certified email service ensures the sending, receiving and checking of electronic communications, ensuring at all times the characteristics of fidelity, authorship, traceability and non-repudiation of the same.
Time Stamping Service (TSA)	Data message that links another data message to a specific time or period, which makes it possible to establish with proof that this data existed at that time or period of time and that it did not undergo any modification from the moment the stamp was made.
Service for Archiving and Preservation of Transferable Electronic Documents and Data Messages	The service consists of a secure and encrypted storage space that can be accessed with credentials or a digital certificate. Documentation stored on this platform will have probative value as long as it is digitally signed.

RATES.

Certificate issuance or renewal fees.

Product detail	Delivery time	Validity	Price without VAT	VAT	Total
Natural Person Certificate	Normal	1	$ 192,794	$ 36,631	$ 229,425
Natural Person Certificate	Normal	2	$ 313,399	$ 59,546	$ 372,945
Certificate Belonging to Company	Normal	1	$ 192,794	$ 36,631	$ 229,425
Certificate Belonging to Company	Normal	2	$ 313,399	$ 59,546	$ 372,945
Professional Certificate Holder	Normal	1	$ 192,794	$ 36,631	$ 229,425
Professional Certificate Holder	Normal	2	$ 313,399	$ 59,546	$ 372,945
Certificate Representative Company	Normal	1	$ 192,794	$ 36,631	$ 229,425
Certificate Representative Company	Normal	2	$ 313,399	$ 59,546	$ 372,945
Public Service Certificate	Normal	1	$ 192,794	$ 36,631	$ 229,425
Public Service Certificate	Normal	2	$ 313,399	$ 59,546	$ 372,945
Legal Entity Certificate	Normal	1	$ 600,000	$ 114,000	$ 714,000
Legal Entity Certificate	Normal	2	$ 1,120,000	$ 212,800	$ 1,332,800
Electronic Billing	Normal	1	$233,286	44.324	$ 277,610
Electronic Billing	Normal	2	$ 313,399	$ 59,546	$ 372,945

These prices are calculated based on one and two-year terms. The figures indicated here for each type of certificate may vary depending on special commercial agreements that may be reached with subscribers, entities or applicants, in the development of promotional campaigns carried out by GSE.

In the case of an electronic signature certificate, there is no cost because it is included in the packages for generating certified electronic signatures.

- The ECD GSE offers the issuance of digital certificates valid for days or months without exceeding 24 months. The sales prices of these certificates will be agreed with the client after negotiation.
- For the issuance of digital certificates with an elliptic curve algorithm, the same prices defined in the tariff table will apply.

Fees for access to certificates.
Access to the status of issued certificates is free and open to the public and therefore does not involve any fees. Fees for revocation or access to status information.
There is no cost to request a certificate revocation. Access to the status information of issued certificates is free and open to the public and therefore no fee applies.

Rates for other services.
Once other services are offered by GSE, they are published in the services PCs on the GSE website.
Return policy.
The Return Policy published on the GSE website must be taken into account: https://ase.com.co/politicas
IMPARTIALITY AND NON-DISCRIMINATION
ECD GSE, headed by the Management Committee and its collaborators, are committed to safeguarding impartiality and independence in the 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 Body of Colombia (ONAC), for which the following compliance mechanisms are established:

- The Management Committee and GSE collaborators declare that they do not participate directly or indirectly in services or activities that may endanger free competition, responsibility or transparency.
- Employees will use the reporting of preventive and corrective actions to respond to any risk that compromises the impartiality of the company.
- Collaborators who are part of accredited digital certification services may not provide consulting services, nor involve the development team in providing technical support services 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 may decline to accept an application or maintain a contract for certification when there are well-founded and demonstrated reasons, for example, the applicant's and/or subscriber's involvement in illegal activities, or similar issues related to the subscriber.
- GSE may decline to accept an application or maintain a contract for certification when there are justified, proven or undue reasons on the part of the applicant and/or subscriber.
- GSE offers access to a digital certification service that does not depend on the size of the applicant or subscriber or the membership of any association or group, nor should it depend on the number of certifications already issued.

Note: Any case that puts at risk the impartiality of the ECD GSE as an ECD or its staff, agency or organization, will be brought to the attention of the Integrated Management System Process.
In accordance with the provisions of the GSE ECD Impartiality and Non-discrimination Policy, which can be found at the following link: https://gse.com.co/politicas.

CERTIFICATION POLICIES.
The interrelation between this CPD and the Certification Policies of the different certificates is fundamental. And this, to the extent that:

- The DPC is the set of practices adopted by ECD GSE for the provision of services accredited by ONAC and contains detailed information about its security system, support, administration and issuance of certificates, as well as the relationship of trust between the Applicant, Subscriber, Responsible Party, Entity, Third Party in good faith and the ECD.
- Certification policies constitute the set of rules that define the characteristics of the different ECD GSE certificates and the applicability of these certificates for certain applications that require the same security requirements and forms of use.

In short, the policy defines "what" requirements are necessary for the issuance of the different ECD GSE certificates while the CPD tells us "how" the security requirements imposed by the policy are met.
For this reason, the following Certificate Policies are related:

- Certificate Policies for Digital Certificates:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.4.16
PC Location	https://gse.com.co/documentos/calidad/politicas/Politica_de_certificado_para_certificados_digitales_V16.pdf

Certificate Policies for Time Stamping Service:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.2.14
PC Location	https://gse.com.co/documentos/calidad/politicas/Politica_de_Certificado_para_Servicio_de_Estampado_Cronologico_V14.pdf

Certificate Policies for Archiving and Conservation Service of Transferable Electronic Documents and Data Messages:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.3.14
PC Location	https://gse.com.co/documentos/calidad/politicas/Politica_Certificado_para_Servicio_de_Correo_Electronico_Certificado_V14.pdf

Policies for the Generation of Certified Electronic Signatures:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.6.5
PC Location	https://gse.com.co/documentos/calidad/politicas/Politica_de_Generacion_de_Firmas_Electronicas_Certificas_V5.pdf

ANNEX 1 DPC MATRIX TECHNICAL PROFILE DIGITAL CERTIFICATES.
ANNEX 2 DPC MODELS AND MINUTES OF THE TERMS AND CONDITIONS DOCUMENTS.
ANNEX 3 DPC MATRIX TECHNICAL PROFILE CERTIFICATES ELECTRONIC SIGNATURE.