


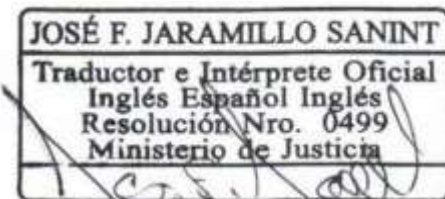


Official Translator: José Fernando Jaramillo Sanint. Address: Calle 70A No. 23B-25 Manizales Colombia
Tel: (57) (6) 8874503 Mobile: (310) 404-0972 - (300) 339-46-01 Email: traducciones@121com.co


	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Document Title	CPS, certification practice statement
Version	16
Working Group	Board of Management
Document Status	Final
Date Issued	2016-11-01
Validity Start Date	10/24/2023
OID (Object Identifier) -IANA	1.3.6.1.4.1.31136.1.1.16
Where to find more info?	„Ds://ase.com.co/documentos/calidad/DPC/Declaracion of Practice s of Certification V16.pdf
Prepared by	Operations Manager
Reviewed by	Integrated management system
Passed	Board of Management

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia. This document is an accurate translation of the original January 19, 2024.



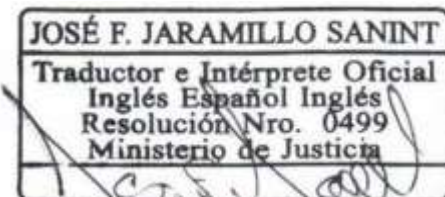


	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public


Change control

Version	Date	Change/Modification
1	2016-11-01	Initial document
2	04-10-2017	<ul style="list-style-type: none"> Update of contact details of the ECD and Logo Update of Enrolling entities Updating contact details Certification Service Providers Information regarding the General Manager of GSE. Update of TSA GSE data.
3	03/04/2018	Updating information and adjustments in relation to CEA-4.1-10 in accordance with the review of the requirements matrices.
4	11/27/2018	Changed from V3 to V4 of 27/11/2018 Update of table of contents, information and adjustments in relation to new charges, rates, access routes to the website, correction of the subordinate, the established and tested phrase is included, paragraph 8.7.4 is expanded naming the technological mechanisms used for data protection, all the certification policies, change of terms and updating of the legal representative were related.
5	12-04-2019	The EE numeral was eliminated, it was clarified that, for the use of the centralized signature certificate, the acquisition of a technological platform with additional costs is necessary. The clarification is made in section 1.6.2 of the requirements and restrictions of the RA and of the Criteria and methods of evaluation of the Applications. Updated RA roles
6	07/06/2019	Clarification of the scope of accreditation under CPD 1.1 Summary 4.1 Application for the certificate, the procedure of how to access the service is clarified. 4.1.1 Clarification of non-discrimination when accessing the service. 8.9.3 Clarification of rights of the subscriber or responsible party
7	03/31/2020	The DPC is adjusted to the changes generated by the new platforms, the target 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 more specifically related.
8	8/14/2020	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	02/12/2021	The link to consult online the Certificate of Existence and Legal Representation for the ECD and the current CA (Paynet SAS) was included. The detailed information of the current (Paynet SAS) and historical (Indenova) CAs was included in accordance with the provisions of item 1 of numeral 10.7 of CEA 4.1-10.

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 January 19, 2024.






	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Version	Date	Change/Modification
		<p>The information of the datacenters was modified in accordance with established in the ONAC accreditation certificate.</p> <p>Deleted paragraph on renewal of digital certificates of section 5.2.2 and 5.2.3.</p> <p>The following paragraphs were updated:</p> <ul style="list-style-type: none"> 6.4.2 Approval or rejection of certificate applications 6.4.3 Deadline for processing certificate requests 7.10.1 Trust Roles 8.1.4 Delivery of the public key of the ECD to accepting third parties <p>Updated links to point to new routes</p>
10	16/07/2021	<p>The numerals were updated:</p> <p>3.6.1 Certification Authority (CA), datacenter provider data.</p> <p>4.1 Repositories</p> <p>Paragraph 6.5.6 was updated.</p> <p>6.5.7 Deadline for processing certificate requests</p> <p>6.8.2 Use of the private key and certificate by bona fide third parties</p> <p>6.12 Revocation and Suspension of Certificates 6.12.3 Revocation Request Procedure 6.13.1 Description of Certificate Content Authority Subordinate 01 GSE 6.13.1.8 Algorithm Object Identifiers (OIDs) 6.14.1.3 CRL Availability 6.14.1.7 OCSP Availability 6.14.3 Optional Features 7.10.1 Trust Roles</p> <p>8.1.4 Delivery of the public key of the ECD to accepting third parties</p> <p>8.1.5 Size of keys</p> <p>8.1.6 Public key generation parameters and quality verification</p> <p>8.2.4 Private Key Backup</p> <p>8.2.5 Private key file</p> <p>8.2.6 Transfer of the private key from the cryptographic module</p> <p>8.2.7 Storage of private keys in a cryptographic module</p> <p>8.5.3 Actions in the Event of an Information Security Event or Incident</p> <p>10. DESCRIPTION OF PRODUCTS and SERVICES, Archiving, Registration, Preservation, Custody and Annotation Service for Electronic Documents</p> <p>Personal Data Treatment Policy</p> <p>11.3 Impartiality and Non-Discrimination</p>

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 January 19, 2024.

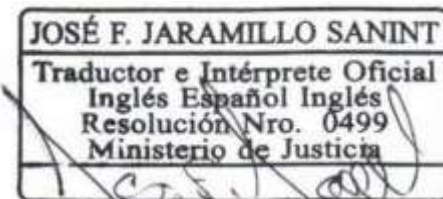





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Version	Date	Change/Modification
		14. ANNEX 1 DPC MATRIX TECHNICAL PROFILE DIGITAL CERTIFICATES 15. ANNEX 2 TERMS and CONDITIONS OID and consultation links of: <ul style="list-style-type: none"> • Statement of Certification Practices • Certificate Policies for Digital Certificates • Chronological Stamping Service Certificate Policies • Certificate Policies for Archiving, Registration, Retention, Custody and Annotation of Electronic Transferable Documents and Data Messages. • Certificate Policies for Certified Email Service
11	10/05/2021	<ul style="list-style-type: none"> • The numerals were updated including electronic signature: <ul style="list-style-type: none"> 6.1 Application for the certificate 6.5 Initial Validation of Identity <ul style="list-style-type: none"> 6.5.1 Method for proving possession of the private key Description of Products and Services <ul style="list-style-type: none"> 11.1.1 Certificate issuance or renewal fees 11.9.3 Obligations of the Subscriber and/or Responsible. • The following numerals were included with reference to electronic signature: <ul style="list-style-type: none"> 5.1.1.1.1 Electronic Signature 5.1.1.2.2 ECD GSE Subscriber Certificates (Matrix Technical Profile of Electronic Signature Certificates) Certification policies 16 Annex 3 DPC matrix technical profile certificates electronic signature <ul style="list-style-type: none"> • A note clarifying the validation of the OCSP was included in sections 4.1, 4.3, 6.12.9, 6.12.10, 6.14.3. • Paragraph 6.12.3 Revocation request procedure was updated by adding a new online revocation channel. • Paragraph 8.3.2 was updated giving clarity of the validation period of the root and subordinate keys of the RSA and ECDSA algorithm • OID and query links are updated
12	27/10/2021	<ul style="list-style-type: none"> • Paragraph 6.5 of Identity Validation was modified • Updated the OID and the link of the Digital Certificates PC • Updated the OID and the link of the DPC with this new version.
13	05/31/2022	According to the new version of CEA, adjustments were made to the following numerals: <ul style="list-style-type: none"> • 3.1 Summary: 4.1-10 was deleted leaving only CEA.

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 January 19, 2024.

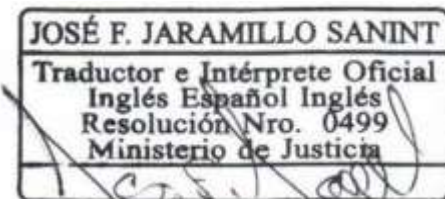




	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Version	Date	Change/Modification
		<p>32 Petition, Complaint, Grievance, and Requests: Removed the term appeal.</p> <ul style="list-style-type: none">• 3.6 PKI Participants: Indenova is deleted as CA.• 5.1.1.1 - 5.1.1.2 Types of Names: Indenova root and subordinate certificates are eliminated and those related to elliptic curve are included.• 6.5 Initial Identity Validation: A final paragraph on confronta consumption in services was included.• 6.13.1 Description of content of the certificates: The alternative name field of the subject was included.• 6.13.1.7 3 key purposes were removed.• 7.10.1 Roles of trust: the roles of the RA agents, RA Administrator and RA Auditor were modified:• 7.16 Termination of an ECD: It was modified in accordance with the requirements of the new CEA.• 9.2 Identity/qualification of the auditor: The assurance requirements were modified. <p>10 Description of products and services: The centralized signature certificate was eliminated, the Archive service name was modified and the electronic signature generation service was modified in accordance with the accreditation certificate.</p> <p>11.4 Exemption due to limits of liability was modified.</p> <ul style="list-style-type: none">• 11.9.6 Obligation of other participants: Item r) was modified by eliminating 4.1-10 leaving only CEA. <p>15 The name of the annex on terms and conditions was modified.</p> <p>16 This item of the technical annex of the electronic signature certificate was included.</p> <ul style="list-style-type: none">• Updated the OID and the link of the Digital Certificates PC• Updated the OID and the link of the DPC with this new version.• The quality code was included in the header of the document.
14	09/23/2022	<ul style="list-style-type: none">• 3.1 Summary: The chapters of the Durscit were included.• The address of the ECD was modified in Items 3.1, 3.2, 3.6.2 and 3.7.1.• The SAS Paynet address was modified in Items 3.6.1 and 3.6.7.2.• Paragraph 3.6.4 was modified by changing responsible for a third party in good faith• Paragraph 3.6.4.1 Precautions to be observed by third parties was included• Paragraph 6.4.1 Performing the identification and authentication functions was modified

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 January 19, 2024.

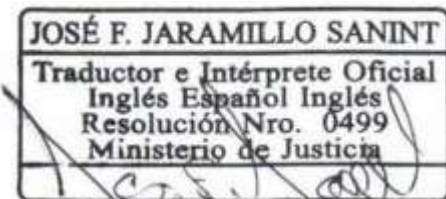





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Version	Date	Change/Modification
		<ul style="list-style-type: none"> Paragraph 6.5.1 Method to demonstrate the possession of the private key was modified, giving clarity in case the applicants generate the pair of keys in their own infrastructure. Section 6.5.5 Criteria for interoperability was modified Paragraph 6.12.7 Frequency of updating the CRLs was modified according to the percentage of availability established in the new CEA. RFC 2560 was modified by RFC 6960 in paragraphs 6.12.10 Online revocation verification requirements, 6.14.1.4 OCSP Profile and 6.14.1.5 Version number. Paragraph 7.7 was modified. Storage system making it clear that the servers are in cloud environments. Paragraph 7.4 was modified. Exposure to water clarifying that it refers to the PKI datacenters. Number 7.16 was modified. Termination of an ECD including a paragraph on the cessation of activities security plan. Number 11.4 Limits of liability were modified, including Liability for the veracity of the Subscriber's information, Liability for service availability, Liability for the functionality of the service in the Subscriber's infrastructure, Liability for computer crimes. Number 11.9.1 Obligations of the ECD GSE was modified, including items o) to y). Paragraphs 12.3 Notification and Communication, 12.5 Prevention and Resolution of Disputes, 12.6 Applicable Law and 12.7 Compliance with Applicable Law were included. Updated the OID and the link of the Digital Certificates PC Updated the OID and the link of the DPC with this new version.
15	05/10/2023	<ul style="list-style-type: none"> The entire order of the document was modified according to the numerals of RFC 3647. Removed Paynet SAS as the CA authority as the PKI was moved to the GSE ECD. Changed to Director of Operations by Operations Manager The data of the main and alternate datacenters were modified, leaving Hostdime and Claro.
16	10/24/2023	<ul style="list-style-type: none"> Section 1.1.6.2 Acronyms is modified: The acronym RNEC is included Paragraph 1.3.1.3 Pseudonymity and pseudonymity are included, nicknames are extended Section 1.3.2 is modified: The section information is updated.

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 January 19, 2024.

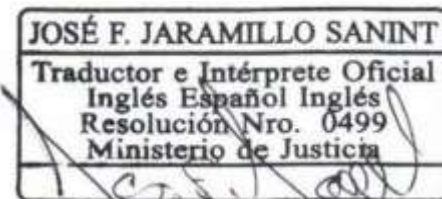





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Version	Date	Change/Modification
		<ul style="list-style-type: none"> • Section 1.3.2.3 is modified: Information on requirements for identity identification and authentication of one individual. • Paragraph 1.3.2.4 is modified, the information of the item • Paragraph 1.3.2.5 is modified, the word is deleted recommendation • Section 1.3.3.1 is modified, the identification and authentication requirements for routine key generation are adjusted. • Section 1.4.1 is modified, including the ECD and information from fully trusted databases. • Section 1.4.2.1 is modified, the word is included information • The number 1.4.3.2 is modified, the words defined are included and authorized personel only. • Section 1.4.4.1 is modified, the word inform you is included and/or • Number 1.4.7.2 is modified: The term is included duly empowered and/or proxies • The number 1.4.7.3 is modified, the media is updated or mechanisms for collecting information from the ECD • Number 1.4.7.4 is modified. The means for Notify Subscriber • Number 1.4.9.3 is modified. The information of online revocation request. • Number 1.4.9.11 is modified. The means for Notify Subscriber • Number 1.4.12.3 is modified. The service table is included for pin Forgotten Cases • Number 1.5.2.2 is modified. The information of the persons required by role. • 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. The information of item • Number 1.9.3.4 is modified. Information is updated relating the TRD. • Number 1.9.4.1 is modified. Related standards are included Personal data processing. • The number 1.9.4.5 is modified, the wording of the numeral is adjusted

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 January 19, 2024.





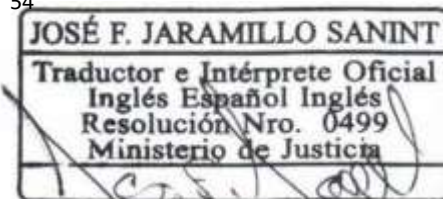
	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Version	Date	Change/Modification
		<ul style="list-style-type: none"> The number 1.9.4.6 is modified, the wording of the numeral is adjusted The number 1.9.11.2 is modified. It is adjusted literally c Number 1.14 Updated OID and location of the Certificate Policy for Digital Certificates


TABLE OF CONTENTS

1.	CONTENT OF THE STATEMENT OF CERTIFICATION PRACTICES	10
1.1.	INTRODUCTION	10
1.1.1.	Overview	10
1.1.2.	Name and identification of the document	11
1.1.3.	PKI Participants	12
1.1.4.	Use of the certificate	15
1.1.5.	Policy administration	16
1.1.6.	Definitions and acronyms	17
1.2.	PUBLISHING AND REPOSITORY RESPONSIBILITIES	21
1.2.1.	PKI Repositories	21
1.2.2.	Publication of Certification Information	22
1.2.3.	Term or Frequency of Publication	22
1.2.4.	Access controls to repositories	23
1.3.	IDENTIFICATION AND AUTHENTICATION	23
1.3.1.	Names	23
1.3.2.	Initial Identity Validation	26
1.3.3.	Identification and Authentication for key renewal	31
1.3.4.	Identification and Authentication in Revocation Requests	31
1.4.	CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS	31
1.4.1.	Certificate Application	31
1.4.2.	Certificate Application Processing	32
1.4.3.	Issuance of the Certificate	33
1.4.4.	Acceptance of the Certificate	33
1.4.5.	Pair of Keys and Use of Certificate	34
1.4.6.	Renewal of Certificate without Change of Keys	35
1.4.7.	Renewal of Certificate with Change of Keys	36
1.4.8.	Modification of Certificate	37
1.4.9.	Revocation and Suspension of the Certificate	38
1.4.10.	Certificate Status Services	43
1.4.11.	End of Subscription	45
1.4.12.	Key Custody and Recovery	45
1.5.	FACILITIES, MANAGEMENT AND OPERATIONAL CONTROLS	46
1.5.1.	Physical Security Controls	46
1.5.2.	Procedural Controls	48
1.5.3.	Personnel controls	49
1.5.4.	Audit Log Procedures	50
1.5.5.	Archiving of Records	51
1.5.6.	Changing Keys	52
1.5.7.	Commitment and Disaster Recovery	53
1.5.8.	Cessation of CA or RA	54

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 January 19, 2024.

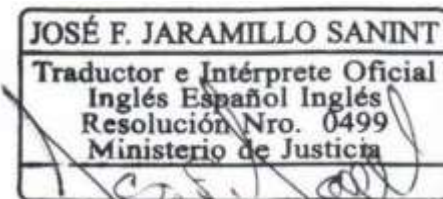





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.6.	TECHNICAL SAFETY CONTROLS	55
1.6.1.	Generation and Installation of Key Pairs	55
1.6.2.	Private Key Protection and Cryptographic Module Engineering Controls	57
1.6.3.	Other Aspects of Key Pair Management	59
1.6.4.	Activation Data	60
1.6.5.	Life Cycle Safety Controls	62
1.6.6.	Network Security Controls	62
1.6.7.	Timestamping	62
1.7.	CERTIFICATE PROFILES CERTIFICATE PROFILES, CRL AND OCSP	63
1.7.1.	Certificate Profile	63
1.7.2.	CRL Profile	66
1.7.3.	OCSP Profile	66
1.8.	COMPLIANCE AUDIT AND OTHER EVALUATION	67
1.8.1.	Frequency or Circumstances of Controls	67
1.8.2.	Identity/qualification of the Auditor	67
1.8.3.	Relationship between the Auditor and the Audited Entity	67
1.8.4.	Aspects Covered by Controls	67
1.8.5.	Actions to be Taken as a Result of the Detection of Deficiencies	67
1.8.6.	Communication of Results	68
1.9.	OTHER BUSINESS AND LEGAL MATTERS	68
1.9.1.	Fees	68
1.9.2.	Financial Responsibility	68
1.9.3.	Confidentiality of Commercial Information	69
1.9.4.	Privacy of Personal Information	70
1.9.5.	Intellectual Property Rights	71
1.9.6.	Representations and Warranties	71
1.9.7.	Disclaimers of Warranties	72
1.9.8.	Limitations of Liability	72
1.9.9.	Indemnities	73
1.9.10.	Term and Termination	74
1.9.11.	Individual Notices and Communication with Participants	75
1.9.12.	Amendments	80
1.9.13.	Dispute Resolution Procedures	81
1.9.14.	Governing Law	81
1.9.15.	Compliance with Applicable Law	82
1.9.16.	Miscellaneous	82
1.9.17.	Other Provisions	82
1.10.	CHANGES AFFECTING DIGITAL CERTIFICATION SERVICES	82
1.10.1.	Procedure for Changes	82
1.11.	DESCRIPTION OF PRODUCTS AND SERVICES	83
1.12.	FEES	85
1.12.1.	Certificate issuance or renewal fees	85
1.12.2.	Certificate access fees	86
1.12.3.	Revocation Fees or Access to Status Information	86
1.12.4.	Fees for other services	86
1.12.5.	Return Policy	86
1.13.	IMPARTIALITY AND NON-DISCRIMINATION	86
1.14.	CERTIFICATION POLICIES	87
1.15.	ANNEX 1 DPC MATRIX TECHNICAL PROFILE DIGITAL CERTIFICATES	89
1.16.	ANNEX 2 DPC MODELS AND MINUTES OF THE TERMS AND CONDITIONS DOCUMENTS	89
1.17.	ANNEX 3 DPC MATRIX TECHNICAL PROFILE CERTIFICATES ELECTRONIC SIGNATURE	89

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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1. CONTENT OF THE DECLARATION OF CERTIFICATION PRACTICES. 1.1. INTRODUCTION.

1.1.1 General Discussion

The Declaration of Certification Practices (DPC)- Global Certification Authority Root GSE (hereinafter DPC) is a document prepared by Gestión de Seguridad Electrónica S.A. (hereinafter GSE) that acting as a Digital Certification Entity, contains the rules, declarations on the policies and procedures that the Digital Certification Entity (hereinafter ECD GSE) as a Digital Certification Service Provider (PSC) applies as a guideline to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014 and the regulations that modify or complement them, in the territory of Colombia.

The DPC complies with the following guidelines:

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

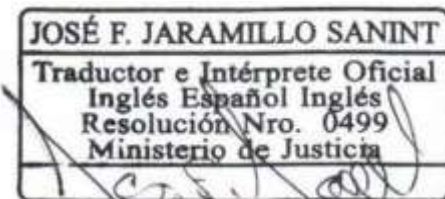
The update and/or modification of the DPC will be carried out through the procedure established by GSE of documented information, any change or adaptation on the document must be reviewed, analyzed and approved by the Management Committee.

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

ELECTRONIC SECURITY MANAGEMENT DATA S.A.:

business name: GESTION DE SEGURIDAD ELECTRONICA S.A.
sign: GSE S.A.
tax identification number: 900.204.272-8
commercial register No: 01779392 OF FEBRUARY 28, 2008
certificate of existence and legal representative:

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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Status of the commercial register: Corporate address: Correspondence: Place / Country: Phone number: Fax: Email, website	https://gse.com.co/documentos/marco-regulatory/Certificate-of-Existence-v-Representative-Leaal-GSE.pdf Active Calle 77 No. 7-44 Office 701 Bogotá D.C., Colombia +57(1)4050082 +57(1)4050082 info@gse.com.co www.gse.com.co
--	---

1.1.2. Name and identification of the document.

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

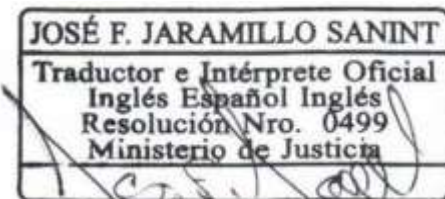
GSE is a company registered (Registered Private Enterprise) with the international organization IANA (Internet Assigned Numbers Authority), with private code No 31136 under branch 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprise). The above information can be consulted at the URL, searching for the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

The hierarchy of OIDs was established by ECD GSE 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	Does not vary
3	Organization	Does not vary
6	I publish	Does not vary
1	Internet	Does not vary
4.1 (31136)	Organization Id	Does not vary, defined by the 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 your group
14	Document version	Modified according to each version of the document

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

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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.1.3. PKI Participants.

1.1.3.1. Certification Authority (CA).

It is that legal entity, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, empowered by the Colombian government or the National Accreditation Body in Colombia to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014 and the regulations that modify or complement them, is the origin of the digital certification hierarchy that allows it to provide services related to communications based on public key infrastructures.

1.1.3.2. Hierarchy of CA's.

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

GSE CERTIFICATION HIERARCHY S.4

Authority Root GSE	GSE ECDSA Root	GSE Electronic Signature Root
Subordinate Authority 01 GSE	GSE ECDSA Subordinate	GSE Intermediate Electronic Signature

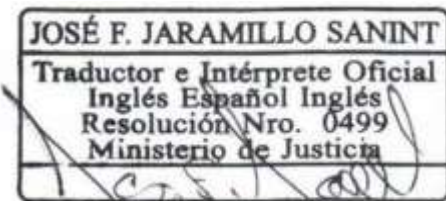
GSE has two datacenters (one main and one alternate), the main datacenter with Hostdime is located in Verganzo, Zona Franca de Tocancipá Int 9, Km 1.5 via Briceño-Zipacquirá, Tocancipá, Cundinamarca, Colombia and the alternate datacenter with Claro is located on the Medellín Km 7.5 Celta Trade Park-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

1.1.3.3. Registration Authority (RA).


It is the area of GSE responsible for certifying the validity of the information provided by the applicant of a digital certification service, by verifying the entity of the subscriber or responsible for digital certification services, in the RA it is decided 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 DPC, the figure of RA is part of the ECD itself and may act as a Subordinate of ECD GSE.

GSE under no circumstances delegates the functions of Registration Authority (RA).





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.1.3.4. Subscriber and/or responsible party.

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

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

1.1.3.5. Third party in good faith.

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

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

1.1.3.6. Precautions to be observed by third parties:

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

1.1.3.7. Applicant.

The Applicant shall be understood as the natural or legal person interested in the digital certification services issued under this DPC. It may match the figure of the Subscriber.

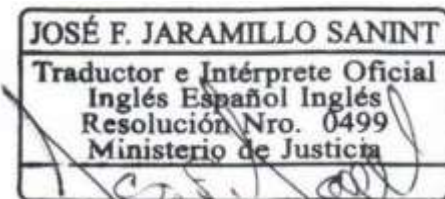
1.1.3.8. Entity to which the subscriber or responsible party is linked.

Where appropriate, the legal entity or organization to which the subscriber or responsible party is closely related by means of an accredited link in the digital certification service.


1.1.3.9. Other participants.

1.1.3.10. 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 CPD as an initial document, as well as authorizing the changes or modifications required on the approved CPD and authorizing its publication.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.1.3.11 .Service providers.

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

1.1.3.12. Reciprocal Digital Certification Entities.

In accordance with the provisions of article 43 of Law 527 of 1999, 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 way as it does with its own certificates, the regularity of the details of the certificate, as well as its validity and validity.

ECD GSE does not currently have reciprocity agreements in place.

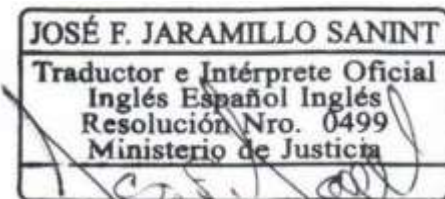
1.1.3.13. Requests, Complaints, Claims and Requests.

Requests, complaints, claims and requests about the services provided by ECD GSE or subcontracted entities, explanations about this DPC and its policies; are received and addressed directly by GSE as ECD and will be resolved by the relevant and impartial persons or by the committees that have the necessary technical competence, for which the following channels are available for the attention of subscribers, managers and third parties.


Phone number: +57(1)4050082
Email: [pqrs\(5\)gse.com.co](mailto:pqrs(5)gse.com.co)
Address: Calle 77 No. 7-44 Office 701
Website: www.qse.com.co
Responsible person: Customer service

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

Once the investigation has been generated, the response is evaluated to subsequently make the decision that the PQRS resolves and its final communication to the subscriber, responsible or interested party.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.1.4. Use of the certificate.

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

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

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

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

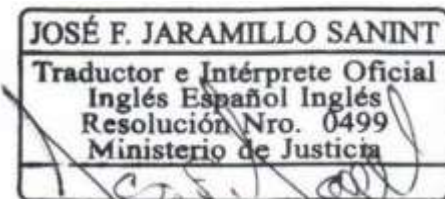
The public key contained in a Digital Certificate can be used to encrypt data messages, such that only the holder of the private key can decrypt said data message and access the information. If the private key used to decrypt is lost or destroyed, the information that has been encrypted cannot be decrypted. The subscriber, responsible parties and third parties in good faith, acknowledge and accept the risks posed by making use of digital certificates to perform encryption processes and especially the use of keys to encrypt data messages is the sole responsibility of the subscriber or responsible party 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 that is not described in this DPC will be considered a violation of this DPC and will constitute a cause for immediate revocation of the digital certification service and termination of the contract with the subscriber and/or responsible party, without prejudice to any criminal or civil actions that may arise on the part of the ECD GSE.

*This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original January 19, 2024.*





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.1.4.2. List of types of applications where the issuance of certificates is prohibited or non-functional. Certificates may only be used for the uses for which they have been issued and specified in this DPC and specifically in the Certificate Policies for Digital Certificates.

Those that are not defined in this DPC are considered improper uses and consequently for legal purposes, ECD GSE is exempt from any responsibility for the use of the certificates in operations that are outside the limits and conditions established for the use of Digital Certificates according to this DPC, including, but not limited to the following prohibited uses:

Illicit purposes or operations under any legal regime in the world.

Any practice contrary to Colombian law.

Any practice contrary to the international agreements signed by the Colombian state,

Any practice contrary to supranational norms.

Any practice contrary to good customs and business practices, or Any use in systems whose failure may cause:

- Death

Injury to people

Damage to the environment

As a control system for high-risk activities such as:

- Maritime navigation systems

- Land transport navigation systems

- Air navigation systems

- Air traffic control systems

- Weapon control systems

1.1.5. Policy administration.

1.1.5.1. Document administration organization.

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

1.1.5.2. ECD Responsible:

Name:

Álvaro de Borja Carreras Amorós

Position:

Legal representative

Address:

77th Street # 7-44 Office 701

Address:

Bogotá D.C., Colombia

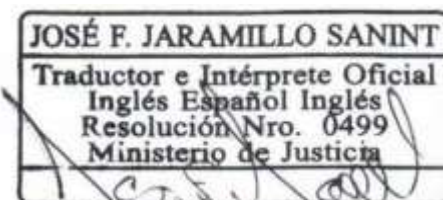
Phone number:

+57(1)4050082


Email:

info@gse.com.co

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia. This document is an accurate translation of the original January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.1.5.3. Responsible for PC and DPC update

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

1.1.5.4. CPD Approval Procedures.

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

1.1.6. Definitions and acronyms.

1.1.6.1. Definitions.

The following terms are in common use and required for the understanding of this DPC:

Certification Authority (CA): In English "Certification Authority" (CA): Certification Authority, root entity and entity providing public key infrastructure certification services.

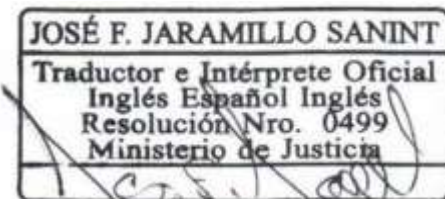
Registration Authority (RA): The entity in charge of certifying the validity of the information provided by the applicant for a digital certificate, by verifying their identity and registration.

Time Stamping Authority (TSA): An acronym for "Time Stamping Authority": Certification Entity providing chronological stamping services


Reliable data file: It is the service that GSE offers to its clients through a technological platform. In essence, 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 signed electronically by a certification service provider that links signature verification data to a signatory and confirms their identity. This is the definition of Law 527/1999 which in this document extends to cases where the linking of signature verification data is 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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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 Key (PIN): An acronym for "Personal Identification Number": A sequence of characters that allow access to the digital certificate.

Commitment of the private key: Commitment means the theft, loss, destruction or disclosure of the private key that may put at risk the use and use of the certificate by unauthorized third parties or the certification system.

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

Declaration of Certification Practices (DPC): In English, "Certification Practice Statement" (CPS): statement of the certification entity about the policies and procedures it applies for the provision of its services.

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

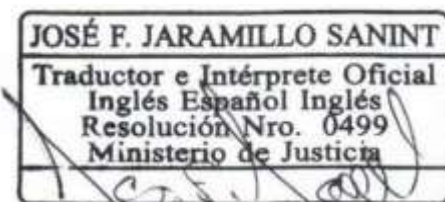
Certification Entity: It is a legal entity, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, empowered by the Colombian government (National Accreditation Body in Colombia) to issue certificates in relation to the digital signatures of customers who acquire them, offer or facilitate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

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


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

Closed certification entity: Entity that offers services of the certification entities only for the exchange of messages between the entity and the subscriber, without demanding remuneration for it.

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Initiator: Person who, acting on their own behalf, or on whose behalf a data message has been acted upon, sends or generates a data message.

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

List of Revoked Certificates (CRL): Acronym for "Certify Revocation List": List where only unexpired revoked certificates are listed.

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

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

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

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

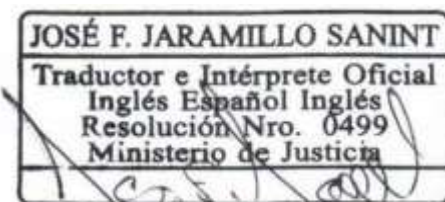
Certification Policy (CP): It is a set of rules that define the characteristics of the different types of certificates and their use.

Certification Service Provider (PSC): A natural or legal person who issues digital certificates and provides other services in relation to digital signatures.


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

Pseudonym: Hides his real name with a false name.

Pseudo-anonym: Intentionally uses a false name





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

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

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

Third party in good faith: Person or entity other than the subscriber and/or controller who decides to accept and rely on a digital certificate issued by ECD GSE.

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

1.1.6.2. Acronyms.

CA: Certification Authority

CA Sub: Subordinate Certification Authority

CP: Certification Policy (Certify Policy)

CPD: Certificate Practice Statement

CRL: Certificate Revocation List

CSP: Certification Service Provider

DNS: Domain Name System

FIPS: Federal Information Processing Standard

HTTP: The HyperText Transfer Protocol (HTTP) is the protocol used in every transaction on the Web (WWW).

C. HTTP defines the syntax and semantics that web architecture software elements (clients, servers, proxies) use to communicate B. It is a transaction-oriented protocol and follows the request-response method between a client and a server

HTTPS: Hypertext Transfer Protocol Secure, better known by its acronym HTTPS, is a network protocol based on the HTTP protocol, intended for the secure transfer of hypertext data, that is, it is the secure version of HTTP.

HSM: 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

OCSF

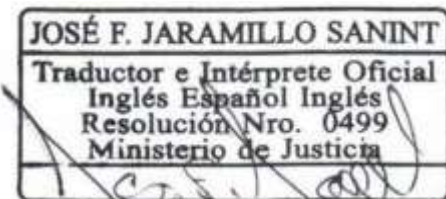
OID: Object identifier

PIN: Personal Identification Number


PUK: Personal Unlocking Key

PKCS: Public Key Cryptography Standards PKI standards developed by RSA Laboratories and accepted internationally.

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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

PKI: Public Key Infrastructure
PKIX: Public Key Infrastructure (X.509)
RA: Registration Authority
RNEC: NATIONAL CIVIL REGISTRY OFFICE
RFC: Request For Comments (Standard issued by the IETF)
URL: Uniform resource locator
VA: Validation Authority

1.1.6.3. Standards and Standardization Bodies.

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

1.2. PUBLISHING AND REPOSITORY RESPONSIBILITIES.

1.2.1. PKI Repositories.

• ECD GSE Root Certificates

https://certs2.ase.com.co/CA_ROOT.crt

https://certs2.gse.com.co/CA_ECROOT.crt

https://certs2.ase.com.co/CA_FEROOT.crt

• ECD GSE Root Revoked Certificate List (CRL)

https://crl2.ase.com.co/CA_ROOT.crl

https://crl2.ase.com.co/CA_ECROOT.crl

https://crl2.ase.com.co/CA_FEROOT.crl

• ECD GSE Subordinated Certificates

https://certs2.gse.com.co/CA_SUB01.crt

https://certs2.ase.com.co/CA_EC_SUB01.crt

https://certs2.gse.com.co/CA_FESUB01.crt

• List of ECD GSE Subordinated Revoked Certificates (CRL)

https://crl2.gse.com.co/CA_SUB01.crl

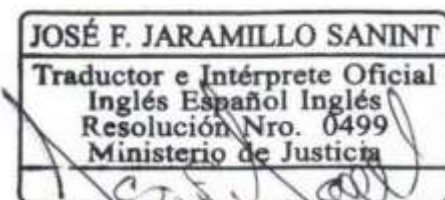
https://crl2.gse.com.co/CA_EC_SUB01.crl

https://crl2.gse.com.co/CA_FESUB01.crl


• Online validation of Digital Certificates

<https://ocsp2.gse.com.co>

*This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia.
This document is an accurate translation of the original January 19, 2024.*





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Note: Online validation of digital certificates using OCSP must be carried out with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such is the case of OPENSLL.

This ECD GSE repository does not contain any confidential or private information.

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

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

1.2.2. Publication of certification information.

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

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

1.2.3. 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

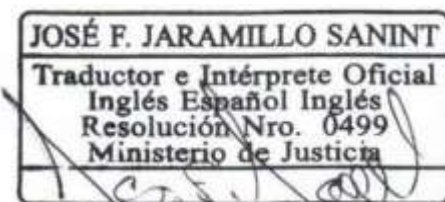
The Subordinate's certificate will be published and will remain on the ECD GSE website for as long as digital certification services are being provided.

Certificate Revocation List (CRL)


ECD GSE will publish on the website, the list of certificates revoked in the events and with the frequency defined in the Frequency of issuance of the CRLs section.

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

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Online Validation of Digital Certificates

ECD GSE will publish the certificates issued in a repository in X.509 format which can be consulted at <https://ocsp2.gse.com.co>

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

1.2.4. Access controls to repositories.

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

1.3. IDENTIFICATION AND AUTHENTICATION.

1.3.1. NAMES

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

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

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

1.3.1.1.1. 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

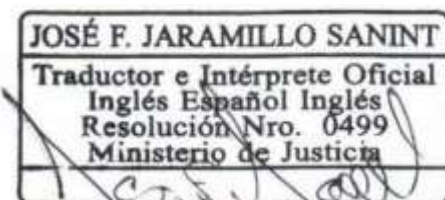
In the DN of the 'subject name' the following fields are included:

C = CO


O = GSE

OU = PKI

CN = GSE Root Authority E = info@gse.com.co





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.3.1.1.1.1. Elliptic Curve (ECDSA).

The DN of the 'issuer yam' of the root certificate has the following fields and fixed values:

C = CO
 S = Capital District L = Bogotá D.C.
 O = GESTIÓN DE SEGURIDAD ELECTRONICA S.A.
 OU = GSE CA RAIZ R2
 SERIALNUMBER = 900204278
 CN = GSE ECDSA RAIZ
 E = info@.qse.com.co
 STREET = www.gse.com.co

The following fields are included in the DN of the 'subject yam':

C = CO
 S = Capital District
 L = Bogotá D.C.
 O = GESTIÓN DE SEGURIDAD ELECTRONICA S.A.
 OU = GSE CA RAIZ R2
 SERIALNUMBER = 900204278
 CN = GSE ECDSA RAIZ
 E = info@.qse.com.co
 STREET = www.gse.com.co

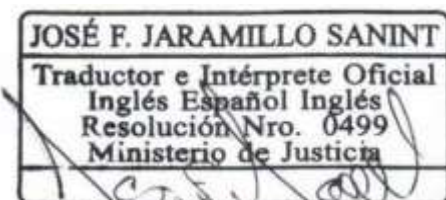
1.3.1.1.1.2. Electronic Signature.

STREET=www.gse.com.co,
 E= info@gse.com.co
 CN=GSE ELECTRONIC SIGNATURE ROOT,
 SN=900204272,
 OU=GSE ELECTRONIC SIGNATURE R1,
 O=GESTIÓN DE SEGURIDAD ELECTRONICA SA,
 L=BOGOTA DC,
 ST=DISTRITO CAPITAL,
 C=CO


1.3.1.1.2. Certificates of Subordinates.

The DN of the 'issuer yam' of the certificates of the subordinates of ECD GSE, have the following characteristics:

C = CO
 O = GSE
 OU = PKI
 CN = GSE Root Authority
 E = jinfo@.Qse.com.co





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

The following fields are included in the DN of the 'subject yam':

C = CO

L = Bogotá D.C.

O = GSE OU = PKI

CN = Subordinate Authority 01 GSE

E = info@gse.com.co

1.3.1.1.2.1. Elliptic Curve (ECDSA).

The DN of the 'issuer yam' of the certificates of the subordinates of ECD GSE, have the following characteristics:

C = CO

S = Capital District

L = Bogotá D.C.

O = GESTIÓN DE SEGURIDAD ELECTRONICA S.A.

OU = GSE CA RAIZ R2

SERIALNUMBER = 900204278

CN = GSE ECDSA RAIZ

E = info@gse.com.co

STREET = www.gse.com.co

The following fields are included in the DN of the 'subject yam':

C = CO

S = Capital District

L = Bogotá D.C.

O = GESTIÓN DE SEGURIDAD ELECTRONICA S.A.

OU = GSE ECDSA R2 SUB1

SERIALNUMBER = 900204278

CN = GSE ECDSA SUBORDINATE

E = info@gse.com.co

STREET = www.gse.com.co

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

The DN of the 'issuer yam' of the ECD GSE subscriber certificates have the following general characteristics:

C = CO

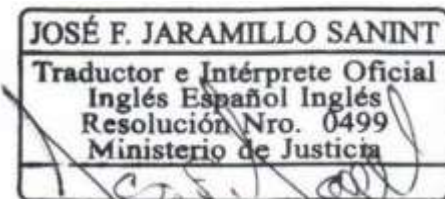
L = Bogotá DC

O = GSE


OU = PKI

CN = Subordinate Authority 01 GSE

E = info@gse.com.co





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

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

STREET=www.gse.com.co,
E=jnfo@gse.com.co.
CN=GSE INTERMEDIATE ELECTRONIC SIGNATURE,
SN=900204272,
OU=GSE ELECTRONIC SIGNATURE R1,
O=GESTIÓN DE SEGURIDAD ELECTRONICA SA,
L=BOGOTA DC,
ST= CAPITAL DISTRICT,
C=CO

1.3.1.2. Significant/ Distinctive Names.

The distinctive names (DN) of the certificates issued by ECD GSE are unique and allow to establish a link between the public key and the subscriber identification number. Because the same person or entity can request several certificates in their name, they will be differentiated by the use of a single value in the DN field.

1.3.1.3. Anonymous/Pseudonymous and Pseudonymous Identification of Subscribers.

Aliases, nicknames, nicknames, diminutives, and/or the like may not be used in the fields of subscriber or manager since the certificate must contain the true name, company name, acronym or name of the certificate applicant.

1.3.1.4. Rule of interpretation of name forms.

The rule used to interpret the distinctive names of the issuer and of the subscribers or managers of digital certificates issued by ECD GSE is the ISO/IEC 9595 (X.500) Distinguished Yam (DN) standard.

1.3.1.5. Unique Names.


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

1.3.1.6. Recognition, Authentication and Role of Recognized Marks.

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.3.2. Initial identity validation.

ECD GSE must receive requests to certify the unequivocal identification of the identity of the subscriber (natural or legal person) the veracity and authenticity of the information through any identification system, as long as it subsists contract, agreement, alliance, and/or any means of contractual and/or commercial relationship, directly and/or indirectly, among others, with the following:

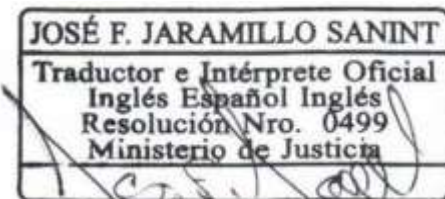
- National Identification File - National Registry of Civil Status.
- Muisca - Unique Model of Automated Revenue, Service and Control - and/or databases of the Dian (Directorate of National Taxes and Customs).
- confront.
- Single Business and Social Registry and/or databases of the Chambers of Commerce (For Legal Entity).
- Migration Colombia (for foreigners).
- Databases provided by the National Registry of Civil Status that allow the unequivocal identification of the applicant. In accordance with current regulations issued by the Entity.

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


The applicant's data: type of identification, identification number, names, surnames, nit (applies to company), company name (applies to company) 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 unequivocal identification of the identity of the applicant (natural or legal person), the veracity and authenticity of the information is verified in a manner analogous to face-to-face validation by consuming some of the services widely used in accordance with the requested digital certificate service, for this purpose listed below:

- National Identification File - National Registry of Civil Status.
- Muisca - Unique Model of Automated Revenue, Service and Control - and/or databases of the Dian (Directorate of National Taxes and Customs).
- confront
- Single Business and Social Registry and/or databases of the Chambers of Commerce (For Legal Entity).
- Migration Colombia (for foreigners).





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

- Databases provided by the National Registry of Civil Status that allow the unequivocal identification of the applicant.

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 Digital Certificate Issuance Procedure

For digital certification services: Chronological Stamping, Certified Email, Generation of Certified Electronic Signatures, Archiving and Preservation of Transferable Electronic Documents and Data Messages, the Confronta identity validation service will not be consumed, but the verification mechanisms that apply to confirm the veracity and authenticity of the information, such as:

- National Identification File - National Registry of Civil Status.
- Muisca - Single Model of Automated Revenue, Service and Control - and/or databases of the Dian (Directorate of National Taxes and Customs).
- Single Business and Social Registry and/or databases of the Chambers of Commerce (For Legal Entity).
- Migration Colombia (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:

(...)

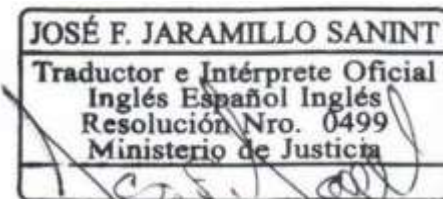
ARTICLE 2. Purpose. It is the object of the National Registry of Civil Status -, to register civil life and identify Colombians and organize electoral processes and mechanisms for citizen participation, in order to support the administration of justice and the democratic strengthening of the country.

(...)


ARTICLE 5. Functions. The functions of the National Registry of Civil Status are as follows:

19. Issue and elaborate the citizenship cards of Colombians, in optimal conditions of security, presentation and quality and adopt a unique system of identification to first-time applications, duplicates and rectifications.

20. Attend to everything related to the management of information, databases, the National Identification Archive and the documents necessary for the technical process of the identification of citizens, as well as inform and issue the certifications of the procedures that may take place.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

24. To attend the requests for issuance of the citizenship card in the consulates of Colombia abroad so that those who are qualified can exercise their political rights as Colombian citizens and provide information about their procedure.

This means that if the application for the 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 prior validation of their 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 is ensured by unequivocal identification of the subscriber, the ECD GSE will maintain the records of the application ensuring the Life Cycle process of the Digital Certification.

In the case of electronic signature certificates, the identity validation of the applicant is not carried out but a verification of the data registered at the time of the signature request by sending an OTP code to the registered email.

1.3.2.1. Mechanism for proving 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 pair of keys and transmits the file in PKCS#10 format through a secure channel where it proves that it is in possession of the private key.

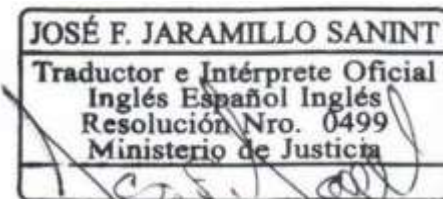
In the event that the certificate is centralized, the generation of the key pair is carried out on an HSM device owned by the ECD GSE and a set of credentials (username and password) is delivered to the subscriber and/or responsible party for their exclusive use.

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


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

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

To ensure the identity of a legal person, the RA GSE requires the presentation of the official document proving the legal existence of the same and its legal representative or attorneys-in-fact who will be the only persons who can request the digital certificate from name of such





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

organization. In the event that the request is made by a third party, the certificate of delegation of the process must be delivered scanned to the attorney-in-fact. The documents will be received scanned, preserving the legibility for the use of the information.

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

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

To ensure the identity of a natural person, the RA GSE requires the registration of information that demonstrates the identity of the applicant and/or presentation of the identity document of the digital applicant and verifies its existence and correspondence against its own and/or third-party databases, whether official and/or private through contracts, agreements, alliances, and/or any type of contractual and/or commercial relationship, whether direct and/or indirect. When the service is requested by a minor, their identity will be secured with the authenticated identity document (identity card) and document that supports the link between the applicant and the minor. In the event that the request is made by a third party, the certificate of delegation of the process must be delivered scanned to the attorney-in-fact. The documents will be received scanned, preserving the legibility for the use of the information.

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

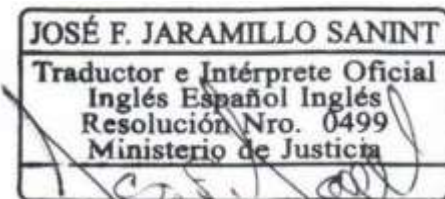
1.3.2.4. Unverified Subscriber Information.

Under no circumstances will ECD GSE omit the verification work that leads to the identification of the applicant and that translates into the request and requirement of the information and/or documents mentioned for organizations and individuals.


In the specific case of the home address, the good faith of the information provided by the applicant is presumed, therefore no verification of it is carried out.

1.3.2.5. 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 the recommendation based on the review of GSE's RA application.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.3.3. Identification and Authentication for key renewal.

1.3.3.1. Identification and authentication requirements for routine key generation.

ECD GSE carries out the authentication process of the applicant at all events, including renewal events, and issues digital certificates based on this. The foregoing, through any identification system whenever there is a contract, agreement, agreement, alliance, and/or any type of contractual and/or commercial relationship directly and/or indirectly, among others, with the National Registry of Civil Status, confront, Databases of credit bureaus or government data sources Only those applications digitally signed by the subscriber, will be renewed the digital certificate without going through a new identification and authentication process, always guaranteeing documentary validation.

1.3.3.2. Post Revocation Identification and Authentication Requirements.

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

1.3.4. Identification and authentication in revocation requests.

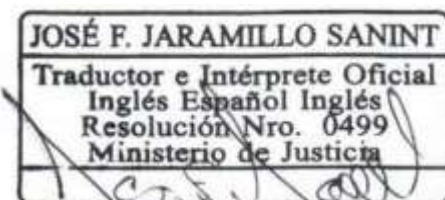
ECD GSE, responds to requests for revocation in accordance with the grounds for revocation specified in the Circumstances for the revocation of a certificate of this DPC and authenticates the identity of the person requesting the revocation of the certificate. In accordance with the provisions of the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

1.4. OPERATIONAL REQUIREMENTS OF THE LIFE CYCLE OF CERTIFICATES.


1.4.1. Certificate application.

Any person who requires the provision of the digital certification service may do so using the channels, means or mechanisms provided by ECD GSE, in which 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 is filed, the information is sent to the Registration Authority, which will be responsible for reviewing the request to ensure the unequivocal identification of the identity of the subscriber (Natural or Legal Person), the veracity and authenticity of the information that allows a recommendation to be made for decision making, complying with the requirements of the Certification Policies.

The applicant provides the necessary information and/or documents as applicable, delivering them scanned or in electronic original, preserving the legibility for the use of the information. The information can also be obtained through fully reliable databases, in accordance with those already mentioned in the preceding paragraphs, with which it is provide the procedures established by the ECD GSE, for obtaining the digital certificate.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

The ECD GSE 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 from the presentation of any document when the identity of the applicant has been sufficiently verified by the ECD GSE through other means or mechanisms provided. The information and/or documentation provided will be reviewed in accordance with the Criteria and Methods of Evaluation of Applications established by GSE.

The applicant accepts that the ECD GSE has the discretionary right to reject 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 put at risk, notifying the applicant of the non-approval.

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

1.4.1.1. Who can apply for a certificate.

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

1.4.1.2. Application Process, Registration and Liability.

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 RA GSE system.

1.4.2. Certificate Application Processing.

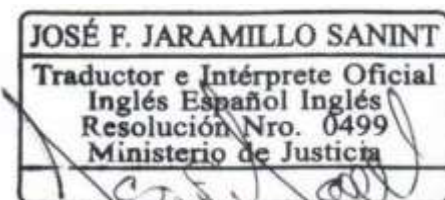
1.4.2.1. Procedure for processing the application/ identification and authentication.

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


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

1.4.2.2. Criteria for acceptance or rejection of the application.

If, once the identity of the applicant has been verified, the information provided complies with the requirements established by this DPC, the request is approved. If this is not possible:





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

full identification of the identity of the applicant or there is no full authenticity of the information provided, the application is denied and the certificate is not issued.

ECD GSE assumes no responsibility for the consequences that may arise from the non-approval of the issuance of a digital certificate and so accepts and acknowledges the applicant who has been denied the issuance of the respective certificate.

Likewise, ECD GSE reserves the right not to issue certificates despite the fact that the identification of the applicant or the information provided by the latter has been fully 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 the filing of an application and the process did not approve the review of the application or the applicant did not carry out the identity validation, after fifteen (15) days without the novelty being corrected, the RA of the ECD GSE will have as an alternative to carry out the rejection of the application and the applicant will be notified to process a new application. For which ECD GSE will notify the applicant of the approval or rejection of the application.

1.4.2.3. Deadline for processing certificate requests

The deadline for processing an application by the GSE RA is one (1) to five (5) business days from the time the requested information and/or documentation is received and the applicant has approved the initial validation of the identity.

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

1.4.3. Issuance of the Certificate.

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

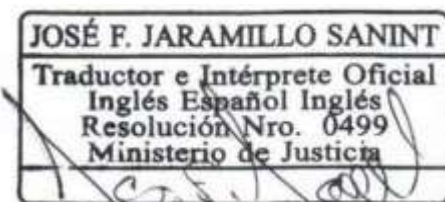
The final step in the process of issuing digital certificates is the issuance of the certificate by ECD GSE and its safe delivery to the subscriber and/or responsible party.

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


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

1.4.3.2. Notification mechanisms authorized by subscribers.

By email or other defined and authorized means; for this purpose, the subscriber is notified of the issuance of his digital certificate and therefore the subscriber accepts and acknowledges that once he 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 did not have satisfactory delivery. In the event that the subscriber requests that the issuance of the certificate





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

on a cryptographic device, it will be understood as delivered once you have the shipping record: delivery letter and/or the shipping guide to the logistics or courier operator and/or confirm in the issuance notification that the cryptographic device has received

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

1.4.4. Acceptance of the Certificate.

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

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

1.4.5. Pair of Keys and Use of Certificate.

1.4.5.1. Responsibilities of the Subscriber for the use of the private key.

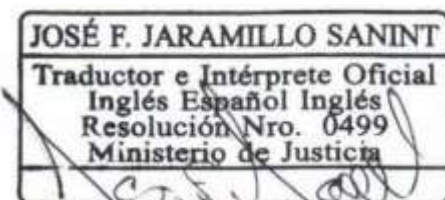
The subscriber or person responsible for the digital certificate and the associated private key accepts the conditions of use established in this DPC by the mere fact of having requested the issuance of the certificate and may only use them for the uses explicitly mentioned and authorized in this DPC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

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


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

In this regard, you must:

- Check that the associated certificate does not breach the effective start and end dates.
- Check that the certificate associated with the private key is not revoked.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

- Check that the fingerprint of the root ECD certificate and that of the ECD GSE subordinate's certificate match the one published by GSE on its website.

1.4.5.2.1. Fingerprint of root ECD certificate:

SHA-256

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

SHA256

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

SHA256

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

1.4.5.2.2. Fingerprint of ECD Subordinate GSE Subordinate Certificate 001:

SHA-256

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

SHA256

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

SHA256

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

1.4.6. Renewal of Certificate without Change of Keys.

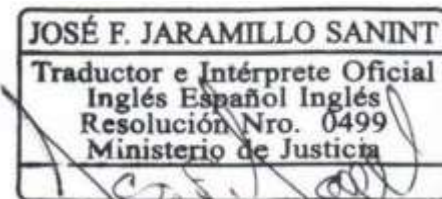
The ECD GSE does not meet requirements for the renewal of a certificate without a change of keys.

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


It does not apply because certificates are not issued without a change of keys.

1.4.6.2. Who can request a renewal without changing keys.

It does not apply because certificates are not issued without a change of keys.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

It does not apply because certificates are not issued without a change of keys.

1.4.6.4. Notification to the subscriber or responsible for the issuance of a new certificate without change of keys.

It does not apply because certificates are not issued without a change of keys.

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

It does not apply because certificates are not issued without a change of keys.

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

It does not apply because certificates are not issued without a change of keys.

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

It does not apply because certificates are not issued without a change of keys.

1.4.7. Renewal of Certificate with Change of Keys.

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

1.4.7.1. Circumstances for renewal of a certificate.

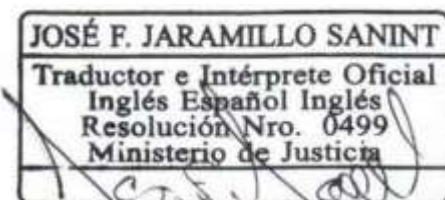
A digital certificate may be renewed at the request of the subscriber or responsible for upcoming loss of validity or revocation in accordance with the causes mentioned in this DPC or when required by the subscriber.

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


For certificates of natural persons, the subscriber can request the renewal of the certificate. For legal entities, the renewal of the digital certificate may be requested by the legal representative, responsible or appointed alternates duly empowered or attorneys-in-fact.

1.4.7.3. Procedure for renewing a digital certificate.

The procedure for renewing digital certificates is the same as the procedure for applying for a new certificate. The subscriber must access the means or mechanisms for this purpose to collect the information from the ECD GSE and initiate the certificate renewal application process in the same way as it did when it requested the certificate for the first time. Your information will be validated again in order to update data if required.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.4.7.4. Notification of Certificate Renewal to Subscriber.

By email or other means for this purpose, the subscriber is notified of the issuance of his digital certificate and therefore the subscriber accepts and acknowledges that once he receives said notification, it will be understood that the certificate has been issued. It will be understood that the information has been received where the issuance of a certificate is notified, when said notification enters the information system designated by the subscriber and/or responsible, the receipt of the notification is evidenced. In the event that the subscriber requests that the issuance of the digital certificate be on a cryptographic device, it will be understood as delivered once the shipping record is obtained: delivery letter and/or the shipping guide to the logistics or courier operator and/or confirm in the issuance notification that the cryptographic device has received

1.4.7.5. Acceptance of certificate renewal.

Confirmation from the subscriber or responsible party is not required as acceptance of the certificate renewal received. It is considered that a renewed certificate is accepted by the subscriber or person in charge from the moment he requests its issuance, therefore, if the information contained in the issued certificate does not correspond to the current state of it or was not supplied correctly, it must be requested to be revoked by the applicant or person in charge and he accepts it.

1.4.7.6. Publication of the certificate

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

1.4.7.7. Notification of issuance of certificates to other entities

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

1.4.8. Certificate Modification.

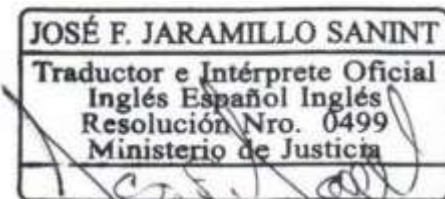
Digital certificates issued by ECD GSE cannot be modified, i.e. no amendments apply. Consequently, the subscriber must request the issuance of a new digital certificate. In this event, a new certificate will be issued to the subscriber; the cost of this modification will be fully borne by the subscriber according to the rates reported by ECD GSE or according to the conditions defined at the contractual level.

1.4.8.1. Circumstances for modification of a certificate.


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

1.4.8.2. Who can request an amendment.

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

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

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

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

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

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

1.4.8.6. Publication of the certificate modified by the ECD.

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

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

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

1.4.9. Revocation and Suspension of the Certificate.

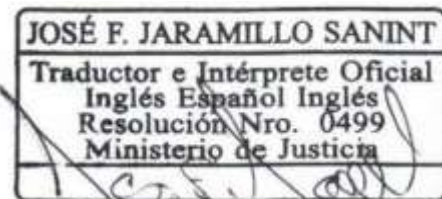
1.4.9.1. Circumstances under which a certificate may be revoked.

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


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

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

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





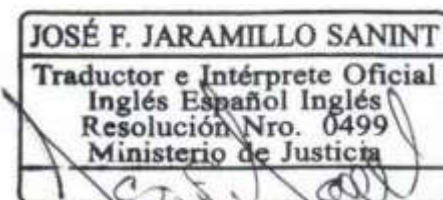
	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

- a. At the request of the subscriber, controller or a third party on their behalf and representation.
- b. By death of the subscriber or responsible party.
- c. By confirmation or evidence that any information or fact contained in the digital certificate is false.
- d. The certification body's private key or its security system has been compromised in a material way that affects the reliability of the certificate.
- e. By court order or competent administrative entity.
- f. By commitment to safety in any reason, mode, situation or circumstance.
- g. For supervening incapacity of the subscriber or responsible party.
- h. By liquidation of the represented legal entity that appears in the digital certificate.
- i. Due to the occurrence of new events that cause the original data not to correspond to reality.
- j. For loss or disablement of the cryptographic device that has been delivered by ECD GSE.
- k. By the termination of the subscription contract, in accordance with the groundsestablished in the contract.
- l. For any reason that reasonably leads to believe that the service of certification has beencompromised to the point that the reliability of the digital certificate,
- m. For the improper handling by the subscriber of the digital certificate,
- n. For the breach of the subscriber or the legal entity it represents or the that is linked through theterms and conditions document or responsible of digital certificates of the ECD GSE.
- o. Knowledge of events that modify the initial state of the data supplied, among others: termination of the Legal Representation, termination of the employment relationship, liquidation or termination of legal personality, cessation in the public function or change to a different one,
- p. At any time that there is evidence of falsity in the data provided by the applicant, subscriber or responsible party.
- q. For non-compliance by the ECD GSE, the subscriber or person in charge of the obligations established in the DPC.
- r. For failure to pay the securities for the certification services, agreed between the applicant and ECD GSE.


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

1.4.9.2. Who can request revocation of a certificate

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

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

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

1.4.9.3. Procedure for requesting revocation of a certificate.

The subscriber and/or responsible party, a bona fide third party or any person will have the opportunity to request the revocation of a digital certificate whose causes are specified in this DPC can do so under the following procedures:

- At GSE offices.

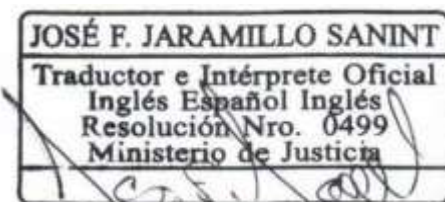
During business hours, written requests for revocation of digital certificates signed by subscribers and/or managers are received by providing the original identification document.

- Online Revocation Request:


The subscriber and/or responsible party may carry out the process of revocation of the digital certificate through the GSE S.A. 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, a notification will arrive with the security code to complete the completion of the online revocation request, the subscriber and/or responsible party must select the reason for the revocation, enter the security code, accept the Terms and Conditions and revoke your digital certificate; once the request ends, the selected certificate will be automatically revoked and the revocation confirmation will be sent to the registered email. Other means available to carry out the revocation of 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 where the request for the issuance of the digital certificate of authorized third parties was filed.

- Revocation Service via email

Through our email revocaciones@gse.com.co, subscribers and/or managers can request the revocation of digital certificates according to the grounds for revocation mentioned in the Circumstances for the revocation of a certificate section of this DPC, by sending a revocation request letter digital signature or email with the subscriber's data and cause for revocation, Digital Certification Service Revocation Form.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Note: The ECD - GSE makes available a guide template to make the revocation request letter which is available on the website <https://gse.com.co/guias-y-manuales>, option Revocations and Root and Subordinate Certificates

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

1.4.9.4. Grace period for requesting revocation of a certificate.

Upon review of a revocation request, 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 application. If it was an erroneous request, the subscriber or person in charge must request a new certificate, since the revoked certificate lost its validity immediately the revocation request was validated and ECD GSE will not be able to reactivate it.

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

Once the revocation of the certificate has been requested, if it is evidenced that said certificate is used in connection with the private key, the subscriber or responsible party releases ECD GSE from all legal responsibility, since it recognizes and accepts that the control, custody and confidentiality of the private key is the exclusive responsibility of the latter.

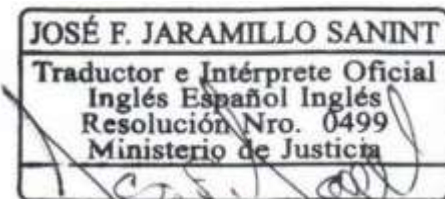
1.4.9.5. Time within which the ECD must process the revocation request.

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


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

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

It is the responsibility of the subscriber and/or responsible for a digital certificate and the latter





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

accepts and acknowledges it, to inform third parties in good faith of the need to verify the validity of the digital certificates on which it is making use at any given time. The subscriber and/or responsible party will also inform the third party in good faith that, to carry out said consultation, it has the list of revoked CRL certificates, published periodically by ECD GSE.

1.4.9.7. Frequency of issuance of CRLs.

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

1.4.9.8. Maximum latency of CRLs.

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

1.4.9.9. Availability of online status check/ revocation.

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

The online validation of digital certificates using OCSP must be carried out with a tool that implements the OCSP protocol and is able to understand the responses generated by the service, such is the case of OPENSSL.

1.4.9.10. Online Revocation Verification Requirements.

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

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

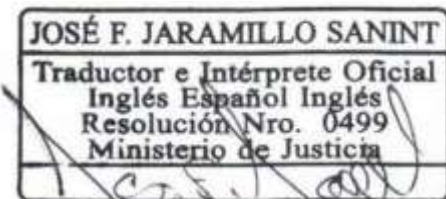
1.4.9.11. Notice of Revocation of a Certificate.

Within 24 hours of the revocation of a certificate, ECD GSE informs the subscriber and/or responsible party, by email or other means for this purpose, the revocation of their digital certificate is notified and therefore the applicant accepts and acknowledges that once they receive the notification it will be understood that their request was met. Shall mean that information has been received notifying the revocation of a certificate when such notification enters the information system designated by the applicant.

Publication of a revoked certificate at the CRL constitutes proof and public notice of its revocation.

1.4.9.12. Other Available Forms of Disclosure of Revocation Information.

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.4.9.13. Special requirements for renewal of committed keys.

If the revocation of a digital certificate was requested due to compromise (loss, destruction, theft, disclosure) of the private key, the subscriber may request a new digital certificate for a period equal to or 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 lies with the subscriber or responsible party and the latter accepts and acknowledges this, therefore, it is he who assumes the cost of the renewal in accordance with the current rates set for the renewal of digital certificates.

1.4.9.14. Circumstances for suspension

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

1.4.9.14.1. Who can request suspension

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

1.4.9.14.2. Suspension Request Procedure

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

1.4.9.14.3. Suspension period limits

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

1.4.10. Certificate Status Services.

1.4.10.1. CRL Profile.

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

1.4.10.1.1. Version Number.

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

1.4.10.1.2. CRL and CRL extensions.

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

1.4.10.2. CRL Availability.

As indicated in section 6.12.9 On-line revocation/availability of status verification.

1.4.10.3. OCSP Profile.

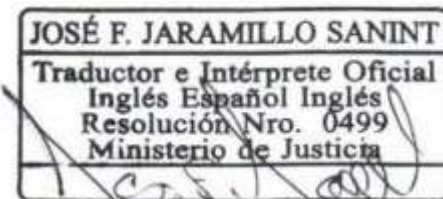
The OCSP service complies with the provisions of RFC6960 "X.509 Internet Public Key Infrastructure OnlineCertificate Status Protocol - OCSP".

1.4.10.3.1. Version Number.


Complies with OCSP Version 1 of RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

1.4.10.3.2. OCSP extensions.

N/A





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.4.10.4. OCSP service availability.

As indicated in section 6.12.9 On-line revocation/availability of status verification.

1.4.10.4.1. Operational characteristics.

For the status of certificates issued by ECD GSE, an online consultation service based on the OCSP protocol is available at <https://ocsp2.qse.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 answered via http or the query via CRL.

1.4.10.4.2. Optional Features.

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

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

1.4.11. End of Subscription.

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

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

1.4.12. Key Custody and Recovery.

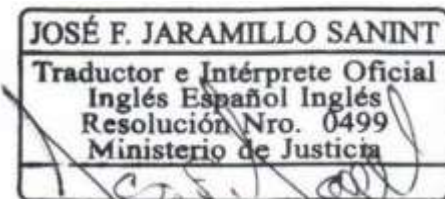
1.4.12.1. Storage of the subscriber's private key.

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


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

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

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

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

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

1.4.12.2. Key custody and retrieval policies.

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

1.4.12.3. Policies for custody and recovery of session keys.

The recovery of the subscriber's session key or pin is not possible since the sole person responsible for assigning it and this so declares and accepts. The responsibility for the custody of the session key or pin is the subscriber who agrees not to keep digital records, written or in any other format and who is obliged to protect access to the pin, so if the pin is forgotten, a case will be filed with the ECD - GSE service desk to verify the request and if required, the subscriber will file a request to revoke the certificate and manage the request for a new digital certificate.

1.5. FACILITIES, MANAGEMENT AND OPERATIONAL CONTROLS.

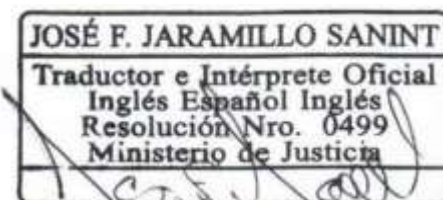
1.5.1. Physical Security Controls.

1.5.1.1. Physical location of the ECD.


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

The ECD GSE guarantees that the PKI servers are in continuous operation virtually in the Amazon cloud.

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

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

1.5.1.2. 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 surveillance personnel. There are restricted areas within the facilities that, due to the type of communications equipment considered critical and sensitive operations that are handled, are allowed access only to certain people.

1.5.1.3. Energy and air conditioning.

The communication center has an air conditioning system and has an adequate electricity 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.

1.5.1.4. Exposure to water.

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

1.5.1.5. Fire prevention and protection.

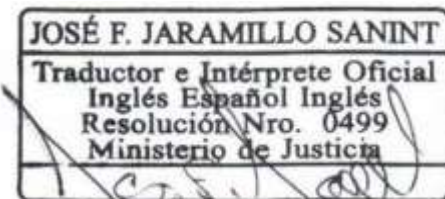
The communication center has a fire detection system and a fire extinguishing system. There is a wiring system that protects internal networks.

1.5.1.6. Backup system.


There are procedures for taking backups, restoring and testing databases for accredited services. Missionary servers are in cloud environments, however, on-premises servers are backed up and stored on a local NAS server with their respective contingency.

1.5.1.7. Disposal of Materials.

Any paper document that contains sensitive information of the entity and that has reached its





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

1.5.1.8. Off-site backup.

ECD GSE will maintain a backup copy of the databases on Amazon that will be taken to the replica in case it is required for restoration.

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

1.5.2. Procedural Controls.

1.5.2.1. ECD trust roles.

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

- RA Agents: Persons responsible for day-to-day operations such as: review and approval of applications attending all activities related to the digital certification services provided by the ECD GSE through the RA, the roles and responsibilities of the RA agents are defined in accordance with the Profiles and Functions of the ECD GSE.
- RA Administrator: The person responsible for managing and configuring the RA.
- RA Auditor: Trained and impartial person in charge of evaluating compliance with the requirements of the RA, auditing the information systems of the RA clarifying that their role is different from that of the internal auditor of the management systems.

1.5.2.2. Number of people required in each role.

For each of the aforementioned roles, the ECD will guarantee the collaborators to perform the tasks that affect the management of cryptographic keys of the ECD itself.

1.5.2.3. Identification and authentication of each role.

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

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

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

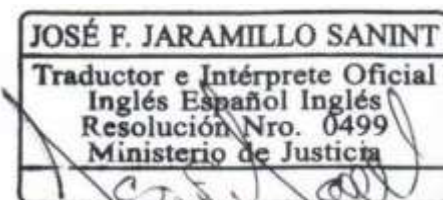
1.5.2.4. Roles requiring segregation of duties.

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


1.5.3. Personnel controls.

1.5.3.1. Requirements on qualification, experience and professional knowledge.

A personnel selection process has been defined based on the profile of each of the positions





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

involved in the process of issuing digital certificates and the procedures of digital certification services. The candidate for a position must have the training, experience, knowledge and skills defined in the Profile and Job Functions document.

1.5.3.2. Background check procedure.

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

1.5.3.3. Training requirements.

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

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

1.5.3.4. Training Update Requirements.

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

1.5.3.5. Frequency and sequence of task rotation.

There is no rotation of tasks in the aforementioned positions.

1.5.3.6. Penalties for unauthorized actions.

It is qualified as serious misconduct to carry out unauthorized actions and the persons will be sanctioned in accordance with counterclaim and/or disciplinary process.

1.5.3.7. Controls for contracting with third parties.

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

1.5.3.8. Documentation provided to staff during induction and reinduction.

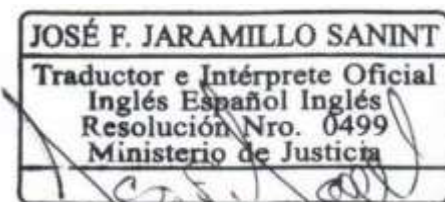
The documentation mentioned in the Training Requirements section is published for easy reference and is part of the induction of personnel.

1.5.4. Audit Log Procedures.


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

1.5.4.1. Type of events recorded.

The most sensitive activities of the certification cycle require the control and monitoring of events





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

that may occur during its operation. According to their level of criticality, events are classified as:

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

1.5.4.2. Log processing frequency.

Audit records are reviewed using manual procedures and/or Automatic

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

1.5.4.3. Retention Period of Audit Logs.

Audit records are kept for three (3) years after the last modification of the file, which guarantees that you can review the problems presented with those that have occurred in the history. Once the 3 years have elapsed and with the authorization of the GSE Management Committee, you can proceed to destroy them, however, if the records are being used in legal proceedings, their retention will be indefinite.

1.5.4.4. Protection of Audit Logs.

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

1.5.4.5. Audit log backup procedure.

Backups of audit logs are replicated to a centralized log site

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

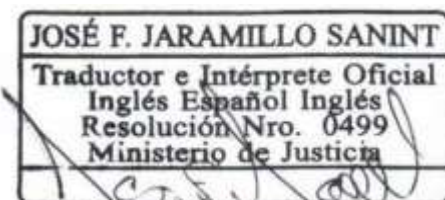
The audit information collection system is based on the automatic logs of the applications that support the certification cycle including application logs, security logs and system logs. Which are stored in CloudWatch and databases for monitoring

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


Judgment of the Information Security Officer, the subject will be notified of a security incident detected through the audit logs in order to have a formal response on what happened.

1.5.4.8. Vulnerability analysis.

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.5.5. Archive of Records.

The archive log and event log is executed by the GSE SOC NOC.

1.5.5.1. Types of records to be archived.

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

1.5.5.2. Retention Period.

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

1.5.5.3. File Protection.

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

1.5.5.4. File Backup Procedures.

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

1.5.5.5. Requirements for time stamping of records.

Servers are kept up to date with UTC Time (Coordinated Universal Time). They are synchronized using the NTP (Network Time Protocol) 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, the synchronization will be carried out with the NTP server of the INM.

1.5.5.6. File collection system (internal or external).

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

1.5.5.7. Procedures for Obtaining and Verifying File Information.

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


1.5.6. Change of Keys.

1.5.6.1. ECD GSE root key change.

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

1.5.6.2. Change of keys of the ECD Subordinate GSE.

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

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

1.5.7. Commitment and Disaster Recovery.

1.5.7.1. Incident Management Procedures.

The ECD GSE has established and tested an Information Security Incident Procedure that establishes the actions to be followed in the event of a vulnerability or security incident. Once the systems reset procedures have been satisfactorily executed, service will be provided to the public.

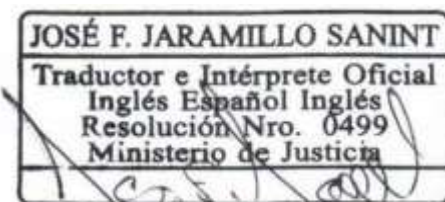
1.5.7.2. Recovery procedure in case of alteration of technological resources.

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


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

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

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

In case of commitment of the ECD GSE:

- a) Apply incident containment to prevent reoccurrence
- b) Inform all Subscribers, Managers, Trusted Third Parties and other CAs with whom it has agreements or another type of relationship of the commitment.
- c) It will indicate that the certificates and information relating to the status of the revocation signed using this key are not valid.
- d) Inform ONAC and clients.

1.5.7.4. Resilience in the event of a natural disaster or catastrophe.

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

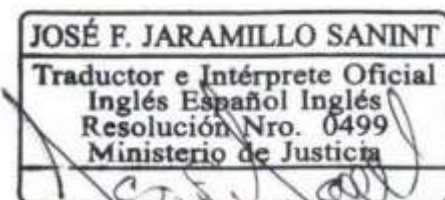
1.5.8. Termination of CA or RA.

1.5.8.1. Procedure in case of cessation of CA and RA


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

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

- a. The termination of the activity or activities and the precise date of cessation.
- b. The Legal Consequences of Cessation with Respect to Accredited Services
- c. The possibility that a subscriber obtains a refund equivalent to the value of the remaining term of the contracted service.
- d. The authorization issued by the Superintendency of Industry and Commerce so that the ECD can cease the service, and if applicable, the operator of the CRL responsible for the publication of the certificates issued by the ECD - GSE until the last of them expires.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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, ECD GSE services, without additional costs, if they do not accept the continuation of the service through the third party, 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 they request it within two (2) months following the second publication on the website and notices.

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

1.6. TECHNICAL SAFETY CONTROLS

1.6.1. Generation and Installation of Key Pairs.

1.6.1.1. Generation of the ECD Root key pair.

The generation of the Root ECD 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. For the storage of the private key, a FIPS 140-2 level 3 approved cryptographic device was used.

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

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

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

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

1.6.1.4. Delivery of the private key to subscribers.

The private key is delivered to the subscriber and/or responsible party on their cryptographic device and it is not possible to extract it. Therefore, there is no private key copy of the subscriber.

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

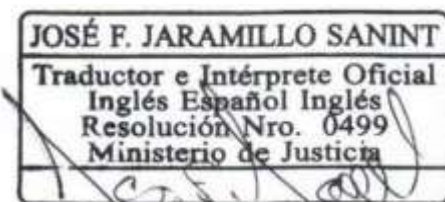
The public key is sent to the ECD GSE as part of the request for the digital certificate in PKCS#10 format.

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


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

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

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.6.1.5. Size of Keys.

For RSA, the following sizes of keys have been defined:

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

When trying to derive the private key, from the 2048-bit public key contained in the end user certificates, the problem lies in finding the prime factors of two large numbers, since there would be 22047 possibilities for each number. It is estimated that decrypting a 2048-bit public key would require processing work on the order of 3x1020MIPS-years*.

*MIPS-year: unit used to measure the processing capacity of a computer running for one year. It is equivalent to the number of millions of instructions that a computer is able to process per second for a year.

For ECDSA, the following sizes of keys have been defined:

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

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

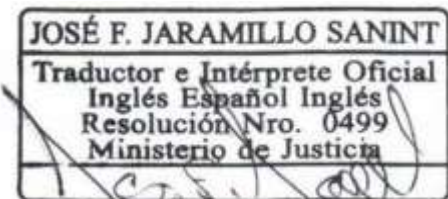
1.6.1.6. Public key generation parameters.

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


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

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

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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.6.1.7. Permitted uses of the key.

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

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

TYPE OF CERTIFICATE	KEY USAGE
signing certificate	DigitalSignature
authentication certificate	NonReputation

1.6.2. Private Key Protection and Cryptographic Module Engineering Controls.

1.6.2.1. Standards for use of cryptographic modules.

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

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

The private keys of the ECD GSE Root and the private keys of ECD GSE subordinates are under multiperson control. The method of activating the private keys is by initializing the ECD GSE software by means of a combination of keys held by several people

1.6.2.3. Custody of the private key of the ECD.

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.

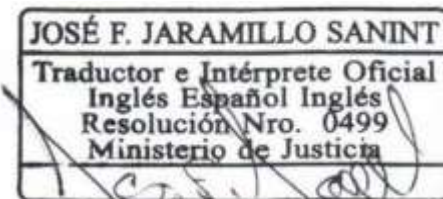
The technical data of the device are as follows:

- SafeNet Luna SA


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

1.6.2.4. Backup copy of the private key.

The private keys of the ECD GSE 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 Custody of the private key).





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

1.6.2.5. Private key file.

The private keys of ECD GSE 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 Custody of the private key).

They are in a cryptographic backup box in a different place from the place where the HSMs are located.

1.6.2.6. Transfer of private keys.

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 Custody of the private key).

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.

1.6.2.7. Storage of private keys.

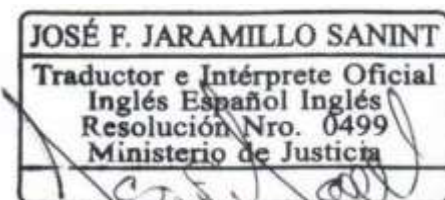
The private keys of the ECD GSE are generated and stored in cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher level of security. (See 8.2.3 Custody of the private key).

The cryptographic keys can be loaded into a cryptographic device of equal performance from the backup copies through a process that requires the participation of at least two operators.


1.6.2.8. Method of activation of the private key.

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

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.6.2.9. Method of deactivating the private key.

Disabling the private key is done by disabling the software or shutting down the ECD server. It is activated again through the use of multi-person control, following the procedures marked by the manufacturer of the cryptographic module.

1.6.2.10. Method for destroying the private key.

The method used in case the destruction of the private key is required is through the deletion of 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 in the case in which it is required.

1.6.2.11. Technical characteristics of the cryptographic modules used.

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

1.6.2.12. Evaluation of the cryptographic module.

The cryptographic device is monitored using its own software to prevent possible failures.

1.6.2.13. Evaluation of the encryption system.

ECD GSE welcomes the recommendations for the use of cryptographic algorithms and key lengths that are published by NIST (National Institute of Standards and Technology) and by ONAC, if any circumstance materializes in which the algorithms used for signature and encryption by ECD GSE are compromised at all levels, ECD GSE will immediately take the measures and recommendations provided by this entity or by ONAC to maintain the security of the signature during the remainder of its life cycle.

1.6.3. Other Aspects of Key Pair Management.

1.6.3.1. Archiving the public key.

ECD GSE will maintain controls for archiving its own public key.

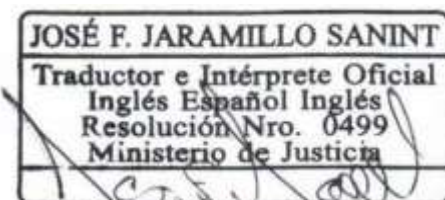
1.6.3.2. Operating periods of the certificates and period of use of the pair of keys.

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


RSA algorithm

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

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

ECDSA Algorithm:

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

1.6.4. Activation Data.

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

1.6.4.2. Protection of Activation Data.

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

1.6.4.3. Other Aspects of Activation Data.

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

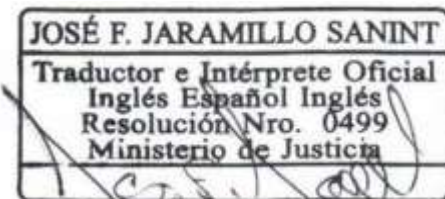
1.6.4.4. Computer Security Controls.

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

- Operating system security settings.
- Application security settings.
- Access control to devices.
- Closure of system vulnerabilities.
- Hardenisation of systems according to good practices.
- Network configuration at the security level (Internal Network, Administrative Network, among others)
- Configuration of Users and permissions.
- Configuring Log events.
- Backup and recovery plan.
- Antivirus settings.
- Network traffic requirements configured in the firewall.

1.6.4.5. Specific technical safety requirements.

ECD GSE has a technological infrastructure duly monitored and equipped with security elements





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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.

1.6.4.6. Computer security assessment.

The security of end-user equipment is managed from ECD GSE and is supported with a risk analysis 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, periodic security tests (ethical hacking) are carried out, so that possible vulnerabilities of the systems are identified and that contribute to their closure.

1.6.4.7. Actions in the Event of an Information Security Event or Incident.

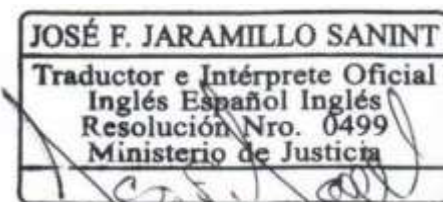
The Information Security Management System implemented by ECD GSE has established an incident management procedure that specifies the actions to be executed, components or resources to be used and how personnel should react in the event of an intentional or accidental event that disables or degrades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

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


1.6.5. Life Cycle Safety Controls.

1.6.5.1. System Development Controls.

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.6.5.2. Safety Management Controls.

ECD GSE maintains control over the inventories of the assets used in its certification process. There is a classification of these according to their level of risk.

ECD GSE periodically monitors its technical capacity in order to guarantee an infrastructure with the minimum availability requested in the CEA.

1.6.5.3. Life Cycle Safety Controls.

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

1.6.6. Network Security Controls.

ECD GSE has a network infrastructure duly monitored and equipped with 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.

1.6.7. Timestamping.

ECD GSE has the chronological stamping service, which is described in the corresponding Certificate Policies for Chronological Stamping Service, published on the <http://www.gse.com.co> portal.

1.7. CERTIFICATE PROFILES CERTIFICATE PROFILES, CRL AND OCSP.

1.7.1. Certificate Profile.


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

Contenido de los certificados. A certificate issued by ECD GSE, in addition to being digitally signed by ECD GSE, shall contain at least the following:

1. Name, address and address of the subscriber.
2. A Unique Identification of the subscriber named on the certificate.
3. The name and place where the CA performs activities
4. Public key of the certificate.
5. The methodology for verifying the subscriber's digital signature imposed on the data message.
6. The (unique) serial number of the certificate.
7. Date of issue and expiration of the certificate.



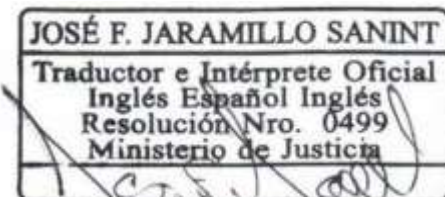


	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public


In addition, the Accreditation Code assigned by the ONAC is included in accordance with the certificate extension defined in numeral 4.2 of RFC 5280 identified in the field: Alternative name of the subject

Field	RSA Value or Constraints	ECDSA Value or Constraints
Version	3(0x2)	3(0x2)
Serial Number	Unique identifier issued by ECD GSE	Unique identifier issued by ECD GSE
Signature algorithm	SHA256withRSAEncryption	SHA384withECDSA
Issuer	See section "Rules for the interpretation of various forms of name". For ECD GSE as issuer it is specified: E= info@gse.com.co , CN= Subordinate Authority 01 GSE, OU=PKI, O=GSE L=BOGOTA, D.C. C=CO	See section "Rules for the interpretation of various forms of name. " For ECD GSE as issuer it is specified: STREET= www.gse.com.co , E= info@gse.com.co , CN=GSE ECDSA SUBORDINATE, SN=900204278, OU=GSE ECDSA R2 SUB1, O= ELECTRONIC SECURITY MANAGEMENT S.A. L=BOGOTA, D.C. S=CAPITAL DISTRICT C=CO
Valid from	Specifies the date and time from which the certificate is valid.	Specifies the date and time from which the certificate is valid.

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 January 19, 2024.

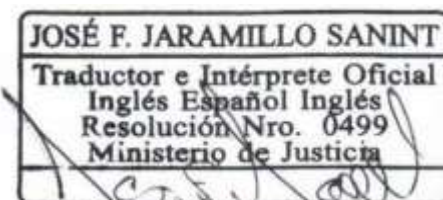





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Field	RSA Value or Constraints	ECDSA Value or Constraints
Valid until	Specifies the date and time from which the certificate ceases to be valid.	Specifies the date and time from which the certificate ceases to be valid.
Subject	In accordance with the policy of Annex 1 and the "Rules for the interpretation of various forms of name".	In accordance with the policy of Annex 1 and the "Rules for the interpretation of various forms of name".
Subject Public Key	Codified in accordance with RFC 5280. The certificates issued by ECD GSE have a length of 2048 bits and RSA algorithm.	Codified in accordance with RFC 5280. The certificates issued by ECD GSE have a length of 256 bits and EC algorithm.
Authority Key Identifier	It is used to identify the root certificate in the certification hierarchy. I normally refer to the "Subject Key Identifier" field of ECD GSE as a digital certification issuing entity.	It is used to identify the root certificate in the certification hierarchy. I normally refer to the "Subject Key Identifier" field of ECD GSE as a digital certification issuing entity.
Subject Key Identifier	It is used to identify a certificate that contains a certain public key.	It is used to identify a certificate that contains a certain public key.
Certificate Directives	Describes the policies applicable to the certificate, specifies the OID and URL where the certification policies are available.	Describes the policies applicable to the certificate, specifies the OID and URL where the certification policies are available.
Using the key	Specifies the permitted uses of the key. It's a CRITICAL FIELD.	Specifies the permitted uses of the key. It's a CRITICAL FIELD.
CRL Distribution Point	It is used to indicate the addresses where the ECD GSE CRL is published. In the Root ECD certificate, this attribute is not specified.	It is used to indicate the addresses where the ECD GSE CRL is published. In the Root ECD certificate, this attribute is not specified.
Access to Authority information	It is used to indicate the addresses where the ECD GSE root certificate is located. In addition, 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. In addition, to indicate the address to access the OCSP service. In the ECD GSE root certificate, this attribute is not specified.
Subject Alternate Name	It is used to indicate the email address and additionally to indicate the accreditation code assigned by the ONAC. Name RFC822 = correo@empresa.com URL= dDS://ase.com.co/documentos/certificaciones /accreditacion/16-ECD-001 .pdf	It is used to indicate the email address and additionally to indicate the accreditation code assigned by the ONAC. Name RFC822 = correo@empresa.com URL= dDS://ase.com.co/documentos/certificaciones /accreditacion/16-ECD-001 .pdf
Uses key extensions	Other purposes in addition to the use of the key are specified.	Other purposes in addition to the use of the key are specified.
Basic constraints	The "PathLenConstraint" extension indicates the number of sub-levels that are supported in the certificate path. There is no restriction for ECD GSE, therefore it is zero.	The "PathLenConstraint" extension indicates the number of sub-levels that are supported in the certificate path. There is no restriction for ECD GSE, therefore it is zero.

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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.7.1.1. Version Number.

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

1.7.1.2. Certificate extensions.

The certificates issued by GSE are described in detail in Annex 1 of this DPC.

1.7.1.3. KeyUsage.

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".

1.7.1.4. Certificate Policy Extension.

The certificate policies extension of the current X.509 is the object identifier of this CPD in accordance with the object identifier section of the Certification Policy of this CPD. Extension is not considered critical.

1.7.1.5. Alternative Subject Name.

The "subjectAltName" extension is optional and the use of this extension is "Non-Critical".

1.7.1.6. Basic Restrictions.

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

1.7.1.7. Extended use of the key.

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

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

1.7.1.8. Object Identifiers (OIDs) of the algorithms.

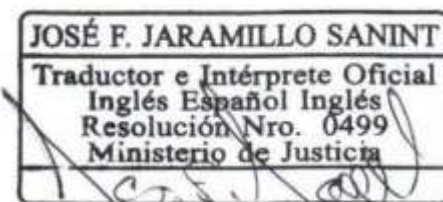
The object identifier of the signature algorithm is: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption

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 SHA384WITHEDSA.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

1.7.1.9. Name formats.

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

1.7.1.10. Name Restrictions.

Names must be written in capital letters and without tildes.

The country code is assigned in accordance with ISO 3166-1 "Codes for the representation of the names of countries and their subdivisions. Part 1: Country codes ". In the case of Colombia it is "CO".

1.7.1.11. Object identifier of the Certification Policy.

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

1.7.1.12. Use of the Policy Constrains extension.

Not stipulated.

1.7.1.13. Syntax and Semantics of Policy Qualifiers

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

1.7.1.14. Semantic treatment for the Certificate Policies extension.

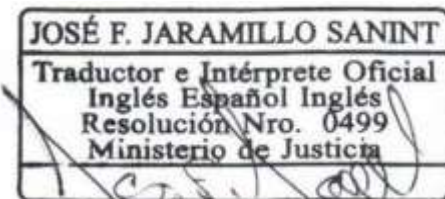
Not stipulated.

1.7.2. CRL Profile.


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

1.7.3. OCSP Profile.

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.8. COMPLIANCE AUDIT AND OTHER EVALUATION.

1.8.1. Frequency or Circumstances of Controls.

Compliance with the controls that guarantee the security in the issuance of digital certificates will be evaluated by means of an annual audit carried out by an external audit firm.

1.8.2. Identity/qualification of the Auditor.

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

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

1.8.3. Relationship between the Auditor and the Audited Entity.

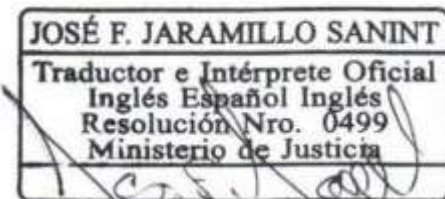
The only relationship established between the auditor and the audited entity is that of auditor and auditee. The audit firm exercises its absolute independence in the performance of its audit activities and there is no conflict of interest as the relationship is purely contractual.

1.8.4. Aspects Covered by Controls.


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

1.8.5. Actions to be Taken as a Result of the Detection of Deficiencies.

The 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.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.8.6. Communication of Results.

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

1.9. OTHER BUSINESS AND LEGAL MATTERS.

1.9.1. Fees.

Does not apply

1.9.2. Financial Responsibility.

1.9.2.1. Other property.

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

1.9.2.2. Insurance or guarantee of coverage for subscribers, managers and bona fide third parties.

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

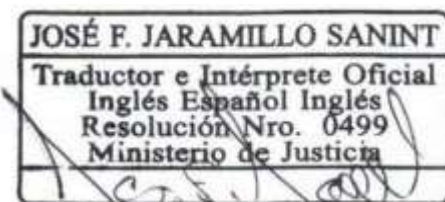
1.9.3 Confidentiality of commercial information.

1.9.3.1. Responsibility to Protect Confidential Information.


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

All non-public information is considered confidential and subject to restricted access, except in those cases provided for by law such as competent courts or administrative bodies or imposed by law, no confidential information is disseminated without the express written consent of the subscriber or the entity that has granted it the character of confidentiality.

However, it reserves the right to disclose to employees and consultants, external or internal, the confidential data necessary to carry out its activities as ECD, obliging all staff to sign a





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

confidentiality agreement within the framework of the contractual obligations contracted with ECD GSE.

1.9.3.2. Confidential Information.

The following information is considered confidential:

- a. Private key of the Certification Authority and/or ECD
- b. Private key of the subscriber or entity
- c. Information provided by the subscriber or entity that is not necessary to validate the trust of the subscriber or entity
- d. Information about the applicant, subscriber and/or controller obtained from different sources (e.g. from a complainant or regulators)
- e. Transaction records
- f. Audit Logs
- g. Security Policies
- h. Business Continuity Plan
- i. All information that is classified as "Confidential" in the documents delivered by ECD GSE

1.9.3.3. Non-Confidential Information.

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

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

1.9.3.4. Duty to protect confidential information.

ECD GSE maintains security measures to protect all confidential information supplied to ECD GSE directly or through the channels established for this purpose from its receipt to its storage and custody, where they will rest as defined in the TRD. ECD GSE has an Integrated Management System that includes an Information Security System. This allows us to ensure that the information of our subscribers will not be compromised, nor disclosed to third parties unless there is a formal request from a competent authority that requires it.

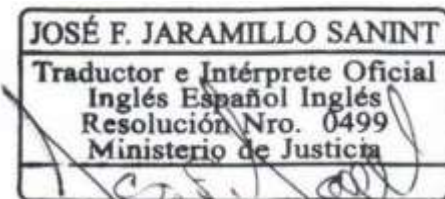
1.9.4. Privacy of Personal Information.

1.9.4.1. Personal Data Processing Policy.


The ECD GSE has as its 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, replace it, which can be consulted on our website <https://qse.com.co/Políticas> in the Personal Data Processing Policy section, as well as the authorization for the processing of personal data.

1.9.4.2. Information treated as private.

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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

1.9.4.3. Information Not Qualified as Private.

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

1.9.4.4. Responsibility for the protection of personal data.

ECD GSE is responsible and has the appropriate technological resources to help ensure the adequate 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 bodies. Certification entities will have, among others, the following duties: Guarantee the protection, confidentiality and due use of the information provided by the subscriber, responsible and entity".

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

1.9.4.5. Notification and consent to use personal data.

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

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

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

1.9.4.7. Other Circumstances of Disclosure.

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


1.9.4.8. Security system to protect information.

With regard to the system that houses the information provided by the subscriber or person in charge of the certification service, the following validations are carried out:

- a. The infrastructure provider must have the good practices of the following Standards:
 - i. ISO 27001
 - ii. ISO 9001
- b. Penetration testing and vulnerability scanning in the network, carried out by a company specialized in Ethical Hacking.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.9.5. Intellectual Property Rights.

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

1.9.6. Representations and Warranties.

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

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

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

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

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

1.9.7. Disclaimers of Warranties.

Not applicable

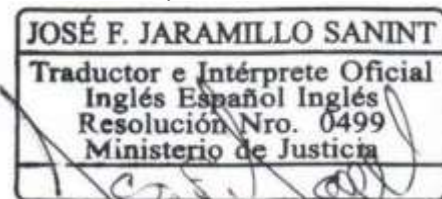
1.9.8. Limitations of Liability.

1.9.8.1. 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.

1.9.8.2. Liability for service availability.

The Subscriber undertakes to act diligently to minimize the chances of failures or interruptions





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

that may occur within its organization. Failures caused by the inability or insufficiency of the Subscriber's equipment, or by their lack of knowledge regarding the use of the service, will in no case be attributable to ECD GSE and no compensation for any damage may be demanded from them.

1.9.8.3. Liability for Service Functionality in Subscriber's Infrastructure.

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

1.9.8.4. Liability for computer crimes.

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

1.9.8.5. Warranty Disclaimers.

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

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

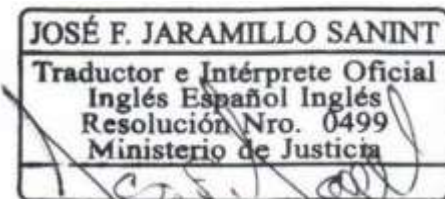
1.9.9. Compensation.

Does not apply


1.9.10. Term and Termination.

1.9.10.1. Commencement of validity of the DPC and PC.

The DPC and PC come 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.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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

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

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

1.9.10.3. Notification and Communication.

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

1.9.10.4. Procedure for Change in the DPC and PC.

1.9.10.4.1. Changes affecting CPD and CP.

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

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

1.9.10.4.2. Circumstances under which the OID must be changed.

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

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

This type of modification will be communicated to the users of the certificates corresponding to the PC or DPC.

1.9.11. Individual Notices and Communication with Participants.


1.9.11.1. Obligations of the ECD GSE.

ECD GSE as an entity providing certification services is obliged according to current regulations and the provisions of the Certification Policies and this DPC to:

- a) Respect the provisions of current regulations, this DPC and the PC Certification Policies.
- b) Publish this CPD and each of the Certification Policies on the GSE website.
- c) Inform ONAC about the modifications to the DPC and the Certification Policies.
- d) Maintain the DPC with its latest version published on the GSE website.
- e) Securely and responsibly protect and guard your private key.
- f) Issue certificates in accordance with the Certification Policies and the standards defined in this DPC.
- g) Generate certificates consistent with the information provided by the applicant or subscriber.
- h) Keep information on digital certificates issued in accordance with current regulations.
- i) Issue certificates whose minimum content is in accordance with the regulations valid for





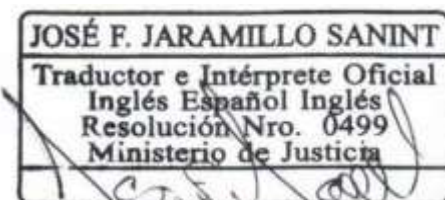
	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

the different types of certificates.


- j) Publish the status of digital certificates issued in an open-access repository.
- k) Do not keep a copy of the private key of the applicant or subscriber.
- l) Revoke digital certificates as provided in the Digital Certificate Revocation Policy.
- m) Update and publish the list of CRL revoked digital certificates with the latest revoked certificates,
- n) Notify the Applicant, Subscriber or Entity of the revocation of the digital certificate within of 24 hours following the revocation of the certificate in accordance with the policy revocation of digital certificates,
- o) Inform subscribers of the proximity of the expiration of their digital certificate,
- p) Have qualified personnel, with the knowledge and experience necessary for the provision of the certification service offered by the ECD GSE.
- q) Provide the applicant on the ECD GSE website with the following information free of charge and free access complying with the parameters and characteristics of the regulations in force without inducing error:
 - The Statement of Certification Practices, its Annexes, the Certificate Policies and all updates to the documents mentioned.
 - Obligations of the subscriber and the way in which the data must be kept.
 - Procedure for requesting the issuance of a certificate.
 - The procedure for revoking your certificate.
 - The conditions and limits of the use of the certificate
- r) Check for themselves or through a different person acting on behalf of and for account, the identity and any other circumstances of the applicants or of data of the certificates, which are relevant for the purposes of the procedure verification prior to shipment,
- s) Inform the Superintendency of Industry and Commerce and the ONAC, in a immediately, the occurrence of any event that compromises or may compromise the provision of the service,
- t) Timely report the modification or update of services included in the scope of accreditation, in the terms established by the procedures, rules and ONAC accreditation service requirements
- u) Update contact information whenever there is a change or modification in the No data provided
- v) Train and warn their users about the security measures they should observe and on the logistics that are required for the use of the mechanisms of the provision of the service,
- w) Ensure the protection, integrity, confidentiality and security of the information provided by the subscriber retaining the documentation supporting the issued certificates
- x) Guarantee the conditions of integrity, availability, confidentiality and security, in accordance with current national and international technical standards and with the specific accreditation criteria established for this purpose by the ONAC.
- y) Provide the services that are accredited on the ECD GSE website.

1.9.11.2. Obligations of the RA.

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





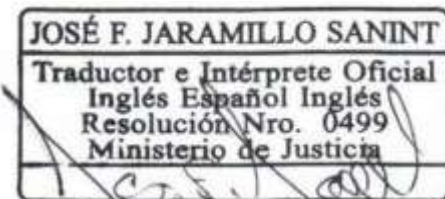
	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

- a) Know and comply with the provisions of this DPC and the Certification Policies corresponding to each type of certificate.
- b) Guard and protect your private key.
- c) Review and/or check the initial validation records of the identity of applicants, Managers or Subscribers of digital certificates.
- d) Verify the accuracy and authenticity of the information provided by the Applicant.
- e) Archive and safeguard the information and/or documentation provided by the applicant or subscriber for the issuance of the digital certificate, during the time established by current legislation.
- f) Respect the provisions of the contracts signed between ECD GSE and the subscriber.
- g) Identify and inform the ECD GSE of the grounds for revocation provided by the applicants on the current digital certificates.


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

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

- a) Use your digital certificate or electronic signature certificate according to the terms of this DPC.
- b) Verify within the next business day that the digital certificate information is correct. If inconsistencies are found, notify the ECD.
- c) Refrain from: lending, assigning, writing, publishing the password for use of your digital certificate and take all necessary, reasonable and timely measures to prevent it from being used by third parties.
- d) Not transfer, share or lend the cryptographic device to third parties.
- e) Provide all the information required in the application form or using the channels, means or mechanisms provided by GSE for the application of digital certificates to facilitate their timely and full identification.
- f) Request the revocation of the digital certificate before the change of name and/or surname.
- g) Request the revocation of the digital certificate when the Subscriber has changed their nationality.
- h) Comply with what is accepted and/or signed in the terms and conditions document.
- i) Provide the required information accurately and truthfully.
- j) Report during the term of the digital certificate any changes in the data initially supplied for the issuance of the certificate,
- k) Responsibly guard and protect your private key.
- l) Use the certificate in accordance with the PCs established in this DPC to each of the types of certificate,
- m) Request as a subscriber and/or responsible immediately the revocation of their digital certificate when it becomes aware that there is a cause defined in numeral Circumstances for the revocation of a certificate of this DPC.
- n) Do not use the private key or the digital certificate once its validity has expired or it has been revoked.
- o) Inform trusted third parties of the need to verify the validity of the digital certificates on which it is making use at any given time,
- p) Inform the third party in good faith of the status of a revoked digital certificate for which





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

the list of revoked CRL certificates is available, published periodically by ECD GSE.

- q) Not use your digital certification in a way that contravenes the law or causes bad reputation for the ECD.
- r) Do not make any statement related to your digital certification in the ECD GSE that may be considered misleading or unauthorized, as provided by this DPC and PC.
- s) Once the digital certification service has expired or been revoked, the subscriber must immediately stop using it in all advertising material that contains any reference to the service.
- t) The subscriber, when referring to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, must inform that it complies with the requirements specified in the PCs of this DPC, indicating the version.
- u) The subscriber may use the conformity marks and information related to the digital certification service provided by ECD GSE in the media, such as documents, brochures or advertising, as long as it complies with the requirements of the previous paragraph.

On the other hand, you have the following rights:

- a) Receive the digital certificate at the times established in the DPC.
- b) Request information regarding applications in process.
- c) Request revocation of the digital certificate by providing the necessary documentation.
- d) Receive the digital certificate in accordance with the scope granted by ONAC to GSE.

1.9.11.4. Obligations of Third Parties in Good Faith.

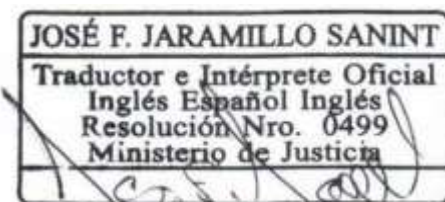
Bona fide Third Parties in their capacity as relying party on the digital certificates issued by ECD GSE are under an obligation to:

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


1.9.11.5. Obligations of the Entity (Client).

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

- a) Request from the RA of the ECD GSE the suspension/revocation of the digital certificate when said linkage ceases or is modified.
- b) All those obligations linked to the head of the digital certification service.
- c) When referring to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, the entity must inform that it complies with the requirements specified in the PCs related in this DPC.





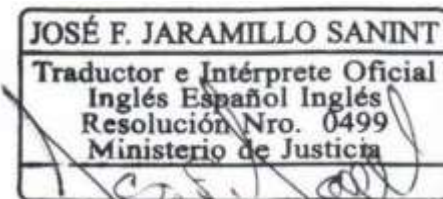
	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

d) The entity may use the conformity marks and the information related to the digital certification service provided by ECD GSE in media, such as documents, brochures or advertising, as long as it complies with the requirements of the previous paragraph.


1.9.11.6. Obligations of Other ECD Participants.

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

- a) Review the consistency of the CPD with current regulations.
- b) Approve and decide on the changes to be made to the certification services, due to regulatory decisions or requests from subscribers or managers.
- c) Approve the notification of any change to subscribers and/or managers by analyzing its legal, technical or commercial impact.
- d) Review and take action on any comments made by subscribers or managers when a change to the certification service is made.
- e) Report the action plans to ONAC on any changes that have an impact on the PKI infrastructure and that affect digital certification services, in accordance with current RAC-3.0-01.
- f) Authorize the changes or modifications required on the DPC.
- g) Authorize the publication of the DPC on the ECD GSE website.
- h) Approve changes or modifications to the Security Policies of the ECD GSE.
- i) Ensure the integrity and availability of the information published on the website of the ECD GSE.
- j) Ensure the existence of controls over the technological infrastructure of the ECD GSE.
- k) Request the revocation of a digital certificate if it had the knowledge or suspicion of the commitment of the private key of the subscriber, entity or any other fact that tends the improper use of the private key of the subscriber, entity or the ECD itself.
- l) Know and take appropriate actions when security incidents occur,
- m) Conduct a review of the DPC with a maximum annual frequency to verify that the lengths of the keys and periods of the certificates that are being used are
- n) Review, approve and authorize changes to certification services accredited by the competent body
- o) Review, approve and authorize the ownership and use of symbols, certificates and any other mechanism that requires ECD GSE to indicate that the certification service digital is accredited.
- p) Ensure that the accreditation conditions granted by the competent body are maintained.
- q) Ensure the proper use in documents or in any other advertising than the 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.
- r) Ensure that its critical suppliers and reciprocal ECD, if any, are kept informed of the obligation to comply with the requirements of the CEA, in the corresponding numerals.
- s) The Integrated Management System will execute corrective action plans and improvement actions to respond to any risk that compromises the impartiality of the ECD, whether it derives from the actions of any person, body, organization, activities, its relationships or the relationships





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

of its personnel 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, delivering to the Management Committee the mechanism that eliminates or minimizes such risk, on an ongoing basis.

t) Ensure that all ECD staff and committees (whether internal or external) that may have an influence on certification activities act with impartiality and non-discrimination, especially those that arise from commercial, financial or other pressures that compromise their impartiality.

u) Document and demonstrate the commitment to impartiality and non-discrimination.

v) Ensure that the administrative, management, technical personnel of the PKI, of the ECD associated with the consulting activities, maintain complete independence and autonomy with respect to the personnel of the review process and decision making on the certification of this ECD.

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

1.9.12. Amendments.

Digital certificates issued by ECD GSE cannot be modified, i.e. no amendments apply. 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 reported by ECD GSE or according to the conditions defined at the contractual level.

1.9.12.1. Circumstances for modification of a certificate.

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

1.9.12.2. Who can request an amendment.

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

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

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

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

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

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

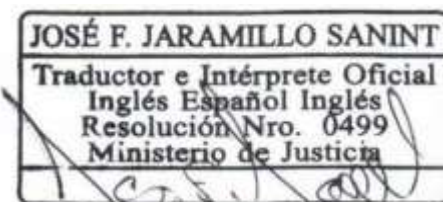
It does not apply since the digital certificates issued by ECD GSE cannot be modified.

1.9.12.6. Publication of the certificate modified by the ECD.


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

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

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





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.9.13. Dispute Resolution Procedures.

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

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

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

At the end of this period, the difference(s) persists, the Parties will be free to go to the ordinary Colombian justice to assert their rights or demands, which will be subject to the current regulations on the matter, the costs caused 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.

1.9.14. Governing Law.

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

- a. Law 527 of 1999, which defines and regulates the access and use of data messages, electronic commerce and digital signatures, and establishes certification bodies and other provisions.
- b. Decree 333 of 2014, which regulates article 160 of Decree-Law 019 of 2012 regarding the characteristics and requirements of certification entities, and what is related to digital certificates.
- c. Chapters 47 and 48 of title 2 of part 2 of book 2 of the Single Decree of the Commerce, Industry and Tourism Sector - DURSCIT.

1.9.15. Compliance with Applicable Law.

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

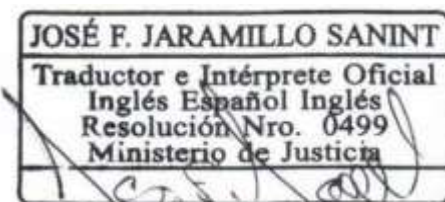
1.9.16. Miscellaneous.

Does not apply


1.9.17. Other Provisions.

1.9.17.1. Assignment.

Not applicable





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

1.9.17.2. Severability.

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

1. 10. CHANGES AFFECTING DIGITAL CERTIFICATION SERVICES.

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

- a. Regulatory changes in ECD legislation.
- b. At the request of the ONAC.
- c. At the request of the Superintendency of Industry and Commerce of Colombia - SIC.
- d. Technological changes affecting digital certification services.
- e. At the request of subscribers or managers, subject to approval by the Management Committee.

For which the Subscriber or person in charge must send a communication addressed to the Management Committee of the ECD GSE about the requested change, the acceptance or rejection will be under the discretion of the Management Committee.

1.10.1. Procedure for Changes.

1.10.1.1. Changes that do not require notification.

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

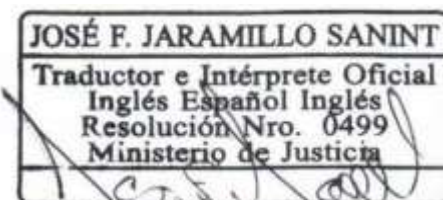
1.10.1.2. Changes requiring notification

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


1.10.1.3. Mechanism and reporting period

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

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





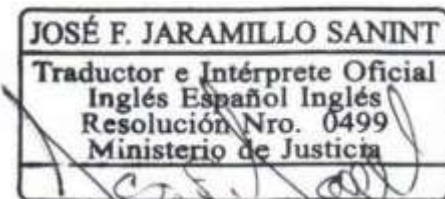
	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

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


1.11. DESCRIPTION OF PRODUCTS AND SERVICES

TYPE OF DIGITAL CERTIFICATE	
Company Membership	It guarantees the identity of the natural person holding the certificate, as well as its link to a certain legal entity by virtue of the position held therein. This certificate will not by itself grant greater powers to its holder than those it possesses for the performance of its usual activity.
Company Representation	It is issued in favor of a natural person representing a certain legal entity. The certificate holder identifies himself not only as a natural person belonging to a company, but also adds his qualification as its legal representative.
Staff case	It guarantees the identity of the natural person holding the certificate, as well as their link to a Public Administration by virtue of their rank as a public official. This certificate will not by itself grant greater powers to its holder than those it possesses for the performance of its usual activity.

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 January 19, 2024.

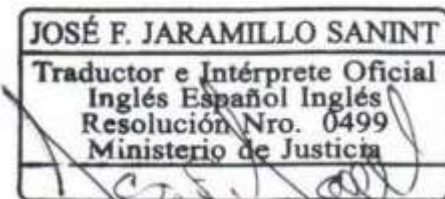





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

TYPE OF DIGITAL CERTIFICATE	OBJECT
Graduate Professional	It guarantees the identity of the natural person holding the certificate, as well as their status as a certified professional. This certificate will not by itself grant greater powers to its holder than those he possesses for the performance of his usual activity in the field of his profession.
Individual	It guarantees only the identity of the natural person.
Electronic Invoice for natural person	Exclusive certificate for electronic invoicing in response to the need of natural persons seeking the security of the certificate for the issuance of electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment supports, adjustment notes of the electronic payroll payment support document and other documents resulting from the processes of the unattended platforms of the technological providers approved by the Dian, the free billing system of the Dian and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Electronic Invoice for legal entity	Exclusive certificate for electronic invoicing in response to the need of companies seeking the security of the certificate for the issuance of electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment supports, adjustment notes of the electronic payroll payment support document and other documents resulting from the processes of the unattended platforms of the technological providers approved by the Dian, the free billing system of the Dian and the RADIAN platform, in compliance with the technical annexes issued by said entity.
Legal Entity	Carrying out business procedures by an application running on a machine in automatic and unattended signature processes on behalf of a legal person under public or private law that require guaranteeing the authenticity and integrity of the data sent or stored digitally together with the establishment of secure communication channels between customers, and which will be represented by a natural person (Responsible), holder of the certificate issued under this policy and called Responsible.
Generation of Certified Electronic Signatures	Exclusive certificate for the generation of certified electronic signatures.

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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

TYPE OF DIGITAL CERTIFICATE	OBJECT
Email service	The certified email service allows to ensure the sending, reception and verification of electronic communications, ensuring at all times the characteristics of fidelity, authorship, traceability and non-repudiation of the same.
Chronological Stamping Service (TSA)	Data message that links to another data message with a specific moment or period of time, which allows to establish with a proof that these data existed at that moment or period of time and that they did not undergo any modification from the moment in which the stamping was made.
Archiving and Preservation Service of Electronic Transferable Documents and Data Messaging	Service consists of a secure, encrypted storage space that you access with credentials or a digital certificate. The documentation stored on this platform will have probative value as long as it is digitally signed.

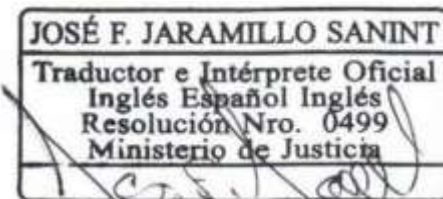
Note: For the verification of the generation process of each service, refer to the corresponding procedures

1.12. FEES.


1.12.1. Certificate issuance or renewal fees.

Single Product	Delivery time	Period	Price without VAT	VAT	Total
Natural Person Certificate	Normal	1	\$191,597	\$36,403	\$228,000
Natural Person Certificate	Normal	2	\$277,310	\$52,689	\$329,999
Certificate Belonging to company	Normal	1	\$191,597	\$36,403	\$228,000
Certificate Belonging to company	Normal	2	\$277,310	\$52,689	\$329,999
Professional Certificate Graduate	Normal	1	\$191,597	\$36,403	\$228,000
Professional Certificate Graduate	Normal	2	\$277,310	\$52,689	\$329,999
Certified Legal Representative	Normal	1	\$191,597	\$36,403	\$228,000
Certified Legal Representative	Normal	2	\$277,310	\$52,689	\$329,999
Public Function Certificate	Normal	1	\$191,597	\$36,403	\$228,000
Public Function Certificate	Normal	2	\$277,310	\$43,907	\$274,999
Certificate of legal entity	Normal	1	\$504,202	\$95,798	\$ 600.000

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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

Single Product	Delivery time	Period	Price without VAT	VAT	Total
CERTIFICATE OF LEGAL ENTITY	Normal	2	\$857,143	\$162,857	\$1,020,000

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

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

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

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

1.12.2. Certificate access fees.

Access to the status check of the certificates issued is free of charge and therefore there is no fee.

1.12.3. Revocation Fees or Access to Status Information.

The request for revocation of a certificate is free of charge. Access to the status information of the certificates issued is free of charge and therefore no fee applies.

1.12.4. Fees for other services.

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

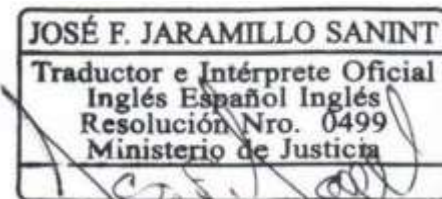
1.12.5. Return Policy.

The Return Policy published on the GSE website (<https://gse.com.co/Nosotros/politicas>) must be taken into account.


1.13. IMPARTIALITY AND NON-DISCRIMINATION

ECD GSE, at the head of the Management Committee and its collaborators, are committed to safeguarding impartiality and independence in certification processes and 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 January 19, 2024.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

digital, in order to prevent conflicts of interest within the company, with relevant and external stakeholders, acting within the legal framework of Law 527 of 1999, Decrees 019 of 2012, 333 of 2014 and 1471 of 2014, and the specific accreditation criteria of the National Accreditation Body of Colombia (ONAC), so the following compliance mechanisms are established:

- The Management Committee and the collaborators of GSE declare that they do not participate directly or indirectly in services or activities, which may jeopardize free competition, responsibility, transparency.
- Employees will use the survey of preventive and corrective actions to respond to any risk that compromises the impartiality of the company.
- Collaborators who are part of the accredited digital certification services may not provide consulting services, nor involve the development team to provide technical support service to the subscriber or customer.
- GSE is responsible for impartiality in the conduct of its activities and does not allow commercial, financial or other pressures to compromise its impartiality.
- GSE may decline acceptance of an application or maintenance of a contract for certification where there are substantiated 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 acceptance of an application or maintenance of a contract for certification where there are substantiated, demonstrated or improper reasons on the part of the applicant and/or subscriber.
- GSE offers access to a digital certification service that does not depend on the size of the applicant or subscriber or the membership of any association or group, nor should it depend on the number of certifications already issued.

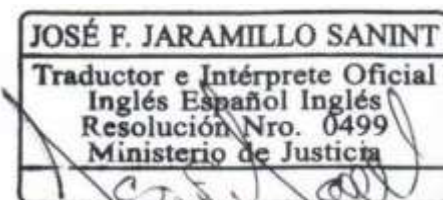
Note: Any case that puts at risk the impartiality of the ECD GSE as ECD or its personnel, agency or organization, will be brought to the attention of the Integrated Management System Process.

In accordance with the provisions of the Fairness and Non-Discrimination Policy of the GSE ECD, which can be found at the following link: <https://gse.com.co/politicas>.


1.14. CERTIFICATION POLICIES.

The interrelationship between this DPC and the Certification Policies of the different certificates is fundamental. And this, to the extent that:

- **The CPD** is the set of practices adopted by ECD GSE for the provision of services accredited by ONAC and contains detailed information on its security system, support, administration and issuance of certificates, in addition to the Trust relationship between applicant, subscriber, responsible party, entity, good faith third party, and the ECD.





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

- **Certification Policies** constitute the set of rules that define the characteristics of the different ECD GSE certificates and the applicability of these certificates for specific applications that require the same security requirements and usage forms.

In summary, the policy defines "**what**" requirements are necessary for the issuance of different ECD GSE certificates, while the CPS 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	1.3.6.1.4.1.31136.1.4.15
PC Location	rooseDs://ase.com.co/documentos/calidad/politicas/Politica certificate p now VI5 diaital certificates.DDF

- Chronological Stamping Service Certificate Policies:

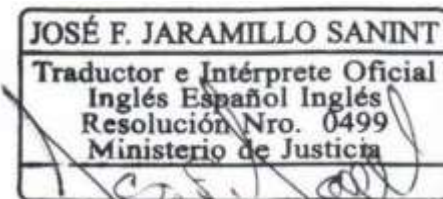
OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.2.14
PC Location	rooseDs://ase.com.co/documentos/calidad/Doliticlas/Politica of Certificate p ara Cronoloaico Stamping Service V14.pdf

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


OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.3.14
PC Location	rooseDs://ase.com.co/documentos/calidad/Doliticlas/Politica of Certificate d ara Trusted Data Archiving Service V14.odf

- Certificate Policies for Certified Email Service:

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.5.14
---------------------------------------	--------------------------





	STATEMENT OF PRACTICES OF CERTIFICATION	Código	POP-DT-1
		Versión	16
		Implementación	10/24/2023
		Clasificación de la información	Public

PC Location	rooseDs://ase.com.co/documentos/calidad/Doliticas/Politica Certificado oara V14.odf Certified Email Service
• Certified Electronic Signature Generation Policies:	
OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.6.5
PC Location	rooseDs://ase.com.co/documentos/calidad/Policies/Generation Policy of Certified Electronic Signatures V5.pdf

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

This translation has been done by JOSE F. JARAMILLO SANINT, official translator and Interpreter for the English-Spanish-English languages according to resolution No. 0499 Issued on April 02, 2004 by the Ministry of the Interior and Justice, Republic of Colombia. This document is an accurate translation of the original January 19, 2024.

