Document Title	**Certification Practices Statement**
Version	14
Working Group	Management Committee
Document status	Final
Date of issue	01/11/2016
Effective date	23/09/2022
OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.1.13
Location of the CPS	https://gse.com.co/documentos/calidad/DPC/Certification_Practice_Statement_V14.pdf
Prepared by	Chief Operating Officer
Reviewed	Integrated Management System
Approved	Management Committee

Change Control

Version	Date	Change/Modification
1	01-11-2016	Initial document
2	04-10-2017	• Update DCE contact details and Logo • Updating of Enrolling Entities • Update contact details Certification Service Providers • Information regarding the GSE General Manager. GSE TSA data update.
3	03-04-2018	Update information and adjustments in relation to CEA-4.1-10 according to the review of the requirements matrices.
4	27-11-2018	Changed from V3 to V4 on 11/27/2018 Updated table of contents, information and adjustments regarding new charges, fees, website access routes, correction of subordinate, included the phrase established and tested, expanded 8.7.4 by naming the technological mechanisms used for data protection, listed all certification policies, change of terms and updating of the legal representative.
5	12-04-2019	The number of the EE was eliminated and it was clarified that, for the use of the centralized signature certificate, it is necessary to acquire a technological platform with additional costs. The clarification is made in the paragraph 1.6.2 of the RA requirements and restrictions and of the Criteria and methods of evaluation of the Applications. The roles of the AR were updated
6	07/06/2019	Clarification of the scope of accreditation under the CPS 1.1 Summary 4.1 Request for the certificate, the procedure for accessing the service is clarified. 4.1.1 Clarification of non-discrimination in accessing the service. 8.9.3 Clarification of subscriber's or responsible party's rights
7	31/03/2020	The CPS is adjusted to the changes generated by the new platforms, the objective and scope items are added, the price list is adjusted, the links are modified so that they point to the new routes, the legal representative is changed, and it is related in a more detailed way to the new platforms. services accredited by ONAC.
8	14/08/2020	Everything related to the digital signature generation service is eliminated, another condition is added in section 5.2.2 Authentication of the identity of an entity for the renewal of digital signature certificates and the services used for the validation of digital signatures are mentioned.

Version	Date	Change/Modification
		identity.
9	12/02/2021	The link to consult online the Certificate of Existence is included. and Legal Representation for DCE and the current CA (Paynet SAS). Detailed information on the current (Paynet SAS) and historical (Indenova) CA was included in accordance with item 1 of section 10.7 of CEA 4.1-10. The datacenter information was modified in accordance with the ONAC accreditation certificate. The paragraph on the renewal of the digital certificates has been eliminated from 5.2.2 and 5.2.3. The following items were updated: • 6.4.2 Approval or rejection of certificate applications • 6.4.3 Deadline for processing certificate applications • 7.10.1 Trust roles • 8.1.4 Delivery of the DCE public key to third party acceptors Links have been updated to point to the new routes.
10	16/07/2021	The numbers have been updated: 3.6.1 Certification Authority (CA), datacenter provider data. 4.1 Repositories Section 6.5.6 has been updated. 6.5.7 Deadline for processing certificate applications 6.8.2 Use of the private key and certificate by bona fide third parties 6.12 Revocation and suspension of certificates 6.12.3Revocation request procedure 6.13.1Description of certificate content Authority Subordinate 01 GSE 6.13.1.8 Algorithm Object Identifiers (OID) 6.14.1.3 CRL Availability 6.14.1.7 OCSP availability 6.14.3Optional Features 7.10.1Trust roles 8.1.4 Delivery of the DCE public key to third-party acceptors 8.1.5 Size of keys 8.1.6 Parameters for public key generation and quality check 8.2.4 Private key backup 8.2.5 Private key file

Version	Date	Change/Modification
		8.2.6 Private key transfer from cryptographic module 8.2.7 Storage of private keys in a cryptographic module 8.5.3 Actions to be taken in the event of a security event or incident Information DESCRIPTION OF PRODUCTS AND SERVICES, Archiving, Recording, Conservation, Custody and Annotation Services for Electronic Documents 11.7.1Personal Data Processing Policy 11.3 Fairness and Non-Discrimination 14. ANNEX 1 DPC MATRIX MATRIX TECHNICAL PROFILE DIGITAL CERTIFICATES 15. ANNEX 2 TERMS AND CONDITIONS OID and consultation links are updated: • Certification Practices Statement • Certificate Policies for Digital Certificates • Certificate Policies for Time Stamping Service • Certificate Policies for Archiving, Recording, Retention, Custody and Annotation of Electronic Transferable Documents and Data Messages. Certificate Policies for Certified Email Service
11	5/10/2021	• The numbers have been updated to include electronic signatures: 6.1 Certificate application 6.5 Initial identity validation 6.5.1 Method of demonstrating possession of private key 10 Description of Products and Services 11.1.1 Fees for issuance or renewal of certificates 11.9.3 Obligations of the Subscriber and/or Responsible Party. • The following items referring to electronic signatures were included: 5.1.1.1.1.1 Electronic Signature 5.1.1.2.2 GSE DCE Subscriber Certificates (Matrix Technical Profile of e-Signature Certificates) 13 Certification Policies 16 Annex 3 CPS matrix technical profile electronic signature

Version	Date	Change/Modification
		certificates • An explanatory note on OCSP validation was included in items 4.1, 4.3, 6.12.9, 6.12.10, 6.14.3. • Section 6.12.3 Revocation request procedure was updated by adding a new online revocation channel. • Section 8.3.2 was updated to clarify the validation period for root and subordinate keys of the RSA and ECDSA algorithms. OID and query links are updated
12	27/10/2021	• Modified section 6.5 of Identity Validation. • Updated the OIDs and the Digital Certificates PC link. The OID and CPS link have been updated with this new version.
13	31/05/2022	According to the new version of the CEA, adjustments were made to the following items: • 3.1 Summary: 4.1-10 was eliminated, leaving only CEA. • Petition, complaint, claim and requests: The term appeal was eliminated. • 3.6 PKI Participants: Indenova is eliminated as a CA. • 5.1.1.1 - 5.1.1.2 Name Types: Indenova's root and subordinate certificates are eliminated and those related to elliptic curve are included. • 6.5 Initial Validation of Identity: A final paragraph was included on confrontational consumption of services. • 6.13.1 Description of certificate contents: The alternate subject name field has been included. • 6.13.1.7 3 key purposes were eliminated. • 7.10.1 Trust Roles: the roles of RA Agents, RA Administrator and RA Auditor have been modified: • 7.16 Termination of a DCE: Modified as required by the new CEA. • 9.2 Auditor identity/qualifications: The assurance requirements were modified. • 10. Description of products and services: The centralized signature certificate was eliminated, the name of the Archive service was modified and the electronic signature generation service was modified in accordance with the accreditation certificate. • 11.4. Exemption for liability limits was modified. • 11.9.6 Obligation of other participants: Item r) was modified by eliminating 4.1-10 leaving only CEA. • 15. The name of the annex on terms and conditions was modified. • 16. This item of the technical annex of the electronic

		signature certificate was included. • Updated the OIDs and the Digital Certificates PC link. • The OID and CPS link have been updated with this new version. • The quality code was included in the document header.
14	23/09/2022	• 3.1 Summary: The Durscit chapters were included. • The DCE address was modified in items 3.1, 3.2, 3.6.2 and 3.7.1. • The address of Paynet SAS was modified in items 3.6.1 and 3.6.7.2. • Item 3.6.4 has been modified by changing responsible for bona fide third parties. • Item 3.6.4.1 Precautions to be observed by third parties was included. • Section 6.4.1 Performance of identification and authentication functions was amended. • Section 6.5.1 Method for demonstrating possession of the private key has been modified to provide clarity in the event that the applicants generate the key pair in their own infrastructure. • Section 6.5.5 Criteria for interoperability has been modified. • Section 6.12.7 CRL update frequency was modified according to the availability percentage established in the new CEA. • RFC 2560 was modified by RFC 6960 in items 6.12.10 On-line revocation verification requirements, 6.14.1.4 OCSP profile and 6.14.1.5 Version number. • Section 7.7 was modified. Storage system making it clear that the servers are in cloud environments. • Section 7.4 was modified. Exposure to water clarifying that it refers to the PKI datacenter. • Number 7.16 was modified. Cessation of a DCE including a paragraph on the security plan for the cessation of activities. • Number 11.4 Limits of liability was amended to include 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. • Section 11.9.1 Obligations of the DCE GSE was modified, including items o) to y) • The numerals 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. • The OID and the link to the Digital Certificates PC were updated. • Updated the OID and CPD link with this new version.

Tabla de contenido

1. OBJECTIVE

To make known to the general public the guidelines established by Gestión de Seguridad Electrónica to provide services as a Digital Certification Entity, 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.

2. SCOPE

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

3. INTRODUCTION

3.1 Summary

The Declaration of Certification Practices (CPS) - Global Certification Authority Root GSE (hereinafter DPC) is a document prepared by **Gestión de Seguridad Electrónica S.A. (hereinafter GSE) acting as a Digital Certification Entity. (hereinafter GSE)** acting as a Digital Certification Entity, contains the rules, statements on policies and procedures that the **Digital Certification Entity (hereinafter DCE GSE)** as a **digital Certification Service Provider (CSP)** applies as guidelines 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 CPS is in accordance with the following guidelines:

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

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

GESTIÓN DE SEGURIDAD ELECTRÓNICA SA DATA:

Company name: GESTIÓN DE SEGURIDAD ELECTRÓNICA SA.

Acronym:	GSE S.A.
Identification Number Tax:	900.204.272 - 8
Mercantile Registry No:	01779392 of February 28, 2008
Certificate of Existence and Legal Representative:	https://gse.com.co/documentos/marco-regulatory/Certificate-Of-Existence-and-Representative-Legal-GSE.pdf
Status of the commercial registry:	Active
Social address and correspondence:	77th Street No. 7 - 44 Office 701
City / Country:	Bogotá D.C., Colombia
Phone:	+57 (1) 4050082
Fax:	+57 (1) 4050082
E-mail:	info@gse.com.co
Website:	www.gse.com.co

3.2 Petitions, Complaints, Grievances, Claims and Requests

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

Phone:	+57 (1) 4050082
E-mail:	pqrs@gse.com.co
Address:	77th Street No. 7 - 44 Office 701
Website:	www.gse.com.co
Responsible:	Integrated Management System

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

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

3.3 Name of document and identification

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

GSE is a Registered Private Enterprise with the international organization IANA (Internet Assigned Numbers Authority), with the private code No 31136 under the branch 1.3.6.1.4.1

(iso.org.dod.internet.private.enterprise). The above information can be consulted at the URL, by searching for the code 31136 http://www.iana.org/assignments/enterprise-numbers

The OID hierarchy was established by DCE GSE from the root 1.3.6.1.1.4.1.31136 defined by IANA and conforms to the following parameters:

HIERARCHY OID	DESCRIPTION	NAME
1	ISO format	Does not vary
3	Organization	Does not vary
6	Public	Does not vary
1	Internet	Does not vary
4.1 (31136)	Organization identification	It 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 its group
13	Document version	It is modified according to each version of the document

In accordance with this hierarchy, this CPS has been identified with the OID:
1.3.6.1.4.1.31136.1.1.13

3.4 Legal Framework

The execution, interpretation, modification or validity of this CPS and its corresponding annexes shall be governed by the provisions of the Colombian legislation in force.

3.4.1 Dispute Resolution Mechanism

I If for any reason any dispute arises between the Parties (subscriber/responsible party and DCE GSE) on the occasion of:

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

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

At the end of said period the dispute(s) persists, the Parties shall be free to resort to the Colombian ordinary justice to enforce their rights or demands, which shall be subject to the regulations in force on the matter, the costs caused on occasion of the summons shall be

totally at the expense of the losing Party.

Translated with www.DeepL.com/Translator (free version)

3.5 Definitions and acronyms

3.5.1 Definitions

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

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

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

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

Reliable data archiving: This is the service that GSE offers its clients through a technological platform. In essence, it consists of a secure and encrypted storage space that can be accessed with credentials or a digital certificate. The documentation stored in this platform will have probative value as long as it is digitally signed.

Digital certificate: A document signed electronically by a certification service provider that links signature verification data to a signatory and confirms the signatory's identity. This is the definition of Law 527/1999, which in this document is extended to cases in which the linking of signature verification data is made to a computer component.

Specific Accreditation Criteria (CEA): Requirements that must be met to obtain the Accreditation as Digital Certification Entity - ECD, before the National Accreditation Body of Colombia - ONAC; i.e. to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 019 of 2012, Chapters 47 and 48 of Title 2 of Part 2 of Book 2 of the Single Decree of the Commerce, Industry and Tourism Sector - DURSCIT and the regulations that modify or complement them.

Personal Identification Number (PIN): Sequence of characters that allow access to the digital certificate.

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

Certified e-mail: Service that ensures the sending, receipt and verification of electronic communications, ensuring at all times the characteristics of fidelity, authorship, traceability and non-repudiation of the same.

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

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

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

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

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

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

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

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

Trust hierarchy: A set of certification authorities that maintain trust relationships whereby a higher-level CCD guarantees the trustworthiness of one or more lower-level CCDs.
Certificate Revocation List (CRL): List of revoked certificates that have not expired.

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

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

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

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

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

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

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

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

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

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

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

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

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

3.5.2 Acronyms

CA: Certification Authority
CA Sub: Subordinate Certification Authority
CP: Certificate Policy
CPS: Certificate Practice Statement (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 World Wide Web (WWW). HTTP defines the syntax and semantics used by the software elements of the web architecture (clients, servers, proxies) to communicate. It is a

transaction-oriented protocol and follows the request-response scheme between a client and a server.
HTTPS: Hypertext Transfer Protocol Secure, better known by its acronym HTTPS, is a network protocol based on the HTTP protocol, intended for the secure transfer of hypertext data, i.e. it is the secure version of HTTP.
HSM: Hardware Security Module (Hardware Security Module)
IEC: International Electrotechnical Commission
IETF: Internet Engineering Task Force (Internet Standardization Body)
IP: Internet Protocol
ISO: International Organization for Standardization LDAP: Lightweight Directory Access Protocol OCSP: Online Certificate Status Protocol.
OID: Object identifier (Unique Object Identifier)
PIN: Personal Identification Number
PUK: Personal Unlocking Key
PKCS: Public Key Cryptography Standards. PKI standards developed by RSA Laboratories and accepted internationally.
PKI: Public Key Infrastructure
PKIX: Public Key Infrastructure (X.509)
RA: Registration Authority
RFC: Request For Comments (Standard issued by the IETF)
URL: Uniform Resource Locator
VA: Validation Authority

3.5.3 Standards and Standardization Bodies

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

3.6 Participating PKIs

3.6.1 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.

GSE has as its current provider of PKI infrastructure services - CA:

Business name:	PAYNET S.A.S
Initials:	PAYNET
Tax identification number:	901.043.004-2
Commercial Registry No:	02766647 of January 13, 2017
Certificate of Existence and Legal Representative:	https://www.paynet.com.co/doc/Certificado_de_Existencia_y_Representante_Legal_Paynet.pdf
Status of the commercial register:	Active
Company address and correspondence:	Cl 77 No. 7 - 14 Of 707
City Country:	Bogota DC, Colombia
Phone:	+57 (1) 4050082
Fax:	+57 (1) 4050082
Email:	representante.legal@paynet.com.co
Web page:	www.paynet.com.co

The provider has two datacenters (one main and one alternate), the main datacenter with UNE - EPM TELECOMUNICACIONES S.A. is located on the Medellin highway kilometer 6 + 200 meters south side, entrance by Festo kilometer 0 + 360 meters, Parque Industrial Siberia Real in Tenjo Cundinamarca, Colombia and the alternate datacenter with IFX Networks Colombia S.A.S. is located at Avenida el Dorado # 68c - 61 office 508 in Bogotá D.C., Colombia.

3.6.2 Registration Authority (RA)

It is the area of GSE in charge of certifying the validity of the information provided by the applicant of a digital certification service, through the verification of the entity of the subscriber or responsible for the digital certification services, in the RA it is decided on the issuance or activation of the digital certification service. To this end, it has defined the criteria and methods for evaluating applications.

Under this CPS, the RA is part of the DCE itself and may act as a Subordinate of DCE GSE.

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

DCE GSE has as registration authority RA:

Company name:	GESTIÓN DE SEGURIDAD ELECTRÓNICA SA.
Acronym:	GSE S.A.
Identification Number Tax:	900.204.272 - 8
Mercantile Registry No:	01779392 of February 28, 2008
Certificate of Existence and Legal Representative:	https://gse.com.co/documentos/marco-regulatory/Certificate-Of-Existence-and-Representative-Legal-GSE.pdf

Status of the commercial registry:	Active
Social address and correspondence:	77th Street No. 7 - 44 Office 701
City / Country:	Bogotá D.C., Colombia
Phone:	+57 (1) 4050082
Fax:	+57 (1) 4050082
E-mail:	info@gse.com.co
Website:	www.gse.com.co

3.6.3 Subscriber and/or responsible

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

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

3.6.4 Bona fide third party

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

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

3.6.4.1 Precautions to be observed by third parties

a) Verify the scope of the certificate in the associated certification policy.
b) Consult the regulations associated with digital certification services.
c) Verify the accreditation status of the DCE 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.
h) Translated with www.DeepL.com/Translator (free version)

3.6.5 Applicant

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

3.6.6 Entity to which the subscriber or responsible person is linked

If applicable, the legal person or organization to which the subscriber or responsible person is closely related by means of the linkage accredited in the digital certification service.

3.6.7 Other participants

3.6.7.1 Management Committee

The Management Committee is an internal body of DCE GSE, made up of the General Manager and directors, who are responsible for approving the CPS as the initial document, as well as authorizing any changes or modifications required to the approved CPS and authorizing its publication.

3.6.7.2 Service providers

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

For the purposes of this CPS, the company PAYNET SAS, hereinafter Paynet SAS, will be the provider and administrator of the DCE GSE infrastructure.

GSE has as its PKI infrastructure service provider entity:

Business name:	PAYNET S.A.S
Initials:	PAYNET
Tax identification number:	901.043.004-2
Commercial Registry No:	02766647 of January 13, 2017
Certificate of Existence and Legal Representative:	https://www.paynet.com.co/doc/Certificado_de_Existencia_y_Representante_Legal_Paynet.pdf
Status of the commercial register:	Active
Company address and correspondence:	Cl 77 No. 7 - 44 Of 707
City Country:	Bogota DC, Colombia
Phone:	+57 (1) 4050082
Fax:	+57 (1) 4050082
Email:	representante.legal@paynet.com.co
Web page:	www.paynet.com.co

The PKI Infrastructure service provided by Paynet SAS has a service provision contract that provides for termination conditioned to DCE GSE having implemented or contracted an infrastructure or technological service that allows it to continue providing its services without any prejudice to subscribers or entities.

DCE GSE and Paynet SAS comply with the legal, technical and infrastructure requirements in accordance with the Specific Accreditation Criteria established by ONAC.

The contracting of Paynet SAS does not exempt DCE GSE from complying with the duty to allow and facilitate ONAC to carry out audits.

The DCE GSE has established a supplier evaluation to ensure the PKI supplier's compliance with the requirements and to monitor the supplier's performance.

3.6.7.3 Reciprocal Digital Certification Entities

In accordance with the provisions of Article 43 of Law 527 of 1999, certificates of digital signatures issued by foreign certification entities may be recognized under the same terms and conditions required by law for the issuance of certificates by domestic certification entities, provided 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.

DCE GSE does not currently have any reciprocity agreements in force.

3.7 DPC and PC administration

3.7.1 Document Management Organization

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

3.7.2 Contact person:

Name:	Alvaro de Borja Carreras Amoros
Post:	Legal representative
Direction:	77th Street No. 7 - 44 Office 701
Address:	Bogotá DC, Colombia.
Phone:	+57 (1) 4050082
Email:	info@gse.com.co

3.7.3 Person or area that determines the adequacy of the Policies to the CPS

Responsible area:	Director of operations
Direction:	77th Street No. 7 - 44 Office 701
Address:	Bogotá DC, Colombia.
Phone:	+57 (1) 4050082
Email:	info@gse.com.co

3.7.4 CPS approval procedures

The Management Committee is the internal GSE body in charge of reviewing, approving and authorizing the publication of the CPS on the http://www.gse.com.co website.

3.8 Changes affecting digital certification services

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

a. Due to regulatory changes in legislation for ECD.
b. At the request of ONAC.
c. At the request of the Superintendence of Industry and Commerce of Colombia - SIC.
d. Technological changes affecting digital certification services.
e. At the request of subscribers or responsible parties, with prior approval of the Management Committee.

For which the Subscriber or responsible party must send a communication addressed to the DCE GSE Management Committee regarding the requested change, acceptance or rejection will be under the discretion of the Management Committee.

3.8.1 Procedure for changes

3.8.1.1 Changes that do not require notification

a. When the changes made do not affect the operation of the services provided to current subscribers or responsible parties, it will be the task of the Management Committee to define the level of impact of the changes.
b. When the changes involve typographical or editorial corrections to the content of the services provided.

3.8.1.2 Changes requiring notification

a. When the changes made affect the operation of the services provided to current subscribers or responsible parties, 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 DCE GSE.

3.8.2 Notification mechanism and period

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

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

The subscribers or responsible for the digital certification services affected by the changes made may submit their comments or rejection to the provision of the DCE GSE service in a communication addressed to the Management Committee within thirty (30) days following the notification, after thirty (30) days it will be understood as accepted the conditions by the subscribers or responsible.

4. RESPONSIBILITIES ABOUT REPOSITORIES Y PUBLICATION OF INFORMATION

4.1 Repositories

- **DCE GSE Root Certificates**

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

- **DCE GSE Root Revoked Certificates List (CRL)**

https://crl2.gse.com.co/CA_ROOT.crl
https://crl2.gse.com.co/CA_ECROOT.crl
https://crl2.gse.com.co/CA_FEROOT.crl

- **Subordinated Certificates DCE GSE**

https://certs2.gse.com.co/CA_SUB01.crt
https://certs2.gse.com.co/CA_ECSUB01.crt
https://certs2.gse.com.co/CA_FESUB01.crt
https://certs2.gse.com.co/CA_FESUB01.crt

- **DCE GSE Subordinate Revoked Certificates List (CRL)**

https://crl2.gse.com.co/CA_SUB01.crl
https://crl2.gse.com.co/CA_ECSUB01.crl
https://crl2.gse.com.co/CA_FESUB01.crl
https://crl2.gse.com.co/CA_FESUB01.crl

- **Online validation of Digital Certificates**

https://ocsp2.gse.com.co

Note: The online validation of digital certificates through OCSP must be performed 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.

This DCE GSE repository does not contain any confidential or proprietary information.

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

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

4.2 Publication of certification information

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

The information on the status of the digital certificates in force is available for consultation on the Web page and with the OCSP protocol.

4.3 Deadline or frequency of publication Root Certificate

The root certificate will be published and will remain on the DCE GSE website for the duration of the time in which digital certification services are being provided.

Subordinated Certificate
The certificate of the Subordinate will be published and will remain on the DCE GSE website for as long as digital certification services are being provided.

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

Certification Practice Statement (CPS) - Global Certification Authority Root GSE

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

Online validation of Digital Certificates
DCE GSE will publish the certificates issued in a repository in X.509 V3 format which can be consulted at https://ocsp2.gse.com.co.

The online validation of digital certificates through OCSP must be performed 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.

4.4 Repository access controls

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

5. IDENTIFICATION AND AUTHENTICATION

5.1 Names

5.1.1 Types of names
The guidance document that DCE GSE uses for the unique identification of subscribers or persons responsible for issued certificates is defined in the Distinguished Name (DN) structure of the ISO/IEC 9595 (X.500) standard.

Certificates issued by DCE GSE contain the X.500 distinguished name (DN) of the issuer and recipient of the certificate in the issuer name and subject name fields respectively.

5.1.1.1 DCE GSE Root Certificates

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

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

5.1.1.1.1 Elliptic Curve (ECDSA)

The DN of the 'issuer name' of the root certificate has the following fields and fixed values:
C = CO
S = Capital District
O = GESTION DE SEGURIDAD ELECTRONICA S.A OU = GSE CA RAIZ R2
SERIALNUMBER = 900204278 CN = GSE ECDSA ROOT
E = info@gse.com.co STREET = www.gse.com.co

The following fields are included in the DN of the subject name:
C = CO
S = Capital District L = Bogota D.C.
O = GESTION DE SEGURIDAD ELECTRONICA S.A OU = GSE CA RAIZ R2
SERIALNUMBER = 900204278 CN = GSE ECDSA ROOT
E = info@gse.com.co STREET = www.gse.com.co

5.1.1.1.2 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=GESTION DE SEGURIDAD ELECTRONICA S.A, L=BOGOTA D.C.,
ST=CAPITAL DISTRICT, C=CO

5.1.1.2 Subordinated Certificates

The DN of the issuer name of the certificates of DCE GSE's subordinated companies has the following characteristics:
C = CO
O = GSE
OU = PKI
CN = GSE Root Authority E = info@gse.com.co

The following fields are included in the DN of the subject name:
C = CO
O = GSE
OU = PKI
CN = Subordinate Authority 01 GSE E = info@gse.com.co

5.1.1.2.1 Elliptic Curve (ECDSA)

The DN of the issuer name of the certificates of DCE GSE's subordinated companies has the following characteristics:
C = CO
S = Capital District
L = Bogota D.C.
O = GESTION DE SEGURIDAD ELECTRONICA S.A
OU = GSE CA ROOT R2
SERIALNUMBER = 900204278
CN = GSE ECDSA ROOT
E = info@gse.com.co
STREET = www.gse.com.co

The following fields are included in the DN of the subject name:
C = CO
S = Capital District
L = Bogota D.C.
O = GESTION 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

5.1.1.2.2 DCE GSE Subscriber Certificates (Matrix Certificate Technical Profile)

The DN of the issuer name of the DCE GSE subscriber certificates has the following general characteristics:
C = CO
L = Bogota D.C.
O = GSE
OU = PKI
CN = Subordinate Authority 01 GSE E = info@gse.com.co

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

5.1.1.2.3 DCE GSE Subscriber Certificates (Matrix Technical Profile of electronic signature certificates)

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

5.1.2 Distinctive Names

The distinguished names (DN) of the certificates issued by DCE GSE are unique and allow establishing a link between the public key and the subscriber's identification number. Since the same person or entity can request several certificates in their name, they will be differentiated by the use of a unique value in the DN field.

5.1.3 Anonymity and pseudo-anonymity of the subscriber or responsible parties

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

5.1.4 Rules for the interpretation of various forms of name

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

5.1.5 Singularity of names

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

5.1.6 Recognition, authentication and role of recognized marks

Recognition, authentication and role of recognized trademarks DCE GSE is not required to collect or request evidence regarding the ownership or subscription or liability of trademarks or other distinctive signs prior to the issuance of digital certificates. This policy extends to the use and employment of domain names.

5.2 Identification and authentication for key renewal requests

5.2.1 Identification and authentication for renewal.

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

5.2.2 Identification and authentication after revocation

The process of replacement of a digital signature certificate as a consequence of the revocation due to the different causes defined in this CPS, require a verification process for that request (Replacement).

5.3 Identification and authentication for revocation requests

DCE GSE, attends the revocation requests in accordance with the revocation grounds specified in the section Circumstances for revocation of a certificate of this CPS and authenticates the identity of the person requesting the certificate revocation. In accordance with the revocation procedure.

6. REQUIREMENTS OPERATIONAL REQUIREMENTS FOR THE TIME FROM LIFETIME FROM THE CERTIFICATES

6.1 Certificate request

Any person who requires the provision of digital certification service, may do so using the channels provided by GSE, accepting the terms and conditions of the DCE and provide them along with the required documentation to authenticate the information provided. Once the information is completed and confirmed by the applicant, the application form is sent to the Registration Authority who will be responsible for validating the information provided and approve it in accordance with compliance with the requirements of the Certification Policies.

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

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

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

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

The applicant agrees that DCE GSE has the discretionary right to reject an application for a digital certificate where in its judgment the credibility, commercial value, goodwill of GSE or legal or moral fitness of the entire digital certification system may be jeopardized by giving notice of non-approval.

The Electronic Signature Procedure (PTI-PD-20) has been established for requesting an electronic signature certificate.

6.2 Who can apply for a certificate

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

6.2.1 Registration process and responsibilities

The GSE RA will approve and digitally sign the certificate of issuance of the digital certificates once the authentication and verification requirements of the applicant's data have been fulfilled. All related information will be registered in the GSE RA system.

6.3 Certificate Uses

6.3.1 Appropriate uses of the certificate

The appropriate uses of the Certificates issued by DCE GSE are specified in Certificate Policies for Digital Certificates.

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

- **Identification of the Subscriber:** The Subscriber of the Digital Certificate can authenticate, before another party, its identity, demonstrating the association of its 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 integral, that is to say, it guarantees that the document was not altered or modified after being signed by the Subscriber. It certifies that the message received by the Receiver or Trusted Recipient is the same as the one issued by the Subscriber.
- **Non-repudiation:** With the use of this Digital Certificate it is also guaranteed that the person who digitally signs the document cannot repudiate it, that is, the Subscriber who has signed it cannot deny the authorship or integrity of the document.

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

DCE 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 CPS shall be considered a violation of this CPS and shall constitute grounds for immediate revocation of the digital certification service and termination of the contract with the subscriber or responsible party, without prejudice to any criminal or civil action that may be taken by the DCE GSE.

6.3.2 Prohibited uses of the certificate and exclusion of liability

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

Improper uses are considered to be those that are not defined in this CPS and consequently for legal purposes, DCE GSE is exempted 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 CPS, including but not limited to the following prohibited uses:

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

6.4 Processing of certificate applications

6.4.1 Performing identification and authentication functions

The functions of authentication and verification of the applicant's identity are performed by the RA of GSE, in charge of authorizing the issuance of the certificate, who checks if the information provided is authentic and if the attached documentation complies with the requirements defined for each type of certificate in accordance with this CPS.
The documentation that the GSE RA must check for the correct issuance of each type of certificate is defined in the Certificate Policies for Digital Certificates.

6.5 Initial Identity Validation

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

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

Identity validation is performed in a manner analogous to face-to-face validation by consuming the widely used services listed below:

- National Identification Archive - National Registry of Civil Status.
- Muisca (Single Model of Income, Service and Automated Control) of the DIAN (National Tax and Customs Directorate).
- Confronts.
- Sole Corporate and Social Registry (For Legal Entity).

The document Registro Único Tributario - RUT will be requested in the updated DIAN format that includes a QR code.

These services are related in the Procedure for issuance of digital certificates.

For digital certification services (Time Stamping, Certified Electronic Mail, Generation of Certified Electronic Signatures, Archiving and Preservation of Electronic Transferable Documents and Data Messages) the Confronta identity validation service will not be used, but the other validation mechanisms will be used.

The DCE 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 DCE GSE through other means.

In the case of electronic signature certificates, the identity of the subscriber is not validated, but the data recorded at the time of the signature request is verified by sending an OTP code to the registered e-mail address.

6.5.1 Method of 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 to the subscriber and/or responsible party to generate the key pair and transmit through a secure channel the file in PKCS#10 format where the subscriber and/or responsible party proves that he/she is in possession of the private key.

In case the certificate is centralized, the generation of the key pair is carried out in an HSM device owned by the DCE GSE and the subscriber and/or responsible is given a set of credentials (user and password) for the exclusive use of the same.

Since the electronic signature certificates are ephemeral and are used only for signature generation, 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.

Pursuant to what is established by ONAC in CEA 3.0-07, in the case where the key pair is generated by the applicant in its own infrastructure, for example, for the use of the certificate in unattended platforms, the applicant must accept and comply with the requirements set forth in the document Annex 1 of Terms and Conditions number 6 literal m), if these were generated by software and by means of devices that comply with Annex F of the CEA, if they were generated by hardware.

6.5.2 Authentication of an entity's identity (legal entity)

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

Notwithstanding the foregoing, DCE 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 jeopardized.

6.5.3 Authentication of an Individual Identity (Natural Person)

To ensure the identity of a natural person, RA GSE requires the presentation of the subscriber's identity document scanned and verifies its existence and correspondence against its own or third party databases, whether official or private. When the service is requested by a minor, his/her identity will be assured with the authenticated identity document (identity card) and a document that supports the link between the applicant and the minor. In case the request is made by a third party, a scanned proof of delegation of the process to the proxy must be submitted. The documents will be received scanned, preserving the legibility for the use of the information.

Notwithstanding the foregoing, DCE 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 jeopardized.

6.5.4 Unverified subscriber or responsible party information

Under no circumstances will DCE GSE omit the verification work that leads to the identification of the subscriber or person responsible and that translates into the request and requirement of the mentioned documents for organizations and individuals.

6.5.5 Criteria for interoperability

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

6.5.6 Approval or rejection of certificate applications

If, once the identity of the applicant has been verified, the information provided complies with the requirements established by this CPS, the application is approved. If it is not possible to fully identify the identity of the applicant or the information provided is not fully authentic, the application is denied and the certificate is not issued. DCE GSE assumes no responsibility for the consequences that may arise from the non-approval of the issuance of a digital certificate and the applicant who has been denied the issuance of the respective certificate accepts and acknowledges this.

Likewise, DCE GSE reserves the right not to issue certificates even though the identification of the applicant or the information provided by the applicant has been fully authenticated, when the issuance of a particular certificate for reasons of legal 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 perform the identity validation, after fifteen (15) days without remedying the novelty, the application will be rejected and the applicant will be notified to file a new application.

DCE GSE will notify the applicant of the approval or rejection of the application.

6.5.7 Deadline for processing certificate applications

The timeframe for processing an application by the GSE RA is from one (1) to five (5) business days from the time the requested documentation and information is received and the applicant has passed the identity validation.
The delivery time of the digital certificate issued in a cryptographic device depends on the place of destination, without exceeding eight (8) working days for its delivery.

6.6 Issuance of certificates

6.6.1 CD GSE's actions during the issuance of certificates

The final step of the digital certificate issuance process is the issuance of the certificate by DCE GSE and its secure 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 digital certificate issuance process securely links the registration information and the generated public key.

6.6.2 Notification to the applicant by the DCE GSE of the issuance of the certificate

The subscriber is notified by e-mail of the issuance of his digital certificate and therefore the subscriber accepts and acknowledges that once he receives the aforementioned e-mail, it will be understood that the certificate has been issued. It shall be understood that the e-mail notifying the issuance of a certificate has been received when said e-mail enters the information system designated by the applicant, that is, the e-mail address that the subscriber reported in the application form. In the case that the subscriber requests that the

issuance of the signature is in a cryptographic device, it will be understood as delivered once the delivery letter and/or the delivery guide to the logistic operator or courier is signed.

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

6.7 Acceptance of the certificate

6.7.1 Manner in which the certificate is accepted

No confirmation by the subscriber or responsible party is required as acceptance of the certificate received. A certificate is considered to be accepted by the subscriber or responsible party from the moment he/she requests its issuance, therefore, if the information contained in the issued certificate does not correspond to the current status of the certificate or was not provided correctly, it is the subscriber's responsibility to request its revocation.

6.8 Use of private key and certificate

6.8.1 Use of the private key and certificate by the subscriber or responsible

The subscriber or person responsible for the digital certificate and the associated private key, accepts the conditions of use established in this CPS by the mere fact of having requested the issuance of the certificate and may only use them for the uses explicitly mentioned and authorized in this CPS and according to what is established in the "Key Usage" fields of the certificates. Therefore, the issued certificates and the private key shall not be used in other activities that are outside the mentioned uses. Once the validity of the certificate has expired, the subscriber or responsible party is obliged to stop using the private key associated to it. Based on the above, the subscriber accepts and acknowledges that in this sense, he/she will be solely responsible for any loss or damage caused to third parties by the use of the private key after the expiration of the certificate. DCE GSE assumes no responsibility for any unauthorized use.

6.8.2 Use of the private key and certificate by bona fide third parties

The subscriber to whom a certificate has been issued is obliged to inform third parties every time he/she makes use of the certificate that it is necessary to consult the status of the certificate in the repository of revoked certificates, as well as in the repository of issued certificates, in order to verify its validity and that it is being applied within the permitted uses established in this CPS.

In this regard, it shall:

- Verify that the associated certificate does not violate the start and end dates of validity.
- Check that the certificate associated with the private key is not revoked.
- Check that the fingerprint of the root ECD's certificate and that of the DCE GSE's subordinate certificate match the one published by the GSE on its website.

Fingerprint of the root DCE 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

Fingerprint of the DCE GSE Subordinate Certificate 001:

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

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

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

6.9 Renewal of the certificate without change of keys

DCE GSE does not attend to requests for renewal of a certificate without a change of keys.

6.9.1 Circumstances for renewal of certificates without change of keys
It does not apply as certificates are not issued without change of keys.

6.9.2 Who can apply for a renewal without a change of keys
It does not apply as certificates are not issued without change of keys.

6.9.3 Procedures for certificate renewal applications without change of keys
It does not apply as certificates are not issued without change of keys.

6.9.4 Notification to the subscriber or responsible party of the issuance of a new certificate without change of keys.
It does not apply as certificates are not issued without change of keys.

6.9.5 How to accept the renewal of a certificate without a change of keys
It does not apply as certificates are not issued without change of keys.

6.9.6 Publication of the certificate renewed by DCE without change of keys
It does not apply as certificates are not issued without change of keys.

6.9.7 Notification of the issuance of a renewed DCE certificate to other entities

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

6.10 Certificate renewal with change of keys

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

6.10.1 Circumstances for the renewal of certificates with change of keys

A digital certificate may be renewed at the request of the subscriber or responsible party due to upcoming loss of validity or revocation in accordance with the grounds mentioned in this CPS or when so required by the subscriber.

6.10.2 Who can apply for a renewal with change of keys

For certificates of natural persons, the subscriber can request the renewal of the certificate. For legal entities, the legal representative, deputies or responsible persons can request the renewal of the digital certificate.

6.10.3 Procedures for the application for renewal of certificates with key changes

The procedure for digital certificate renewal is the same as the procedure for requesting a new certificate. The subscriber must access the GSE products and services request web portal and initiate the certificate renewal request process in the same way as when he/she first requested the certificate. Your information will be re-validated in order to update data if required.

6.10.4 Notification to the subscriber or responsible party of the issuance of a new certificate with change of keys.

The subscriber is notified by e-mail of the issuance of its digital certificate and therefore the subscriber accepts and acknowledges that once the aforementioned e-mail is received, it will be understood that the certificate has been issued. It shall be understood that the e-mail notifying the issuance of a certificate has been received when said e-mail enters the information system designated by the applicant, that is, the e-mail address that the subscriber reported in the application form. In case the subscriber requests the issuance of the signature in a cryptographic device, it will be understood as delivered once the letter of delivery to the logistic operator is signed.

6.10.5 Form in which the renewal of a certificate is accepted

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

6.10.6 Publication of the certificate renewed by DCE with change of keys

Not applicable because DCE GSE does not publish certificates.

6.10.7 Notification of the issuance of a renewed DCE certificate to other entities

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

6.11 Modification of certificates

Digital certificates issued by DCE 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 borne entirely by the subscriber according to the fees informed by DCE GSE or according to the conditions defined at the contractual level.

6.11.1 Circumstances for certificate modification

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

6.11.2 Who can request a modification

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

6.11.3 Procedures for requesting a certificate modification

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

6.11.4 Notification to the subscriber or person responsible for the issuance of a new certificate

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

6.11.5 Form in which the modification of a certificate is accepted

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

6.11.6 Publication of the modified DCE certificate

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

6.11.7 Notification of the issuance of a certificate by DCE to other entities

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

6.12 Revocation and suspension of certificates

6.12.1 Circumstances for revocation of a certificate.

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

a. Loss or disablement of the private key or digital certificate.
b. The private key has been exposed or is at risk of misuse.
c. Changes in the circumstances under which DCE 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 becomes outdated or invalid.

If the subscriber or responsible party does not request the revocation of the certificate in the event of the above situations, he shall be liable for the losses or damages incurred by third parties in good faith without fault who trusted the content of the certificate.

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

a. At the request of the subscriber, responsible party or a third party in his name and on his behalf.
b. Death of the subscriber or responsible party.
c. By the confirmation or evidence that some information or fact contained in the digital certificate is false.
d. The certification authority's private key or its security system has been compromised in a material way that affects the trustworthiness of the certificate.
e. By court order or by order of a competent administrative entity.
f. For compromise of safety in any reason, manner, situation or circumstance.
g. Due to 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 facts that cause the original data not to correspond to reality.
j. For loss or disablement of the cryptographic device that has been delivered by DCE GSE.
k. For the termination of the subscription contract, in accordance with the grounds established in the contract.
l. For any cause that reasonably leads to believe that the certification service has been compromised to the extent that the trustworthiness of the digital certificate is in doubt.
m. For improper handling by the subscriber of the digital certificate.
n. For non-compliance of the subscriber or the legal entity that represents or to which it is linked through the document terms and conditions or responsible for digital certificates of the DCE GSE.
o. Knowledge of events that modify the initial status of the data provided, among others: termination of the Legal Representation, termination of the labor relationship, liquidation or extinction of the legal status, cessation of the public function or change to a different one.
p. At any time that there is evidence of false information provided by the applicant, subscriber or responsible party.
q. For non-compliance by the DCE GSE, the subscriber or responsible party of the obligations established in the CPS.
r. Failure to pay the amounts for certification services agreed between the applicant and DCE GSE.

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

6.12.2 Who can request a revocation

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

A third party in good faith or any interested person who has demonstrable evidence that a digital certificate has been used for purposes other than those set out in the section Appropriate uses of the certificate of this CPS.

Any interested party 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 highest control body responsible for the administration of the security of the technological infrastructure of DCE GSE, is able to request the revocation of a certificate if it has knowledge or suspicion of the compromise of the subscriber's private key, responsible or any other fact in accordance with the circumstances for the revocation of a certificate.

6.12.3 Revocation request procedure

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

- At the GSE offices.
  Written requests for revocation of digital certificates signed by subscribers and responsibles are received during public service hours, providing the original identification document.

- Online revocation request:
  The subscriber and/or responsible, will be able to carry out the process of revocation of the digital certificate through the web portal of GSE S.A., https://gse.com.co/consultas- en-linea/ - Request revocation, when filling out the request the current digital certificates will be displayed, the certificate to be revoked must be selected and a notification with the security code will be sent to the subscriber's registered e-mail address to complete 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 the digital certificate; once the request is completed, the selected certificate will be automatically revoked and the revocation confirmation will be sent to the registered e-mail address. Another means available for the revocation of the digital certificate by the subscriber and/or responsible party is through the tool from where the application for the issuance of the digital certificate was filed.

- Revocation Service via e-mail

Through our e-mail revocaciones@gse.com.co, subscribers and/or responsible parties may request the revocation of digital certificates according to the revocation grounds mentioned in the Circumstances for revocation of a certificate section of this CPS, by sending a digitally signed revocation request letter or e-mail with the subscriber's data and revocation grounds.

Note: The DCE - GSE provides a template guide for 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 develop the certification activities according to the digital certificate revocation procedure, will verify the revocation request.

6.12.4 Revocation request grace period

Upon validation of the authenticity of a revocation request, DCE GSE will immediately proceed with the requested revocation, within its office hours. Consequently, there is no grace period allowing the applicant to cancel the request. If the request was erroneous, the subscriber or responsible party must request a new certificate, since the revoked certificate lost its validity immediately after the revocation request was validated and DCE GSE will not be able to reactivate it.

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

Once the revocation of the certificate is requested, if it is evidenced that such certificate is used in connection with the private key, the subscriber or responsible party relieves DCE GSE of all legal responsibility, since he/she acknowledges and accepts that the control, custody and confidentiality of the private key is the exclusive responsibility of the subscriber or responsible party.

6.12.5 Deadline for the DCE to resolve the revocation request

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

Once the formalities for revocation have been complied with and if for any reason, the revocation of a certificate is not effective under the terms established by this CPS,
DCE GSE as a certification service provider shall be liable for damages caused to subscribers or third parties in good faith arising from errors and omissions, bad faith of managers, legal representatives or employees of DCE GSE in the development of the activities for which it is authorized and for this purpose it has a liability insurance in accordance with Article 9°. Guarantees, of Decree 333 of 2014. DCE GSE does not assume any other commitment or provide any other guarantee, nor does it assume any other liability

to the subscriber or persons responsible for certificates or trusted third parties except for what is established by the provisions of this CPS.

6.12.6 Requirements for verification of revocations by bona fide third parties

It is the responsibility of the subscriber or person responsible for a digital certificate, and he/she accepts and recognizes it, to inform third parties in good faith of the need to check the validity of the digital certificates he/she is using at any given time. The subscriber or responsible party shall also inform the bona fide third party that, in order to make such consultation, the list of revoked certificates CRL, published periodically by DCE GSE, is available.

6.12.7 Update frequency of CRLs

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

6.12.8 Maximum latency time of CRLs

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

6.12.9 On-line revocation/availability of status verification

DCE GSE will publish both the CRL and the status of revoked certificates in freely accessible and easily consulted repositories, with 7X24 availability every day of the year. DCE GSE offers an online query service based on OCSP protocol at https://ocsp2.gse.com.co.

The online validation of digital certificates through OCSP must be performed 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.

6.12.10 On-line revocation verification requirements

To obtain information on the revocation status of a certificate at a given time, the certificate can be consulted online at https://ocsp2.gse.com.co. To do so, you must have software capable of operating with the RFC6960 protocol. Most browsers offer this service.

The online validation of digital certificates through OCSP must be performed 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.

6.12.11 Notification of certificate revocation

Within 24 hours following the revocation of a certificate, DCE GSE informs the subscriber or responsible, by email, the revocation of its digital certificate and therefore the applicant accepts and acknowledges that once the aforementioned email is received, it will be understood that the request was attended. It will be understood that the e-mail notifying the revocation of a certificate has been received when said e-mail enters the information system designated by the applicant, that is, the e-mail address that appears in the application form. The publication of a revoked certificate in the CRL constitutes proof and public notification of its revocation.

6.12.12 Other Available Ways for Disclosure of Revocation Information

DCE GSE will maintain a historical archive of up to three (3) years of generated CRL's which will be available to subscribers upon written request to DCE GSE.

6.12.13 Special renewal requirements for 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 is of the subscriber or responsible and he/she accepts and acknowledges it, therefore, it is he/she who assumes the cost of the renewal in accordance with the current rates set for the renewal of digital certificates.

6.12.14 Circumstances for suspension

DCE GSE does not have a digital certificate suspension service, only revocation.

6.12.14.1 Who can request the suspension

It does not apply because DCE GSE does not have the service of suspension of digital certificates, only revocation.

6.12.14.2 Suspension request procedure

It does not apply because DCE GSE does not have the service of suspension of digital certificates, only revocation.

6.12.14.3 Limits of the suspension period

It does not apply because DCE GSE does not have the service of suspension of digital certificates, only revocation.

6.13 Certificate profiles

The certificates comply with the X.509 version 3 standard and the authentication infrastructure is based on RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

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

1. Name, address and domicile of the subscriber or responsible party.
2. Identification of the subscriber or person in charge named in the certificate.
3. The name, address and place where the DCE carries out its activities.
4. The public key of the subscriber or legal entity.
5. The methodology to verify the digital signature of the subscriber or legal entity imposed in the data message.
6. The serial number of the certificate.
7. Date of issuance and expiration of the certificate.

6.13.1 Description of certificate contents

Field	Value or RSA restrictions	Value or restrictions ECDSA
Version	3 (0x2)	3 (0x2)
Serial Number	Unique identifier issued by DCE GSE	Unique identifier issued by DCE GSE
Signature Algorithm	SHA256withRSAEncryption	SHA384withECDSA
Emitter	See section "Rules for the interpretation of various name forms". For DCE GSE as issuer, it is specified: E=info@gse.com.co, CN=Subordinate Authority 01 GSE, OU=PKI, O=GSE, L=Bogot a D.C., C=CO	See section "Rules for the interpretation of various name forms". For DCE GSE as sender you specify: STREET=www.gse.com.co, E=info@gse.com.co, CN=GSE ECDSA SUBORDINATE, SN=900204278, OU=GSE ECDSA R2 SUB1, O=MANAGEMENT DE SEGURIDAD ELECTRONICA S.A, L=Bogota D.C., S=Capital District, C=CO
Valid from	Specifies the date and time from which the certificate is valid.	Specifies the date and time from which the certificate is valid.
Valid until	Specifies the date and time after which the certificate is no longer valid.	Specifies the date and time after which the certificate is no longer valid.
Subject	In accordance with the policy in Annex 1 and the *"Rules for the interpretation of various forms of name".*	In accordance with the policy in Annex 1 and the *"Rules for the interpretation of various forms of name".*
Subject's public key	Encrypted in accordance with RFC 5280. Certificates issued by DCE GSE have a length of 2048 bits and RSA algorithm.	Encrypted in accordance with RFC 5280. Certificates issued by DCE GSE have a length of 256 bits and EC algorithm.
Authority key identifier	It is used to identify the root certificate in the certification hierarchy. Normally it references the "Subject Key Identifier" field of DCE GSE as the issuing entity for digital certification.	It is used to identify the root certificate in the certification hierarchy. Normally it references the "Subject Key Identifier" field of DCE GSE as the issuing entity for digital certification.
Subject key identifier	It is used to identify a certificate containing a particular public key.	It is used to identify a certificate containing a particular public key.
Certificate Guidelines	Describes the policies applicable to the certificate, specifies the OID and the URL where the certificate policies are available. certification.	Describes the policies applicable to the certificate, specifies the OID and the URL where the certificate policies are available. certification.
Use of the key	Specifies the permitted uses of the key. It is a CRITICAL FIELD.	Specifies the permitted uses of the key. It is a CRITICAL FIELD.

Field	Value or RSA restrictions	Value or restrictions ECDSA
CCC distribution point	It is used to indicate the addresses where the DCE GSE CRL is published. In the Root DCE certificate, this attribute is not specified.	It is used to indicate the addresses where the DCE GSE CRL is published. In the Root DCE certificate, this attribute is not specified.
Access to Authority information	It is used to indicate the addresses where the DCE GSE root certificate is located. Also, to indicate the address to access the OCSP service. In the certificate DCE GSE root, this attribute is not specified.	It is used to indicate the addresses where the DCE GSE root certificate is located. Also, to indicate the address to access the OCSP service. In the certificate DCE GSE root, this attribute is not specified.
Alternate name of subject	It is used to indicate the e-mail address and additionally to indicate the accreditation code assigned by ONAC. Name RFC822=correo@empresa.com URL= https://gse.com.co/documentos/certificaciones /accreditation/16-ECD-001.pdf	It is used to indicate the e-mail address and additionally to indicate the accreditation code assigned by ONAC. Name RFC822=correo@empresa.com URL= https://gse.com.co/documentos/certificaciones /accreditation/16-ECD-001.pdf
Widespread uses of the key	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 restrictions	The extension "PathLenConstraint" indicates the number of sub-levels that are supported in the certificate path. There is no restriction for DCE GSE, therefore, it is zero.	The extension "PathLenConstraint" indicates the number of sub-levels that are supported in the certificate path. There is no restriction for DCE GSE, therefore, it is zero.

6.13.1.1 Version number

The certificates issued by DCE GSE comply with the X.509 Version 3 standard.

6.13.1.2 Certificate extensions

A detailed description of the certificates issued by GSE is provided in Annex 1 of this CPS.

6.13.1.3 Key Usage

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

6.13.1.4 Certificate policy extension

The "certificatepolicies" extension of X.509 version 3 is the object identifier of this CPS in accordance with the object identifier section of the Certification Policy of this CPS. The extension is not considered critical.

6.13.1.5 Alternate name of subject

The extension "sujectAltName" is optional and the use of this extension is "Not critical".

6.13.1.6 Basic restrictions

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

6.13.1.7 Widespread use of the key

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

OID	Description	Types of Certificates
1.3.6.1.5.5.7.3.4	Mail protection	Digital Signature of 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

6.13.1.8 Object Identifiers (OID) of the algorithms

The object identifier of the signature algorithm is: 1.2.840.113549.1.1.1.11 SHA256 with RSA Encryption

The object identifier of the public key algorithm is: 1.2.840.113549.1.1.1.1 rsaEncryption

The object identifier of the signature algorithm is: 1.2.840.10045.4.3.3 SHA384WITHECDSA.

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

6.13.1.9 Name formats

In accordance with what is specified in the Types of Names section of this CPS.

6.13.1.10 Name restrictions

Names should be written in capital letters and without accents.

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

6.13.1.11 Certification Policy object identifier

The object identifier of the Certificate Policy corresponding to each type of certificate is a subclass of the class defined in the Document Name and Identification section of this CPS, as established in the Certificate Policies for digital certificates.

6.13.1.12 Using the Policy Constrains extension

It is not stipulated.

6.13.1.13 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 CPS is published.

6.13.1.14 Semantic processing for Certificate Policies extension

It is not stipulated.

6.14 Certificate status information services

6.14.1 CRL Profile

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

6.14.1.1 Version number

The CRL's issued by DCE GSE comply with the X.509 version 2 standard.

6.14.1.2 CRL and CRL extensions

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

6.14.1.3 CRL Availability

As per 6.12.9 On-line revocation/availability of status verification.

6.14.1.4 OCSP Profile

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

6.14.1.5 Version number

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

6.14.1.6 OCSP extensions

Does not apply

6.14.1.7 OCSP Availability

As per 6.12.9 On-line revocation/availability of status verification.

6.14.2 Operational characteristics

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

6.14.3 Optional features

To obtain information on the certificate status at a given moment, you can make an online query at https://ocsp2.gse.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.gse.com.co.

The online validation of digital certificates through OCSP must be performed 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.

6.15 Termination of the validity of a certificate

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

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

6.16 Custody and recovery of keys

6.16.1 Subscriber's private key storage

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

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

6.16.2 Private key storage to a responsible person

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

The hardware cryptographic device used by DCE 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 cryptographic chip certifications: security level CC EAL5+ PP 9806, BSI-PP- 002-2001, FIPS 140-2 LEVEL 3 and the cryptographic chip SO certifications: security level CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3) - BSI -DSZ-CC- (CWA 14169 SSCD Type-3) - BSI -DSZ-CC- (CWA 14169 SSCD Type-3). 0422-2008 and support PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPsec/IKE standards.

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

6.16.3 Custody and key recovery practices and policies

The generation of the private key is stored on a secure device (hardware), from which it cannot be exported. Consequently, it is not possible to retrieve the subscriber's private key. The responsibility for the safekeeping of the private key rests with the subscriber and is accepted and acknowledged by the subscriber.

6.16.4 Session key custody and recovery policies and practices

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

7. PHYSICAL INSTALLATION, MANAGEMENT AND OPERATIONAL CONTROLS

7.1 Physical location and construction

DCE 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 performed through a service provider. Access to the rack that houses the servers through which the DCE GSE's communication services are managed is only allowed to previously identified and authorized persons who carry in a visible place the visitor's card.

The DCE GSE's technological infrastructure provider guarantees that the PKI servers are in continuous virtual operation in the Amazon cloud. Said provider has procedures in place to carry out the administration operations of the DCE GSE's communications infrastructure, to which only authorized personnel have access.

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

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

j. There is no frequent transit of people in the surrounding area.

7.2 Physical access

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

7.3 Power supply and air conditioning

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

7.4 Water exposure

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

7.5 Physical controls of the technological infrastructure through which DCE GSE provides its services.

The technological infrastructure services through which DCE GSE provides its services is contracted with the supplier Paynet SAS.

7.6 Fire prevention and protection

The communications center has a fire detection system and a fire extinguishing system. There is a cabling system that protects the internal networks.

7.7 Storage system

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

The mission servers are in cloud environments; however, onpremises servers are backed up and stored in a local NAS server with their respective contingency.

7.8 Disposal of information storage material

All paper documents containing sensitive information of the entity and that have fulfilled their useful life must be physically destroyed to ensure the impossibility of information recovery. If the document or information is stored on magnetic media, the device must be formatted, permanently erased 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 unknown at the time.

7.9 Off-site backup

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

7.10 Procedural controls

7.10.1 Roles of trust

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

- **RA Agents:** Persons responsible for daily operations such as: review and approval of applications attending all activities related to digital certification services provided by DCE GSE through the RA, the roles and responsibilities of the RA agents are defined according to the DCE GSE Profiles and Roles.

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

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

7.10.2 Number of people required per task

One person is required for each of the above roles. The DCE guarantees the collaboration of at least two people to perform the tasks that affect the ECD's own cryptographic key management.

7.10.3 Identification and authentication for each role

RA Agents and RA Administrators are authenticated by digital certificates issued by DCE GSE.

Each person only controls the assets required for his role, thus ensuring that no one person accesses unallocated resources.
Access to resources is done depending on the asset by login/password, digital certificates.

7.10.4 Roles requiring segregation of duties

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

7.11 Personnel controls

7.11.1 Qualifications, professional experience and knowledge requirements

A personnel selection process has been defined based on the profile of each of the positions involved in the digital certificate issuance process. The candidate for a position must have the training, experience, knowledge and skills defined in the document Profile and functions of the position.

7.11.2 Background check procedure

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

7.11.3 Training requirements

The training requirements for each of the aforementioned positions are included in the Profile and functions of the position, which is made known to the person selected for the position as part of his or her induction. The most important aspects that are part of the training are:

- Knowledge of the Certification Practices Statement.
- Knowledge of the regulations in force and related to open certification entities and the services they provide.
- Knowledge of the Security Policies and acceptance of a confidentiality agreement on the information handled by virtue of the position.
- Knowledge of software and hardware operation for each specific role.
- Knowledge of safety procedures for each specific role.
- Knowledge of operating and administrative procedures for each specific role.
- Knowledge of Business Continuity Plans

7.11.4 Training update requirements and frequency

The annual training program includes an update on Information Security for the members of the digital certificate issuance cycle.

7.11.5 Frequency and sequence of task rotation

There is no rotation of tasks in the aforementioned positions.

7.11.6 Penalties for unauthorized actions

It is considered a serious offense to perform unauthorized actions and individuals will be sanctioned in accordance with the disciplinary process.

7.11.7 Third-party contracting requirements

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 by reason of the contractual relationship with GSE.

7.11.8 Documentation provided to personnel

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

7.12 PKI Security Audit Procedures

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

7.12.1 Types of events recorded

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

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

7.12.2 Frequency of audit trail processing (log)

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

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

7.12.3 Retention period for audit records

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

7.12.4 Protection of audit trails

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

7.12.5 Audit log backup procedures

Audit log backups are replicated to a centralized log site.

7.12.6 Audit information 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. These are stored in CloudWatch and databases for monitoring.

7.12.7 Notification to the subject causing the event

At the discretion 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.

7.12.8 Vulnerability analysis

In addition to periodic log reviews, DCE GSE sporadically or in case of suspicious activities, reviews the logs in accordance with the established internal procedures. It also reviews the results obtained from Ethical Hacking and the activities described for the correction of findings.

7.13 Archive of PKI logs and events

Archiving and event logging is performed by the PKI infrastructure service provider (Paynet SAS).

7.13.1 Archived event types

A record file is kept of the most relevant events of the operations performed during the digital certificate issuance process.

7.13.2 Conservation period

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

7.13.3 File protection

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

7.13.4 Log file backup procedures

Backups of the Archives of Records are performed according to the procedures established for backups and recovery of backups of the rest of the information systems.

7.13.5 Requirements for time stamping of records

The servers are kept up to date with UTC Time (Coordinated Universal Time). They are synchronized through the NTP protocol (Network Time Protocol). Given that according to the provisions of numeral 14 of article 6 of Decree number 4175 of 2011, the National Metrology Institute 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 performed with the NTP server of the INM.

7.13.6 Archiving system for audit information (internal or external)

Both external and internal audit information is stored and kept in an off-site location outside DCE GSE's facilities once it has been digitized. Digitized audit files are accessed only by authorized personnel using viewing tools. Databases are maintained on Amazon's CloudWatch service.

7.13.7 Procedures for obtaining and verifying archived information.

Log files are accessed only by authorized personnel using event viewing and management tools for the purpose of verifying log integrity or for security incident audits.

7.14 DCE key replacement

7.14.1 DCE GSE Root Key Replacement

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

Before the use of the DCE GSE private key expires, a key exchange will be performed. The previous root CA and its private key will only be used for signing 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 differentiates it from the previous one.

7.14.2 Change of keys of a Subordinated Company of DCE GSE

The procedure for changing the keys of an DCE GSE subordinate is the equivalent of generating a new digital certificate. The certificates issued with the previous key of the subordinate must be revoked or the infrastructure must be maintained until the expiration of the last certificate issued. If it is decided to revoke the certificates and issue new ones, these will have no cost for the subscriber or responsible party.

Before the use of the private key of the DCE GSE subordinate expires, a key exchange will be performed. The previous DCE subordinate and its private key will only be used for signing the CRL as long as there are active certificates issued by the previous DCE subordinate. A GSE DCE Subordinate will be generated with a new private key and a new DN. The public key will be published in the same repository with a new name that differentiates it from the previous one.

7.15 Recovery in case of key compromise and natural disaster or other catastrophic event

7.15.1 Incident management procedures

DCE GSE has established and tested an Information Security Incident Procedure for both the RA and CA that establishes the actions to be taken in the event of a vulnerability or security incident. Once the procedures for restoring the systems have been satisfactorily executed, service will be provided to the public.

7.15.2 Alteration of the hardware, software or data resources.

In the event of a suspected disruption of hardware, software, or data resources, the DCE shall be shut down until the security of the environment is restored. To avoid a recurrence

of the incident, the cause of the disturbance must be identified. In the event of such an occurrence DCE GSE will inform ONAC giving explanation and justification.

7.15.3 Procedure for action in the event of vulnerability of an Authority's private key

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

a. When the certification body's security system has been breached.
b. When failures occur in the certification body's system that compromise the provision of the service.
c. When the encryption systems become obsolete because they do not offer the level of security contracted by the subscriber.
d. When any other information security event or incident occurs.

In case of DCE commitment:

a) Apply containment of the incident to prevent recurrence
b) Inform all Subscribers, Responsible Parties, Relying Parties and other CAs with which it has agreements or other types of relationship of the commitment.
c) It will indicate that certificates and revocation status information signed using this key are invalid.
d) ONAC and customers will be informed.

7.15.4 Resilience after a natural disaster or other type of catastrophe

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

7.16 Termination of an ECD

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

The DCE - GSE will inform all subscribers and/or responsible parties 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 for a subscriber to obtain a refund equivalent to the value of the remaining term of the contracted service.
d. The authorization issued by the Superintendence of Industry and Commerce for the DCE to cease the service, and if applicable, the CCC operator responsible for the service publication of the certificates issued by the DCE - GSE until the last one expires.

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

The DCE GSE has a security plan in case of termination of activities, which contemplates the guidelines and activities for its execution.

8. TECHNICAL SAFETY CONTROLS

8.1 Key pair generation and installation

8.1.1 Key pair generation

8.1.1.1 DCE Root key pair generation
The generation of the DCE Root key pair was carried out at the platform service provider's facilities under the strictest security measures and under the key generation ceremony protocol established for this type of event and in the presence of an DCE GSE delegate. A FIPS 140-2 level 3 approved cryptographic device was used to store the private key.

8.1.1.2 Key pair generation of DCE GSE subordinates
The generation of the key pair of the DCE GSE subordinates was performed at the DCE GSE service provider's facilities under the key generation ceremony protocol. A FIPS 140-2 level 3 approved cryptographic device is used to store the subordinate private key.

8.1.1.3 Generation of key pair for DCE GSE subscribers or managers
The generation of the DCE GSE subscriber key pair is performed at the DCE GSE service provider's facilities. A FIPS 140-2 level 3 approved cryptographic device is used to store the subscriber's private key.

8.1.2 Delivery of the private key to subscribers

The private key is delivered to the subscriber and/or responsible party in his cryptographic device and cannot be extracted. There is therefore no copy of the subscriber's private key.

8.1.3 Delivery of the public key to the certificate issuer

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

8.1.4 Delivery of the DCE public key to third-party acceptors

The public key of the Root DCE and the Subordinate DCE is included in its digital certificate.

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

The certificates of the Subordinated DCE can be consulted by trusted third parties in the repositories listed in numeral 4.1 Repositories, DCE GSE Subordinated Certificates.
The following key sizes have been defined for RSA:

- DCE Root of DCE GSE is 4096 bits.
- Subordinate DCE GSE is 4096 bits.
- Certificates issued by DCE 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 a processing workload in the order of 3 x1020 MIPS-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 capable of processing per second during a year.

The following key sizes have been defined for ECDSA:

- DCE GSE DCE Root is 384 bits.
- Subordinate DCE GSE is 384 bits.
- Certificates issued by DCE GSE to end users is 256 bits.

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

8.1.5 Parameters for public key generation and quality check

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

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

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

8.1.6 Permitted key usage (according to the X.509 key usage field)

The allowed 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 DCE GSE.

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

TYPE OF CERTIFICATEKEY USAGE
Digital Signature Certificate
Certificate of AuthenticationNon Repudiation

8.2 Private key protection and engineering controls of cryptographic modules

8.2.1 Controls and standards for cryptographic modules

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

8.2.2 Private key multi-person (n of m) control

The private keys, of the DCE GSE Root and the private keys of the DCE GSE subordinates, are under multi-person control. The method of activation of the private keys is by initialization of the DCE GSE software by means of a combination of keys held by multiple persons.

8.2.3 Custody of the private key

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

The technical data of the device are as follows:

- SafeNet Luna SA

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

8.2.4 Private key backup

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

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

8.2.5 Private key file

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

They are located in a cryptographic backup box in a different location than the HSMs.

8.2.6 Private key transfer from cryptographic module

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

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

8.2.7 Storage of private keys in a cryptographic module

DCE GSE private keys 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 security level (See 8.2.3 Custody of the private key).

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

8.2.8 Private key activation method

The private keys, of the GSE Root DCE and the Subordinate ECDs, are under multi-person control. The method of private key activation is by initialization of the DCE GSE software by means of a combination of keys held by multiple operators.

Multi-person control is required for DCE private key activation. At least 2 persons are required for key activation.

8.2.9 Private key deactivation method

The private key is deactivated by deactivating the software or shutting down the DCE server. It is activated again by using multi-person control, following the procedures marked by the manufacturer of the cryptographic module.

8.2.10 Method to destroy the private key

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

8.2.11 Technical characteristics of the cryptographic modules used

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

8.2.12 Evaluation of the cryptographic module

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

8.2.13 Evaluation of the encryption system

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

8.3 Other aspects of key pair management

8.3.1 Public key file

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

8.3.2 Certificate operating periods and key pair usage period

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

RSA ALGORITHM:

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

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

ECDSA ALGORITHM:

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

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

8.4 Activation data

8.4.1 Generation and installation of activation data

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

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

8.4.2 Protection of activation data

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

8.4.3 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.

8.5 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 configuration.
- Access control to the devices.
- Closure of system vulnerabilities.
- Hardenization of the systems according to best practices.
- Network configuration at security level (DMZ, Internal Network, Administrative Network, among others).
- Correct sizing of the system.
- Configuration of Users and permissions.
- Log event configuration.
- Backup and recovery plan.
- Service continuity plan
- Antivirus configuration.
- Network traffic requirements.

8.5.1 Specific technical safety requirements

DCE GSE has a technological infrastructure duly monitored and equipped with the security elements required to guarantee high availability 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 knowledge of it.

8.5.2 Computer security assessment

The Paynet SAS supplier's information security management system evaluates the processes related to the technological infrastructure in order to identify possible weaknesses and define continuous improvement plans with the support of periodic audits.

Equipment security is supported by an initial risk analysis in such a way that the security measures implemented are a response to the probability and impact produced when a group of defined threats can take advantage of security breaches.
This analysis is performed periodically in order to identify possible vulnerabilities in the systems.

8.5.3 Actions in case of an information security event or incident

The information security management system implemented by DCE GSE has established an incident management procedure for both the CA and the RA that specifies the actions to be taken, components or resources to be used and how the personnel should react in the event of an intentional or accidental event that disables or degrades DCE GSE's digital certification resources and services.

a. Incident detection and reporting: Security incidents should be reported through seguridad.informacion@gse.com.co, which is managed by the DCE GSE Information Security Officer.
   Incidents may be detected through monitoring systems, intrusion detection systems, system logs, notification by staff or by subscribers and/or managers.
b. Incident analysis and evaluation: 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, i.e. to find out the extent of the attack and the maximum possible information about the incident.
c. Incident damage control: React quickly to contain the incident and prevent it from spreading by taking measures such as blocking access to the system.
d. Investigation and evidence gathering: Review audit records to follow up on what happened.
e. Recovery and countermeasures: Restore the system to its correct operation and document the procedure and ways to prevent the incident from recurring.
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.

8.6 Life cycle engineering controls

8.6.1 System development controls

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

8.6.2 Security management controls

DCE GSE maintains control over the inventories of assets used in its certification process. These assets are classified according to their risk level.

DCE GSE regularly monitors its technical capacity in order to guarantee a high availability infrastructure.

8.6.3 Life cycle safety controls

DCE GSE has the proper security controls throughout the life cycle of the systems that have any impact on the security of digital certificates issued.

8.7 Network security controls

DCE GSE has a network infrastructure duly monitored and equipped with security elements required to ensure high 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 knowledge of it.

8.8 Chronological stamping

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

9. COMPLIANCE AUDIT AND OTHER CONTROLS

9.1 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 performed by an external audit firm.

9.2 Auditor identity/qualifications

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

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

9.3 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 auditing firm exercises its absolute independence in the performance of its auditing activities and there is no conflict of interest as the relationship is purely contractual.

9.4 Aspects covered by the controls

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

9.5 Actions to be taken as a result of deficiency detection

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

9.6 Communication of results

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

10. DESCRIPTION OF PRODUCTS AND SERVICES

TYPE OF CERTIFICATE	OBJECT
Certificate of Company Membership	It guarantees the identity of the natural person who holds the certificate, as well as his or her link to a specific legal entity by virtue of the position he or she holds in it. This certificate does not in itself The same is the case for the holder, who has greater powers than those he/she possesses for the performance of his/her usual activity.
Company Representation Certificate	It is issued in favor of a natural person representing a specific legal entity. The certificate holder identifies himself not only as a natural person belonging to a company, but also adds his qualification as its legal representative.
Public Function Certificates	It guarantees the identity of the natural person who holds the certificate, as well as his or her link to a Public Administration by virtue of his or her rank as a public official. This certificate shall not in itself grant greater powers to its holder than those he/she possesses by virtue of the performance of his/her duties as a public servant. of its usual activity.
Certified Professional Certificates	It guarantees the identity of the natural person who holds the certificate, as well as his or her status as a qualified professional. This certificate will not grant by itself greater powers to its holder than those possessed by the

TYPE OF CERTIFICATE	OBJECT
	performance of his usual activity in the scope of his profession.
Natural Person Certificates	It guarantees only the identity of the natural person.
Electronic Invoice Certificates for natural persons	Exclusive certificate for electronic invoicing to meet the needs of individuals seeking the security of the certificate for the issuance of electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment supports, adjustment notes of the electronic payroll payment support document and other documents resulting from the processes of the unattended platforms of the technological suppliers approved by the DIAN, the DIAN's free invoicing system and the DIAN platform. RADIAN, in compliance with the technical annexes issued by said entity.
Electronic Invoice Certificates for legal entities	Exclusive certificate for electronic invoicing to meet the needs of companies seeking the security of the certificate for the issuance of electronic invoices. Exclusive certificate for the digital signature of electronic invoices, credit notes, debit notes, electronic payroll payment supports, adjustment notes of the electronic payroll payment support document and other documents resulting from the processes of the unattended platforms of the technological suppliers approved by the DIAN, the DIAN's free invoicing system and the DIAN platform. RADIAN, in compliance with the technical annexes issued by said entity.
Legal Person Certificate	Carrying out business procedures by an application running on a machine in automatic and unattended signature processes on behalf of a legal entity of public or private law that requires guaranteeing the authenticity and integrity of the data sent or stored digitally together with the establishment of secure communication channels between clients, and that will be represented by a natural person (Responsible), holder of the certificate issued under this policy and called Responsible.
Generation of Certified Electronic Signatures	Exclusive certificate for the generation of certified electronic signatures.

TYPE OF CERTIFICATE	OBJECT
Certified e-mail service	The certified e-mail service ensures the sending, receiving and receipt of e-mails. y verification of 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 another data message to a specific time or time period, which allows to establish with a proof that this data existed at that time or time period and that it did not undergo any modification from that time in which the stamping was performed.
Electronic Document Archiving and Retention Service Transferable and Message Data	Service consists of a secure and encrypted storage space that can be accessed with credentials or a digital certificate. The documentation stored in this platform will have probative value as long as it is digitally signed.

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

11. OTHER LEGAL AND COMMERCIAL MATTERS

11.1 Rates

11.1.1 Certificate issuance or renewal fees

Product detail	Delivery time	Validity	Price (Cop) without Taxes	Taxes	Total
Natural Person Certificate	Normal	1	$ 191.597	$ 36.403	$ 228.000
Natural Person Certificate	Normal		$ 277.310	$ 52.689	$ 329.999
Certificate Belonging to company	Normal	1	$ 191.597	$ 36.403	$ 228.000
Certificate Belonging to company	Normal		$ 277.310	$ 52.689	$ 329.999
Qualified Professional Certificate	Normal	1	$ 191.597	$ 36.403	$ 228.000
Qualified Professional Certificate	Normal		$ 277.310	$ 52.689	$ 329.999
Legal Representative Certificate	Normal	1	$ 191.597	$ 36.403	$ 228.000
Legal Representative Certificate	Normal		$ 277.310	$ 52.689	$ 329.999
Civil Service Certificate	Normal	1	$ 191.597	$ 36.403	$ 228.000
Civil Service Certificate	Normal		$ 277.310	$ 43.907	$ 274.999
Legal Entity Certificate	Normal	1	$ 504.202	$ 95.798	$ 600.000
Legal Entity Certificate	Normal		$ 857.143	$ 162.857	$ 1.020.000

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

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

11.1.2 Certificate access fees

Access to the consultation of the status of issued certificates is free and free of charge and therefore no fee applies.

11.1.3 Fees for revocation or access to status information

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

11.1.4 Rates for other services

Once other services are offered by GSE, they are posted on the services' PCs on the GSE website.

11.1.5 Return policy

Please refer to the Returns Policy published on the GSE website (https://gse.com.co/Nosotros/politicas).

11.2 Warranties

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

The DCE GSE will act in the coverage of its liabilities by itself or through the insurance entity, satisfying the requirements of the certificate applicants, subscribers/responsible parties and third parties relying on the certificates.

The responsibilities of the DCE GSE include those established in this CPS, as well as those applicable as a result of Colombian and international regulations.

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

- The accuracy of all information contained in the certificate at the date of issuance.
- The guarantee that, at the time of delivery of the certificate, the Subscriber holds the private key corresponding to the public key given or identified in the certificate.
- The guarantee that the public and private key work together and complementarily.

- The correspondence between the certificate requested and the certificate delivered.
- Any liability established by current legislation.

11.3 Fairness and Non-Discrimination

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

- The Management Committee and the employees of GSE declare that they do not participate directly or indirectly in services or activities that may jeopardize free competition, accountability and transparency.
- Employees will use preventive and corrective actions to respond to any risk that compromises the company's impartiality.
- The collaborators that are part of the accredited digital certification services may not provide consulting services, nor involve the development team to provide technical support services to the subscriber or customer.
- GSE is responsible for impartiality in the conduct of its activities and does not allow commercial, financial or other pressures to compromise its impartiality.
- GSE will not issue digital signature certificates to natural or legal persons related to groups outside the law or that develop illegal activities.
- GSE may decline to accept an application or maintain a contract for certification when there are substantiated, demonstrated or improper reasons on the part of the applicant and/or subscriber.
- GSE offers access to a digital certification service that does not depend on the size of the applicant or subscriber or the membership of any association or group, nor should it depend on the number of certifications already issued.

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

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

11.4 Limits of liability

11.4.1. Responsibility for the accuracy 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 documents or incomplete or outdated information.

11.4.2. Liability for service availability

The Subscriber agrees to work diligently to minimize the possibility of failures or interruptions that may occur within its organization. Failures caused by the inability or inadequacy of the Subscriber's equipment, or by his lack of knowledge in the use of the service, shall in no case be attributable to DCE GSE and no compensation for any damage may be demanded from him.

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

The Subscriber shall be solely responsible for the provision and payment of the costs necessary to ensure the compatibility of the service (digital signature certificate) with 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, access and connection to the Internet, links, browsers, or other programs, equipment and services required to access and use the service, including, but not limited to, telecommunications services, access and connection to the Internet, links, browsers, or other programs, equipment and services required to access and use the service Internet, links, browsers, or other programs, equipment and services required to access and use the service.

11.4.4. Liability for computer crimes

In the event that the Subscriber is victim of any of the behaviors typified 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, etc., the Subscriber shall be solely responsible and shall be liable for any damages that may arise, since it is its obligation to adopt security measures, policies, cultural campaigns, cultural campaigns, legal instruments and other legal instruments, as appropriate, due to negligence in the handling and confidentiality of the digital certificate, it will be the only responsible and shall be liable for the damages that may arise, since it is its obligation to adopt security measures, policies, cultural campaigns, legal instruments and other mechanisms to safeguard the confidentiality and proper use of its digital certificate.

11.4.5. Warranty disclaimers

DCE GSE no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales, terrorismo, huelgas o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente DPC y sus Anexos.
- Por el uso indebido o fraudulento de los certificados o CRL’s emitidos por la Autoridad de Certificación.
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el incumplimiento de las obligaciones establecidas para el Suscriptor, Entidades, Responsables o Terceros que confían en la normativa vigente, lapresente DPC y sus Anexos.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación

/suspensión.

- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Suscriptoro Entidad.
- Fraude en la documentación presentada por el solicitante.

11.5 Financial and legal responsibilities

11.5.1 Other goods

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

11.5.2 Insurance or guarantee of coverage for subscribers, responsible and third parties in good faith

In compliance with Article 9°. Guarantees, of Decree 333 of 2014, DCE GSE has acquired insurance issued by an insurance company authorized to operate in Colombia, which covers all contractual and extra-contractual damages of subscribers, responsible parties and third parties in good faith exempt from fault arising from errors and omissions, or acts of bad faith of managers, legal representatives or employees of DCE GSE in the development of the activities for which it has authorization.

11.6 Confidentiality of information

11.6.1 Responsibility to protect confidential information

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

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

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

11.6.2 Confidential information

The following information is considered confidential:

a. Private key of the Certification Authority and/or ECD
b. Subscriber's or entity's private key
c. Information provided by the subscriber or entity and not necessary to validate the subscriber's or entity's confidence
d. Information about the applicant, subscriber and/or responsible party obtained from different sources (e.g., from a complainant or regulators).
e. Transaction records
f. Audit records
g. Security policies
h. Business Continuity Plan
i. All information that is classified as "Confidential" in the documents provided by DCE GSE.

11.6.3 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 qualified as "PUBLIC" in the documents provided by DCE GSE.

11.6.4 Duty to protect confidential information

DCE GSE maintains security measures to protect all confidential information provided to DCE GSE directly or through the channels established for this purpose from its receipt to its storage and custody, where it will remain for 10 years. DCE GSE has an Integrated Management System that includes an Information Security System. This allows us to ensure that our subscribers' information will not be compromised or disclosed to third parties unless formally requested by a competent authority.

11.7 Protection of personal information

11.7.1 Personal Data Processing Policy

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

11.7.2 Information treated as private

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

11.7.3 Information not classified as private

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

11.7.4 Responsibility for personal data protection

DCE GSE is responsible and has adequate technological resources to help ensure the proper custody and preservation of personal data collected through the channels used by the company, in compliance with Law 527 of 1999 "Article 32. Certification entities shall have, among others, the following duties: Guarantee the protection, confidentiality and proper use of the information provided by the subscriber, responsible party and entity".

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

11.7.5 Notification and consent to the use of personal data

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

11.7.6 Disclosure in the context of an administrative or judicial process

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

11.7.7 Other disclosure circumstances

DCE GSE has as its privacy policy the strictly established in the data protection law: "Private information shall be that which, because it concerns personal information or not, and

because it is in a private area, can only be obtained or offered to third parties authorized by the Subscriber or responsible or by law".

11.7.8 Security system to protect information

The following validations are performed on the system that houses the information provided by the subscriber or person responsible for the certification service:

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 of the network, performed by a company specialized in Ethical Hacking.

11.8 Intellectual property rights

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

11.9 Obligations

11.9.1 DCE GSE Obligations

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

a) Respect the provisions of current regulations, this CPS and the CP Certification Policies.
b) Publish this CPS and each of the Certification Policies on the GSE website.
c) Inform ONAC about modifications to the CPS and Certification Policies.
d) Maintain the CPS with its latest version published on the GSE website.
e) Protect and safeguard your private key in a secure and responsible manner.
f) Issue certificates in accordance with the Certification Policies and standards defined in this CPS.
g) Generate certificates consistent with the information provided by the applicant or subscriber.
h) Keep the information on digital certificates issued in accordance with current regulations.
i) Issue certificates whose minimum content is in accordance with current regulations for 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 applicant's or subscriber's private key.
l) Revoke digital certificates as provided in the Digital Certificate Revocation Policy.
m) Update and publish the list of revoked digital certificates CRL with the last revoked certificates.
n) Notify the Applicant, Subscriber or Entity of the revocation of the digital certificate within 24 hours after the revocation of the certificate in accordance with the digital certificate revocation policy.
o) Inform subscribers of the proximity of the expiration of their digital certificate.
p) Have qualified personnel, with the necessary knowledge and experience to provide the certification service offered by the DCE GSE.
q) Provide the applicant on the DCE GSE website the following information free of charge and free access:
    - The Policies and Certification Practices Statement and all its updates.
    - Obligations of the subscriber and the way in which the data must be kept.
    - Procedure to request the issuance of a certificate.
    - The procedure for revocation of your certificate.
    - The conditions and limits of use of the certificate.
r) Verify by itself or through a different person acting in its name and on its behalf, the identity and any other circumstances of the applicants or certificate data, which are relevant for the purposes of the verification procedure prior to its issuance.
s) Immediately inform the Superintendency of Industry and Commerce and ONAC of the occurrence of any event that compromises or may compromise the provision of the service.
t) Inform in a timely manner the modification or update of services included in the scope of accreditation, under the terms established in the procedures, rules and requirements of ONAC's accreditation service.
u) Update contact information whenever there is a change or modification in the data provided.
v) Train and warn its users on the security measures to be observed and on the logistics required for the use of the mechanisms for the provision of the service.
w) Guarantee the protection, integrity, confidentiality and security of the information provided by the subscriber, preserving the documentation that supports the certificates issued.
x) Guarantee the conditions of integrity, availability, confidentiality and security, in accordance with current national and international technical standards and with the specific accreditation criteria established by ONAC for this purpose.
y) Provide the services that are accredited on the DCE GSE website.

11.9.2 Obligations of the RA

The RA of the DCE GSE is in charge of performing the identification and registration work, therefore, the RA is obliged in the terms defined in this Certification Practices Statement to:

a) Know and comply with the provisions of this CPS and the Certification Policies

corresponding to each type of certificate.
b) Custody and protection of your private key.
c) Verify the identity of the applicants, responsible or subscribers of digital certificates.
d) Verify the accuracy and authenticity of the information provided by the Applicant.
e) File and keep custody of the documentation provided by the applicant or subscriber for the issuance of the digital certificate, during the time established by the legislation in force.
f) Respect the provisions of the contracts signed between DCE GSE and the subscriber.
g) Identify and report to the DCE GSE the causes of revocation provided by the applicants on the digital certificates in force.

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

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

a) Use your digital certificate or electronic signature certificate according to the terms of this CPS.
b) Verify within the next business day that the digital certificate information is correct. In case of inconsistencies, notify the ECD.
c) Refrain from: lending, transferring, writing, publishing the password for use of its digital certificate and take all necessary, reasonable and appropriate measures to prevent it from being used by third parties.
d) Do not transfer, share or lend the cryptographic device to third parties.
e) Provide all the information required in the application form for digital certificates to facilitate their timely and full identification.
f) Request the revocation of the digital certificate in the event of a change of name and/or surname.
g) Request the revocation of the digital certificate when the Subscriber has changed its nationality.

h) Comply with what has been accepted and/or signed in the terms and conditions document.
i) Provide accurate and truthful information as required.
j) To inform during the validity of the digital certificate any change in the data initially provided for the issuance of the certificate.
k) Responsible custody and protection of your private key.
l) Use the certificate of conformity with the CPs established in this CPS for each type of certificate.
m) Request as subscriber and/or responsible immediately the revocation of its digital certificate when it has knowledge that there is a cause defined in numeral Circumstances for the revocation of a certificate of the present CPS.
n) Not to make use of the private key or the digital certificate once its validity has expired or it has been revoked.
o) Inform trusted third parties of the need to check the validity of the digital certificates they are using at any given time.
p) Inform the bona fide third party of the status of a revoked digital certificate for which the list of revoked certificates CRL, published periodically by DCE GSE, is available.
q) Not to use its digital certification in a way that contravenes the law or brings DCE into disrepute.
r) Not to make any statement related to its digital certification in the DCE GSE that it may consider misleading or unauthorized, as provided by this CPS and CP.
s) Once the digital certification service has expired or been revoked, the subscriber must immediately stop using it in all advertising material containing any reference to the service.
t) The subscriber when referring to the digital certification service provided by DCE GSE in media, such as documents, brochures or advertising, must inform that it complies with the requirements specified in the CPs of this CPS, indicating the version.
u) The subscriber may use the marks of conformity and the information related to the digital certification service provided by DCE GSE in the following media communication, such as documents, brochures or advertising, since it complies with the requirements of the preceding paragraph.

11.9.4 Obligations of Bona Fide Third Parties

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

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

11.9.5 Obligations of the Entity (Client)

In accordance with the provisions of the CPs related in this document, in the case of certificates where the subscriber's and/or responsible party's relationship with the Entity is accredited, it shall be the Entity's obligation:

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

11.9.6 Obligations of other DCE participants

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

a) Review the consistency of the CPS with current regulations.
b) Approve and decide the changes to be made to the certification services, due to regulatory decisions or requests from subscribers or responsible parties.
c) Approve the notification of any change to subscribers and/or responsible parties analyzing its legal, technical or commercial impact.
d) Review and take action on any comments made by subscribers or managers when a change in the certification service is made.
e) Report action plans to ONAC on any changes that have an impact on the PKI infrastructure and affect digital certification services, in accordance with RAC-3.0-01.
f) Authorize the required changes or modifications to the CPS.
g) Authorize the publication of the CPS on the DCE GSE website.
h) Approve changes or modifications to the DCE GSE Security Policies.
i) Ensure the integrity and availability of the information published on the DCE GSE website.
j) Ensure the existence of controls over the DCE GSE's technological infrastructure.
k) Request the revocation of a digital certificate if it has knowledge or suspicion of the compromise of the private key of the subscriber, entity or any other fact that tends to the improper use of private key of the subscriber, entity or of the DCE itself.
l) Be aware of and take appropriate action when security incidents occur.
m) Perform a review of the CPS at least once a year to verify that the lengths of the keys and periods of the certificates being used are adequate.
n) Review, approve and authorize changes to certification services accredited by the competent body.

o) Review, approve and authorize the ownership and use of symbols, certificates and any other mechanism required by DCE GSE to indicate that the digital certification service is accredited.
p) Ensure that the accreditation conditions granted by the competent body are maintained.
q) Ensure the proper use in documents or any other publicity that the symbols, certificates, and any other mechanism indicating that DCE GSE has an accredited certification service and complies with the provisions of the ONAC Accreditation Rules.
r) Ensure that its critical suppliers and reciprocal DCEs, if any, are kept informed of the obligation to comply with the CEA requirements, in the corresponding items.
s) The Integrated Management System will implement corrective action plans and improvement actions to respond to any risk that compromises the fairness of the ECD, whether arising from the actions of any person, body, organization, activities, its relationships or the relationships of its personnel or itself, for which it uses the ISO 31000 standard for the identification of risks that compromise the fairness and non-discrimination of the ECD, providing the Management Committee with the mechanism that eliminates or minimizes such risk, on an ongoing basis.
t) Ensure that all DCE staff and committees (whether internal or external) that may have an influence on certification activities act with impartiality and non-discrimination, especially those arising from commercial, financial or other pressures that compromise their impartiality.
u) Document and demonstrate commitment to fairness and non-discrimination.
v) Ensure that the administrative, management and technical personnel of the PKI, of the DCE 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 critical suppliers such as the DCE reciprocal and datacenter that meet DCE accreditation requirements are kept informed in order to support their contracting and compliance with administrative and technical requirements.

12. CPS AND PC TERMS AND CONDITIONS

12.1 Effectiveness of the CPS and CP

The CPS and CP come into force from the moment they are published on the DCE GSE website, from that moment the previous version of the document is repealed and the new version replaces the previous version in its entirety.

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

i. Effects of termination and commencement of effectiveness of the CPS and CP

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 statements of the previous version.

ii. Changes affecting CPS and PC

Any changes affecting the DCE GSE CPS and CP shall follow the following procedure:

a. The Management Committee shall approve the changes it deems pertinent to the CPS and CPs.
b. The updated CPS and CP is published on the DCE GSE website once authorized by the Management Committee.

iii. Circumstances under which the OID must be changed

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

a. The authorization of a new certification hierarchy, in which case the OIDs must be defined in accordance with the structure.
b. In case of changes in the DPC and PC that affect the acceptability of digital certification services, the OID adjustment is made.

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

12.2 Effects of termination and commencement of effectiveness of the CPD and CP

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 statements of the previous version.

12.3 Notification and communication

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

12.4 CPD and CP Change Procedure

12.4.1 Changes affecting the CPD and CP

Any changes affecting the DCE GSE CPD and CP will follow the following procedure:

a. The Management Committee will approve any changes it deems appropriate to the CPD and CPs.
b. The updated CPD and CP is published on the DCE GSE website once it is authorized by the Management Committee.

12.4.2 Circumstances under which the OID must be changed

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

a. The authorization of a new certification hierarchy, event in which the OIDs shall be defined according to the structure.
b. In the event of changes to the CPD and CP that affect the acceptability of digital certification services proceed to make the OID adjustment.

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

12.5 Dispute Prevention and Resolution

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

12.5.1 Applicable Law

The operation and operations performed by the Certification Authority Paynet SAS, as well as this Certification Practices Statement and the Certification Policies applicable to each type of certificate are subject to the applicable regulations 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 the certification entities and other provisions.
b. Decree 333 of 2014, which regulates Article 160 of Decree-Law 19 of 2012 regarding the characteristics and requirements of certification entities, and what is related to digital certificates.
c. Chapters 47 and 48 of Title 2 of Part 2 of Part 2 of Book 2 of the Sole Decree of the Commerce, Industry and Tourism Sector - DURSCIT.

12.6 Compliance with applicable law

DCE GSE declares compliance with Law 527 of 1999 and that the Certification Practice Statement is satisfactory in accordance with the requirements established by the National Accreditation Organization of Colombia

13. CERTIFICATION POLICIES

The interrelation between this CPS and the Certification Policy of the different certificates is fundamental. And this, to the extent that:

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

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

In short, the policy defines "**what**" requirements are necessary for the issuance of the different DCE 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 listed:

- Certificate Policies for Digital Certificates

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.4.12

Location of the CPS	https://gse.com.co/documentos/calidad/politicas/Certificate_Policies_for_Digital_Certificate_Services_V12.pdf

- Certificate Policies for Time Stamping Service

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.2.11
Location of the PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_Certificado_pfor_Chronological_Stamping_Service_V11.pdf

- Certificate Policies for Archiving and Retention Service for Electronic Transferable Documents and Data Messages.

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.3.11
Location of the PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_Certificado_para_Data_Archiving_Reliable_Archive_Service_V11.pdf

- Certificate Policies for Certified Email Service

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.5.11
Location of the PC	https://gse.com.co/documentos/calidad/politicas/Politica_Certificado_para_Electronic_Mail_Service_Certificate_V11.pdf

- Certified Electronic Signature Generation Policies

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.6.3
Location of the PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_Generacion_de_Electronic_Signatures_Certified_V3.pdf

14. ANNEX 1 DPC MATRIX MATRIX TECHNICAL PROFILE DIGITAL CERTIFICATES

15. ANNEX 2 DPC MODELS AND MINUTES OF TERMS AND CONDITIONS DOCUMENTS

16. ANNEX 3 CPS MATRIX PROFILE TECHNICIAN CERTIFICATES ELECTRONIC SIGNATURE