

Digital Certification Entity




Certification Practice Statement for Certificate Issuance


Document Information


Name	CERTIFICATION PRACTICE STATEMENT FOR CERTIFICATE ISSUANCE
Performed by	THOMAS SIGNE S.A.S.
Country	COLOMBIA
Version	2.8
Date	JULY, 2023
Document Type	PUBLIC
Code	THS-CO-AC-DPC-01


Document Version

Version	Date	Description
1.0	06/28/2017	Preparation of initial document.
1.1	01/03/2018	Inclusion and adaptation of new structures and procedures.
1.2	05/08/2018	Corrections and clarifications in sections of the document.
1.3	05/20/2018	Applicable technical standards are specified. The uses of the Root CA's private key are added. The certificate life cycle process is detailed.
1.4	05/22/2018	Minor modification in the section on DCE Identification and Provider Obligations. Permitted uses of the digital certificate are added. Specifications in the Security Controls section.
1.5	06/08/2018	Sections for applicable formats and records have been added.
1.6	11/02/2018	The reference to THS-PR-GRAL-02-F01 Document Structure v1.0 has been removed from the footer.
1.7	01/22/2019	The possibility has been added for the RO to optionally verify the Applicant's identity in person, instead of by videoconference. Minor corrections.

	Certification Practice Statement for Certificate Issuance		Version 2.8
	Code: THS-CO-AC-DPC-01		Page 3 of 67
1.8	05/09/2019	<p>Integration with the Group's management system</p> <p>Document name change from THS-DP-CER-01 to THS-CO-CPS-AC-01.</p> <p>Thomas Signe Root is added as a PKI participant of Thomas Signe S.A.S. (see section 3.2.1).</p> <p>Removed sections on applicable formats and records.</p> <p>Minor corrections.</p>	
1.9	09/18/2019	<p>Adjustment of the coding according to GSIGNE-GRAL-PR-01 Control of Documented Information Ed 2.1.</p> <p>In the Component Certificates, the possibilities that the Subscriber can be a Natural Person and that the Applicant can be a Legal Person different from the Subscriber are added.</p> <p>In the certificate request, depending on the type of certificate, the required document is added as the citizenship or foreigner's identification card of the Legal Representative, in addition to the authorization signed by him/her with the data of the Natural Person or the Legal Entity authorized to request and obtain a digital certificate.</p> <p>In the review of the certificate request, in the validation of the identity document of the Applicant (Natural Person), the consultation before a Database for Natural Persons is eliminated.</p> <p>The Formats and Records sections have been added.</p> <p>Minor corrections.</p>	
1.10	11/29/2019	<p>Changes in the identification data of the DCE and its suppliers, including the certificate of existence and legal representation and the active status in the Chamber of Commerce or equivalent.</p> <p>It is indicated that the continuity and contingency plan has been established and tested.</p> <p>The Applicants, Subscribers, Third Party acceptors or the general public may only indicate their PQRSA by sending an email to the email address pqrsa@thsigne.com.</p> <p>DCE's responsibility to inform its suppliers that it extends compliance with the requirements of CEA 4.1-10 is added.</p> <p>Change of the current account number to make the deposit of the respective amount for each service.</p> <p>Added format and record for identity verification videoconferences.</p> <p>Minor corrections.</p>	


	Certification Practice Statement for Certificate Issuance		Version 2.8
	Code: THS-CO-AC-DPC-01		Page 4 of 67
2.0	01/31/2020	<p>General review of the content of the CPS based on the applicable legislation and regulations and the content of the Management System documentation by a multidisciplinary work team.</p> <p>Changes in the organization of the document content to follow the recommendations of the RFC 3647 standard.</p> <p>In Component Certificates, the Subscriber may be a company or entity Natural Person and the Applicant may be a company or entity Natural Person other than the Subscriber.</p> <p>In the case of Company Membership Certificates, the possibility is added that the Entity to which the Subscriber (Natural Person) is linked may be a company or entity Natural Person.</p> <p>The current account number for the deposit of the respective amount for each service is eliminated (to be indicated in the Commercial Proposal).</p>	
2.1	06/19/2020	<p>Adjustments in the title of the document.</p> <p>The obligations of the Entity to which the Subscriber is bound are added.</p> <p>Minor corrections.</p>	
2.2	11/06/2020	<p>The revocation reasons that can be selected when processing the revocation of a certificate in the RA are indicated.</p> <p>The methods of activation and deactivation of the private key are described in more detail.</p> <p>The responsibilities of the DCE to inform Applicants, Subscribers, Relying Third Parties and the general public on the Thomas Signe S.A.S. website of the activities and services accredited in accordance with the provisions of the current ONAC document RAC-3.0-03, and of the general information of the company, such as its nature, type of company, etc., are added.</p> <p>A format and a record for the document retention table are added. Minor corrections.</p>	
2.3	06/24/2021	<p>Rebranding of Thomas Signe.</p> <p>Names of certificate types are changed.</p> <p>The Card/Token support, which was limited to certificates of the RA trusted roles, is eliminated and replaced by certificates in the Centralized HSM support.</p> <p>The possibility is added that the type of identity document of the Legal Representative of the Legal Entity or of the Natural Person, of the Subscriber or of the Entity to which the Subscriber is affiliated, may be the Passport.</p> <p>New circumstances are added for the revocation of a certificate.</p> <p>The request for revocation of certificates by the DCE itself, through internal procedures, has been added.</p>	

	Certification Practice Statement for Certificate Issuance		Version 2.8
	Code: THS-CO-AC-DPC-01		Page 5 of 67
		<p>Online revocation checking requirements by OCSP is added.</p> <p>Multi-person control for access to Root CA and Subordinate CA private keys is described in more detail.</p> <p>Changes in the method of destruction of the private key of the CAs, so that the rest of the keys managed by the hardware cryptographic devices used (HSM) are not affected.</p> <p>Added a section on responsibility in the protection of confidential information.</p> <p>Minor corrections.</p>	
2.4	11/19/2021	<p>The fax is removed from the identification data of DCE Thomas Signe S.A.S. and its suppliers.</p> <p>S.A.S. and its suppliers.</p> <p>Changes in the operational requirements for the life cycle of certificates and in the trust roles, to ensure independence and impartiality between the review and decision functions of digital certification (certificate issuance), and to document the processes and results related to the review, including the recommendation for decision based on the review.</p> <p>Certificate revocations requested through internal procedures and e-mail are handled by RA Decision Operators instead of Registry Operators.</p> <p>Custody of private keys and backup copies of private keys of Subscriber certificates in Centralized HSM is added.</p> <p>The obligations of Relying Third Parties are specified in more detail.</p> <p>It is added that changes in the content of this CPS and associated CPs that could affect the acceptance of the services will be notified in advance to the interested parties.</p> <p>Minor corrections.</p>	
2.5	07/08/2022	<p>Adaptation to the new version of CEA-3.0-07. Added subscriber's rights.</p> <p>Updated means of revocation. Modification of contractual documentation. Added alternative time source.</p> <p>Changed the PQRS procedure in line with the new CEA version.</p>	
2.6	30/09/2022	<p>Phone numbers updated in line with the new prefix.</p> <p>Adjustment in the review and request of the certification services.</p> <p>Update of regulations and standards used.</p> <p>Video identification process included.</p>	
2.7	20/01/2023	<p>CA private key archiving defined.</p> <p>CRL archive time defined.</p> <p>Certificate distribution included.</p>	
2.8	03/07/2023	<p>Review and minor changes</p>	


	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 6 of 67

Contents


1	INTRODUCTION	12
1.1	PRESENTATION OF THE DOCUMENT	12
1.2	DOCUMENT NAME AND IDENTIFICATION	12
1.3	THOMAS SIGNE S.A.S. PKI PARTICIPANTS.....	12
1.3.1	THOMAS SIGNE S.A.S. PKI CERTIFICATE HIERARCHY	12
1.3.2	THOMAS SIGNE ROOT	13
1.3.3	DCE THOMAS SIGNE S.A.S. (DCE THOMAS SIGNE COLOMBIA).....	14
1.3.4	APPLICANT.....	15
1.3.5	SUBSCRIBER	15
1.3.6	THIRD PARTY WHO TRUSTS.....	16
1.3.7	ENTITY TO WHICH THE SUBSCRIBER IS RELATED	16
1.4	TYPES AND USES OF CERTIFICATES	16
1.4.1	PERSONAL CERTIFICATES.....	16
1.4.2	CORPORATE CERTIFICATES.....	16
1.4.3	APPROPRIATE USES OF CERTIFICATES.....	17
1.4.4	UNAUTHORIZED USES OF CERTIFICATES	17
1.5	CPS AND CP ADMINISTRATION.....	17
1.5.1	RESPONSIBLE ORGANIZATION	17
1.5.2	CONTACT DETAILS	17
1.5.3	APPROVAL PROCEDURE.....	18
1.6	DEFINITIONS AND ABBREVIATIONS	18
1.6.1	DEFINITIONS.....	18
1.6.2	ACRONYMS.....	20
2	RESPONSIBILITIES REGARDING REPOSITORIES AND PUBLICATION OF INFORMATION.....	21
2.1	REPOSITORIES.....	21
2.2	PUBLICATION OF CERTIFICATION INFORMATION.....	22
2.2.1	TIMING OR FREQUENCY OF PUBLICATION.....	22
2.2.2	REPOSITORY ACCESS CONTROLS	22
3	IDENTIFICATION AND AUTHENTICATION.....	22
3.1	NAMES.....	22
3.1.1	TYPES OF NAMES.....	22
3.1.2	NEED FOR NAMES TO HAVE MEANING.....	22
3.1.3	ANONYMITY AND PSEUDO-ANONYMITY OF SUBSCRIBERS.....	23
3.1.4	UNIQUENESS OF NAMES	23
3.1.5	RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS.....	23
3.2	INITIAL VALIDATION OF IDENTITY	23
3.2.1	METHOD OF PROOF OF POSSESSION OF THE PRIVATE KEY.....	23
3.2.2	AUTHENTICATION OF THE IDENTITY OF A COMPANY OR ENTITY.....	23
3.2.3	AUTHENTICATION OF AN INDIVIDUAL NATURAL PERSON'S IDENTITY	24

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 7 of 67


3.2.4	UNVERIFIED SUBSCRIBER AND APPLICANT INFORMATION	24
3.3	IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUESTS WITH CHANGE OF KEYS	24
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS	24
4	OPERATIONAL REQUIREMENTS FOR THE CERTIFICATE LIFECYCLE	25
4.1	CERTIFICATE REQUEST	25
4.1.1	WHO CAN REQUEST A CERTIFICATE	25
4.1.2	MARKETING.....	25
4.1.3	CONTRACTING AND PAYMENT	26
4.1.4	REQUEST	26
4.2	PROCESSING OF CERTIFICATE APPLICATIONS	27
4.2.1	REVIEW	27
4.2.2	DECISION.....	27
4.3	CERTIFICATE ISSUANCE	28
4.3.1	DCE ACTIONS DURING CERTIFICATE ISSUANCE	28
4.3.2	NOTIFICATION TO THE APPLICANT AND SUBSCRIBER BY THE DCE OF CERTIFICATE ISSUANCE	28
4.3.3	CERTIFICATE DISTRIBUTION	28
4.4	ACCEPTANCE OF THE CERTIFICATE.....	28
4.4.1	FORM IN WHICH THE CERTIFICATE IS ACCEPTED	28
4.4.2	PUBLICATION OF THE CERTIFICATE BY THE DCE	28
4.4.3	NOTIFICATION OF THE ISSUANCE OF THE CERTIFICATE BY THE DCE TO OTHER ENTITIES	28
4.5	USE OF KEYS AND CERTIFICATE.....	28
4.5.1	USE OF THE PRIVATE KEY AND CERTIFICATE BY THE SUBSCRIBER	28
4.5.2	USE OF THE PRIVATE KEY AND THE CERTIFICATE BY TRUSTED THIRD PARTIES.....	29
4.6	RENEWAL OF THE CERTIFICATE WITH CHANGE OF KEYS.....	29
4.7	RENEWAL OF THE CERTIFICATE WITH CHANGE OF KEYS.....	29
4.8	MODIFICATION OF CERTIFICATES	29
4.9	REVOCATION AND SUSPENSION OF CERTIFICATES	29
4.9.1	CONDITIONS FOR THE REVOCATION OF A CERTIFICATE.....	29
4.9.2	WHO CAN REQUEST A REVOCATION	30
4.9.3	REVOCATION REQUEST PROCEDURES	31
4.9.4	TIME PERIOD IN WHICH THE CA MUST PROCESS THE REVOCATION REQUEST	31
4.9.5	OBLIGATION FOR TRUSTED THIRD PARTIES TO VERIFY REVOCATIONS	31
4.9.6	FREQUENCY OF ISSUANCE OF CRL	31
4.9.7	MAXIMUM TIME BETWEEN THE GENERATION AND PUBLICATION OF CRL'S	31
4.9.8	AVAILABILITY OF ON-LINE CERTIFICATE STATUS VERIFICATION SYSTEMS.....	32
4.9.9	ONLINE REVOCATION CHECKING REQUIREMENTS.....	32
4.9.10	CRL ARCHIVE	33
4.10	CERTIFICATE STATUS INFORMATION SERVICES	33
4.10.1	OPERATIONAL CHARACTERISTICS	33
4.10.2	SERVICE AVAILABILITY	33
4.10.3	ADDITIONAL FEATURES	33
4.11	SUBSCRIPTION TERMINATION.....	33
4.12	KEY ESCROW AND RECOVERY	33
5	PHYSICAL, FACILITY, MANAGEMENT AND OPERATIONAL SECURITY CONTROLS.....	33

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 8 of 67


5.1	PHYSICAL CONTROLS	34
5.1.1	PHYSICAL LOCATION AND CONSTRUCTION.....	34
5.1.2	PHYSICAL ACCESS	34
5.1.3	POWER SUPPLY AND AIR CONDITIONING	34
5.1.4	WATER EXPOSURE.....	34
5.1.5	FIRE PREVENTION AND PROTECTION.....	35
5.1.6	STORAGE SYSTEM	35
5.1.7	DISPOSAL OF INFORMATION STORAGE MATERIAL	35
5.1.8	OFF-SITE BACKUPS.....	35
5.2	PROCEDURAL CONTROLS	35
5.2.1	TRUST ROLES.....	35
5.2.2	NUMBER OF PEOPLE REQUIRED PER TASK.....	36
5.2.3	IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE.....	36
5.2.4	ROLES REQUIRING SEGREGATION OF DUTIES.....	36
5.3	PERSONNEL CONTROLS.....	36
5.3.1	REQUIREMENTS FOR PROFESSIONAL QUALIFICATIONS, EXPERIENCE AND KNOWLEDGE.....	36
5.3.2	BACKGROUND CHECK PROCEDURE	37
5.3.3	TRAINING REQUIREMENTS.....	37
5.3.4	REQUIREMENTS AND FREQUENCY OF TRAINING UPDATES.....	37
5.3.5	PENALTIES FOR UNAUTHORIZED ACTIONS.....	37
5.3.6	REQUIREMENTS FOR HIRING THIRD PARTIES	37
5.3.7	DOCUMENTATION PROVIDED TO PERSONNEL.....	37
5.4	SAFETY AUDIT PROCEDURES.....	37
5.4.1	TYPES OF EVENTS RECORDED.....	37
5.4.2	AUDIT LOG PROCESSING FREQUENCY	38
5.4.3	AUDIT LOG RETENTION PERIOD.....	38
5.4.4	PROTECTION OF AUDIT LOGS	38
5.4.5	AUDIT LOG BACKUP PROCEDURES.....	38
5.4.6	AUDIT INFORMATION COLLECTION SYSTEM (INTERNAL OR EXTERNAL).....	38
5.4.7	VULNERABILITY ANALYSIS	39
5.4.8	OVERSIGHT	39
5.5	ARCHIVING OF RECORDS	39
5.5.1	TYPES OF RECORDS ARCHIVED.....	39
5.5.2	RECORDS RETENTION PERIOD.....	39
5.5.3	ARCHIVE PROTECTION.....	39
5.5.4	ARCHIVAL BACKUP PROCEDURES	39
5.5.5	REQUIREMENTS FOR TIME STAMPING OF RECORDS	39
5.5.6	AUDIT INFORMATION ARCHIVING SYSTEM (INTERNAL OR EXTERNAL).....	40
5.5.7	PROCEDURES FOR OBTAINING AND VERIFYING ARCHIVED INFORMATION.....	40
5.6	CHANGE OF PASSWORDS.....	40
5.7	INCIDENT AND VULNERABILITY MANAGEMENT PROCEDURES	40
5.7.1	RECOVERY IN CASE OF KEY COMPROMISE.....	40
5.7.2	BUSINESS CONTINUITY AFTER A DISASTER.....	41
5.8	TERMINATION OF THE CERTIFICATE ISSUANCE SERVICE	41

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 9 of 67


6	TECHNICAL SECURITY CONTROLS	41
6.1	KEY PAIR GENERATION AND INSTALLATION.....	41
6.1.1	KEY PAIR GENERATION	41
6.1.2	DELIVERY OF THE PRIVATE KEY TO THE APPLICANT OR SUBSCRIBER.....	41
6.1.3	DELIVERY OF THE PUBLIC KEY TO THE CERTIFICATE ISSUER	42
6.1.4	DELIVERY OF THE PUBLIC KEY OF THE DCE TO TRUSTED THIRD PARTIES.....	42
6.1.5	KEY SIZE AND VALIDITY PERIOD.....	42
6.1.6	PARAMETERS OF PUBLIC KEY GENERATION AND QUALITY VERIFICATION	42
6.1.7	SUPPORTED KEY USAGES (X.509 V3 KEY USAGE FIELD)	42
6.2	PRIVATE KEY PROTECTION AND ENGINEERING CONTROLS FOR CRYPTOGRAPHIC MODULES.....	42
6.2.1	CONTROLS AND STANDARDS FOR CRYPTOGRAPHIC MODULES.....	43
6.2.2	MULTI-PERSON (N OF M) CONTROL OF THE PRIVATE KEY	43
6.2.3	PRIVATE KEY ESCROW	43
6.2.4	PRIVATE KEY BACKUP	43
6.2.5	PRIVATE KEY ARCHIVING	43
6.2.6	TRANSFERRING THE PRIVATE KEY TO OR FROM A CRYPTOGRAPHIC MODULE	44
6.2.7	STORAGE OF THE PRIVATE KEY IN A CRYPTOGRAPHIC MODULE.....	44
6.2.8	PRIVATE KEY ACTIVATION METHOD	44
6.2.9	PRIVATE KEY DEACTIVATION METHOD	44
6.2.10	PRIVATE KEY DESTRUCTION METHOD	44
6.2.11	CLASSIFICATION OF CRYPTOGRAPHIC MODULES.....	45
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	45
6.3.1	PUBLIC KEY ARCHIVING	45
6.3.2	OPERATIONAL PERIOD OF THE CERTIFICATES AND PERIOD OF USE OF THE KEY PAIR.....	45
6.4	ACTIVATION DATA.....	45
6.4.1	GENERATION AND INSTALLATION OF ACTIVATION DATA.....	45
6.4.2	PROTECTION OF ACTIVATION DATA	45
6.4.3	IT SECURITY CONTROLS	46
6.4.4	SPECIFIC TECHNICAL SECURITY REQUIREMENTS.....	46
6.4.5	IT SECURITY ASSESSMENT	46
6.5	LIFE CYCLE SECURITY CONTROLS.....	46
6.5.1	SYSTEM DEVELOPMENT CONTROLS.....	46
6.5.2	SECURITY MANAGEMENT CONTROLS.....	46
6.6	NETWORK SECURITY CONTROLS.....	48
6.7	TIME STAMPING	48
7	CERTIFICATE, CRL AND OCSP PROFILES	48
7.1	CERTIFICATE PROFILE	48
7.1.1	CERTIFICATE FORMAT	48
7.1.2	CERTIFICATE EXTENSIONS	50
7.1.3	OBJECT IDENTIFIERS (OID) OF ALGORITHMS	51
7.1.4	NAME FORMATS.....	51
7.1.5	NAME RESTRICTIONS	52
7.1.6	CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)	52
7.1.7	USE OF POLICY CONSTRAINTS EXTENSION.....	52

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 10 of 67

7.1.8	SYNTAX AND SEMANTICS OF POLICY QUALIFIERS	52
7.1.9	SEMANTIC TREATMENT FOR CERTIFICATE POLICIES EXTENSION	53
7.2	CRL PROFILE.....	53
7.2.1	FORMAT AND VALIDITY PERIOD	53
7.2.2	CRL EXTENSIONS AND CRL INPUT EXTENSIONS	53
7.3	OCSP PROFILE.....	54
7.4	OCSP CERTIFICATE PROFILE	54
7.4.1	CERTIFICATE FORMAT	54
7.4.2	CERTIFICATE EXTENSIONS	54
7.4.3	OBJECT IDENTIFIERS (OID) OF ALGORITHMS	55
7.4.4	NAME FORMATS	55
7.4.5	NAME RESTRICTIONS	55
7.4.6	CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)	55
7.4.7	USE OF POLICY CONSTRAINTS EXTENSION.....	56
7.4.8	SYNTAX AND SEMANTICS OF POLICY QUALIFIERS	56
7.4.9	SEMANTIC TREATMENT FOR THE CERTIFICATE POLICY EXTENSION	56
8	COMPLIANCE AUDIT AND OTHER CONTROLS	56
8.1	AUDIT FREQUENCY.....	56
8.2	AUDITOR IDENTITY/QUALIFICATION.....	56
8.3	RELATIONSHIP BETWEEN THE AUDITOR AND THE AUDITED ENTITY	56
8.4	ASPECTS COVERED BY THE CONTROLS	56
8.5	ACTIONS TO BE TAKEN AS A RESULT OF DETECTION OF DEFICIENCIES	56
8.6	COMMUNICATION OF RESULTS	57
9	OTHER LEGAL AND BUSINESS MATTERS	57
9.1	FEEES.....	57
9.1.1	CERTIFICATE ISSUANCE FEES.....	57
9.1.2	CERTIFICATE ACCESS FEES	57
9.1.3	REVOCAATION OR ACCESS TO STATUS INFORMATION FEES.....	57
9.1.4	FEES FOR OTHER SERVICES	57
9.1.5	REFUND POLICY.....	57
9.2	FINANCIAL LIABILITIES.....	57
9.2.1	INSURANCE COVERAGE.....	57
9.3	CONFIDENTIALITY OF INFORMATION	58
9.3.1	CONFIDENTIAL INFORMATION	58
9.3.2	NON-CONFIDENTIAL INFORMATION	58
9.3.3	RESPONSIBILITY FOR THE PROTECTION OF CONFIDENTIAL INFORMATION	58
9.4	DATA PROTECTION POLICY	59
9.5	INTELLECTUAL PROPERTY RIGHTS.....	59
9.6	OBLIGATIONS AND RIGHTS.....	59
9.6.1	OBLIGATIONS OF DCE	59
9.6.2	OBLIGATIONS OF SUPPLIERS	60
9.6.3	OBLIGATIONS OF APPLICANTS.....	61
9.6.5	RIGHTS OF SUBSCRIBERS	61
9.6.6	OBLIGATIONS OF RELYING ON THIRD PARTIES.....	61

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 11 of 67

9.6.7	OBLIGATIONS OF THE ENTITY TO WHICH THE SUBSCRIBER IS BOUND	62
9.7	RESPONSIBILITIES	62
9.7.1	RESPONSIBILITIES OF THE DCE.....	62
9.7.2	RESPONSIBILITIES OF THE SUBSCRIBER	63
9.8	LIMITATION OF LIABILITY	63
9.9	INDEMNITIES.....	64
9.9.1	INDEMNITIES FOR DAMAGES CAUSED BY DCE	64
9.9.2	INDEMNITIES FOR DAMAGES CAUSED BY APPLICANTS, BY SUBSCRIBERS AND BY ENTRUSTED THIRD PARTIES	64
9.10	PERIOD OF VALIDITY	64
9.10.1	TERM.....	64
9.10.2	REPLACEMENT AND ABROGATION OF THE CPS AND CP	64
9.10.3	EFFECTS OF TERMINATION	65
9.11	PQRS.....	65
9.12	CHANGES IN CPS AND CP	65
9.13	DISPUTE RESOLUTION PROCEDURE	65
9.14	APPLICABLE LAW.....	65
9.15	COMPLIANCE WITH APPLICABLE LAW	65
9.16	MISCELLANEOUS STIPULATIONS.....	66
9.16.1	APPLICATION AND ACCEPTANCE DOCUMENT.....	66
9.16.2	FULL ACCEPTANCE CLAUSE.....	66
9.16.3	INDEPENDENCE.....	66
9.17	OTHER STIPULATIONS.....	66
10	FORMATS	66
11	RECORDS.....	67

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 12 of 67

1 INTRODUCTION

1.1 PRESENTATION OF THE DOCUMENT

This document constitutes the Certification Practices Statement (CPS) for the issuance of Thomas Signe S.A.S. certificates, in compliance with the Specific Criteria for Accreditation of Digital Certification Entities - CEA-43.0-07 established by the National Accreditation Body of Colombia - ONAC, in accordance with Colombian legislation and the provisions of the regulatory bodies.

This CPS establishes the practices carried out by Thomas Signe S.A.S. to issue, manage, revoke, and renew digital certificates, following the standard RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", and according to the following standards:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
- RFC 4523 - Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates

In addition to the practices established in this CPS, each type of certificate issued by Thomas Signe S.A.S. is governed by the requirements established in the corresponding Certificate Policy (CP).

Signe S.A.S. is governed by the requirements established in the corresponding Certificate Policy (CP). These CPs are published on the same Thomas Signe S.A.S. website as this document (see section 1.2).

This document is of a public nature and is addressed to all natural and legal persons, Applicants, Subscribers, Trusting Third Parties, and the public.

If vulnerabilities are detected, or the technical standards or infrastructure indicated in this CPS are no longer valid, Thomas Signe S.A.S. will inform ONAC of this fact, to proceed with the respective update.

1.2 DOCUMENT NAME AND IDENTIFICATION

The identification data of the present document are specified in the initial table *Identification of the document*. Additionally, the present document is identified with the following OID.


CPS OID FOR THE ISSUANCE OF CERTIFICATES OF THOMAS SIGNE S.A.S.	
1.3.6.1.4.1.51362.0.0.1	CPS

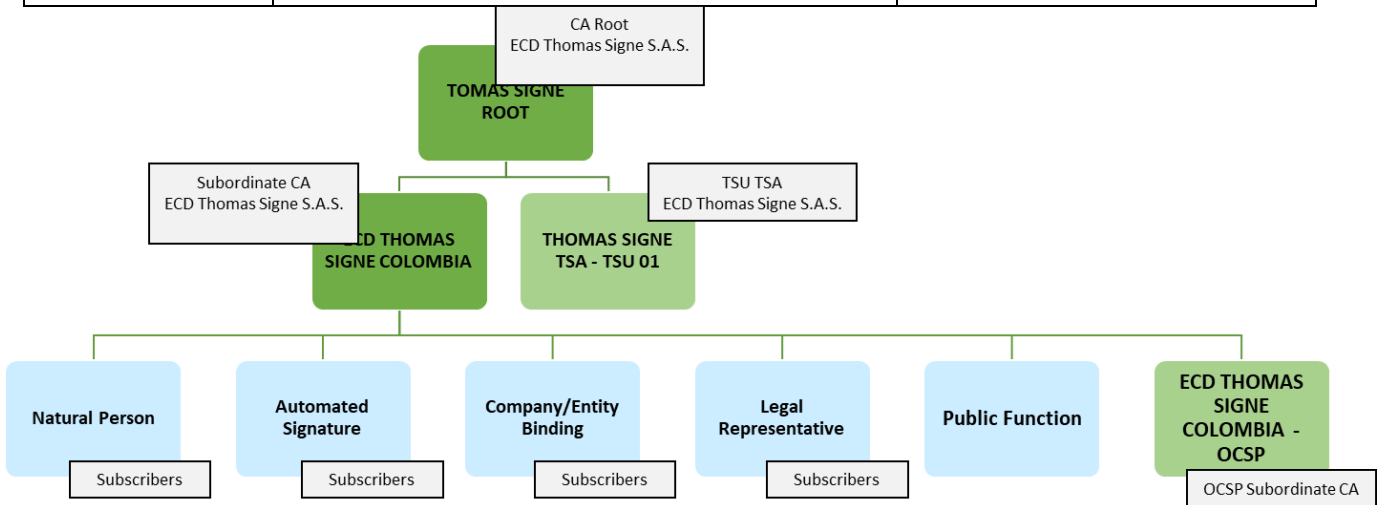
This document is published on the following web page:

<https://thomas-signe.co/declaracion-de-practicas-y-politicas-de-certificacion/>

1.3 THOMAS SIGNE S.A.S. PKI PARTICIPANTS

1.3.1 THOMAS SIGNE S.A.S. PKI CERTIFICATE HIERARCHY

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 13 of 67



Root Certification Authority

Root Certification Authority (Root CA) is the entity within the hierarchy that issues certificates to other Certification Authorities, and whose public key certificate has been self-signed. Its function is to sign the certificate of the other CAs belonging to the Certification Hierarchy.

CN: Thomas Signe Root

Hash SHA1: F683 47D8 A59B 9312 389B CB01 0BEB 7E6C 3E06 7FE5

Valid from March 14, 2018, to March 14, 2038

RSA Key Length 4096 - SHA256

Subordinate Certification Authority

Subordinate Certification Authorities (Sub CA) are entities within the certification hierarchy that issue end-entity certificates and whose public key certificate has been digitally signed by the Root Certification Authority.

Thomas Signe S.A.S has a Subordinate Certification Authority, with a single valid version of its certificate, generated with the SHA256 algorithm and technically restricted through the use of the Extended Key Usage (EKU - extKeyUsage) extension as established in the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly Trusted Certificates and Mozilla CA Certificate Inclusion Policy in force at the time of entry into force of this CPS:

CN: DCE Thomas Signe Colombia

Hash SHA1: 902D E8CA E134 3F4C C913 D7F9 7735 995C 0CC9 C0B7

Valid from March 14, 2018, to March 14, 2038


Key Type: RSA 4096 bits – SHA256

1.3.2 THOMAS SIGNE ROOT

Thomas Signe Root is the Root Certification Authority (Root CA) of Thomas Signe S.A.S. that issues the certificate of the Subordinate Certification Authority (Subordinate CA) of DCE Thomas Signe S.A.S. (DCE Thomas Signe Colombia). Therefore, Thomas Signe Root is the Root CA of the Thomas Signe S.A.S. PKI certificate hierarchy.

The Thomas Signe S.A.S. Root CA also issues the certificate of the Time Stamping Unit (TSU) of the Time Stamping Authority (TSA) of the DCE Thomas Signe S.A.S. (Thomas Signe TSA - TSU 01).

Furthermore, the Thomas Signe S.A.S. Root CA may issue certificates from other Subordinate CAs of the Thomas Signe group, which must be reflected in the corresponding TSAs of these Subordinate CAs. Therefore, Thomas Signe Root may also be the Root CA of other PKIs of the Thomas Signe group.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 14 of 67

1.3.3 DCE THOMAS SIGNE S.A.S. (DCE THOMAS SIGNE COLOMBIA)

Signe S.A. (hereinafter 'Signe') is a company based in Spain, which mainly provides services consisting in the edition and printing of security documents for public and private companies.

Since 2010, Signe performs its activity as a Trusted Service Provider (TSP) for the issuance of qualified and unqualified certificates for electronic signature and qualified certificates for electronic seal according to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (also known as eIDAS Regulation), and according to Spanish Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

In 2016, in a business alliance between Signe and Thomas Greg & Sons de Colombia, the company Thomas Signe S.A.S. is created to act as Certification Entity, Registration or Verification Entity, Digital Signature Software and Value-Added Service Provider of Time Stamping and Digital Intermediation; and thus provide such services in Colombia and comply with the regulation established by the Competent Administrative Authority (AAC), ONAC.

As a Certification Entity - CE, Thomas Signe S.A.S. provides certification services of issuance, revocation, and revocation status information of digital certificates.

The technological and operational infrastructure of the CE of Thomas Signe S.A.S. is provided by Signe. This infrastructure has obtained eIDAS qualification and is verified annually by authorized auditors.

In addition to certification services, Thomas Signe S.A.S. provides registration or verification services, as well as the value-added services of time stamping and digital intermediation.

Thomas Signe S.A.S. in its role of Digital Certification Entity (DCE), is the private legal entity that provides indistinctly services of production, issuance, management, cancellation, or other services inherent to digital certification.

To Thomas Signe S.A.S. as DCE, will be responsible for carrying out all the necessary administrative procedures and formalities before ONAC in order to achieve and maintain the accreditation.

DCE Thomas Signe S.A.S., in its role as Subordinate CA, issues and revokes certificates, and provides revocation verification services through CRL and OCSP.

Likewise, DCE Thomas Signe S.A.S. provides the services of Registration Authority, which is in charge of certifying the validity of the information provided by the Applicant of a digital certificate, through the verification of its identity and the respective evidence record, and of managing the requests for issuance and revocation of digital certificates.

Below are the identification data of the DCE Thomas Signe S.A.S. sites relevant to the provision of certification services:

Digital Certification Entity

Name - Company Name: THOMAS SIGNE SOLUCIONES TECNOLÓGICAS GLOBALES S.A.S.

Acronym: THOMAS SIGNE S.A.S.

T.I.N.: 900962071-5

Chamber of Commerce registration number: 02680791

Certificate of existence and legal representation in the Chamber of Commerce: https://www.thomas-signe.co/CERL_Thomas_Signe.pdf


Active status in the Chamber of Commerce: in <https://www.rues.org.co/> consult using the following ID number 900962071

Business address and correspondence - commercial: Avenida de las Americas No. 44 - 57 - Bogota D.C., Colombia

Address for correspondence - judicial notifications: Cr. 42 Bis No. 17 A 75 - Bogota D.C., Colombia

Telephone: +60 (1) 3810240

E-mail address: comercial@thomas-signe.co

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 15 of 67

PQRS Office: PQRS - pqrsa@thsigne.com

Web Page: www.thomas-signe.co

Technological infrastructure and corporate services - Executive Vice-Presidency - Technical Operation Center

Name - Company Name: SIGNE, S.A.

N.I.F. (equivalent in Spain to N.I.T. in Colombia): A11029279

Registration data in the Mercantile Registry (equivalent in Spain to the registration number of the Chamber of Commerce in Colombia): Mercantile Registry of Madrid, volume 8101, book 7029, folio 95, section 3, page 78156-2, current page M-66591, of section 8.

Certificate of good standing and charges in the Commercial Registry (equivalent in Spain to the certificate of existence and legal representation in the Chamber of Commerce in Colombia): https://www.thomas-signe.co/CVC_Signe.pdf

Current status in the Commercial Registry (equivalent in Spain to active status in the Chamber of Commerce in Colombia): in <https://sede.registradores.org/site/mercantil> consult using the following ID NIF number A11029279

Business address and correspondence - commercial: Avenida de la Industria 18 - 28760 Tres Cantos (Madrid), Spain Telephone: +34 918 06 00 99

E-mail address: comercial@signe.es

PQRS Office:

Technical Support - soporte@signe.es

Web page: www.signe.es

Local Services - Executive Management

Name - Company Name: THOMAS GREG & SONS LIMITED (GUERNSEY) S.A.

T.I.N.: 830012157-0

Chamber of Commerce registration number: 00656972

Certificate of existence and legal representation in the Chamber of Commerce: https://www.thomas-signe.co/CERL_TGSL.pdf

Active status in the Chamber of Commerce: in <https://www.rues.org.co/> consult using the following ID number 830012157

Business address and correspondence - commercial: Avenida de las Americas No. 44 - 57 - Bogotá D.C., Colombia

Business address and correspondence - commercial: Cr. 42 Bis No. 17 A 75 - Bogotá D.C., Colombia

Telephone: +60 (1) 3810240

E-mail address: servicioalclientetgsc@thomasgreg.com

PQRS Office:


Customer service - servicioalclientetgsc@thomasgreg.com

Web page: www.tgscolombia.com

1.3.4 APPLICANT

Applicant is the natural or legal person who requests DCE Thomas Signe S.A.S. to issue a certificate.

1.3.5 SUBSCRIBER

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 16 of 67

Subscriber is the natural or legal person in whose name DCE Thomas Signe S.A.S. issues a digital certificate and, therefore, acts as the person responsible for it, and who, with knowledge and full acceptance of the rights and duties established and published in this CPS and in the corresponding CP and having signed the respective application and acceptance document with Thomas Signe S.A.S., accepts the conditions of the certificate issuance service provided by the latter.

The Subscriber is responsible for the use of the private key associated with the certificate issued in his/her name by DCE Thomas Signe S.A.S., who is exclusively bound to an electronic document digitally signed using said private key.

1.3.6 THIRD PARTY WHO TRUSTS

Relying Third Party (or Accepting Third Party) are all those natural or legal persons who decide to accept and trust a digital certificate issued by DCE Thomas Signe S.A.S.

1.3.7 ENTITY TO WHICH THE SUBSCRIBER IS RELATED

Entity to which the Subscriber is related is, if applicable, the legal entity or natural person (whether it is a company or other type of public or private entity that performs an economic activity for which it is obliged to register in a fiscal or tax registry) to which the Subscriber is related by means of the relationship evidenced in the certificate.

1.4 TYPES AND USES OF CERTIFICATES

1.4.1 PERSONAL CERTIFICATES

Certificates for Natural Persons: these are certificates that allow the Subscriber to identify and sign as a Natural Person without being linked to any company or entity.

OID OF PERSONAL CERTIFICATE POLICIES	
1.3.6.1.4.1.51362.0.2.1.1.D	CP for Natural Person of Thomas Signe S.A.S.

D = Device:

3 = Centralized HSM

1.4.2 CORPORATE CERTIFICATES

Corporate certificates are digital signature certificates whose Subscriber is a Natural Person linked to a company or entity (whether it is a company, or another type of public or private entity that performs an economic activity for which it is obliged to register in a fiscal or tax registry) or the company or entity itself:


Certificates for Company/Entity Binding: these are certificates that allow the Subscriber to identify and sign as a Natural Person linked to a company or entity (Legal Entity or Natural Person), either as an employee, associate, collaborator, client, or supplier.

Certificates for Legal Representative: these are certificates that allow the Subscriber to identify and sign as a Natural Person linked to a company or entity (Legal Person), as its legal representative.

Certificates for Automated Signature: are certificates that allow to identify and sign the Subscriber as a company or entity (Legal Entity or Natural Person), which are issued for computer devices, programs or applications dedicated to sign on behalf of the company or entity in automated digital signature systems.

Certificates for Public Function: these are certificates that allow to identify and sign the subscriber in his role as a public official or individual in the exercise of a public function.

OID OF CORPORATE CERTIFICATE POLICIES

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 17 of 67

1.3.6.1.4.1.51362.0.2.1.2.D	CP for Thomas Signe S.A.S. Company/Entity Binding
1.3.6.1.4.1.51362.0.2.1.3.D	CP for Legal Representative of Thomas Signe S.A.S.
1.3.6.1.4.1.51362.0.2.1.4.D	CP for Thomas Signe S.A.S. Automated Signature.
1.3.6.1.4.1.51362.0.2.1.5.D	CP for Public Function.

D = Device:

3 = Centralized HSM,

2 = Other Devices (only on CP for Automated Signature)

1.4.3 APPROPRIATE USES OF CERTIFICATES

In the description of each type of certificate in this CPS and in the corresponding CP, the respective appropriate uses of the certificates are indicated.

In the case of the use of certificates for centralized signature, the digital signature formats constructed by services offered by Thomas Signe S.A.S. follow the following technical standards:

- ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES). Updated with ETSI EN 319 132 XAdES digital signatures.

- ETSI TS 102 778 PDF Advanced Electronic Signature Profiles (PAdES). Updated with ETSI EN 319 142 PAdES digital signatures.

1.4.4 UNAUTHORIZED USES OF CERTIFICATES

Use contrary to Colombian regulations, customs, morals, and public order is not permitted. The use different from what is established in this CPS and in the corresponding CP is not allowed either.

The certificates have not been designed, cannot be destined, and are not authorized for use or resale as hazardous situation control equipment or for uses that require fail-safe performance, such as the operation of nuclear facilities, navigation or air communications systems, or weapons control systems, where a failure could directly lead to death, personal injury or severe environmental damage.

Certificates issued to Subscribers cannot be used to sign public key certificates of any kind, nor to sign certificate revocation lists.

DCE Thomas Signe S.A.S. does not offer a private key recovery service, and it is not possible to recover the encrypted data with the corresponding public key in case of loss or disablement of the private key or the device that holds it by the Subscriber. The person or organization that decides to encrypt information will do so in any case under his or her own and sole responsibility, without Thomas Signe S.A.S. having any responsibility for loss of information derived from the loss of the encryption keys. Therefore, Thomas Signe S.A.S. does not recommend the use of digital certificates for the encryption of information.


1.5 CPS AND CP ADMINISTRATION

1.5.1 RESPONSIBLE ORGANIZATION

Thomas Signe S.A.S. administers this CPS and the associated CPs.

1.5.2 CONTACT DETAILS

For questions or comments related to this CPS or the associated CPs, the interested party may contact Thomas Signe S.A.S. through any of the following means: registered office and correspondence - commercial, telephone, commercial email addresses or PQRS of the Digital Certification Entity indicated in section 1.3.3.

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 18 of 67

1.5.3 APPROVAL PROCEDURE

This CPS and the associated CPs are approved by the Thomas Signe S.A.S. Management Systems Committee before being published, after version control of the CPs, in order to avoid unauthorized modifications and impersonations and the use of obsolete documentation.

New approved versions of this CPS and associated CPs are sent to ONAC and published on the Thomas Signe S.A.S. website. Changes in each new version will be indicated in the initial version history table.

1.6 DEFINITIONS AND ABBREVIATIONS

1.6.1 DEFINITIONS

Algorithm: a prescribed set of well-defined, ordered and finite instructions or rules that allows an activity to be carried out by means of successive steps that do not generate doubts for the person who must carry out the activity. Given an initial state and following the successive steps, a final state is reached and a solution is obtained.

Certification Authority: Certification Authority (CA). It is a trusted entity, responsible for issuing and revoking digital certificates, publication of certificates, publication of lists of revoked certificates, etc.. Named within the Colombian regulations as Digital Certification Entity - DCE.

Registration Authority: legal person, except for notaries public, or internal part of the DCE necessarily independent of its CA, which according to current regulations, is responsible for receiving requests related to digital certification, to:

- Register the requests made by the applicants to obtain a certificate.
- Check the veracity and correctness of the data provided by the users in the requests.
- Send the requests that meet the requirements to a CA for processing.

Time Stamping Authority (TSA): trusted entity that issues time stamps by means of one or more TSUs. Named within the Colombian regulations as Digital Certification Entity - DCE. The time stamps issued by the DCE, according to the regulation established by ONAC, include the date and time referenced by the time source reported by the National Institute of Metrology of Colombia.

Root CA: First level Certification Authority, trusted base.

Subordinate CA: Certification Authority of second level or more levels.

Private key: see Signature Creation Data. Public key: see Signature Verification Data.

Digital certificate: electronic data message signed by the DCE, which identifies both the issuing DCE and the subscriber and contains the subscriber's public key.

Client: in digital certification services, the term "client" identifies the natural or legal person with whom the DCE establishes a business relationship.


Signature Creation Data (Private Key): unique numeric values that, used in conjunction with a known mathematical procedure, serve to generate the digital signature of a data message.

Signature Verification Data (Public Key): data used to verify that a digital signature was generated with the subscriber's private key.

Certification Practices Statement (CPS): document that details the procedures applied by the DCE for the provision of its services. A statement of the practices that the DCE uses to issue, manage, revoke and renew certificates without and with key change.

Certification Entity: in accordance with the provisions of Law 527 of 1999, Article 2, Section d, that natural or legal person who, authorized under that law, is empowered to issue digital certificates in relation to digital signatures of persons, offer or facilitate registration services and time stamping of the transmission and receipt of data messages, as well as perform other functions related to communications based on digital signatures.

Digital Certification Entities - DCE: name established to particularize and differentiate this type of organizations as Certification Entities from other Certification Bodies accredited by ONAC. Certification Entity that provides the service of issuing certificates, including other digital certificate management, according to the regulation established by ONAC.

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 19 of 67

Time stamp (Time stamp, Time stamp or Time stamping): data message digitally signed and time stamped by a TSA that links another data message with a specific moment in time, which allows to establish with a proof that these data existed at that time and did not undergo any modification from the time when the stamping was performed.

Centralized signature: "Centralized signature" is the centralized management of digital certificates, so that these certificates operate from a single, controlled, and secure repository. In practice, this implies that digital certificates are generated and stored in the server, which allows them to be used from any computer or mobile device.

Digital Signature: shall be understood as a numerical value that is attached to a data message and that, using a recognized mathematical procedure, linked to the initiator's key and the message text, allows determining that this value has been obtained exclusively with the initiator's key and that the initial message has not been modified after the transformation has been carried out.

Hash function: operation performed on a set of data of any size, so that the result obtained is another set of data of fixed size, regardless of the original size, and which has the property of being univocally associated with the initial data.

Centralized HSM: cryptographic device in which the cryptographic keys of the subscribers are generated, stored and protected in a secure way, allowing centralized signature or signature in the cloud.

List of Revoked Digital Certificates (CRL): that list that must include all the certificates revoked by the DCE.

Log: event registration service of the information system, leaving the previous and current information, identifies who and when the event took place.

Security levels: various levels of assurance offered by electronic signature variables, the benefits, and risks of which must be evaluated by the person, company or institution that intends to opt for an electronic signature modality to send or receive data messages or electronic documents.

OID: unique object identifier (object identifier). OID. Acronym of the English term "Object Identifier", which consists of a unique identification number assigned based on international standards and commonly used to identify documents, systems, equipment, etc., in order, among other things, to know the origin, ownership and age of the identified object.

Request (PQRS): request submitted by a customer or interested party regarding the services provided by the DCE.

PKI: Public Key Infrastructure. It is the set of hardware, software, policies, procedures, and technological elements that, through the use of a pair of cryptographic keys, a private one that only the subscriber of the service possesses and a public one, which is included in the digital certificate, achieve:

- Identify the sender of an electronic data message.
- Prevent third parties from observing messages sent through electronic means.
- Prevent a third party from altering the information that is sent through electronic means.
- Prevent that the subscriber of the digital certification service that sent an electronic message can later deny such sending.

Certificate Policy (CP): set of rules indicating the requirements of a certificate in a particular community and/or class, within the framework of legal, regulatory, and common security requirements.


Supplier: the term "supplier" includes organizations, individuals, manufacturers, distributors, technology assemblers and others that supply products, goods and services. DCE suppliers include Reciprocal entities, technology companies that provide services in their different modalities such as: hosting, colocation, document repository (electronic or physical), device provider, telecommunications provider, etc.

Claim (PQRS): expression of a dissatisfaction presented by a client or interested party regarding the services provided by the DCE or the complaint handling process itself.

Complaint (PQRS): expression of a dissatisfaction presented by a client or stakeholder regarding the services provided by the DCE, for which compensation is sought.

Revocation: process by which the digital certificate issued is disabled and its validity period of use is terminated from the date of revocation, upon the occurrence of any of the causes established in the Certification Practices Statement.

Digital certification service: set of certification activities offered by the DCE to certify the origin and integrity of data messages, based on digital or electronic signatures, time stamping, as well as the applicability of technical standards supported and in force in public key infrastructure - PKI.

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 20 of 67

Time stamping: see Time stamping.

OCSP online certificate status service: activity of consulting in real time to the DCE system, on the status of a digital certificate through the OCSP protocol.

Applicant: natural or legal person who, with the purpose of obtaining digital certification services from a DCE, demonstrates compliance with the requirements established in the CPS and the corresponding CP to access the digital certification service. Natural or legal person that requests the DCE to issue a certificate.

Suggestion (PQRS): recommendation proposed by a client or interested party for the improvement of the services provided by the DCE.


Subscriber: natural or legal person in whose name a digital certificate is issued. Natural or legal person who, having signed the respective application and acceptance document, accepts the conditions of the certificate issuance service provided by the DCE.

Trusting Third Party (Third Party Acceptor): natural or legal person who receives a document, log, notification or any other digitally signed data, and who trusts the validity of the corresponding digital certificate issued by the DCE.

Time-stamping unit (TSU): set of hardware and software that is managed as a unit and has a single timestamp signing key active at an instant of time.

1.6.2 ACRONYMS

CA	Certification Authority
CRL	Certificate Revocation List
DN	Distinguished Name
CPS	Certification Practices Statement
DCE	Digital Certification Entity that provides digital certification services and is equivalent to a Certification Entity as defined in law 527 of 1999. It should also be understood as a Conformity Assessment Body - CAB as defined in ISO/IEC 17000.
ETSI	European Telecommunications Standards Institute
ERP	Enterprise Resource Planning
FIPS	Federal Information Processing Standards (FIPS). These are publicly announced standards developed by the U.S. government for use by all non-military government agencies and government contractors. Many FIPS standards are modified versions of standards used in the broader communities (ANSA, IEEE, ISO, etc.).
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NIF	Tax Identification Number
NIT	Tax Identification Number
NOC	Network Operation Center
OCSP	Online Certificate Status Protocol
ONAC	National Accreditation Organization of Colombia
RO	Registry Operator
CP	Certificate Policy
PKCS	Public-Key Cryptography Standards. Public-key cryptography standards devised and published by RSA Laboratories.
PKI	Public Key Infrastructure
PQRS	Petitions, Complaints, Claims and Suggestions
RA	Registration Authority

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 21 of 67

RFC	Request For Comments. A series of publications from the Internet Engineering Task Force (IETF) describing various aspects of the operation of the Internet and other computer networks, such as protocols, procedures, etc.
RSA	Rivset, Shamir and Adleman. It is a public key cryptographic system developed in 1977. It is the first and most widely used algorithm of this type and is valid for both encryption and digital signing.
RUES	Single Corporate and Social Registry
SAR	Signe Registration Authority
SHA	Secure Hash Algorithm
SOC	Security Operation Center
TSA	Time Stamping Authority
TSU	Time Stamping Unit

2 RESPONSIBILITIES REGARDING REPOSITORIES AND PUBLICATION OF INFORMATION

2.1 REPOSITORIES

Thomas Signe S.A.S. Root CA Certificate.

http://thsigne.com/certs/thomas_signe_root.crt

https://thsigne.com/certs/thomas_signe_root.crt

Thomas Signe S.A.S. Subordinated CA Certificate

http://thsigne.com/certs/DCE_thomas_signe_colombia.crt

https://thsigne.com/certs/DCE_thomas_signe_colombia.crt

Thomas Signe S.A.S. Root CA Revoked Certificate List (CRL).

http://crl.thsigne.com/thomas_signe_root.crl

https://crl.thsigne.com/thomas_signe_root.crl

List of Revoked Certificates (CRL) CA Subordinate CA of Thomas Signe S.A.S.

http://crl-co.thsigne.com/DCE_thomas_signe_colombia.crl

https://crl-co.thsigne.com/DCE_thomas_signe_colombia.crl

OCSP Service CA Subordinated of Thomas Signe S.A.S.

<http://ocsp-co.thsigne.com>


Certification Practice Statement (CPS), Certificate Policy (CP) and Subscription Contract (Application and Acceptance Document)

<http://thsigne.com/cps>

<https://thomas-signe.co/declaracion-de-practicas-y-politicas-de-certificacion/>

Repositories are referenced by URL. Any change in 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 changed

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 22 of 67

without notice.

The information in the URLs will be available online 24 hours a day, 7 days a week.

In the event of system failure, or any other factor beyond the DCE's control, the DCE will make every effort to ensure that the information in the URLs is not unavailable for longer than the maximum 24-hour period.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The Management Systems Committee of Thomas Signe S.A.S. is responsible for the approval of the CPS, CPs and the application and acceptance document published on <http://thsigne.com/cps>.

The Management Systems Manager, the Digital Registration Manager and the CA System Administrator are responsible for the information published on the Thomas Signe S.A.S. website www.thomas-signe.co.

2.2.1 TIMING OR FREQUENCY OF PUBLICATION

Root CA and Subordinate CA Certificates

Root CA and Subordinate CA certificates will be published and remain on the Thomas Signe S.A.S. website for as long as the DCE is providing digital certification services.

List of Revoked Certificates (CRL)

Thomas Signe S.A.S. shall publish on its website the CRLs of the Root CA and the Subordinate CA in the events and with the periodicity defined in section 4.9.6.

Certification Practice Statement (CPS), Certificate Policy (CP) and Application and Acceptance document.

Thomas Signe S.A.S. will publish on its website each new approved version of the CPS, CPs and the Application and Acceptance document.

Thomas Signe S.A.S. keeps the previous versions of the CPS and CPs published on its website for as long as there are valid certificates issued in accordance with these documents. The versions removed from its website may be requested by interested parties at the DCE PQRS e-mail address.

2.2.2 REPOSITORY ACCESS CONTROLS

The aforementioned available repositories are freely accessible for consultation by the general public. The integrity and availability of the published information is the responsibility of Thomas Signe S.A.S..

The organization has the necessary resources and procedures to restrict access to these repositories for purposes other than consultation by persons outside Thomas Signe S.A.S.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMES


3.1.1 TYPES OF NAMES

All certificates require a distinguished name (DN or distinguished name) of the certificate holder in accordance with the X.500 standard.

Additionally, certificate holder DNs are consistent with the following standards:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)

3.1.2 NEED FOR NAMES TO HAVE MEANING

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 23 of 67

The fields of the DN of the certificate holder referring to Name and Surname and/or Name or Company Name shall correspond to the data contained in the Citizenship Card, Alien Registration Card or Passport and/or in the Certificate of Existence and Legal Representation in the Chamber of Commerce and/or Single Tax Registry (or equivalent documents).

If the data contained in the DN of the certificate holder is fictitious or its invalidity is expressly indicated in said DN (e.g., by the word "TEST" or "INVALID"), the certificate will be considered without legal validity, only valid for technical interoperability tests (test certificate), and that it does not comply with all that is specified in this CPS and in the corresponding CP.

3.1.3 ANONYMITY AND PSEUDO-ANONYMITY OF SUBSCRIBERS

No anonymity or pseudonyms are allowed to identify subscribers.

3.1.4 UNIQUENESS OF NAMES

The distinguished name (DN) of the issued certificate holders will be unique for each Subscriber.

Attributes of the DN of the certificate holder containing the type and number of the identity document and/or tax identification number are used to distinguish between two identities when there is a problem of duplicity of names.

3.1.5 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

DCE makes no commitments in the issuance of certificates regarding the use by Subscribers of a trademark.

Thomas Signe S.A.S. does not knowingly permit the use of a name whose right of use is not owned by the Subscriber. However, DCE is not obliged to search for evidence of trademark ownership prior to the issuance of certificates.

3.2 INITIAL VALIDATION OF IDENTITY

3.2.1 METHOD OF PROOF OF POSSESSION OF THE PRIVATE KEY

The CP for each type of certificate specifies the method of proof of possession of the private key for each of the media types on which the corresponding certificates can be issued.


3.2.2 AUTHENTICATION OF THE IDENTITY OF A COMPANY OR ENTITY

The RA will verify the following data to authenticate the identity of the company or entity (Legal Entity or Natural Person, whether it is a company or other type of public or private entity that performs an economic activity for which it is obliged to register in a fiscal or tax registry) identified in the certificate:

- The data relating to the name or corporate name of the company or entity (Legal Entity or Natural Person).
- The data relative to the constitution and legal personality of the company or entity (Legal Person).
- The data relative to the extension and validity of the powers of representation of the legal representative of the company or entity (Legal Entity).
- Data relative to the tax identification number of the company or entity (Legal Entity or Natural Person).
- Data related to the complete address of the company or entity (Legal Entity or Natural Person).

The RA will verify the above data through the following procedures:

- Certificate of existence and legal representation request at the Chamber of Commerce or equivalent document, in cases where applicable; issued in Colombia (by default) or in another country a maximum of 30 days before.
- Single Tax Registry or equivalent document, in all cases; issued in Colombia (by default) or in another country.
- Additional official document showing a complete current address of the company or entity (for example, a Certificate of Residence for Natural Persons), in case the Subscriber wishes the certificate to show an address different from those included in the Certificate of existence and legal representation in the Chamber of Commerce and/or in the Single Tax Registry or equivalent documents; issued in Colombia (by default) or in another country a maximum of 30 days before.

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 24 of 67

- For those cases in which it is possible, consultation of the tax identification number of the company or entity in an online database (in Colombia, for companies of the type of Legal Entity or Natural Person, RUES database), to verify the existence of the company or entity and that it is active.

The DCE reserves the right not to issue the certificate if it considers that the documentation provided is not sufficient or adequate for the verification of the data.

The RA will keep the documentation related to the support of the validation of the identity of the company or entity identified in the certificate.

Additionally, if the type of certificate admits the possibility that the Applicant is a company or entity (Legal Entity or Natural Person, whether it is a company, or another type of public or private entity that performs an economic activity for which it is obliged to register in a fiscal or tax registry) other than the Subscriber, the RA will verify the identity of this company or entity as specified in the corresponding CP.

The RA will reliably verify the identity of the Natural Person identified as the legal representative of the entity (subscriber) in the certificate by the means of: video conference, unassisted video identification process or face-to-face. In the event of video conference, the Natural Person individual identified as the legal representative must scan and provide a legally recognized document that identifies himself and show the original document during the video conference. In the event of face-to-face, the individual Natural Person must show to a Registration Officer the original document to obtain a photocopy.

3.2.3 AUTHENTICATION OF AN INDIVIDUAL NATURAL PERSON'S IDENTITY

The RA shall reliably verify the identity of the individual Natural Person identified in the certificate (Subscriber) or of the individual Natural Person requesting the certificate, by videoconference, by the unassisted video identification process, or in person. For this, in the case of verification by videoconference, the individual Natural Person must scan and send a legally recognized document that identifies him/her and show the original document during the videoconference, and, in the case of verification in person, the individual Natural Person must show the original document in person to a RO and the RO must make, or have received from the individual Natural Person, a photocopy of the same.

The RA will validate that the identity document presented is apparently legitimate and that the data contained therein (country of issuance, type and number of the identity document, names and surnames) are in accordance with the corresponding data entered in the certificate application form and the documents attached in the SAR platform. Also, where applicable, the RA will verify that the document was valid at the time of submission.

The RA will keep the documentation related to the support of the validation of the identity of the individual Natural Person Subscriber and/or Applicant of the certificate.

3.2.4 UNVERIFIED SUBSCRIBER AND APPLICANT INFORMATION

Under any circumstances the RA shall not omit the verification of information leading to the identification of the Subscriber and the Applicant as specified in sections 3.2.2 and 3.2.3.

The CP for each type of certificate specifies the unverified Subscriber and Applicant information for the corresponding certificates.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUESTS WITH CHANGE OF KEYS


DCE Thomas Signe S.A.S. does not attend digital certificate renewal requirements with key change.

Cases in which a new digital certificate with change of keys is required, due to expiration, upcoming expiration or revocation of a certificate, are treated as a new certificate issuance, performing the same identity validation that was initially done for the first digital certificate, as specified in section 3.2.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

The identification and authentication of the Subscriber or Applicant for a certificate revocation request may be performed by:

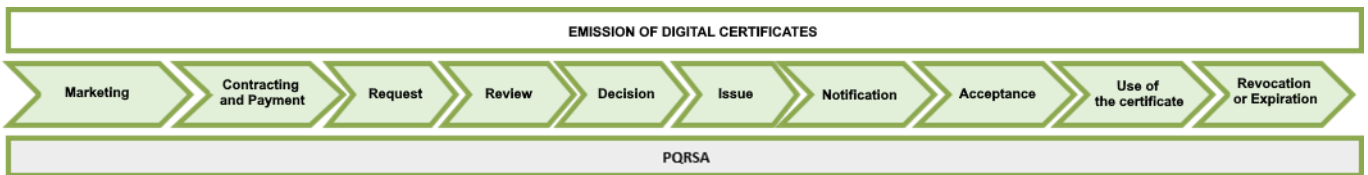
- The Subscriber or Requestor itself, in case the Subscriber or Requestor uses the online revocation procedure. The CP of each type of certificate specifies the method by which the Subscriber or Applicant is identified and authenticated for an online revocation request, depending on the type of media on which the certificate was issued.

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 25 of 67

- A Registration Operator (RO), in case the Subscriber or Applicant uses the revocation procedure by Registration Operator. The RO shall identify and authenticate the Subscriber or Applicant to a revocation request received by e-mail, verifying that it has been sent from the respective e-mail address declared in the application form for the issuance of the certificate.

4 OPERATIONAL REQUIREMENTS FOR THE CERTIFICATE LIFECYCLE

The life cycle of digital certificates issued by DCE Thomas Signe S.A.S. extends from the initial marketing to the revocation or expiration of the certificate.



4.1 CERTIFICATE REQUEST

4.1.1 WHO CAN REQUEST A CERTIFICATE

They are authorized to request the issuance of a certificate:

1) The Subscriber who is a Natural Person and who correctly supports the information required by the RA, as specified in section 4.1.4 and in the respective CP.

2) An individual Natural Person linked to the Subscriber (Legal Entity or Natural Person), including a legal representative, attorney-in-fact, employee or person authorized by a legal representative of the Subscribing Legal Entity or by the Subscribing Natural Person itself to request and obtain a certificate for computer devices, programs or applications dedicated to sign on behalf of the company or entity in automated digital signature systems, who can correctly support the information required by the RA, as specified in section 4.1.4 and in the respective CP.

3) A company or entity (Legal Entity or Natural Person, whether it is a company, or any other type of public or private entity that performs an economic activity for which it is obliged to register in a fiscal or tax registry) other than the Subscriber, who has been authorized by the legal representative of the Subscribing Legal Entity or by the Subscribing Natural Person itself to request and obtain a certificate for computer devices, programs or applications dedicated to sign on behalf of the company or entity in automated digital signature systems, which can correctly support the information required by the RA, as specified in section 4.1.4 and in the respective CP.

4.1.2 MARKETING

The Applicant and/or, where applicable, the Subscriber and/or the Entity to which the Subscriber is bound may receive information about the digital certification process in the following ways:


- Consulting the web page www.thomas-signe.co
- Via e-mail to comercial@thomas-signe.co
- Dealing directly with commercial agents.

By any of these means, they will be provided with information about such process, necessary requirements, fees or other related matters.

After being informed, if the Applicant is an individual Natural Person, the Applicant and/or, in the applicable cases, the Subscriber and/or the Entity to which the Subscriber is linked will inform the Commercial Area and/or an RO:

- 1) The type of certificate required and, if the certificate supports multiple media types, the type of media required.
- 2) The validity of the certificate required.
- 3) The full name of the Applicant.
- 4) The type and number of the Applicant's identity document.

5) The email account of the Applicant that will be associated to the digital certificate and through which the DCE will send notifications and official communications.

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 26 of 67

Where applicable:

- 6) The name or company name of the Subscriber or of the Entity to which the Subscriber is bound.
- 7) The TIN of the Subscriber or of the Entity to which the Subscriber is linked.

If the Applicant is an individual Natural Person, the Commercial Area and/or an RO will send by e-mail to the Applicant and/or, where applicable, to the Subscriber and/or to the Entity to which the Subscriber is linked: the Commercial Proposal (sent by the Commercial Area), where applicable; the Application and Acceptance document; in the types of certificate that allow it, an authorization model for the application and obtaining of the certificate in the event it is required; optionally, a link to the SAR platform; and the respective indications.

4.1.3 CONTRACTING AND PAYMENT

To proceed with the contracting and payment, the Applicant and/or, where applicable, the Subscriber and/or the Entity to which the Subscriber is bound shall:

- Make payment of the respective fee by a valid method, where applicable. The evidence of this process shall be the voucher or proof of payment.

Thomas Signe S.A.S. makes available to the public a bank account to make the deposit of the respective amount for each service (see section 9.1). The details of this bank account shall be indicated in the Commercial Proposal. However, Thomas Signe S.A.S. may require an alternative method of payment in the case of a Service Contract.

- Approve all terms and conditions set forth in the Application and Acceptance document between Thomas Signe S.A.S. and the Subscriber by signing it. The evidence of this process will be the signed document itself.

It should be noted that, in addition to the Application and Acceptance document with each Subscriber of a digital certificate, depending on the type of contract, a Service Agreement may be required between Thomas Signe S.A.S. and, for personal certificates, the Subscriber, or, for corporate certificates, the company or entity that appears in the digital certificate.

- If the Applicant is a company or entity (Legal Entity or Natural Person) other than the Subscriber, approve all the terms and conditions set forth in a Service Agreement between Thomas Signe S.A.S. and the Applicant, by means of the respective signature. The evidence of this process will be the signed Service Agreement.


4.1.4 REQUEST

The process of requesting the issuance of a digital certificate will depend on the type of certificate required. The CP for each type of certificate specifies the issuance request process for the corresponding certificates. The general issuance request process is described below.

To request the issuance of a digital certificate, the Applicant and/or, where applicable, the Subscriber and/or the Entity to which the Subscriber is linked, may enter the SAR platform. Within the platform, they will proceed to enter the required data and attach the requested documents, and finally save their request. Alternatively, the Applicant and/or, where applicable, the Subscriber and/or the Entity to which the Subscriber is linked may personally deliver or send the required data and documents to the Commercial Area and/or an RO, and they will enter the data and attach the requested documents in the SAR platform.

The DCE Thomas Signe S.A.S. RA requests all information necessary for the verification of the Applicant's and/or Subscriber's identity. The required documents depend on the type of certificate (specified in the respective CP), which may be and are not limited to the following:

- Citizenship Card, Identification Card, or Passport of the Applicant (Individual Natural Person); issued in Colombia (by default) or in another country (equivalent document).
- Certificate of existence and legal representation in the Chamber of Commerce or equivalent document of the Subscriber or of the Entity to which the Subscriber is linked; issued in Colombia (by default) or in another country a maximum of 30 days before.
- Single Tax Registration or equivalent document of the Subscriber or of the Entity to which the Subscriber is related; issued in Colombia (by default) or in another country (equivalent document).
- Authorization signed by the Legal Representative of the Legal Entity or by the Natural Person of the Subscriber or of the Entity to which the Subscriber is linked, with the data of the Natural Person or of the Legal Entity authorized to request and obtain the digital certificate; issued a

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 27 of 67

maximum of 30 days before.

- Citizenship Card, Identification Card, or Passport of the Legal Representative of the Legal Entity or of the Natural Person signing the authorization; issued in Colombia (by default) or in another country (equivalent document).
- Additional official document showing a complete current address of the Subscriber, for example, a Certificate of Residence for Natural Persons, issued a maximum of 30 days before.

Furthermore, the RA of DCE Thomas Signe S.A.S. requests the following additional documents for the issuance of a certificate:

- Evidence of payment of the certificate fee indicated in the Commercial Proposal or in the Service Agreement, where applicable.
- Signed Application and Acceptance Document.
- Act of appointment of public official. (Only applicable for Public Function certificates)

Thomas Signe S.A.S. has the right to request additional documents to guarantee the correct authentication of the Applicant and/or the Subscriber and to carry out a proper digital certification service.

4.2 PROCESSING OF CERTIFICATE APPLICATIONS

4.2.1 REVIEW

It is the RA's responsibility to reliably identify the Applicant and/or Subscriber according to the type of certificate requested. To this end, an RO shall verify the validity of the documentation submitted and, where possible, consult an online database to verify the company or entity Subscriber or the Entity to which the Subscriber is linked, as specified in sections 3.2.2 and 3.2.3 and in the corresponding CP.

If payments or documentation need to be regularized, the email address declared by the Applicant or Subscriber will be notified as required.

In the event of the subscriber or the applicant performs a request for certificate issuance attaching a CSR, the RA automatically validates the information of the request and the CSR information match, showing an error in case of data discrepancy.

Once all the required documentation and evidence has been collected and reviewed, a RO will coordinate with the Subscriber (Natural Person) or with the Subscriber's Legal Representative (Legal Entity) an un-assisted video identification process or an appointment for a videoconference. In this session, the RO will ask a series of questions to verify the identity of the Subscriber (Natural Person) or the Subscriber's Legal Representative (Legal Entity) and will ask the Subscriber to show the original identity document that has been scanned in order to verify that it matches the document received. In order to evidence such videoconference, the AR platform will record the entire session and the recording will be saved together with the information collected from the Subscriber (Natural Person) or the Subscriber's Legal Representative (Legal Entity). This process will be carried out prior to the issuance of the certificate.


Alternatively to the un-assisted video identification process or videoconference, an RO may have verified the identity of the Subscriber (Natural Person) or the Subscriber's Legal Representative (Legal Entity) in person, in which case he/she must have received the required documents, which must have been entered in the SAR platform in digital format and, in addition, must file and keep in paper format (not scanned) the original documents received in said format, which must include the Application and Acceptance document signed in handwriting by the Subscriber (Natural Person) or by the Subscriber's Legal Representative (Legal Entity), as evidence of the Subscriber's identification in person.

Once the RO has reviewed the documents submitted and the data entered in the certificate request form and has performed and reviewed the validation of the subscriber's identity, the RO will approve or reject the request for issuance of the certificate on the RA platform based on the review.

Approval of the request by the RO shall be the documented recommendation for the decision to issue the certificate. Rejection of the application by the RO will result in a documented recommendation for a decision to cancel the certificate issuance. In both cases, the RO shall have documented the processes and results related to the review of the application.

4.2.2 DECISION

The DCE Thomas Signe S.A.S. is responsible for the decision taken with respect to digital certification, ensuring independence and impartiality between the functions of review and certification decision. To this end, an RA Decision Operator, independent of the RO who has performed the review of the certificate

	Certification Practice Statement for Certificate Issuance	Version 2.7
	Code: THS-CO-AC-DPC-01	Page 28 of 67

issuance request, after considering the recommendation for decision and the documented processes and results related to such review, as well as other possible substantiated and demonstrated reasons, will make the decision to issue the certificate or to cancel the issuance of the certificate.

In the case of cancellation, the RA Decision Operator will send an email to the Applicant and the Subscriber notifying the reasons for the decision not to issue the certificate.

4.3 CERTIFICATE ISSUANCE

4.3.1 DCE ACTIONS DURING CERTIFICATE ISSUANCE

Once the Decision Operator of the RA has made the decision to issue the certificate, the issuance of the certificate will proceed, which must be done in a secure manner. In issuing the digital certificate, the DCE Thomas Signe S.A.S.:

- Uses a certificate generation procedure that securely binds the certificate to the registration information, including the certified public key.
- It protects the confidentiality and integrity of the registration data.
- All certificates will become valid at the time indicated on the certificate itself.

The CP of each type of certificate specifies the actions of the DCE during the issuance of the certificate for each of the types of media on which the corresponding certificates can be issued.

4.3.2 NOTIFICATION TO THE APPLICANT AND SUBSCRIBER BY THE DCE OF CERTIFICATE ISSUANCE

DCE Thomas Signe S.A.S. will notify the Applicant and the Subscriber of the certificate issuance and will send them the digital certification documentation by e-mail.

The CP for each type of certificate specifies how the DCE notifies the Applicant and the Subscriber of the issuance of the certificate and what documentation of the digital certification is sent to them, for each of the types of media on which the corresponding certificates can be issued.

4.3.3 CERTIFICATE DISTRIBUTION

Thomas Signe S.A.S. provides to relevant parties the certificates issued by the CA via active directory designed for that purpose. The access to the active directory is always performed through authorized personal of Thomas Signe S.A.S.

4.4 ACCEPTANCE OF THE CERTIFICATE

4.4.1 FORM IN WHICH THE CERTIFICATE IS ACCEPTED

The certificate shall be deemed accepted by the Subscriber, once the RA has made its delivery and the DCE has notified the same to the Applicant and the Subscriber, as specified in the respective CP.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE DCE

DCE Thomas Signe S.A.S. does not publish issued certificates in any repository.

4.4.3 NOTIFICATION OF THE ISSUANCE OF THE CERTIFICATE BY THE DCE TO OTHER ENTITIES


Thomas Signe S.A.S. does not notify the issuance of certificates to third parties.

4.5 USE OF KEYS AND CERTIFICATE

4.5.1 USE OF THE PRIVATE KEY AND CERTIFICATE BY THE SUBSCRIBER

The certificates may be used as stipulated in this CPS and the respective CP.

The Key Usage and Extended Key Usage extensions may be used to establish technical limits to the

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 29 of 67

uses of the private key of the corresponding certificate. The application of these limits will depend largely on their correct implementation by computer applications, and their regulation is beyond the scope of this document.

4.5.2 USE OF THE PRIVATE KEY AND THE CERTIFICATE BY TRUSTED THIRD PARTIES

Relying Third Parties may use the certificates for the purposes set forth in this CPS and the respective CP.

It is the responsibility of the Relying Third Parties to verify the status of the certificate through the services offered by Thomas Signe S.A.S. specifically for that purpose and specified in this document.

4.6 RENEWAL OF THE CERTIFICATE WITH CHANGE OF KEYS

DCE Thomas Signe S.A.S. does not handle digital certificate renewal requests without a change of keys.

Cases in which a new digital certificate is required, due to expiration, upcoming expiration or revocation of a certificate, are treated as a new certificate issuance, with change of keys.

4.7 RENEWAL OF THE CERTIFICATE WITH CHANGE OF KEYS

DCE Thomas Signe S.A.S. does not attend digital certificate renewal requirements with key change.

Cases in which a new digital certificate is required, due to expiration, upcoming expiration or revocation of a certificate, are treated as a new certificate issuance, with change of keys.

4.8 MODIFICATION OF CERTIFICATES

DCE Thomas Signe S.A.S. does not attend requests for modification of digital certificates.

The cases in which it is required to modify some data in a digital certificate (update of the information contained in a certificate) are treated as a certificate revocation and a new certificate issuance, with change of keys.

4.9 REVOCATION AND SUSPENSION OF CERTIFICATES


The revocation of a certificate means the loss of its validity and is irreversible. Revocations take effect from the moment they are published in the CRL or in the OCSP service.

Likewise, the suspension of certificates that does not lead to an immediate revocation status is not permitted. DCE Thomas Signe S.A.S. does not perform certificate suspensions.

4.9.1 CONDITIONS FOR THE REVOCATION OF A CERTIFICATE

A certificate may be revoked due to the following causes:

- a) Events affecting the information contained in the certificate:
 - Confirmation that some information or fact contained in the certificate is false.
 - Occurrence of new facts that cause that the original data do not correspond to the real ones, for example, loss or change of the link of the Subscriber with the Entity that appears in the certificate.
 - Modification of any data contained in the certificate.
 - Liquidation of the legal entity appearing on the certificate.
 - Termination of the performance of the economic activity for which it was obliged to register in a fiscal or tax registry, by the natural person that appears in the certificate as a company or entity.
- b) Conditions affecting the security of the private key or the certificate:
 - Compromise or suspected compromise of the private key or of the DCE's infrastructure or systems, if it affects the reliability of the certificates issued from that incident.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 30 of 67

- Infringement by the DCE of the requirements foreseen in the certificate management procedures established in this CPS or in the corresponding CP.

- Any reason that leads to reasonably believe that the certification service has been compromised, casting doubt on the reliability of the digital certificate.

- Compromise or suspected compromise of the security of the private key or certificate.

- Loss, disabling of the digital certificate that has been reported to the DCE.

- Unauthorized access or use by a third party of the certificate's private key.

- Failure by the Subscriber to comply with the rules of use of the certificate set forth in this CPS, in the corresponding CP or in the Application and Acceptance document.

- In case it is noticed that the cryptographic mechanisms used for the generation of the private key or the certificate do not comply with the minimum security standards necessary to guarantee its security.

c) Conditions affecting the security of the cryptographic device:

- Security of the cryptographic device is compromised or suspected to be compromised

- Loss or disablement due to damage of the cryptographic device.

- Unauthorized access by a third party to the activation data of the cryptographic device.

- Failure by the Subscriber to comply with the rules of use of the cryptographic device set forth in this CPS, in the corresponding CP or in the Application and Acceptance document.

d) Events affecting the Subscriber and/or Applicant:

- Termination of the legal relationship between DCE and the Subscriber.

- Termination of the contract with DCE, in accordance with the grounds established in the Application and Acceptance document.

- Modification or termination of the underlying legal relationship or reason that allowed the issuance of the certificate to the Subscriber.

- Opposition or modification, by the Subscriber and/or Applicant, of the data contained in the Thomas Signe S.A.S. personal data file.

- Infringement by the Applicant of the certificate of the requirements and obligations established for its application in this CPS, in the corresponding CP or in the contractual documents signed with DCE.

- Infringement by the Subscriber or the Entity to which the Subscriber is bound of its obligations and responsibilities established in this CPS, in the corresponding CP or in the Application and Acceptance document.

- Total or partial disability or death of the Subscriber.

- Request of the Subscriber or of an authorized third party.

e) Other circumstances:

- Judicial or administrative resolution ordering it.

- Any other lawful cause specified in this CPS or in the corresponding CP.

4.9.2 WHO CAN REQUEST A REVOCATION

The revocation of a certificate may be requested:

a) The Subscriber and/or Applicant itself, who shall request the revocation of the certificate in the event of having knowledge, by indication or confirmation, of any of the circumstances indicated above.


b) The DCE itself, which shall request the revocation of a certificate if it becomes aware, by evidence or confirmation, of any of the circumstances indicated above.

c) Any other person may request the revocation of a certificate if they have knowledge, by evidence or confirmation, of any of the above circumstances.

The revocation of the certificate may be processed:

- Subscriber and/or Applicant itself, in cases of online certificate revocation.

- Authorized operators of the DCE (RA Decision Operators).

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 31 of 67

In any case, when the certificate is revoked, a communication will be sent by e-mail to the Subscriber.

4.9.3 REVOCATION REQUEST PROCEDURES

There are different alternatives to request the revocation of a certificate.

In all alternatives, at the time of processing the revocation in the RA, the reason that best corresponds to the circumstances that cause the revocation of the certificate must be selected from the following possible reasons: Not specified, Key compromised, Membership changed, Replacement, Cessation of operation. The selected revocation reason shall be included in the CRLs and OCSP service queries, as specified in sections 7.2 and 7.3.

Online procedure

Thomas Signe S.A.S. provides the online revocation service through the links contained in its website through the following [link](#). Subscribers and/or Applicants who wish to revoke their certificates online must access these links and enter the respective authentication data.

The CP of each type of certificate specifies the authentication data to be entered in these links for each of the media types in which the corresponding certificates can be issued and revoked online.

Internal procedures

The DCE shall request the revocation of a certificate through internal procedures.

An RA Decision Operator shall identify and authenticate the revocation requestor through the procedures it deems appropriate and verify that the cause reported corresponds to any of the circumstances indicated above.

Once the revocation requestor has been correctly identified and the cause reported has been verified, the RA Decision Operator shall proceed to process the revocation.

4.9.4 TIME PERIOD IN WHICH THE CA MUST PROCESS THE REVOCATION REQUEST

Once the revocation has been duly processed in the RA, it will be processed by the CA immediately.

4.9.5 OBLIGATION FOR TRUSTED THIRD PARTIES TO VERIFY REVOCATIONS

Verification of certificate status is mandatory for each use of certificates, either by querying the CRL or the OCSP service.


4.9.6 FREQUENCY OF ISSUANCE OF CRL

The Thomas Signe Root CRL (Root CA) is issued before 180 days have elapsed since the issuance of the previous CRL (prior to its end of validity) or upon revocation.

The Thomas Signe Colombia DCE CRL (Subordinate CA) is issued every 24 hours or upon revocation of a certificate.

4.9.7 MAXIMUM TIME BETWEEN THE GENERATION AND PUBLICATION OF CRL'S

Once the Thomas Signe Root CRL (Root CA) is issued, it is published at least before the end of validity of the previous CRL (180 days after its issuance); under normal conditions, the CRL is published on the same day of its issuance.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 32 of 67

Once the CRL of the DCE Thomas Signe Colombia (Subordinate CA) is issued, the CRL is instantly generated, so the elapsed time is considered zero or null.

4.9.8 AVAILABILITY OF ON-LINE CERTIFICATE STATUS VERIFICATION SYSTEMS

Thomas Signe S.A.S. has two online certificate status verification systems available, one by CRL revocation check and the other by OCSP, both free of charge and without access restrictions.

The access addresses to both online systems can be found in section 2.1, as well as in the issued certificates, in their respective CRL Distribution Points and Authority Information Access extensions.

4.9.9 ONLINE REVOCATION CHECKING REQUIREMENTS

For the use of the online revocation checking system by CRL, freely accessible, the following should be considered:

- The revocation status of the Subscriber's certificate must be checked in the latest CRL issued by the Subordinate CA, which may be downloaded at the URL address contained in the certificate itself, in its CRL Distribution Points extension.

- Additionally, the revocation status of the certificate of the Subordinate CA must be checked in the last CRL issued by the Root CA, which can be downloaded at the URL address contained in the certificate itself, in its CRL Distribution Points extension.

- Each CRL must be checked to ensure that it is current (with a value in the *nextUpdate* field after the current date and time) and signed by the CA that issued the certificate to be validated.

- The information provided in the last CRL issued by the Subordinate CA is updated, under normal conditions, when a revocation occurs (automatic process).

- The information provided in the last CRL issued by the Root CA is updated, at the latest, 24 hours after each revocation (manual process).

- The information of each revoked certificate in the CRLs shall include the corresponding revocation reason according to RFC 5280, except when the revocation reason is *unspecified (0)*.

- Revoked certificates that expire may be removed from the CRL.

For the use of the online revocation checking system by OCSP, the following should be considered:

- The revocation status of the Subscriber's certificate shall be checked in the OCSP service of the Subordinate CA, whose access URL is contained in the certificate itself, in its Authority Information Access extension.

- Additionally, the revocation status of the certificate of the Subordinate CA must be checked in the last CRL issued by the Root CA, which can be downloaded at the URL address contained in the certificate itself, in its CRL Distribution Points extension.

- The revocation status of the certificates can be checked in the OCSP service using GET or POST methods.


- It shall be verified that each OCSP response is sufficiently recent (with a value of the *thisUpdate* field very close to the current date and time) and signed with a valid certificate (not expired) issued by the CA that issued the certificate to be validated, and that it includes the Key Usage extensions with the *digitalSignature* and/or *nonRepudiation* and Extended Key Usage with the *OCSPSigning* usage.

- The revocation status of the certificate used to sign each OCSP response must be checked in the last CRL issued by the CA that issued the certificate, which can be downloaded at the URL address contained in the certificate itself, in its CRL Distribution Points extension.

- The information provided through the OCSP service of the SIGNE Subordinate CA is updated immediately (automatic process).

- The information of each revoked certificate provided through the OCSP service will include the corresponding revocation reason according to RFC 5280, except when the revocation reason is *unspecified (0)*.

- The information provided through the OCSP service is maintained after the certificates whose revocation status is being queried have expired. That is, if the revocation status of a revoked certificate is

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 33 of 67

checked after it has expired, the OCSP service will still respond that it is revoked, as well as the date and time and the reason for revocation.

4.9.10 CRL ARCHIVE

When the DCE Thomas Signe S.A.S. CRL is issued, it is archived during 30 days to provide historic evidence if necessary.

4.10 CERTIFICATE STATUS INFORMATION SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

Thomas Signe S.A.S. offers a free web publication service of Certificate Revocation Lists (CRL), without access restrictions, at the addresses indicated in section 2.1, as well as on the certificates, in its CRL Distribution Points extension.

Thomas Signe S.A.S. offers a free certificate validation service using the OCSP protocol, without access restrictions, at the address indicated in section 2.1, as well as on the certificates, in its Authority Information Access extension.

In addition, Thomas Signe S.A.S. may offer other commercial certificate validation services.

4.10.2 SERVICE AVAILABILITY

Information about the status of certificates will be available online 24 hours a day, 7 days a week.

In the event of system failure, or any other factor beyond the control of the DCE, the DCE will make every effort to ensure that this information service is not unavailable for longer than the maximum period of 8 hours.

4.10.3 ADDITIONAL FEATURES

Information on the status of certificates, not only until they expire, but beyond that date, can be consulted through the OCSP service.

Thomas Signe S.A.S. may have advanced certificate validation services that require a specific license.

4.11 SUBSCRIPTION TERMINATION

The subscription of the certificate will end when the certificate expires or is revoked.

4.12 KEY ESCROW AND RECOVERY


In the case of Subscriber certificates in Centralized HSM, DCE Thomas Signe S.A.S. safeguards the private keys as specified in section 6.2.3, as well as the minimum number of backup copies of the private keys necessary to ensure continuity of service, with the same level of security as for the original private keys and does not offer private key recovery services.

In the case of Subscriber certificates on Other Devices, DCE Thomas Signe S.A.S. does not hold the private keys or backup copies of the private keys, nor does it offer private key recovery services.

5 PHYSICAL, FACILITY, MANAGEMENT AND OPERATIONAL SECURITY CONTROLS

The systems and equipment used for the operations of the digital certification service are managed in outsourced Data Centers.

Security controls cover the physical environment, networks and systems, among others, which are

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 34 of 67

specified below.

All physical security controls are described in procedure GSIGNE-SI-PR-11 Physical and environmental security.

5.1 PHYSICAL CONTROLS

DCE has established physical and environmental security controls to protect the resources of the facilities where the systems and equipment used for operations are located.

The physical and environmental security applicable to certificate issuance and revocation services provides protection against:

- Unauthorized physical access
- Natural disasters
- Fire
- Failure of support systems (electrical power, telecommunications, etc.)
- Floods
- Robbery

- Unauthorized removal of equipment, information, media and applications of components used for DCE services.

The facilities have preventive and corrective maintenance systems with 24h- 365 days a year assistance, with assistance within 24 hours of notification. The location of the facilities guarantees the presence of security forces within 30 minutes.

5.1.1 PHYSICAL LOCATION AND CONSTRUCTION

The DCE facilities are built with materials that guarantee protection against brute force attacks, are located in a low disaster risk area and allow quick access.

The room where cryptographic operations are carried out has a false floor, fire detection and extinguishing, anti-humidity systems, double cooling system and double power supply system.

5.1.2 PHYSICAL ACCESS

Physical access to the premises where certification processes are carried out is limited and protected by a combination of physical and procedural measures.

Access is limited to specifically authorized personnel, with identification at the time of access and registration of access, including CCTV filming.

Access to the rooms is through badge readers.


5.1.3 POWER SUPPLY AND AIR CONDITIONING

The DCE facilities have power stabilizing equipment and a duplicate power supply system for the equipment through a redundant generator set with fuel tanks that can be refilled from the outside.

Rooms housing computer equipment have temperature control systems with duplicate air conditioning equipment.

5.1.4 WATER EXPOSURE

Rooms housing computer equipment are equipped with a humidity detection system.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 35 of 67

5.1.5 FIRE PREVENTION AND PROTECTION

Rooms housing computer equipment are equipped with automatic fire detection and extinguishing systems.

5.1.6 STORAGE SYSTEM

The server systems are run by deploying a highly available virtualized environment, supported by redundant computing devices, high-performance storage and independent production, management and storage networks.

5.1.7 DISPOSAL OF INFORMATION STORAGE MATERIAL

When it is no longer useful, sensitive information is destroyed in the most appropriate way for the medium containing it:

- Printed matter and paper: using shredders or in garbage cans provided for this purpose to be subsequently destroyed, under control.

- Storage media: before being discarded or reused, they must be processed for erasure, either by physical destruction or by rendering the information contained therein unreadable.

5.1.8 OFF-SITE BACKUPS

The DCE maintains a secure off-site storage facility for the custody of paper documents, electronic devices and documents separate from the Data Centers.

At least two specifically authorized persons are required for access, deposit, or removal of devices.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUST ROLES

There are different trust roles for the administration and operation of the Thomas Signe S.A.S. Root CA and Subordinate CA platforms, for the generation of keys and the administration of the Thomas Signe S.A.S. Root CA and Subordinate CA certificate and CRL profiles, and for the administration and operation of the Thomas Signe S.A.S. RA platforms (SAR, RA and Centralized HSM platforms), for the administration and operation of the Thomas Signe S.A.S. Registration Authority.

This ensures a segregation of duties that disseminates control and limits internal fraud, not allowing a single person to control from start to finish all registration and certification functions.


The roles of trust established in the document THS-CO-RRHH-PR-01 Roles and Responsibilities for the administration and operation of these platforms are:

- Information Systems Manager: overall responsible for digital certification processes, registration and digital signature services and data message protection. Within the Root CA and Subordinate CA platforms of Thomas Signe S.A.S., he fulfills the role of CA Auditor

- Digital Certification Manager: responsible for managing the technical infrastructure of electronic services of the DCE, in compliance with the Certification Practices. Within the Root CA and Subordinate CA platforms of Thomas Signe S.A.S., he fulfills the roles of CA Administrator and CA Auditor.

- CA Systems Administrator: responsible for overseeing the technical infrastructure of the DCE's digital certification services. Within the Root CA and Subordinate CA platforms of Thomas Signe S.A.S., he fulfills the roles of CA Administrator and CA Auditor.

- Digital Registry Manager: responsible for the configuration of Thomas Signe's RA platforms, for the supervision of the operations performed on such platforms by the operators with the other roles, and for the

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 36 of 67

operation of the timestamping and data message archiving and preservation services. Within the RA platforms of Thomas Signe S.A.S., he fulfills the role of RA Administrator.

- Registry Operator: responsible for the activities of identity validation of subscribers and review and approval of requests for issuance of digital certificates. Within the RA platforms of Thomas Signe S.A.S., he fulfills the role of RA Agent.

- Registration Authority Decision Operator: responsible for decisions related to the issuance and revocation of digital certificates. Within the RA platforms of Thomas Signe S.A.S., fulfills the role of RA Decision Operator.

- Registration Authority Auditor: audits the LOGs of the Registration Authority. Within the Thomas Signe S.A.S. RA platforms, fulfills the role of RA Auditor.

5.2.2 NUMBER OF PEOPLE REQUIRED PER TASK

Thomas Signe S.A.S. guarantees at least two people to perform the tasks that require multi-person control, according to the procedure THS-CO-AC-AC-PR-10 CA System Access Management, and which are detailed below:

- The generation of CA keys.
- The recovery of a back-up of the CA private key.
- CA certificates issuance.
- The revocation of CA certificates.
- CA private key activation.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

Each trusted role of the Root CA, Subordinate CA and RA platforms is authenticated through the use of secure authentication mechanisms. Authentication within the aforementioned platforms allows access to certain Thomas Signe S.A.S. information assets.

Each person controls the assets required for his or her role, thus ensuring that no person accesses unassigned resources.

5.2.4 ROLES REQUIRING SEGREGATION OF DUTIES

Separation of roles and incompatibilities are determined in document THS-CO-RRHH-PR- 01 Roles and Responsibilities.

CA roles (CA Auditor, CA Administrator) are incompatible with RA roles (RA Administrator, RA Agent, RA Decision Operator, RA Auditor).

RA roles (RA Administrator, RA Agent, RA Decision Operator, RA Auditor) are incompatible with each other.

The incompatibility between the roles of RA Agent and RA Decision Operator ensures independence and impartiality between the functions of reviewing and deciding on the issuance of digital certificates.


5.3 PERSONNEL CONTROLS

5.3.1 REQUIREMENTS FOR PROFESSIONAL QUALIFICATIONS, EXPERIENCE AND KNOWLEDGE

All personnel who perform tasks qualified as reliable without supervision have been working for the DCE for at least two months with an indefinite employment relationship.

All personnel are qualified and have been properly instructed to perform the operations assigned to them.

The DCE ensures that RA personnel are reliable to perform the registration tasks. To this effect an Authorization for their role within Thomas Signe S.A.S. is required.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 37 of 67

The Registration Operator will have completed a preparation course for the performance of registration tasks and validation of requests.

The DCE will remove an employee from his or her trusted functions when it becomes aware of the commission of any criminal act that could affect the performance of these functions.

There is a Signe Group procedure GSIGNE-RRHH-PR-02 Personnel Selection that defines all the requirements for the selection of personnel for professional roles.

5.3.2 BACKGROUND CHECK PROCEDURE

Relevant investigations are conducted prior to the hiring of any employee.

5.3.3 TRAINING REQUIREMENTS

The necessary courses are given to personnel to ensure the correct performance of the tasks assigned to their respective roles, and according to the personal knowledge of each person.

There is a procedure, GSIGNE-RRHH-PR-03 Training, which determines the actions carried out by the group companies for adequate training. There is also an annual training plan.

5.3.4 REQUIREMENTS AND FREQUENCY OF TRAINING UPDATES

Training updates will be provided to personnel at least when changes are made to the tasks assigned to a role that require it, or when requested by an individual.

5.3.5 PENALTIES FOR UNAUTHORIZED ACTIONS

There is an internal sanctioning system (GSIGNE-RRHH-PR-05 Sanctioning Procedure) for unauthorized actions, which may lead to the termination of the employee's employment.

5.3.6 REQUIREMENTS FOR HIRING THIRD PARTIES

Employees of Thomas Signe S.A.S. local technology infrastructure and service companies who have an assigned role within the Thomas Signe S.A.S. business to perform trusted tasks must sign prior confidentiality clauses and operational requirements employed by Thomas Signe S.A.S. Any action that compromises the security of accepted critical processes may result in termination of employment.

5.3.7 DOCUMENTATION PROVIDED TO PERSONNEL

Thomas Signe S.A.S. shall make available to all personnel the documentation detailing the functions entrusted, the policies and practices governing these processes and safety documentation.


In addition, the documentation required by the personnel will be always provided, in order to enable them to perform their duties competently.

5.4 SAFETY AUDIT PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

Thomas Signe S.A.S. records and saves logs of all events related to the DCE security system. These include the following events:

- System startup and shutdown.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 38 of 67

- Login and logout attempts.
- Unauthorized access attempts to DCE systems through the network.
- DCE application logs.
- Powering on and off DCE applications.
- Changes to DCE configuration and/or passwords.
- Changes in the creation of certificate profiles.
- Generation of own keys.
- Certificate lifecycle events.
- Events associated with the cryptographic module.
- Records of the destruction of the media containing the keys, activation data.

Additionally, Thomas Signe S.A.S. keeps, either manually or electronically, the following information:

- CA key creation ceremonies.
- Changes in personnel performing trusted tasks.
- Records of the destruction of material containing key information, activation data or Subscriber personal information, if such information is managed.
- Possession of activation data, for operations with the DCE's private keys.

5.4.2 AUDIT LOG PROCESSING FREQUENCY

Audit logs will be reviewed quarterly and, in any case, when there is a system alert due to the existence of an incident, looking for suspicious or unusual activity.

5.4.3 AUDIT LOG RETENTION PERIOD

Audit log information will be stored for a period of three (03) years to ensure the security of the system.

5.4.4 PROTECTION OF AUDIT LOGS

System logs are protected from tampering by mechanisms that ensure their integrity.

The devices are always operated by authorized personnel.

5.4.5 AUDIT LOG BACKUP PROCEDURES


Thomas Signe S.A.S. has an adequate backup procedure in place so that, in case of loss or destruction of relevant files, corresponding backup copies of the logs are available within a short period of time.

Daily incremental and weekly full copies are made.

In addition, a copy of the audit logs is kept in an external custody center.

5.4.6 AUDIT INFORMATION COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Event audit information is collected internally and automated by the operating system and certification software.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 39 of 67

5.4.7 VULNERABILITY ANALYSIS

The DCE periodically performs a vulnerability review and penetration testing to analyze the DCE infrastructure. Vulnerabilities that DCE believes to be a risk to DCE will then be analyzed and remediated.

5.4.8 OVERSIGHT

Thomas Signe S.A.S. has a SOC (Security Operation Center) and a NOC (Network Operation Center) to monitor all security and communications supervision tasks of the services offered.

These operation centers are described in procedure GSIGNE-SI-PR-11 Physical and environmental security and are located in secure areas.

5.5 ARCHIVING OF RECORDS

5.5.1 TYPES OF RECORDS ARCHIVED

The DCE Thomas Signe S.A.S. will keep the system data that takes place during the life cycle of the certificate. It shall be stored by the CA or, by delegation of the CA, in the RA:

- all audit records (logs),
- all data relating to certificates, including contracts with Subscribers and/or Applicants and data relating to their identification,
- requests for issuance and revocation of certificates,
- all issued certificates,
- CRLs issued or records of the status of certificates generated (OCSP queries).

The DCE is responsible for the correct archiving of all this material and documentation.

5.5.2 RECORDS RETENTION PERIOD

System data relating to the life cycle of certificates shall be retained in accordance with the document retention schedule. The data shall be retained for the period established by current legislation when applicable. Certificates shall be retained for at least seven (07) years from their expiration or revocation. Contracts with Subscribers and/or Applicants and any information relating to the identification and authentication of the Subscriber and/or Applicant shall be retained for at least seven (07) years from their termination.

5.5.3 ARCHIVE PROTECTION

Thomas Signe S.A.S. ensures the proper protection of files, including, among others, the information that is collected for the purpose of issuing certificates, by assigning qualified personnel for their treatment and storage in facilities outside the DCE Data Centers in cases where this is required.


In addition, there are technical and configuration documents detailing all the actions taken to ensure the protection of the files.

5.5.4 ARCHIVAL BACKUP PROCEDURES

Thomas Signe S.A.S. has an external storage center to guarantee the availability of copies of the electronic file archive. Physical documents are stored in secure locations with access restricted to authorized personnel only.

5.5.5 REQUIREMENTS FOR TIME STAMPING OF RECORDS

The records are dated with the reliable source of the National Institute of Metrology (INM) of

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 40 of 67

Colombia, by synchronization through the NTP v4 protocol, according to the RFC 5905 standard "Network Time Protocol Version 4: Protocol and Algorithms Specification". As a secondary time, source, the Time Section of the Royal Institute and Observatory of the Navy in Spain is used.

The technical and configuration documentation of the DCE includes a section on the time configuration of the equipment used in the issuance of certificates.

5.5.6 AUDIT INFORMATION ARCHIVING SYSTEM (INTERNAL OR EXTERNAL)

The DCE's audit information archiving system is internal, although an external storage center is available to ensure the availability of copies of the electronic file archive.

5.5.7 PROCEDURES FOR OBTAINING AND VERIFYING ARCHIVED INFORMATION

Recorded events are protected against unauthorized manipulation.

Only authorized personnel have access to the physical media files and computer files to obtain and carry out integrity checks of these files.

5.6 CHANGE OF PASSWORDS

The procedure for providing, in case of a change of keys of the Root CA or Subordinate CA, the new public key of the CA to Subscribers, Applicants and Third-Party acceptors of certificates issued with the new keys is the same as for providing the current public key of the Root CA and Subordinate CA.

Accordingly, the new CA certificate containing its new public key will be published on the Thomas Signe S.A.S. website.

5.7 INCIDENT AND VULNERABILITY MANAGEMENT PROCEDURES

Thomas Signe S.A.S. has established and tested the continuity and contingency plan aimed at ensuring the continuity of the certification service, should any event occur that compromises the provision of the service (procedure GSIGNE-SI-PR-17 Information Security Aspects for BCM).

Any failure to achieve the goals set by this continuity and contingency plan will be treated as reasonably unavoidable unless such failure is due to a breach of the DCE's obligations to implement such processes.

The security procedure for incident handling, defined in procedure GSIGNE-SI- PR-16 Information Security Incident Management, complies with Annex A of ISO 27001.

As part of the security incidents that are recorded by Thomas Signe S.A.S., are:


- When the security of a DCE private key has been compromised.
- When the DCE security system has been breached.
- When there are failures in the DCE system that compromise the provision of the service.
- When the encryption systems become ineffective because they do not offer the level of security contracted by the Subscriber.
- When any other information security event or incident occurs.

5.7.1 RECOVERY IN CASE OF KEY COMPROMISE

The Thomas Signe S.A.S. hierarchy contingency plan treats the compromise of a DCE private key as a disaster.

In case of compromise of the Root CA's or Subordinate CA's private key, the security of the certificate issuance service will be severely affected, and proceed according to procedure THS- CO- CO-AC-PR-05 Key Management to:

- Inform all subscribers, users and other DCEs with which it has agreements or other types of relationship of the commitment, at least by publishing a notice on the Thomas Signe S.A.S. website

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 41 of 67

- Indicate that certificates and revocation status information signed using this key are invalid.

5.7.2 BUSINESS CONTINUITY AFTER A DISASTER

Thomas Signe S.A.S. has developed the continuity plan to recover all systems after a disaster according to the procedures GSIGNE-SI-PR-17 Information Security Aspects for BCM and THS-CO-SI-PR-01 Risk Management - 03 BIA -DRP.

5.8 TERMINATION OF THE CERTIFICATE ISSUANCE SERVICE

Upon termination of the certificate issuance service of DCE Thomas Signe S.A.S., the following procedure shall be followed according to THS-CO-CO-AC-PR-01 Procedure for Termination of Services:

- Inform ONAC and the Superintendence of Industry and Commerce in the first instance about the cessation of activities thirty (30) days in advance and request their authorization.

- After having been authorized, inform by means of two notices published in newspapers of wide circulation and by the declared e-mail, to all the Subscribers with an interval of fifteen (15) days about the termination of its activity or activities, the precise date of cessation and the legal consequences of this with respect to the certificates issued.

In any case, the continuity of service is guaranteed to users who have already contracted the services of DCE Thomas Signe S.A.S., directly or through third parties, without any additional cost to the services contracted.

6 TECHNICAL SECURITY CONTROLS

Thomas Signe S.A.S. has implemented an organizational security in charge of its management under the regulation UNE-ISO/IEC 27001:2007 subjected to security audits each year. The procedures and security controls of the DCE are performed under the applicable controls of said security standard.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

The generation of the Root CA and Subordinate CA keys is performed, according to a documented key ceremony procedure, inside a secure room, on a FIPS 140-2 level 3 certified hardware cryptographic device (HSM), by authorized personnel with dual control, and in the presence of witnesses and an external auditor.

DCE Thomas Signe S.A.S. guarantees that the signature keys of the Root CA and the Subordinate CA are not used for any other purpose than those indicated in this document.


For Subscriber certificates, key generation shall be performed on devices that reasonably ensure that the private key can only be used by the Subscriber, either by physical means or by the Subscriber establishing appropriate controls and security measures.

In cases where Thomas Signe S.A.S. can guarantee that the Subscriber's cryptographic keys have been created on a cryptographic device that meets the minimum requirements (if the media type is HSM Centralized), this will be indicated on the certificate itself by including the corresponding OID identifier in the Certificate Policies extension.

In any other case (if the media type is Other Devices), the certificates will be issued with a different OID identifier in the Certificate Policies extension.

6.1.2 DELIVERY OF THE PRIVATE KEY TO THE APPLICANT OR SUBSCRIBER

In cases where the DCE generates the private key of the certificates (if the type of support is HSM Centralized), the DCE does not deliver the private key to the Applicant or the Subscriber but will be responsible for ensuring secure access to it by the Subscriber.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 42 of 67

6.1.3 DELIVERY OF THE PUBLIC KEY TO THE CERTIFICATE ISSUER

The public key is sent to the Subordinate CA for certificate generation using the self-signed PKCS #10 format, using a secure channel for transmission.

6.1.4 DELIVERY OF THE PUBLIC KEY OF THE DCE TO TRUSTED THIRD PARTIES

Relying Third Parties will be able to consult the certificates of the Root CA and the Subordinate CA on the Thomas Signe S.A.S. website.

6.1.5 KEY SIZE AND VALIDITY PERIOD

Certificate	RSA key size (bits)	Period of validity
Root CA	4096	20 years From: 14/03/2018 13:50:35, UTC Time To: 14/03/2038 13:50:35, UTC Time
CA Subordinated	4096	From: 14/03/2018 13:59:37, UTC Time To: 14/03/2038 00:00:00, UTC Time
OCSP CA Subordinated	2048	From: 05/04/2018 10:53:48, UTC Time To: 14/03/2038 00:00:00, UTC Time
Subscribers	2048	As a maximum, as established in current legislation and regulations.

6.1.6 PARAMETERS OF PUBLIC KEY GENERATION AND QUALITY VERIFICATION

The parameters recommended in the technical specification document ETSI TS 119 312 are used.

Specifically, the parameters used are as follows:

Signature suite	Hash function	Signature algorithm
sha256-with-rsa	SHA-256	RSA-PKCSv1_5


6.1.7 SUPPORTED KEY USAGES (X.509 V3 KEY USAGE FIELD)

All certificates include the Key Usage and Extended Key Usage extensions, except for the Root CA and Subordinate CA certificates themselves, which only include the Key Usage extension, indicating in both extensions the enabled uses of the keys.

The supported uses for Root CA and Subordinate CA certificates are certificate signing and CRL signing.

The supported key usages for each type of Subscriber certificate are defined in the corresponding Certificate Policy.

6.2 PRIVATE KEY PROTECTION AND ENGINEERING CONTROLS FOR CRYPTOGRAPHIC MODULES

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 43 of 67

6.2.1 CONTROLS AND STANDARDS FOR CRYPTOGRAPHIC MODULES

The cryptographic modules used to generate and store Root CA and Subordinate CA (HSM) keys are FIPS 140-2 level 3 certified.

The keys of the Certificate Subscribers in Centralized HSM are securely generated in a cryptographic device with FIPS 140-2 level 3 certification, resulting in a high level of assurance, to protect the private keys against risks such as:

- Malicious code attacks
- Unauthorized export of keys
- Spoofing due to carelessness of the Subscriber in the custody of cryptographic devices
- Physical damage to the cryptographic module

6.2.2 MULTI-PERSON (N OF M) CONTROL OF THE PRIVATE KEY

Access to the Root CA and Subordinate CA private keys is under multi-person control, requiring 2 of 3 authorized persons, using their respective PIN-protected cryptographic devices, to access and activate the private keys.

This control ensures that one person does not have individual control, decentralizing the responsibility for activating and using the private keys of the Root CA and the Subordinate CA.

6.2.3 PRIVATE KEY ESCROW

The Root CA's private key is guarded by hardware cryptographic devices (HSM) certified with the FIPS 140-2 level 3 standard, guaranteeing that the private key is never in the clear outside the cryptographic device. The activation and subsequent use of the private key requires the multi-person control detailed in Section 6.2.2.

The private key of the Subordinate CA is guarded by hardware cryptographic devices (HSM) certified to the FIPS 140-2 level 3 standard, guaranteeing that the private key is never in the clear outside the cryptographic device. Activation of the private key requires the multi-person control detailed in section 6.2.2.

In the case of subscriber certificates in Centralized HSM, DCE Thomas Signe S.A.S. safeguards the private keys protected by strong encryption methods in FIPS 140-2 level 3 certified hardware cryptographic devices (HSMs) that use a key residing in the HSMs and another key derived from a password defined by the Subscriber or Applicant.

6.2.4 PRIVATE KEY BACKUP

There are devices that allow the restoration of the Root CA and Subordinate CA private keys, which are securely stored and only accessible by authorized personnel, using different controls, one of them being dual control on a secure physical medium.


The private keys of the Root CA and Subordinate CA can be restored by a process that requires the use of 2 of 3 cryptographic devices.

In the case of subscriber certificates in Centralized HSM, the DCE Thomas Signe S.A.S. keeps the minimum number of backup copies of the private keys necessary to ensure continuity of service, with the same level of security as for the original private keys.

6.2.5 PRIVATE KEY ARCHIVING

Thomas Signe S.A.S. will archive the private key of the Root CA after the expiration of all self- signed certificates containing the corresponding public key for two years.

Thomas Signe S.A.S. will archive the private key of the Subordinate CA after the expiration or

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 44 of 67

revocation of all certificates issued by the Root CA containing the corresponding public key for two years.

The archived keys are subjected to the same security controls as the private keys that are currently in use. These keys are destroyed after the archive period by means of dual control in a secure environment.

The access to the private keys is reserved to the processes that require to validate historic evidence. It is carried out by dual control in a secure environment.

6.2.6 TRANSFERRING THE PRIVATE KEY TO OR FROM A CRYPTOGRAPHIC MODULE

Private keys from the Root CA and Subordinate CA can be transferred to or from a cryptographic module (HSM) by a process that requires the use of 2 of 3 cryptographic devices.

6.2.7 STORAGE OF THE PRIVATE KEY IN A CRYPTOGRAPHIC MODULE

There are key ceremony documents from Thomas Signe S.A.S., where the processes of generation and storage of private keys by the cryptographic modules used (HSM) are described.

6.2.8 PRIVATE KEY ACTIVATION METHOD

The private keys of the Root CA and the Subordinate CA are activated in their HSMs by a process that requires the use of 2 of 3 cryptographic devices, which, together with their respective PINs, constitute, therefore, the activation data of the private key.

In the case of certificates for Natural Person, Company/Entity Binding and Legal Representative in Centralized HSM, the access to the private key is done by means of a username of the Subscriber, a user password defined by the Subscriber, a certificate password defined by the Subscriber, and by a code that the Subscriber receives in his/her cell phone every time he/she tries to access the private key. This username, these two passwords and this code constitute, therefore, the activation data of the private key.

In the case of certificates for Automated Signature in Centralized HSM, the access to the private key is done by means of a password of the certificate defined by the Applicant, and by codes provided to the Applicant by the RA. This password and these codes constitute, therefore, the activation data of the private key.

In the case of certificates for Automated Signature in Other Devices, the access to the private key is done by means of the specific data determined by the type of cryptographic device where the private key has been generated or installed, according to the security level that the Subscriber considers appropriate. This specific data determined by the type of cryptographic device therefore constitutes the activation data of the private key.

6.2.9 PRIVATE KEY DEACTIVATION METHOD

The Root CA's private key will be deactivated in its HSMs after use, procedurally.

The private key of the Subordinate CA shall only be deactivated in its HSMs in extraordinary situations.


In the case of Subscriber certificates in Centralized HSM, the private key will be deactivated after each use.

In the case of Subscriber certificates in Other Devices, the private key shall be deactivated in the specific manner determined by the type of cryptographic device where the private key was generated or installed, according to the security level that the Subscriber deems appropriate.

6.2.10 PRIVATE KEY DESTRUCTION METHOD

The destruction of the private key of the Root CA or the Subordinate CA is carried out according to the procedure THS-CO-AC-AC-PR-05 Key Management, by authorized personnel.

A secure deletion of the CA's private key will be performed, using the functions provided by the

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 45 of 67

hardware cryptographic devices used (HSM), so that the rest of the keys managed by the devices are not affected.

Likewise, all backup copies of the CA's private key, which have been identified, will be securely erased.

6.2.11 CLASSIFICATION OF CRYPTOGRAPHIC MODULES

As specified in Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVING

The certificates issued by DCE Thomas Signe S.A.S., and therefore the public keys, shall be kept for the period required by current legislation where applicable, or for at least 3 years from their expiration.

6.3.2 OPERATIONAL PERIOD OF THE CERTIFICATES AND PERIOD OF USE OF THE KEY PAIR

The operational period of a certificate and the period of use of its key pair will be determined by the validity period or revocation of the certificate.

The private key must not be used after the validity period or revocation of the certificate.

The public key must not be used after the validity period or revocation of the certificate, except by relying on Third Parties to verify historical data.

6.4 ACTIVATION DATA

6.4.1 GENERATION AND INSTALLATION OF ACTIVATION DATA

The activation data for the Root CA and Subordinate CA private keys were securely generated during the Thomas Signe S.A.S. key ceremony.


In the case of Subscriber certificates in the Centralized HSM, the private key activation data are generated before the keys are generated in the Centralized HSM (Subscriber's username, user password defined by the Subscriber, part of the codes provided to the Applicant by the RA), at the same time the keys are generated in the Centralized HSM in the instant prior to the issuance of the certificate (certificate password defined by the Subscriber or the Applicant), after the issuance of the certificate (code related to the certificate provided to the Applicant by the RA), and each time the private key is accessed in the Centralized HSM (code received on the Subscriber's cell phone).

In the case of Subscriber certificates in Other Devices, the private key activation data is generated in the specific way determined by the type of cryptographic device where the private key has been generated or installed, according to the security level that the Subscriber considers appropriate.

6.4.2 PROTECTION OF ACTIVATION DATA

Only authorized personnel have access/knowledge to/from the activation data of the Root CA and Subordinate CA private keys.

For Subscriber certificates, once delivery of the device and/or activation data has been made, it is the Subscriber's responsibility to maintain the confidentiality of this data.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 46 of 67

6.4.3 IT SECURITY CONTROLS

Thomas Signe S.A.S. employs reliable systems and commercial products to provide its certification services.

The equipment used is initially configured with the appropriate security profiles by Thomas Signe S.A.S. systems personnel in the following aspects:

- Security configuration of the operating system.
- Application security configuration.
- Correct sizing of the system.
- Configuration of users and permissions.
- Event log configuration.
- Backup and recovery plan.
- Network traffic requirements.

The technical and configuration documentation of Thomas Signe S.A.S. details the architecture of the equipment providing the certification service both in its physical and logical security.

6.4.4 SPECIFIC TECHNICAL SECURITY REQUIREMENTS

Each Thomas Signe S.A.S. server includes the following functionalities:

- Access control to Thomas Signe S.A.S. services and privilege management.
- Imposition of separation of duties for privilege management.
- Identification and authentication of roles associated with identities.
- Archiving of Subscriber and Thomas Signe S.A.S. history and audit data.
- Auditing of security-related events.
- Self-diagnosis of security related to Thomas Signe S.A.S. services.
- Thomas Signe S.A.S. system and key recovery mechanisms.

The above functionalities are provided through a combination of operating system, PKI software, physical protection, and procedures.

6.4.5 IT SECURITY ASSESSMENT

The security of the equipment is reflected 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.

Physical security is guaranteed by the facilities already defined above and personnel management is easy due to the reduced number of people working in the outsourced Data Centers.

6.5 LIFE CYCLE SECURITY CONTROLS


6.5.1 SYSTEM DEVELOPMENT CONTROLS

Thomas Signe S.A.S. has a procedure to control changes in the versions of operating systems and applications that imply an improvement in their security functions or that correct any detected vulnerability.

6.5.2 SECURITY MANAGEMENT CONTROLS

Security management

Thomas Signe S.A.S. develops the necessary activities for the training and awareness of employees in security matters.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 47 of 67

Classification and management of information and assets

Thomas Signe S.A.S. maintains an inventory of assets and documentation.

Documents are catalogued in three levels: PUBLIC, INTERNAL and CONFIDENTIAL.

Classification and management of information and assets

Thomas Signe S.A.S. has procedures for incident management (GSIGNE-SI-PR-16 Information Security Incident Management) and business continuity (GSIGNE-SI-PR-17 Information Security Aspects for BCM).

Thomas Signe S.A.S. has fireproof security boxes for the storage of physical media.
media.

Thomas Signe S.A.S. has documented the entire procedure related to the roles and responsibilities of the personnel involved in the certification process.

Handling of media and security

All media will be handled securely in accordance with information classification requirements. Media containing sensitive data are securely destroyed if they are no longer required.

System Planning

The Systems department of Thomas Signe S.A.S. keeps a record of equipment capacities.

A resizing can be planned in coordination with the resource control application of each system.


System Access Management

Thomas Signe S.A.S. makes every effort reasonably within its power to confirm that access to the system is limited to authorized persons. In particular:

- a) General management of Thomas Signe S.A.S.:
 - High-availability firewall-based controls are in place.
 - Sensitive data are protected by cryptographic techniques or access controls with strong authentication.
 - A procedure is in place for changing the owners and custodians of safes.
 - A procedure is in place to ensure that operations are carried out in accordance with the established roles.
 - Each person has an identifier associated with him/her to perform certification operations according to his/her role.
 - Thomas Signe S.A.S. personnel are responsible for their actions, for example, for withholding event logs.

- b) Certificate generation:
 - The DCE facilities are equipped with continuous monitoring systems and alarms to detect, record and be able to act upon an unauthorized and/or irregular access attempt to its resources.
 - Authentication for the certificate issuance process is performed through a system of m operators for the activation of the private key of the Root CA and the Subordinate CA of Thomas Signe S.A.S.

- c) Revocation Management:
 - DCE facilities are equipped with continuous monitoring systems and alarms to detect, record and be able to act upon an unauthorized and/or irregular attempt to access its resources through the revocation system.
 - Revocation refers to the permanent loss of effectiveness of a digital certificate. The revocation will

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 48 of 67

be performed by strong authentication by certificate to the applications by an authorized operator. The log systems will generate the proofs that guarantee the non-repudiation of the action performed by the operator of Thomas Signe S.A.S.

d) Revocation status

- The revocation status application has an access control based on certificate authentication to prevent attempts to modify revocation status information.

CA cryptographic hardware lifecycle management

- Thomas Signe S.A.S. ensures that the cryptographic hardware used for signing certificates is not tampered with during transport.
- The cryptographic hardware is built on supports prepared to avoid any manipulation.
- Thomas Signe S.A.S. records all relevant device information to add to the Thomas Signe S.A.S. asset catalog.
- The use of cryptographic certificate signing hardware requires the use of at least two trusted employees.
- Thomas Signe S.A.S. performs periodic tests to ensure the correct functioning of the devices.
- The cryptographic devices are only handled by trusted personnel.
- The Root CA and Subordinate CA private signing keys stored in the cryptographic hardware will be deleted once the devices have been removed.
- The configuration of the DCE system as well as its modifications and updates are documented and controlled.
- Thomas Signe S.A.S. has a maintenance contract for the device for its proper maintenance. Changes or updates are authorized by the security manager and are reflected in the corresponding work reports. These configurations are performed by at least two reliable persons.

6.6 NETWORK SECURITY CONTROLS

The DCE protects physical access to network management devices and has an architecture that sorts the generated traffic based on its security characteristics by creating clearly defined network sections. This division is done using firewalls.

6.7 TIME STAMPING

The time for DCE services are obtained by consulting the National Metrology Institute (INM) of Colombia, in accordance with the provisions of Article 14 of Decree 4175 of 2011, which split some functions of the Superintendence of Industry and Commerce and created the National Metrology Institute -INM, from November 3, 2011, the latter institution is responsible for maintaining, coordinating and disseminating the legal time of the Republic of Colombia, adopted by Decree 2707 of 1982.


The servers are kept updated with UTC time, by synchronization through the NTP v4 protocol, according to the RFC 5905 standard "Network Time Protocol Version 4: Protocol and Algorithms Specification".

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 CERTIFICATE FORMAT

The certificates issued by DCE Thomas Signe S.A.S. are X.509 v3 certificates, according to the following standards:

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 49 of 67

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

- ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

Additionally, the certificates issued by Thomas Signe S.A.S. are consistent with the following standards:

The following table specifies the common profile of the certificates issued by the Root CA and the Subordinate CA of DCE Thomas Signe S.A.S.

COMMON PROFILE OF CERTIFICATES		
Certificate field	Description	Value
Version	Version Number	v3
serialNumber	Serial Number	Unique positive integer with respect to the CA issuing the certificate ¹
Signature	Signature Algorithm	OID ² and signature algorithm parameters
Issuer	Issuer (DN)	DN of the CA issuing the certificate ³
validity	notBefore	Valid from Certificate validity start date and time, UTC Time ⁴
	notAfter	Valid to Date and time of end of certificate validity, UTC Time ⁵
Subject	Subject (DN)	DN of the certificate holder ⁶
subjectPublicKeyInfo	Public Key	OID ⁷ and algorithm parameters and public key value ⁸
Extensions	Certificate Extensions	Certificate extensions ⁹

¹ Random value of 20 bytes

² sha256WithRSAEncryption (see OID in section 7.1.3)

³ DCE Thomas Signe S.A.S. Root CA, Subordinate CA and TSU TSA certificates: see Root CA DN in section 7.1.4; DCE Thomas Signe S.A.S. OCSP Subordinate CA and Subscriber certificates: see Subordinate CA DN in section 7.1.4.

⁴ Date and time of certificate issuance.


⁵ Thomas Signe S.A.S. DCE Root CA, Subordinate CA and OCSP Subordinate CA Certificates: see validity period in section 6.1.5; Thomas Signe S.A.S. DCE TSU TSA Certificate: see validity period in the CPS for Thomas Signe S.A.S. timestamp; Thomas Signe S.A.S. DCE Subscriber Certificates: see validity period in the CP corresponding to the type of certificate.

⁶ Thomas Signe S.A.S. DCE Root CA and Subordinate CA Certificates: see DN in section 7.1.4; Thomas Signe S.A.S. DCE Subordinate CA OCSP Certificate: see DN in section 7.4.4; Thomas Signe S.A.S. DCE TSU TSA Certificate: see DN in section 7.4.4; Thomas Signe S.A.S. DCE TSU TSA Certificate: see DN for Thomas Signe S.A.S. timestamp. A.S: see DN in the CPS for Thomas Signe S.A.S. time stamping; DCE Thomas Signe S.A.S. Subscriber Certificates: see DN of the holder in the CP corresponding to the type of certificate.

⁷ rsaEncryption (see OID in section 7.1.3)

⁸ Thomas Signe S.A.S. DCE Root CA, Subordinate CA, OCSP Subordinate CA and Subscriber certificates: see RSA key size in section 6.1.5; Thomas Signe S.A.S. DCE TSU TSA certificate: see RSA key size in the CPS for Thomas Signe S.A.S. timestamp.

⁹ Thomas Signe S.A.S. DCE Root CA and Subordinate CA Certificates: see extensions in section 7.1.2 Thomas Signe S.A.S. DCE Subordinate CA OCSP Certificate: see extensions in section 7.4. 2; DCE Thomas Signe S.A.S. TSU TSA Certificate: see extensions in the CPS for Thomas Signe S.A.S. time stamping; DCE Thomas Signe S.A.S. Subscriber Certificates: see extensions in the CP corresponding to the type of certificate.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 50 of 67

7.1.2 CERTIFICATE EXTENSIONS

The following tables specify the certificate extensions of the Root CA and Subordinate CA certificates of DCE Thomas Signe S.A.S.


CA ROOT CERTIFICATE EXTENSIONS - THOMAS SIGNE ROOT		
Extension	Critical	Value
Subject Key Identifier	-	Identifier of the public key of the certificate, obtained from the SHA-1 hash of the certificate.
Key Usage	Yes	keyCertSign cRLSign
Certificate Policies	-	OID anyPolicy (2.5.29.32.0) URI of CPS: http://thsigne.com/cps
Basic Constraints	Yes	cA: TRUE

EXTENSIONS TO THE SUBORDINATED AC CERTIFICATE - DCE THOMAS SIGNE COLOMBIA		
Extension	Critical	Value
Authority Key Identifier	-	Public key identifier of the Root CA certificate, obtained from the SHA-1 hash of the Root CA certificate.
Subject Key Identifier	-	Identifier of the public key of the certificate, obtained from the SHA-1 hash of the certificate.
Key Usage	Yes	keyCertSign cRLSign
Certificate Policies	-	OID anyPolicy (2.5.29.32.0) URI of CPS: http://thsigne.com/cps
Basic Constraints	Yes	cA: TRUE pathLenConstraint: 0
CRL Distribution Points	-	URI of CRL: http://crl.thsigne.com/thomas_signe_root.crl
Authority Information Access	-	URI of the Root CA certificate: http://thsigne.com/certs/thomas_signe_root.crt

Section 7.4.2 specifies the OCSP certificate extensions of the DCE Thomas Signe S.A.S. Subordinate CA.

In the CP for each type of certificate, the extensions of the corresponding DCE Thomas Signe S.A.S. Subscriber certificates are specified.

The CPS for the Thomas Signe S.A.S. time stamping specifies the extensions of the TSU certificate of the TSA of DCE Thomas Signe S.A.S.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 51 of 67

7.1.3 OBJECT IDENTIFIERS (OID) OF ALGORITHMS

Name	OID	Description
sha256WithRSAEncryption	1.2.840.113549.1.1.11	Certificate signing algorithm, CRL and OCSP responses
rsaEncryption	1.2.840.113549.1.1.1	Public key algorithm in certificates

7.1.4 NAME FORMATS


The following tables specify the corresponding attributes of the DN of the Root CA and the Subordinate CA of the DCE Thomas Signe S.A.S.

DN OF THE ROOT CA - THOMAS SIGNE ROOT		
DN attribute	Description	Value
Country Name (C)	Country	CO ¹⁰
State or Province Name (ST)	State/Province	Capital District ¹¹
Locality Name (L)	City	Bogota ²
Street Address (STREET)	Address	see current address at www.thomas-signe.com ²
Organization Identifier (2.5.4.97)	Organization Identifier	900962071-5 ²
Organization Name (O)	Organization Name	Thomas Signe Soluciones Tecnológicas Globales S.A.S. ²
Common Name (CN)	Name	Thomas Signe Root ²

¹⁰ Encoded in PrintableString

¹¹ Encoded in UTF8String

DN OF SUBORDINATE CA - DCE THOMAS SIGNE COLOMBIA		
DN attribute	Description	Value
Country Name (C)	Country	CO ¹²
State or Province Name (ST)	State/Province	Capital District ¹³
Locality Name (L)	City	Bogota ²
Street Address (STREET)	Address	see current address at www.thomas-signe.com ²

	Certification Practice Statement for Certificate Issuance		Version 2.8
	Code: THS-CO-AC-DPC-01		Page 52 of 67
Organization Identifier (2.5.4.97)	Organization Identifier	900962071-5 ²	
Organization Name (O)	Organization Name	Thomas Signe Soluciones Tecnológicas Globales S.A.S. ²	
Common Name (CN)	Name	DCE Thomas Signe Colombia ²	

Section 7.4.4 specifies the DN of the OCSP certificate of the DCE Thomas Signe S.A.S. Subordinate CA.

In the CP for each type of certificate, the DN of the holder of the corresponding DCE Thomas Signe S.A.S. Subscriber certificates are specified.

The CPS for the Thomas Signe S.A.S. time stamping specifies the DN of the TSU certificate of the Thomas Signe S.A.S. TSA.

7.1.5 NAME RESTRICTIONS

As specified in sections 3.1 and 7.1.4 and in the CP of each type of certificate

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)

The OCSP certificate policy OID of the DCE Thomas Signe S.A.S. Subordinate CA is specified in section 7.4.2 and also below: 1.3.6.1.1.4.1.51362.0.2.0.1

The Certificate Policy OIDs of each type of DCE Thomas Signe S.A.S. Subscriber certificates are specified in section 1.4 and in the corresponding CP.

The Thomas Signe S.A.S. DCE TSA TSU certificate policy OID is specified in the CPS for Thomas Signe S.A.S. time stamping.

¹² Encoded in PrintableString

¹³ Encoded in UTF8String


7.1.7 USE OF POLICY CONSTRAINTS EXTENSION

Certificates issued by the Root CA and Subordinate CA of DCE Thomas Signe S.A.S. do not contain the Policy Constraints extension.

7.1.8 SYNTAX AND SEMANTICS OF POLICY QUALIFIERS

The Certificate Policies extension of the certificates issued by the Root CA and the Subordinate CA of DCE Thomas Signe S.A.S. contains the following Policy Qualifiers:

- id-qt-cps (URI of the CPS): contains the URI where the latest version of the present CPS can be found, as well as, in the case of DCE Thomas Signe S.A.S. Subscriber certificates, the PC corresponding to the type of certificate.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 53 of 67

7.1.9 SEMANTIC TREATMENT FOR CERTIFICATE POLICIES EXTENSION

The Certificate Policies extension of the certificates issued by the Root CA and the Subordinate CA of DCE Thomas Signe S.A.S. allows identifying the policy that DCE Thomas Signe S.A.S. associates to the type of certificate and where this CPS can be found, as well as, in the case of DCE Thomas Signe S.A.S. Subscriber certificates, the CP corresponding to the type of certificate.

7.2 CRL PROFILE

7.2.1 FORMAT AND VALIDITY PERIOD

The CRLs issued by DCE Thomas Signe S.A.S. are CRL X.509 v2, according to the following standards:


- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

The following table specifies the common profile of the CRLs issued by Thomas Signe S.A.S. Root CA and Subordinate CA.

CRL PROFILE			
CRL Field		Description	Value
version		Version Number	v2
signature		Signature Algorithm	OID ¹⁴ and signature algorithm parameters
issuer		Issuer (DN)	DN of the CA issuing the CRL ¹⁵
thisUpdate		Date and time of issuance of this CCC	Date and time of issuance of the CCC, UTC Time
nextUpdate		Date and time of issuance of the next CRL	CRL end of validity date, UTC Time ¹⁶
revokedCertificates	userCertificate	Serial number of the revoked certificate	Serial number of the revoked certificate
	revocationDate	Certificate revocation date and time	Date and time of certificate revocation, UTC Time
	crlEntryExtensions	CRL input extensions	CRL Entry Extensions
crlExtensions		CRL Extensions	CRL Extensions

7.2.2 CRL EXTENSIONS AND CRL INPUT EXTENSIONS

CRL EXTENSIONS		
Extension	Critical	Value
Authority Key Identifier	-	Identifier of the public key of the certificate of the CA issuing the CRL, obtained from the SHA-1 hash of the certificate.
CRL Number	-	Incremental number, with respect to the CA issuing the CRL

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 54 of 67

CRL INPUT EXTENSIONS		
Extension	Critical	Value
Reason Code	-	Certificate revocation reason code

¹⁴ sha256WithRSAEncryption (see OID in section 7.1.3)

¹⁵ Root CA CRL: see DN of the Root CA in section 7.1.4; Subordinate CA CRL: see DN of the Subordinate CA in section 7.1.4

¹⁶ Root CA CRL: 180 days; Subordinate CA CRL: 4 days

7.3 OCSP PROFILE

The OCSP profile of the DCE Thomas Signe S.A.S. Subordinate CA conforms to the RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" standard, with the following particularities:

- OCSP response signing algorithm: sha256WithRSAEncryption (see OID in section 7.1.3)

7.4 OCSP CERTIFICATE PROFILE

7.4.1 CERTIFICATE FORMAT

The format of the OCSP certificate of the DCE Thomas Signe S.A.S. Subordinate CA complies with that specified in section 7.1.1.

Additionally, the OCSP certificate of the DCE Thomas Signe S.A.S. Subordinate CA is consistent with the following standards:

- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.


The OCSP certificate of the Subordinate CA of DCE Thomas Signe S.A.S. has been issued by the Subordinate CA itself (Thomas Signe Colombia).

The key size and validity period of the certificate is indicated in section 6.1.6.

7.4.2 CERTIFICATE EXTENSIONS

The following table specifies the OCSP certificate extensions of the DCE Thomas Signe S.A.S. Subordinate CA.

Extension	Critical	Value
Authority Key Identifier	-	Identifier of the public key of the certificate of the Subordinate CA, obtained from the SHA-1 hash of the certificate.
Subject Key Identifier	-	Identifier of the public key of the certificate, obtained from the SHA-1 hash of the certificate.
Key Usage	Yes	digitalSignature nonRepudiation
Certificate Policies	-	OID 1.3.6.1.4.1.51362.0.2.0.1 URI of CPS: http://thsigne.com/cps

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 55 of 67

Basic Constraints	Yes	cA: FALSE
Extended Key Usage	Yes	OCSPSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points	-	URI of CRL: http://crl-co.thsigne.com/DCE_thomas_signe_colombia.crl
Authority Information Access	-	URI of the certificate of the Subordinate CA: http://thsigne.com/certs/DCE_thomas_signe_colombia.crt

7.4.3 OBJECT IDENTIFIERS (OID) OF ALGORITHMS

As specified in Section 7.1.3.

7.4.4 NAME FORMATS

The following table specifies the corresponding attributes of the DN of the OCSP certificate of the DCE Thomas Signe S.A.S. Subordinate CA.


DN attribute	Description	Value
Country Name (C)	Country	CO ¹⁷
State or Province Name (ST)	State/Province	Capital District ¹⁸
Locality Name (L)	City	Bogota ²
Street Address (STREET)	Address	see current address at www.thomas-signe.com ²
Organization Identifier (2.5.4.97)	Organization Identifier	900962071-5 ²
Organization Name (O)	Organization Name	Thomas Signe Soluciones Tecnológicas Globales S.A.S. ²
Common Name (CN)	Name	DCE Thomas Signe Colombia – OCSP ²

7.4.5 NAME RESTRICTIONS

As specified in sections 3.1, 7.1.4 and 7.4.4.

7.4.6 CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)

The OCSP certificate policy OID of the DCE Thomas Signe S.A.S. Subordinate CA is specified in section 7.4.2 and also below: 1.3.6.1.1.4.1.51362.0.2.0.1

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 56 of 67

7.4.7 USE OF POLICY CONSTRAINTS EXTENSION

The OCSP certificate of the DCE Thomas Signe S.A.S. Subordinate CA does not contain the Policy Constraints extension.

¹⁷ Encoded in PrintableString

¹⁸ Encoded in UTF8String

7.4.8 SYNTAX AND SEMANTICS OF POLICY QUALIFIERS

As specified in section 7.1.8.

7.4.9 SEMANTIC TREATMENT FOR THE CERTIFICATE POLICY EXTENSION

As specified in section 7.1.9.

8 COMPLIANCE AUDIT AND OTHER CONTROLS

Thomas Signe S.A.S. is subject to accreditation audits conducted by ONAC in accordance with the provisions of Article 162 of Decree-Law 19 of 2012. Likewise, in accordance with the requirements of ONAC's Specific Accreditation Criteria, Thomas Signe S.A.S. submits to internal audits and third-party audits in the terms set forth in said document.

If required, Thomas Signe S.A.S. allows and facilitates audits by the Superintendence of Industry and Commerce of Colombia.

8.1 AUDIT FREQUENCY

Audits will be performed annually following the internal procedure GSIGNE-GRAL-PR-03 Audit.

8.2 AUDITOR IDENTITY/QUALIFICATION

Accreditation audits that fall under the responsibility of Thomas Signe S.A.S. are performed by auditors appointed by ONAC.

Internal and third-party audits are carried out by auditors who comply with the ONAC Specific Criteria in force and following the internal procedure GSIGNE-GRAL-PR-03 Audit.

8.3 RELATIONSHIP BETWEEN THE AUDITOR AND THE AUDITED ENTITY


The companies that perform external audits never present conflicts of interest that could distort their performance in their relationship with Thomas Signe S.A.S.

8.4 ASPECTS COVERED BY THE CONTROLS

The audits generally verify compliance with the principles established in the accreditation requirements (ONAC Specific Criteria in force), the applicable legislation in force and the documentation established in the DCE's management system. These aspects must be identified and controlled following the internal procedure GSIGNE-GRAL-PR-03 Audit.

8.5 ACTIONS TO BE TAKEN AS A RESULT OF DETECTION OF DEFICIENCIES

If incidents or non-conformities are detected, the appropriate measures will be taken to resolve them as soon as possible, following the internal procedure GSIGNE-GRAL-PR-03 Audit.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 57 of 67

8.6 COMMUNICATION OF RESULTS

The auditing body will communicate with the DCE through the interlocutor established in each case.

9 OTHER LEGAL AND BUSINESS MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE FEES

In the CP of each type of certificate, the issuance fees for the corresponding certificates are specified.

The rates specified in the CP are referential, so they may vary according to the type of certificate and the contract with each client.

The same rates are published on the Thomas Signe S.A.S. website.

The final price including VAT for the requested certificate will be indicated in the commercial proposal.

9.1.2 CERTIFICATE ACCESS FEES

Access to the certificates issued by the respective Subscribers and/or Applicants is free of charge.

9.1.3 REVOCATION OR ACCESS TO STATUS INFORMATION FEES

There is no fee for certificate revocation, nor for access to certificate status information.

Thomas Signe S.A.S. provides free access to certificate status information through the publication of the corresponding CRLs and the OCSP service.

Thomas Signe S.A.S. may offer other commercial certificate validation services, the fees for which will be negotiated with each customer for these services.

9.1.4 FEES FOR OTHER SERVICES

The rates applicable to other possible services will be negotiated between Thomas Signe S.A.S. and the customers of the services offered.

9.1.5 REFUND POLICY

DCE Thomas Signe S.A.S. has a Refund Policy (THS-CO-AC-POL-07 Refund Policy), which is referenced in contracts with its customers and published on the Thomas Signe website.


9.2 FINANCIAL LIABILITIES

9.2.1 INSURANCE COVERAGE

to face the risk of liability for damages to the users of its services and to third parties, guaranteeing its responsibilities in its activity as a DCE as defined in the Colombian legislation in force.

The guarantee is established by means of a Civil Liability Insurance with a coverage equal to or higher than that required by the Colombian legislation in force.

The characteristics of such insurance are as follows:

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 58 of 67

- It is issued by an insurance company supervised by the Financial Superintendence of Colombia.
 - It covers contractual and extra-contractual risks and damages of subscribers and third parties in good faith.
 - The insurance company is responsible for previously informing ONAC of the termination of the insurance contract or if modifications are made that reduce the scope or amount of the agreed coverage.
 - Covers the automatic restitution of the insured value.
 - The insurance entity, the policyholder and the insured are obliged to previously inform ONAC of the termination of the insurance contract or if modifications are made that reduce the scope or amount of coverage.
- The insurance shall cover all amounts that Thomas Signe S.A.S. may be legally obliged to pay, up to the contracted limit of coverage, as a result of any legal proceedings in which its liability may be declared, derived from any negligent act, error or unintentional breach of the legislation in force, among others.
- There is no coverage for third party acceptors.

9.3 CONFIDENTIALITY OF INFORMATION

Thomas Signe S.A.S. considers confidential all information that is expressly classified as confidential. No information declared as confidential shall be disseminated without the express written consent of the person or entity that has granted it the confidential nature, unless there is a legal imposition, in which case, unless prohibited by law, such person or entity shall be notified of the information provided.

9.3.1 CONFIDENTIAL INFORMATION


- In particular, the following information will be considered confidential:
- Thomas Signe S.A.S. Root CA and Subordinate CA private keys.
 - Minutes of the Root CA and Subordinate CA key generation procedure. Root CA and Subordinate CA Key Generation Procedure.
 - Business information provided and/or elaborated jointly with Thomas Signe S.A.S. by its customers, suppliers or other persons with whom Thomas Signe is committed to keep legally or conventionally established secrecy.
 - The results of identity validations of Subscribers and/or Applicants, provided by public or private sources.
 - Subscriber and/or Applicant information obtained from sources other than the Subscriber and/or Applicant and which has been expressly classified as confidential.
 - Data collected during digital certification

9.3.2 NON-CONFIDENTIAL INFORMATION

- The following information shall be considered non-confidential:
- That contained in this CPS.
 - The information contained in the different Certificate Policies (CP).
 - The information contained in the certificates, since for their issuance the Subscriber and/or Applicant previously grants its consent, including the different states or situations of the certificate.
 - The lists of revoked certificates (CRL), as well as the remaining revocation status information.
 - Any other information whose publication is required by law.

9.3.3 RESPONSIBILITY FOR THE PROTECTION OF CONFIDENTIAL INFORMATION

It is the responsibility of DCE Thomas Signe S.A.S. and its suppliers to establish adequate measures for the protection of confidential information.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 59 of 67

9.4 DATA PROTECTION POLICY

Thomas Signe S.A.S. guarantees the protection of personal data of Subscribers and/or Applicants of digital certification services, in compliance with the Statutory Law 1581 of 2012, partially regulated by National Decree 1377 of 2013; Decrees 1377 of 2013 and 886 of 2014, Law 1266 of 2008 and other related regulatory decrees, which regulates the provisions of Law 1581 of 2012, which issued the General Regime for the Protection of Personal Data, which aims to "(..) to develop the constitutional right of all persons to know, update and rectify the information collected about them in databases or files, and the other rights, freedoms and constitutional guarantees referred to in Article 15 of the Constitution; as well as the right to information enshrined in Article 20 of the same" and the Specific Criteria for Accreditation of Digital Certification Entities - CEA-3.0-07 in force.

Information such as names, address, email, and any information that can be linked to the identity of a natural or legal person, contained in the contracts and applications of Subscribers and/or Applicants, will be considered personal data. This information will be considered confidential and will be used exclusively for the stipulated digital certification operations, unless there is a prior consent of the end user of such data or there is a judicial or administrative order that so determines, in which case, unless prohibited by law, the Subscriber or the person involved will be notified of the information provided.

It is the responsibility of the Subscribers and/or Applicants to ensure that the information provided to Thomas Signe S.A.S. is truthful and current. Likewise, they are responsible for any damage they may cause by providing false, incomplete, or inaccurate information.

Thomas Signe S.A.S. has a Privacy Policy for personal data that details the principles, collection and processing of personal data and is published on the website: <https://thomas-signe.co/otras-politicas-y-procedimientos/>.

9.5 INTELLECTUAL PROPERTY RIGHTS

In accordance with the provisions of national laws and international treaties, all intellectual and industrial property rights related to the systems, documents, procedures, certificates, lists of revoked certificates and any others, related to its activity as DCE, including this CPS and the associated CPs, shall correspond exclusively to Thomas Signe S.A.S.

9.6 OBLIGATIONS AND RIGHTS

9.6.1 OBLIGATIONS OF DCE


DCE Thomas Signe S.A.S. is obligated under the provisions of this document, mainly to:

- a) Comply with the provisions of this CPS and the associated CPs, as well as the Service Request and Acceptance document.
- b) To publish this CPS, the associated CPs and the Application and Acceptance document on its web page, in its current version.
- c) Inform Subscribers, Applicants, and the general public about the modifications of this CPS and the associated CPs, including such modifications in the initial version history table.
- d) To have a civil liability insurance that covers the minimum value required by the regulations in force.
- e) Use reliable systems to store certificates that allow checking their authenticity and prevent unauthorized persons from altering the data, restricting their accessibility in the cases or to the persons that the Subscriber and/or Applicant may request. the Subscriber and/or Applicant have indicated and allow the detection of any change that affects these security conditions.

As far as certificates are concerned:

- f) Issue certificates in accordance with this CPS, the corresponding CPs and the applicable standards.
- g) Issue certificates according to the information in its possession and free of data entry errors. data entry errors.
- h) Issue certificates whose minimum content is the one defined by the regulations in force, when applicable. applicable.
- i) Revoke certificates according to the provisions of this CPS and the corresponding CPs and publish the revocations in the CRL (List of Revoked Certificates).

Custody of information:

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 60 of 67

a) Retain the information on the certificate issued for the minimum period required by current regulations, when applicable.

b) Not to store or copy the Subscriber's signature creation data, unless the certificate's media type is HSM Centralized.

c) Protect, with due care, the Subscriber's signature creation data, in case the certificate media type is HSM Centralized, while in their custody.

d) Protect their private keys in a secure manner.

e) Establish the mechanisms for the generation and custody of the relevant information in the described activities, protecting them against loss, destruction, or falsification.

f) Submit to ONAC, on an annual basis, for the completion of Stage 1 of each accreditation evaluation:

- File with the issued certificates and their respective content.

- File with control totals (issued, valid, revoked and expired).

As Registration Authority (RA) it is also obliged in the terms defined in the present CPS for the issuance of certificates, mainly to:

a) Respect the provisions of this CPS and the CP corresponding to the type of certificate issued.

g) Respect the provisions of the contracts signed with the Subscriber. In the life cycle of the certificates:

- Verify the identity of Certificate Applicants as described in this CPS or by another procedure that has been approved by the DCE.

- Verify the accuracy and authenticity of the information provided by the Applicant.

- Inform the Subscriber, prior to the issuance of a certificate, of the obligations it assumes, the manner in which it must safeguard the signature creation data or devices and/or the activation data thereof, the procedure to be followed to report the loss or misuse of the signature creation data or devices, of its price, of the precise conditions for the use of the certificate, of its limitations of use and of the way in which it guarantees its possible patrimonial responsibility, and of the web page where it can consult any information of the DCE, of the CPS and of the CP corresponding to the certificate.

- To process and deliver the certificates in accordance with the stipulations of this CPS and the corresponding CP.

- Process the Application and Acceptance document as established by the applicable Certificate Policy.

- Archive, for the period stipulated in the current legislation, the documents provided by the Subscriber and/or Applicant.

- Inform the Subordinate CA of the causes for revocation.

- Communicate with the Subscribers, by the means they consider appropriate, for the correct management of the certificate life cycle. Specifically, carry out communications regarding the approaching expiration of certificates and certificate revocations.

9.6.2 OBLIGATIONS OF SUPPLIERS

The suppliers of DCE Thomas Signe S.A.S. are obliged to comply with the minimum requirements demanded by ONAC, set forth in the current document CEA-3.0-07, such as:

a) Responsibility and financing

b) Confidentiality

c) Resource requirements


d) Process requirements - Life cycle of the digital certificate

e) Management system requirements

f) CA requirements

g) RA requirements

h) Technical requirements

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 61 of 67

9.6.3 OBLIGATIONS OF APPLICANTS

The Applicant for a certificate shall be obliged to comply with the provisions of the regulations in force and must be:

- a) Provide the Commercial Area and/or the RA and/or, in applicable cases, the Subscriber, with the necessary information to carry out a correct identification.
- b) Make reasonable efforts to confirm the accuracy and truthfulness of the information provided.
- c) Respect the provisions of the contractual documents signed with DCE.
- d) Notify any change in the data provided for the creation of the certificate during its period of validity.
- e) Inform as soon as possible of the knowledge of any cause for revocation.

9.6.4 RIGHTS OF SUBSCRIBERS

The Subscriber shall be obliged to comply with the provisions of the regulations in force and must be:

- a) Provide the Commercial Area and/or the RA and/or, in applicable cases, the Applicant or the Entity to which the Subscriber is linked, with the necessary information to make a correct identification.
- b) Make reasonable efforts to confirm the accuracy and truthfulness of the information provided.
- c) To diligently guard their private keys and/or their activation data (such as passwords or secret codes defined or received by any means).
- d) Use the certificate as established in this CPS and in the corresponding CP.
- e) Respect the provisions of the legal instruments binding on the DCE.
- f) Notify any change in the data provided for the creation of the certificate during its period of validity.
- g) Inform as soon as possible of the existence of any cause for revocation.
- h) Not to use the private key or the certificate from the moment it is requested or warned by the DCE or the RA of its revocation, or once the certificate's validity period has expired.


9.6.5 RIGHTS OF SUBSCRIBERS

- a) Request and use the services provided by DCE in accordance with current regulations and practices defined in the CPS and CPs.
- b) Obtain a treatment of their data in accordance with the provisions of the personal data protection policy.
- c) Use and preservation of information about certificates by the DCE in an appropriate, secure and confidential manner.
- d) To request the revocation of their certificates due to key compromise or by their own will.

9.6.6 OBLIGATIONS OF RELYING ON THIRD PARTIES

It shall be the obligation of the relying on Third Parties to comply with the provisions of the regulations in force and furthermore:

- a) Verify the validity of the certificates before performing any operation based on them, which will include verifying that the certificates have not expired or been revoked (by consulting the CRL or the OCSP service).
- b) Verify that the certificates have been signed with the private key associated with a valid certificate of the DCE Thomas Signe S.A.S. Subordinate CA.
- c) To be aware of and agree to abide by the guarantees, limits, and responsibilities applicable to the acceptance and use of the certificates they trust, and to accept to abide by them.
- d) To notify Thomas Signe S.A.S. of any irregular situation with respect to the service provided by the DCE. the DCE.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 62 of 67

9.6.7 OBLIGATIONS OF THE ENTITY TO WHICH THE SUBSCRIBER IS BOUND

In the applicable certificate types, the Entity to which the Subscriber is linked shall be obliged to comply with the provisions of current regulations and in addition to:

- a) Provide the RA and/or the Applicant with the information necessary to make a correct identification.
- b) Make reasonable efforts to confirm the accuracy and veracity of the information provided.
- c) Respect the provisions of the contractual documents signed with the DCE.
- d) Notify any change in their knowledge in the data provided for the creation of the certificate during its period of validity.
- e) Inform as soon as possible of the knowledge of any cause for revocation.

9.7 RESPONSIBILITIES

9.7.1 RESPONSIBILITIES OF THE DCE

- Comply with the Specific Criteria for Accreditation of Digital Certification Entities - CEA-3.0-07 in force, established by ONAC.

- Inform its suppliers that it extends to them compliance with the requirements set forth in the current CEA-3.0-07 document, when applicable.

- Inform the Applicants, Subscribers, Third Parties and the general public on the Thomas Signe S.A.S. website of the activities and services accredited in accordance with the provisions of the RAC-3.0-03 document in force of ONAC.

- To inform Applicants, Subscribers, Relying Third Parties and the general public on the Thomas Signe S.A.S. website of general information about the company, such as its nature, type of company, etc.

- Ensure that the certificates comply with all material requirements set out in the CPS and that there are no factual errors in the information contained in the certificates, known or made by DCE Thomas Signe S.A.S.

- To provide the Subscriber and the Applicant with the necessary documents in their latest version.

- Provide the Subscriber with information on how to validate the certificate, including the requirement to check the status of the certificate and the conditions under which the certificate can be reasonably relied upon, which is applicable when the Subscriber acts as a Relying Third Party.

- Notify the Subscriber of changes in DCE Thomas Signe S.A.S. policies and practices.

- Notify the Subscriber of any changes to the basic terms and conditions (policy identifiers, limitations of use, Subscriber obligations, form of validation of a certificate, dispute resolution procedure, period within which audit trails will be retained, applicable legal system and compliance with ONAC requirements).


- The use of the symbols that characterize the accreditation of Thomas Signe S.A.S. DCE will be restricted to the accredited scope, and may not be transferred to third parties or inherited outside the digital certification services, persons, processes and third parties evaluated by ONAC; as described in the document Policy of use of Thomas Signe S.A.S. symbols.

- Exercise control over the accredited digital certification services, regarding the ownership and use of symbols, certificates, any other mechanism to indicate that the digital certification service is accredited.

- References to the scope of accreditation granted, or the misleading use of the scope of accreditation granted, symbols, certificates, and any other mechanism to indicate that a digital certification service, or that the DCE is accredited, in documentation or other publicity shall be subject to compliance with the current ONAC Accreditation Rules RAC-3.0-01 and RAC-3.0-03.

- Attend and respond to requests, complaints, claims and appeals from Subscribers and related parties.

- Regarding its activities as RA, notify ONAC when a new Registration Office is established, where it will follow the same procedures and comply with the same requirements as Thomas Signe S.A.S. Main Office.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 63 of 67

- Act impartially in accordance with its Impartiality and Non-Discrimination Policy.


9.7.2 RESPONSIBILITIES OF THE SUBSCRIBER

- Act in accordance with the provisions of this CPS of DCE Thomas Signe S.A.S.
- Provide DCE Thomas Signe S.A.S. with complete, current, and accurate information.
- Properly use the certificate with respect to its application, limitations, and prohibitions of use as established in the Thomas Signe S.A.S. CPS.
- Comply with the requirements stipulated by Thomas Signe S.A.S. for the respective digital certification service.
- Comply with new requirements, when Thomas Signe S.A.S. implements changes in the digital certification services, prior communication of such changes by the DCE to the Subscriber.
- That the certification statements are consistent with the scope of the digital certification service.
- Not to use its digital certification in a way that contravenes the law or causes bad reputation for DCE Thomas Signe S.A.S. and does not make any statement related to its certification that Thomas Signe S.A.S. may consider misleading or unauthorized. This in turn implies not to monitor, manipulate, or reverse engineer the technical implementation of ONAC and DCE Thomas Signe S.A.S.; nor to intentionally compromise the security of the ONAC Hierarchy and DCE Thomas Signe S.A.S.
- Immediately upon cancellation or termination of the digital certification, stop using it in all advertising material containing any reference to it, and take the actions required by the digital certification service and any other previously notified measures.
- When referring to the digital certification service in media, such as documents, brochures, or advertising, inform that it complies with the requirements specified in the respective Thomas Signe S.A.S. CP.
- Comply with the requirements that may be prescribed by the digital certification service in relation to the use of marks of conformity and information related to the service.
- Inform the DCE, without delay, about the changes that may affect the digital certification that was issued by the DCE.
- Be diligent in the custody of your private key and the access passwords that protect your private key, to avoid unauthorized uses.
- At all times be responsible for protecting your private key, access passwords and the cryptographic device where your private key is stored without being able to transfer this responsibility to any third party.
- Request the revocation of the digital certificate in case of loss, theft or misplacement of the electronic security device that stores your private key; potential compromise of the private key; loss of control over your private key, due to the compromise of the activation data or for any other cause; inaccuracies or changes in the content of the certificate that you know or could know.
- To stop using the private key, after the expiration of the certificate's validity period.
- Not to validly use the expired certificate from the date on which it expires.
- Request the revocation of certificates when it fails to comply with the obligations to which it is committed within ONAC's requirements.
- Inform that it complies with the stipulated in the Thomas Signe S.A.S. CPS, when it refers to the digital certification service in the media (articles, documents, brochures or advertising).

9.8 LIMITATION OF LIABILITY

Thomas Signe S.A.S. shall not be liable in any case when faced with any of these circumstances:

- a) State of War, natural disasters, malfunction of electrical services, telematic and/or telephone networks or computer equipment used by the Subscriber, the Applicant or relying Third Parties, or any other case of force majeure.
- b) For the improper use of the information contained in the certificate, in the CRL or in the OCSF service.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 64 of 67

c) For the content of the messages or documents signed or encrypted by means of the certificates.

d) In relation to actions or omissions of the Applicant and/or Subscriber:

- Lack of truthfulness or accuracy of the information provided to issue the certificate.
- Delay in the communication of the causes for revocation of the certificate.
- Absence of certificate revocation request when applicable.
- Negligence in the conservation of its signature creation data or its activation data, in the assurance of its confidentiality and in the protection of any access or disclosure.
- Use of the certificate outside its period of validity, or when the DCE Thomas Signe S.A.S. or the RA notifies you of the revocation of the certificate.
- Extra limitation in the use of the certificate, as provided in the current regulations and in the DCE's CPS exceeding the limits that appear in the certificate in terms of its possible uses and the individualized amount of the transactions that can be made with it or not using it in accordance with the conditions established and communicated to the Applicant and/or Subscriber by the DCE.

e) In relation to actions or omissions of the Relying Party:

- Lack of verification of the restrictions contained in the certificate or in the DCE's CPS regarding its possible uses and the individualized amount of the transactions that can be carried out with it.
- Lack of verification of the loss of validity of the certificate published in the consultation service on the validity of the certificates or lack of verification of the digital signature.

9.9 INDEMNITIES

9.9.1 INDEMNITIES FOR DAMAGES CAUSED BY DCE

Thomas Signe S.A.S. shall assume the corresponding indemnities for damages incurred to Applicants, Subscribers, relying Third Parties or any other interested party based on the terms established in the regulations governing the provision of services for the issuance, revocation and distribution of digital certificates, as well as this CPS and the associated CPs.

9.9.2 INDEMNITIES FOR DAMAGES CAUSED BY APPLICANTS, BY SUBSCRIBERS AND BY ENTRUSTED THIRD PARTIES

Both the Subscribers, the Applicants, as well as the trusting Third Parties are responsible for seizing, destroying, modifying, improperly altering the data of a digital signature or certificate during or after the date of creation of the certificate and shall be subject to the payment of compensation for the corresponding damages caused according to the provisions of the regulations governing the provision of services for the issuance, revocation and distribution of digital certificates.


9.10 PERIOD OF VALIDITY

9.10.1 TERM

This CPS and the associated CPs shall enter into force as soon as they are published on the Thomas Signe S.A.S. website and shall remain in force until they are expressly repealed by the publication of a new version.

9.10.2 REPLACEMENT AND ABROGATION OF THE CPS AND CP

This CPS and the associated CPs will be replaced by new versions regardless of the significance of the changes made to it, so that they will always apply in their entirety. When the CPS is repealed, it will be removed from the Thomas Signe S.A.S. website, although it will be retained for at least three (03) years from its termination or the period established by the legislation in force.

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 65 of 67

9.10.3 EFFECTS OF TERMINATION

The obligations and restrictions set forth in this CPS and the associated CPs, in reference to audits, confidential information, obligations and responsibilities of Thomas Signe S.A.S. arising under its validity, shall survive its replacement or repeal by a new version in everything that does not oppose it.

9.11 PQRS

Requests, complaints, claims and suggestions (PQRS) about the services provided by Thomas Signe S.A.S., are received directly by the Responsible for PQRS of the DCE.

Applicants, Subscribers, Relying Third Parties or the general public shall indicate their PQRS regarding the digital certification services offered by Thomas Signe S.A.S. by sending an email to the address pqrsa@thsigne.com detailing the situation for which it is presented.

The PQRS will be managed by the PQRS Manager of Thomas Signe S.A.S., who will be responsible for referring the incident to the respective Department or role. Such management will be carried out, resulting in a solution in a period not exceeding fifteen (15) days. The user will receive an e-mail message confirming receipt of the PQRS and when it is resolved. Thomas Signe S.A.S. has the THS-CO-AC-PR-02 PQRS Procedure for the treatment of PQRS that details each of the processes and is published on the Thomas Signe S.A.S. website.

9.12 CHANGES IN CPS AND CP

The content of this CPS and the associated CPs may be changed unilaterally by Thomas Signe S.A.S. without notice, except where such changes may affect the acceptance of the services by Subscribers and/or Relying Third Parties.

S.A.S. without prior notice, except where the changes could affect the acceptance of the services by Subscribers and/or relying Third Parties, in which case they will be notified in advance to the interested parties (e.g., by publication of the notification on the Thomas Signe S.A.S. website), without the need to include the details of the changes in the notification. Changes may be made for legal, technical or commercial reasons.

All changes to this CPS and associated CPs will require new versions of the documents.

The changes in each new version will be indicated in the initial version history table.

New approved versions of this CPS and associated CPs will be submitted to ONAC and published on the Thomas Signe S.A.S. website.

Changes that may materially affect Subscribers will be notified to interested parties.

9.13 DISPUTE RESOLUTION PROCEDURE


For the resolution of any conflict that may arise in relation to this CPS or the associated CPs, the parties, waiving any other jurisdiction that may correspond to them, submit to the Colombian Courts, regardless of the place where the issued certificates were used.

9.14 APPLICABLE LAW

The legislation applicable to this document, as well as to the associated CPs and the operations deriving from them, is recorded in the internal document GSIGNE-GRAL-PR-01-F05 List of External Documents, including the following, as well as the regulations that modify or complement it:

- a) Law 527 of 1999
- b) Statutory Law 1581 of 2012
- c) Decree Law 0019 of 2012
- d) Decree 1074 of 2015
- e) Decree 333 of 2014
- f) Decree 1471 of 2014

9.15 COMPLIANCE WITH APPLICABLE LAW

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 66 of 67

It is the responsibility of Thomas Signe S.A.S. to ensure compliance with the applicable legislation listed in the previous section.

9.16 MISCELLANEOUS STIPULATIONS

9.16.1 APPLICATION AND ACCEPTANCE DOCUMENT

The model of the Application and Acceptance document for the current certificate issuance service is published on the following web page:

<https://thomas-signe.co/declaracion-de-practicas-y-politicas-de-certificacion/>

The same subscription form is used for all types of certificates. In each model, the type of certificate contracted, and its validity must be filled in, as well as the Subscriber's identification data and the date of the Subscriber's signature.

In the case of Automated Signature Certificates, if the Subscriber is a Legal Entity, the contract will be signed by its Legal Representative.

Since each model is filled in with the Subscriber's identification data, the document is catalogued with CONFIDENTIAL level, even though the document model is published in the indicated web page.

In the case of certificates for Automated Signature, it will be the Subscriber's responsibility to disseminate, as appropriate in terms of confidentiality, the conditions set forth in the model, to the entire community of users defined for the use of the contracted service.

9.16.2 FULL ACCEPTANCE CLAUSE

All Applicants, Subscribers, Relying Third Parties and any other interested parties assume in its entirety the contents of the latest version of this CPS and the associated CPs.

9.16.3 INDEPENDENCE

If any of the sections contained in this CPS or in the associated CPs is declared, partially or totally, null and void or illegal, this shall not affect the rest of the document.

9.17 OTHER STIPULATIONS

Not considered.

10 FORMATS

THS-CO-AC-AC-DPC-01-F01 Automated Signature Certificate Application Form

THS-CO-AC-AC-DPC-01-F02 Legal Representative Certificate Request Form

THS-CO-AC-AC-DPC-01-F03 Application Form for Certificate for Natural Person

THS-CO-AC-AC-DPC-01-F04 Company/Entity Binding Certificate Application Form

THS-CO-AC-AC-DPC-01-F10 Authorization Application Form for Certificate for Automated Signature - Individual Natural Person


THS-CO-AC-AC-DPC-01-F12 Authorization Application for Automated Signature Certificate - Other Entity

THS-CO-AC-AC-DPC-01-F13 Authorization Pre-Application Authorization for Automated Signature Certificate - Other Entity

THS-CO-AC-AC-DPC-01-F14 Service Agreement for the Provision of Digital Certificates for Automated Signatures

THS-CO-AC-AC-DPC-01-F15 Reading Protocol for Identity Verification Videoconference

THS-CO-AC-AC-DPC-F16 Documentary Retention Chart

	Certification Practice Statement for Certificate Issuance	Version 2.8
	Code: THS-CO-AC-DPC-01	Page 67 of 67

THS-CO-AC-AC-DPC-01-F17 Application and Acceptance of Digital Certification Service Provision (Legal Representative)

THS-CO-AC-AC-DPC-01-F18 Application and Acceptance of Digital Certification Service Provision (Subscriber)

THS-CO-AC-AC-DPC-01-F20 Commercial Proposal for Digital Certificates

11 RECORDS

ID	SUPPORT	RESPONSIBLE	FILE	RETENTION TIME
Completed Certificate Application Forms	TI	Registry Operator	SAR Platform	7 years or according to applicable regulations
Signed commercial proposals for Digital Certificates	TI	Commercial Manager	SAR Platform	7 years or according to applicable regulations
Signed Certificate Issuance Application and Acceptance Forms	TI	Registry Operator	SAR Platform	7 years or according to applicable regulations
Recorded Identity Verification Videoconferences	TI	Registry Operator	RA Platform	7 years or according to applicable regulations
Completed Documentary Retention Table	TI	Information Systems Manager	Filesystem	7 years or according to applicable regulations