


Digital Certification Entity



Certificate Policy for Legal Representative

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 2 of 22


Document Information

Name	CERTIFICATE POLICY FOR LEGAL REPRESENTATIVE
Prepared by	THOMAS SIGNE S.A.S.
Country	COLOMBIA
Version	2.6
Date	AUGUST, 2023
Document Type	PUBLIC
Code	THS-CO-AC-PC-COR-03


Document version

Version	Date	Description
1.0	06/28/2017	Preparation of initial document.
1.1	05/20/2018	The Obligations section is added. The Certificate Operating Procedure is specified.
1.2	05/24/2018	The section on Circumstances for revocation of a certificate has been added.
1.3	06/06/2018	Sections have been added for applicable formats and records.
1.4	11/02/2018	The reference to THS-PR-GRAL-02-F01 Document Structure v1.0 is removed from the footer. The "INTRODUCTION" section has been removed.
1.5	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.
1.6	05/09/2019	Integration with the Group's management system. Document name change from THS-PC-PJ-01 to THS-CO-POL-COR-COR-AC-03.

		The sections on formats and applicable records have been eliminated. Minor corrections.
--	--	--------------------------------------------------------------------------------------------


		Certificate Policy for Legal Representative	Version 2.7
		Code: THS-CO-AC-PC-COR-03	Page 3 of 22
1.7	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 review of the certificate request, in the validation of the Applicant's identity document, the query against an online database is eliminated.</p> <p>It is indicated that the issuance and installation of the certificate in the Centralized HSM are automatically performed by the RA upon receipt of the certificate request in PKCS #10 format, without the intervention of an OR (change implemented in January 2019).</p> <p>In the Serial Number attribute of the DN of the certificates, the format of the Subscriber's identification document type is indicated.</p> <p>The Formats and Records sections are added.</p> <p>In the subscription contract (Annex II), the Signature of the Applicant is changed to the Signature of the Subscriber (the Applicant and the Subscriber are the same Natural Person).</p> <p>Minor corrections.</p>	
1.8	11/29/2019	<p>Change of the current account number to make the deposit of the respective amount for each service.</p> <p>Added a format and a register for identity verification videoconferences.</p> <p>Minor corrections.</p>	
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>Change of the name of the document from "Legal Entity Certification Policy" to "Legal Entity Certificate Policy."</p> <p>Changes in the organization of the content of the document to follow the recommendations of the RFC 3647 standard.</p> <p>Elimination of the current account number to make the deposit of the respective amount for each service (to be indicated in the Commercial Proposal).</p>	
2.1	06/19/2020	<p>The obligations of the Entity to which the Subscriberis bound are added.</p> <p>Minor corrections.</p>	
2.2	11/06/2020	<p>Added the possibility for the Applicant's (and Subscriber's) identity document type to be Passport.</p> <p>Minor corrections.</p>	
2.3	06/24/2021	<p>Rebranding of Thomas Signe.</p> <p>Change of the name of the document from "Certificate Policy for Legal Representative" to "Certificate Policy for Legal Representative".</p>	
		<p>Changes in certificate issuance fees.</p> <p>Minor corrections.</p>	

2.4	11/19/2021	<p>Changes in the processing of certificate requests and issuance of certificates, to ensure independence and impartiality between the review and certification (certificate issuance) decision functions, and to document the processes and results related to the review, including the recommendation for decision based on the review.</p> <p>Certificate revocation requests sent to the PQRSA Manager by email are referred to an RA Decision Operator.</p> <p>Minor Corrections.</p>
2.5	07/08/2022	<p>Adaptation to the new version of CEA-3.0-07.</p> <p>Added issuerAltName to the certificate profile.</p> <p>Updated revocation means.</p>
2.6	20/01/2023	<p>Corrections and minor changes.</p>
2.7	16/08/2023	<p>Fees update.</p>


	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 5 of 22

CONTENTS

1	INTRODUCCIÓN	8
1.1	PRESENTATION OF THE DOCUMENT	8
1.2	DOCUMENT NAME AND IDENTIFICATION	8
1.3	THOMAS SIGNE S.A.S. PKI PARTICIPANTS	9
1.3.1	THOMAS SIGNE S.A.S. PKI CERTIFICATE HIERARCHY	9
1.3.2	THOMAS SIGNE ROOT	9
1.3.3	DCE THOMAS SIGNE S.A.S. (DCE THOMAS SIGNE COLOMBIA)	9
1.3.4	APPLICANT	9
1.3.5	SUBSCRIBER	9
1.3.6	TRUSTING THIRD PARTY	9
1.3.7	ENTITY TO WHICH THE SUBSCRIBER IS RELATED	9
1.4	TYPES OF SUPPORT AND USES OF CERTIFICATES	10
1.4.1	CENTRALIZED HSM SUPPORT	10
1.4.2	APPROPRIATE USES OF CERTIFICATES	10
1.4.3	AUTHORIZED USES OF CERTIFICATES	10
1.5	CPS AND CP ADMINISTRATION	10
1.6	DEFINITIONS AND ACRONYMS	11
1.6.1	DEFINITIONS	11
1.6.2	ACRONYMS	11
2	RESPONSIBILITIES REGARDING REPOSITORIES AND PUBLICATION OF INFORMATION	12
3	DENTIFICATION AND AUTHENTICATION	12
3.1	NAMES	12
3.2	INITIAL IDENTITY VALIDATION	12
3.2.1	METHOD OF PROOF OF POSSESSION OF THE PRIVATE KEY	12
3.2.2	AUTHENTICATION OF A COMPANY'S OR ENTITY'S IDENTITY	12
3.2.3	AUTHENTICATION OF THE IDENTITY OF AN INDIVIDUAL NATURAL PERSON	12
3.2.4	UNVERIFIED SUBSCRIBER AND APPLICANT INFORMATION	12
3.3	IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUESTS WITH CHANGE OF PASSWORDS CHANGE OF KEYS	13
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS	13
4	OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF THE CERTIFICATES	13
4.1	CERTIFICATE APPLICATION	13
4.1.1	WHO CAN APPLY FOR A CERTIFICATE	13
4.1.2	MARKETING	13
4.1.3	CONTRACTING AND PAYMENT	14
4.1.4	APPLICATION	14
4.2	PROCESSING OF CERTIFICATE APPLICATIONS	15
4.2.1	REVIEW	15
4.2.2	DECISION	15
4.3	ISSUANCE OF CERTIFICATES	16
4.3.1	DCE ACTIONS DURING ISSUANCE OF CERTIFICATES	16
4.3.2	NOTIFICATION TO THE APPLICANT AND SUBSCRIBER BY DCE OF CERTIFICATE	16
ISSUANCE		
4.4	ACCEPTANCE OF THE CERTIFICATE	16
4.4.1	FORM IN WHICH THE CERTIFICATE IS ACCEPTED	16
4.4.2	PUBLICATION OF THE CERTIFICATE BY DCE	16
4.4.3	NOTIFICATION OF THE ISSUANCE OF THE CERTIFICATE BY DCE TO OTHER	16
ENTITIES		
4.5	USES OF KEYS AND CERTIFICATE	17
4.6	CERTIFICATE RENEWAL WITHOUT CHANGE OF KEYS	17
4.7	CERTIFICATE RENEWAL WITH KEY CHANGE	17
4.8	CERTIFICATE MODIFICATION	17
4.9	CERTIFICATE REVOCATION AND SUSPENSION	17
4.10	CERTIFICATE STATUS INFORMATION SERVICES	17
4.11	SUBSCRIPTION TERMINATIONS	17
4.12	KEY ESCROW AND RECOVERY	17
5	PHYSICAL, FACILITY, MANAGEMENT AND OPERATIONAL	18

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 6 of 22

6	SECURITY CONTROLS	18
7	CERTIFICATE PROFILE, CRL AND OCSP	18
7.1	CERTIFICATE PROFILE.....	18
7.1.1	CERTIFICATE FORMAT AND VALIDITY PERIOD.....	18
7.1.2	CERTIFICATE EXTENSIONS.....	18
7.1.3	OBJECT IDENTIFIERS (OID) OF ALGORITHMS	19
7.1.4	NAME FORMATS.....	20
7.1.5	NAME RESTRICTIONS.....	21
7.1.6	CERTIFICATE POLICY OBJECT IDENTIFIERS (OID).....	21
7.1.7	USE OF THE EXTENSION POLICY CONSTRAINTS	21
7.1.8	SYNTAX AND SEMANTICS OF POLICY QUALIFIERS	21
7.1.9	SEMANTIC TREATMENT FOR THE CERTIFICATE POLICY EXTENSION	21
7.2	CRL PROFILE	21
7.3	OCSP PROFILE	21
8	COMPLIANCE AUDIT AND OTHER CONTROLS.....	21
9	OTHER LEGAL AND COMMERCIAL AFFAIRS	21
9.1	FEES.....	21
9.1.1	CERTIFICATE ISSUANCE FEES.....	21
9.1.2	CERTIFICATE ACCESS FEES	22
9.1.3	FEES FOR REVOCATION OR ACCESS TO STATUS INFORMATION.....	22
9.1.4	FEES FOR OTHER SERVICES.....	22
9.1.5	REFUND POLICY	22
9.2	FINANCIAL RESPONSIBILITIES.....	22
9.2.1	INSURANCE COVERAGE	22
9.3	CONFIDENTIALITY OF INFORMATION	22
9.4	DATA PROTECTION POLICY	22
9.5	INTELLECTUAL PROPERTY RIGHTS	22
9.6	OBLIGATIONS	23
9.6.1	OBLIGATIONS OF DCE.....	23
9.6.2	OBLIGATIONS OF SUPPLIERS.....	23
9.6.3	OBLIGATIONS OF APPLICANTS	23
9.6.4	OBLIGATIONS OF SUBSCRIBERS	23
9.6.5	OBLIGATIONS OF REL YING ON THIRD PARTIES	23
9.6.6	OBLIGATIONS OF THE ENTITY TO WHICH THE SUBSCRIBER IS RELATED	23
9.7	RESPONSIBILITIES.....	23
9.7.1	DCE'S RESPONSIBILITIES	23
9.7.2	SUBSCRIBER'S RESPONSIBILITIES	23
9.8	LIMITATION OF LIABILITY	23
9.9	INDEMNITIES.....	23
9.9.1	INDEMNITIES FOR DAMAGES CAUSED BY DCE	23
9.9.2	COMPENSATION FOR DAMAGES CAUSED BY CLAIMANTS, BY SUBSCRIBERS AND BY THIRD PARTIES WHO TRUST.....	24
9.10	PERIOD OF VALIDITY	24
9.10.1	TERM.....	24
9.10.2	REPLACEMENT AND REPEAL OF THE CPS AND CP'S.....	24
9.10.3	EFFECTS OF TERMINATION.....	24
9.11	PQRS	24
9.12	CHANGES IN CPS AND CP	24
9.13	CLAIMS AND DISPUTE RESOLUTION	24
9.14	APPLICABLE LAW	24
9.15	IN ACCORDANCE WITH APPLICABLE LAW	24
9.16	OTHER PROVISIONS.....	24
9.16.1	SUBSCRIPTION AGREEMENT	24
9.16.2	FULL ACCEPTANCE CLAUSE.....	25
9.16.3	INDEPENDENCE	25
9.17	OTHER STIPULATIONS	25
10	FORMATS	25
11	RECORDS.....	25

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 7 of 22

1 INTRODUCTION

1.1 PRESENTATION OF THE DOCUMENT

This document constitutes the Certificates Policy (CP) for Legal Representative issued by Thomas Signe S.A.S., in compliance with the Specific Criteria for Accreditation of Digital Certification Entities - CEA 3.0-07 established by the National Accreditation Body of Colombia - ONAC, in accordance with Colombian legislation and the provisions of the regulatory authorities.

The Certificates for Legal Representative issued by Thomas Signe S.A.S. are certificates that allow to identify and sign the Subscriber as a natural person linked to a company or entity (legal 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), as its legal representative.

This CP establishes the requirements of the Certificates for Legal Representative issued by Thomas Signe S.A.S, 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.

In addition to the requirements established in this CP, the Certificates for Legal Representative issued by Thomas Signe S.A.S. are governed by the practices established in the Certification Practice Statement (CPS) for the issuance of certificates of Thomas Signe S.A.S. This CPS is published in the same web page of Thomas Signe S.A.S. as this document (see section 1.2).

If vulnerabilities are detected, or the technical standards or infrastructure indicated in this CP are no longer in force, Thomas Signe S.A.S. will be responsible for informing ONAC of this fact, in order 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, this document is identified with the following OIDs, contained in the X.509 v3 Certificate Policies extension of the Legal Representative Certificates issued by Thomas Signe S.A.S. in the indicated media types.

OID OF THE CERTIFICATE CP FOR LEGAL REPRESENTATIVE 1.3.6.1.4.1.51362.0.2.1.3.	
1.3.6.1.4.1.51362.0.2.1.3.3	Centralized HSM Support

This document is available 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

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

1.3.2 THOMAS SIGNE ROOT

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 8 of 22

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

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

1.3.4 APPLICANT

In this CP, Applicant is the natural person who requests DCE Thomas Signe S.A.S. to issue a Certificate for Legal Representative.

In this CP, Applicant is always the same natural person as the Subscriber.

1.3.5 SUBSCRIBER

In this CP, the Subscriber is the natural person in whose name the DCE Thomas Signe S.A.S. issues a Certificate for Legal Representative and, therefore, acts as responsible for it, and who, with knowledge and full acceptance of the rights and duties established and published in this CP and in the CPS for the issuance of Thomas Signe S.A.S. certificates and having signed the respective Subscription Contract 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 for Legal Representative issued in the name by DCE Thomas Signe S.A.S., who is exclusively bound to an electronic document digitally signed using said private key.

In this CP, Subscriber is a natural person linked to an Entity (legal person), as its legal representative.

1.3.6 TRUSTING THIRD PARTY

In this CP, Relying Third Party (or Accepting Third Party) are all those natural or legal persons who decide to accept and rely on a Certificate for Legal Representative issued by DCE Thomas Signe S.A.S.

1.3.7 ENTITY TO WHICH THE SUBSCRIBER IS RELATED

In this CP, the Entity to which the Subscriber is related to is the legal 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) to which the Subscriber is related by means of the relationship accredited in the certificate and as its legal representative.

1.4 TYPES OF SUPPORT AND USES OF CERTIFICATES


1.4.1 CENTRALIZED HSM SUPPORT

The emission of Certificates for Legal Representative in Centralized HSM is available to any Subscriber that complies with the requirements established in this CP and in the CPS for the emission of Thomas Signe S.A.S. certificates.

The private keys of the Certificates for Legal Representative issued in this support are generated in a cryptographic device of the HSM type with FIPS 140-2 level 3 certification, resulting in a high level of security, 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

Access to the private key of a Legal Representative Certificate issued on this cryptographic device is provided by 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 on his cell phone each time he tries to access the private key. This username, these two passwords and this code therefore constitute the activation data of the private key.

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 9 of 22

Legal Representative Certificates issued in HSM Centralized are identified by the OID (1.3.6.1.4.1.51362.0.2.1.3.3.3) in the X.509 v3 Certificate Policies extension.

1.4.2 APPROPRIATE USES OF CERTIFICATES

The certificates for Legal Representative issued by Thomas Signe S.A.S. may be used under the terms established in this CP, in the CPS for the issuance of Thomas Signe S.A.S. certificates and in the provisions of the legislation in force in this regard.

Certificates for Legal Representative must, in general, be used within the framework of the legal relationship between the Subscriber and the Entity (Legal Entity) to which the Subscriber is related by means of the link accredited in the certificate and as its legal representative. Specifically, they can be used for the following purposes:

- Integrity of the signed document.
- Non-repudiation of origin.
- Identification of the Subscriber and its relationship with the Entity accredited in the certificate and as its legal representative, and/or identification of the Entity.

The use of these certificates is allowed in the Subscriber 's personal relations with the Public Administrations and in other strictly personal uses, as long as there is no prohibition of the Entity to which the Subscriber is related by means of the link accredited in the certificate and as its legal representative.

1.4.3 UNAUTHORIZED USES OF CERTIFICATES

It is not allowed to use other than what is established in this CP and the CPS for the emission of Thomas Signe S.A.S. certificates.

1.5 CPS AND CP ADMINISTRATION

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.


1.6 DEFINITIONS AND ACRONYMS

1.6.1 DEFINITIONS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

1.6.2 ACRONYMS

CA	Certification Authority
CRL	Certificate Revocation List
DN	Distinguished Name
CPS	Certification Practice 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 Organization - CAB as defined in ISO/IEC 17000.
FIPS	Federal Information Standards 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

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 10 of 22

NIT	Tax Identification Number
OCSP	Online Certificate Status Protocol
ONAC	National Accreditation Organization of Colombia
RO	Registry Operator
CP	Certificate Policy
PKCS	Public-Key Cryptography Standards. Standards for cryptography conceived and published by the laboratories of RSA.
PKI	Public Key Infrastructure
PQRS	Petitions, Complaints, Claims and Suggestions
RA	Registration Authority
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	Corporate and Social Registry
SAR	Signe Registration Authority
SHA	Secure Hash Algorithm

2 RESPONSIBILITIES REGARDING REPOSITORIES AND PUBLICATION OF INFORMATION

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMES

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD OF PROOF OF POSSESSION OF THE PRIVATE KEY


When a certificate is issued in Centralized HSM, the private key is generated in the HSM at the previous moment to the issuance of the certificate, by means of a procedure that guarantees its confidentiality and its binding with the Applicant. The RA will verify the identity of the Entity (Legal Entity) to which the Subscriber is related by means of the link accredited in the certificate and as its legal representative as specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

3.2.2 AUTHENTICATION OF A COMPANY'S OR ENTITY'S IDENTITY

The RA will verify the identity of the Entity (Legal Entity) to which the Subscriber is related by means of the link accredited in the certificate and as its legal representative as specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

3.2.3 AUTHENTICATION OF THE IDENTITY OF AN INDIVIDUAL NATURAL PERSON

The RA will reliably verify the identity of the individual Natural Person Subscriber as specified in the

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 11 of 22

CPS for the issuance of Thomas Signe S.A.S. certificates.

Additionally, for those cases in which it is possible, in the verification of the tax identification number of the Entity to which the Subscriber is linked in an online database (in Colombia, for companies, RUES database), the RA will verify, in addition to the existence of the Entity and that it is active, that the data shown of the legal representative match those of the Subscriber, because it could be that it has ceased to be so after having been issued the Certificate of existence and legal representation in Chamber of Commerce or equivalent document presented.

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 Applicant as specified in sections 3.2.2 and 3.2.3.

The RA shall not verify the following data of the Subscriber and Applicant entered in the certificate application form in the SAR platform, assuming the good faith of the information provided by the Subscriber:

-Data contained in the certificate: area of the Subscriber in the Entity; position, title or role of the Subscriber in the Entity; email of the Subscriber.

-Data not contained in the certificate: Subscriber's cell phone number.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUESTS WITH CHANGE OF PASSWORDS CHANGE OF KEYS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

The identification and authentication of the Subscriber and Applicant, in case he/she uses the online revocation procedure, through the links contained in the Thomas Signe S.A.S. website, is performed according to the following method:

- Centralized HSM: the Subscriber must enter his or her user and password to access the Centralized HSM, and a code that he or she will receive on the cell phone.

4 OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF THE CERTIFICATES

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN APPLY FOR A CERTIFICATE


Only the Subscriber can apply for a Legal Representative Certificate.

4.1.2 MARKETING

The Applicant (and Subscriber) may receive information about the digital certification process in the following ways:

- Accessing the website www.thomas-signe.co
- Via informative e-mail to comercial@thomas-signe.co
- Dealing directly with Commercial Agents.

By any of these means, you will be provided with information about the process, necessary requirements, fees and other related information. After being informed, the Applicant (and Subscriber) will indicate to the Commercial Area and/or a RO:

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 12 of 22

After being informed, the Applicant (and Subscriber) will indicate to the Commercial Area and/or a RO:

- 1) The type of certificate required (Certificate for Legal Representative).
- 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.
- 6) The name or company name of the Entity to which the Applicant is linked.
- 7) The TIN of the Entity to which the Applicant is linked.

The Commercial Area and/or an RO will send by e-mail to the Applicant (and Subscriber): the Commercial Proposal (sent by the Commercial Area), where applicable; the Subscription Agreement; optionally, a link to the SAR platform; and the respective instructions.

4.1.3 CONTRACTING AND PAYMENT

To proceed with the contracting and payment, the Applicant (and Subscriber) and/or the Entity to which it is linked must:

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

Thomas Signe S.A.S. makes available to the public a bank account for 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 Subscription Agreement between Thomas Signe S.A.S. and the Subscriber by signing it. The evidence of this process will be the signed Subscription Agreement.


Also note that, in addition to the Subscription Agreement with the Subscriber, depending on the type of contract, a Service Agreement between Thomas Signe S.A.S. and the Entity to which the Subscriber is linked may be required.

4.1.4 APPLICATION

To request the issuance of a digital certificate, the Applicant (and Subscriber) may enter the SAR platform and correctly complete the information in the certificate request form (see Annex I). In addition, within the SAR platform, the following documents must be attached:

- Identity document of the Applicant, scanned on both sides: Citizenship Card, Alien Registration Card or Passport; 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 Entity to which the Subscriber is linked as its legal representative, in virtual copy or scanned, in the applicable cases; issued in Colombia (by default) or in another country a maximum of 30 days before.
- Single Tax Registry or equivalent document of the Entity to which the Subscriber is linked as its legal representative, in virtual copy or scanned, in all cases; issued in Colombia (by default) or in another country.
- Additional official document showing a complete current address of the Entity to which the Subscriber is linked as its legal representative, in the event that the Applicant 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.
- Proof of payment of the certificate fee indicated in the Commercial Proposal or in the Service Rendering Contract, if applicable.
- Application and acceptance document signed.

Alternatively, the Applicant (and Subscriber) may personally deliver or send the required data and

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 13 of 22

documents to the Commercial Area and/or an RO, and they will enter the data in the certificate application form and attach the requested documents in the SAR platform.

4.2 PROCESSING OF CERTIFICATE APPLICATIONS

4.2.1 REVIEW

A RO will verify that all required documents have been attached in the SAR platform and that they all fulfill the following:

- They are complete and legible.
- They look genuine.
- In the appropriate cases, they were in force when they were attached to the SAR platform.
- The data they contain regarding the Subscriber, the Entity to which it is linked, the type and validity of the certificate, and the payment of the certificate fee are in accordance with the corresponding data entered in the certificate application form and, where applicable, in the Commercial Proposal. Discrepancy will be accepted only for the complete address of the Entity to which the Subscriber is related contained in the Certificate of existence and legal representation in the Chamber of Commerce and/or in the Single Tax Registry and/or in the additional official document, in which case the address contained in the document with the most recent date of issue will be considered as valid.

Additionally, for those cases in which it is possible, the RO will consult the NIT of the Entity to which the Subscriber is linked in an online database (in Colombia, for companies of the type Legal Entity or Natural Person, RUES database), to verify the existence of the Entity and that it is active and to verify that the data shown for the legal representative coincide with those of the Subscriber, because it could have ceased to be so after having been issued the Certificate of existence and legal representation in the Chamber of Commerce or equivalent document presented.

If there is a need to regularize payments or documentation, the Applicant's (and Subscriber's) stated e-mail address will be notified as required.

Once all the required documentation and evidence has been collected and reviewed, the RO will coordinate with the Applicant an appointment for a videoconference. In this session, the RO will ask a series of questions to verify the Applicant's identity and will ask the Applicant to show the original identity document that has been scanned to verify that it matches the document received. In order to evidence such videoconference, the RA platform will record the entire session and the recording will be saved together with the information collected from the Applicant. This process will be carried out prior to the issuance of the certificate.

Alternatively to the videoconference, an RO may have verified the Applicant's identity 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 such format, which must include the Subscription Contract signed in handwriting by the Subscriber, as evidence of the Applicant's (and Subscriber's) in-person identification.


Once the RO has reviewed the documents submitted and the data entered in the certificate application form and has performed and reviewed the identity validation of the Applicant (and Subscriber), the RO will approve or reject the certificate issuance request on the RA platform based on the review.

Approval of the request by the RO will 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

DCE Thomas Signe S.A.S. is responsible for the decision taken with respect to digital certification, ensuring independence and impartiality between the review and certification decision functions. To this end, an RA Decision Operator, independent of the RO who has performed the review of the certificate 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 of Decision Operator will send an email to the Applicant (and Subscriber) notifying the reasons for the decision not to issue the certificate.

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 14 of 22

4.3 ISSUANCE OF CERTIFICATES

4.3.1 DCE ACTIONS DURING ISSUANCE OF CERTIFICATES

Once the Decision Operator of the RA has made the decision to issue the certificate, the certificate issuance will proceed, during which the DCE Thomas Signe S.A.S. (RA and Subordinate CA) performs the following actions:

1) The keys will be generated by the Subscriber in the Centralized HSM, delivering to the RA a certificate request in PKCS #10 format.

2) The RA will sign the certificate request in PKCS #10 format received and the data that will be contained in the certificate that have been entered in the SAR platform, and will send the resulting request to the CA, receiving from the CA the corresponding issued certificate.

This process will be performed automatically when the RA receives the certificate request in PKCS #10 format, without the intervention of an RA operator.

3) Finally, the RA will deliver the certificate.

The certificate is automatically installed in the Centralized HSM associated to the keys generated by the Subscriber.

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

The Centralized HSM itself notifies the Requestor (and Subscriber) that the certificate has been issued and has been installed in the HSM.

In addition, the RA sends an email to the Requestor (and Subscriber) that includes the following:

- Data document of the acquired certificate, which constitutes the formal documentation of the digital certification service, with the following content: contact details of the DCE Thomas Signe S.A.S.; information about the content of the acquired certificate (type and support of the certificate, dates of issue and expiration of the certificate, data of the Subscriber and the Entity to which it is bound contained in the certificate); data necessary for the use of the certificate in Centralized HSM by the Subscriber; signature of the RA Decision Operator who has made the decision to issue the certificate.
- Link to the web page where the CPS for issuing Thomas Signe S.A.S. certificates and the present CP are published.
- The current version of Use of the certificate Handbook in HSM Centralized.

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 Subscriber), as specified in sections 4.3.1 and 4.3.2.

4.4.2 PUBLICATION OF THE CERTIFICATE BY 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 DCE TO OTHER ENTITIES


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

4.5 USES OF KEYS AND CERTIFICATE

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

4.6 CERTIFICATE RENEWAL WITHOUT CHANGE OF KEYS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 15 of 22

4.7 CERTIFICATE RENEWAL WITH KEY CHANGE

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

4.8 CERTIFICATE MODIFICATION

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

The Subscriber must request the revocation of his/her certificate in case of loss, risks and security compromises of keys contained in the cryptographic device or other causes specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

To request the revocation of the certificate the Subscriber has the following options:

-Revoke the certificate online through the links contained in the Thomas Signe S.A.S. website through the following [link](#). The Subscriber must enter the username and password to access the Centralized HSM, and a code that will be sent to the cell phone.

In the Thomas Signe S.A.S. CPS for the issuance of certificates you will find all the complementary information regarding the revocation of certificates.

4.10 CERTIFICATE STATUS INFORMATION SERVICES

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

4.11 SUBSCRIPTION TERMINATION.

The subscription of the certificate will end at the moment of expiration or revocation of it.

4.12 KEY ESCROW AND RECOVERY

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

5 PHYSICAL, FACILITY, MANAGEMENT AND OPERATIONAL

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

6 SECURITY CONTROLS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.


7 CERTIFICATE PROFILE, CRL AND OCSP

7.1 CERTIFICATE PROFILE

7.1.1 CERTIFICATE FORMAT AND VALIDITY PERIOD

The format of the certificates for Legal Representative complies with the CPS for the issuance of Thomas Signe S.A.S. certificates, except that the ETSI EN 319 412-3 standard is not applicable for these certificates.

Legal Representative Certificates are valid for up to 2 years (730 days).

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 16 of 22

7.1.2 CERTIFICATE EXTENSIONS

The following table specifies the extensions of the Certificates for Legal Representative.

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 1.3.6.1.4.1.51362.0.2.1.3.x ¹ URI of CPS: http://thsigne.com/cps
Subject Alternative Name		rfc822Name: <i>e-mail address of Subscriber</i>
Basic Constraints	Yes	cA: FALSE
Extended Key Usage	-	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)

¹ Centralized HSM: x=3

CRL Distribution Points	-	URI of CRL: http://crl-co.thsigne.com/ecd_thomas_signe_colombia.crl
Authority Information Access	-	URI of the certificate of the Subordinate CA: http://thsigne.com/certs/ecd_thomas_signe_colombia.crt URI of the OCSP service of the Subordinate CA http://ocsp-co.thsigne.com
Issuer Alternative Name	-	Accreditation code assigned by ONAC: 18-DCE - 001

7.1.3 OBJECT IDENTIFIERS (OID) OF ALGORITHMS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

7.1.4 NAME FORMATS

The following table specifies the corresponding attributes of the DN of the holder of a Civil Service Certificate (Certificate Subscriber).

DN Attribute	Description	Value
--------------	-------------	-------

Country Name (C)	Country	Code of two capital letters according to ISO 3166-1 of the country of the Entity ¹ Default: CO
State or Province Name (ST)	State/Provincze	<i>Department of the Entity</i> ²
Locality Name (L)	Location	<i>Municipality of the Entity</i> ²
Street Address (STREET)	Address	<i>Address of the Entity</i> ²
Organization Identifier (2.5.4.97)	Organization Identifier	<i>Identification Tax Number of the Entity (in Colombia: NIT)</i> ²
Organization Name (O)	Organization Name	<i>Name or corporate name of the Entity</i> ²
Organizational Unit Name (OU)	Organizational Unit	<i>Subscriber's area in the Entity or type of Subscriber's relationship with the Entity</i> ²
Title (title)	Title	<i>Position, title or role of the Subscriber in the Entity. By default: "Public Officer"</i> ² .
Serial Number (serialNumber)	Serial Number	<i>TipoDoc-NumDoc</i> ¹ <i>TipoDoc</i> : Type of identity document of the Subscriber, equal to the two-letter code according to ISO 3166-1 of the country issuing the document (by default: CO) followed by CC (Citizenship Card or equivalent) , CE (Foreigner's Identity Card or equivalent) or PA (Passport); in Colombia: COCC, COCE or COPA.
Surname (SN)	Last Name	<i>Subscriber's Last Name</i> ²
Given Name (givenName)	Name	<i>Subscriber's Name</i> ²
Common Name (CN)	Full Name	<i>Subscriber's full name (first and last name)</i> ²

¹ PrintableString Codified


² UTF8String Codified

7.1.5 NAME RESTRICTIONS

As specified in section 7.1.4 and in the CPS for the issuance of Thomas Signe S.A.S. certificates.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)

The OIDs of the Civil Service Certificate Policy are specified in sections 1.2, 1.4 and 7.1.2, as well as in the CPS for the issuance of Thomas Signe S.A.S. certificates.

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 18 of 22

7.1.7 USE OF THE EXTENSION POLICY CONSTRAINTS

Civil Service Certificates do not contain the Policy Constraints extension.

7.1.8 SYNTAX AND SEMANTICS OF POLICY QUALIFIERS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

7.1.9 SEMANTIC TREATMENT FOR THE CERTIFICATE POLICY EXTENSION

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

7.2 CRL PROFILE

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

7.3 OCSP PROFILE

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

8 COMPLIANCE AUDIT AND OTHER CONTROLS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9 OTHER LEGAL AND COMMERCIAL AFFAIRS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE FEES

The rates are published on the website of Thomas Signe S.A.S. <https://www.thomas-signe.co/solicitud-de-servicios>

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

9.1.2 CERTIFICATE ACCESS FEES

The access to the consultation of the status of the issued certificates is free and free of charge.

9.1.3 FEES FOR REVOCATION OR ACCESS TO STATUS INFORMATION


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

9.1.4 FEES FOR OTHER SERVICES

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

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.

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 19 of 22

9.2 FINANCIAL RESPONSIBILITIES

9.2.1 INSURANCE COVERAGE

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.3 CONFIDENTIALITY OF INFORMATION

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.4 DATA PROTECTION POLICY

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.5 INTELLECTUAL PROPERTY RIGHTS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.6 OBLIGATIONS

9.6.1 OBLIGATIONS OF DCE

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.6.2 OBLIGATIONS OF SUPPLIERS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.6.3 OBLIGATIONS OF APPLICANTS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.6.4 OBLIGATIONS OF SUBSCRIBERS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.


9.6.5 OBLIGATIONS OF RELYING ON THIRD PARTIES

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.6.6 OBLIGATIONS OF THE ENTITY TO WHICH THE SUBSCRIBER IS RELATED

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.7 RESPONSIBILITIES

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 20 of 22

9.7.1 DCE'S RESPONSIBILITIES

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.7.2 SUBSCRIBER'S RESPONSIBILITIES

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.8 LIMITATION OF LIABILITY

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.9 INDEMNITIES

9.9.1 INDEMNITIES FOR DAMAGES CAUSED BY DCE

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.9.2 COMPENSATION FOR DAMAGES CAUSED BY CLAIMANTS, BY SUBSCRIBERS AND BY THIRD PARTIES WHO TRUST

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.10 PERIOD OF VALIDITY

9.10.1 TERM

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.10.2 REPLACEMENT AND REPEAL OF THE CPS AND CP'S

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.10.3 EFFECTS OF TERMINATION

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.11 PQRS

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.


9.12 CHANGES IN CPS AND CP

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.13 CLAIMS AND DISPUTE RESOLUTION

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.14 APPLICABLE LAW

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 21 of 22

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.15 IN ACCORDANCE WITH APPLICABLE LAW

As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

9.16 OTHER PROVISIONS

9.16.1 SUBSCRIPTION AGREEMENT

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, as well as the Subscriber's identification data and the date of signing of the contract by the Subscriber must be filled in.

Since each model is filled in with the Subscriber 's identification data, the document is classified as CONFIDENTIAL, although the document model is published on the indicated web page.

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 CP and associated CPS.

9.16.3 INDEPENDENCE

If any of the sections contained in this CP 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-CPS-01-F02 Legal Representative Certificate Application Form

THS-CO-AC-AC-CPS-01-F17 Application and Acceptance of Digital Certification Service

Provision (Legal Representative) v1.0

THS-CO-AC-AC-CPS-01-F18 Application and Acceptance of Digital Certification Service


Provision (Subscriber) v1.0

THS-CO-AC-AC-CPS-01-F15 Reading Protocol for Identity Verification Videoconferencing

THS-CO-AC-AC-CPS-01-F20 Digital Certificates Commercial Proposal v1.0

11 RECORDS

ID	SUPPORT	RESPONSIBLE	FILE	RETENTION TIME
----	---------	-------------	------	----------------

	Certificate Policy for Legal Representative	Version 2.7
	Code: THS-CO-AC-PC-COR-03	Page 22 of 22

Completed Legal Representative Certificate Application Forms	TI	Registry Operator	SAR Platform	7 years or according to applicable regulations
Signed Commercial Proposals of Digital Certificates - Legal Representative	TI	Sales Manager	SAR Platform	7 years or according to applicable regulations
Signed Application and Acceptance Forms for Issuance of Certificates	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
-------------------------------------------------	----	-------------------	-------------	------------------------------------------------