


# **Digital Certification Entity**



## **Automated Signature Certificate Policy**


	Automated Signature Certificate Policy	Version <b>2.6</b>
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 2 of 26

## Document Information


<b>Name</b>	AUTOMATED SIGNATURE CERTIFICATE POLICY
<b>Performed by</b>	THOMAS SIGNE S.A.S.
<b>Country</b>	COLOMBIA
<b>Version</b>	2.6
<b>Date</b>	JANUARY, 2023
<b>Document Type</b>	PUBLIC
<b>Code</b>	<b>THS-CO-AC-PC-COR-01</b>

## Document version


<b>Version</b>	<b>Date</b>	<b>Description</b>
1.0	06/28/2017	Preparation of initial document.
1.1	05/12/2018	Clarifications in the life cycle procedure. Minor nomenclature changes.
1.2	05/20/2018	The Obligations section is added. The Certificate Operating Procedure is specified.
1.3	05/24/2018	The section on Circumstances for revocation of a certificate has been added.
1.4	06/08/2018	Sections for formats and records have been added.
1.5	11/02/2018	The reference to THS-PR-GRAL-02-F01 Document Structure v1.0 is removed from the footer. The "INTRODUCTION" section is deleted.
1.6	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.
1.7	05/09/2019	Integration in the management system of the Group.

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 3 of 26

		<p>Change of document name from THS-PC-CC-01 to THS-CO-POL-COR-COR-AC-01.</p> <p>Added the possibility of optionally issuing the certificate on the Other Devices media, based on a certificate request in PKCS #10 format delivered by the Applicant, instead of on the Centralized HSM media.</p> <p>The sections on formats and applicable records are deleted.</p> <p>Minor corrections.</p>
1.8	09/18/2019	<p>Adjustment of the coding according to GSIGNE-GRAL-PR-01 Control of Documented Information Ed 2.1.</p> <p>The possibilities are added that the Subscriber can be a Natural Person, that the Applicant can be a Legal Person other than the Subscriber, and that, in the case that the type of support is Other Devices, there are two Applicants (a Legal Person other than the Subscriber and a Natural Person).</p> <p>In the certificate application, in cases where the Applicant is not the Legal Representative or there are two Applicants, the identity document of the Legal Representative shall be attached, in addition to the authorization signed by him/her with the data of the Natural Person or Legal Entity authorized to apply for and obtain the 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 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>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 different Natural Persons or Legal Entities).</p> <p>Minor corrections.</p>
1.9	11/29/2019	<p>Change of the current account number to deposit 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 contents of the CP based on the applicable legislation and regulations and the contents of the Management System documentation by a multidisciplinary work team.</p> <p>Change of the name of the document from "Component Certificates Certification Policy" to "Component Certificates Policy".</p> <p>Certification Policy" to "Component Certificates Policy".</p> <p>Changes in the organization of the document content to follow the recommendations of the RFC 3647 standard.</p> <p>The possibility that the Subscriber may be a company or entity Natural Person is added.</p>


	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 4 of 26

		<p>The possibilities that the Applicant may be a company or entity Natural Person other than the Subscriber and that, in the case of two Applicants, the first Applicant may be a company or entity Natural Person other than the Subscriber are added.</p> <p>The case in which the Applicant is a company or entity (Legal Entity or Natural Person) different from the Subscriber is described in more detail, including the functions of the Group Operator (GO) and the Certificate Administrator.</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	Minor corrections.
2.2	11/06/2020	<p>The possibility is added that the certificate presented by a Group Operator (GO) when accessing the SAR platform can be a Natural Person certificate, as an alternative to a Company Membership certificate, previously issued to the GO by the DCE in Centralized HSM.</p> <p>The possibility is added that the type of identity document of the Applicant (Natural Person) and of the Legal Representative of the Subscriber (Legal Entity) or of the Subscriber (Natural Person) can be the 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 "Component Certificate Policy" to "Automated Signature Certificate Policy".</p> <p>Changes in the certificate issuance fees.</p> <p>In the certificate request form (Annex I), the field Charge is added in the Administrator data.</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 Added issuerAltName to the certificate profile.</p> <p>Updated revocation means</p> <p>Changed the PQRS procedure in line with the new CEA version.</p>
2.6	20/01/2023	Corrections and minor changes.


	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 5 of 26

## CONTENTS

1	INTRODUCTION .....	7
1.1	PRESENTATION OF THE DOCUMENT.....	7
1.2	DOCUMENT NAME AND IDENTIFICATION .....	7
1.3	THOMAS SIGNE S.A.S. PKI PARTICIPANTS .....	8
1.3.1	THOMAS SIGNE S.A.S. PKI CERTIFICATE HIERARCHY .....	8
1.3.2	THOMAS SIGNE ROOT .....	8
1.3.3	DCE THOMAS SIGNE S.A.S. (DCE THOMAS SIGNE COLOMBIA).....	8
1.3.4	APPLICANT .....	8
1.3.5	SUBSCRIBER .....	9
1.3.6	TRUSTING THIRD PARTY.....	9
1.4	TYPES OF SUPPORT AND USES OF CERTIFICATES .....	9
1.4.1	CENTRALIZED HSM SUPPORT .....	9
1.4.2	OTHER DEVICE SUPPORT .....	9
1.4.3	APPROPRIATE USES OF CERTIFICATES .....	10
1.4.4	UNAUTHORIZED USES OF CERTIFICATES .....	10
1.5	CPS AND CP ADMINISTRATION .....	10
1.6	DEFINITIONS AND ACRONYMS.....	10
1.6.1	DEFINITIONS.....	10
1.6.2	ACRONYMS.....	11
2	RESPONSIBILITIES REGARDING REPOSITORIES AND PUBLICATION OF INFORMATION .....	12
3	IDENTIFICATION 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 .....	13
3.2.4	UNVERIFIED SUBSCRIBER AND APPLICANT INFORMATION .....	13
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 .....	14
4.1	CERTIFICATE APPLICATION.....	14
4.1.1	WHO CAN APPLY FOR A CERTIFICATE.....	14
4.1.2	MARKETING .....	14
4.1.3	CONTRACTING AND PAYMENT.....	15
4.1.4	APPLICATION .....	15
4.2	PROCESSING OF CERTIFICATE APPLICATIONS.....	16
4.2.1	REVIEW.....	16
4.2.2	DECISION.....	17
4.3	ISSUANCE OF CERTIFICATES .....	17
4.3.1	DCE ACTIONS DURING ISSUANCE OF CERTIFICATES .....	17
4.3.2	NOTIFICATION TO THE APPLICANT AND SUBSCRIBER BY DCE OF CERTIFICATE ISSUANCE.....	18
4.4	ACCEPTANCE OF THE CERTIFICATE .....	18
4.4.1	FORM IN WHICH THE CERTIFICATE IS ACCEPTED.....	18
4.4.2	PUBLICATION OF THE CERTIFICATE BY DCE.....	18
4.4.3	NOTIFICATION OF THE ISSUANCE OF THE CERTIFICATE BY DCE TO OTHER ENTITIES .....	18
4.5	USES OF KEYS AND CERTIFICATE .....	18
4.6	CERTIFICATE RENEWAL WITHOUT CHANGE OF KEYS.....	18
4.7	CERTIFICATE RENEWAL WITH KEY CHANGE .....	19
4.8	CERTIFICATE MODIFICATION.....	19
4.9	CERTIFICATE REVOCATION AND SUSPENSION.....	19
4.10	CERTIFICATE STATUS INFORMATION SERVICES.....	19
4.11	SUBSCRIPTION TERMINATION .....	19
4.12	KEY ESCROW AND RECOVERY .....	19
5	PHYSICAL, FACILITY, MANAGEMENT AND OPERATIONAL .....	19
6	SECURITY CONTROLS .....	19
7	CERTIFICATE PROFILE, CRL AND OCSP .....	20

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 6 of 26

7.1	CERTIFICATE PROFILE .....	20
7.1.1	CERTIFICATE FORMAT AND VALIDITY PERIOD .....	20
7.1.2	CERTIFICATE EXTENSIONS .....	20
7.1.3	OBJECT IDENTIFIERS (OID) OF ALGORITHMS .....	20
7.1.4	NAME FORMATS .....	21
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 .....	22
7.1.9	SEMANTIC TREATMENT FOR THE CERTIFICATE POLICY EXTENSION .....	22
7.2	CRL PROFILE .....	22
7.3	OCSP PROFILE .....	22
8	COMPLIANCE AUDIT AND OTHER CONTROLS .....	22
9	OTHER LEGAL AND COMMERCIAL AFFAIRS .....	22
9.1	FEES .....	22
9.1.1	CERTIFICATE ISSUANCE FEES .....	22
9.1.2	CERTIFICATE ACCESS FEES .....	22
9.1.3	FEES FOR REVOCATION OR ACCESS TO STATUS INFORMATION .....	23
9.1.4	FEES FOR OTHER SERVICES .....	23
9.1.5	REFUND POLICY .....	23
9.2	FINANCIAL RESPONSIBILITIES .....	23
9.2.1	INSURANCE COVERAGE .....	23
9.3	CONFIDENTIALITY OF INFORMATION .....	23
9.4	DATA PROTECTION POLICY .....	23
9.5	INTELLECTUAL PROPERTY RIGHTS .....	23
9.6	OBLIGATIONS .....	23
9.6.1	OBLIGATIONS OF DCE .....	23
9.6.2	OBLIGATIONS OF SUPPLIERS .....	23
9.6.3	OBLIGATIONS OF APPLICANTS .....	24
9.6.4	OBLIGATIONS OF SUBSCRIBERS .....	24
9.6.5	OBLIGATIONS OF RELYING THIRD PARTIES .....	24
9.7	RESPONSIBILITIES .....	24
9.7.1	DCE'S RESPONSIBILITIES .....	24
9.7.2	SUBSCRIBER'S RESPONSIBILITIES .....	24
9.8	LIMITATION OF LIABILITY .....	24
9.9	INDEMNITIES .....	24
9.9.1	INDEMNITIES FOR DAMAGES CAUSED BY DCE .....	24
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 .....	25
9.11	PQRS .....	25
9.12	CHANGES IN CPS AND CP .....	25
9.13	CLAIMS AND DISPUTE RESOLUTION .....	25
9.14	APPLICABLE LAW .....	25
9.15	IN ACCORDANCE WITH APPLICABLE LAW .....	25
9.16	OTHER PROVISIONS .....	25
9.16.1	SUBSCRIPTION AGREEMENT .....	25
9.16.2	FULL ACCEPTANCE CLAUSE .....	25
9.16.3	INDEPENDENCE .....	26
9.17	OTHER STIPULATIONS .....	26
10	FORMATS .....	26
11	RECORDS .....	26

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 7 of 26

# 1 INTRODUCTION

## 1.1 PRESENTATION OF THE DOCUMENT

This document constitutes the Policy of Certificates (CP) for Automated Signature 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 bodies.

The Certificates for Automated Signature issued by Thomas Signe S.A.S. are certificates that allow to identify and sign the Subscriber as 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), which are issued for computer devices, programs or applications dedicated to sign on behalf of the company or entity in automated digital signature systems.

This CP establishes the requirements of the Certificates for Automated Signature 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 Binding to Company/Entity issued by Thomas Signe S.A.S. are governed by the practices established in the

Company/Entity Certificates issued by Thomas Signe S.A.S. are governed by the practices established in the Certification Practices Statement (CPS) for the issuance of Thomas Signe S.A.S. certificates. This CPS is 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 intended for all natural and legal persons, Applicants, Subscribers, Relying Third Parties, and the public.

If vulnerabilities are detected, or the technical standards or infrastructure indicated in this CP 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, this document is identified with the following OIDs, contained in the X.509 v3 Certificate Policies extension of the Automated Signature Certificates issued by Thomas Signe S.A.S. in the indicated media types.

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 8 of 26

<b>OID OF THE CERTIFICATE CP FOR AUTOMATED SIGNATURE 1.3.6.1.4.1.51362.0.2.1.4</b>	
1.3.6.1.4.1.51362.0.2.1.4.3	Centralized HSM Support
1.3.6.1.4.1.51362.0.2.1.4.2	Support Other Devices

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

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.

#### 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 or legal person that requests to DCE Thomas Signe S.A.S. the issuance of a Certificate for Automated Signature.

In this CP, the Applicant includes:

- 1) The Legal Representative of the Subscriber who is a Legal Entity.
- 2) The Subscriber who must be a Natural Person.
- 3) An individual Natural Person with a position in the Subscriber's company or entity, authorized by 1) or 2) to request and obtain the Subscriber's certificate.
- 4) A company or entity (Legal Entity or Natural Person, whether it is a company or other type of public or private entity that carries out an economic activity for which it is obliged to register in a fiscal or tax registry) other than the Subscriber, authorized by 1) or 2) to request and obtain the certificate of the Subscriber.

If the Subscriber is the only Applicant 4), the Applicant must designate one or more individual Natural Person(s) with a position in the company or entity (Group Operator(s)) as responsible for entering the data in the certificate application form and attaching the requested documents. In turn, the Group Operator shall enter in the certificate application form the data of another individual Natural Person with a position in the company or entity (who may be the same) as Administrator of the certificate, who will be the one to whom the certificate will be delivered.



	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 9 of 26

### 1.3.5 SUBSCRIBER

In this CP, Subscriber is the natural or legal person in whose name the DCE Thomas Signe S.A.S. issues a Certificate for Automated Signature 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 Agreement 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 Automated Signature issued in his 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 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).

### 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 Automated Signature issued by DCE Thomas Signe S.A.S.

The Relying Third Party, in turn, may or may not be an Applicant and/or Subscriber.

## 1.4 TYPES OF SUPPORT AND USES OF CERTIFICATES

### 1.4.1 CENTRALIZED HSM SUPPORT

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

The private keys of the Automated Signature Certificates 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
- Identity theft due to carelessness of the Subscriber in the custody of cryptographic devices.
- Physical damage to the cryptographic module


The access to the private key of a Certificate for Automated Signature issued in this cryptographic device is made 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.

Automated Signature Certificates issued in HSM Centralized are identified by the OID (1.3.6.1.4.1.51362.0.2.1.4.3) in the X.509 v3 Certificate Policies extension.

### 1.4.2 OTHER DEVICE SUPPORT

The issuance of Certificates for Automated Signature on Other Devices is limited to the case where an Applicant submits a certificate request in PKCS #10 format, containing an RSA public key of size 2048 bits.

The emission of the Certificates for Automated Signature in this support, it is contemplated the possibility of having two Applicants. The first Applicant will be a company or entity (Legal Entity or Natural Person) other than the Subscriber, who submits the certificate request in PKCS #10 format and some data from the certificate request form (see Annex I), while the second Applicant will be the Legal Representative of the Subscriber (Legal Entity) or the Subscriber (Natural Person), who completes the data from the certificate request form and attaches the documents required in the SAR platform (see section 4.1.4).

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page <b>10</b> of <b>26</b>

The private keys of the Certificates for Automated Signature issued in this support, associated to the public keys contained in the certificate requests in PKCS #10 format delivered by the Applicants, will have been generated in cryptographic devices of any type (software, HSM, token/card), according to the security level that the Subscribers consider adequate. These cryptographic devices may be FIPS 140-2 level 3 certified, resulting in a high level of security, to protect the private keys against risks such as:

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

The access to the private key of a Certificate for Automated Signature issued in one of these cryptographic devices is made by means of the specific data determined by the type of cryptographic device where the private key has been generated or installed, which constitute, therefore, the activation data of the private key.

Certificates for Automated Signature issued in Other Devices are identified by the OID (1.3.6.1.4.1.51362.0.2.1.4.2) in the X.509 v3 Certificate Policies extension

### 1.4.3 APPROPRIATE USES OF CERTIFICATES

Certificates for Automated Signature emitted by Thomas Signe S.A.S. may be used in the terms established in the present CP, in the CPS for the emission of certificates of Thomas Signe S.A.S. and in what is established in the current legislation in this respect.

Certificates for Automated Signature can be used as identification and authentication mechanism in automated digital signature systems.

The use of these certificates is permitted in the Subscriber's relations with the Public Administrations.

### 1.4.4 UNAUTHORIZED USES OF CERTIFICATES

It is not allowed to use other than what is established in this CP and the CPS for the issuance 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.

Additionally, in this CP the following definitions are also applicable:


**Certificate Administrator:** individual natural person to whom the Subscriber's digital certificate will be delivered. It is the same natural person as the Applicant, except when the latter is a company or entity (legal person or natural person) other than the Subscriber, in which case the Certificate Administrator will be the individual natural person with the data entered by the Group Operator in the certificate application form, who must have a position in such company or entity.

**Group Operator:** individual natural person designated by the Applicant, when the latter is a company or entity (legal entity or natural person) other than the Subscriber, as the person responsible for entering the data in the certificate application form and attaching the requested documents, who must have a position in said company or entity.

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 11 of 26

## 1.6.2 ACRONYMS

<b>CA</b>	Certification Authority
<b>CRL</b>	Certificate Revocation List
<b>DN</b>	Distinguished Name
<b>CPS</b>	Certification Practices Statement
<b>DCE</b>	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.
<b>FIPS</b>	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.).
<b>HSM</b>	Hardware Security Module
<b>IEC</b>	International Electrotechnical Commission
<b>ISO</b>	International Organization for Standardization
<b>ITU</b>	International Telecommunication Union
<b>NIT</b>	Tax Identification Number
<b>OCSP</b>	Online Certificate Status Protocol
<b>ONAC</b>	National Accreditation Organization of Colombia
<b>RA</b>	Registry Operator
<b>CP</b>	Certificate Policy
<b>PKCS</b>	Public-Key Cryptography Standards. Cryptography standards conceived and published by RSA laboratories.
<b>PKI</b>	Public Key Infrastructure
<b>PQRS</b>	Petitions, Complaints, Claims and Suggestions
<b>RA</b>	Registration Authority
<b>RFC</b>	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.
<b>RSA</b>	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.
<b>RUES</b>	Single Corporate and Social Registry
<b>SAR</b>	Signe Registration Authority
<b>SHA</b>	Secure Hash Algorithm

 THOMAS SIGNE	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page <b>12</b> of <b>26</b>

## 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 in the instant prior to certificate issuance, through a procedure that guarantees its confidentiality and its binding to the Applicant.


When a certificate is issued for Other Devices, the method of proof of possession of the private key shall be the delivery to the RA of a certificate request in PKCS #10 format containing the corresponding public key.

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

The RA will verify the identity of the company or entity (Legal Entity or Natural Person) Subscriber As specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

Additionally, if the Applicant is a company or entity (Legal Entity or Natural Person) other than the Subscriber, the RA will verify the identity of this company or entity through the following procedures:

- The previous signature of a Service Contract between the company or entity and Thomas Signe S.A.
- Verification of the identity of the individual Natural Person with a position in the company or entity (called Group Operator or GO) designated by the company or entity as responsible for entering the data in the certificate application form and attaching the requested documents in the SAR platform, as indicated in section 3.2.3. In turn, the GO shall enter in the certificate application form in the SAR platform the data of another individual Natural Person with a position in the company or entity (which may be him/herself) as Certificate Administrator, who will be the one to whom the certificate will be delivered, through a process in which the Certificate Administrator must click on a link with a unique code that he/she will receive in the email address entered by the GO in the certificate application form. The RA will not verify the identity of this Certificate Administrator.
- The verification of the company or entity data in the signed authorization attached by the GO in the certificate request in the SAR platform, by means of which the Subscriber authorizes the company or entity to request and obtain its certificate.

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page <b>13</b> of <b>26</b>

### 3.2.3 AUTHENTICATION OF THE IDENTITY OF AN INDIVIDUAL NATURAL PERSON

The RA shall reliably verify the identity of the Applicant Natural Person as specified in the CPS for the issuance of Thomas Signe S.A.S. certificates.

In the case of certificates for Automated Signature whose Applicant is a company or entity (Legal Entity or Natural Person) other than the Subscriber, the RA shall verify the identity of the individual Natural Person OG designated by such company or entity (see section 3.2.2), by automatically checking, when the OG accesses the SAR platform, the username and password entered and the certificate presented, which must be a certificate for Company/Entity Binding, for Legal Representative or for Natural Person previously issued to the OG by the DCE in Centralized HSM. To present this certificate when accessing the SAR platform, the OG must enter his user and password to access the Centralized HSM, and then, as activation data of the private key, a password, defined by him when generating the keys in the Centralized HSM at the previous moment to the issuance of the certificate, and a code that the OG will receive on his cell phone.

### 3.2.4 UNVERIFIED SUBSCRIBER AND APPLICANT INFORMATION

Under any circumstances shall the RA 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 RA shall not verify the following data of the Subscriber and the Applicant entered in the certificate application form in the SAR platform, by other means than verifying them in the corresponding signed authorization, by which the Subscriber authorizes the Applicant to request and obtain the certificate, in cases where such authorization is required, presuming the good faith of the information provided by the Applicant and the Subscriber:

- Data contained in the certificate: name of the automated signature system or application and/or area of the Subscriber managing the automated signature system or application; contact email of the Subscriber. In cases where a signed authorization is required from the Applicant, whether it is an individual Natural Person or a company or entity (Legal Entity or Natural Person), the RA will verify that the data entered in the certificate application form conforms to the data in said authorization.

- Data not contained in the certificate, if the Applicant is an individual Natural Person (data of the Certificate Administrator): position in the company or entity Subscriber; cell phone number; e-mail. In cases where a signed authorization is required from the Applicant, the RA will verify that the data entered in the certificate application form conforms to the data in the authorization.

- Data not contained in the certificate, if the Applicant is a company or entity (Legal Entity or Natural Person) other than the Subscriber: all the data of the Certificate Administrator entered in the certificate application form in the SAR platform by the GC designated by the Applicant. The RA will not perform any verification of the data entered in the certificate application form.


### 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 or 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, depending on the type of media on which the certificate has been issued:

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 14 of 26

- Centralized HSM: The Subscriber or Applicant must enter his/her username and password to access the Centralized HSM, and a code that will be sent to the mobile phone.

- Other Devices: The Subscriber or Applicant must enter the revocation code provided upon delivery of the certificate.

## 4 OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF THE CERTIFICATES

### 4.1 CERTIFICATE APPLICATION

#### 4.1.1 WHO CAN APPLY FOR A CERTIFICATE

The following are eligible to apply for a Certificate for Automated Signature:

- 1) The Legal Representative of the Subscriber who is a Legal Entity.
- 2) The Subscriber is a Natural Person.
- 3) An individual Natural Person with a position in the Subscriber's company or entity, authorized by 1) or 2) to request and obtain the Subscriber's certificate.
- 4) 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, authorized by 1) or 2) to request and obtain the Subscriber's certificate.

If the sole Applicant is 4), the Applicant must designate one or more individual Natural Person(s) with a position in the company or entity (called Group Operator(s)) as responsible for entering the data in the certificate application form and attaching the requested documents. In turn, the Group Operator shall enter in the certificate application form the data of another individual Natural Person with a position in the company or entity (who may be the same) as Administrator of the certificate, who will be the one to whom the certificate will be delivered.

#### 4.1.2 MARKETING

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


- Consulting the web page [www.thomas-signe.co](http://www.thomas-signe.co)
- Via informative e-mail to [comercial@thomas-signe.co](mailto:comercial@thomas-signe.co)
- Directly dealing 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 the Subscriber will indicate to the Commercial Area and/or a RO:

- 1) The type of certificate and the type of support required (Certificate for Automated Signature in Centralized HSM or in Other Devices).
- 2) The validity of the certificate required.
- 3) The full name of the Applicant.
- 4) The type and number of the Applicant's ID document.
- 5) The email account of the Applicant that will be associated to the digital certificate and through which the DCE will send official notifications and communications.
- 6) The Subscriber's name or company name.
- 7) The NIT of the Subscriber.

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 the Subscriber: The Commercial Proposal (sent by the Commercial Area), if applicable; the Subscription Contract; an authorization model for the application and obtaining of the certificate, if required; optionally, a link to the SAR platform; and the respective indications.

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 15 of 26

### 4.1.3 CONTRACTING AND PAYMENT

To proceed with the contracting and payment, the Applicant and/or Subscriber shall:

- Make 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 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 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.


Note that, additionally to the Subscription Agreement with the Subscriber, depending on the type of contract, a Service Agreement between Thomas Signe S.A.S. and the Subscriber may be required.

- If the Applicant is a company or entity (Legal Entity or Natural Person) other than the Subscriber, approve all terms and conditions set forth in a Service Agreement between Thomas Signe S.A.S. and the Applicant, by signing it. The evidence of this process will be the signed Service Agreement.
- If the Applicant is a company or entity (Legal Entity or Natural Person) other than the Subscriber, designate one or more individual Natural Person(s) with a position in such company or entity (Group Operators) as responsible for entering the data in the certificate application form and attaching the documents requested in the SAR platform.

### 4.1.4 APPLICATION

To request the issuance of a digital certificate, the Applicant (and Subscriber) and/or the Entity to which it is linked may enter the SAR platform and correctly complete the data in the certificate request form (see Annex I). In addition, within the SAR platform, they will proceed to attach the documents indicated below:

- In cases where the Subscriber is an individual Natural Person, identity document of the Subscriber, 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 Subscriber, in virtual copy or scanned, in the applicable cases; issued in Colombia (by default) or in another country no more than 30 days before.
- Single Tax Registration or equivalent document of the Subscriber, 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 Subscriber (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 no more than 30 days before.

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page <b>16</b> of <b>26</b>

- In cases where the Applicant is neither the Legal Representative of the Subscriber (Legal Entity) nor the Subscriber (Natural Person), or there are two Applicants (see section 1.4.2):
  - o Authorization signed by the Legal Representative of the Subscriber (Legal Entity) or by the Subscriber (Natural Person), with the data of the individual Natural Person or of the company or entity (Legal Entity or Natural Person) authorized to request and obtain the Subscriber's Automated Signature Certificate; issued a maximum of 30 days before.
  - o Identification document of the Legal Representative or of the Subscriber (Natural Person) signing the authorization, scanned on both sides: Citizenship Card, Alien Registration Card, or Passport; issued in Colombia (by default) or in another country (equivalent document).
- Proof of payment of the certificate fee indicated in the Commercial Proposal or in the Service Rendering Agreement, where applicable.
- Signed Subscription Contract.

Additionally, in the case that the type of support is Other Devices, the Applicant shall attach the certificate request in the SAR platform in PKCS #10 format, unless there are two Applicants in which case the request will have already been attached in the SAR platform once sent by the first Applicant.

Alternatively, the Applicant and/or the Subscriber may personally deliver or send the required data and documents to the Commercial Area and/or an RO, and they will enter the data in the certificate request 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 on the SAR platform and that they all meet the following:

- They are complete and legible.
- They are apparently genuine.
- If applicable, they were current when they were attached on the SAR platform.


- The data they contain regarding the Subscriber, the Applicant, 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 and/or in the Service Agreement. Discrepancy will be accepted only for the complete address of the Subscriber 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 Subscriber's NIT 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.

If it is necessary to regularize payments or documentation, the Applicant or Subscriber will be notified at the e-mail address provided by the Applicant or Subscriber.

Once all the required documentation and evidence has been collected and reviewed, an RO will coordinate with the Subscriber (Natural Person) or with the Subscriber's Legal Representative (Legal Entity) 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 to verify that it matches the document received. 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.



	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page <b>17</b> of <b>26</b>

Alternatively to the 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 identity of the subscriber, the RO will approve or reject the request for issuance of the certificate in 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 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 Subscriber) notifying them of the reasons for the decision not to issue the certificate.

## 4.3 ISSUANCE OF CERTIFICATES

### 4.3.1 DCE ACTIONS DURING ISSUANCE OF CERTIFICATES

Once the RA Decision Operator 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 activities:

1) The keys will be generated by the Certificate Manager in the Centralized HSM or will have been previously generated in Subscriber or Applicant systems, delivering to the RA, in both cases, 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 latter the corresponding issued certificate.

- In the case that the type of support is HSM Centralized, this process will be performed automatically when the RA receives the certificate request in PKCS #10 format, without the intervention of an RA operator.

- In case the media type is Other Devices, this process will be performed automatically when an RA Decision Operator makes the decision to issue the certificate.

3) Finally, the RA will deliver the certificate.

- In case the type of support is Centralized HSM, the certificate is automatically installed in the Centralized HSM associated to the keys generated in it by the Certificate Manager.

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page <b>18</b> of <b>26</b>

- In case the media type is Other Devices, the RA will automatically send to the Certificate Manager and the Subscriber an e-mail message containing a link to download the certificate and a random revocation code.

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

If the media type is Centralized HSM, the Centralized HSM itself notifies the Certificate Manager that the certificate has been issued and installed on the HSM.

In case the media type is Other Devices, the RA notifies the Certificate Manager and the Subscriber of the certificate issuance in the same email in which it sends the download link and a random revocation code

Then, in both cases, the RA sends an email to the Certificate Administrator and the Subscriber that includes the following:

- Data document of the purchased 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 purchased certificate (type and support of the certificate, issue and expiration dates of the certificate, Subscriber data contained in the certificate); data necessary for the use of the certificate in Centralized HSM by the Subscriber, in case the type of support is Centralized HSM; signature of the RA Decision Operator who has made the decision to issue the certificate.
- Link to the web page where the CPS for the issuance of Thomas Signe S.A.S. certificates and the present CP are published.
- Integration and use manual of the certificate in HSM Centralized by applications in its current version, in the case that the type of support is HSM Centralized, in the applicable cases.

### 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.

 THOMAS SIGNE	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page <b>19</b> of <b>26</b>

#### 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 the 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. S.A.S. through the following [link](#). In case the type of support is HSM Centralized, the Subscriber must enter his/her user and password to access the HSM Centralized, and a code that will be sent to the mobile.

In the Thomas Signe S.A.S. CPS for the issuance of certificates you will find all the additional information concerning 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 same time of expiration or revocation of the certificate

#### 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 Automated Signature complies with the CPS for the issuance of Thomas Signe S.A.S. certificates.

Certificates for Automated Signature have a validity period of up to 2 years (730 days).

#### 7.1.2 CERTIFICATE EXTENSIONS

The following table specifies the extensions of the Automated Signature Certificates.

Extension	Critical	Value
<b>Authority Key Identifier</b>	-	Identifier of the public key of the certificate of the Subordinate CA, obtained from the SHA-1 hash of the certificate.
<b>Subject Key Identifier</b>	-	Identifier of the public key of the certificate, obtained from the SHA-1 hash of the certificate.
<b>Key Usage</b>	Yes	digitalSignature nonRepudiation
<b>Certificate Policies</b>	-	OID 1.3.6.1.4.1.51362.0.2.1.2.x <sup>1</sup> URI of CPS: <a href="http://thsigne.com/cps">http://thsigne.com/cps</a>
<b>Subject Alternative Name</b>		rfc822Name: <i>e-mail address of Subscriber</i>
<b>Basic Constraints</b>	Yes	cA: FALSE
<b>Extended Key Usage</b>	-	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)
<b>CRL Distribution Points</b>	-	URI of CRL: <a href="http://crl-co.thsigne.com/ecd_thomas_signe_colombia.crl">http://crl-co.thsigne.com/ecd_thomas_signe_colombia.crl</a>
<b>Authority Information Access</b>	-	URI of the certificate of the Subordinate CA: <a href="http://thsigne.com/certs/ecd_thomas_signe_colombia.crt">http://thsigne.com/certs/ecd_thomas_signe_colombia.crt</a>  URI of the OCSP service of the Subordinate CA: <a href="http://ocsp-co.thsigne.com">http://ocsp-co.thsigne.com</a>
<b>Issuer Alternative Name</b>	-	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.

<sup>1</sup> Centralized HSM: x=3; Other Devices (PKCS #10): x=2

#### 7.1.4 NAME FORMATS

The following table specifies the corresponding attributes of the DN of the holder of an Automated Signature Certificate (Certificate Subscriber).

DN attribute	Description	Value
<b>Country Name (C)</b>	Country	<i>Two-letter code according to ISO 3166-1 of the country of the Entity</i> <sup>1</sup> Default: CO
<b>State or Province Name (ST)</b>	State/Province	<i>Department of the Entity</i> <sup>2</sup>
<b>Locality Name (L)</b>	Location	<i>Municipality of the Entity</i> <sup>2</sup>
<b>Street Address (STREET)</b>	Address	<i>Subscriber Address</i> <sup>2</sup>
<b>Organization Identifier (2.5.4.97)</b>	Organization Identifier	<i>Tax Identification Number of the Entity (in Colombia: NIT)</i> <sup>2</sup>
<b>Organizational Unit Name (OU)</b>	Organizational Unit	<i>Name or corporate name of the Entity</i> <sup>2</sup>
<b>Organizational Unit Name (OU)</b>	Organizational Unit	<i>Area of the Subscriber managing the automated signature system or application or name of the automated signature system or application</i> <sup>2</sup>
<b>Common Name (CN)</b>	Name	<i>Name of the automated signature system or application and/or name or company name of the Subscriber</i> <sup>2</sup>

#### 7.1.5 NAME RESTRICTIONS

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

#### 7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)

The OIDs of the Certificate Policy for Company/Entity Binding 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.


#### 7.1.7 USE OF THE EXTENSION POLICY CONSTRAINTS

Automated Signature Certificates do not contain the Policy Constraints extension.

---

<sup>1</sup> Encoded in PrintableString

<sup>2</sup> Encoded in UTF8String

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 22 of 26

### 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 fees specified are referential and may vary according to the type of certificate and the contract with each client.

CERTIFICATE	VALIDITY	PRICE*
<b>For Automated Signature Centralized HSM Support</b>	1 year	\$ 450.000 COP
	2 years	\$ 810.000 COP
<b>For Automated Signature Other Devices Support (PKCS #10 request)</b>	1 year	\$ 105.000 COP
	2 years	\$ 185.000 COP


\* Price excluding VAT in Colombian pesos for a certificate of the indicated validity period.

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

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

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 23 of 26

### 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

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 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.

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 24 of 26

### 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.

## 9.7 RESPONSIBILITIES

### 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.



	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 25 of 26

### 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

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


In the case of Automated Signature Certificates, if the Subscriber is a Legal Entity, the contract shall 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, although 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 CP and associated CPS.

	Automated Signature Certificate Policy	Version 2.6
	Code: <b>THS-CO-AC-PC-COR-01</b>	Page 26 of 26

### 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-F01 Automated Signature Certificate Application Form THS-CO-AC-AC-CPS-01-F08 Commercial Proposal for Digital Certificates - Automated Signature THS-CO-AC-AC-CPS-01-F08 Authorization Application for Automated Signature Certificate - Individual Natural Person

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

THS-CO-AC-AC-CPS-01-F12 Authorization Application for Certificate for Automated Signature - Other Entity THS-CO-AC-AC-CPS-01-F13 Authorization Pre-Application for Certificate for Automated Signature - Other

Entity

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

THS-CO-AC-AC-CPS-01-F15 Reading Protocol for Identity Verification Videoconference THS-CO-AC-AC-CPS-01-F19 Authorization Request Certificate for Automated Signature

## 11 RECORDS

ID	SUPPORT	RESPONSIBLE	FILE	RETENTION TIME
Complete Certificate Application Forms for Automated Signatures	TI	Registry Operator	SAR Platform	7 years or according to applicable regulations
Signed Commercial Proposals for Digital Certificates - Automated Signatures	TI	Sales Manager	SAR Platform	7 years or according to applicable regulations
Signed Application and Acceptance Forms for Certificate Issuance	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