Digital Certification Entity

THOMAS SIGNE

Soluciones Tecnológicas Globales

Certificate Policy for Company/Entity Binding

Document Information

Name	CERTIFICATE POLICY FOR COMPANY/ENTITY BINDING
Prepared by	THOMAS SIGNE S.A.S.
Country	COLOMBIA
Version	2.7
Date	AUGUST, 2023
Document Type	PUBLIC
Code	**THS-CO-AC-PC-COR-02**

Document version

Version	Date	Description
1.0	06/28/2017	Preparation of the 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 is added.
1.3	06/08/2018	Sections for applicable formats and records are added.
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 eliminated.
1.5	01/22/2019	The possibility is added for the RO to optionally perform the verification of the Applicant's identity in person, instead of by videoconference. Minor corrections.
1.6	05/09/2019	Integration with the management system of the Group. Document name change from THS-PC-PE-01 to THS-CO-POL-COR-AC-02. Removed sections on applicable formats and records. Minor corrections.

1.7	09/18/2019	Coding adjustment according to GSIGNE-GRAL-PR-01 Control of Documented Information Ed 2.1. In the certificate request, the identity document of the Legal Representative shall be attached, in addition to the authorization signed by him/her with the data of the person authorized to request and obtain the certificate. In the review of the certificate request, in the validation of the identity document of the Applicant, the consultation before an online database is eliminated. 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). In the Serial Number attribute of the DN of the certificates, the format of the Subscriber's identification document type is indicated. The Formats and Records sections are added. 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). Minor corrections.
1.8	11/29/2019	Change of the current account number to deposit the amount for each service. Added a format and a register for identity verification videoconferences. Minor corrections.
2.0	01/31/2020	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. Change of the name of the document from "Company Membership Certification Policy" to "Company Membership Certificate Policy". Changes in the organization of the content of the document to follow the recommendations of the RFC 3647 standard. Added the possibility that the Entity to which the Subscriber (Natural Person) is linked can be a company or Natural Person entity. The current account number to make the deposit of the respective amount for each service has been eliminated (it will be indicated in the Commercial Proposal).
2.1	19/06/2020	The obligations of the Entity to which the Subscriber is bound are added. Minor corrections.
2.2	11/06/2020	Minor corrections.
2.3	06/24/2021	Rebranding of Thomas Signe. Change of the name of the document from "Company Membership Certificate Policy" to "Company/Entity Binding Certificate Policy".

		The Card/Token support, which was limited to certificates of the RA's trusted roles, is eliminated and replaced by certificates in the Centralized HSM support. The possibility that the type of identity document of the Legal Representative of the Entity (Legal Entity) to which the Subscriber is linked or of the Entity itself (Natural Person) is the Passport is added. Changes in the certificate issuance fees. Minor corrections.
2.4	11/19/2021	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. Certificate revocation requests sent to the PQRSA Manager by email are referred to an RA Decision Operator. Minor Corrections.
2.5	07/08/2022	Adaptation to the new version of CEA-3.0-07 Added issuerAltName to the certificate profile. Updated revocation means. Changed the PQRS procedure in line with the new CEA version.
2.6	20/01/2023	Corrections and minor changes
2.7	16/08/2023	Fees update

CONTENTS

1 INTRODUCTION

1.1 PRESENTATION OF THE DOCUMENT

This document constitutes the Certificate Policy (CP) for Company/Entity Binding 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 Company/Entity Binding issued by Thomas Signe S.A.S. are certificates that allow the Subscriber to identify and sign as a natural person linked to a company or entity (legal entity or natural person, 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), either as an employee, associate, collaborator, customer or supplier.

This CP establishes the requirements of the Certificates for Company/Entity Binding 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 Company/Entity Binding 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 Certificates for Company/Entity Binding issued by Thomas Signe S.A.S. in the indicated media types.

OID OF THE CERTIFICATE CP FOR COMPANY/ENTITY BINDING 1.3.6.1.1.4.1.51362.0.2.2.1.2.	
1.3.6.1.4.1.51362.0.2.1.2.3	Centralized HSM Support

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 person who requests DCE Thomas Signe S.A.S. to issue a Certificate for Company/Entity Binding.

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

1.3.5 SUBSCRIBER

In this CP, Subscriber is the natural person in whose name DCE Thomas Signe S.A.S. issues a Certificate for Company/Entity Binding 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 Thomas Signe S.A.S..

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

In this CP, Subscriber is a natural person linked to an Entity (legal entity or natural person), either as an employee, associate, collaborator, customer, or supplier. This Entity must sign an authorization with the Subscriber's data, including the Entity's data, the area of the Subscriber in the Entity or the type of relationship of the Subscriber with the Entity, and the position, title, or role of the Subscriber in the Entity, authorizing the Subscriber to request and obtain a certificate with such data.

1.3.6 TRUSTING THIRD PARTY

In this CP, Relying Third Party (or Accepting Third Party) are all those natural or legal persons that decide to accept and rely on a Certificate for Company/Entity Binding issued 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 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) to which the Subscriber is related through the relationship accredited in the certificate, whether as an employee, associate, collaborator, client or supplier.

1.4 TYPES OF SUPPORT AND USES OF CERTIFICATES

1.4.1 CENTRALIZED HSM SUPPORT

The issuance of Enterprise/Entity Binding 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 Certificates for Company/Entity Binding 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

Access to the private key of an Enterprise/Entity Binding Certificate issued in this cryptographic device is performed by means of a Subscriber's username, 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 constitute, therefore, the activation data of the private key.

Certificates for Company/Entity Binding issued in HSM Centralized are identified by the OID (1.3.6.1.4.1.51362.0.2.2.1.2.3) in the X.509 v3 Certificate Policies extension.

1.4.2 APPROPRIATE USES OF CERTIFICATES

Certificates for Company/Entity Binding 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 Company/Entity Binding must, in general, be used within the framework of the legal or binding relationship between the Subscriber and the Entity (Legal Entity or Natural Person) to which the Subscriber is related by means of the binding accredited in the certificate. 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.

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

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 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.

1.6.2 ACRONYMS

CA	Certification Authority
CRL	Certificate Revocation List

DN	Distinguished Name
CPS	Certification Practices Statement
DCE	Digital Certification Entity that provides digital certification services and is equivalent to a Certification Entity as defined in law 527 of 1999. It should also be understood as a Conformity Assessment Body - CAB as defined in ISO/IEC 17000.
FIPS	Federal Information Processing Standards (FIPS). These are publicly announced standards developed by the U.S. government for use by all non-military government agencies and government contractors. Many FIPS standards are modified versions of standards used in the broader communities (ANSA, IEEE, ISO, etc.).
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NIT	Tax Identification Number
OCSP	Online Certificate Status Protocol
ONAC	National Accreditation Organization of Colombia
RA	Registry Operator
CP	Certificate Policy
PKCS	Public-Key Cryptography Standards. Cryptography standards conceived and published by RSA laboratories.
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	Single 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 in the instant prior to certificate issuance, through a procedure that guarantees its confidentiality and its binding to the Applicant.

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

The RA will verify the identity of the Entity (Legal Entity or Natural Person) to which the Subscriber is related by means of the link accredited in the certificate 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 CPS for the issuance of Thomas Signe S.A.S. certificates.

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, by any means other than verifying them in the corresponding signed authorization, by which the Entity to which the Subscriber is related by means of the link accredited in the certificate authorizes the Subscriber to apply for and obtain the certificate, presuming the good faith of the information provided by the Subscriber and the Entity:

- Data contained in the certificate: area of the Subscriber in the Entity or type of linkage of the Subscriber with the Entity; position, title, or role of the Subscriber in the Entity; email of the Subscriber. The RA will verify that the data entered in the certificate request form conforms to the data in the signed authorization.
- Data not contained in the certificate: Subscriber's cell phone number. The RA will check that the data entered in the certificate application form conforms to the data in the signed authorization.

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 his or her 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 request a Certificate for Company/Entity Binding.

4.1.2 MARKETING

The Applicant (and Subscriber) and/or the Entity to which it is linked may receive information about the digital certification process in the following ways:

- Consulting the web pagewww.thomas-signe.co

- By 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, requirements, fees, and other related information.

After being informed, the Applicant (and Subscriber) and/or the Entity to which it is linked will indicate to the Commercial Area and/or an RO:

1) The type of certificate required (Certificate for Binding to Company/Entity).

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 NIT 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) and/or the Entity to which it is linked: the Commercial Proposal (sent by the Commercial Area), where applicable; the Subscription Contract; an authorization model for requesting and obtaining the certificate if required; optionally, a link to the SAR platform; and the respective indications.

4.1.3 CONTRACTING AND PAYMENT

To proceed with the contracting and payment, the Applicant (and 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 shall 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 Agreement.

- 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 in addition to the Subscription Agreement with each Subscriber of a digital certificate, depending on the type of contract, a Service Agreement between Thomas Signe S.A.S. and the Entity to which the Subscribers are linked may be required.

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:

- Identity document of the Applicant, scanned on both sides: Citizenship Card, Alien's Identity 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, 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, 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 (for example, a Certificate of Residence for Natural Persons), 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.
- Authorization signed by the Legal Representative of the Entity (Legal Entity) to which the Subscriber is linked or by the Entity itself (Natural Person), with the data of the Natural Person authorized to request and obtain a Certificate for Linking to a Company/Entity; issued a maximum of 30 days before.
- Identity document of the Legal Representative or of the Entity (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 Contract, if applicable.
- Application and acceptance document signed.

Alternatively, the Applicant (and Subscriber) and/or the Entity to which it is linked may personally deliver or send the required data and documents to the Commercial Area and/or an RO, and they will enter the data 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 legitimate.
- Where applicable, they were current when attached on 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.

In addition, for those cases in which it is possible, the RO will consult the TIN of the Entity to which the Subscriber is linked 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 Entity and that it is active.

If it is necessary to regularize payments or documentation, the Applicant's (and Subscriber's) 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. 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 face-to-face identification of the Applicant (and Subscriber).

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

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 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 latter 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 on 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 of the Entity to which it is linked contained in the certificate); data necessary for the use of the certificate in HSM Centralized by the Subscriber; signature of the Decision Operator of the RA who has taken 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.
- Current version of the Use of Certificate Centralized handbook.

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.

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 moment 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 Company/Entity Binding complies with the Thomas Signe S.A.S. CPS for issuing certificates, except that the ETSI EN 319 412-3 standard is not applicable for these certificates.

Certificates for Company/Entity Binding have a validity period of up to 2 years (730 days).

7.1.2 CERTIFICATE EXTENSIONS

The following table specifies the extensions of the Company/Entity Binding Certificates.

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 1.3.6.1.4.1.51362.0.2.1.2.x [1] URI of CPS: http://thsigne.com/cps
Subject Alternative Name		rfc822Name: *e-mail address of Subscriber*
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)
CRL Distribution Points	-	URI of CRL: http://crl-co.thsigne.com/ecd_thomas_signe_colombia.crl

[1] Centralized HSM: x=3

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 an Enterprise/Entity Binding Certificate (Certificate Subscriber).

DN attribute	Description	Value
Country Name (C)	Country	*Two-letter code according to ISO 3166-1 of the country of the Entity* [2] Default: CO
State or Province Name (ST)	State/Province	*Department of the Entity*[3]
Locality Name (L)	Location	*Municipality of the Entity*[2]
Street Address (STREET)	Address	*Address of the Entity* [2]
Organization Identifier (2.5.4.97)	Organization Identifier	*Tax Identification Number of the Entity* (in Colombia: NIT) [2]
Organization Name (O)	Organization Name	*Name or corporate name of the Entity* [2]
Organizational Unit Name (OU)	Organizational Unit	*Area of the Subscriber in the Entity or type of relationship of the Subscriber with the Entity* [2]
Title	Title	*Position, title or role of the Subscriber in the Entity* [2]
Serial Number	Serial Number	*DocType - DocNum* [1] *DocType: Type of identity document of the Subscriber, equal to the two-letter code according to ISO 3166-1 of the country issuing the document (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 *DocNum: ID card number of the Subscriber*
Surname (SN)	Surname	*Last Name of Subscriber*[2]

Given Name	First Name	*First Name of Subscriber* [2]
Common Name (CN)	Name	*Full name (first and last name) of Subscriber*[2]

[2] Encoded in PrintableString

[3] Encoded in UTF8String

7.1.5 NAME RESTRICTIONS

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

Certificates for Company/Entity Binding 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

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.

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

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 IMITATION 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

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

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-F04 Certificate Request Form for Binding to Company/Entity THS-CO-AC-AC-CPS-01-F17 Application and Acceptance of Digital Certification Service Provision

(Legal Representative)

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

THS-CO-AC-AC-CPS-01-F11 Authorization Request Certificate for Binding to Company/Entity THS-CO-AC-AC-CPS-01-F15 Reading protocol for identity verification videoconference THS-CO-AC-AC-CPS-01-F20 Digital Certificates Business Proposal

11 RECORDS

ID	SUPPORT	RESPONSIBLE	FILE	RETENTION TIME
Completed Company/Entity Binding Certificate Application Forms	TI	Registry Operator	SAR Platform	7 years or according to applicable regulations
Digital Certificates Signed Commercial Proposals - Company/Entity Binding	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