

Digital Certification Entity



Certificate Policy for Natural Person


Document Information


Name	CERTIFICATE POLICY FOR NATURAL PERSON
Prepared by	THOMAS SIGNE S.A.S.
Country	COLOMBIA
Version	2.7
Date	AUGUST, 2023
Document Type	PUBLIC
Code	THS-CO-AC-PC-PER-04


Document version

Version	Date	Description
1.0	01/28/2018	Document preparation
1.1	05/20/2018	The Obligations section is added. The Certificate Operating Procedure is detailed.
1.2	05/24/2018	The section on Circumstances for revocation of a certificate has been added.
1.3	06/08/2018	Sections are added for applicable formats and records
1.4	11/02/2018	The reference to THS-PR-GRAL-02-F01 Document Structure v1.0 is removed from the footer. v1.0 document structure. The "INTRODUCTION" section is eliminated.
1.5	01/22/2019	The possibility is added for the OR to optionally verify the Applicant 's identity in person, instead of by videoconference. Minor adjustments.
1.6	05/09/2019	Integration with the Group's management system. Change of document name from THS-PC-PN-01 to THS CO-POL-PER- AC-04.

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


	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 3 of 21
1.7	09/18/2019	<p>Adjustment of the coding according to GSIGNE-GRAL-PR-01 Control of Documented Information Ed 2.1.</p> <p>In the review of the certificate request, in the validation of the Applicant's identity document, the query against an online database is eliminated.</p> <p>It is indicated that the issuance and installation of the certificate in the Centralized HSM are automatically performed by the RA upon receipt of the certificate request in PKCS #10 format, without the intervention of an OR (change implemented in January 2019).</p> <p>In the Serial Number attribute of the DN of the certificates, the format of the Subscriber's identification document type is indicated.</p> <p>The Formats and Records sections are added.</p> <p>In the subscription contract (Annex II), the Signature of the Applicant is changed to the Signature of the Subscriber (the Applicant and the Subscriber are the same Natural Person). Minor adjustments.</p>
1.8	11/29/2019	<p>Change of the current account number to place the deposit of the respective amount for each service.</p> <p>Added a format and a register for identity verification videoconferences.</p> <p>Minor adjustments.</p>
2.0	01/31/2020	<p>General review of the content of the CPS based on the applicable legislation and regulations and the content of the Management System documentation by the multidisciplinary work team.</p> <p>Change of the name of the document from "Natural Person Certification Policy" to "Natural Person Certificate Policy."</p> <p>Changes in the organization of the content of the document to follow the recommendations of the RFC 3647 standard.</p> <p>Elimination of the current account number for the deposit of the respective amount for each service (to be indicated in the Commercial Proposal).</p>
2.1	06/19/2020	Minor adjustments.
2.2	11/06/2020	Minor adjustments.
2.3	06/24/2021	<p>Change of image of Thomas Signe.</p> <p>Change of the name of the document from "Certificate Policy for Natural Person" to "Certificate Policy for Natural Person".</p> <p>Changes in certificate issuance fees.</p> <p>Minor adjustments.</p>
2.4	11/19/2021	Changes in the certificate request processing and certificate issuance, to ensure independence and impartiality between the review and certification

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 4 of 21
		<p>decision (certificate issuance) 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 adjustments.</p>
2.5	07/08/2022	<p>Adaptation to the new version of CEA-3.0-07</p> <p>Added issuerAltName to the certificate profile.</p> <p>Updated revocation methods.</p> <p>Changed the PQRS procedure in line with the new CEA version.</p>
2.6	20/01/2023	<p>Corrections and minor changes.</p>
2.7	16/08/2023	<p>Fees Update</p>


	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 5 of 21

CONTENTS


1	INTRODUCTION	8
1.1	PRESENTATION OF THE DOCUMENT	8
1.2	DOCUMENT NAME AND IDENTIFICATION	8
1.3	THOMAS SIGNE S.A.S. PKI PARTICIPANTS	9
1.3.1	THOMAS SIGNE S.A.S. PKI CERTIFICATE HIERARCHY	9
1.3.2	THOMAS SIGNE ROOT.....	9
1.3.3	DCE THOMAS SIGNE S.A.S. (DCE THOMAS SIGNE COLOMBIA)	9
1.3.4	APPLICANT.....	9
1.3.5	SUBSCRIBER	9
1.3.6	TRUSTING THIRD PARTY	9
1.4	TYPES OF SUPPORT AND USES OF CERTIFICATES	9
1.4.1	CENTRALIZED HSM SUPPORT	9
1.4.2	APPROPRIATE USES OF CERTIFICATES	10
1.4.3	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.....	10
2	RESPONSIBILITIES REGARDING REPOSITORIES AND PUBLICATION OF INFORMATION	11
3	IDENTIFICATION AND AUTHENTICATION	11
3.1	NAMES	11
3.2	INITIAL IDENTITY VALIDATION.....	12
3.2.1	METHOD OF PROOF OF POSSESSION OF THE PRIVATE KEY	12
3.2.2	AUTHENTICATION OF THE IDENTITY OF COMPANY OR ENTITY.....	12
3.2.3	AUTHENTICATION OF THE IDENTITY OF AN INDIVIDUAL NATURAL PERSON.....	12
3.2.4	UNVERIFIED SUBSCRIBER AND APPLICANT INFORMATION.....	12
3.3	IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUESTS WITH CHANGE OF PASSWORDS CHANGE OF KEYS	12
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS	12
4	OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF THE CERTIFICATES.....	13
4.1	CERTIFICATE APPLICATION	13
4.1.1	WHO CAN APPLY FOR A CERTIFICATE.....	13
4.1.2	MARKETING.....	13
4.1.3	CONTRACTING AND PAYMENT.....	13
4.1.4	APPLICATION	14
4.2	PROCESSING OF CERTIFICATE APPLICATIONS.....	14
4.2.1	REVIEW.....	14
4.2.2	DECISION.....	15
4.3	ISSUANCE OF CERTIFICATES	15
4.3.1	DCE ACTIONS DURING ISSUANCE OF CERTIFICATES	15
4.3.2	NOTIFICATION TO THE APPLICANT AND SUBSCRIBER BY DCE OF CERTIFICATE ISSUANCE.....	15
4.4	ACCEPTANCE OF THE CERTIFICATE.....	16
4.4.1	FORM IN WHICH THE CERTIFICATE IS ACCEPTED	16
4.4.2	PUBLICATION OF THE CERTIFICATE BY DCE.....	16
4.4.3	NOTIFICATION OF THE ISSUANCE OF THE CERTIFICATE BY DCETO OTHER ENTITIES.....	16
4.5	USES OF KEYS AND CERTIFICATE	16
4.6	CERTIFICATE RENEWAL WITHOUT CHANGE OF KEYS.....	16

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 6 of 21

4.7	CERTIFICATE RENEWAL WITH KEY CHANGE.....	16
4.8	CERTIFICATE MODIFICATION	16
4.9	CERTIFICATE REVOCATION AND SUSPENSION	16
4.10	CERTIFICATE STATUS INFORMATION SERVICES	16
4.11	SUBSCRIPTION TERMINATION	17
4.12	KEY ESCROW AND RECOVERY	17
5	PHYSICAL, FACILITY, MANAGEMENT AND OPERATIONAL	17
6	SECURITY CONTROLS	17
7	CERTIFICATE PROFILE, CRL AND OCSP	17
7.1	CERTIFICATE PROFILE	17
7.1.1	CERTIFICATE FORMAT AND VALIDITY PERIOD	17
7.1.2	CERTIFICATE EXTENSIONS	17
7.1.3	OBJECT IDENTIFIERS (OID) OF ALGORITHMS	18
7.1.4	NAME FORMATS	18
7.1.5	NAME RESTRICTIONS	19
7.1.6	CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)	19
7.1.7	USE OF THE EXTENSION POLICY CONSTRAINTS	19
7.1.8	SYNTAX AND SEMANTICS OF POLICY QUALIFIERS	19
7.1.9	SEMANTIC TREATMENT FOR THE CERTIFICATE POLICY EXTENSION	19
7.2	CRL PROFILE	19
7.3	OCSP PROFILE	19
8	COMPLIANCE AUDIT AND OTHER CONTROLS	19
9	OTHER LEGAL AND COMMERCIAL AFFAIRS	20
9.1	FEEES	20
9.1.1	CERTIFICATE ISSUANCE FEES	20
9.1.2	CERTIFICATE ACCESS FEES	20
9.1.3	FEES FOR REVOCATION OR ACCESS TO STATUS INFORMATION	20
9.1.4	FEES FOR OTHER SERVICES	20
9.1.5	REFUND POLICY	20
9.2	FINANCIAL RESPONSIBILITIES	20
9.2.1	INSURANCE COVERAGE	20
9.3	CONFIDENTIALITY OF INFORMATION	21
9.4	DATA PROTECTION POLICY	21
9.5	INTELLECTUAL PROPERTY RIGHTS	21
9.6	OBLIGATIONS	21
9.6.1	OBLIGATIONS OF DCE	21
9.6.2	OBLIGATIONS OF SUPPLIERS	21
9.6.3	OBLIGATIONS OF APPLICANTS	21
9.6.4	OBLIGATIONS OF SUBSCRIBERS	21
9.6.5	OBLIGATIONS OF RELYING ON THIRD PARTIES	21
9.7	RESPONSIBILITIES	21
9.7.1	DCE'S RESPONSIBILITIES	21
9.7.2	SUBSCRIBER'S RESPONSIBILITIES	21
9.8	LIMITATION OF LIABILITY	21

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 7 of 21

9.8	LIMITATION OF LIABILITY	21
9.9	INDEMNITIES.....	22
9.9.1	INDEMNITIES FOR DAMAGES CAUSED BY DCE.....	22
9.9.2	COMPENSATION FOR DAMAGES CAUSED BY CLAIMANTS, BY SUBSCRIBERS AND BY THIRD PARTIES WHO TRUST	22
9.10	PERIOD OF VALIDITY	22
9.10.1	TERM	22
9.10.2	REPLACEMENT AND REPEAL OF THE CPS AND CP'S	22
9.10.3	EFFECTS OF TERMINATION	22
9.11	PQR	22
9.12	CHANGES IN CPS AND CP.....	22
9.13	CLAIMS AND DISPUTE RESOLUTION	22
9.14	APPLICABLE LAW	22
9.15	COMPLIANCE WITH APPLICABLE LAW.....	22
9.16	OTHER PROVISIONS.....	23
9.16.1	SUBSCRIPTION AGREEMENT	23
9.16.2	FULL ACCEPTANCE CLAUSE	23
9.16.3	INDEPENDENCE	23
9.17	OTHER PROVISIONS.....	23
10	FORMATS	23
11	RECORDS.....	23

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 8 of 21

1 INTRODUCTION

1.1 PRESENTATION OF THE DOCUMENT

This document constitutes the Certificate Policy (CP) for Natural Persons 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.

Certificates for Natural Persons issued by Thomas Signe S.A.S. are certificates that allow the Subscriber to identify and sign as a natural person not linked to any company or entity.

This CP establishes the requirements of the Certificates for Natural Persons issued by Thomas Signe S.A.S., following the RFC 3647 standard "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", and in accordance with 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, Certificates for Natural Persons issued by Thomas Signe S.A.S. are governed by the practices established in the Certification Practice Statement (CPS) for the issuance of certificates of Thomas Signe S.A.S. This CPS is published in the same web page of Thomas Signe S.A.S. as this document (see section 1.2).

This document is of a public nature and is intended for all natural and legal persons, Applicants, Subscribers, Third Parties and the general public.

In the event that vulnerabilities are detected, or the technical standards or infrastructure indicated in this CP are no longer valid, Thomas Signe S.A.S. will be responsible for informing ONAC of this fact, in order to proceed with the respective update.

1.2 DOCUMENT NAME AND IDENTIFICATION

The identification data of the present document are specified in the initial table *Identification of the document*.

Additionally, this document is identified with the following OIDs, contained in the X.509 v3 Certificate Policies extension of the Public Function Certificates issued by Thomas Signe S.A.S. in the indicated media types.

OID OF THE CP OF CERTIFICATES FOR NATURAL PERSON 1.3.6.1.4.1.51362.0.2.1.1	
1.3.6.1.4.1.51362.0.2.1.1.3	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.

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 9 of 21

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 to DCE Thomas Signe S.A.S. the issuance of a Certificate for Natural Person.

In this CP, 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 Natural Person 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 Thomas Signe S.A.S..

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

In this CP, Subscriber is a natural person not related to any company or entity.

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 Natural Person issued by DCE Thomas Signe S.A.S.

1.4 TYPES OF SUPPORT AND USES OF CERTIFICATES

1.4.1 CENTRALIZED HSM SUPPORT

The issuance of Certificates for Natural Person 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 Natural Person 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 of the cryptographic module


Access to the private key of a Certificate for Natural Person issued in this cryptographic device is made 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 cellular phone each time he tries to access the private key. This username and two passwords and this code constitute, therefore, the activation data of the private key.

Certificates for Natural Person issued in HSM Centralized are identified by the OID (1.3.6.1.4.1.1.51362.0.2.1.1.1.3) in the X.509 v3 Certificate Policies extension.

1.4.2 APPROPRIATE USES OF CERTIFICATES

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

Certificates for Natural Persons can be used for the following purposes:

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 10 of 21

- Integrity of the signed document.
- Non-repudiation of origin.
- Identification of the Subscriber.

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

1.4.3 UNAUTHORIZED USES OF CERTIFICATES

It is not allowed to use other than what is established in this CP and the 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
	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. 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
TIN	Tax Identification Number
OCSP	Online Certificate Status Protocol
ONAC	National Accreditation Organization of Colombia
RO	Registry Operator
CP	Certificate Policy
PKCS	Public-Key Cryptography Standards. Public-key cryptography standards devised and published by RSA Laboratories.
PKI	Public Key Infrastructure
PQR	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

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 11 of 21

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.
- SRA** Signe Registration Authority
- SHA** Secure Hash Algorithm

2 RESPONSIBILITIES REGARDING REPOSITORIES AND PUBLICATION OF INFORMATION

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMES

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

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD OF PROOF OF POSSESSION OF THE PRIVATE KEY

When a certificate is issued in Centralized HSM, the private key is generated in the HSM at the moment prior to the issuance of the certificate, through a procedure that guarantees its confidentiality and its binding to the Applicant.

3.2.2 AUTHENTICATION OF THE IDENTITY OF COMPANY OR ENTITY

It is not applicable to certificates for Natural Persons.

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

In addition, RA will verify the Subscriber 's full residential address data entered in the certificate application form by requesting an official document showing a current full address of the Subscriber, e.g. a Certificate of Residence for Natural Persons, issued in Colombia (by default) or in another country a maximum of 30 days before.


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, presuming the good faith of the information provided by the Subscriber:

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

3.3 IDENTIFICATION AND AUTHENTICATION FOR RENEWAL REQUESTS

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 12 of 21

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 Subscribers and Applicants use 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/her user and password to access the Centralized HSM, and a code that he/she will receive on their 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 Natural Person.

4.1.2 MARKETING

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

- Visiting the web site www.thomas-signe.co
- Via informative e-mail from the following address comercial@thomas-signe.co
- Dealing directly with commercial agents.

By any of these channels, you will be provided with information about the process, requirements, fees and other related information.

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

- 1) The type of certificate required (Certificate for Natural Person).
- 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 Applicant's email account, which will be associated to the digital certificate and through which DCE will send official notifications and communications.

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


4.1.3 CONTRACTING AND PAYMENT

To proceed, the Applicant (and Subscriber) shall:

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

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

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

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 13 of 21

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

4.1.4 APPLICATION

To request the issuance of a digital certificate, the Applicant (and Subscriber) may enter the SAR platform and correctly complete the information in the certificate request form (see Annex I). In addition, within the SAR platform, he/she will proceed to attach the documents indicated below:

- Identity document of the Applicant, scanned on both sides: Citizenship Card, Alien Registration Card or Passport; issued in Colombia (by default) or in another country (equivalent document).
- Official document showing a complete current address of the Applicant (for example, a Certificate of Residence for Natural Persons); issued in Colombia (by default) or in another country a maximum of 30 days before.
- Proof of payment of the certificate fee indicated in the Commercial Proposal or in the Service Rendering Agreement, in the applicable cases.
- Signed Subscription Agreement.

Alternatively, the Applicant (and 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 application form and attach the requested documents in the SAR platform.

4.2 PROCESSING OF CERTIFICATE APPLICATIONS

4.2.1 REVIEW

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

- They are complete and legible.
- They look legitimate.
- Where applicable, they were current when attached on the SAR platform.

-The data they contain regarding the Subscriber, 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 Business Proposal.

If payments or documentation need to be regularized, the Applicant's (and Subscriber's) stated email 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 performed 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

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 14 of 21

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 Applicant (and Subscriber) that the certificate has been issued and has been installed in the HSM.

In addition, the RA sends an email to the Applicant (and 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 DCE Thomas Signe S.A.S.; information about the content of the purchased certificate (type and support of the certificate, dates of issuance and expiration of the certificate, data of the Subscriber contained in the certificate) ; data necessary for the use of the certificate in Centralized HSM by the Subscriber ; signature of the RA Decision Operator who has made the decision to issue the certificate.
- Link to the web page where the CPS for issuing Thomas Signe S.A.S. certificates and the present CP are published.
- Manual of use of the certificate in HSM Centralized in its current version.


4.4 ACCEPTANCE OF THE CERTIFICATE

4.4.1 FORM IN WHICH THE CERTIFICATE IS ACCEPTEDTE 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.

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 15 of 21

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

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

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

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

4.10 CERTIFICATE STATUS INFORMATION SERVICES

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

4.11 SUBSCRIPTION TERMINATION

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

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 16 of 21

7 CERTIFICATE PROFILE, CRL AND OCSP

7.1 CERTIFICATE PROFILE

7.1.1 FORMAT AND VALIDITY PERIOD

The format of the certificates for Natural Persons follows the Thomas Signe S.A.S. CPS for the issuance of certificates, except that the ETSI EN 319 412 -3 standard is not applicable for these certificates

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

7.1.2 CERTIFICATE EXTENSIONS

The following table specifies the extensions of the Certificates for Natural Persons.

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 1.3.6.1.4.1.51362.0.2.1.1.x ¹ URI de la CPS: http://thsigne.com/
Subject Alternative Name		rfc822Name: <i>Subscriber's email address</i>

¹ HSM Centralized: x=3


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

7.1.3 OBJECT IDENTIFIERS (OID) OF ALGORITHMS

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

7.1.4 NAME FORMATS

The following table specifies the corresponding attributes of the DN of the holder of a Certificate for

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 17 of 21

Natural Person (Subscriber of the certificate).

DN Attribute	Description	Value
Country Name (C)	Country	<i>Two-letter capital letter code according to ISO 3166-1 of the country where Subscriber resides¹</i> Default: CO
State or Province Name (ST)	State/Province	<i>Department where the Subscriber resides²</i>
Locality Name (L)	Location	<i>Municipality where the Subscriber resides²</i>
Street Address (STREET)	Address	<i>Address where Subscriber resides²</i>
Serial Number (serialNumber)	Serial Number	<i>TipoDoc-NumDoc</i> 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 (by default: CO) followed by CC (Cédula de Ciudadanía or equivalent), CE (Cédula de Extranjería or equivalent) or PA (Pasaporte); in Colombia: COCC, COCE or COPA.

¹ Encoded in PrintableString

² UTF8String Encoded

		<i>NumDoc: Subscriber's ID Number</i>
Surname (SN)	Last Name	<i>Last Name of Subscriber²</i>
Given Name (givenName)	Name	<i>Suscriptor Name²</i>
Common Name (CN)	Name	<i>Full name (first and last) of Subscriber²</i>

7.1.5 NAME RESTRICTIONS

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

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIERS (OID)


The OIDs of the Certificate Policy for Natural Persons 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 Natural Persons 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.

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 18 of 21

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

 THOMAS SIGNE	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 19 of 21

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.

9.7 RESPONSIBILITIES

9.7.1 DCE'S RESPONSIBILITIES

As specified in the 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

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 20 of 21

9.9.1 INDEMNITIES FOR DAMAGES CAUSED BY

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 PQR

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 COMPLIANCE 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 current Subscription Agreement for the certificate issuance service is published on the following web page:

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

The same contract model is used for all types of certificates. In each contract, 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.

	Certificate Policy for Natural Person	Version 2.7
	Code: THS-CO-AC-PC-PER-04	Page 21 of 21

Due to the fact that each contract is filled in with the Subscriber's identification data, the document is classified as CONFIDENTIAL, despite the fact that the contract 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 is declared, partially or totally, null and void or illegal, this shall not affect the rest of the document.

9.17 OTHER PROVISIONS

Not considered.

10 FORMATS

THS-CO-AC-CPS-01-F03 Certificate Request Form for Natural Person

THS-CO-AC-CPS-01-F15 Read protocol for identity verification videoconferencing

THS-CO-AC-CPS-01-F17 Application and Acceptance of Digital Certification Service Provision (Legal Representative) v1.0

THS-CO-AC-CPS-01-F18 Application and Acceptance of Digital Certification Service Provision (Subscriber) v1.0

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

11 RECORDS

ID	SUPPORT	RESPONSIBLE	FILE	RETENTION TIME
Completed Certificate Application Forms for Natural Persons	TI	Registry Operator	SAR Platform	7 years or according to applicable regulations

Signed business proposals for Digital Certificates - Natural Person	TI	Sales Manager	SAR Platform	7 years or according to applicable regulations
Signed Subscription Contracts for Issuance of Certificates	TI	Registry Operator	SAR Platform	7 years or according to applicable regulations
Recorded identity verification videoconferences	TI	Registry Operator	RA Platform	7 years or according to applicable regulations