VinCAsign Certification Practice Statement

16/11/2020: v2r11

General information

Control of the document

Security classification:	Public
Destination entity:	víntegris SEGURIDAD DE LA INFORMACIÓN
Version:	2.11
Date published:	16/11/2020
File:	Vintegris CPS-EN v2r11
Format:	Office 365
Authors:	Víntegris

Version control

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	AC, FA, NA	26/02/2016
1.1	Sección 5.8	Se incluye comunicación al Ministerio en caso de cese.	AC	03/05/2016
1.2	Sección 1.2 y 1.4	Inclusión de los certificados de sello de empresa. Se eliminan referencias a la ley 11/2007 por las de la ley 40/2015	AC	20/04/2017
	Todo el documento	Inclusión aspectos REIDAS. Se cambia la denominación de certificados reconocidos por certificados cualificados. Se cambia la denominación de DSCF por DCCF.	AC	20/04/2017

2.0	1.3.1.3	Se incluye la referencia al producto nebulaCERT	SSF	05/05/2017
	1.3.1.4	Se incluye la referencia del cese de la jerarquía anterior	SSF	05/05/2017
2.1	Sección 1.3	Ampliación de información sobre la firma de CRL y OCSP Re-capitulación.	SSF	11/05/2017
	Sección 5.8	Modificación fondos contingencia.	SSF	11/05/2017
2.2	4.9.3.	Procedimientos de solicitud de revocación. Se incluye método email en web de ayuda	SSF	22/05/2017
2.2	4.9.7	Se incluye que los estados de revocación permanecen en las CRL indefinidamente	SSF	30/05/2017
2.2	9.6.10	Ampliación tratamiento de quejas y disputas	SSF	30/05/2016
2.3		Incorporación certificado de representante de entidad sin personalidad jurídica	AC	30/08/2017
2.4	1.3.1.3 6.1.1	Indicación de la nueva CA subordinada	AC	09/10/2017
	1.3.1.6	Nuevos servicios de OCSP		
	4.9.6 4.9.9 4.9.11	Nuevas CRL y OCSP		
	En general	Se cambian las referencias a la Ley de Firma Electrónica por el REIDAS.		
2.5	2.5	Indicación del hardware criptográfico usado	AC	14/02/2018
	6.2.5	Redacción nueva que incluye la descripción de la creación de las claves privadas de los	AC	14/02/2018

		usuarios en el hardware criptográfico centralizado.		
	6.8	Se describe qué hardware criptográfico es usado en cada caso.	AC	14/02/2018
2.6	6.2.7.2	Se aclaran las condiciones de importación de claves	NA	08/03/2018
2.7		Revisión anual DPC	AC VH	14/05/2018 19/05/2018
		Eliminación vinCAsign nebulaSUITE Authority	AC	17/07/2018
		Cambio referencias al RGPD	FA	20/07/2018
		Revisiones menores	AC	18/10/2018
2.8		Inclusión nuevos tipos de certificados	AC	16/01/2019
		Actualización referencias ETSI	GA	06/02/2019
		Revisiones por inclusión certificados con seudónimo	AC/FA	27/02/2019
		Cambio de ubicación de las definiciones y acrónimos para adecuación a RFC 3647	AC	27/02/2019
	3.5; 4.5.3.1; 4.9.7; 9.3.2; 9.6.5.2	Se modifican los aspectos relacionados con la suspensión	VH/AC	12/03/2019
	4.7.3	Modificación sobre la renovación de certificados	VH	12/03/2019
	1.3.1	Modificación datos OCSP y otros	VH	12/03/2019
	4.9	Modificaciones URLs	VH	12/03/2019
	6.9	Modificaciones sobre fuentes de tiempo	VH	12/03/2019
	4.9	Se eliminan estos apartados relacionados con la suspensión	VH/AC	13/03/2019
	1.4.1; 3.1.1	Cambio denominación “1 uso” por “efímeros”	AC	14/03/2019

	5.4.8	Cambio en la temporalidad de los análisis de vulnerabilidades	VH	15/3/2019
	4.9.9	Creación de la última CRL	AC	18/03/2019
2.9		Inclusión tipos de certificados de persona física sin vinculación (suscriptores individuales).	AC/FA	20/06/2019
		Inclusión de tipos de certificados no cualificados para suscriptores individuales.	AC/FA	05/07/2019
		Inclusión del uso de la video-identificación para certificados no cualificados	AC	10/07/2019
		Inclusión de tipos de certificados Representante AGID	VH	17/09/2019
2.10	1.4.1.4; 1.4.1.6; 1.4.1.8; 1.4.1.10; 1.4.1.12; 1.4.1.14; 1.4.1.16; 1.4.1.18; 1.4.1.20; 1.4.1.22; 1.4.1.23; 1.4.1.26; 1.4.1.32;	Amplitud de la gestión de los certificados a la gestión descentralizada (software y en Tarjeta QSCD).	VH	20/04/2020
		Inclusión de certificados de autenticacion web	VH	30/04/2020
	1.2.1; 2.2; 4.9.9;	Modificaciones Cabforum	VH	03/05/2020

		Revision anual de la DPC	VH	05/06/2020
2.11		inclusión subordinada nebulaSUITE5 Inclusión de nueva regulación normativa y eliminación de la normativa derogada	VH	16/11/2020

Contents

1. Introduction

1.1. Presentation

This document sets out the electronic signature practices of vinCAsign, the Víntegris Certification Authority.

The following certificates are issued:

- Corporate certificates for linked natural person
- Corporate certificates for natural person representative
- Corporate certificates for individuals Spanish Public Administration Employees
- Corporate organization seal certificates for Spanish public administration
- Corporate certificates for company seals
- Electronic time stamp certificates
- Individual certificates for natural persons
- Certificates for Electronic Sites
- SSL Certificates

Regarding the media:

- Certificates issued on qualified electronic signature and electronic stamping device (QSCD)
- Certificates issued in software

Regarding the representation:

- Certificates of representative of legal person
- Certificates of representative of an entity without legal personality

Regarding the time of validity:

- Certificates with temporary validity up to 3 years
- Certificates with ephemeral validity

As regards its function:

- Certificates to identify natural or legal persons
- Certificates to identify objects (IoT)
- Certificates with a pseudonym
- Certificates to authenticate websites

As regards its qualification:

- Qualified certificates, in accordance with Regulation (EU) EIDAS[1] .
- Unqualified certificates (non qualified)

1.2. Document name and ID

Name:	Certification Practice Statement (CPS)
Description:	vinCAsign Certification Practice Statement
Version:	2r11
Date of Issue:	16/11/2020
Location	www.vincasign.net
OID	1.3.6.1.4.1.**47155**

1.2.1. Certificate IDs

VinCAsign has given each of its certification policies an object ID (OID), so they may be identified by the applications.

OID	Type of certificate
1.3.6.1.4.1.**47155.1.1.1**	Corporate Certificates of a linked Natural Person, on QSCD
1.3.6.1.4.1.**47155.1.1.2**	Corporate Certificates of a linked Natural Person, on Software
1.3.6.1.4.1.**47155.1.1.51**	Corporate Certificates and ephemeral of a linked Natural Person, on QSCD
1.3.6.1.4.1.**47155.1.1.52**	Corporate Certificates and ephemeral of a linked Natural Person, on Software

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

OID	Type of certificate
1.3.6.1.4.1.**47155.1.2.1**	Certificates of representative of legal person, on QSCD
1.3.6.1.4.1.**47155.1.2.2**	Certificates of representative of legal person, on Software
1.3.6.1.4.1.**47155.1.2.51**	Ephemeral Certificates of representative of legal person, on QSCD
1.3.6.1.4.1.**47155.1.2.52**	Ephemeral Certificates of representative of legal person, on Software
1.3.6.1.4.1.**47155.1.11.1**	Certificates of representative of legal person, on QSCD. Digital Italy Agency (AgID) recommendations.
1.3.6.1.4.1.**47155.1.11.2**	Certificates of representative of legal person, on Software. Digital Italy Agency (AgID) recommendations.

OID	Type of certificate
1.3.6.1.4.1.**47155.1.2.11**	Certificates of representative of an entity without legal personality, on QSCD
1.3.6.1.4.1.**47155.1.2.12**	Certificates of representative of an entity without legal personality, on Software
1.3.6.1.4.1.**47155.1.2.151**	Ephemeral Certificates of representative of an entity without legal personality, on QSCD
1.3.6.1.4.1.**47155.1.2.152**	Ephemeral Certificates of representative of an entity without legal personality, on Software

OID	Type of certificate
1.3.6.1.4.1.**47155.1.4.1**	Natural Person. Public Employee - High Level
1.3.6.1.4.1.**47155.1.4.2**	Natural Person. Public Employee - Medium Level
1.3.6.1.4.1.**47155.1.4.11**	Natural Person. Public Employee with a pseudonym - High Level
1.3.6.1.4.1.**47155.1.4.21**	Natural Person. Public Employee with a pseudonym - Medium Level

OID	Type of certificate
1.3.6.1.4.1.**47155.1.5.1**	Public organism seal – High Level
1.3.6.1.4.1.**47155.1.5.2**	Public organism seal - Medium Level

OID	Type of certificate
1.3.6.1.4.1.**47155.1.6.1**	corporate seal, on QSCD
1.3.6.1.4.1.**47155.1.6.2**	corporate seal, on Software
1.3.6.1.4.1.**47155.1.6.51**	Ephemeral corporate seal, on QSCD
1.3.6.1.4.1.**47155.1.6.52**	Ephemeral corporate seal, on Software

OID	Type of certificate
1.3.6.1.4.1.**47155.1.7.2**	corporate seal for IoT (Internet of things)

OID	Type of certificate
1.3.6.1.4.1.**47155.1.9.1**	Corporate Electronic Time Stamp Certificates

OID	Type of certificate
1.3.6.1.4.1.**47155.1.10.1**	Natural Person, on QSCD
1.3.6.1.4.1.**47155.1.10.2**	Natural Person, on Software
1.3.6.1.4.1.**47155.1.10.51**	Ephemerals and Natural Person, on QSCD
1.3.6.1.4.1.**47155.1.10.52**	Ephemerals and Natural Person, on Software

OID	Type of certificate
1.3.6.1.4.1.**47155.1.110.1**	Natural Person and non qualified, on QSCD
1.3.6.1.4.1.**47155.1.110.2**	Natural Person and non qualified, on Software
1.3.6.1.4.1.**47155.1.110.51**	Ephemerals, non qualified and Natural Person, on QSCD
1.3.6.1.4.1.**47155.1.110.52**	Ephemerals, non qualified, and Natural Person, on Software

OID	Type of certificate
1.3.6.1.4.1.47155.1.13.1	Electronic Site Certificate
1.3.6.1.4.1.47155.1.14.1	SSL OV Certificate
1.3.6.1.4.1.47155.1.14.2	SSL EV Certificate

The structure of this document is based on the specifications of standard “RFC3647 - Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework “, created by the working group PKIX of the IETF.

In the event of any contradictions between this Certification Practice Statement and other practice and procedure documents, the information contained in this Practice Statement shall prevail.

Furthermore, Vintegris respects and complies with the current version of the CA-Browser Forum document "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates". The latest version is published at https://wwww.cabforum.org/.

Web authentication certificates issued under this CPS conform to the current version of the "EV SSL Certificate Guidelines" published at https://wwww.cabforum.org/.

In the case of incompatibility between any indication included in the CPS and the requirements of the CAB Forum, the latter shall prevail.

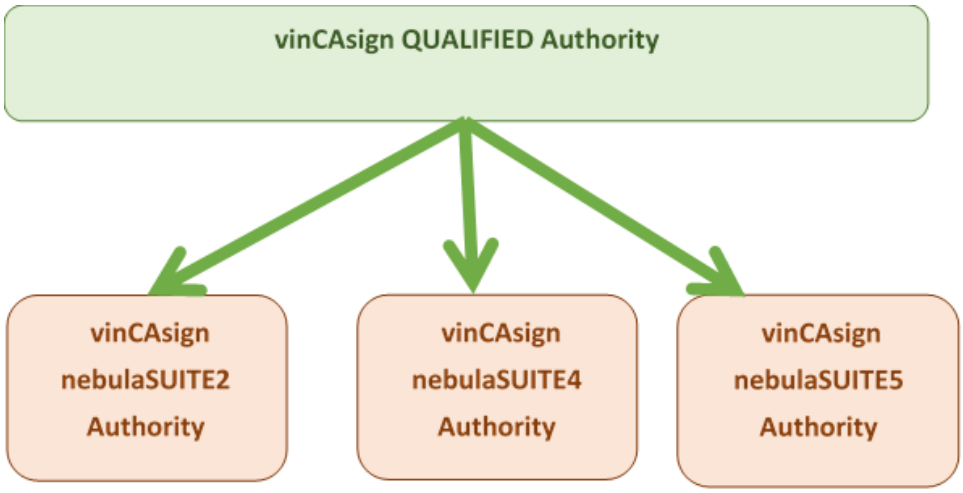
1.3. Participants in certification services

1.3.1. Certification services provider

The certification services provider is the natural or legal person that issues and manages certificates for end-entities by means of a Certification Authority, or that provides other services related to electronic signatures.

Víntegris SL is a certification service provider, acting in accordance with the provisions of Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, and the ETSI technical standards applicable to the issuance and management of qualified certificates, mainly ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2, in order to facilitate compliance with legal requirements and international recognition of its services.

For the provision of its certification services, Víntegris SL has established a hierarchy of certification authorities named "vinCAsign":



1.3.1.1. vinCAsign Qualified Authority

This is the root certification authority in the hierarchy which issues certificates to other certification authorities and whose public key certificate has been self-confirmed.

Identification data:

CN:	vinCAsign Qualified Authority
Digital fingerprint:	3e 92 ea 16 7f 59 ea b1 60 fe 5a 7b 74 eb 79 5b c3 ec 01 73
Valid from:	Thursday, 20/04/2017
Valid to:	Sunday, 20/04/2042
RSA key length:	4096 bits

1.3.1.2. vinCAsign nebulaSUITE2 Authority

It is a **subordinate certification authority** within the hierarchy which issues certificates to final entities, and whose public key certificate has been electronically signed by the vinCAsign Qualified Authority.

Identification data:

CN:	vinCAsign nebulaSUITE2 Authority
Digital fingerprint:	0e 92 72 b3 cd a9 62 15 a8 ca 55 d7 82 2b 86 a2 7a 4e d4 66
Valid from:	Wednesday, 27/09/2017 16:20:46
Valid to:	Friday, 27/09/2030 16:20:46
RSA key length:	4096 bits

1.3.1.3. vinCAsign nebulaSUITE3 Authority

This is a **subordinate certification authority** within the hierarchy that issues **unqualified** certificates to final entities, and whose public key certificate has been digitally signed by the vinCAsign Qualified Authority.Identification data:
Identification data:

CN:	vinCAsign nebulaSUITE3 Authority
Digital fingerprint:	7D:27:4C:84:83:6D:2E:14:5A:AF:54:FC:07:12:55:2D:AA:7B:0B:BA
Valid from:	8/08/2019 11:29:50 CEST
Valid to:	8/08/2032 11:29:50 CEST
RSA key length:	4096 bits

1.3.1.4. vinCAsign nebulaSUITE4 Authority. Web authentication certificates

This is a **subordinate certification authority** within the hierarchy that issues unqualified certificates to final entities, and whose public key certificate has been digitally signed by the vinCAsign Qualified Authority. This CA also issues web authentication certificates.

Identification data:

CN:	vinCAsign nebulaSUITE4 Authority
Digital fingerprint:	67d8255c38597d23398c465654b3440a25955be0
Valid from:	Friday, May 8, 2020 13:19:48
Valid to:	Sunday, May 8, 2033 13:19:48
RSA key length:	4096 bits

1.3.1.5. vinCAsign nebulaSUITE5 Authority. Web authentication certificates

This is a subordinate certification entity intended exclusively to issue qualified certificates for the Web authentication certificates issuing service, and whose public key certificate has been digitally signed by the vinCAsign Qualified Authority.
Identification data:

CN:	vinCAsign nebulaSUITE5 Authority
Digital fingerprint:	724f627a2ca6abcb751cdc5c0f7f2e4be56f502c
Valid from:	Wednesday, November 11, 2020 16:46:15
Valid to:	Friday, November 11, 2033 16:46:15
RSA key length:	4096 bits

1.3.1.6. OCSP service vinCAsign nebulaSUITE2

The certificate of signature of the responses of the new vinCAsign OCSP services has been digitally signed by the'v**inCAsign nebulaSUITE2 Authority'**.

Identification data:

OCSP1

CN:	Servicio OCSP1 vinCAsign
Digital fingerprint:	0DF1B4AC91E58C09
Valid from:	2019-12-05 11:18:07+01:00
Valid to:	2020-12-04 11:18:07+01:00
RSA key length:	2048 bits

OCSP2

CN:	Servicio OCSP2 vinCAsign
Digital fingerprint:	101FF659DEF1CCBC
Valid from:	2019-12-05 11:20:35+01:00
Valid to:	2020-12-04 11:20:35+01:00
RSA key length:	2048 bits

1.3.1.7. OCSP service vinCAsign nebulaSUITE4

The certificate of signature of the responses of the new vinCAsign nebulaSUITE4 OCSP services has been digitally signed by the'v**inCAsign nebulaSUITE4 Authority'**.

Identification data:

OCSP1

CN:	Servicio OCSP1 vinCAsign nebulaSUITE4
Digital fingerprint:	0B8B23C195836BDC
Valid from:	2020-05-23 11:50:52+02:00
Valid to:	2021-05-23 11:50:52+02:00
RSA key length:	2048 bits

OCSP2

CN:	Servicio OCSP2 vinCAsign nebulaSUITE4
Digital fingerprint:	08DFEF048224A0B4
Valid from:	2020-05-23 12:22:36+02:00
Valid to:	2021-05-23 12:22:36+02:00
RSA key length:	2048 bits

1.3.1.8. OCSP service vinCAsign nebulaSUITE5

The certificate of signature of the responses of the new vinCAsign nebulaSUITE5 OCSP services has been digitally signed by the'v**inCAsign nebulaSUITE5 Authority'**.

Identification data:

OCSP1

CN:	Servicio OCSP1 vinCAsign nebulaSUITE5
Digital fingerprint:	4B5023603D0F01462FF67289595B809ED0A7CFB4
Valid from:	2020-11-18 13:02:31+01:00
Valid to:	2021-11-18 13:02:31+01:00
RSA key length:	2048 bits

OCSP2

CN:	Servicio OCSP1 vinCAsign nebulaSUITE5
Digital fingerprint:	FBC589DE02E17841E8D960AA637506C5114B51B2
Valid from:	2020-11-18 13:23:58+01:00
Valid to:	2021-11-18 13:23:58+01:00
RSA key length:	2048 bits

1.3.1.9. NEBULACert

Centralized certificate management platform for the following uses:

- Management of applications and certificates approvals
- Management of certificate requests
- Management of applications for renewal and revocation of certificates.

More information about NEBULACert platform at
http://www.vintegris.tech/nebulacert/

This platform uses a "nshield HSM Family" v.11.72.02 that is certified according to ISO/IEC 15408 (Common Criteria) v.3.1 EAL4+ (AVA_VAN.5) as a qualified signature or electronic seal creation device according to Regulation (EU) 910/2014.

1.3.1.10. VinCAsign 2016 hierarchy in disuse

The initial hierarchy of VinCAsign created in 2016 has been renewed by the previously described.
This hierarchy is no longer in use as of the date of release of the v2r6 version of the DPC.

1.3.1.10.1. vinCAsign ROOT Authority (CA in disuse)

It is the root certification entity of the hierarchy that issued certificates to other certification bodies, and whose public key certificate has been self-signed.
Identification data:

CN:	vinCAsign Root Authority
Digital fingerprint:	90 9e 58 84 aa 2f 36 45 78 67 79 05 24 47 79 43 66 6ª fd 1c
Valid from:	Thursday, 28/01/2016
Valid to:	Thursday, 28/01/2027
RSA key length:	4096 bits

1.3.1.10.2. vinCAsign GLOBAL Authority (subordinate CA in disuse)

It is the certification entity within the hierarchy that issued the certificates to the final entities, and whose public key certificate has been digitally signed by VinCAsign Root Authority.

Identification Data:

CN:	vinCAsign Global Authority
Digital fingerprint:	ef 29 4b 28 3b 41 5f 7c 8f 10 89 2c f4 56 e8 a6 8c 55 b7 94
Valid from:	Thursday, 28/01/2016
Valid to:	Thursday, 28/01/2022
RSA key length:	4096 bits

1.3.1.10.3. vinCAsign nebulaSUITE Authority (subordinate CA in disuse)

It is the **subordinate certification entity** within the hierarchy that issued the certificates to the final entities, and whose public key certificate has been digitally signed by vinCAsign Qualified Authority.

Identification Data:

CN:	vinCAsign nebulaSUITE Authority
Huella digital:	65 a3 33 88 e0 b9 b4 0a 6d 84 f0 c7 3a af 9c ff f5 c3 b4 0d
Válido desde:	Thursday, 20/04/2017
Válido hasta:	Saturday, 20/04/2030
Longitud de clave RSA:	4096 bits

1.3.2. Registration service

In general, the certification services provider acts as the authority that registers – RA - the identity of the certificate subscribers.

They are also registrars of the certificates subject to this CPS, because of their condition as corporate certificates, the units designated for this function by the subscribers of the certificates, such as a personnel department, since they have the authentic records of the signatories' relationship with the subscriber.

Also registerers of so-called "individual" certificates, subject to this CPS, are entities that have a contract as Registration Entities.

Subscriber registration functions are performed by delegation and according to the instructions of the certification services provider, pursuant to article 24.1 of Regulation EU 910/2014 and with the certification services provider taking full responsibility before third parties.

1.3.3. End entities

The final entities are the persons and organizations that are the destination of the services of issuing, management and use of digital certificates, for the uses of identification and electronic signature.

The end entities of the Víntegris certification services are as follows:

1. Applicants for certificates
2. Subscribers to the certification service.
3. Signers.
4. Relying parties.

1.3.3.1. Applicants for certificates

These are those individuals who, in their own name or on behalf of a third party, request the issuance of a certificate.
Depending on the certificate requested, the applicant must meet the necessary requirements for this purpose, which are set out in section 4.1 of this CPS

1.3.3.2. Subscribers to the certification service

The subscribers to the certification service are the companies, entities or organisations that acquire the services from vinCAsign for use in the corporate or organisational sphere and which are identified on the certificates.

The certification service subscriber acquires a licence for the personal use the certificate, for their own use (electronic seal certificates), or in order to facilitate certification of the identity of a specific person who is duly authorised to perform different functions within the subscriber's organisation (electronic signature certificates). In the latter case, this person is identified on the certificate as described in the following section.

The certification service subscriber is therefore the client of the certification services provider, in accordance with commercial legislation, and has the rights and obligations defined by the certification services provider, which are additional and without prejudice to the rights and obligations of the signers, as authorised and regulated by the European technical standards applicable to the issuance of qualified electronic certificates, particularly and currently ETSI EN 319 411-2, sections 5.4.2 and 6.3.4.

1.3.3.3. Signers

Signatories are natural persons who have under their exclusive control the electronic signature keys for identification and advanced or qualified electronic signature, and are normally as follows: employees, clients and other persons linked to the subscribers, on natural person certificates; the holders of powers of attorney and letters of representation, in representative certificates; or people in the service of the Public Administration, in public employee certificates.

The signers are duly authorised by the subscriber and duly identified in the certificate by means of their given name and surname and Tax ID Code valid for the jurisdiction where the certificate is issued. In general, the use of pseudonyms is not possible.

A signer's private key cannot be retrieved by the certification service provider because the identified natural or legal person has exclusive control over it.

Given the existence of certificates for uses other than electronic signatures, such as identification, we also use the more general term of "natural person identified in the certificate", while always fully complying with electronic signature legislation relating to the signer's rights and obligations.

1.3.3.4. Relying parties

The relying parties are the persons and organisations that receive electronic signatures, electronic seals and digital certificates.

Prior to being able to rely on the certificates, the relying parties or users must validate them as described in this certification practice statement and the corresponding instructions, which are available on the Certification Authority's website https://www.vincasign.net and in the informative texts issued for each type of certificate (PDS)

1.3.4. Issuing of test certificates

VinCAsign issues test certificates for review in inspection or notification processes by the Supervisor and in evaluation processes in conformity audits. These certificates issued under the VinCAsign production hierarchy include fictitious data that are described in the document vinCAsign Emisión Certificados Prueba-v1.1.pdf

1.4. Use of certificates

This section lists the uses allowed for each type of certificate, defining limits for certain uses and prohibiting certain other uses.

1.4.1. Allowed use of certificates

The permitted uses indicated in the various fields of the certificate profiles, visible on the website https://www.vincasign.net , must be taken into account.

1.4.1.1. Corporate natural person certificate, issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.1.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-N-qscd

This are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

This certificates, work with a qualified electronic signature creation device, in accordance with Annex II to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates are managed in a centralized way or issued on a cryptographic card.

These certificates guarantee the identity of the signer and their relationship with the certification service subscriber, allowing the generation of a “qualified electronic signature”; that is to say, an advanced electronic signature based on a qualified certificate that has been generated using a qualified device, for this reason, in accordance with

Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Secure email signature.
b) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    a. Electronic signature (to perform authentication)
    b. Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    b. QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
    c. The "User Notice" field describes the use of this certificate.

1.4.1.2. Corporate natural person certificate issued in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.1.2	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n

This certificates are qualified in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 2014 and comply with the technical standards identified by ETSI EN 319 411-2.
These certificates do not operate with a qualified signature creation device.

These certificates guarantee the identity of the signer and of the person indicated in the certificate and make it possible to generate an “advanced electronic signature based on a qualified electronic certificate”.

The uses of these certificates include the following:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature uses, in accordance with the agreements made between the parties or the legal rules that apply in each case.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    a. Electronic signature (to perform authentication)
    b. Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
c) In the field "Qualified Certificate Statements" the QcSSCD statement (0.4.0.1862.1.4) **does not appear**, as this certificate is not used with a qualified device.
d) The "User Notice" field describes the use of this certificate.

1.4.1.3. Corporate and ephemeral certificate of natural person issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.1.51	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-n-qscd

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical regulation identified by the reference ETSI EN 319 411-2.
These certificates, work with a qualified electronic signature creation device, in accordance with Annex II to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates are managed in a centralized way.

These certificates guarantee the identity of the signer and their relationship with the certification service subscriber, allowing the generation of a "qualified electronic signature"; that is to say, an advanced electronic signature based on a qualified certificate that has been generated using a qualified device, for this reason, in accordance with Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

These certificates are only valid for a short period of time, after which the certificate expires. This period of time shall always be less than 1 hour

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Secure email signature.
b) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:

- Electronic signature (to perform authentication)
- Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:

- QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
- QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.4. Corporate and ephemeral certificate of physical person issued on software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.1.52	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n

These certificates are qualified in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 2014 and comply with the technical standards identified by ETSI EN 319 411-2.
These certificates are managed in a centralized way.
These certificates do not operate with a qualified signature creation device.
These certificates guarantee the identity of the signer and of the person indicated in the certificate and make it possible to generate an “advanced electronic signature based on a qualified electronic certificate”.

These certificates are only valid for a short period of time, after which the certificate expires. This period of time shall always be less than 1 hour.

The uses of these certificates include the following:

d) Authentication in access control systems.
e) Secure email signature.
f) Other electronic signature uses, in accordance with the agreements made between the parties or the legal rules that apply in each case.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    a. Electronic signature (to perform authentication)
    b. Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
c) In the field "Qualified Certificate Statements" the QcSSCD statement (0.4.0.1862.1.4) **does not appear**, as this certificate is not used with a qualified device.
d) The "User Notice" field describes the use of this certificate.

1.4.1.5. Corporate certificate of a natural person representing a legal person issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-n-qscd
2.16.724.1.3.5.8	For being a certificate of representative of a legal entity, with full legal powers, sole or joint administrator of the organization, or at least with specific general powers to act in front of the Spanish Public Administration

These certificates are managed in a centralized way , or issued on a cryptographic card.

These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates work with a qualified electronic signature creation device, in accordance with Annex II to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and the entity, company or organisation described in the “O” (Organisation) field, allowing the generation of a “qualified electronic signature”; that is to say, an advanced electronic signature based on a qualified certificate that has been generated using a qualified device, for this reason, in accordance with Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.
This certificate includes a field (Description) in the Subject, indicating the public document that reliably accredits the signatory's faculties to act on behalf of the entity it represents and, if mandatory, the registration of the Registry data.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Secure email signature.
b) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents.

Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    - qCCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    - QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified electronic signature creation device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.6. Corporate representative natural person certificate issued in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.2	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n
2.16.724.1.3.5.8	For being a certificate of representative of a legal entity, with full legal powers, sole or

	joint administrator of the organization, or at least with specific general powers to act in front of the Spanish Public Administration

These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature-creation device.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and the entity, company or organisation described in the “O” (Organisation) field, allowing the generation of an “advanced electronic signature based on a qualified electronic certificate".

This certificate includes a field (Description) in the Subject, indicating the public document that reliably accredits the signatory's faculties to act on behalf of the entity it represents and, if mandatory, the registration of the Registry data.

Furthermore, the uses of corporate representative natural person certificates issued in software also include the following:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.
The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)

- Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
   - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.

c) The QcSSCD statement (0.4.0.1862.1.4) does not appear in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

d) The "User Notice" field describes the use of this certificate.

1.4.1.7. Corporate and ephemeral certificate of a natural person representing a legal entity issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.51	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-n-qscd
2.16.724.1.3.5.8	For being a certificate of representative of a legal entity, with full legal powers, sole or joint administrator of the organization, or at least with specific general powers to act in front of the Spanish Public Administration

These certificates are managed in a centralized way , or issued on a cryptographic card.

These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates work with a qualified electronic signature creation device, in accordance with Annex II to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and

the entity, company or organisation described in the "O" (Organisation) field, allowing the generation of a "qualified electronic signature"; that is to say, an advanced electronic signature based on a qualified certificate that has been generated using a qualified device, for this reason, in accordance with Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.
This certificate includes a field (Description) in the Subject, indicating the public document that reliably accredits the signatory's faculties to act on behalf of the entity it represents and, if mandatory, the registration of the Registry data.

These certificates are only valid for a short period of time, after which the certificate expires. This period of time shall always be less than 1 hour.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature uses, in accordance with the agreements made between the parties or the legal rules that apply in each case.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the "key usage" field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to create the electronic signature)

b) In the "Qualified Certificate Statements" field, the following declaration appears:
    - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    - QcSSCD (0.4.0.1862.1.4), which states that the certificate is only used in conjunction with a qualified signature creation device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.8. Corporate and ephemeral certificate of a natural person representing a legal entity issued in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.52	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n
2.16.724.1.3.5.8	For being a certificate of representative of a legal entity, with full legal powers, sole or joint administrator of the organization, or at least with specific general powers to act in front of the Spanish Public Administration

These certificates are managed in a centralized way.
These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature-creation device.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and the entity, company or organisation described in the “O” (Organisation) field, allowing the generation of an “advanced electronic signature based on a qualified electronic certificate".

This certificate includes a field (Description) in the Subject, indicating the public document that reliably accredits the signatory's faculties to act on behalf of the entity it represents and, if mandatory, the registration of the Registry data.

These certificates are only valid for a short period of time, after which the certificate expires. This period of time shall always be less than 1 hour.

Furthermore, the uses of corporate representative natural person certificates issued in software also include the following:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.
The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
c) The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.
d) The "User Notice" field describes the use of this certificate.

1.4.1.9. Corporate certificate of natural person representing non-incorporated entity issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.11	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-n-qscd
2.16.724.1.3.5.9	For being a certificate of representative of natural person representing non-incorporated entity in which the Representative has full powers to act on behalf of the Entity without Legal Personality front the Public Administrations[2]

These certificates are managed in a centralized way , or issued on a cryptographic card.

This certificate includes a field (Description) in the Subject field where the public document is indicated that certifies the signatory's faculties to act on behalf of the entity without legal personality that it represents and, if it is mandatory, the registration of the Registry data.
These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates work with a qualified electronic signature creation device, in accordance with Annex II to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and the entity, company or organisation described in the “O” (Organisation) field, allowing the generation of a “qualified electronic signature”; that is to say, an advanced electronic

[2] According to point 14.1.3.1 of the document "Electronic Certificate Profiles" of the Spanish Ministry of Finance and Public Administration (April 2016)

signature based on a qualified certificate that has been generated using a qualified device, for this reason, in accordance with Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Secure email signature.
b) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents.

Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    - qCCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    - QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified electronic signature creation device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.10. Corporate certificate of natural person representing non-incorporated entity issued in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.12	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n
2.16.724.1.3.5.9	For being a certificate of representative of natural person representing non-incorporated entity in which the Representative has full powers to act on behalf of the Entity without Legal Personality front the Public Administrations[3]

This certificate includes a field (Description) in the Subject field where the public document is indicated that certifies the signatory's faculties to act on behalf of the entity without legal personality that it represents and, if it is mandatory, the registration of the Registry data

This certificates QSCD are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2..

These certificates do not work with a qualified signature-creation device.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and the entity, company or organisation described in the “O” (Organisation) field, allowing the generation of a "advanced electronic signature based on qualified electronic certificate".

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Authentication in access control systems.

[3] According to point 14.1.3.1 of the document "Electronic Certificate Profiles" of the Spanish Ministry of Finance and Public Administration (April 2016)

b) Secure email signature.

c) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
   - Electronic signature (to perform authentication)
   - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
   - qCCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.

c) The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

d) The "User Notice" field describes the use of this certificate.

1.4.1.11. Corporate and ephemeral certificate of natural person representing non-incorporated entity issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.151	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-n-qscd
2.16.724.1.3.5.9	For being a certificate of representative of natural person representing non-incorporated entity in which the Representative has full legal powers to act on behalf of the Entity without Legal Personality front the Public Administrations[4]

These certificates are managed in a centralized way.

This certificate includes a field (Description) in the Subject field where the public document is indicated that certifies the signatory's faculties to act on behalf of the entity without legal personality that it represents and, if it is mandatory, the registration of the Registry data.

These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates work with a qualified electronic signature creation device, in accordance with Annex II to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and the entity, company or organisation described in the "O" (Organisation) field, allowing the

[4] According to point 14.1.3.1 of the document "Electronic Certificate Profiles" of the Spanish Ministry of Finance and Public Administration (April 2016)

generation of a “qualified electronic signature”; that is to say, an advanced electronic signature based on a qualified certificate that has been generated using a qualified device, for this reason, in accordance with Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

These certificates are only valid for a short period of time, after which the certificate expires. This period of time shall always be less than 1 hour.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

c) Secure email signature.
d) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents.

Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

d) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to create the electronic signature)

e) In the “Qualified Certificate Statements” field, the following declaration appears:
    - qCCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    - QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified electronic signature creation device.

f) The "User Notice" field describes the use of this certificate.

1.4.1.12. Corporate and ephemeral certificate of a natural person representing a non-incorporated entity issued in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.152	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n
2.16.724.1.3.5.9	For being a certificate of representative of natural person representing non-incorporated entity in which the Representative has full legal powers to act on behalf of the Entity without Legal Personality front the Public Administrations[5]

These certificates are managed in a centralized way.

This certificate includes a field (Description) in the Subject field where the public document is indicated that certifies the signatory's faculties to act on behalf of the entity without legal personality that it represents and, if it is mandatory, the registration of the Registry data.

These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature-creation device.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and the entity, company or organisation described in the “O” (Organisation) field, allowing the generation of a "advanced electronic signature based on qualified electronic certificate".

[5] According to point 14.1.3.1 of the document "Electronic Certificate Profiles" of the Spanish Ministry of Finance and Public Administration (April 2016)

These certificates are only valid for a short period of time, after which the certificate expires. This period of time shall always be less than 1 hour.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    - qCCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
c) The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.
d) The "User Notice" field describes the use of this certificate

1.4.1.13. High-level public employee natural person certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.4.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-n-qscd.
2.16.724.1.3.5.7.1	which indicates that it is a Spanish public employee certificate, of high level.

High-level public employee natural person certificates are Qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are managed in a centralized way, or issued on a cryptographic card.

These certificates are issued to public employees to identify them as persons in the service of the Public Administration, binding them to the latter, complying with the requirements established in article 43 of Law 40/2015, of 1 October, on the Legal System of the Public Sector, for the electronic signature of personnel in the service of the Public Administration.

High-level public employee natural person certificates work with a qualified electronic signature creation device, in accordance with Annex II to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

High-level public employee natural person certificates are issued in accordance with the High-assurance levels of the certificate profiles, set out in paragraph 10 of the document "Profiles of electronic certificates" of the Subdirectorate General for Information, Documentation and Publications of the Ministerio de Hacienda y Administraciones Públicas.

These certificates guarantee the identity of the subscriber and the signer, and they also make it possible to generate “qualified electronic signatures”; that is to say, an advanced electronic signature based on a qualified certificate that has been generated using a

qualified device, for this reason, in accordance with Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Secure email signature.
b) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    a. Electronic signature (to perform authentication)
    b. Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    b. QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure electronic signature creation device.
c) The “User Notice” field describes the use of this certificate.

1.4.1.14. Medium-level public employee natural person certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.4.2	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n.
2.16.724.1.3.5.7.2	which indicates that it is a Spanish public employee certificate, of medium level.

Medium-level public employee natural person certificates are Qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as persons in the service of the Public Administration, binding them to the latter, complying with the requirements established in article 43 of Law 40/2015, of 1 October, on the Legal System of the Public Sector, for the electronic signature of personnel in the service of the Public Administration.

These certificates do not work with a qualified signature-creation device.

Medium-level public employee natural person certificates are issued in accordance with the medium-assurance levels of the certificate profiles, set out in paragraph 10 of the document "Profiles of electronic certificates" of the Subdirectorate General for Information, Documentation and Publications of the Ministerio de Hacienda y Administraciones Públicas.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Secure email signature.
b) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    a. Electronic signature (to perform authentication)
    b. Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
c) The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.
d) The "User Notice" field describes the use of this certificate.

1.4.1.15. Certificate of natural person public employee with pseudonym, high level

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.4.11	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-n-qscd
2.16.724.1.3.5.4.1	which indicates that it is a Spanish public employee certificate, of high level with pseudonym

These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are managed in a centralized way.

These certificates are issued to public employees to identify them as persons in the service of the Public Administration, binding them to the latter, complying with the requirements established in article 43 of Law 40/2015, of 1 October, on the Legal System of the Public Sector, for the electronic signature of personnel in the service of the Public Administration.
These certificates, due to privacy and security reasons, do not include the public employee's personal data, such as national ID card, name and surname. Instead, there is a pseudonym that corresponds to the professional identification number of that employee.

VinCAsign stores in a strictly confidential manner, the real identity of the signatory.

These certificates work with a qualified electronic signature creation device, in accordance with Annex II to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

Likewise, these certificates are issued in accordance with the high security levels of the certificate profiles established in point 10 of the document "Electronic Certificate Profiles"

of the Subdirectorate General for Information, Documentation and Publications of the Ministerio de Hacienda y Administraciones Públicas.

These certificates guarantee the identity of the subscriber and the signer, and they also make it possible to generate "qualified electronic signatures"; that is to say, an advanced electronic signature based on a qualified certificate that has been generated using a qualified device, for this reason, in accordance with Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

c) Secure email signature.
d) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the "key usage" field, the following functions are activated and can therefore be used:
    a. Electronic signature (to perform authentication)
    b. Content commitment (to create the electronic signature)

b) In the "Qualified Certificate Statements" field, the following declaration appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    b. QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure electronic signature creation device.
c) The "User Notice" field describes the use of this certificate.

1.4.1.16. Certificate of natural person public employee with pseudonym, medium level

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.4.12	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n.
2.16.724.1.3.5.7.2	which indicates that it is a Spanish public employee certificate, of medium level with pseudonym.

Medium-level public employee natural person certificates are Qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as persons in the service of the Public Administration, binding them to the latter, complying with the requirements established in article 43 of Law 40/2015, of 1 October, on the Legal System of the Public Sector, for the electronic signature of personnel in the service of the Public Administration.

These certificates, due to privacy and security reasons, do not include the public employee's personal data, such as national ID card, name and surname. Instead, there is a pseudonym that corresponds to the professional identification number of that employee.

VinCAsign stores in a strictly confidential manner, the real identity of the signatory.

These certificates do not work with a qualified signature-creation device.

Medium-level public employee natural person certificates are issued in accordance with the medium-assurance levels of the certificate profiles, set out in paragraph 10 of the document "Profiles of electronic certificates" of the Subdirectorate General for Information, Documentation and Publications of the Ministerio de Hacienda y Administraciones Públicas.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Secure email signature.
b) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    a. Electronic signature (to perform authentication)
    b. Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
c) The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.
d) The "User Notice" field describes the use of this certificate.

1.4.1.17. High-level body electronic seal certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.4.12	in vinCAsign cerification hierarchy
0.4.0.194112.1.3	in accordance with the policy QCP-l-qscd
2.16.724.1.3.5.6.1	Which indicates to be a certificate of electronic seal of a Spanish Public Administration body, of high level.

These certificates are qualified certificates in accordance with article 38 and Annex III of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are managed in a centralized way.

These certificates are issued for the identification and authentication of the exercise of competence in automated administrative action in accordance with Article 42 of Law 40/2015, of October 1, on the Legal System of the Public Sector.

These certificates are issued in accordance with the High-assurance levels of the certificate profiles, set out in paragraph 9 of the document "Profiles of electronic certificates" of the Subdirectorate General for Information, Documentation and Publications of the Ministerio de Hacienda y Administraciones Públicas.

These certificates operate with a qualified signature-creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the Public Body subscribing to the certification service, and allow the generation of the **"qualified electronic seal"**; that is, the advanced electronic seal based on a qualified certificate and which has been generated using a qualified device, and therefore, in accordance with the provisions of Article 35.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014,

shall have the benefit of the presumption of data integrity and of the correctness of the origin of the data to which the qualified electronic seal is linked.

These certificates do not allow the encryption of documents, content, or data messages. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    b. QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified electronic signature creation device.
c) The “User Notice” field describes the use of this certificate.

1.4.1.18. Medium-level body electronic seal certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.5.2	in vinCAsign cerification hierarchy
0.4.0.194112.1.1	in accordance with the policy QCP-l
2.16.724.1.3.5.6.2	Which indicates to be a certificate of electronic seal of a Spanish Public Administration body, of medium level.

These certificates are qualified certificates in accordance with article 38 and Annex III of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are issued for the purposes of identifying and authenticating parties exercising powers in automated administrative procedures, in accordance with article 42 of Spanish Law 40/2015, of 01 October , on Legal Regime of the Public Sector.

These certificates do not work with a qualified signature creation device.

These certificates are issued in accordance with the medium-assurance levels of the certificate profiles, set out in paragraph 9 of the document "Profiles of electronic certificates" of the Subdirectorate General for Information, Documentation and Publications of the Ministerio de Hacienda y Administraciones Públicas.

These certificates guarantee the identity of the subscriber and of the public body included in the certificate.

These certificates do not allow the encryption of documents, content, or data messages. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    a. Electronic signature (to perform authentication)
    b. Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.

c) The QcSSCD statement (0.4.0.1862.1.4) does **not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.
d) The "User Notice" field describes the use of this certificate.

1.4.1.19. Legal person seal certificate issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.6.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.3	in accordance with the policy QCP-l-qscd

These certificates are qualified certificates in accordance with article 38 and Annex III of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are managed centrally.

These certificates operate with a qualified signature-creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber of the certification service, and allow the generation of the "qualified electronic seal", that is, the advanced electronic seal based on a qualified certificate and which has been generated using a qualified device. Therefore, in accordance with Article 35.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall enjoy the presumption of data integrity and the correctness of the origin of the data to which the qualified electronic seal is linked.

These certificates do not allow the encryption of documents, content, or data messages. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    a. Electronic signature (to perform authentication)
    b. Content commitment (to create the electronic signature)

b) In the "Qualified Certificate Statements" field, the following declaration appears:
   a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
   b. QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified electronic signature creation device.
c) The "User Notice" field describes the use of this certificate.

1.4.1.20. Legal person eSEAL certificate issued in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.6.2	in vinCAsign cerification hierarchy
0.4.0.194112.1.1	in accordance with the policy QCP-l

These certificates are qualified certificates in accordance with article 38 and Annex III of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and the company or entity included in the certificate.

These certificates do not allow the encryption of documents, content, or data messages. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the "key usage" field, the following functions are activated and can therefore be used:
   - Electronic signature (to perform authentication)
   - Content commitment (to create the electronic signature)

b) In the "Qualified Certificate Statements" field, the following declaration appears:

- QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.

- The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.21. Ephemeral eSEAL certificate of legal person in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.6.51	in vinCAsign cerification hierarchy
0.4.0.194112.1.3	in accordance with the policy QCP-l-qscd

These certificates are qualified certificates in accordance with article 38 and Annex III of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are managed centrally.

These certificates work with a qualified signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber of the certification service, and allow the generation of the "qualified electronic seal"; that is, the advanced electronic seal that is based on a qualified certificate and that has been generated using a qualified device. Therefore, in accordance with the provisions of Article 35.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, it will enjoy the presumption of data integrity and the correction of the origin of the data to which the qualified electronic seal is linked.

These certificates are only valid for a short period of time, after which the certificate expires. This period of time will always be less than 1 hour.

These certificates do not allow the encryption of documents, content, or data messages. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
   - Electronic signature (to perform authentication)
   - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
   - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
   - QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.22. Ephemeral eSEAL certificate of legal person in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.6.52	in vinCAsign cerification hierarchy
0.4.0.194112.1.1	in accordance with the policy QCP-l

These certificates are qualified certificates in accordance with article 38 and Annex III of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are managed centrally.
These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and the company or entity included in the certificate.

These certificates are only valid for a short period of time, after which the certificate expires. This period of time will always be less than 1 hour.

These certificates do not allow the encryption of documents, content, or data messages. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
   - Electronic signature (to perform authentication)
   - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
   - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.

   - The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.23. eSEAL Certificate for Electronic Time Stamp Service

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.9.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.1	in accordance with the policy QCP-l

These TSA/TSU electronic seal certificates are qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standards identified with reference ETSI EN 319 421 and ETSI EN 319 422.

This certificate allows Time Stamp Units or TSU to issue time stamps when they receive an application under the specifications of RFC3161.

The keys are generated in the media of a qualified device (QSCD).

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
   - Content Commitment

b) The "extend key usage" field has activated the function:
   - TimeStamping

c) In the “Qualified Certificate Statements” field, the following declaration appears:
   - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.

d) The "User Notice" field describes the use of this certificate.

1.4.1.24. Individual certificate of a natural person issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.10.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.1	in accordance with the policy QCP-n-qscd

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified with reference ETSI EN 319 411-2.

These certificates operate with a qualified signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates are managed centrally.

These certificates guarantee the identity of the individual holder (as the signatory and subscriber are the same person) without being linked to any entity and allow the generation of the "qualified electronic signature"; in other words, the advanced electronic signature that is based on a qualified certificate and which has been generated using a qualified device, and therefore, in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, will have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

a) Secure email signature.
b) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
   - Electronic signature (to perform authentication)
   - Content commitment (to perform the electronic signature function)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
   - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
   - QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure electronic signature creation device.

c) The “User Notice” field describes the use of this certificate.

1.4.1.25. Individual certificate of a natural person issued in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.10.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n

These certificates are qualified in accordance with Art. 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified with reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the individual holder (as the signatory and subscriber are the same person) without any link to any entity, and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

The certificates can be used in applications such as the following:
a) Authentication in access control systems
b) Secure e-mail signature.
c) Other electronic signature applications, in accordance with what the parties agree or with the legal rules applicable in each case.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
   - Electronic signature (to perform authentication)
   - Content commitment (to perform the electronic signature function)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
   - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
   - The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

c) The “User Notice” field describes the use of this certificate.

1.4.1.26. Individual and ephemeral certificate of physical person issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.10.51	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-n-qscd

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified with reference ETSI EN 319 411-2.

These certificates operate with a qualified signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates are managed centrally.

These certificates guarantee the identity of the individual holder (as the signatory and subscriber are the same person) without being linked to any entity and allow the generation of the "qualified electronic signature"; in other words, the advanced electronic signature that is based on a qualified certificate and which has been generated using a qualified device, and therefore, in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, will have a legal effect equivalent to that of a handwritten signature.

These certificates are only valid for a short period of time, after which the certificate expires. This period of time will always be less than 1 hour.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

c) Secure email signature.
d) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

d) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to perform the electronic signature function)

e) In the “Qualified Certificate Statements” field, the following declaration appears:
    - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    - QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure electronic signature creation device.
f) The “User Notice” field describes the use of this certificate.

1.4.1.27. Individual and ephemeral certificate of a natural person issued in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.10.52	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n

These certificates are qualified in accordance with Art. 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified with reference ETSI EN 319 411-2.
These certificates are managed centrally
These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the individual holder (as the signatory and subscriber are the same person) without any link to any entity, and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

These certificates are only valid for a short period of time, after which the certificate expires. This period of time will always be less than 1 hour.

The certificates can be used in applications such as the following:

a) Authentication in access control systems
b) Secure e-mail signature.
c) Other electronic signature applications, in accordance with what the parties agree or with the legal rules applicable in each case.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)

- Content commitment (to perform the electronic signature function)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
   - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
   - The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

c) The “User Notice” field describes the use of this certificate.

1.4.1.28. Non-qualified individual certificate of a natural person

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.110.1	in vinCAsign cerification hierarchy
0.4.0.2042.1.3	in accordance with the policy LCP

These certificates are non-qualified.

These certificates comply with the LCP (Lightweight Certificate Policy) in the technical standard identified with the reference ETSI EN 319 411-1.

These certificates are managed centrally.

These certificates allow the generation of advanced electronic signatures.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

a) Secure e-mail signature.
b) Other electronic signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, vinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

a) The field "key usage" has the following functions activated, and therefore allows you to perform them:

- Electronic signature (to perform the authentication function)
- Commitment to content (to perform the electronic signature function)

b) These certificates do not have "Qualified Certificate Statements" fields because they are not qualified.

1.4.1.29. Non-qualified and ephemeral individual certificate of a natural person

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.110.51	in vinCAsign cerification hierarchy
0.4.0.2042.1.3	in accordance with the policy LCP

These certificates are only valid for a short period of time, after which the certificate expires. This period of time will always be less than 1 hour.

These certificates are non-qualified.

These certificates comply with the LCP (Lightweight Certificate Policy) in the technical standard identified with the reference ETSI EN 319 411-1.

These certificates are managed centrally.

These certificates allow the generation of advanced electronic signatures.
They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

a) Secure e-mail signature.

b) Other electronic signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, vinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

a) The field "key usage" has the following functions activated, and therefore allows you to perform them:

- Electronic signature (to perform the authentication function)
- Commitment to content (to perform the electronic signature function)

b) These certificates do not have "Qualified Certificate Statements" fields because they are not qualified.

1.4.1.30. AGID Corporate certificate of a natural person representing a legal person issued in QSCD

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.11.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.2	in accordance with the policy QCP-n-qscd

These certificates are managed in a centralized way.

These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates work with a qualified electronic signature creation device, in accordance with Annex II to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and the entity, company or organisation described in the “O” (Organisation) field, allowing the generation of a “qualified electronic signature”; that is to say, an advanced electronic signature based on a qualified certificate that has been generated using a qualified device, for this reason, in accordance with Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

These certificates has been created on the basis of the regulations and recommendations of the Agency for Italy digital AGID.

They can also be used in applications that do not require a electronic signature equivalent to the written one, such as the following:

c) Secure email signature.
d) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents.

Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    - qCCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    - QcQSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified electronic signature creation device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.31. AGID Corporate representative natural person certificate issued in software

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.11.2	in vinCAsign cerification hierarchy
0.4.0.194112.1.0	in accordance with the policy QCP-n

These certificates are qualified certificates in accordance with article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014 and give effect to the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature-creation device.

These certificates guarantee the identity of the subscriber and the signer, and a relationship of legal representation or general power of attorney between the signer and the entity, company or organisation described in the “O” (Organisation) field, allowing the generation of an “advanced electronic signature based on a qualified electronic certificate".
These certificates has been created on the basis of the regulations and recommendations set by the Agency for Italy digital AGID.

Furthermore, the uses of corporate representative natural person certificates issued in software also include the following:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

These certificates do not allow the encryption of data messages, content or documents. Under no circumstances shall vinCAsign accept liability for the loss of encrypted information that cannot be recovered.
The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
    - Electronic signature (to perform authentication)
    - Content commitment (to create the electronic signature)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
    - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
    - The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.32. Certificate of Electronic Site

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.13.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.4	in accordance with the policy QCP-w
2.16.724.1.3.5.5.2	that indicates to be a certificate of electronic site

The certificates of electronic site are qualified certificates in accordance with Annex IV of Regulation (EU) 910/2014 of the European Parliament and Council of 23 July 2014 and comply with the provisions of the technical standard identified with the reference ETSI EN 319 411-2.

These certificates are issued to Public Administrations, complying with the indications of Article 38 of Law 40/2015, of October 1, on the Legal System of the Public Sector, for the electronic signature of personnel in the service of Public Administrations, to identify the Site and to guarantee the establishment of secure communications.

The electronic site certificates are issued in accordance with the medium security levels and certificate profiles established in point 8 of the document "Electronic Certificate Profiles" of the Subdirectorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

These Electronic Site certificates are used as an unequivocal identification mechanism for users, services and applications, as well as to provide public sector electronic sites with SSL/TSL capabilities.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
   - Electronic signature (to perform authentication)
     Key Encipherment (Used for key management and key transport)

b) In the “Qualified Certificate Statements” field, the following declaration appears:

- QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
- The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.33. SSL OV Certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.14.1	in vinCAsign cerification hierarchy
0.4.0.194112.1.4	in accordance with the policy QCP-w

The SSL OV server certificates are qualified certificates in accordance with Annex IV of Regulation (EU) 910/2014 of the European Parliament and Council of 23 July 2014 and comply with the provisions of the technical standard identified with the reference ETSI EN 319 411-2.
These SSL OV certificates are used as a mechanism to uniquely identify users, services and applications, as well as to provide websites with SSL/TLS capabilities.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
   - Electronic signature (to perform authentication)
     Key Encipherment (Used for key management and key transport)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
   - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
   - The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

c) The "User Notice" field describes the use of this certificate.

1.4.1.34. SSL EV Certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.14.2	in vinCAsign cerification hierarchy
0.4.0.194112.1.4	in accordance with the policy QCP-w

The SSL EV server certificates are qualified certificates in accordance with Annex IV of Regulation (EU) 910/2014 of the European Parliament and Council of 23 July 2014 and comply with the provisions of the technical standard identified with the reference ETSI EN 319 411-2.
These SSL EV certificates are used as a mechanism to uniquely identify users, services and applications, as well as to provide websites with SSL/TLS capabilities.

The usage information in the certificate profile includes the following:

a) In the “key usage” field, the following functions are activated and can therefore be used:
   - Electronic signature (to perform authentication)
     Key Encipherment (Used for key management and key transport)

b) In the “Qualified Certificate Statements” field, the following declaration appears:
   - QcCompliance (0.4.0.1862.1.1), which informs that the certificate is being issued as a qualified certificate.
   - The QcSSCD statement (0.4.0.1862.1.4) **does not appear** in the 'Qualified Certificate Statements' field, as this certificate is not used with a qualified device.

c) The "User Notice" field describes the use of this certificate.

1.4.2. Limits and prohibitions on the use of certificates

The certificates are used for their own specified function and purpose and may not be used for any other functions or purposes.

Similarly, the certificates may only be used in accordance with the applicable laws, with special consideration to the import and export restrictions valid at each moment.

The certificates may not be used to sign requests for certificate issue, renewal, suspension or revocation, nor to sign any type of public certificates or to sign certificate revocation lists (CRLs).

The certificates have not been designed, cannot be employed for and may not be used or resold as devices for the control of dangerous situations or for uses that require fault-proof procedures, such as the functioning of nuclear facilities, air traffic navigation or communication systems, or weapons control systems, where any fault could directly lead to death, personal injury or extreme environmental damage.

It is essential to take into account the limits indicated in the different fields of the certificate profiles, which can be seen on the vinCAsign website (https://www.vincasign.net).

The use of:

- the digital certificates in operations that contravene this CPS,
- the legal documents linked to each certificate or
- the agreements with the registration authorities or their signers/subscribers,

shall be considered as improper use for legal purposes, thus releasing vinCAsign from any liability for said improper use of the certificates by the signer or any other third party, in accordance with current legislation.

VinCAsign does not have access to the data to which the use of a certificate can be applied. Therefore, and as a consequence of this technical impossibility of accessing the content of a message, vinCAsign is not able to issue any evaluation of said content. As a result, the subscriber, signer or custodian shall assume any liability arising from the content linked to the use of a certificate.

Likewise the subscriber, signer or custodian shall accept any liability arising from:

- the use of certificates outside the limits and conditions of use set out in this CPS,
- the legal documents linked to each certificate or
- the contracts and agreements with the registration authorities or their subscribers,

as well as any other improper use thereof derived from this section or that could be considered as such pursuant to current legislation.

1.5. Management of the policy

1.5.1. Organisation responsible for managing the policy

VÍNTEGRIS SL (vinCAsign)
Av. Carrilet, 3
Ciutat de la Justícia de Barcelona
Edificio D - Planta 4ª
08902 L´Hospitalet de Llobregat (Barcelona)
TEL.: (+34) 902 362 436 / (+34) 934 329 098
FAX: (+34) 934 329 344

1.5.2. Contact details of the organisation

VÍNTEGRIS SL (vinCAsign)
Av. Carrilet, 3
Ciutat de la Justícia de Barcelona
Edificio D - Planta 4ª
08902 L´Hospitalet de Llobregat (Barcelona)
TEL.: (+34) 902 362 436 / (+34) 934 329 098
FAX: (+34) 934 329 344

1.5.3. Document management procedures

The documentary and organizational system of vinCAsign guarantees, through the existence and application of the corresponding procedures, the correct maintenance of this document and the service specifications related to it.

The procedure for reviewing and approving changes to the CPS is detailed in the internal documentation. (vinCAsign Gestion Politicas v1r1.pdf).

This CPS will be reviewed and updated annually by VinCAsign.

1.6. Definitions and Acronyms

1.6.1. Definitions

Certification Authority	*It is the entity responsible for issuing and managing digital certificates.*
Registration Authority	*Entity responsible for the management of applications, identification and registration of certificate applicants. It can be part of the Certification Authority or be an external one.*
Certificate	*File that associates the public key with some identifying data of the Subject/Signer and is signed by the CA.*
Public Key	*Publicly known mathematical value used for the verification of a digital signature or the encryption of data.*
Private key	*Mathematical value known only to the Subject/Signer and used for creating a digital signature or decrypting data.* *The private key of the CA will be used for certificate signing and CRL signing.*
CPS	*Set of practices adopted by a Certification Authority for the issuance of certificates in accordance with a specific certification policy.*
CRL	*File containing a list of certificates that have been revoked in a given period of time and that is signed by the CA.*

Activation Data	*Private data, such as PIN's or passwords used for private key activation*
DCCF (QSCD)	*Qualified signature creation device. Software or hardware element, conveniently certified, used by the Subject/Signatory to generate electronic signatures, so that cryptographic operations are performed within the device and its control is guaranteed solely by the Subject/Signatory.*
Digital Signature	*The result of the transformation of a message, or any type of data, by the application of the private key in conjunction with known algorithms, thus guaranteeing:* *a) that the data has not been modified (integrity)* *b) that the person who signs the data is who he says he is (identification)* *c) that the person who signs the data cannot deny having done so (not repudiation in origin)*
OID	*Unique numerical identifier registered under ISO standardization and referred to a given object or object class.*
Key pair	*A set formed by the public and private key, both mathematically related to each other.*
PKI	*Set of hardware, software, human resources, procedures, etc., that make up a system based on the creation and management of public key certificates.*
Applicant	*In the context of this document, the applicant will be a natural person with a special power of attorney to carry out certain procedures in the name and on behalf of a legal person, or of itself for individual certificates or web authentication certificates.*
Subscriber	*In the context of this document the legal entity that owns the certificate (at corporate level) or the natural person in individual certificates.*
Subject/Signer	*In the context of this document, the natural person whose public key is certified by the CA and has, or has exclusive access to, a valid private key for generating digital signatures.*

User Part	*In the context of this document, the person who voluntarily trusts the digital certificate and uses it as a means of accrediting the authenticity and integrity of the signed document.* *Trusted parties for Web authentication certificates are both application client users and applications and services with SSL/TLS capabilities that connect to Web sites.*

1.6.2. Acronyms

AC (*o también CA*)	*Certificate Authority* Autoridad de Certificación
AR (o también RA)	*Registration Authority* Autoridad de Registro
CPD *(or DPC in english)*	*Data Processing Center* Centro de Proceso de Datos
CPS (o también DPC)	*Certification Practice Statement*. Declaración de Prácticas de Confianza
CRL (o tambien LRC)	*Certificate Revocation List.* Lista de certificados revocados
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital
DNI	Documento Nacional de Identidad *NATIONAL IDENTITY CARD*
ETSI EN	*European Telecommunications Standards Institute – European Standard.*
FIPS	*Federal Information Processing Standard Publication*
HSM	*Hardware Security Module* Módulo de seguridad en Hardware
IETF	*Internet Engineering Task Force*
NIF	Número de Identificación Fiscal *Tax ID number*
NTP	*Network Time Protocol* Protocolo de tiempo en red.

OCSP	*On-line Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier*. Identificador de objeto
PDS	*PKI Disclosure Statements* Texto de Divulgación de PKI.
PIN	*Personal Identification Number*. Número de identificación personal
PKI	*Public Key Infrastructure*. Infraestructura de clave pública
PKCS#10	*standard developed by RSA Labs and universally accepted, which defines the syntax of a certificate request*
QSCD (o también DCCF)	*Qualified Electronic Signature/Seal Creation Device.* Dispositivo cualificado de creación de firma/sellos
QCP	*Qualified Certificate Policy* Política de certificados cualificados
QCP-n	*Policy for EU qualified certificate issued to a natural person* Política de certificados cualificados para personas físicas.
QCP-l	*Policy for EU qualified certificate issued to a legal person* Política de certificados cualificados para personas jurídicas.
QCP-n-qscd	*Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD* Política de certificados cualificados para personas físicas con dispositivo cualificado de firma/sello
QCP-l-qscd	*Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD* Política de certificados cualificados para personas jurídicas con dispositivo cualificado de firma/sello
QCP-w	*Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person* Política de certificados cualificados para autenticación de sitios web, emitidos a personas jurídicas o físicas.
RFC	*Request for Comments*

	Documento RFC
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado *Type of encryption algorithm*
SEPBLAC	Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (Sepblac). *Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences*
SHA	*Secure Hash Algorithm.* Algoritmo seguro de Hash
SSL	*Secure Sockets Layer.* *A protocol designed by Netscape and converted into a network standard, it allows the transmission of encrypted information between an Internet browser and a server* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
TCP/IP	*Transmission Control. Protocol/Internet Protocol*. *System of protocols, defined in the framework of the IEFT.* Sistema de protocolos, definidos en el marco de la IEFT.
UTC	*Coordinated Universal Time* Tiempo universal coordinado
VPN	*Virtual Private Network.* Red privada virtual

2. Publication of information and certificate repository

2.1. Certificate repository/repositories

VinCAsign has a certificate repository where it publishes information relating to the certification services.

Said service is available 24 hours a day, 7 days a week and, in the event of a system failure beyond vinCAsign's control, vinCAsign will make its best efforts to make the service available again within the time frame set forth in section 5.7.4 of this Certification Practice Statement.

2.2. Publication of information on the certification services provider

VinCAsign publishes the following information in its Repository:

- The certificates issued, when the consent of the natural person indicated in the certificate has been obtained.
- The lists of revoked certificates and other information on the revocation status of certificates.
- The Certification Practice Statement.
- The informative texts (PKI Disclosure Statements - PDS), published at least in English.

In addition to what is specified in this CPS, VinCAsing has test websites that allow application providers to test their software with web authentication certificates:

VALID https://valid.vincasign.net

REVOCATED https://revoked.vincasign.net

EXPIRED https://expired.vincasign.net

2.3. Frequency of publication

The information of the certification services provider, including dissemination texts, is published as soon as it is available.

The changes made to the Certification Practice Statement are governed by the provisions of section 1.5 of this document.

Information on the revocation status of certificates is published in accordance with the provisions of sections 4.9.7 and 4.9.8 of this Certification Practice Statement.

2.4. Access control

VinCAsign does not limit access for the purpose of reading the information established in section 2.2, but it does have controls in place to prevent non-authorised persons from adding, modifying or deleting records from the Repository, in order to protect the integrity and authenticity of the information, especially information on revocation statuses.

VinCAsign uses reliable systems for the Repository, so that:

- Only those authorised persons may make notes and modifications.
- The authenticity of the information can be verified.
- The certificates are only available for consultation if the consent of the natural person indicated in the certificate has been obtained.
- Any technical changes that may affect the security requirements can be detected.

2.5. Cryptographic hardware

The cryptographic hardware used by vinCAsign is described in section 6.8 of this CPS.

3. Identification and authentication

3.1. Initial registration

3.1.1. Types of name

All the certificates contain a differentiated X.501 name in the *Subject* field, including a *Common Name* component (CN=) relating to the identity of the subscriber and the natural person identified in the certificate, as well as additional pieces of identity information in the *SubjectAlternativeName* field.

In web authentication certificates, the Common Name includes the name of the domain name where the certificate will reside

The names contained in the certificates are those listed below,

3.1.1.1. Corporate Corporate certificates for natural persons

- Issued in QSCD, with OID 1.3.6.1.4.47155.1.1
- Issued in SOFT, with OID 1.3.6.1.4.47155.1.1.2
- Issued in QSCD and ephemeral, with OID 1.3.6.1.4.47155.1.1.51
- Issued in SOFT and ephemeral, with OID 1.3.6.1.4.47155.1.1.52

Country (C)	E.g.: “ES” (or that corresponding to the subscriber’s country)
Organization (O)	Organisation to which the signer is linked
Organizational Unit (OU)	Department within the Organisation to which the signer is linked, or other information on the Organisation
Organizationidentifier	NIF of the legal entity to which it is linked in ETSI format EN 319412-1 (Example: "VATES-Q0000000J)
Surname	Surname(s)
Given Name	Given Name(s)
Title	Position/other
Serial Number	National ID No./Tax ID No.
Common Name (CN)	Given name, surname and number of the natural person

3.1.1.2. Corporate certificate of a natural person representing a legal entity

- Issued in QSCD, with OID 1.3.6.1.4.47155.1.2.1
- Issued in SOFT, with OID 1.3.6.1.4.47155.1.2.2
- Issued in QSCD and ephemeral, with OID 1.3.6.1.4.47155.1.2.51
- Issued in SOFT and ephemeral, with OID 1.3.6.1.4.47155.1.2.52

Country (C)	E.g.: "ES" (or that corresponding to the subscriber's country)
Organization (O)	Organisation that the signer represents
Organizational Unit (OU)	Indication regarding the representation
Organizationidentifier	NIF of the legal entity to which it is linked in ETSI format EN 319412-1 (Example: "VATES-Q0000000J)
Surname	Surname(s) (as stated on the DNI/NIE)
Given Name	Given Name(s) (as stated on the DNI/NIE)
Title	Role or function as regards representation
Serial Number	NIF of the holder (NIF is the number and letter that appears in the DNI or NIE as appropriate "123456789Z"). Or encoding according to ETSI EN 319 412-1 "IDCES-123456789Z"
Common Name (CN)[6]	Ej.: "00000000T Ricardo Ribes (R: Q0000000J)"
Description	- Reg: XXX /Letter: XXX /Volume:XXX /Section:XXX /Book:XXX /Polio:XXX /Date: dd-mm-yyyy /Inscription: XXX - Notary: First name Surname1 Surname2 /Protocol number XXX /Date of Award: dd-mm-yyyy - In Official Bulletins: Bulletin: XXX/ /Date: dd-mm-yyyy /Number resolution: XXX

[6] According to the proposal in section 14.1.3.3 (codification of the Common Name attribute) of the document "Electronic Certificates Profiles (April 2016)" of the Ministry of Finance and Public Administration: DNI/NIE, Name and Surname, "(R:", Nif of the represented company, ")". Maximum 64 characters according to RFC 5280

3.1.1.3. Corporate certificate of natural person representing non-incorporated entity

- Issued in QSCD, with OID 1.3.6.1.4.47155.1.2.11
- Issued in SOFT, with OID 1.3.6.1.4.47155.1.2.12
- Issued in QSCD and ephemeral, with OID 1.3.6.1.4.47155.1.2.151
- Issued in SOFT and ephemeral, with OID 1.3.6.1.4.47155.1.2.152

Country [C]	E.g.: “ES” (or that corresponding to the subscriber’s country)
Organization (O)	Organisation that the signer represents
Organizational Unit (OU)	Indication regarding the representation
Organizationidentifier	NIF of the legal entity to which it is linked in ETSI format EN 319412-1 (Example: "VATES-Q0000000J)
Surname	The representative’s surname(s) (as stated on the DNI/NIE)
Given Name	The representative’s given name(s) (as stated on the DNI/NIE)
Title	Role or function as regards representation
Serial Number	NIF of the holder (NIF is the number and letter that appears in the DNI or NIE as appropriate "123456789Z”). Or encoding according to ETSI EN 319 412-1 "IDCES-123456789Z"
Common Name (CN) [7]	E.g: “00000000T Ricardo Ribes (R: Q0000000J)”
Description	Codification (code id) of the public document that accredits the powers of the signatory or the Registry data.

[7] According to the proposal in section 14.1.3.3 (codification of the Common Name attribute) of the document'Electronic Certificate Profiles (April 2016)' of the Ministry of Finance and Public Administration: DNI/NIE, Name and Surname,'(R:', NIF of the unincorporated entity represented,')'. Maximum 64 characters according to RFC 5280

3.1.1.4. Public employee natural person certificate

- Issued for HIGH level, with OID 1.3.6.1.4.47155.1.4.1
- Issued for MEDIUM level, with OID 1.3.6.1.4.47155.1.4.2

Country (C)	"ES"
Organization (O)	Public Administration in which the signer provides their services
Organizational Unit (OU)	Unit to which the signer is assigned
OrganizationIdentifier	NIF of the P.A. to which the public employee holding the certificate is attached, in ETSI format EN 319412-1 (Example: "VATES-Q0000000J)
Surname	Surnames of the natural person (as it appears in the DNI / NIE)
Given Name	Given Name(s) (as it appears in the DNI / NIE)
Title	Position
Serial Number	NIF of the holder (NIF is the number and letter that appears in the DNI or NIE as appropriate "123456789Z"). Or encoding according to ETSI EN 319 412-1 "IDCES-123456789Z"
Common Name (CN)[8]	Nombre Apellido1 Apellido2 – DNI 00000000G
OID:2.16.724.1.3.5.7.1.4 (* high) OID: 2.16.724.1.3.5.7.2.4 (* medium)	The signer's DNI / NIE
OID: 2.16.724.1.3.5.7.1.5 OID: 2.16.724.1.3.5.7.2.5	Personal ID No. in the Public Administration
OID: 2.16.724.1.3.5.7.1.6 OID: 2.16.724.1.3.5.7.2.6	The signer's given name
OID: 2.16.724.1.3.5.7.1.7 OID: 2.16.724.1.3.5.7.2.7	The signer's first surname
OID: 2.16.724.1.3.5.7.1.8 OID: 2.16.724.1.3.5.7.2.8	The signer's second surname
OID: 2.16.724.1.3.5.7.1.9 OID: 2.16.724.1.3.5.7.1.9	The signer's email address

(high) The branch of OID indicated as 2.16.724.1.3.5.7.1.x corresponds to the High level*
(medium) The branch of OID indicated as 2.16.724.1.3.5.7.2.x corresponds to the Medium level*

[8] The name and two surnames must be entered according to identity document (DNI/Passport), as well as DNI (See Composition Criteria of the CN field for a public employee of the "Electronic Certificate Profiles (April 2016)" document of the Ministry of Finance and Public Administration)

3.1.1.5. Public employee natural person certificate under a pseudonym

- Issued for HIGH level, with OID 1.3.6.1.4.47155.1.4.11

- Issued for MEDIUM level, with OID 1.3.6.1.4.47155.1.4.12

Country (C)	"ES"
Organization (O)	Public Administration in which the signer provides their services
Organizational Unit (OU)	Unit to which the signer is assigned
OrganizationIdentifier	NIF of the P.A. to which the public employee holding the certificate is attached, in ETSI format EN 319412-1 (Example: "VATES-Q0000000J)
Pseudonym	Identification number in the Administration
Given Name	Given Name(s) (as it appears in the DNI / NIE)
Title	Position
Common Name (CN)[9]	Indication of position/"Pseudonym" - registration number in Public Administration -- Public Administration name
OID: 2.16.724.1.3.5.4.1.2 (*high) OID: 2.16.724.1.3.5.4.2.2 (*medium)	The entity that owns this certificate
OID: 2.16.724.1.3.5.4.1.3 OID: 2.16.724.1.3.5.7.2.3	Unique identification number of the entity
OID: 2.16.724.1.3.5.4.1.9 OID: 2.16.724.1.3.5.7.2.9	Contact Email
OID: 2.16.724.1.3.5.4.1.11 OID: 2.16.724.1.3.5.4.2.11	Position held by the certificate subscriber within the administration.
OID: 2.16.724.1.3.5.4.1.12 OID: 2.16.724.1.3.5.4.2.12	Pseudonym

(high) The branch of OID indicated as 2.16.724.1.3.5.4.1.x corresponds to the High level*
(medium) The branch of OID indicated as 2.16.724.1.3.5.4.2.x corresponds to the Medium level*

[9] See Composition Criteria of the CN field for a public employee with a pseudonym in section 11.1 of the document "Electronic Certificate Profiles (April 2016)" of the Ministry of Finance and Public Administration)

3.1.1.6. Public Administration body electronic seal certificates

- Issued for HIGH level, with OID 1.3.6.1.4.47155.1.5.1
- Issued for MEDIUM level, with OID 1.3.6.1.4.47155.1.5.2

Country (C)	"ES"
Organization (O)	Public Administration to which the seal belongs
Surname	Surname(s) of the head of the body to which the seal belongs
Given Name	Name of the head of the body to which the seal belongs
Serial Number	National ID No. of the public entity
OID: 2.16.724.1.3.5.6.1.4 (* high) OID: 2.16.724.1.3.5.6.2.4 (* medium)	DNI/NIE of responsible for the seal
OID: 2.16.724.1.3.5.6.1.6 OID: 2.16.724.1.3.5.6.2.6	Given name of responsible for the seal
OID: 2.16.724.1.3.5.6.1.7 OID: 2.16.724.1.3.5.6.2.7	First surname of the party responsible for the seal
OID: 2.16.724.1.3.5.6.1.8 OID: 2.16.724.1.3.5.6.2.8	Second surname of of responsible for the seal
OID: 2.16.724.1.3.5.6.1.9 OID: 2.16.724.1.3.5.6.2.9	Email of responsible for the seal

(* high) The branch of OID indicated as 2.16.724.1.3.5.6.1.x corresponds to the High level

(* medium) The branch of OID indicated as 2.16.724.1.3.5.6.2.x corresponds to the Medium level

3.1.1.7. Legal person seal certificate

- Issued in QSCD, with OID 1.3.6.1.4.47155.1.6.1
- Issued in SOFT, with OID 1.3.6.1.4.47155.1.6.2
- Issued in QSCD and ephemeral, with OID 1.3.6.1.4.47155.1.6.51
- Issued in SOFT and ephemeral, with OID 1.3.6.1.4.47155.1.6.52

Country (C)	"ES"
Organization (O)	Official name of the legal entity
Organizationidentifier	NIF of the legal entity to which it is linked in ETSI format EN 319412-1
Serial Number	ID card of the legal entity (DNI)

3.1.1.8. Electronic seal certificate for IoT

- Issued in SOFT, with OID 1.3.6.1.4.47155.1.7.2

Country (C)	"ES"
Organization (O)	Official name of the legal entity
OrganizationUnit (OU)	Identifier of the thing
Organizationidentifier	NIF of the legal entity to which it is linked in ETSI format EN 319412-1
Serial Number	VAT number of the legal entity / NIF

3.1.1.9. Electronic Seal Certificate for Electronic Time Stamp Service- Issued in SOFT

- Issued in SOFT, with OID 1.3.6.1.4.47155.1.9.1

Country (C)	"ES"
Organization (O)	Official name of the legal entity
OrganizationUnit (OU)	Identifier of the thing
Organizationidentifier	Name of the TSU in whose name this certificate has been issued
Common Name (CN)	Name of the TSU in whose name this certificate has been issued

3.1.1.10. Individual certificates for natural persons

- Issued in QSCD, with OID 1.3.6.1.4.47155.1.10.1
- Issued in SOFT, with OID 1.3.6.1.4.47155.1.10.2
- Issued in QSCD and ephemeral, with OID 1.3.6.1.4.47155.1.10.51
- Issued in SOFT and ephemeral, with OID 1.3.6.1.4.47155.1.10.52

Country (C)	E.g.: "ES" (or that corresponding to the subscriber's country)
Surname	Surnames of the natural person (as it appears in the DNI / NIE)
Given Name	Given Name(s) (as it appears in the DNI / NIE)
Serial Number	DNI/NIE
Common Name (CN)	Name, surname and number of the natural person

3.1.1.11. Electronic Site certificate

- Medium level, with OID 1.3.6.1.4.47155.X1.13.1

Organization (O)	Name (Official Name of the Organisation) of the subscriber of the certificate
Organizational Unit (OU)	SEDE ELECTRONICA
Organization Unit (OU)	Descriptive name of the Site
Organization Identifier	Organisation identifier According to the technical standard ETSI EN 319 412-1 (VATES + Tax Identification Number of the Entity)
Country Name (CN)	2-digit country code according to ISO 3166-1 By default " ES ".
Locality (L)	Name of the subscriber's location (City)
Business Category	Category of the subscribing organisation "Government Entity"
Jurisdiction Country	Name of the applicable jurisdiction "ES"
Serial Number	Unique identification number of the Certification Service Subscriber Entity (NIF)
Common Name (CN)	Unique identification number of the Certification Service Subscriber Entity (NIF)

3.1.1.12. SSL certificate

- OV with OID 1.3.6.1.4.47155.1.14.1

Organization (O)	Name (Official Name of the Organisation) of the subscriber of the certificate
Organizational Unit (OU)	SSL-OV Certificate
Organization Identifier	Organisation identifier According to the technical standard ETSI EN 319 412-1 (VATES + Tax Identification Number of the Entity)
Country Name (CN)	2-digit country code according to ISO 3166-1 By default " ES "
Locality (L)	Name of the subscriber's location (City)
Business Category	Category of the subscribing organisation "PRIVATE ORGANIZATION", "GOVERNMENT ENTITY", "BUSINESS ENTITY", o "NON-COMMERCIAL ENTITY"
Jurisdiction Country	Name of the applicable jurisdiction (Country)
Serial Number	Unique identification number of the Certification Service Subscriber Entity (NIF)
Common Name (CN)	Name of the domain name (DNS) where the certificate will reside

- EV with OID 1.3.6.1.4.47155.1.14.2

Organization (O)	Name (Official Name of the Organisation) of the subscriber of the certificate
Organizational Unit (OU)	SSL-EV Certificate
Organization Identifier	Organisation identifier According to the technical standard ETSI EN 319 412-1 (VATES + Tax Identification Number of the Entity)
Locality (L)	Name of the subscriber's location (City)
Business Category	Category of the subscribing organisation "PRIVATE ORGANIZATION", "GOVERNMENT ENTITY", "BUSINESS ENTITY", o "NON-COMMERCIAL ENTITY"
Jurisdiction Country	Name of the applicable jurisdiction (Country)
Country Name (CN)	2-digit country code according to ISO 3166-1
Serial Number	Unique identification number of the Certification Service Subscriber Entity (NIF)
Common Name (CN)	Name of the domain name (DNS) where the certificate will reside

3.1.2. Meaning of the names

The names contained in the *SubjectName* and *SubjectAlternativeName* fields of the certificates are understandable in natural language, in accordance with the provisions of the previous section.

3.1.3. Use of anonyms and pseudonyms

In no case are anonymous certificates issued.

VinCAsign will issue the certificates under a pseudonym so that the actual signatory of the certificate can be uniquely identified.

The fields "pseudonym" and "common name" of the "subject" of the certificate include the specific references of the pseudonym.
VinCAsign keeps the actual signatory's identity confidential.
The pseudonym certificate is not provided by Vintegris to entities, companies or organisations.

3.1.4. Interpretation of name formats

The name formats shall be interpreted in accordance with the law of the subscriber's country of establishment, on its own terms.
The "country" field will be that of the subscriber's country, and will always be Spain in the certificates issued to the Spanish Public Administrations.
The certificate shows the relationship between a natural person and the company, entity or organisation with which he or she is linked, regardless of the natural person's nationality. This derives from the corporate nature of the certificate, of which the entity, company or organisation is the subscriber, and the individual linked to the person authorised to use it.
In the certificates issued to Spanish subscribers, the "serial number" field must include the signatory's NIF, for the purpose of admitting the certificate for the purpose of carrying out procedures with the Spanish authorities. In the case of certificates with a pseudonym, the "pseudonym" field must be used for identification purposes

Furthermore, Vintegris takes into account the requirements of ISO 9595 (X.500) for the interpretation of the names contained in the certificates, as well as the requirements (Baseline Requirements) of CA/Browser- Forum.

3.1.5. Uniqueness of names

For each vinCAsign certificate policy, the certificate subscriber shall have a unique name.

It will not be possible to assign a subscriber name that has already been used, and this should not occur thanks to the presence of the National ID Document or equivalent number in the naming scheme.

A subscriber may request more than one certificate as long as the combination of the following values in the request differs from any valid certificates:

- Tax ID Number (NIF) or other legally valid ID number of the natural person.
- Tax ID Number (NIF) or other legally valid ID number of the subscriber.
- Certificate Type (description of certificate field).

3.1.6. Resolution of conflicts regarding names

Parties requesting certificates may not include names in the requests that may represent a breach of third-party rights by the future subscriber.

VinCAsign shall not be obliged to perform a previous check as to whether a certificate requester holds the industrial property rights to the name that appears in a certificate request, rather it will generally proceed to issue the certificate.

Furthermore, it will not act as arbitrator or mediator, neither shall it resolve in any other way any disagreements concerning the property rights to the names of people or organisations, domain names, brands or trade names.

However, in the event it receives a notification regarding a conflict of names, pursuant to the legislation of the subscriber's country, it may undertake actions aimed at blocking or withdrawing the issued certificate.

In any case, the service provider reserves the right to reject a certificate request due to a conflict of names.

Any dispute or conflict arising from the present document shall be definitively resolved through the legal arbitration of an arbiter within the framework of and in accordance with the Regulations and By laws of the Spanish Court of Arbitration, which shall be responsible for processing the arbitration and assigning an arbiter or arbitration tribunal. The parties agree to comply with the ruling that is issued.

3.1.7. Trademark recognition, authentication and function

VinCAsing checks, through consultations with official registers or documents certified by third parties, the evidence of the possession of the brand that an applicant wishes to incorporate into the certificate requested, claiming to have a right to it. VinCAsign does not assume any commitment regarding the issuance of certificates with respect to the use of a trademark by the applicants of the same. The verification method used by Vintegris is reflected in section 4.1.3.2 of this CPD.

3.2. Initial validation of identity

3.2.1. According to the type of certificate

3.2.1.1. Corporate certificates

The identity of certificate subscribers is established the moment the contract is signed between vinCAsign and the subscriber, when the existence of the subscriber and the powers of the person acting as their representative are verified. For the purpose of said verification, public or notarial documents may be used or the corresponding public Registers may be directly consulted.

The identity of the natural persons identified in the certificates is validated through the corporate records of the entity, company or organization (public or private entity) which

is the subscriber of the certificates. The subscriber will produce a certification of the necessary data, and will send it to vinCAsign, by the means that it enables, for the registration of the identity of the signatories.

In relation to the personal data of each entity, company or organization of public or private law, vinCAsign acts as the **Controller** in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), and in the Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), and in the terms indicated in paragraph 9. 4 of this document.

3.2.1.2. Individual certificates

The identity of the natural persons identified in the certificates is validated by their physical presence before a Registration Entity, providing the necessary documentation that identifies them as a DNI, NIF or passport.

In relation to the personal data of this type of certificates vinCAsign acquires the condition of Responsible of the treatment in the terms indicated in the section 9.4 of this document.

3.2.1.3. Web authentication certificates

Applicants for Web authentication certificates must be authorised by the entity to apply for such certificates on behalf of the organisation. The identity of the applicants is validated by accessing the NEBULASUITE platform, where they are previously identified.

3.2.1.4. Non-qualified certificates

The identity of the natural persons identified in these certificates is carried out by videoconference in accordance with the SEPBLAC standard.

3.2.2. Proof for the possession of the private key

Possession of the private key is demonstrated by the reliable procedure of delivery and acceptance of the certificate by the subscriber, in seal certificates, or by the signatory, in signature certificates.

In case the key pair is generated by the subscriber, the subscriber must prove that he or she is in possession of the private key corresponding to the public key from which certification is requested, by sending the certification request in PKSC#10 or other method that vinCAsign considers valid and approved.

3.2.3. Authentication of the identity of an organisation, company or entity via a representative

Natural persons with the capacity to act on behalf of subscribing public or private persons may act as representatives thereof as long as there is a pre-existing power of attorney or letter of representation signed between the natural person and the public or private person that requests their acknowledgement by vinCAsign. Said acknowledgement shall be performed in person by means of the following procedure:

1. The subscriber's representative will meet in person with an authorized representative of vinCAsign, who will make available an authentication form.

   Alternatively, the subscriber's representative may obtain the form on the vinCAsign website and fill it in beforehand.

2. The representative shall fill in the form with the following information and shall present it with the following documents:

   - Their identification details as a representative:

     - Given name and surname
     - Place and date of birth
     - Document: Tax ID Code (DNI/NIF) of the representative

   - The identification details of the subscriber they are representing:

     - Company name.
     - All existing registration information, including data relating to the incorporation and legal personality and the extent and validity of the applicant's powers of representation.

- Document: Tax ID Code (NIF) of the public or private entity.
- Document: Public documents that can be used to reliably accredit the information given and its registration in the corresponding public Registry, if applicable. Said verification may be performed by consulting the public registry in which the documents of incorporation and power of attorney are registered, for which purpose the telematic means provided by said public Registries may be used.
- In the case of Entities without legal personality that must be registered in a public or special Register, they must present the certificate or simple note accrediting their registration, issued on the date of application or within the previous fifteen days.
- In the case of Entities without Legal Personality that do not have to be registered in any public or special Register, they will present the public deeds, contracts, statutes, agreements or any other documents that can accredit their constitution, validity and identification of the members that make them up.

- The details of the representation or powers of attorney:
  - Validity of the representation or capacity to act (start and end date).
  - The scope and limits, where applicable, of the representation or powers of attorney:
    - TOTAL. Total representation or powers of attorney. This verification shall be performed via telematic means at the public Registry where the powers of representation are registered.
    - PARTIAL: Partial legal representation or capacity. This verification may be carried out by means of an authentic electronic copy of the notarial deed of attorney, under the terms of the notarial regulations.
  - In the case of representation of entities without legal personality:
    - By means of the notarial documents that accredit the powers of representation of the applicant for the

certificate, or by means of a special power of attorney granted for this purpose.

- By means of private documents appointing the appropriate representative in each case. In particular, proof of representation may be furnished by the following documents:

    1. Document of appointment of the representative of the surviving heir, signed by all the heirs, with the name, surname and ID number or passport number of the representative, when he has not been appointed judicial administrator or executor with full powers of administration.
    2. Copy of the Minutes of the meeting of the Board of Owners in which the President of the Community was appointed, in the case of communities under the horizontal property regime.
    3. Document signed by a number of members sufficient in accordance with article 398 of the Civil Code to represent the majority of the interests of the entity, in the case of communities of property and civil societies without legal personality, designating the person who represents them to apply for the certificate.

3. Once the form has been filled in and signed, it will be signed and submitted to vinCAsign together with the aforementioned documents.

4. VinCAsign personnel will check the identity of the representative by means of their National ID Card as well as checking the content of the powers of representation against the documents submitted.

5. The VinCAsign personnel will then present a form confirming the authentication, and return the documentation to the subscriber's representative.

6. Alternatively, in accordance with the provisions of Article 24.1 of Regulation (EU) No 910/2014 of the European Parliament and of the Council, the signature of the form may be legitimated by a notary and sent to vinCAsign by registered post, in which case steps 3 to 5 above will not be precise..

The digital certificate service provision is formalised by means of the relevant contract between vinCAsign and the duly represented subscriber.

3.2.4. Authentication of the identity of a natural person

This section describes the methods used to verify the identity of a natural person indicated in a certificate.

3.2.4.1. For Corporate certificates

The identification information of the natural persons named in the certificates is verified by comparing the information in the request with the records of the public or private entity, company or organisation to which they are linked, ensuring that the information to be certified is correct.

3.2.4.2. For Individual certificates

See section 3.2.1.2.

3.2.4.3. For Web authentication certificates

See section 3.2.1.3.

3.2.4.4. Domain validation

In web authentication certificates, vinCAsign must verify that the entity requesting the certificate has control over the domain it is requesting to include in the certificate. To this end, Vintegris can carry out the following checks:

- Organisational: the ownership of the domain name is requested, certified by a legal representative of the organisation, in addition to the name of the legal entity

to which the certificate is issued and, where applicable, the registration number, as stated in the official registers.

- The procedure for verification by vinCAsign is set out in section 4.1.1.3.3.

3.2.4.5. Need to appear in person

3.2.4.5.1. Corporate certificates

When requesting certificates, the person in question does not need to be physically present as the relationship between the natural person and the public or private entity, company or organisation to which they are linked has already been accredited.

However, before delivering a certificate, the certification officer (if one exists) or other designated member of the subscribing public or private entity, company or organisation must verify the identity of the natural person named in the certificate by means of their physical presence.

During this procedure, the identity of the natural person indicated in the certificate will be duly confirmed.

For this reason, in all cases in which a certificate is issued, the identity of the signing natural person shall be verified in person.

The Registration Authority shall verify through the exhibition of documents or through its own sources of information, the rest of the data and attributes to be included in the certificate, keeping documentation accrediting their validity.

3.2.4.5.2. Individual certificates

In all cases in which a certificate is issued, the identity of the natural person signing is verified in person.

The Registration Authority will verify, by means of the exhibition of documents or through its own sources of information, the rest of the data and attributes to be included in the certificate, keeping documentation accrediting the validity of these.

3.2.4.5.3. Non-qualified certificates

See section 3.2.1.4.

3.2.4.6. Relationship with the natural person

In corporate certificates, the documentary justification of the link of a natural person identified in a certificate with a public or private law entity, company or organisation is given by its record in the internal registers (employment contract as an employee, or the commercial contract that links him, or the minutes where his position is indicated, or the application as a member of the organisation...) of each of the public and private organisations to which they are linked.

In the case of web authentication certificates (of electronic site or SSL), the applicant who uses a certificate of legal representative of the entity (whether public or private) for the application, does not need to provide any other type of documentary justification concerning his or her link to the entity. In the event that the application is signed with an individual qualified certificate, the applicant must present the necessary documentation that determines his/her capacity to represent the entity that owns the domain to which the application refers and the possession of the domain itself, as well as, if applicable, the authorisation of the legal representative to request this type of certificate. See section 4.1.1.3 of this CPS.

3.2.5. Non-validated subscriber information

VinCAsign does not include any non-validated subscriber information in the certificates.

3.2.6. Authentication of Registration Authorities

VinCAsign performs the necessary verifications to confirm the existence of the organization that wishes to become a Registration Authority. VinCAsign obtains documentation from the organization being submitted, in addition to using its own sources of information.

VinCAsign verifies and validates the identity of the operators of the Registration Authority with the information sent to it by the subscriber, which includes their authorization to act as such.

VinCAsign ensures that the operators of the Registration Authority receive sufficient training for the performance of their functions, which will be verified in the corresponding evaluations.

The operators and those responsible for certification are always authenticated with digital certificates for the rendering of their services front the Registration Authority.

3.3. Identification and authentication of renewal requests

3.3.1. Validation of the routine renewal of certificates

Before renewing a certificate, vinCAsign or a Registration Authority checks that the information used to validate the identity and other data of the subscriber and the natural person identified in the certificate are still valid.

The following methodologies may be used to perform this check:

- The use of the current certificate to renew the certificate, as long as it is a certificate issued by vinCAsign and the maximum period allowed by law has not expired.
- A renewal request is made through the nebulaSUITE application, the RA Operator verifies the request if the defined values and documentation are correct and no variations have occurred, the renewal is approved and the certificate is issued

If any information regarding the subscriber or natural person identified in the certificate has changed, the new information is suitably recorded and complete authentication is performed in accordance with the provisions of this section 3.2.

The renewal of the web authentication certificates will be carried out using the same technique as the initial identification and authentication, which is described in point 3.2.1.3 of this CPS.

3.3.2. Identification and authentication of revocation requests

Before generating a certificate for a subscriber whose certificate has been revoked, vinCAsign, or a Registration Authority, will check that the information used to validate the identity and other data of the subscriber and the natural person identified in the certificate are still valid, in which case the provisions of the previous section shall apply.

After revocation, certificates may not be renewed in the following cases:

- If the certificate was revoked due to erroneous issuance to a person other than the person identified in the certificate.
- If the certificate was revoked due to non-authorised issuance by the natural person identified in the certificate.
- If the certificate was revoked for containing erroneous or false information.

If any information regarding the subscriber or natural person identified in the certificate has changed, the new information is suitably recorded and complete authentication is performed in accordance with the provisions of this section3.2.

3.4. Identification and authentication of revocation requests

VinCAsign or a Registration Authority shall authenticate the certificate revocation requests and reports, checking that they come from an authorised person.

The following methods may be used to perform this check:

- The sending of a revocation request by the subscriber or by the natural person identified in the certificate, by means of the NEBULA electronic platform for managing the life cycle of the certificates.
- The sending of an electronically signed revocation request by the subscriber or the natural person identified in the certificate.
- By going in person to an office of the subscribing company, entity or organisation.
- Other means of communication, such as telephone, when vinCAsign considers that there are reasonable guarantees as to the identity of the party requesting the revocation.

3.5. Authentication of suspension requests

Not applicable, as VINCASIGN does not suspend certificates.

4. Certificates' life cycle operation requirements

4.1. Certificate issuance request

4.1.1. Legitimisation for requesting issuance

4.1.1.1. Corporate certificates

The public or private entity, company or organisation in question must sign a certification services provision agreement with vinCAsign.

Also, prior to the issuance and delivery of a certificate, there must be a request for certificates in a specific certificate application sheet document, which may be in electronic format via the NebulaCERT platform.

When the applicant is a person other than the subscriber, there must be an authorization from the subscriber for the applicant to make the application, which is legally implemented through a certificate application form signed by the applicant on behalf of the entity, company or organization under public or private law, which may be in electronic format through the NebulaCERT platform.

4.1.1.2. Individual certificates

The individual subscriber makes a request, which is legally instrumented through a certificate request form signed by the individual subscriber that can be in electronic format through the NebulaCERT platform.

4.1.1.3. Web authentication certificates

The entity, company or organisation under public or private law concerned must sign a contract for the provision of certification services with vinCAsign.

Likewise, before the issue and delivery of a certificate, there must be a request for certificates in a specific certificate request sheet document, which may be in electronic format through the NebulaCERT platform.

When the applicant is a person other than the subscriber, there must be an authorisation from the subscriber so that the applicant can make the request, which is legally implemented by means of a certificate request sheet signed by the applicant on behalf of

the public or private law entity, company or organisation, which may be in electronic format through the NebulaCERT platform.

The request for certificates is made through the NebulaCERT platform and will be carried out by a previously authorised person.

VinCAsign will record the checks and verifications made.

4.1.1.3.1. Electronic Site certificates

This type of certificate is intended only for entities belonging to the public sector.

The applicant must be previously authorised to apply for this type of certificate: to do so, he or she must attach to the application the document of appointment or assumption of the position of responsibility that accredits it, or the authorisation of the person responsible, in electronically signed pdf format. In addition, the applicant must submit the reference of the Official Journal where the creation of the Electronic Site is published, and indicate:

- Name of the Electronic Site
- Identification of the rule of creation (Official Journal and date of publication)
- url of the Electronic Site
- Holder of the Electronic Site

VinCAsign will check the data incorporated in the application, prior to its approval

4.1.1.3.2. OV and EV SSL Certificates

To verify the identity of the applicant, it depends on:

1. If the applicant is a legal entity: its existence, name, address and country of the organization are verified. This can be done in the following way,
    - Private entity: The existence of the organization will be verified (name and NIF). This will be done by consulting the official register (Commercial Register, Register of Associations, National Chamber of Commerce, or by consulting a reliable and updated database of a third party, or a reliable source such as Legal Entity Identifier -LEI-). A signed document issued by an official registry 825 days prior to the issuance of the certificate will be accepted, as well as notarization or public official certification.

      The applicant's capacity to represent him/her will be verified by consulting the corresponding public registry, a signed document issued by an official registry 825 days before the certificate is issued, as well as notarization or certification by a public official. It will be verified that the entity is operational by its physical location where it carries out its activity, online consultation of a reliable database such as LEI, or notarial certificate.

- Public government entity. The existence of the organisation will be verified (name and NIF). This will be done by consulting the official register, consulting a reliable source such as LEI. A signed document issued by an official registry 825 days prior to the issuance of the certificate will be accepted, as well as notarization or public official certification.

  The applicant's capacity to represent him/her will be verified by consulting the corresponding public registry, a signed document issued by an official registry 825 days before the certificate is issued, as well as notarization or certification by a public official.

  It will be verified that the entity is operational by its physical location where it carries out its activity, online consultation of a reliable database such as LEI, or notarial certificate.
- Commercial entity (any other not reflected in the concepts of private entity, public entity, non-commercial entity) The existence of the organisation will be verified (name and NIF). This will be done by consulting the official register. For professional associations, the information in the association's Statutes of creation and its publication in the BOE, as well as the CIF, will be verified. A signed document issued by an official register 825 days before the certificate is issued will be accepted, as well as certification by a notary or public official.

  The applicant's capacity to represent him/her will be verified by consulting the corresponding public register, an official appointment document issued by the General Meeting, as well as the notarial or civil servant's certification.

  It will be verified that the entity is operational by its physical location where it carries out its activity, online consultation of a reliable database such as LEI, or notarial certificate.
- Non-commercial entities (NGOs.): The existence of the organisation will be verified (name and tax number). It will be verified by means of a document of incorporation or by consulting a reliable source such as Legal Entity Identifier (LEI)

  It will be verified that the entity is operational by its physical location where it carries out its activity, online consultation of a reliable database such as LEI, or notarial certificate.

- Trade name or trademark: It will be verified by means of a document from the official registry that certifies the registration of the trademark or trade name as well as its validity of use, or its online consultation in the official registers.

  It will be verified that the entity is operational by its physical location where it carries out its activity, online consultation of a reliable database such as LEI, or notarial certificate.

2. If the applicant is a natural person: the name, address and country are verified using one of the following means,
    - A copy of his/her identity card, where the name and address of the applicant are verified.
    - If the address to be included in the certificate is different from the one on the identity card, a bank statement or electricity bill or a certificate of registration will be requested where the person is associated with the address to be included.

4.1.1.3.3. Verification of control over the domain name

For web authentication certificates (Electronic Site and SSL), before their issuance, vinCAsign will verify that the applicant has control over the domain for which the certificate is requested. The verification will be done using one of the following methods (at the applicant's choice):

A) Sending mail with a random code to an automatically constructed address using a generic mail "admin", "postmaster", "hostmaster", "administrator", plus @ and domain name for which the web authentication certificate is requested. The applicant must reply to the email indicating which code he has received.

B) DNS modification: when the request is made, vinCAsign automatically generates a value associated to a DNS field, which the applicant will have to modify in the DNS record (in the CNAME, TXT or CAA field). VinCAsign will check this modification.

C) Web modification: a unique numerical value associated with a specific entry within the domain being requested is generated and sent to the contact requesting the certificate, so that they can introduce it. VinCAsign will check this entry.

4.1.2. Registration procedure and responsibilities

vinCAsign receives requests for corporate certificates, made by public or private law entities, companies or organisations, and requests for individual certificates made by individual subscribers, as well as requests for web authentication certificates.

The requests are instrumented by means of a document in electronic format, completed, in the corporate certificates by the entity, company or organisation of public or private law, or in the individual certificates by the individual subscriber, or by its applicant (whether a natural or legal person) in the web authentication certificates, through the NEBULACERT platform, whose addressee is vinCAsign, which will include the data of the persons to whom the certificates will be issued. The request will be made by the operator authorised by the subscriber or Registration Entity (certification manager) and who has been identified in the contract between this subscriber or Registration Entity and vinCAsign.
The request must be accompanied by documentation justifying the identity and other circumstances of the natural person identified in the certificate, in accordance with that established in section 3.2.4. It must also be accompanied by a physical address, or other data, that allows the natural person identified in the certificate or in the request for the web authentication certificates to be contacted.

4.2. Processing of certification requests

4.2.1. Performance of identification and authentication

Once a certification request has been received, vinCAsign checks that the request is complete, precise and duly authorised before processing it.

If these checks are satisfactory, vinCAsign verifies the information provided, including the aspects described in section 3.2

In the case of a qualified certificate, the documentation supporting the approval of the application must be kept and duly recorded with guarantees of security and integrity for

a period of 15 years from the expiry of the certificate, even in the event of early loss of validity due to revocation. This documentation can be kept safely through the NebulaCERT platform.

4.2.2. Approval or rejection of requests

If the data is verified correctly, vinCAsign must approve the certificate request and proceed to issue and deliver it.
If the verification indicates that the information is not correct, or if it is suspected that it is not correct or that it could affect the reputation of the Certification Authority or of the subscribers, vinCAsign will refuse the request, or stop its approval until it has carried out the complementary checks it considers appropriate.
If the additional checks do not reveal the correctness of the information to be verified, vinCAsign will definitively reject the request.
VinCAsign notifies the applicant of the approval or rejection of the application.
VinCAsign may automate the procedures for verifying the correction of the information that will be contained in the certificates, and for approving the applications, through the NebulaCERT platform

4.2.3. Term for resolving requests

vinCAsign deals with certificate requests on a first-come, first-served basis, and a maximum term guarantee can be specified in the certificate issuance agreement.
Requests remain active until they are either approved or rejected.
Before issuing a web authentication certificate (Electronic Headquarters and SSL EV), the application must be approved by someone other than the person who verified the data, differentiating both roles (verifier and approver)

4.2.4. Keys generation in web authentication certificates

Applicants for Web authentication certificates (both Electronic Site and SSL) will generate the key pair on their systems, using their own applications that are compatible with PKI standards, and must be RSA keys with a minimum length of 2048 bits. Normally these applications that are configured with the SSL protocol include tools for generating keys and certificate requests (such as Microsoft's Internet Information Services -IIS-

4.3. Issuance of the certificate

4.3.1. Actions performed by vinCAsign during the issuance process

After approval of the certificate request, the certificate is issued securely and placed at the disposal of the signer for their acceptance, by means of the NebulaCERT platform.

The procedures established in this section also apply to certificate renewals, given that this process involves the issuance of a new certificate.

During the process, vinCAsign:

- Protects the confidentiality and integrity of the registration data in its possession.
- Uses reliable systems and products that are protected against any alteration and that guarantee the technical and, where applicable, cryptographic security of the certification processes they support.
- Generates the key pair by means of a certificate generation procedure securely linked to the key generation procedure.
- Uses a certificate generation procedure that securely links the certificate with the registration information, including the certified public key.
- Ensures that the certificate is issued by systems that are equipped with protection against falsification and that guarantee the confidentiality of the keys during the key generation process.
- Includes the information established in annex I of the Regulation (EU) No. 910/2014 as specified in sections 3.1.1 and 7.1. of this CPS.
- States the date and time at which the certificate was issued.

4.3.2. Issuance of web authentication certificates

The applicant of the web authentication certificate will deliver to vinCAsign a certificate request in PKCS#10 format, as explained in section 4.2.4 of this CPS. VinCAsign will carry

out the technical validation of this request, as well as the validation of the data contained therein.

4.3.3. Notification of issuance to the subscriber

VinCAsign notifies the subscriber and the natural person identified in the certificate that the certificate has been issued.

4.4. Delivery and acceptance of the certificate

4.4.1. VinCAsign's responsibilities

During this process vinCAsign must perform the following actions:

- Definitively accredit the identity of the natural person identified in the certificate, with the collaboration of the subscriber (company, entity or organisation in the corporate certificates and web authentication certificates), and with the Registration Entity (in the individual certificates) in accordance with what is established in the sections 3.2.3 and 3.2.4 of this CPS.
- Deliver to the natural person identified in the certificate with the collaboration of the subscriber (company, entity or organization) or the Registration Entity the certificate delivery and acceptance sheet with the following minimum contents:
    - Basic information on the use of the certificate, especially information on the certification services provider and the applicable Certification Practice Statement, as well as its obligations, powers and responsibilities.
    - Information about the certificate.
    - Recognition by the signer of having received the certificate, and acceptance of the aforementioned information.
    - The signer's obligations.
    - The signer's responsibilities.

  - The method in which the private key and certificate activation data shall be assigned exclusively to the signer, in accordance with the provisions of sections 6.2 and 6.4 of this CPS.
  - The date of the act of acceptance of the certificate
- Obtain the electronic or written signature of the person identified in the certificate. In the option of electronic signature of the delivery sheet, this is done through the services of the NebulaCERT platform.

The subscriber or the Registration Entity collaborates in these processes, having to document the previous acts and keep the mentioned original documents (delivery and acceptance sheets), sending an electronic copy to vinCAsign, as well as the originals when vinCAsign needs access to them. When this documentation is stored electronically, it is done through the services of the NebulaCert platform.

4.4.2. Conduct that constitutes acceptance of the certificate

The natural person identified in the certificate accepts the certificate by signing the acceptance form.
When this acceptance is electronic, it is done through the NebulaCERT platform.

4.4.3. Publication of the certificate

As long as it has been authorised to do so by the natural person identified on certificate, vinCAsign publishes the certificate in the Repository referred to in section 2.1, following the relevant security controls.

4.4.4. Notification of issuance to third parties

VinCAsign does not make any notifications of issuance to third parties.

4.5. Use of the key pair and the certificate

4.5.1. Use by the signer

VinCAsign obliges the signer to:

- Provide vinCAsign with full suitable information, in accordance with the requirements of this Certification Practice Statement, especially as regards the registration process.
- Give their prior consent for the issuance and delivery of a certificate.
- Use the certificate in accordance with the provisions of section 0 of this CPS.
- When the certificate is to be used together with an QSCD, acknowledge its capacity to produce qualified electronic signatures; that is, ones which are equivalent to handwritten signatures, as well as other types of electronic signature and information encryption mechanisms.
- Be particularly diligent in safeguarding their private key in order to avoid non-authorised use, in accordance with the provisions of sections 6.1, 6.2 and 6.4 of this CPS.
- Notify vinCAsign and any person who they believe may rely on the certificate, without undue delay:
    - If their private key is lost, stolen or potentially compromised.
    - If they lose control over their private key as a result of the activation data (e.g. the PIN code) becoming compromised, or for any other reason.
    - Of any errors or changes in the content of the certificate that the subscriber is aware of or could be aware of.
- Cease to use the private code after expiry of the period indicated in section 6.3.2 of this CPS.
- Do not use the private key in case of: compromise of said key; revocation or commitment of the CA keys.

4.5.2. Use by the Subscriber or the Registry Entity

4.5.2.1. Obligations of the corporate subscriber

VinCAsign contractually binds the corporate and web authentication subscriber to:

- Provide the Certification Authority with complete and adequate information, in accordance with the requirements of this Certification Practice Statement, especially regarding the registration procedure.
- Express their consent prior to the issue and delivery of a certificate.
- Use the certificate in accordance with the provisions of section 1.4. of this CPD.
- Communicate to vinCAsign and to any person that the subscriber believes can trust the certificate, without unjustifiable delay:
    - The loss, theft or potential compromise of its private key.
    - Inaccuracies or changes in the content of the certificate known or likely to be known to the corporate subscriber.
- Transfer to the natural persons identified in the certificate the fulfilment of their specific obligations, and establish mechanisms to guarantee effective fulfilment of these.
- Not to monitor, manipulate or perform acts of reverse engineering on the technical implementation of the vinCAsign certification services, without prior written permission.
- Not to compromise the security of the certification services of the vinCAsign certification services provider, without prior written permission.

4.5.2.2. Obligations of the individual subscriber

VinCAsign contractually binds the individual subscriber to:

- Provide the Certification Authority with full suitable information, in accordance with the requirements of this Certification Practice Statement, especially as regards the registration process.
- Give their prior consent for the issuance and delivery of a certificate.
- Use the certificate in accordance with the provisions of section 0 of this CPS.
- Notify vinCAsign and any person who the subscriber believes may rely on the certificate, without undue delay, of:
    - If their private key is lost, stolen or potentially compromised.
    - Of any errors or changes in the content of the certificate that the subscriber is aware of or could be aware of.

- Not monitor, manipulate or perform reverse engineering on the technical implementation of the vinCAsign certification services without prior written permission.
- Not compromise the security of the certification services of the vinCAsign certification services provider without prior written permission.
- Take responsibility for:
  - That all statements made in the application are correct.
  - That all informations provided and contained in the certificate are correct.
  - That the certificate is used exclusively for legal and authorized uses, in accordance with this Certification Practice Statement.
  - That no unauthorized person has ever had access to the certificate's private key, and that he or she is solely responsible for damages caused by his or her failure to comply with the duty to protect the exclusive control of access to the private key.
  - That he/she is an end recipient and not a certification service provider, and that he/she will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other form of certified public key), Certificate Revocation List, certification service provider designation, or on any other circumstances.

4.5.2.3. Obligations of the Registration Entity

VinCAsign contractually binds the Registration Entity to:

- To provide the Certification Authority with complete and adequate information, in accordance with the requirements of this Certification Practice Statement, especially with regard to the registration procedure.
- Communicate to vinCAsign without unjustifiable delay:
  - The loss, theft or potential compromise of the private key.
  - Inaccuracies or changes in the content of the certificate that you know or could know.
- Transfer to the natural persons identified in the certificate the fulfilment of their specific obligations, and establish mechanisms to guarantee the effective fulfilment of these.
- Not to monitor, manipulate or perform acts of reverse engineering on the technical implementation of the vinCAsign certification services, without prior written permission.

- Not to compromise the security of the certification services of the vinCAsign certification services provider, without prior written permission.

4.5.2.4. Civil liability of the signer

VinCAsign obliges to be accountable for:

- That all statements made in the application are correct.
- All the informations supplied by the signer and contained in the certificate are correct.
- The certificate is used exclusively for legal, authorised uses, in accordance with the Certification Practice Statement.
- No unauthorised persons has ever had access to the private key of the certificate, and that he is solely responsible for the damage caused by his breach of the duty to protect the exclusive control of access to the private key.
- The signer is a subject and not a certification service provider, and that they will not use the private key corresponding to the public key listed on the certificate to sign any certificates (or any other format of certified public key), Certificate Revocation lists, certification services provider certifications, or anything else.

4.5.3. Use by the relying party

4.5.3.1. Obligations of the relying party

VinCAsign obliges the relying party to:

- Seek independent advice on whether the certificate is suitable for the intended use.
- Verify the validity, suspension or revocation of the certificates issued, using information on the status of the certificates.

- Verify all the certificates in the certificate hierarchy before relying on the electronic signature or on any of the certificates in the hierarchy.
- Acknowledge that the validated electronic signatures produced using a Qualified Electronic Signature Creation Device (QSCD) are legally classed as qualified electronic signatures; i.e. they are equivalent to handwritten signatures, and that the certificate allows for the creation of other types of electronic signature and encryption mechanisms.
- Take into consideration any limits on the use of the certificate, whether in the certificate itself or in the relying party agreement.
- Take into consideration any precaution established in a contract or other instrument, regardless of its legal status.
- Not monitor, manipulate or perform reverse engineering on the technical implementation of the vinCAsign certification services without prior written permission.
- Not compromise the security of the vinCAsign certification services without prior written permission.

4.5.3.2. Civil liability of the relying party

VinCAsign contractually obliges the relying party to confirm that:

- It has enough information to take an informed decision as regards whether or not to rely on the certificate.
- It is the only party responsible for deciding whether or not to rely on the information contained in the certificate.
- It will be the only party responsible if it fails to comply with its obligations as a relying party.

4.6. Renewal of certificates

Certificate renewal requires the renewal of keys, for which purpose the provisions of section 4.7 of this CPS must be adhered to.

4.7. Renewal of keys and certificates

4.7.1. Reasons for renewing keys and certificates

Current certificates can be renewed by means of a specific, simplified request procedure for the purpose of ensuring the continuity of the certification service. When this procedure is done electronically, the NebulaCERT platform is exclusively used

4.7.2. Legitimisation for requesting renewal

Prior to the issuance and delivery of a renewed certificate, a certificate renewal request must be made ex officio or on the request of the interested party.

Likewise, for corporate certificates, an authorisation from the subscriber is envisaged so that the applicant can make the application, which is legally instrumented by means of a certificate renewal sheet signed by the company, entity or organisation.

For its part, vinCAsign informs subscribers and signatories requesting the renewal, of the existence, if any, of new CPS, PDS or other legal documents.

4.7.3. Renewal request procedures

4.7.3.1. Making the request

VinCAsign, in relation to corporate certificates, receives requests for the renewal of certificates, made by public or private law entities, companies or organisations.

VinCAsign, in relation to individual certificates, receives requests for the renewal of certificates, made by the certificate holders.

There is a document, either on paper or in electronic format, concerning the request for renewal of certificates, which will include the details of the persons to whom the certificates will be issued.
When it is in electronic format, the request is made exclusively through the NebulaCERT platform.

4.7.3.2. Performance of identification and authentication functions

Once a certification request has been received, vinCAsign checks that the request is complete, precise and duly authorised before processing it.

4.7.3.3. Approval or rejection of requests

If the data is correctly verified, vinCAsign must approve the request for renewal of the certificate (if the certificate has not yet expired, it must be revoked in order to approve the issuance of the new certificate or otherwise, this approval will be made on the same day of the expiration of the current certificate) and proceed to its issuance and delivery.

VinCAsign notifies the requesting party of the approval or rejection of the request.

VinCAsign may automate the processes used to verify the information to be contained in the certificates and to approve the requests.

4.7.3.4. Term for resolving requests

VinCAsign deals with certificate renewal requests by order of arrival within a reasonable time period not exceeding the expiration date of the certificates to be renewed, and a guarantee regarding the maximum allowed period may be specified in the certificate issuance agreement.
Renewal requests remain active until they are either approved or rejected.

4.7.4. Notification of issuance of the renewed certificate

VinCAsign notifies the subscriber and the natural person identified in the corporate certificate, and the subscriber of the individual certificate, of the issue of the certificate.

4.7.5. Conduct that constitutes acceptance of the certificate

The certificate is accepted by signing, in writing or electronically, the delivery and acceptance sheet in the presence of the certification officer of the public or private law entity, company or organisation or Registry Entity.
When the signature is produced electronically, this is done through the NebulaCERT platform.

4.7.6. Publication of the certificate

VinCAsign publishes the renewed certificate in the repository referred to in section 2.1 of this CPS, in accordance with the relevant security controls.

4.7.7. Notification of issuance to third parties

VinCAsign does not make any notifications of issuance to third parties.

4.8. Modification of certificates

Modification of certificates, except for modification of the certified public key, which is considered a renewal, will be treated as a new issue of a certificate, and sections 4.1, 4.2, 4.3 and 4.4 of this CPD will apply.

4.9. Revocation of certificates

4.9.1. Reasons for revoking certificates

vinCAsign revokes a certificate when any of the following causes are present:

1) Circumstances that affect the information contained in the certificate:
   a) Modification of any of the data contained in the certificate, after issuance of the corresponding certificate including the modifications.
   b) If it is discovered that any of the data contained in the certificate request are incorrect.
   c) If it is discovered that any of the data contained in the certificate are incorrect.
2) Circumstances that affect the security of the key or certificate:
   a) If the private key, the infrastructure or the systems of the certification services provider that issued the certificate are compromised, and if this affects the reliability of the certificates issued as from the moment said event occurs.
   b) A breach by vinCAsign of the certificate management procedure requirements contained in this Certification Practice Statement.
   c) If the security of the key or issued certificate is compromised or suspected to be compromised.
   d) Non-authorised access or use by a third party of the private key corresponding to the public key contained in the certificate.
   e) The irregular use of the certificate by the natural person identified therein, or lack of due diligence in safeguarding the private key.
3) Circumstances affecting the subscriber of the individual certificate or the natural person identified in the corporate certificate:
   a) Termination of the legal relationship between vinCasign and the subscriber (corporate or individual) for the provision of services.
   b) Modification or expiration of the underlying legal relationship or cause that led to the issuance of the certificate to the natural person identified therein.
   c) Breach by the certificate requester of the pre-established requirements for requesting certificates.
   d) Breach by the corporate or individual subscriber, or by the person identified in the certificate, of his obligations, responsibilities and guarantees, established in the corresponding legal document or in this CPS.
   e) The supervening incapacity or death of the signatory of the corporate certificate or of the holder of the individual certificate.
   f) In corporate certificates, the extinction of the legal entity subscribing to the certificate, as well as the end of the subscriber's authorisation to the key

holder or the end of the relationship between the subscriber and the person identified in the certificate

g) A request by the subscriber to revoke the certificate, in accordance with the provisions of section 3.4 of this CPS.

4) Other circumstances:

a) Termination of the certification service of the Víntegris Certification Authority, in accordance with the provisions of section 5.8 of this CPS.

b) Use of the certificate, on a continuous basis, that is harmful to vinCAsign. Certain types of use are considered to be harmful based on the following criteria:

- The nature and number of complaints received.
- The identity of the entities that make complaints.
- The relevant legislation applicable at each moment.
- The response of the subscriber or person identified in the certificate to the complaints received.

c) By judicial or administrative decision ordering its revocation.

d) For any other reason contained in this CPS.

4.9.2. Legitimisation for requesting revocation

Can request the revocation of a certificate:

- The natural person (signatory) identified in the corporate certificate.

- The subscriber of the corporate or web authentication certificate, through the person responsible for the certification service.

- The subscriber of the individual certificate, by means of the Registration Entity.

- Any person who has knowledge of any of the causes mentioned in section 4.9.1.

4.9.3. Revocation request procedures

The corporate subscriber or an individual subscriber who needs to revoke a certificate must send a request to vinCAsign.

The revocation request can be requested through the NebulaCERT platform or by e-mail to info@vincasign.net or through the form available at

- https://www.vincasign.net/ (in Spanish)

- https://www.vincasign.net/ (in English)

- https://www.vincasign.net/ (in Catalan)

The revocation request must contain the following information:

- The date of the revocation request.
- The identity of the subscriber.
- A detailed description of the reason for requesting the revocation.
- The name and title of the person requesting the revocation.
- The contact details of the person requesting the revocation.

The request must be authenticated by vinCAsign, in accordance with the provisions of section 3.4 of this policy, before proceeding with the revocation.
VinCAsign may include any other requirement for confirmation of revocation requests[10].

The revocation service can be accessed on the vinCAsign website, at: https://www.vincasign.net.

If the recipient of a revocation request by a natural person identified in the certificate is the subscribing entity or Register Entity, once the request has been authenticated, the pertinent request must be sent to vinCAsign.

The revocation request shall be processed as soon as it is received and the subscriber (corporate or individual) and, where applicable, the natural person identified in the certificate shall be informed of the change of status of the revoked certificate.

VinCAsign will not reactivate the certificate once it has been revoked.

[10] App. REV-6.2.4-01, c) of ETSI EN 319 411-1

Both the revocation management service and the consultation service are considered critical services and are included in the Contingency Plan and the Business Continuity Plan of vinCasign.

4.9.4. Time period for requesting revocation

Revocation requests shall be sent immediately, as soon as the cause of revocation is known on a time basis of 24x7 and shall not exceed 24 hours[11].

4.9.5. Time period for processing revocation requests

Revocation requests shall be processed as soon as they are received, on a time basis of 24x7.

4.9.6. Obligation to consult certificate revocation information

Relying parties must check the status of those certificates on which they wish to rely.

One way the status of certificates is checked, is performing consult to OCSP Service of VinCAsign.
VinCAsign validates the status of all certificates before a signature is made.
The Certificate Revocation Lists are published in the Repository of the Víntegris Certification Authority as well as well as at the following web addresses, which are indicated on the certificates:

For certificates issued by the qualified CA “vinCAsign nebulaSUITE2 Authority”

- http://crl1.vincasign.net/canebula2.crl
- http://crl2.vincasing.net/canebula2.crl

For certificates issued by the CA “vinCAsign nebulaSUITE3Authority”

[11] Ap REV-6.2.4-01, d) de ETSI EN 319 411-1

- http://crl1.vincasign.net/canebula3.crl
- http://crl2.vincasing.net/canebula3.crl

For certificates issued by the qualified CA "vinCAsign nebulaSUITE4 Authority"

- http://crl1.vincasign.net/canebula4.crl
- http://crl2.vincasing.net/canebula4.crl

For certificates issued by the qualified CA "vinCAsign nebulaSUITE5 Authority"

- http://crl1.vincasign.net/canebula5.crl
- http://crl2.vincasing.net/canebula5.crl

The status of the certificates can also be checked by means of the OCSP protocol.

- For certificates issued by Vincasign's CAs
- http://ocsp.vincasign.net

4.9.7. Frequency with which certificate revocation lists (CRLs) are published

VinCAsign issues a CRL at least every 24 hours.

The CRL indicates the moment scheduled for issuance of the next CRL, although, to reflect revocations, another CRL listing new revocations may be issued before this time.

The CRL list must keep the certificate revoked until it expires.

4.9.8. Maximum time period for publishing CRLs

After they are generated, CRLs are published in the Repository within a reasonable period that never exceeds a few minutes.

4.9.9. Availability of online services for checking certificate status

Alternatively, relying parties may check the vinCAsign certificate Repository, which is available 24/7 at the following web address: https://validator.vincasign.net/

To check the last CRL issued on each CA you must download:

For certificates issued by the CA “vinCAsign nebulaSUITE2 Authority”

- http://crl1.vincasign.net/canebula2.crl
- http://crl2.vincasing.net/canebula2.crl

For certificates issued by the Root CA "vinCAsign QUALIFIED Authority".

- http://crl3.vincasign.net/casub.crl
- http://crl4.vincasing.net/casub.crl

For certificates issued by the CA “vinCAsign nebulaSUITE3 Authority”

- http://crl1.vincasign.net/canebula3.crl
- http://crl2.vincasing.net/canebula3.crl

For certificates issued by the CA “vinCAsign nebulaSUITE4 Authority”

- http://crl1.vincasign.net/canebula4.crl
- http://crl2.vincasing.net/canebula4.crl

For certificates issued by the qualified CA “vinCAsign nebulaSUITE5 Authority”

- http://crl1.vincasign.net/canebula5.crl
- http://crl2.vincasing.net/canebula5.crl

In the event of failure of the systems for checking certificate status due to causes beyond the control of vinCAsign, the latter shall make its best efforts to ensure that the service is resumed as soon as possible and at most within a period of 1 day.

VinCAsign supplies information to relying parties regarding the functioning of the certificate status information service.

Certificate status checking services are free of charge[12].
VinCAsign, keeps the expired certificates in the OCSP service for a period of 5 years.

VinCAsign keeps available the information of the revocation status after the validity period of the certificate[13] through the OCSP service. This availability is maintained in case of termination of PKI services by VinCAsign, transferring this obligation to another provider.

[12] Ap 6.3.10 de ETSI EN 319 411-2

[13] Ap 6.3.10.b) de ETSI EN 319 411-2,

In the event that the CA issues the last CRL, the "nextUpdate" field should be set[14] to "99991231235959Z", as defined in IETF RFC 5280[15]

4.9.10. Obligation to consult the services for checking certificate status

It is mandatory to check the status of the certificates before relying on them.

4.9.11. Other ways of checking certificate revocation information

VinCAsign also provides information on certificate revocation statuses by means of the OCSP protocol. This protocol allows certificate status to be checked online at the following web addresses:

For certificates issued by vinCAsign: http://ocsp.vincasign.net/

4.9.12. Special requirements for compromised private keys

The compromise of the vinCAsign private key is notified to all participants in the certification services, as far as possible, by publishing this fact on the vinCAsign website, as well as, if deemed necessary, in other media, including paper.

4.10. Termination of the subscription

Once the certificate's validity period has expired, the subscription to the service will end.

As an exception, the subscriber may continue to subscribe to the service, requesting the renovation of the certificate, giving the prior notice established in this Certification Practice Statement.

[14] Ap 6.3.9 de la ETSI EN 319 411-2 -> Ap CSS-6.3.9-06 de la ETSI EN 319 411-1

[15] Ap 4.1.2.5 (validity) de la IETF RFC 5280

VinCAsign may issue a new certificate ex officio as long as the subscribers maintain said status.

4.11. Services for checking certificate status

4.11.1. Operative features of the services

The services for checking certificate status are provided using a web interface on the website: http://www.vincasign.net.

4.11.2. Availability of the services

The services for checking certificate status are available 24/7 throughout the year, except for the scheduled stoppages.

4.11.3. Optional features

Not stipulated.

4.12. Key escrow and recovery

4.12.1. Policy and practices for key escrow and recovery

VinCAsign does not provide key escrow and recovery services.

4.12.2. Session key encapsulation and recovery policy and practices

Not stipulated.

5. Physical security, management and operational controls

The company Víntegris, which provides support for the certificate management operations of vinCAsign, is subject to the annual validations stipulated in standard ISO/IEC 27001, which regulates the establishment of suitable processes to guarantee correct information security management.

5.1. Physical security controls

VinCAsign has established physical and environmental security controls to protect the resources of the facilities where the systems are installed, the systems themselves and the equipment used for the registration and approval of requests, technical generation of the certificates and management of the cryptographic hardware.

Specifically, it has established a physical and environmental security policy applicable to the services for the generation of certificates and cryptographic devices and the management of revocations includes provisions for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Fire protection measures.
- Failure of the support systems (electric power, telecommunications, etc.).
- Collapse of the structure.
- Floods.
- Anti-theft protection.
- Non-authorised release of equipment, information, media and applications relating to the components used for the services of the certification services provider.

These measures apply to the facilities where the certificates are generated under the full responsibility of vinCAsign, which, from its high-security facilities, provides both main services and contingency services, which are duly audited on a regular basis.

The facilities have preventive and corrective maintenance systems with 24/7/365 service with assistance within 24 hours of notice.

5.1.1. Location and construction of the facilities

Clearly defined security perimeters are established around the services to ensure their physical protection. The quality and solidity of the facilities' construction materials guarantee suitable levels of protection against forceful intrusion. Furthermore, they are located in an area that allows rapid access and has a low risk of natural disasters.

The room in the Data Processing Centre where the cryptographic operations are carried out:

- Has infrastructure redundancy.
- Has several alternative sources of power and cooling in the event of emergency.
- Uses maintenance operations that do not require the Centre to be offline at any time.
- Has 99.982% availability.

VinCAsign has facilities that physically protect the certificate request approval and revocation management services from the danger posed by non-authorised access to the systems or data as well as non-authorised release of data.

5.1.2. Physical access

VinCAsign has three levels of physical security (entrance to the building where the DC is located, access to the DC room and access to the RACK to protect the certificate generation service; access is from the lower to the higher levels.

Physical access to the vinCAsign facilities where the certification processes are performed is limited and protected using a combination of physical measures and procedures. In this way:

- Physical access is limited to expressly authorised personnel. These personnel are identified at the moment they access the building, their access is registered and filed and they are recorded on CCTV.

- The data-processing rooms are accessed using ID card readers and access is managed through a computer system that keeps an automatic log of personnel entering and leaving the rooms.

- To access the rack where the cryptographic processes are located, prior authorisation from vinCAsign must be given to the administrators of the hosting service that have the key to open the cage.

5.1.3. Electricity and air conditioning

VinCAsign's facilities are equipped with voltage stabilisers and an equipment power supply system that is duplicated with a generator.

The rooms that house IT equipment are equipped with temperature control systems with air conditioning.

5.1.4. Exposure to water

The facilities are located in an area with a low risk of floods.

The rooms that house the IT equipment are equipped with a humidity detection system.

5.1.5. Fire prevention and protection

VinCasign's facilities and assets have automatic fire detection and extinction systems.

5.1.6. Data storage

Only authorised personnel have access to stored data.

The most highly classified information is stored in a safe outside of the Data Centre facilities.

5.1.7. Waste management

Both paper and magnetic media are destroyed using methods that ensure the data cannot be recovered.

In the case of magnetic media, the data is formatted, permanently erased or physically destroyed using specialist software that performs at least 3 wipe cycles with variable deletion patterns.

Meanwhile paper media is destroyed using shredders or paper bins specifically for this purpose, the content of which are then destroyed under control conditions.

5.1.8. Off-site backup copy

VinCAsign uses a secure off-site warehouse for storing documents, magnetic and electronic media that are independent from the operations centre.

At least two expressly authorised persons are needed to access, deposit or remove material.

5.2. Procedure controls

VinCasign guarantees that its systems operate securely, and to this end it has established and implemented procedures for those functions that affect service provision.

VinCAsign's personnel perform the relevant administrative and management procedures in accordance with the security policy.

5.2.1. Positions of trust

In accordance with its security policy, vinCAsign has identified the following functions or roles that are classed as positions of trust:

- **Internal auditor:** Responsible for complying with the operational procedures. This is an individual who is external to the Information Systems department. The tasks of the Internal Auditor are incompatible, time-wise, with those of Certification, and are also incompatible with those of Systems. The Internal Auditor reports to both the Operations Management Department and the Technical Management Department.
- **Systems Administrator**: This person is responsible for the correct operation of the certification platform's hardware and software.
- **CA Administrator**: Responsible for the operations to be performed with the cryptographic material or the performance of any operations that involve the activation of the private keys of the certification authorities described in this document, or any of their elements.
- **CA Operator:** This person has joint responsibility with the AC Administrator for safeguarding the cryptographic key activation material, as well as being responsible for CA backup and maintenance operations.
- **Registration Administrator:** Person responsible for approving the certification requests made by the subscriber.
- **Security Officer**: Responsible for coordinating, controlling and ensuring compliance with the security measures set out in the vinCAsign security policies. They are in charge of aspects related to information security: logical, physical, organisational, network, etc.

The people who hold the abovementioned positions are subject to specific background checks and control procedures. These persons shall perform their functions on the basis of the principle of least privilege.

5.2.2. Number of people per task

VinCAsign guarantees that there will be at least two people to perform the functions detailed in the corresponding Certification Policies, and particularly for handling the root and intermediate Certification Authority key storage device.

5.2.3. Identification and authentication of each role

The people assigned to each role are identified by the internal auditor, who insures that each person performs the operations with which they are entrusted.

Each person controls only those assets required for their role, thus ensuring that nobody can access non-assigned resources.

Resources are accessed, depending on the assets, using cryptographic cards and activation codes.

5.2.4. Roles that must be performed by more than one person

The following tasks must be performed by at least two people:

- Issuance and replication of certificates and access to the Repository.
- Generation, issuance and destruction of the Certification Authority's certificates.
- Start-up of the Certification Authority.

5.2.5. PKI management system

The PKI system consists of the following modules:

- Subordinate Certification Authority management component/module
- Registration Authority component/module
- Request management component/module
- Key management component/module (HSM)
- Database component/module

- CRL management component/module
- OCSP service component/module

5.3. Personnel checks

5.3.1. Background, qualifications, experience and authorisation

All personnel in positions of trust must have spent at least one year working in the production centre and have a permanent employment contract.

All our personnel are qualified and have been properly trained to perform the tasks assigned to them.

Personnel in positions of trust do not have any personal conflicts of interest that could affect the performance of their duties.

VinCAsign ensures that the registry personnel can be trusted to perform the registration tasks.

The Registry Administrator has completed a training course on request validation.

In general, vinCasign will remove any employee from positions of trust if it becomes aware they have committed any illegal act that could affect the performance of their duties.

VinCasign will not place employees in management positions or positions of trust if they are not suitable for the role, especially if they have a criminal record. For this reason, background checks are run on all potential employees, **within the bounds of applicable legislation**, regarding the following:

- Academic experience including alleged degree.
- Previous professional experience, over a period of up to 5 years, including following up references.
- Credit rating.

5.3.2. Background check procedures

Before hiring any individual or before they begin working for the company, vinCAsign performs the following checks:

- The professional positions held over the previous few years.
- Professional references.
- Academic experience and purported qualifications.

VinCAsign carries out these checks in strict compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
The checks are repeated on a suitable periodic basis.

All the checks are performed within the bounds of applicable legislation. The following may be causes for rejecting a candidate for a position of trust:

- If the candidate gives false information in the job application.
- Professional references that are very negative or cast doubt over the candidate's trustworthiness.

Candidates are informed in the job application of the need to undergo background checks and warned that failure to agree with said checks will result in their application being rejected.

5.3.3. Training requirements

VinCAsign trains personnel in positions of trust until they achieve the necessary qualifications, keeping records of the training activity.

The training programmes are updated and improved on a regular basis.

Training includes at least the following content:

- Security principals and mechanisms in the certification hierarchy, as well as the user environment of the person receiving training.

- The tasks to be performed by the person.
- VinCAsign security policies and procedures. Use and operation of the installed machines and applications.
- Management and processing of incidents and security breaches.
- Business continuity and emergency procedures.
- Management and security procedures for processing personal data.

5.3.4. Training update requirements and frequency

VinCAsign updates it staff training courses in accordance with needs and frequently enough to ensure employees can perform their duties competently and satisfactorily, especially when significant modifications are made to the certification tasks.

5.3.5. Staff turnover sequence and frequency

Not applicable.

5.3.6. Penalties for non-authorised actions

VinCAsign uses a system of penalties for the parties responsible for non-authorised actions. This system adheres to applicable labour law and has been created in line with the system of penalties set out in the collective bargaining agreement applicable to the company's personnel.

The disciplinary actions include suspension and dismissal of personnel responsible for harmful, non-authorised actions, depending on the seriousness of said actions.

5.3.7. Requirements for hiring personnel

Before the commencement of employment, the personnel hired to hold positions of trust are required to sign the confidentiality clauses and operational requirements used by

vinCasign. Any actions that compromise the security of the processes accepted could, subsequent to assessment, result in dismissal.

In the event that all or part of the certification services are performed by a third party, the controls and provisions set out in this section and other sections of the CPS shall be applicable and shall be complied with by the third party operating the certification services, although the certification authority shall at all times be responsible for effective execution of the services. These aspects are specified in the legal document used to agree to the provision of certification services by a third party other than vinCAsign.

5.3.8. Supply of documentation to personnel

The certification services provider shall supply its personnel with the documents they need at each moment in order to perform their work in a competent and satisfactory manner.

5.4. Security audit procedures

VinCAsign is subject to the annual validations of standard ISO/IEC 27001 which regulates the establishment of suitable processes to guaranteeing correct security management in IT systems that support electronic certification services.

5.4.1. Types of event recorded

VinCasign keeps a log of at least the following events related to the security of the entity:

- Start-up and shut-down of the system.
- Attempts to create, erase or establish passwords or change privileges.
- Attempts to start and end sessions.
- Non-authorised attempts to access the CA system via the network.
- Non-authorised attempts to access the filing system.
- Physical access to the logs.
- Changes to the system's configuration and maintenance.

- CA application logs.
- Start-up and shut-down of the CA application.
- Changes to the details of the CA and/or its keys.
- Changes in the creation of certification policies.
- Generation of own keys.
- Creation and revocation of certificates.
- Records on the destruction of media containing keys and activation data.
- Events related to the life cycle of the cryptographic module, such as receipt, use and uninstallation of the module.
- Routers and Firewalls activity[16].
- The key generation ceremony and key management databases.
- Physical access logs.
- System configuration maintenance and changes.
- Personnel changes.
- Commitment and discrepancy reports.
- Records of the destruction of material containing information on keys, activation data or the personal information of the subscriber, in the case of individual certificates, or that of the natural person identified in the certificate, in the case of organisation certificates.
- Possession of activation data for operations with the private key of the Certification Authority.
- Full reports of the physical intrusion attempts in the infrastructures that support the issuance and management of certificates.

The log entries include the following information:

- Time and date of the entry.
- In automated records, the serial number or sequence of the entry.
- Identity of the entity entering the records.
- Type of entry.

5.4.2. Processing frequency of audit logs

[16] Ap OVR-6.4.5-02 de ETSI EN 319 411-1

VinCAsign checks its logs when a system alert is generated due to an incident.

The process for checking the audit logs consists of looking at the logs that show the system has not been manipulated, briefly inspecting all the log entries and performing a more detailed inspection of any alert or irregularity found in the logs. All the actions performed as part of the audit checks are recorded.

VinCAsign has a system that makes it possible to guarantee:

- Sufficient space for storing logs.
- That log files are not overwritten.
- That the information saved includes at least: the type of event, time and date, user that executes the event, and the result of the operation.
- The log files are saved in structured files that can be incorporated into a DB for subsequent analysis.

5.4.3. Storage period of audit logs

VinCAsign stores log data for at least 15 years.

5.4.4. Protection of audit logs

The system logs:

- They are protected against possible tampering, erasure or deletion[17] by signing the files that contain them.
- Are stored in fireproof devices.
- Are protected by being stored in facilities external to the centre where the CA is located.

Access to log files is restricted to authorised persons. Furthermore, the devices are handled at all times by authorised personnel.

[17] Ap REQ-7.10-08 de ETSI EN 319 401

There is an internal procedure that describes the management processes for the devices containing the audit log data.

5.4.5. Backup copy procedures

VinCAsign has a suitable backup procedure to ensure that, in the event of loss or destruction of important files, the corresponding backup copies of the logs will be available for a short period of time.

VinCAsign uses a secure audit log backup procedure, making a weekly backup copy of all the logs in an external device. Additionally, a copy is kept in an external centre.

5.4.6. Location of the audit log accumulation system

The event audit information is automatically collected internally by the operating system, the network communications and the certificate management software, as well as through data generated manually and stored by duly authorised personnel. All these features make up the audit log accumulation system.

5.4.7. Notification of audit events to the party that has triggered the event

When the audit log accumulation system registers an event, it is not necessary to send notification to the individual, organisation, device or application that triggered the event.

5.4.8. Vulnerability analysis

Vulnerability analysis is covered by the vinCAsign audit processes.
Vulnerability analyses must be executed, revised and checked by means of an examination of these monitored events. These analyses are carried out on a quarterly basis.

The auditing data of the systems are stored so they can be used to investigate any incidents and pinpoint vulnerabilities.

5.5. Data archives

VinCAsign guarantees that all information pertaining to certificates shall be preserved for a suitable period of time, as established in section 5.5.2 of this policy.

5.5.1. Types of records archived

The following documents involved in the certificate life cycle are stored by vinCAsign (or by the registration authorities):

- All the system's audit data (PKI, TSA and OCSP)
- All the data relating to the certificates, including the agreements with the signers and data relating to their identity and location.
- Certificate issuance and revocation requests. including all reports relating to the revocation process.
- -Any specific elections that the signatory or subscriber may make during the subscription agreement[18].
- The type of document presented in the certificate request.
- The identity of the Registration Authority that accepts the certificate request.
- The unique ID number provided by the previous document.
- All the certificates issued or published.
- CRLs issued or registered on the status of the generated certificates.
- The key log.
- The communications between the elements of the PKI.
- Certification Policies and Practices
- All the audit data identified in section 5.4
- Information on certification requests.
- Documentation provided to justify certification requests.
- Certificate life cycle information.

[18] Ap OVR-6.4.5-04, d) de ETSI EN 319 411-1

VinCAsign is responsible for correctly archiving all this material.

5.5.2. Log storage period

VinCAsign archives the abovementioned records for a period of 15 years.

5.5.3. Protection of archives

VinCAsign projects its archives so that only duly authorised persons may obtain access to them. Archives are protected from being viewed, modified, erased or tampered with in any other way through storage in a reliable system.

VinCAsign ensures its archives are correctly protected by assigning qualified personnel to the tasks of handling and storage in fireproof security boxes and external facilities.

5.5.4. Backup copy procedures

VinCAsign uses an external storage centre to guarantee availability of the copies of the electronic file archives. The physical documents are stored in secure places with access restricted to authorised personnel.

VinCAsign makes at least two incremental backup copies of all its electronic documents on a daily basis, as well as full weekly backup copies for cases of data recovery.

Furthermore, vinCAsign (or the organisations that perform registration) keeps copies of the paper documents in a secure place other than the facilities of the certification Entity.

5.5.5. Time and date seal requirements

The records are dated with a reliable source via NTP from the ROA (Royal Institute and Observatory of the Armada).

VinCAsign has a procedure that describes the time configuration of the equipment used to issue certificates.

This information does not need to be digitally signed.

5.5.6. Location of the archiving system

VinCAsign as a centralised system to collect information on the activity of the equipment involved in the certificate management service.

5.5.7. Procedures for obtaining and validating archive information

VinCAsign has a procedure that describes the process used for checking that the archived information is correct and accessible.

5.6. Renewal of keys

The CA's key is changed for a new one prior to expiry. The old CA and its private key shall only be used to sign CRLs as long as there exist active certificates issued by said CA. A new CA will be generated with a new private key and a new DN.

The subscriber's keys are changed by performing a new issuance process.

5.7. Compromised keys and disaster recovery

5.7.1. Procedures for managing incidents and compromised security

Security copies of the following information are stored by vinCAsign in off-site facilities, to be used in the event of compromised security or disaster: technical data for certificate requests; audit data; and database records of all the certificates issued.

The backup copies of vinCAsign's private keys are generated and maintained in accordance with the provisions of section 6.2.4

5.7.2. Corruption of resources, applications or data

When an event occurs that causes the corruption of resources, applications or data, security shall be notified of the incident and the relevant management procedures shall be implemented for scaling, investigation and response. If necessary, the vinCAsign processes for compromised keys or disaster recovery shall be implemented.

5.7.3. Compromise of the entity's private keys

If there is a suspicion or knowledge that vinCAsign has been compromised, the key compromise procedures shall be activated. These shall be managed by a response team that shall assess the situation and develop a plan of action to be executed under the approval of the Certification Authority's management.

If the private key of vinCAsign is compromised, it may be the case that the status of the certificates and revocation processes using this key may not be valid[19].

VinCAsign has developed a Contingency Plan to recover critical systems, if necessary, in an alternative data centre.

If the root key is compromised, this must be dealt with as a separate case within the business continuity and contingency process. If the keys need to be replaced, this incident

[19] Ap OVR-6.4.8-13 de ETSI EN 319 411-1

will affect their recognition by the different applications and private and public services. The recovery of the effectiveness of the keys in business terms will depend mainly on how long these processes take. The business continuity and contingency document deals with the purely operational terms for the availability of the new keys, but not their recognition by third parties.

Any failure to achieve the goals set by this Contingency Plan will be treated as reasonably unavoidable unless such failure is due to a breach of the AC's obligations to implement such processes.

5.7.4. Business continuity after a disaster

VinCAsign will re-establish the critical services (Revocation and publication of revoked certificates) in accordance with the business continuity and contingency plan, restoring normal operation of said services within 24 hours following a disaster.

There is a Contingency Plan that defines the actions to be carried out, resources to be used and personnel to employ in the event of an intentional or accidental event that depletes or degrades the resources and certification services provided by VINTEGRIS.
The main objectives of the Contingency Plan are:
• To achieve the highest effectiveness of recovery operations through the establishment of three phases:

Evaluation / Activation Phase to detect, evaluate impacts and activate the plan.

Recovery Phase to temporarily and partially restore services until recovery of damages caused in the original system.

Ressumption Phase to restore the system and processes to their normal operation.

• Identify the activities, resources and procedures necessary for the efficient and effective implementation of the three phases
VinCAsign has alternatives, if necessary, for the implementation of the vinCAsign certification systems described in the business continuity plan.

5.8. Termination of the service

VinCAsign guarantees that any possible interruptions experienced by subscribers and third parties as a result of termination of the services of the certification services provider will be minimal and, in particular, guarantees continuous maintenance of the logs required to provide proof of certification in the event of civil or criminal investigation, by means of transfer to a notarial repository.

Before terminating its services, vinCAsign will develop a termination plan that includes the following provisions:

- The necessary funds (through a civil liability insurance policy and provision of own funds) to continue finalising the revocation activities.
- Notification to the Signers/Subscribers/Relying Parties and other CAs with which it holds agreements or any other type of relationship of the termination, giving at least 6 months' notice.
- Revocation of all authorisations to entities subcontracted to act on behalf of the CA in the certificate issuance process.
- Transfer of its obligations regarding the maintenance of the registry information and logs during the period of time indicated to the subscribers and users.
- Destruction or deactivation of the CA's private keys.
- The certificates shall remain active and the validation and revocation system shall remain operational until expiry of all the certificates issued.
- Execution of the tasks needed to transfer the obligations to maintain the registration information and event log archives during the respective time periods indicated to the subscriber and relying parties.
- Communication to the Ministry of Industry, Energy and Tourism in advance a minimum of 2 months, the cessation of activity and the fate of certificates specifying whether the management is transferred and to whom or if their application is extinguished .
- It will also inform the Ministry responsible for opening the qualification of trusted electronic services of any bankruptcy proceedings against vinCAsign as well as any other relevant circumstance that may prevent the continuation of the activity.

6. Technical security controls

VinCAsign uses reliable systems and products that are protected against any alteration and that guarantee the technical and cryptographic security of the certification processes.

6.1. Generation and installation of the key pair

6.1.1. Generation of the key pair

The key pair of intermediate certification entities are created by the root certification entity "vinCAsign Qualified Authority" in accordance with the ceremony procedures of vinCAsign, within the high-security perimeter used for this task.

The activities performed during the key generation ceremony have been recorded, dated and signed by all the individuals participating in the ceremony, in the presence of a Notary or an Auditor. Said records are safeguarded for the purposes of auditing and monitoring for a suitable period determined by vinCAsign.

Devices with certifications FIPS 140 level 3 or Common Criteria EAL 4+ (with the supplement ALC_FLR.1) are used to generate keys for the root and intermediate certification authorities.

vinCAsign QUALIFIED Authority	**4.096 bits**	**25 Y.**
VinCAsign NEBULASUITE2 Authority	4.096 bits	13 years
- End entity certificates	2.048 bits	3 years
Time Stamp Unit	4.096 bits	5 years
VinCAsign NEBULASUITE4 Authority	4.096 bits	13 years
- End entity certificates	2.048 bits	2 years
VinCAsign NEBULASUITE5 Authority	4.096 bits	13 years
- End entity certificates	2.048 bits	2 years

More information can be found on the following web pages: https://policy.vincasign.net

6.1.1.1. Generation of the signer's key pair

The signer's keys can be created by the signer themselves using hardware or software devices authorised by vinCAsign, or they can be created by vinCAsign.

The keys are generated using the RSA public key algorithm, with a minimum length of 2048 bits.
If a secure signature creation device is used, the device used for key generation must be certified in accordance with the requirements of Annex 2 to Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.
To maintain the previous point vinCAsign establishes the internal procedure of "**VinCASIGN Device validity management**".

6.1.2. Private key delivery to the signer

For certificates in a qualified signature creation device, the private key is duly protected inside said device.

For software certificates the signatory's private key is created either in the signature creation device and under the exclusive control of the holder is managed from the Nebulacert platform, or in files with PKCS#12 format, which contain the keys and certificates in properly encrypted files.

6.1.3. Public key delivery to the certificate issuer

The method used to send the public key to the certification services provider is PKCS#10, another equivalent cryptographic test or any other method approved by vinCAsign.

When keys are generated in a QSCD, vinCAsign ensures that the public key that is sent to the certification service provider comes from a pair of keys generated by that QSCD[20].

6.1.4. Distribution of the public key of the certification services provider

Relying parties are informed of vinCAsign's keys, ensuring the integrity of the key and authenticating its source, through publication in the Repository.

Users can access the Repository to obtain the public keys and, additionally, in S/MIME applications, the data message may contain a chain of certificates that are thus distributed to the users.

The certificates of the root and subordinate CAs shall be made available to users on the vinCAsign website.

6.1.5. Key sizes

The length of the keys of the "vinCAsign Qualified Authority" is 4096 bits.

The length of the keys of the subordinate "vinCAsign nebulasuite2 Authority" is 4096 bits.

The certificate keys of the end entity have a length of 2048 bits.

6.1.6. Generation of public key parameters

The public key of the Root and the subordinate CAs, and the certificates of the subscribers, are encoded in accordance with RFC 5280.
The keys of the Root CA and Subordinate CA are created with the RSA algorithm

[20] Ap SDP-6.5.1-03, SDP-6.5.1-04, SDP-6.5.1-05 y SDP-6.5.1-06 de ETSI EN 319 411-2

6.1.7. Public key parameter quality checks

The parameters defined in the 001 cryptographic suite specified in ETSI TS 001 176-1 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms" are used. ModLen=1024 is defined.

- Module Length = 4096
- Key generation algorithm: rsagen1
- Coding method: emsa-pkcs1-v1_5
- Summary cryptographic functions: SHA256.

6.1.8. Generation of keys in computer applications or equipment assets

All the keys are generated in equipment assets, in accordance with section 6.1.1.of this document.

6.1.9. Key usage purposes

The keys of the Certification Authority certificates may be used exclusively for signing certificates and CRLs.

The uses of keys for certificates of final entity for natural persons are exclusively for electronic signature and non-repudiation.

The uses of the keys for the final entity certificates for electronic seals are exclusively for electronic signature, non-repudiation and encryption.

The uses of the keys for web authentication certificates are for digital signature and encryption.

6.2. Private key protection

6.2.1. Cryptographic module standards

In relation to the modules that manage the keys of vinCAsign and electronic signature certificate subscribers, the levels required by the standards mentioned in the previous sections are assured.

6.2.2. Private key (n out of m) multi-person control

A multi-person control is required for the activation of the CA private key. In the case of this CPD, there is a **2 out of 5** person policy for key activation.

The cryptographic devices are physically protected as described in this document.

The CA facilities are equipped with continuous monitoring systems and alarms to detect, record and be able to act immediately on an attempt to access their resources unauthorized and / or irregular.

6.2.3. Private key escrow

VinCAsign does not store copies of the signers' private keys.

6.2.4. Private key backup

VinCAsign makes backup copies of the private keys of the CAs so they can be recovered in the event of disaster, loss or deterioration. Both the generation of the copy and the recovery of the key require the intervention of at least two people.

These recovery files are stored in fireproof cabinets and in the external storage centre.

The subscriber's keys in software can be stored separately from the installation key in an external storage device, for possible recovery in case of emergency.

The signer's keys in hardware cannot be copied and may not leave the cryptographic device.

6.2.5. Private key archival

The private keys of the CAs are archived for a period of **10 years** after issue of the last certificate. They shall be stored in secure fireproof archives and in the external storage centre. At least two people will be required to recover the CA's private key in the initial cryptographic device.

6.2.6. Private key transfer onto the cryptographic module

The private keys are generated directly in vinCAsign's cryptographic production modules.

6.2.7. Storage of the private key on the cryptographic module

6.2.7.1. Storage of the Certification Authorities' private key

The private keys of the Certification Authority are stored in encrypted format in vinCAsign's cryptographic production modules.

6.2.7.2. Storage of the signatory's private key

- Keys generated in Nebula.
  With the start up of the electronic platform NebulaSuite[21] the private keys for the qualified electronic signature and the qualified electronic seal are generated exclusively in the cryptographic[22] hardware provided for this function.

[21] See section 1.3.1.6. nebulacert

[22] See section 6.8.4 Cryptographic hardware for the certificates' keys.).

- Keys generated in other certification authorities and imported into Nebula by the holder.

  With the implementation of the NebulaSuite[23] electronic platform, the private keys of the certificates of signatories/creators of seals of certification authorities other than vinCAsign can be imported by the holder into the NebulaSuite program, in which case they are stored in the cryptographic[24] hardware.

  The aforementioned possibility is only applicable in the case of the advanced electronic signature or the advanced electronic seal and is carried out by the certificate holder himself, so that vinCAsign does not know the corresponding private key. The holder of the certificate should only import it if such action is not prohibited, or can be considered to be prohibited, by the trusted service provider who issued the certificate to be imported.

  Under no circumstances is it possible to import qualified electronic signature or qualified electronic seal private keys into NebulaSuite.

This complies with Article 26(c) of Regulation EU 910/2014, which states that advanced electronic signatures must "have been created using electronic signature creation data that the signatory can use, with a high level of confidence, under his sole control", and Article 36(c) of Regulation EU 910/2014, which states that advanced electronic seals must "have been created using electronic seal creation data that the seal creator can use, with a high level of confidence, under his sole control".

Furthermore, for qualified electronic signatures, this generation of keys by the qualified provider makes it possible to comply with recital 51 of Regulation EU 910/2014, which states that it should be possible for the signatory to entrust qualified electronic signature-creation devices to a third party provided that appropriate procedures and mechanisms are in place to ensure that the signatory has sole control over the use of its electronic signature-creation data and that the use of the device complies with the requirements of qualified electronic signatures.

This reliable subscriber key generation environment, as described in recital 52 of Regulation EU 910/2014, is based on cryptographic hardware described in paragraph 6.8.4 of this CPS.

[23] See section 1.3.1.6. nebulacert

[24] See 6.8.4 Cryptographic hardware for the certificates' keys.).

Finally, this reliable environment for the generation of the keys complies with the generation of the signature creation data on behalf of the signatory indicated in article 18.a) of spanish Law Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

It is confirmed that the private keys for the certificates of signature or seal are under the exclusive control of the signatory or the creator of the seal

6.2.8. Method of activating private keys

VinCAsign's private key is activated by executing the corresponding secure start-up procedure for the cryptographic module, by the persons indicated in section 6.2.2.

The CA's keys are activated using an M out of N process (2 out of 5).

The activation of the intermediate CA's private keys is performed using the same M out of N process that is used for the Root CA keys.

6.2.9. Method of deactivating private keys

VinCAsign's private key is deactivated following the steps described in the administrator's manual for the corresponding cryptographic module.

The signer, meanwhile, must enter the PIN for the new activation.

6.2.10. Method of destroying private keys

Prior to the destruction of the private keys, a revocation of the certificate of the public keys associated with them will be issued.

The devices used to store any part of vinCAsign's private keys will be physically destroyed or re-initialised at a low level. The keys will be eliminated following the steps described in the administrator's manual for the corresponding cryptographic module.

Finally, the backup copies will be securely destroyed.

The signer's keys on software can be destroyed be erasing them following the instructions for the application in which they are housed.

The signer's keys in hardware can be destroyed using a special computer application at the facilities of the RA or vinCAsign.

6.2.11. Classification of cryptographic modules

See section 6.2.1

6.3. Other aspects of key pair management

6.3.1. Public key archival

VinCAsign routinely archives its public keys in accordance with the provisions of section 5.5 of this document.

6.3.2. Public and private key usage periods

The key usage periods are determined by the expiry date of the certificate, after which they may no longer be used.

As an exception, the decryption private key can continue to be used even after the certificate has expired..

6.4. Activation data

6.4.1. Activation data generation and installation

The activation data of the devices that protect vinCAsign's private keys are generated in accordance with the provisions of section 6.2.2 and the key ceremony procedures.

The creation and distribution of these devices is registered.

Likewise, VinCAsign generates all the activation data securely.

6.4.2. Activation data protection

The activation data of the devices that protect the private keys of the root and subordinate certification authorities are protected by the owners of the cryptographic module administrator cards, as described in the key ceremony document.

The certificate signer is responsible for protecting their private key with the most complete password possible, which they should memorise.

6.5. Computer security controls

VinCAsign uses trustworthy systems for its certification services. VinCAsign has performed computer audits and controls in order to establish management processes for its computer assets that are suitable for the level of security required for electronic certification systems.

As regards information security, vinCAsign follows the ISO 27001 standard for information management systems.

The equipment used is initially configured with suitable security profiles by vinCAsign's systems personnel, as follows:

- Security configuration of the operating system.

- Security configuration of the applications.
- Correct system dimensioning.
- Configuration of users and permissions.
- Configuration of log events.
- Backup and recovery plan.
- Antivirus configuration.
- Network traffic requirements.

6.5.1. Specific computer security technical requirements

Each vinCAsign server includes the following functions:

- Access control to the services of the SubCA and management of privileges.
- Imposition of separation of tasks for managing privileges.
- Identification and authentication of associated and identified roles.
- Archival of the subscriber and SubCA logs and audit data.
- Audit of events related to security.
- Self-diagnosis of security related to the services of the SubCA.
- Mechanisms for the recovery of keys and the system of the SubCA.

The listed functions are performed using a combination of the operating system, PKI software, physical protection and procedures.
Verification of Qualified Device Certification (QSCD) is performed throughout the period of validity of the certificate[25]. If the QSCD loses its certification as such, vinCAsing will notify users of this fact and execute a plan for renewal of these devices.

6.5.2. Computer security rating

The certification authority and registration applications used by vinCAsign are trustworthy.

6.6. Life cycle technical controls

[25] Ap SDP-6.5.1-07 de ETSI EN 319 411-2

6.6.1. System development controls

The applications are developed and implemented by vinCAsign in accordance with change control and development standards.

The applications have methods to check the integrity, authenticity and correctness of the version to be used.

6.6.2. Security management controls

VinCAsign implements specific activities to train its employees and raise their awareness regarding security. The training materials and documents describing the processes are updated after being approved by a security management group. An annual training plan exists for this purpose.

VinCAsign holds contractual agreements to ensure any external suppliers involved in certification activities follow the necessary security measures.

6.6.2.1. Classification and management of information and assets

VinCAsign keeps an inventory of assets and documents and has a procedure to manage this material and ensure its correct use.

VinCAsign's security policy details the information management procedures including classification according to level of confidentiality.

The documents are classified into three levels: NON-CLASSIFIED, INTERNAL USE, CONFIDENTIAL AND SECRET/RESTRICTED.

6.6.2.2. Management operations

VinCAsign has a suitable incident response and management procedure that involves implementing a system of alerts and generating periodic reports.

VinCAsign's security document gives a detailed description of the incident management process.

VinCAsign has documented the procedure relating to the functions and responsibilities of the personnel involved in controlling and handling parts of the certification process.

6.6.2.3. Handling of media and security

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

6.6.2.3.1. System planning

VinCAsign's Systems Department keeps a record of the capacity of the equipment. Together with the resource control application for each system, possible redimensioning can be anticipated.

6.6.2.3.2. Incident and response reports

VinCAsign has a procedure to monitor incidents and their resolution that involves recording the response provided and an assessment of the economic cost of the response.

6.6.2.3.3. Operational procedures and responsibilities

VinCAsign has defined a series of activities that are assigned to people in trusted roles other than those people responsible for performing everyday, non-confidential operations.

6.6.2.4. Management of the access system

VinCAsign makes all reasonable efforts to confirm that the access system is limited to authorised persons.

In particular:

6.6.2.4.1. General CA

- There are controls based on high-availability firewalls, antivirus and IDS.
- Sensitive data are protected using cryptographic techniques or access controls with strong identification.
- Within its security policy, VinCAsign has a documented procedure for the management of user registrations and de-registrations and the access policy.
- VinCAsign has procedures to ensure that the operations are performed in accordance with the role policy.
- Each person is given a role within the certification operations.
- VinCAsign personnel are held responsible for their actions through the confidentiality agreement signed with the company.

6.6.2.4.2. Certificate generation

Authentication for the issuance process is performed using a system of M out of N operators to activate vinCAsign's private key.

6.6.2.4.3. Revocation management

Revocation is performed using strong authentication of the applications of an authorised administrator. The log systems will generate the tests to guarantee the commitment to the action performed by the vinCAsign administrator.

6.6.2.4.4. Revocation status

For changes to the revocation status, there is an access control based on authentication with certificates or with double authentication factor, to avoid attempts to modify revocation status information.

6.6.2.5. Cryptographic hardware life cycle management

VinCAsign ensures that the cryptographic hardware used to sign certificates is not tampered with during transport, by performing an inspection of the material on delivery.

The cryptographic hardware is transported using specific packaging to avoid tampering.

VinCAsign records all the information regarding the device and adds it to its asset catalogue.

The cryptographic certificate signature hardware must be used by at least two employees in trusted roles.

VinCAsign performs regular tests to ensure the device is functioning properly.

The cryptographic hardware device is only handled by employees in trusted roles.
VinCAsign's private signature key stored in the cryptographic hardware will be erased once the device has been withdrawn.

The configuration of vinCAsign's system, as well as any modifications and upgrades, are documented and controlled.

VinCAsign has a maintenance contract for the device. The changes and upgrades are authorised by the head of security and are noted in the corresponding work records. These configurations are performed by at least two people in trusted roles.

6.7. Network security controls

VinCAsign protects the physical access to the network management devices and has an architecture that orders traffic based on security characteristics, creating clearly defined network sections. These divisions are created using firewalls.

Confidential information sent over non-secure networks is encoded using SSL protocols or VPN system protocols with double-factor authentication.

6.8. Cryptographic module engineering controls

The cryptographic modules are subject to the engineering controls described in the standards mentioned in this section.

The key generation algorithms used are generally accepted for the use of the key to which they are related.

All vinCAsign's cryptographic operations are performed in modules with FIPS 140 level 3 or Common Criteria EAL 4+ (with the supplement ALC_FLR.1) certification.

6.8.1. Cryptographic Hardware for CA Root "vinCAsign QUALIFIED Authority".

The certificate key of the root certification authority "vinCAsign Qualified Authority" is stored in Realsec's HSM "Cryptosec 2048 by Realia Technologies S.L".

6.8.2. Cryptographic hardware for the SubCA "vinCAsign nebulaSUITE2 Authority".

The certificate key of the subordinate certification authority "vinCAsign nebulaSUITE2 Authority" is stored in the Primekey HSM "SafeGuard® CryptoServer Se from Utimaco IS GmbH".

6.8.3. Cryptographic hardware for the SubCA "vinCAsign nebulaSUITE4 Authority".

The certificate key of the subordinate certification authority "vinCAsign nebulaSUITE4 Authority" is stored in the Primekey HSM "SafeGuard® CryptoServer Se from Utimaco IS GmbH".

6.8.4. Cryptographic hardware for the SubCA "vinCAsign nebulaSUITE5 Authority".

The certificate key of the subordinate certification authority "vinCAsign nebulaSUITE5 Authority" is stored in the Primekey HSM "SafeGuard® CryptoServer Se from Utimaco IS GmbH".

6.8.5. Cryptographic hardware for certificate keys

The private keys of the certificates issued to subscribers in the subordinate authorities are generated in the HSM "nShield XC" and "nShield Connect 1500" belonging to the "nShield HSM Family v.11.72.02".

6.9. Time source entities

VinCAsign has its own time source, it is an NTP Stratum 1 in the COLT Barcelona DPC facilities. (Meinberg LANTIME M200/GPS model) with which it synchronises all its services.
Furthermore, vinCAsign has a time synchronization procedure coordinated with the ROA Royal Institute and Observatory of the Navy in San Fernando via NTP.

7. Certificate profiles and revoked certificate lists

7.1. Certificate profiles

All qualified certificates issued under this policy comply with X.509 version 3, RFC 3739, ETSI EN 319 412- 1, ETSI EN 319 412-2, and ETSI EN 319 411-1, ETSI 319 411-2 and ETSI EN 319 401 standards as well as CA-Browser Forum requirements for web authentication certificates.

7.1.1. Version number

VinCAsign issues X.509 Version 3 certificates.

7.1.2. Certificate Extensions

The certificate extensions are listed in the profile documents, which can be accessed from the vinCAsign website (https://www.vincasign.net).

This makes it possible to maintain more stable versions of the CPS and detach them from the frequent adjustments to the profiles.

7.1.3. Algorithm object identifiers (OIDs)

The signature algorithm object identifier is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The public key algorithm object identifier is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Name forms

The certificates must contain the information necessary for their use, as set out in the corresponding policy.

7.1.5. Name constraints

The names contained in the certificates are restricted to “Distinguished Names” X.500, which are unique and non-ambiguous.

Additionally, name constraints can be established in relation to the certificates in the corresponding authentication, electronic signature, encryption or electronic evidence policies, provided that these are objective, proportionate, transparent and non-discriminatory.

7.1.6. Certificate policy object identifier (OID)

All certificates include a certificate policy identifier under which they have been issued, according to the structure indicated in point 1.2.1. of this document.

7.2. Certificate revocation list profile

7.2.1. Version number

The CRLs issued by vinCAsign are Version 2.

7.2.2. OCSP profile

In accordance with standard IETF RFC 6960.

8. Government approval

VinCAsign as a certification service provider by the Ministry responsible for trusted electronic services will be subject to the control reviews that this body considers necessary.
VinCAsign is a company committed to the security and quality of its services by obtaining and maintaining the ISO/IEC 27001:2013 certification.

8.1. Frequency of the compliance audit

VinCAsign performs a compliance audit on an annual basis, in addition to the internal audits it performs in accordance with its own criteria whenever it suspects non-compliance with any security measures.

8.2. Identity and qualifications of the auditor

Audits are performed by an independent external firm of auditors with proven technical competency and experience in computer security, information system security, public key certification services conformity audits, and related aspects.

8.3. Auditor's relationship to the assessed entity

The auditing firms are firms of recognised prestige with departments specialised in performing computer audits, thus avoiding any conflicts of interest that may bias their actions in relation to vinCAsign.

8.4. Topics covered by the audit

The audit assesses the following aspects in relation to vinCAsign:

a) That the entity's management system guarantees the quality of the service provided.
b) That the entity complies with the requirements of the CPS and other documentation related to the issuance of the different digital certificates.
c) That the CPS and other related legal documentation is in line with that agreed by vinCAsign and with the provisions of the applicable standards.
d) That the entity suitably manages its information systems.

Specifically, the following aspects shall be covered by the audit:

a) Processes of the CA, RAs and related elements.
b) Information systems.
c) Protection of the data processing centre.
d) Documents.

8.5. Actions taken as a result of deficiency

Once the management has received the audit report, it analyses the deficiencies found together with the auditors and creates and implements a corrective plan to resolve said deficiencies.

If the Víntegris Certification Authority is incapable of creating and/or implementing said plan, or if the deficiencies found represent an immediate threat to the security or integrity of the system, it must immediately inform the Víntegris Corporate Security Committee, which may implement the following measures:

- Temporary suspension of operations.
- Revocation of the CA's key and renewal of the infrastructure.
- Termination of the CA's services.
- Any other additional actions that are deemed necessary.

8.6. Communication of audit results

The audit results reports shall be submitted to the Víntegris Corporate Security Committee within a maximum period of 15 days after performance of the audit.

9. Business and legal requirements

9.1. Fees

9.1.1. Certificate issuance or renewal fees

VinCAsign may charge a fee for issuing or renewing certificates, in which case the subscribers shall be duly informed.

9.1.2. Certificate access fees

VinCAsign does not charge any fee for access to certificates.

9.1.3. Certificate status information access fees

VinCAsign does not charge any fee for access to certificate status information.

9.1.4. Fees for other services

Not stipulated.

9.1.5. Refund policy

Not stipulated.

9.2. Financial capacity

VinCAsign has sufficient funds to maintain its operations and comply with its obligations, as well as to meet its damage liability commitments, in accordance with ETSI EN 319 401-1 7.12 c), related to management of termination of its services and its termination plan.

9.2.1. Insurance coverage

VinCAsign has adequate civil liability coverage provided by a professional civil liability insurance policy, which complies with the provisions of article 24.2.c) Regulation (UE) 910/2014, , and with a policy limit of at least 5,000,000 euros.

9.2.2. Other assets

Not stipulated.

9.2.3. Insurance coverage for subscribers and relying parties

VinCAsign has adequate civil liability coverage provided by a professional civil liability insurance policy, which complies with the provisions of article article 24.2.c) Regulation (UE) 910/2014s, and with a policy limit of at least 5,000,000 euros.

9.3. Confidentiality

9.3.1. Confidential information

The following information is kept confidential by vinCAsign:

- Certificate requests, both approved and rejected, as well as all other personal information obtained for the purpose of issuing and maintaining certificates, except the information listed in the following section.
- Private keys generated and/or stored by the certification services provider.

- Transaction records, including the complete records and audit logs for transactions.
- Internal and external audit trails created and/or maintained by the Certification Authority and its auditors.
- Business continuity and emergency plans.
- Security policy and plans.
- Documentation on operations and other operational plans, such as archiving, monitoring and similar.
- All other information identified as 'Confidential".

9.3.2. Information not within the scope of confidential information

The following information is not considered confidential:

- Certificates issued or in the process of being issued.
- The link between a subscriber and a certificate issued by the Certification Authority.
- The given name and surname(s) of the natural person identified in the certificate, as well as any other circumstances or personal data of said person, if it is significant in light of the purpose of the certificate.
- The email address of the natural person identified in the certificate, or the email address assigned by the subscriber, if it is significant in light of the purpose of the certificate.
- The economic uses and limits mentioned in the certificate.
- The period of validity of the certificate, as well as its date of issue and expiry.
- The certificate's serial number.
- The different statuses and situations of the certificate and the start date of each, specifically: pending generation and/or delivery; valid; revoked; suspended; or expired, and the reason for the change in status.
- The certificate revocation lists (CRLs) as well as other information on revocation status.
- The information contained in the certificate repositories.
- Any other information that is not indicated in the previous section.

9.3.3. Disclosure of suspension and revocation information of certificates

Please refer to the previous section.

9.3.4. Disclosure pursuant to judicial or administrative process

VinCAsign only discloses confidential information when required to do so by law.

Specifically, the records that prove the reliability of the data contained in the certificate, as well as records related to the reliability of the data and those related to the operation[26] will be disclosed if so required to provide evidence of certification for judicial proceedings, even without the consent of the certificate subscriber.

The Certification Authority mentions this fact in the privacy policy set out in section 9.4. of this document.

9.3.5. Disclosure of information on the request of the owner

In the privacy policy set out in section 9.4, VinCAsign makes allowances for directly disclosing the information of the subscriber and, where applicable, the natural person identified on the certificate, to third parties or to the natural person.

9.3.6. Other information disclosure circumstances

Not stipulated.

9.4. Personal data protection

[26] Apartado REQ-7.10-04 de la ETSI EN 319 401

In order to provide the service, vinCAsign needs to collect and store certain information, including personal data.

In the corporate certificates, such information is collected through the subscribers, based on the corporate relationship that links them to the signatories (employees, positions, partners...), or in the rest of the certificates, directly from the affected parties, or through the Registration Entities, always in strict compliance with the conditions for legitimate treatment referred to in Article 6 of the General Data Protection Regulation, and in accordance with the LOPDGDD.

VinCAsign collects the data exclusively necessary for the issue and maintenance of the certificate.

VinCAsign has developed a privacy policy, and documented in this Declaration of Trust Practices the corresponding security aspects and procedures in accordance with the General Regulation of Data Protection.

VinCAsign does not divulge or transfer personal data, except in the cases provided for in sections 9.3.2 to 9.3.6, and in section 5.8 of this document, in the event of termination of the certification service.

Confidential information in accordance with personal data protection regulations is protected from loss, destruction, damage, falsification and illegal or unauthorised processing, in accordance with the requirements established in this document in compliance with the General Data Protection Regulations and the LOPDGDD.

9.5. Intellectual property rights

9.5.1. Ownership of certificates and revocation information

Only VinCAsign holds intellectual property rights to the certificates it issues, notwithstanding the rights of the subscribers, key owners and third parties, who are given the non-exclusive right to reproduce and distribute certificates, free of charge, as long as they are reproduced in their entirety without any alterations and it is necessary in relation to electronic signatures and/or encryption systems within the sphere of use of the certificate, in accordance with the relevant binding documentation.

Furthermore, the certificates issued by vinCAsign contain a legal notice regarding intellectual property rights.

The same rules apply to the use of certificate revocation information.

9.5.2. Ownership of the Certification Practice Statement

Only VinCAsign holds intellectual property rights over this Certification Practice Statement.

9.5.3. Ownership of information relating to names

The subscriber and, where applicable, the natural person identified in the certificate, maintains full rights over the brand, product or trade name contained in the certificate, should such rights exist.

The subscriber is the owner of the name mentioned in the certificate, formed by the information specified in section 3.1.1

9.5.4. Ownership of keys

The key pairs are the property of the signers, natural persons who have exclusively electronic signature keys.

When a key is separated into different parts, all the parts of the key are the property of the key owner.

9.6. Obligations and civil liability

9.6.1. Obligations of the Víntegris Certification Entity

VinCAsign guarantees and takes full responsibility for its compliance with all the requirements set out in the CPS, and is the only party responsible for ensuring compliance

with the procedures described therein, even if some or all of the operations are outsourced.

VinCAsign provides its certification services pursuant to this Certification Practice Statement.

Prior to the issuance and delivery of the certificate to the subscriber, vinCAsign informs the subscriber of the terms and conditions for the use of the certificate, its price and usage restrictions, through a subscriber agreement.

This requirement to provide information is also complied with through a PDS[27], which is also classed as an informative text, and which incorporates the content specified in Annex A of ETSI EN 319 411-1 v1.2.2 (2018-04), This document may be sent by electronic means, using a long-lasting means of communication and comprehensible language.

VinCAsign permanently communicates changes[28] in its obligations by publishing new versions of its legal documentation on its website providing subscribers, key owners and relying parties with at least the following information through said PDS, in written, comprehensible language:

- Instructions for compliance with the provisions of sections **¡Error! No se encuentra el origen de la referencia.**, 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 and 9.6.10.
- Information on the applicable policies, noting that the certificates are not issued to the public.
- Declaration that the information contained in the certificate is correct, unless otherwise notified by the subscriber.
- Consent for the publication of the certificate in the Repository and access by third parties.
- Consent for the storage of the information used to register the subscriber and for said information to be transferred to third parties in the event that the Certification Authority terminates its operations without revoking valid certificates.

[27] PKI Disclosure Statement.

[28] Ap REG-6.2.3-08 de ETSI EN 319 411-1

- Restrictions of use for the certificate, including those described in section 0
- Information on how to validate a certificate, including the requirement to check the certificate status, and the conditions under which the certificate can be reasonably trusted, which apply when the subscriber acts as a relying party.
- The manner in which the Certification Authority guarantees its financial liability.
- Limitations to the applicable responsibilities, including the uses for which the Certification Authority accepts or refuses liability.
- Period during which certificate request information is archived.
- Period during which audit logs archived.
- Applicable procedures for resolving disputes.
- Applicable law and competent jurisdiction
- Whether the Certification Authority has been declared compliant with the certification policy and, if so, with which system.

9.6.2. Warranties offered to subscribers and third parties who rely on certificates

In the documentation that relates it to subscribers and relying parties, vinCAsign establishes and rejects the applicable warranties and limitations of liability.

VinCAsign makes the following minimum guarantees to the subscriber:

- There are no factual errors in the information contained in the certificates, known or made by the Certification Entity..
- There are no errors of fact in the information contained in the certificates resulting from a lack of due diligence in the management of the certification request or in the creation of the certificate.
- That the certificates comply with all the material requirements set out in the Certification Practice Statement.
- That the revocation and Repository use services comply with all the material requirements set out in the Certification Practice Statement.

vinCAsign makes the following minimum guarantees to relying parties:

- That the information contained or included by reference in the certificate is correct, except when indicated otherwise.

- In the case of certificates published in the Repository, that the certificate has been issued to the subscriber identified therein and that the certificate has been accepted in accordance with section 4.4 of this document.
- That, in the approval of the certificate request and issuance of the certificate, all the material requirements set out in the Certification Practice Statement have been complied with.
- That the services shall be provided rapidly and securely, especially the services of revocation and Repository.

Furthermore, vinCAsign guarantees to the subscriber and the third party that it has relied on the certificate:

- That the certificate contains the information that must be included in a qualified certificate, as specified by Annex 1 to REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014
- That, if it generates the private keys of the subscriber or, where applicable, the natural person identified in the certificate, the confidentiality thereof shall be maintained throughout the process.
- The liability of the Certification Entity, within the established limits.

9.6.3. Disclaimer of warranty

VinCAsign rejects all other warranties that are not legally applicable, except those contemplated in section **¡Error! No se encuentra el origen de la referencia.**. of this document.

9.6.4. Limitation of liability

VinCAsign limits its liability to the issuance and management of the subscriber certificates and key pairs supplied by the Certification Entity.

9.6.5. Indemnities

9.6.5.1. Subscriber indemnity clause

In the contract with the subscriber, VinCAsign includes a clause through which the subscriber undertakes to hold the Certification Entity harmless for any damages arising from any action or omission that results in liability, damage or loss, or costs of any type, including court costs and legal costs, as a result of the publication and use of the certificate, when any of the following causes apply:

- False or erroneous statements made by the certificate user.
- Errors made by the certificate user in the request data, if such action or omission involves deceit or negligence towards the Certification Authority or relying party.
- Negligence in protecting the private key, in using a trustworthy system, or in taking the necessary precautions to avoid the compromise, loss, disclosure, modification or non-authorised use of said key.
- The use by the subscriber of names (including common names, email addresses and domain names) and other information in the certificate that infringes the intellectual or industrial property rights of third parties.

9.6.5.2. Indemnity clause for third parties relying on the certificate

In the PDS, VinCAsign includes a clause through which the relying party undertakes to hold the Certification Entity harmless for damages arising from any action or omission that results in liability, damage or loss, or costs of any type, including court costs and legal costs, as a result of the publication and use of the certificate, when any of the following causes apply:

- The relying party fails to comply with their obligations.
- Reckless trust in a certificate in light of the circumstances.
- Failure to check the status of a certificate to ensure that it has not been revoked.

9.6.6. Unforeseeable circumstances and force majeure

In the PDS, vinCAsign includes clauses that limit its liability in the event of unforeseeable circumstances and force majeure.

9.6.7. Applicable law

In the subscriber agreement and the PDS, the Certification Entuty specifies that the service provision, including the certification policy and practices, shall be subject to Spanish Law.

VinCAsign assumes the enforcement of the following regulations:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 999/93/EC (eIDAS Regulation)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)
- COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 laying down minimum technical specifications and procedures for security levels of means of electronic identification as provided for in Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- Spanish Law “Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza”
- Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations
- Law 40/2015, of 1 October, on the Legal Regime of the Public Sector
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD)
- Latest version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published at http://www.cabforum.org by the CA/Browser Forum.
- Guidelines For The Issuance And Management of Extended Validation Certificates publicados en http://www.cabforum.org by the CA/Browser Forum.

9.6.8. Severability, survival, entire agreement and notification clauses

In the subscriber agreement and the PDS, vinCAsign specifies severability, survival, entire agreement and notification clauses:

- In virtue of the severability clause, the invalidity of any of the clauses will not affect the rest of the agreement.
- In virtue of the survival clause, certain rules will continue to be valid after termination of the legal relationship that regulates the service between the parties. To this end, the Certification Authority ensures that at least the requirements contained in sections **¡Error! No se encuentra el origen de la referencia.** (Representations and warranties), 8 (Compliance audit) and 9.3 (Confidentiality) will remain extant after termination of the services and of the general conditions of issuance/use.
- In virtue of the entire agreement clause, it is understood that the legal document that regulates the service reflects the complete will and all the agreements between the parties.
- The notification clause sets out the procedure to be followed for notifications to be sent between the parties.

9.6.9. Competent jurisdiction clause

In the subscriber agreement and the PDS, vinCAsign includes a competent jurisdiction clause specifying that the international jurisdiction falls to Spanish judges.

Regional and functional jurisdiction shall be determined in virtue of the applicable rules of private international law and the rules of procedural law.

9.6.10. Dispute resolution

In the subscriber agreement and the PDS, vinCAsign specifies the applicable dispute mediation and resolution procedures. The procedure to follow is described in the internal document " VINCASIGN proc disputas v1r1.pdf".