VinCAsign Certification Practice Statement

General information

Control of the document

Security classification:	Public
Destination entity:	víntegris SEGURIDAD DE LA INFORMACIÓN
Version:	1.1
Date published:	03/05/2016
File:	Vintegris CPS v1r1
Format:	Office 2016
Authors:	Víntegris

Contents

1. Introduction

1.1. Presentation

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

The following certificates are issued:

- Corporate natural person certificate issued in SSCD[1].
- Corporate natural person certificate issued in software.
- Corporate representative natural person certificate issued in SSCD.
- Corporate representative natural person certificate issued in software.
- High-level public employee natural person certificate.
- Low-level public employee natural person certificate.
- High-level body stamp certificate.
- Low-level body stamp certificate.

1.2. Document name and ID

This document is the "vinCAsign Certification Practice Statement".

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.

[1] Secure Electronic Signature Creation Device.

OID	Type of certificate
1.3.6.1.4.1.**47155.1.1.1**	Corporate Natural Person Certificates in SSCD
1.3.6.1.4.1.**47155.1.1.2**	Corporate Natural Person Certificates in Software
1.3.6.1.4.1.**47155.1.2.1**	Corporate Representative Certificates in SSCD
1.3.6.1.4.1.**47155.1.2.2**	Corporate Representative Certificates in Software
1.3.6.1.4.1.**47155.1.4.1**	High-Level Public Employee Natural Person Certificates
1.3.6.1.4.1.**47155.1.4.2**	Medium-Level Public Employee Natural Person Certificates
1.3.6.1.4.1.**47155.1.5.1**	High-level body stamp certificates
1.3.6.1.4.1.**47155.1.5.2**	Medium-level body stamp certificates

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.

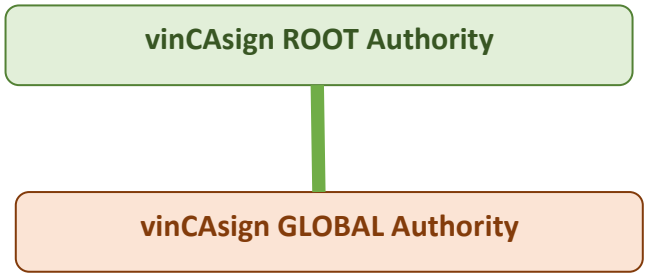
1.3. Participants in certification services

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 digital signatures.

Víntegris SL is a certification services provider that operates in accordance with the provisions of Spanish Law 59/2003 of 19 December on digital signatures and with the ETSI technical standards applicable to the issuance and management of qualified certificates, mainly ETSI TS 101 456, EN 319 411-1 and EN 319 411-2, for the purpose of facilitating compliance with the 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 ROOT 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 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

1.3.1.2. VinCAsign GLOBAL Authority

This is the certification authority within the hierarchy which issues certificates to end users and whose public key certificate has been electronically signed by the 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

1.3.2. Registration service

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

The departments that are assigned this function by the certificate subscribers, such as an HR department, also register the certificates subject to this Certification Practice Statement, due to the fact that they are corporate certificates, as these departments possess authentic records regarding the connection between the signer and the subscriber.

The subscribers are registered by delegation, in accordance with the instructions of the certification services provider, pursuant to article 13.5 of Spanish Law 59/2003 of 19 December on digital signatures and with the certification service provider taking full responsibility before third parties.

1.3.3. End entities

End entities are the people or organisations that make use of the electronic certificate issuance, management and use services for the purposes of identification and digital signature.

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

1. Subscribers to the certification service.
2. Signers.
3. Relying parties.

1.3.3.1. 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 (electronic stamp 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 (digital 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 ETSI TS 101 456, section 4.4, maintained in its subsequent versions, and currently ETSI EN 319 411, sections 5.4.2 and 6.3.4.e.

1.3.3.2. Signers

The signers are the natural persons who are the exclusive owners of the digital signature keys for identification and advanced or qualified digital 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 is not stored and, therefore, may not be recovered by the certification services provider. This means that the natural persons identified in the corresponding certificates have sole responsibility for safeguarding their keys and must take into consideration the implications of losing a private key.

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

1.3.3.3. Relying parties

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

Prior to being able to rely on the certificates, the relying parties must validate them as described in this certification practice statement and the corresponding instructions, which are available on the Certification Authority's website.

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

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

1.4.1.1. Corporate natural person certificate, issued in SSCD

This certificate has OID 1.3.6.1.4.1.47155.1.1.1

Corporate natural person certificates issued in SSCD are qualified certificates in accordance with the provisions of article 11.1, with the content prescribed by article 11.2, and are issued in compliance with the obligations contained in articles 12, 13, and 17 to 20 of Spanish Law 59/2003 of 19 December on digital signatures.

Corporate natural person certificates issued in SSCD work with a secure digital signature creation device, in accordance with article 24.3 of Spanish Law 59/2003 of 19 December on digital signatures, and comply with technical standard TS 101 456 of the European Telecommunications Standards Institute.

These certificates guarantee the identity of the signer and their relationship with the certification service subscriber, allowing the generation of a "qualified digital signature"; i.e. an advanced digital signature based on a qualified certificate that has been generated using a secure device, meaning that the digital signature has the legal validity of a written signature without the need for any additional requirements.

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

a) Secure email signature.
b) Other digital 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. Digital signature (to perform authentication)

b. Content commitment (to create the digital 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. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure digital signature creation device.

1.4.1.2. Corporate natural person certificate issued in software

This certificate has OID 1.3.6.1.4.1.47155.1.1.2

Corporate natural person certificates issued in software are qualified certificates in accordance with the provisions of article 11.1, with the content prescribed by article 11.2, and are issued in compliance with the obligations contained in articles 12, 13, and 17 to 20 of Spanish Law 59/2003 of 19 December on digital signatures.

Corporate natural person certificates issued in software are not guaranteed to work with the secure digital signature creation devices referred to in article 24.3 of Spanish Law 59/2003 of 19 December.

These certificates guarantee the identity of the signer and the person indicated in the certificate and make it possible to generate an "advanced digital 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 digital 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. Digital signature (to perform authentication)
    b. Content commitment (to create the digital 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.

1.4.1.3. Corporate representative natural person certificate issued in SSCD

This certificate has OID 1.3.6.1.4.1.47155.1.2.1

Corporate representative natural person certificates issued in SSCD are qualified certificates in accordance with the provisions of article 11.1, with the content prescribed by articles 11.2 and 11.4, and are issued in compliance with the obligations contained in articles 12, 13, and 17 to 20 of Spanish Law 59/2003 of 19 December on digital signatures.

Corporate representative natural person certificates issued in SSCD work with a secure digital signature creation device, in accordance with article 24.3 of Spanish Law 59/2003 of 19 December, and comply with technical standard TS 101 456 of the European Telecommunications Standards Institute.

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 digital signature"; i.e. an advanced digital

signature based on a qualified certificate that has been generated using a secure device, meaning that the digital signature has the legal validity of a written signature without the need to fulfil any additional requirements.

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

a) Secure email signature.
b) Other digital 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. Digital signature (to perform authentication)
    b. Content commitment (to create the digital 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. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure digital signature creation device.

1.4.1.4. Corporate representative natural person certificate issued in software

This certificate has OID 1.3.6.1.4.1.47155.1.2.2

Corporate representative natural person certificates issued in software are qualified certificates in accordance with the provisions of article 11.1, with the content prescribed

by articles 11.2 and 11.4, and are issued in compliance with the obligations contained in articles 12, 13, and 17 to 20 of Spanish Law 59/2003, of 19 December, on digital signatures, and comply with technical standard TS 101 456 of the European Telecommunications Standards Institute.

Corporate representative natural person certificates issued in software are not guaranteed to work with the secure digital signature creation devices referred to in article 24.3 of Spanish Law 59/2003 of 19 December.

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 digital signature based on a qualified electronic certificate".

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 digital 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. Digital signature (to perform authentication)
    b. Content commitment (to create the digital 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.

1.4.1.5. High-level public employee natural person certificate

This certificate has OID 1.3.6.1.4.1.47155.1.4.1

High-level public employee natural person certificates are qualified certificates in accordance with the provisions of article 11.1, with the content prescribed by article 11.2, and are issued in compliance with the obligations contained in articles 12, 13, and 17 to 20 of Spanish Law 59/2003 of 19 December on digital signatures.

These certificates are issued to public employees to identify them as either working for or being associated with the Public Administration, in compliance with the requirements laid down by Spanish Law 11/2007, of 22 June, on electronic access of citizens to public services and its implementing regulations.

High-level public employee natural person certificates work with a secure digital signature creation device, in accordance with article 24.3 of Spanish Law 59/2003, of 19 December, on digital signatures, and comply with technical standard TS 101 456 of the European Telecommunications Standards Institute. Furthermore, high-level public employee natural person certificates are issued in accordance with the version of the Public Administration identification and digital signature scheme that is valid at the date of publication of this document.

These certificates guarantee the identity of the subscriber and the signer, and they also make it possible to generate “qualified digital signatures”, i.e. advanced digital signatures based on a qualified certificate created using a secure device. In accordance with the provisions of article 3 of Spanish Law 59/2003 of 19 December, the signature will have full legal validity, without the need to fulfil any other additional requirement.

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

a) Secure email signature.
b) Other digital 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. Digital signature (to perform authentication)
    b. Content commitment (to create the digital 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. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure digital signature creation device.
c) The "User Notice" field describes the use of this certificate.

1.4.1.6. Medium-level public employee natural person certificate

This certificate has OID 1.3.6.1.4.1.47155.1.4.2

Medium-level public employee natural person certificates are qualified certificates in accordance with the provisions of article 11.1, with the content prescribed by article 11.2, and are issued in compliance with the obligations contained in articles 12, 13, and 17 to 20 of Spanish Law 59/2003 of 19 December on digital signatures.

These certificates are issued to public employees to identify them as either working for or being associated with the Public Administration, in compliance with the requirements laid down by Spanish Law 11/2007, of 22 June, on electronic access of citizens to public services and its implementing regulations.

Medium-level public employee natural person certificates are not guaranteed to work with the secure digital signature creation devices referred to in article 24.3 of Spanish Law 59/2003 of 19 December.

Medium-level public employee natural person certificates are issued in accordance with the version of the Public Administration identification and digital signature scheme that is valid at the date of publication of this document.

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

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

a) Secure email signature.
b) Other digital 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. Digital signature (to perform authentication)
    b. Content commitment (to create the digital 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 "User Notice" field describes the use of this certificate.

1.4.1.7. High-level body electronic stamp certificate

This certificate has OID 1.3.6.1.4.1.47155.1.5.1

High-level body electronic stamp certificates are qualified certificates in accordance with the provisions of article 11.1, with the content prescribed by article 11.2, and are issued in compliance with the obligations contained in articles 12, 13, and 17 to 20 of Spanish Law 59/2003 of 19 December on digital signatures.

These certificates are issued for the purposes of identifying and authenticating parties exercising powers in automated administrative procedures, in accordance with article 18.1 of Spanish Law 11/2007, of 22 June, on electronic access of citizens to public services.

High-level body electronic stamp certificates are issued in accordance with the version of the Public Administration identification and digital signature scheme that is valid at the date of publication of this document.

These certificates guarantee the identity of the subscriber, the public body and, where applicable, the head of the body that are indicated in the certificate.

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. Digital signature (to perform authentication)
    b. Content commitment (to create the digital 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. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure digital signature creation device.

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

1.4.1.8. Medium-level body electronic stamp certificate

This certificate has OID 1.3.6.1.4.1.47155.1.5.2

Medium-level body electronic stamp certificates are qualified certificates in accordance with the provisions of article 11.1, with the content prescribed by article 11.2, and are issued in compliance with the obligations contained in articles 12, 13, and 17 to 20 of Spanish Law 59/2003 of 19 December on digital signatures.

These certificates are issued for the purposes of identifying and authenticating parties exercising powers in automated administrative procedures, in accordance with article 18.1 of Spanish Law 11/2007, of 22 June, on electronic access of citizens to public services.

Medium-level body electronic stamp certificates are issued in accordance with the version of the Public Administration identification and digital signature scheme that is valid at the date of publication of this document.

These certificates guarantee the identity of the subscriber, the public body and, where applicable, the head of the body that are indicated in the certificate.

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. Digital signature (to perform authentication)
    b. Content commitment (to create the digital 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 "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

By establishing and applying the relevant procedures, vinCAsign's document and organisation system ensures the correct maintenance of this document and the related service specifications.

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 24/7 and, in the event of system failures beyond vinCAsign's control, the latter shall make every effort to ensure the service is available again within the period specified 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 applicable certificate policies.
- The Certification Practice Statement.
- The informative texts (Policy Disclosure Statements - PDS), published at least in English.

2.3. Frequency of publication

The information of the certification services provider, including the policies and the Certification Practice Statement, 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 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.

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.

The names contained in the certificates are those listed below.

3.1.1.1. Corporate natural person certificate, issued in SSCD

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
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 natural person certificate issued in software

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
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

3.1.1.3. Corporate representative natural person certificate issued in SSCD

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
Surname	The representative's surname(s)
Given Name	The representative's given name(s)
Title	Role or function as regards representation
Serial Number	The representative's National ID No.
Common Name (CN)	The representative's given name and surname
Subject Directory Attributes	1.3.6.1.4.1.47155.2.1: Level of power of attorney 1.3.6.1.4.1.47155.2.2: Representation document 1.3.6.1.4.1.47155.2.3:

	Additional circumstances of the natural person 1.3.6.1.4.1.47155.2.4: Limit of use 1.3.6.1.4.1.47155.2.5: Registration data of the representation

3.1.1.4. Corporate representative natural person certificate issued in software

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
Surname	The representative's surname(s)
Given Name	The representative's given name(s)
Title	Role or function as regards representation
Serial Number	The representative's National ID No.
Common Name (CN)	The representative's given name and surname
Subject Directory Attributes	1.3.6.1.4.1.47155.2.1: Level of power of attorney 1.3.6.1.4.1.47155.2.2: Representation document 1.3.6.1.4.1.47155.2.3: Additional circumstances of the natural person 1.3.6.1.4.1.47155.2.4: Limit of use 1.3.6.1.4.1.47155.2.5: Registration data of the representation

3.1.1.5. High-level public employee natural person certificate

Country (C)	"ES"
Organization (O)	Public Administration in which the signer provides their services
Organizational Unit (OU)	Unit to which the signer is assigned
Organizational Unit (OU)	ID number within the Public Administration of the signer
Surname	Surname(s)
Given Name	Given Name(s)
Title	Position
Serial Number	The signer's National ID No.
Common Name (CN)	The signer's given name, surname and National ID No.
OID: 2.16.724.1.3.5.3.1.4	The signer's National ID No./Tax ID No.
OID: 2.16.724.1.3.5.3.1.5	Personal ID No. in the Public Administration
OID: 2.16.724.1.3.5.3.1.6	The signer's given name
OID: 2.16.724.1.3.5.3.1.7	The signer's first surname
OID: 2.16.724.1.3.5.3.1.8	The signer's second surname
OID: 2.16.724.1.3.5.3.1.9	The signer's email address

3.1.1.6. Medium-level public employee natural person certificate

Country (C)	"ES"
Organization (O)	Public Administration in which the signer provides their services
Organizational Unit (OU)	Unit to which the signer is assigned
Organizational Unit (OU)	ID number within the Public Administration of the signer
Surname	Surname(s)
Given Name	Given Name(s)
Title	Position
Serial Number	The signer's National ID No.
Common Name (CN)	The signer's given name, surname and National ID No.
OID: 2.16.724.1.3.5.3.2.4	The signer's National ID No./Tax ID No.

OID: 2.16.724.1.3.5.3.2.5	Personal ID No. in the Public Administration
OID: 2.16.724.1.3.5.3.2.6	The signer's given name
OID: 2.16.724.1.3.5.3.2.7	The signer's first surname
OID: 2.16.724.1.3.5.3.2.8	The signer's second surname
OID: 2.16.724.1.3.5.3.2.9	The signer's email address

3.1.1.7. High-level body electronic stamp certificate

Country (C)	"ES"
Organization (O)	Public Administration to which the stamp belongs
Surname	Surname(s) of the head of the body to which the stamp belongs
Given Name	Name of the head of the body to which the stamp belongs
Serial Number	National ID No. of the public entity
OID: 2.16.724.1.3.5.2.1.4	ID No./Tax ID No. of the party responsible for the stamp
OID: 2.16.724.1.3.5.2.1.6	Given name of the party responsible for the stamp
OID: 2.16.724.1.3.5.2.1.7	First surname of the party responsible for the stamp
OID: 2.16.724.1.3.5.2.1.8	Second surname of the party responsible for the stamp
OID: 2.16.724.1.3.5.2.1.9	Email of the party responsible for the stamp

3.1.1.8. Medium-level body electronic stamp certificate

Country (C)	"ES"
Organization (O)	Public Administration to which the stamp belongs
Surname	Surname(s) of the head of the body to which the stamp belongs
Given Name	Name of the head of the body to which the stamp belongs
Serial Number	National ID No. of the public entity
OID: 2.16.724.1.3.5.2.2.4	ID No./Tax ID No. of the party responsible for the stamp
OID: 2.16.724.1.3.5.2.2.6	Given name of the party responsible for the stamp
OID: 2.16.724.1.3.5.2.2.7	First surname of the party responsible for the stamp
OID: 2.16.724.1.3.5.2.2.8	Second surname of the party responsible for the stamp

OID: 2.16.724.1.3.5.2.2.9	Email of the party responsible for the stamp

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

Under no circumstances may pseudonyms be used to identify an entity/company/organisation or signer.

Under no circumstances shall anonymous certificates be issued.

3.1.4. Interpretation of name formats

Name formats are interpreted in accordance with the law of the country in which the subscriber is established, under the terms of said country.

The “country” field shall be the country of the subscriber and shall always be Spain in certificates issued by Spanish Public Administrations.

The certificate shows the relationship between a natural person and the company, entity or organisation to which they are linked, and does not take into account the nationality of the natural person. This results from the corporate nature of the certificate, for which the entity, company or organisation is the subscriber and the related natural person is the party authorised to use the certificate.

In certificates issued to Spanish subscribers, the “serial number” field must include the Tax ID number of the signer for the certificate to be accepted for performing transactions with Spanish Public Administrations.

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 or other legally valid ID number of the natural person.
- Tax ID Number 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 Bylaws 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.

3.2. Initial validation of identity

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 records may be directly consulted.

The identity of the natural persons identified in the certificates shall be validated by means of the corporate records of the subscribing public or private entity, company or organisation. The subscriber shall produce a certificate with the necessary data and send it to vinCAsign, via the means indicated by the latter, to register the identity of the signers.

Each public or private entity, company or organisation must register their personal data files with the corresponding Data Protection Agency. They shall be responsible for this task rather than vinCAsign, which shall be responsible for the processing.

3.2.1. Test for the possession of the private key

Possession of the private key is proven by means of the procedure for the reliable delivery of the certificate and its acceptance by the subscriber, in the case of stamp certificates, or by the signer, in the case of signature certificates.

3.2.2. 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 shall meet in person with an authorised representative of vinCAsign and shall be given 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 of the representative

   - The identification details of the subscriber they are representing:

     - Company name.
     - All existing registry information including details related to incorporation and legal personality and the extension and validity of the requester's powers of representation.
     - Document: Tax ID Code 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.

- The details of the representation or powers of attorney:

  - The term of the representation or powers of attorney (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 representation or powers of attorney. This verification may be performed with an authentic electronic copy of the notarial deed of powers of representation, under the terms of the notarial regulations.

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, before returning the documents provided.

6. Alternatively, in accordance with article 13.1 of Spanish Law 59/2003 of 19 December, the signature of the form may be legitimised by a notary and sent to vinCAsign by certified post, in which case steps 3 to 5 described above shall not be necessary.

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

3.2.3. 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.

3.2.3.1. In the 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.

3.2.3.2. Need to appear in person

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.

3.2.3.3. Relationship with the natural person

Documentary proof of the link between a natural person identified in a certificate and the public or private entity, company or organisation will be given in the form of the internal records (employment contract or commercial contract, the deed indicating their position or the document inviting them to join the organisation, etc.) of each entity, etc.

3.2.4. Non-validated subscriber information

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

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 methods may be used to perform this check:

- An “identity check phrase” or other personal authentication methods consisting of information that only the natural person identified in the certificate knows and which allows them to automatically renew their certificate, as long as the maximum period allowed by law has not expired.
- 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.

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.

3.3.2. 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 an electronically signed revocation request by the subscriber or the natural person identified in the certificate.
- The use of an “identity check phrase” consisting of information that only the natural person identified in the certificate knows and which allows them to automatically revoke their 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

Suspension requests can be made by the subscriber 24 hours a day, seven days a week using the form available on the vinCAsign website, choosing the "suspension" option (https://www.vincasign.net).

When, during office hours, the subscriber wishes to initiate a revocation request but there are doubts about their identity, the status of their certificate will be changed to suspended.

4. Certificate life-cycle operation requests

4.1. Certificate issuance request

4.1.1. Legitimisation for requesting issuance

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

Furthermore, prior to the issuance and delivery of a certificate, there must exist a certificate request either in the agreement itself or in a specific certificate request form.

When the requester is not the same person as the subscriber, the subscriber must give their authorisation for the requester to make a request. The legally valid means of doing so will be through a certificate request form signed by said requester in the name of the public or private entity, company or organisation.

4.1.2. Registration procedure and responsibilities

VinCAsign receives certificate requests from public or private entities, companies or organisations.

The requests are presented as an electronic document filled in by the public or private entity, company or organisation and addressed to vinCAsign, and the latter shall include the details of the person to which the certificates are issued. The request shall be made by the operator who is authorised by the subscriber (the certification officer) and who is named in the agreement signed between the subscriber and vinCAsign.

The request must be presented together with documentation proving the identity and other details of the natural person identified in the certificate, in accordance with that established in section 3.2.3. It must also be presented with a physical address or other information that makes it possible to contact the natural person identified in the certificate.

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 qualified certificates, the documentation used to approve requests must be stored and duly recorded, guaranteeing its security and integrity, for a period of 15 years from the expiry of the certificate, even when the certificate is revoked prematurely.

4.2.2. Approval or rejection of requests

If the checks performed on the information are satisfactory, vinCAsign approves the certificate request and proceeds to issue and deliver the certificate.

If the information proves to be incorrect, or if it is suspected to be incorrect or that it could affect the reputation of the Certification Authority or that of the subscribers, vinCAsign rejects the request or postpones its approval until it has performed the necessary additional checks that it deems appropriate.

If the information is still seen to be incorrect after the additional checks, vinCAsign definitively denies the request.

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.

4.2.3. Term for resolving requests

VinCAsign deals with certificate requests by order of arrival within a reasonable time period, and a guarantee regarding the maximum allowed period may be specified in the certificate issuance agreement.

Requests remain active until they are either approved or rejected.

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.

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.
- 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 article 11 of Spanish Law 59/2003 of 19 December in the certificate, in accordance with that set out in sections 3.1.1 and 7.1.
- States the date and time at which the certificate was issued.

4.3.2. 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 assistance of the subscriber (company, entity or organisation), in accordance with the provisions of sections 3.2.2 and 3.2.3.
- Submit the certificate delivery and acceptance form to the natural person identified in the certificate with the assistance of the subscriber (company,

entity or organisation). Said form must contain at least the following information:

- 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 on 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.
- The data of the deed of delivery and acceptance.

- Obtain the electronic or written signature of the person identified in the certificate.

The subscriber shall assist in these processes. It must keep documentary records of previous deeds and safeguard the aforementioned original documents (delivery and acceptance forms), sending vinCAsign an electronic copy and, whenever it so requires, the original copies.

4.4.2. Certificate acceptance process

The natural person identified in the certificate accepts the certificate by signing the delivery and acceptance form.

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 1.4.
- When the certificate is to be used together with an SSCD, acknowledge its capacity to produce qualified digital signatures; i.e., ones which are equivalent to handwritten signatures, as well as other types of digital 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.
- 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.

4.5.2. Use by the subscriber

4.5.2.1. Obligations of the certificate subscriber

VinCAsign contractually obliges the 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 1.4.
- 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.
    - 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.
    - Where applicable, the loss, alteration, non-authorised use, theft or compromised security of the card.
- Pass on the responsibility for complying with the specific obligations relating to the certificates to the natural persons identified in the certificates and implement mechanisms to ensure effective compliance.
- 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.

4.5.2.2. Civil liability of the signer

VinCAsign obliges the signer to ensure that:

- All the information supplied by the signer and contained in the certificate is correct.
- The certificate is used exclusively for legal, authorised uses, in accordance with the Certification Practice Statement.
- No non-authorised persons ever have access to the private certificate key, and that the signer is the only party responsible for damage caused by their failure to protect 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.

4.5.2.3. Civil liability of the certificate subscriber

VinCAsign contractually obliges the subscriber to ensure that:

- All the statements contained in the certificate are correct.
- All the information supplied by the subscriber and contained in the certificate is correct.
- The certificate is used exclusively for legal, authorised uses, in accordance with the Certification Practice Statement.
- No non-authorised persons ever have access to the private certificate key, and that the signer is the only party responsible for damage caused by their failure to protect the private key.
- The subscriber is an end entity 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 digital signature or on any of the certificates in the hierarchy.
- Acknowledge that the validated digital signatures produced using a Secure Electronic Signature Creation Device (SSCD) are legally classed as qualified digital signatures; i.e. they are equivalent to handwritten signatures, and that the certificate allows for the creation of other types of digital 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 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.

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.

Alternatively, the subscriber may authorise the requester to perform the request. The legally valid means of doing so will be through a certificate renewal request form signed by the entity, company or organisation.

4.7.3. Renewal request procedures

4.7.3.1. Making the request

VinCAsign receives certificate requests from public or private entities, companies or organisations.

The certificate renewal request can be made either in paper or electronic format by the public or private entity, company or organisation, including the details of the persons to whom the certificates will be issued.

The request must state that the certificate data have not changed; the only changes allowed will be to the physical address or other contact data of the natural person indicated in the certificate.

4.7.3.2. 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.

4.7.3.3. Approval or rejection of requests

If the checks performed on the information are satisfactory, vinCAsign approves the certificate renewal request and proceeds to issue and deliver the certificate.

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 certificate that the certificate has been issued.

4.7.5. Certificate acceptance process

The natural person identified on the certificate accepts the certificate by signing the delivery and acceptance form, using either a digital or handwritten signature, in the presence of the certification officer of the public or private entity, company or organisation.

4.7.6. Publication of the certificate

VinCAsign publishes the renewed certificate in the repository referred to in section 2.1, 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

Certificate modifications, except modifications to certified public keys, which shall be considered renewals, shall be dealt with as a new certificate issuance, and the provisions of sections 4.1, 4.2, 4.3 and 4.4 shall therefore apply.

4.9. Revocation and suspension of certificates

4.9.1. Reasons for revoking certificates

VinCAsign revokes certificates under any of the following circumstances:

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 that affect the subscriber or the natural person identified in the certificate:

a) Termination of the legal relationship between vinCasign and the subscriber 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 subscriber or the person identified in the certificate of the obligations, responsibilities and guarantees set out in the corresponding legal documents.

e) The unforeseeable incapacity or death of the owner of the keys.

f) The expiration of the legal person that is the certificate subscriber, the end of the subscriber's authorisation to the owner of the keys, 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.

4) Other circumstances:

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

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.

4.9.2. Legitimisation for requesting revocation

The following parties may request the revocation of a certificate:

- The person identified in the certificate.
- The certificate subscriber, through the certification officer.

4.9.3. Revocation request procedures

Entities that wish to revoke a certificate must send a request to vinCAsign. 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.

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, 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 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.

Both the revocation management service and the consultation service are considered to be critical services and are classed as such in vinCasign's business continuity and contingency plan.

4.9.4. Time period for requesting revocation

Revocation requests shall be sent immediately, as soon as the cause of revocation is known.

4.9.5. Time period for processing revocation requests

Revocation requests shall be processed as soon as they are received, within vinCAsign's normal office hours.

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 to check the status of certificates is to consult the most recent copy of the Certificate Revocation List published by the Víntegris Certification Authority.

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:

- http://crl1.vincasign.net/casub.crl
- http://crl2.vincasign.net/casub.crl

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

- http://ocsp1.vincasign.net
- http://ocsp2.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 another CRL listing new revocations may be issued before this time.

The CRL lists revoked or suspended certificates until the moment of their expiration.

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://www.vincasign.net/validation.

The most recent CRL can be obtained by downloading:

- *ROOT CA: vinCAsign Root Authority*
    - http://crl1.vincasign.net/caroot.crl
    - http://crl2.vincasign.net/caroot.crl

- *INTERMEDIATE CA: vinCAsign Global Authority*
    - http://crl1.vincasign.net/casub.crl
    - http://crl2.vincasign.net/casub.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 all efforts to ensure that the service is resumed as soon as possible and at most within a period of 24 hours.

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

4.9.10. Obligation to consult the services for checking certificate status

Relying parties are obliged to check the status of 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:

- *http://ocsp1.vincasign.net*
- *http://ocsp2.vincasign.net*

4.9.12. Special requirements for compromised private keys

As far as possible, all the participants in the certification services are informed of the fact that the vinCAsign private key has been compromised through the publication of this fact on the vinCAsign website and, if considered necessary, through additional means including printed notifications.

4.9.13. Reasons for suspending certificates

VinCAsign certificates may be suspended due to the following causes:

- When so requested by the subscriber or natural person identified on the certificate.

- When the documentation required for the revocation request is sufficient but the subscriber or natural person identified on the certificate cannot be duly identified.
- When the documentation required for the revocation request is insufficient, even though the subscriber or natural person identified on the certificate can be duly identified.
- When the documentation required for the revocation request is insufficient and neither can the subscriber or natural person identified on the certificate be duly identified.
- If the certificate is not used for an extended, previously-established period of time.
- If it is suspected that the key has become compromised, until this fact can be confirmed. In this case, vinCAsign must ensure that it is not suspended for more time than is necessary to confirm whether or not the key has become compromised.

4.9.14. Suspension requests

Certificate suspension requests can be made by:

- The natural person identified in the certificate.
- The certificate subscriber, through authorised representatives.

4.9.15. Suspension request procedures

- The user accesses a web form on the vinCAsign website.
- Once they have filled in the form with their National ID No./Tax ID Code No. and letter, a temporary password is sent to the email address with which the user requested the certificate.
- The user then uses this password to confirm their suspension request.
- Once the request has been confirmed, vinCAsign proceeds to suspend the certificate.

The subscriber and, in all cases, the natural person identified in the certificate are informed of the change in status of the suspended certificate.

4.9.16. Maximum suspension period

Certificates may be suspended for a maximum period of one week.

4.10. Subscription expiry

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.

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. Policy and practices for session key escrow and recovery

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 and incident resolution within 24 hours.

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 RAC) 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.

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 and purported qualifications.
- 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 obtains the unequivocal consent of the potential employee to perform these checks, and processes and protects their personal data in accordance with Spanish Organic Law 15/1999 of 13 December on Personnel Data Protection and Spanish Royal Decree 1720/2007 of 21 December, which approves the Implementing Regulations of Spanish Organic Law 15/1999 of 13 December on Personnel Data Protection.

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.
- 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

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:

- Are protected from tampering by using signatures on the files in which they are stored.
- 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.
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 must be performed daily, monthly and annually.

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.
- 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.
- 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.

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 Authority.

5.5.5. Time and date stamp 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. Recognition 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.

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 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.

It should be reasonably possible to avoid any failure to meet the objectives of this Contingency Plan, unless said failure is due to non-compliance of the CA in implementing said process.

5.7.4. Business continuity after a disaster

VinCAsign will re-establish the critical services (Revocation and publication of revoked statuses) in accordance with the business continuity and contingency plan, restoring normal operation of said services within 24 hours following a disaster.

If necessary, vinCAsign has an alternative centre for operating the certification services 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) 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 .
- Communication, also the Ministry of Industry , Energy and Tourism, the opening of any bankruptcy proceedings taken against vinCAsign As Well As any other relevant circumstances that would 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 the intermediate certification authority "vinCAsign Global Authority" is created by the root certification authority "vinCAsign Root Authority" in accordance with the ceremony procedures of vinCAsign, within the high-security perimeter used fir 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. 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 ROOT Authority	**4,096 bits**	**11 years**
VinCAsign Global Authority	4,096 bits	6 years
- Corporate natural person certificate, issued in SSCD	2,048 bits	1 year
- Corporate natural person certificate issued in software	2,048 bits	1 year

- Corporate representative natural person certificate issued in SSCD	2,048 bits	1 year
- Corporate representative natural person certificate issued in software	2,048 bits	1 year
- High-level public employee natural person certificate	2,048 bits	1 year
- Medium-level public employee natural person certificate	2,048 bits	1 year
- High-level body electronic stamp certificate	2,048 bits	1 year
- Medium-level body electronic stamp certificate	2,048 bits	1 year

More information can be found on the following web pages:

- Corporate natural person certificate, issued in SSCD	https://www.vincasign.net/policy/es/PDS-PF-hard/
- Corporate natural person certificate issued in software	https://www.vincasign.net/policy/es/PDS-PF-soft/
- Corporate representative natural person certificate issued in SSCD	https://www.vincasign.net/policy/es/PDS-REP-hard/
- Corporate representative natural person certificate issued in software	https://www.vincasign.net/policy/es/PDS-REP-soft/
- High-level public employee natural person certificate	https://www.vincasign.net/policy/es/PDS-EP-ALTO/
- Medium-level public employee natural person certificate	https://www.vincasign.net/policy/es/PDS-EP-MEDIO/
- High-level body electronic stamp certificate	https://www.vincasign.net/policy/es/PDS-SELLO-ALTO/
- Medium-level body electronic stamp certificate	https://www.vincasign.net/policy/es/PDS-SELLO-MEDIO/

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.

6.1.2. Private key delivery to the signer

For certificates in a secure signature creation device, the private key is duly protected inside said secure device.

For certificates in software, the signer's private key is created in the computer system the signer uses when the certificate request is made, and in this case, therefore, the private key is not sent.

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.

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 ROOT Authority" is 4096 bits.

The length of the keys of the subordinate "vinCAsign Global 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.

6.1.7. Public key parameter quality checks

- 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.

6.1.9. Key usage purposes

The keys for the CA certificates may be used exclusively for signing certificates and CRLs.

The keys for the end entity certificates may be used exclusively for digital signatures and content commitment.

6.2. Private key protection

6.2.1. Cryptographic module standards

In relation to the modules that manage the keys of vinCAsign and digital 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

The CA's private keys must be activated by more than one person. The policy specified in this CPS is that the keys must be activated by **2 to 5** people.

The cryptographic devices are physically protected as described in this document.

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 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 in the external storage centre. At least two people will be required to recover the CA's private key in the initial cryptographic device.

The subscriber may store the keys delivered in software for as long as the certificate is valid. After this period it must destroy them, ensuring beforehand that there exists no information encrypted with the public key.

Only in the case of encryption certificates, the subscriber may store the private key for however long it wishes. In this case vinCAsign will also keep a copy of the private key associated with the encryption certificate.

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

The private keys of the Certification Authority are stored in encoded format in vinCAsign's cryptographic production modules.

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 CA's 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 keys, the certificate of the public keys associated with the keys will be revoked.

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 decoded private key may still be used even after expiry of the certificate.

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 size.
- Configuration of users and permits.
- 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.

6.5.2. Computer security rating

The certification authority and registration applications used by vinCAsign are trustworthy.

6.6. Life cycle technical controls

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 correction 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.

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.

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.

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:

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.

Certificate generation

Authentication for the issuance process is performed using a system of M out of N operators to activate vinCAsign's private key.

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.

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.

6.9. Time source entities

VinCAsign has a time synchronisation procedure coordinated with the ROA (Royal Institute and Observatory of the Armada) in San Fernando via NTP.

7. Certificate profiles and revoked certificate lists

7.1. Certificate profiles

All the qualified certificates issued under this policy comply with standard X.509 version 3, RFC 3739 and ETSI 101 862 “Qualified Certificate Profile”.

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.

Name constraints may also be established in relation to the certificates in the corresponding authentication, digital signature, encryption or electronic evidence policy, as long as they are objective, proportionate, transparent and non-discriminatory.

7.1.6. Certificate policy object identifier (OID)

All the certificates include a certificate policy identifier under which they were issued, in accordance with the structure indicated in point 1.2.1

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 has requested to be registered as a certification services provider by the Ministry of Industry and to undergo the checks considered necessary by said body.

VinCAsign's commitment to the security and quality of its services is reflected by the fact that it holds 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 20.2 of Spanish Law 59/2003, of 19 December, on electronic signatures, and with a policy limit of at least 3,000,000 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 20.2 of Spanish Law 59/2003, of 19 December, on electronic signatures, and with a policy limit of at least 3,000,000 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

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 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.

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.

9.3.6. Other information disclosure circumstances

Not stipulated.

9.4. Personal data protection

To provide its services, vinCAsign must gather and store certain information, including personal data. Such information is obtained from the subscribers based on the corporate relationship that links them to the owners of the keys (employees, manager, partners, etc.) or, in certain cases, directly from the parties in question, either with their explicit consent or without it, in cases where the law allows personal data to be gathered without the consent of the affected party.

VinCAsign gathers only that data which is necessary to issue and maintain the certificate.

VinCAsign has created a privacy policy in accordance with Spanish Organic Law 15/1999, of 13 December, on Personal Data Protection, and this Certification Practice Statement includes the security aspects and procedures required of the security document envisaged in Spanish Royal Decree 1720/2007, of 21 December, which approves the Implementing Regulations of Spanish Organic Law 15/1999, of 13 December, on Personal Data Protection. This Certification Practice Statement is therefore deemed to be a security document.

VinCAsign does not disclose or transfer personal data, except in the cases listed in sections 9.3.2 to 9.3.6 and in section 5.8, in the event that it terminates its certification services.

In accordance with personal data protection regulations, the data is protected from loss, destruction, damage, falsification and illegal or non-authorised processing, in accordance with the provisions of this document, which comply with the obligations set out in Spanish Royal Decree 1720/2007, of 21 December, which approves the Implementing Regulations of Spanish Organic Law 15/1999, of 13 December, on Personal Data Protection.

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 digital 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 digital 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. Representations and warranties

9.6.1. Víntegris Certification Authority representations

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[2], which is also classed as an informative text, and which complies with the content specified in Annex A of ETSI EN 319 411-1 v1.0.0 (2015-06). This document may be sent by electronic means, using a long-lasting means of communication and comprehensible language.

[2] PKI Disclosure Statement.

VinCAsign provides 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 4.5.2, 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.
- Restrictions of use for the certificate, including those described in section 1.4.2
- 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. Subscriber and relying party representations and warranties

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 errors of fact in the information contained in the certificates which the Certification Authority is aware of or has generated.
- 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 and signer identified therein and that the certificate has been accepted in accordance with section 4.4
- 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 deposit.

Furthermore, vinCAsign guarantees to the subscriber and the relying party:

- That the certificate contains the information that must be included in a qualified certificate, as specified by article 11 of Spanish Law 59/2003, of 19 December.
- 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 Authority, 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 9.6.2.

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 Authority.

9.6.5. Indemnities

9.6.5.1. Indemnification by the subscriber

In the contract with the subscriber, VinCAsign includes a clause through which the subscriber undertakes to hold the Certification Authority 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. Indemnification by the relying party

In the PDS, VinCAsign includes a clause through which the relying party undertakes to hold the Certification Authority 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 suspended or 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 Authority specifies that the service provision, including the certification policy and practices, shall be subject to Spanish Law.

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 9.6.1 (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.