1. IoT seal certificate

INFORMATIVE TEXT-PDS

APPLICABLE TO

IoT SEAL CERTIFICATES

This document contains the essential information that must be known in relation to the certification service of the vinCAsign Certification Authority.
This document follows the structure defined in Annex A of the ETSI EN 319 411-1, in accordance with the instructions of paragraph 4.3.4 of the ETSI EN 319 412-5.

1.1 Contact details

1.1.1 Organisation responsible

The vinCAsign Certification Authority, hereinafter "vinCAsign", is an initiative of:

VINTEGRIS
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

1.1.2 Contact

For any queries, please contact:

VINCASIGN
INFO@VINCASIGN.NET

TEL.: (+34) 902 362 436 / (+34) 934 329 098
FAX: (+34) 934 329 344

1.1.3 Contact for revocation processes

For any queries, please contact:

VINCASIGN
INFO@VINCASIGN.NET
TEL.: (+34) 902 362 436 / (+34) 934 329 098
FAX: (+34) 934 329 344

1.2 Type and purpose of the IoT seal certificate

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

These certificates are not issued to the public under any circumstances.

These certificates guarantee the identity of the subscriber, the legal person, entity or organisation that are indicated in the certificate. These certificates are for use in the scope of Internet of Things (IoT).
These certificates guarantee the univocal identification of its location.
These certificates do not allow the encryption of own 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 perform the digital signature function)

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.

This certificate has OID

- 1.3.6.1.4.1.47155.1.7.2
- 0.4.0.194112.1.1

1.2.1 Issuing Certification Authority

IoT seal certificates are issued by vinCAsign and identified using the aforementioned data.

1.3 Limits to the use of certificates

1.3.1 Limits of use int it operation

IoT's electronic seal certificate certification service must be used provided by vinCAsign exclusively for the uses authorised in the agreement signed between VINTEGRIS and the SUBSCRIBER and which are listed below (“obligations in its use” section).

There is also the obligation to use the certification service in accordance with the instructions, manuals or procedures supplied by vinCAsign.

The seal creator must comply with any laws and regulations that may affect their right to use the encryption tools.

In its use, no inspection, alteration or reverse engineering of vinCAsign's digital certification services can be taken without prior express permission.

1.3.2 Limits to use for validators

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

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, seal creator or custodian shall assume any liability arising from the content linked to the use of a certificate.

Likewise the subscriber, seal creator or custodian shall accept any liability arising from the use of certificates outside of the limits and conditions of use set out in this informative text or in the agreements with the subscribers, as well as any other improper use thereof

derived from this section or any use that could be considered improper pursuant to current legislation.

1.4 Subscribers' obligations

1.4.1 Generation of keys

The subscriber authorises vinCAsign to generate public and private keys, and requests, in their name, the issuance of the IoT's electronic seal.

1.4.2 Certificate requests

The subscriber is obliged to make the IoT's electronic seal requests in accordance with the procedure and, if necessary, the technical components supplied by vinCAsign, in accordance with the content of the Certification Practice Statement (CPS) and the vinCAsign operations documents.

1.4.3 Veracity of information

The subscriber shall be responsible for ensuring that all the information included in the certificate request is exact, complete for the purpose of the certificate and up-to-date at all times.

The subscriber must inform vinCAsign immediately of any errors detected in the certificate once it has been issued, as well as any changes to the information provided and/or registered for the issuance of the certificate.

1.4.4 Storage obligations

The subscriber is obliged to store all the information they generate in their activity as a registration authority.

1.5 Seal creators' obligations

1.5.1 Storage obligations

The seal creator must store the personal identification number or any technical information provided by vinCAsign, the private keys and, if applicable, specifications belonging to vinCAsign that they have been provided with. The seal creator must store the personal identification number (PIN).

If the private certificate key is lost or stolen or if the seal creator suspects that the private key is no longer reliable for any reason, the subscriber must immediately notify vinCAsign of this fact.

1.5.2 Obligations in its correct use

The electronic seal certificate certification service for IoT provided by vinCAsign must be used exclusively for the authorized uses in the CPS and in any other instruction, manual or procedure given to the subscriber.
Any law and regulation that may affect the right to use the cryptographic tools used must be complied with.
Measures of inspection, alteration or decompilation of the digital certification services provided may not be adopted.

The seals creator must discontinue the use of the private key in the event of a compromise of that key, in case of revocation and revocation, or compromise of the keys of the CA.

The seal creator recognises that:

a) When they use any certificate, as long as the certificate has not expired or been suspended or revoked, they must have accepted said certificate and it must be operative.

b) They are not acting as a certification authority and therefore may not use private keys corresponding to the public keys contained in the certificates for the purpose of signing a certificate.

1.5.3 Prohibited operations

The seal creator may not use their private codes, certificates or any other technical information provided by vinCAsign to perform any operations prohibited by the applicable law.

The digital certification services provided by vinCAsign have not been designed for, nor may they be used or resold as devices for the control of dangerous situations, or for uses that require error-proof operations, such as the operation of nuclear facilities, air traffic navigation or communication systems, air traffic control systems, or weapons control systems, where any error could directly lead to death, personal injury or extreme environmental damage.

1.6 Validators' obligations

1.6.1 Informed decision

VinCAsign informs validators that they have access to enough information to take informed decisions regarding the validation of a certificate and the reliability of the information it contains.

Furthermore, the validator shall recognise that the vinCAsign Register and Certificate Revocation Lists (the CRLs) must be used in accordance with the vinCAsign CPS and shall undertake to comply with the technical, operational and security requirements described in the CPS.

1.6.2 Digital signature validation requirements

Checks shall normally be performed automatically by the validator's software and shall always be performed in accordance with the CPS and the following requirements:

- A software program must be used that is suitable for validating digital signatures with the algorithms and key lengths authorised in the certificate and/or executing any other encryption operation, and establishing a chain of certificates on which the digital signature to be validated is based, as digital signatures shall be validated using this chain of certificates.

- It is necessary to ensure that the chain of certificates identified is the most suitable one for the digital signature being validated, as a digital signature may be based on more than one chain of certificates and it is up to the validator to ensure the use of the most suitable chain for validation purposes.

- The revocation status of the certificates in the chain must be checked against the information supplied to the vinCAsign Register (with CRLs, for example) to establish the validity of all the certificates in the certificate chain, as a digital signature may only be considered as properly validated if each and every one of the certificates in the chain are correct and valid.

- It must be ensured that all the certificates in the chain authorise the use of the private key by the subscriber of the certificate and the seal creator, as it is possible that some of the certificates may include usage limits that affect the trustworthiness of the digital signature to be validated. Each certificate in the chain has an indicator that shows the applicable conditions of use and which must be checked by the validators.

- The signature of all the certificates in the chain must be technically validated before the trustworthiness of the certificate used by the seals creator can be guaranteed.

1.6.3 Trustworthiness of non-validated certificates

If the validator trusts a non-validated certificate, they shall assume responsibility for all the risks resulting from this action.

1.6.4 Purpose of validation

In virtue of the correct validation of the IoT seal certificates, in accordance with this informative text, the validator may trust the identification and, where applicable, the public key of the seal creator, within the corresponding limits of use, to generate encrypted messages.

1.6.5 Correct use and prohibited activities

The validator may not use any type of information on the status of the certificates or of any other type that has been provided by vinCAsign to perform any operation that is prohibited by the laws that apply to said operation.

The validator may not inspect, interfere with or perform reverse engineering on the technical implementation of the vinCAsign public certification services without prior written consent.

Furthermore, the validator may not intentionally compromise the security of the vinCAsign public certification services.

The digital certification services provided by vinCAsign have not been designed for, nor may they be used or resold as devices for the control of dangerous situations, or for uses that require error-proof operations, such as the operation of nuclear facilities, air traffic navigation or communication systems, air traffic control systems, or weapons control systems, where any error could lead to death, personal injury or extreme environmental damage.

1.6.6 Indemnity clause

The relying party shall hold vinCAsign 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:

- 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.

1.7 VinCAsign's obligations

1.7.1 In relation to the digital certificate service provision

VinCAsign is obliged to:

a) Issue, submit, administer, suspend, revoke and renew certificates in accordance with the instructions supplied by the subscriber, in the cases and for the reasons described in the vinCAsign CPS.

b) Execute the services with the suitable technical and material means and with personnel that have the qualifications and experience specified in the CPS.

c) Comply with the service quality levels as regards technical, operational and security matters, pursuant to the provisions of the CPS.

d) Inform the subscriber, before the certificate expiry date, of the possibility of renewing the certificates, suspending them, lifting the suspension or revoking them, when applicable.

e) Inform any third parties that so request of the status of the certificates, pursuant to the provisions of the CPS regarding the different certificate validation services.

1.7.2 In relation to the register checks

VinCAsign is obliged to issue certificates based on the data supplied by the subscriber. It may therefore perform any checks it considers appropriate as regards the identity and

any other additional personal information of the subscribers and, when necessary, of the seal creators.

These checks may include the justification document provided by the seal creator via the subscriber, if vinCAsign deems it necessary, and any other relevant documents and information provided by the subscriber and/or seal creator.

If vinCAsign detects errors in the data that must be included in the certificates or that justify said data, it may make the changes it deems necessary before issuing the certificate or suspending the issue process and managing the corresponding incident together with the subscriber. If vinCAsign corrects the data without previously managing the corresponding incident with the subscriber, it must inform the subscriber of the data finally included in the certificate.

VinCAsign reserves the right not to issue the certificate when it considers that the justification documents are insufficient to correctly identify and authenticate the subscriber and/or seal creator.

The aforementioned obligations shall be suspended in cases where the subscriber acts as the registration authority and has the corresponding technical elements required to generate keys, issue certificates and record cooperative signature devices.

1.8 Limited guarantees and rejection of guarantees

1.8.1 VinCAsign's guarantee of the digital certification services

VinCAsign guarantees to the subscriber that:

- 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.

- The certificates comply with all the material requirements set out in the CPS.

- The services of revocation and use of the Repository comply with all the material requirements set out in the CPS.

VinCAsign guarantees to the relying party:

- 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 seal creator identified therein and that the certificate has been accepted.

- That, in the approval of the certificate request and issuance of the certificate, all the material requirements set out in the CPS 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. Under no circumstances shall vinCAsign be liable for unforeseeable circumstances or force majeure.

1.8.2 Disclaimer of guarantee

VinCAsign rejects any other guarantee different to the aforementioned that is not legally enforceable.

Specifically, vinCAsign shall not provide guarantees for any software used by any person to sign, verify the signatures of, encrypt or decrypt any digital certificate issued by vinCAsign, or use such a certificate in any other way, except when a written statement exists to the contrary.

1.9 Applicable agreements and CPS

1.9.1 Applicable agreements

The following agreements are applicable to legal person seal certificates:

- Certification services agreement that regulates the relationship between vinCAsign and the subscribing company.

- General service conditions included in the informative text for the certificate or the PDS.

- CPS, which regulates the issuance and use of the certificates.

1.9.2 CPS

VinCAsign certification services are regulated technically and operatively by the vinCAsign CPS and subsequent updates, as well as by complementary documentation.

The CPS and operative documentation is modified on a regular basis in the Register and can be accessed via the internet at: https://policy.vincasign.net.

1.10 Rules for the trustworthiness of long-term signatures

Point b.2 of article 18 of Spanish Law 59/2003, of 19 December, on digital signatures refers to the obligation of certification authorities to inform requesting parties of the mechanisms to ensure the trustworthiness of digital signatures on a document over a period of time.

VinCAsign informs parties requesting IoT seal certificates that its service does not guarantee the trustworthiness of digital signatures over an extended period of time.

To ensure the trustworthiness of a document's digital signature over an extended period of time, vinCAsign recommends using the standards indicated in section 7.3 (Rules for the trustworthiness of long-term signatures) of the Technical Interoperability Standard Application Guide, "Policy governing digital signatures and certificates of the administration".

The general considerations for the trustworthiness of long-term signatures are set out in sub-section IV.3 of the digital signatures Technical Interoperability Standard.

1.11 Confidentiality policy

VinCAsign may not reveal or be obliged to reveal any confidential information regarding certificates without a specific request:

a) from the person with respect to whom vinCAsign is obliged to keep the information confidential; or

b) in the form of a court order, an administrative order or any other type of order contemplated in the current legislation.

Notwithstanding, the subscriber accepts that certain information, personal or otherwise, provided in certificate requests, may be included in their certificates and in the mechanism used to check the certificate status, and that said information shall not be considered as confidential under the law.

VinCAsign shall not release the data given specifically for the purpose of providing the certification service to anyone.

1.12 Privacy policy

VinCAsign has a privacy policy, set out in section 9.4 of the CPS, as well as specific privacy regulations relating to the registration process, the confidentiality of records, protection of access to personal data, and user consent.

It also adheres to the policy that the documentation used to approve requests must be stored and duly registered, guaranteeing its security and integrity, for a period of 15 years from the expiry of the certificate, even when the certificate is revoked prematurely.

1.13 Reimbursement policy

Under no circumstances shall vinCAsign reimburse the costs of the certification service.

1.14 Applicable law, competent jurisdiction, and complaints and disputes regime

Relations with vinCAsign shall be governed by the Spanish law in the area of trust services in force, as well as by the civil and commercial legislation in whatever matters.
The competent jurisdiction is that indicated in the Law 1/2000, of 7 January, for Civil Procedure.
In case of discrepancy between the parties, the parties will seek the prior amicable settlement.For this purpose, the parties shall send a communication to vinCAsign by any means which acts as proof, to the contact address listed in point 1.1.2. of this PDS.
If the parties do not reach an agreement, either party may submit the dispute to the civil jurisdiction, subject to the Courts of the registered office of vinCAsign.
An extension of the dispute resolution information is available at the internet address www.vintegris.com

1.15 Quality seals and accreditations

As regards the certification of trustworthy systems, vinCAsign has accreditation corresponding to the CryptoSec Openkey CA solution by Realia Technologies, HSM Cryptosec PCI: the certificates FIPS 140 level 3 or Common Criteria EAL 4+ (with the supplement ALC_FLR.1).

Víntegris is certified UNE-ISO / IEC 27001: 2014 Information technology. Security techniques. Information Security Management Systems (ISMS) with the scope: "Information Systems and all the internal business processes that support the integral services of: Strategic Consulting of Information Security, Design, Implementation and Management of Architectures Of Information Security; Life cycle management of digital certificates (issuance, validation, renewal and revocation); In accordance with the applicable statement of applicability. "

1.16 Inclusion in the list of suppliers

http://www.minetad.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

1.17 Severability of the clauses, survival, entire agreement and notification

The clauses contained in the present informative text are independent of each other. Therefore, if any of the clauses should be considered invalid or non-applicable, the remaining clauses shall still be applicable unless expressly agreed otherwise by the parties.

The requirements set out in sections 9.6.1 (Obligations and responsibility), 8 (Compliance audit) and 9.3 (Confidentiality) of the vinCAsign CPS shall remain extant after termination of the service.

This text expresses the complete will and all the agreements of the parties.

The parties shall inform each other mutually of events via email to the following email address: info@vincasign.net