Informative text - PDS for web authentication certificates

Contents

Change log

Version	Parts changed	Description	Author	Date
1.0	All	Creation of the document	FAD	21/05/2020

1 Web authentication certificate

INFORMATIVE TEXT

APPLICABLE TO

WEB AUTHENTICATION CERTIFICATES

This document contains the essential information to know about the certification service of the vinCAsign Certification Authority.
This document adheres to the structure defined in Annex A of the ETSI EN 319 411-1 standard, in accordance with the instructions detailed in Section 4.3.4 of the ETSI EN 319 412-5 standard.

1.1.1 Contact details

1.1.1.1 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) SPAIN
TEL.: (+34) 934 329 098
FAX: (+34) 934 329 344

1.1.1.2 Contact

For any queries, please contact:

VINCASIGN

INFO@VINCASIGN.NET

TEL.: (+34) 934 329 098

FAX: (+34) 934 329 344

1.1.1.3 Contact for revocation processes

For any queries, please contact:

VINCASIGN

INFO@VINCASIGN.NET

TEL.: (+34) 934 329 098

FAX: (+34) 934 329 344

1.1.2 Type and purpose of web authentication certificates

Web authentication certificates are certificates qualified in accordance with Annex IV of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and they comply with the provisions of the requirements of the CA/Browser Forum established in the latest version of the *"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"* .

These certificates are issued for the unequivocal identification of public sector web pages and electronic office by computer services and applications and the encryption of the transmitted data channel, as well as to provide them with SSL/TSL capabilities.

VinCAsign issues three types of web authentication certificate:

- Electronic Office Certificate: these certificates are issued to the public sector, in accordance with the provisions of Article 38 of Law 40/2015, of 1 October, on the public sector legal regime.

Electronic office certificates are issued in accordance with the average levels of assurance of the certificate profiles established in Point 8 of the document "Electronic Certificate Profiles" of the Sub-Directorate General for Information, Documentation and Publications of the Spanish Ministry of Finance and Public Administrations.

SSL OV (Organisation Validation) certificate: these certificates are issued to public and private entities, commercial and non-commercial entities, and to trademarks and trade names, guaranteeing that the domain to which the certificate refers belongs to the requesting organisation.

- SSL EV (Extended Validation) certificates: these show an additional level of security when issued according to a series of specific criteria to verify the identity of the organisation to which it refers.

The usage information in the certificate profile specifies 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 confirms that the certificate is issued as a qualified certificate.
c) The “User Notice” field describes the use of this certificate.

These certificates have the following OIDs:

- Electronic office:
    - 1.3.6.1.4.1.47155.1.13.1
    - 0.4.0.194112.1.4
    - 2.16.724.1.3.5.5.2
- SSL OV:
    - 1.3.6.1.4.147155.1.14.1

  - 0.4.0.194112.1.4
- SSL EV:
  - 1.3.6.1.4.147155.1.14.2
  - 0.4.0.194112.1.4

1.1.2.1 Issuing Certification Authority

Web authentication certificates are issued by vinCAsign, identified by the aforementioned details.

1.1.3 Limits on the use of certificates

1.1.3.1 Limits on use for applicants of web authentication certificates

Electronic office or SSL certificate applicants must use vinCAsign's service for certifying web authentication certificates exclusively for those uses authorised in the agreement signed between VINTEGRIS and the SUBSCRIBER and which are listed below (in the "Obligations of web authentication certificate applicants" section).

Furthermore, electronic office or SSL certificate applicants must use the digital certification service in accordance with the instructions, manuals or procedures supplied by vinCAsign.

Electronic office or SSL certificate applicants must comply with any laws and regulations that may affect their right to use the encryption tools.

Electronic office or SSL certificate applicants may not take measures to inspect, alter or reverse engineer the vinCAsign digital certification services without express prior consent.

1.1.3.2 Limits on use for validators

The web authentication certificates issued by vinCAsign are used as a website identification mechanism and to provide said websites with SSL/TSL capabilities. Accordingly, these 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 any given time.

The certificates may not be used to sign requests for certificate issue, renewal, suspension or revocation, nor to sign public key certificates of any kind 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 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 web authentication certificate applicants 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 result of this technical impossibility of accessing the content of a message, vinCAsign is not able to issue any evaluation of said content. Accordingly, the subscriber, as the custodian, shall assume any liability arising from the content linked to the use of a certificate.

Likewise the subscriber, or the 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.

1.1.4 Subscribers' obligations

1.1.4.1 Key generation

Applicants will generate the signature keys in their applications, complying with PKI standards, and these must be 2048-bit RSA keys.

1.1.4.2 Certificate requests

The applicant undertakes to request web authentication certificates in accordance with the procedure and, if necessary, the technical components supplied by vinCAsign, in line with the content of the Certification Practice Statement (CPS) and the vinCAsign operations documents.

1.1.4.3 Veracity of information

The subscriber shall be responsible for ensuring that all the information included in the certificate request is accurate, complete for the purpose of the certificate and up-to-date at all times.
VinCAsign shall perform the technical validation of said request, as well as the validation of the data contained therein.
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.

1.1.4.4 Storage obligations

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

1.1.5 Obligations of web authentication certificate applicants

1.1.5.1 Storage obligations

Web authentication certificate applicants 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.

If the certificate's private key is lost or stolen or if the certificate applicant suspects that the private key is no longer reliable for any reason, vinCAsign must be notified immediately of this fact.

1.1.5.2 Obligations of correct use

Electronic office or SSL certificate applicants must use vinCAsign's service for the certification of web authorisation certificates exclusively for the uses authorised in the CPS and in any other instructions, manual or procedure given to the subscriber.

Certificate applicants must comply with any laws and regulations that may affect their right to use the encryption tools.

Certificate applicants may not take measures to inspect, alter or decompile the digital certification services provided.

Certificate applicants must stop using the private key if it is compromised or revoked, or if the CA keys are compromised.

1.1.5.3 Prohibited operations

Web authentication certificate applicants undertake not to use their private keys, certificates or any other technical information provided by vinCAsign to perform any operations prohibited by applicable legislation.

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.

1.1.6 VinCAsign's obligations

1.1.6.1 Concerning the provision of the digital certification service

VinCAsign undertakes 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.

1.1.6.2 Concerning register checks

VinCAsign undertakes 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 personal and supplementary information of subscribers.

These checks may include the justification document provided by the certificate applicant, if vinCAsign deems it necessary, and any other relevant documents and information provided by the subscriber.

vinCAsign will verify that the applicant has control over the domain for which the certificate is requested, using one of the methods established in the CPS.
All checks will be carried out prior to approving certificate issuance.

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 suspend 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 ultimately 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 the certificate applicant.

1.1.7 Limited guarantees and rejection of guarantees

1.1.7.1 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 of which the Certification Authority is aware or has generated.

- That 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 CPS.

- That 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 domain 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 revocation and deposit services.

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

- That the certificate contains the information referred to in Annex IV of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, in relation to qualified web authentication certificates.

- 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.

1.1.7.2 Disclaimer of guarantee

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

Specifically, vinCAsign will provide no 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.

1.1.8 Applicable agreements and CPS

1.1.8.1 Applicable agreements

The following agreements are applicable to web authentication 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.

1.1.8.2 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 online at: https://policy.vincasign.net

1.1.9 Confidentiality policy

VinCAsign may not disclose or be obliged to disclose any confidential information regarding certificates without a specific prior 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 above, 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 disclose the data given specifically for the purpose of providing the certification service to anyone.

1.1.10 Privacy policy

VinCAsign has a privacy policy, as set out in Section 9.4 of the CPS, as well as specific privacy regulations relating to the registration process, the confidentiality of the register, 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 the security and integrity thereof, for a period of 15 years from the expiry of the certificate, even when the certificate is revoked prematurely.

1.1.11 Refund policy

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

1.1.12 Applicable law, competent jurisdiction and system for claims and disputes

Relationships with vinCAsign will be governed by Spanish law on trust services in force at any given time, as well as by civil and commercial legislation, where applicable.

The competent jurisdiction is that indicated in Spanish law 1/2000, of 7 January, on Civil Prosecution.

Should there be a dispute between the parties, they shall first attempt to reach an amicable solution. To this end, the parties must send a communication to vinCAsign by any means that records the contact address specified in point 1.1.1.2. of this PDS.

If such a solution is impossible, either of them may submit the dispute to civil jurisdiction, in the courts that correspond to the registered address of vinCAsign.

Further information on dispute resolution is available at the website www.vintegris.com

1.1.13 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 has UNE-ISO/IEC 27001:2014 information technology certification. Security techniques. Information Security Management Systems (ISMS) with the scope: "Information Systems and all internal business processes that support the comprehensive services of: Strategic Information Security Consulting, Design, Implementation and Management of Information Security Architectures; management of the life cycle of digital certificates (issuance, validation, renewal and revocation); in accordance with the current statement of applicability".

Víntegris has the "eIDAS-compliant" certification for the following services:

- Service for issuing **qualified electronic certificates for electronic signatures**, in accordance with the ETSI EN 319 411-2 standard: [QCP-n], [QCP-n-qscd]

- Service for the issuance of **qualified electronic certificates for electronic seals**, in accordance with the ETSI EN 319 411-2 standard: [QCP-l], [QCP-l-qscd]

- Services for issuing qualified electronic certificates for Public Administrations - **Qualified electronic certificates for Public Employees**, in accordance with the ETSI EN 319 411-2 standard: [QCP-n] - Medium Level, [QCP-n-qscd] - High Level

- Services for the issuance of qualified electronic certificates for Public Administrations - **Qualified certificates for Electronic Seals for the Public Administration**, in accordance with the ETSI EN 319 411-2 standard: [QCP-l] - Medium Level, [QCP-l-qscd] - High level

- Electronic Signature/Qualified Electronic Stamp creation service - **Trusted service that enables signature on the server** (TW4S), in accordance with the CEN TS 419 241-1 standard

1.1.14 Inclusion in the list of providers

vinCAsign is included in the list of **Qualified providers** of trusted electronic services of the Spanish Ministry of Economy and Business Affairs:

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

vinCAsign is included in the "Trust List" of the European Union as a **Qualified provider** of electronic trust services:
https://webgate.ec.europa.eu/tl-browser/#/tl/ES/26

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

The clauses contained in this informative text are independent of each other. Therefore, if any of the clauses should be considered invalid or inapplicable, 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 liability), 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 of, and all the agreements between the parties.

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