Texto de divulgación – PDS de los certificados de Autenticación web

Índice

Índice **2**

Control de cambios 3

1 Certificado de autenticación web **4**

1.1.1 Información de contacto 4

1.1.2 Tipo y finalidad de los certificados de autenticación web 5

1.1.3 Límites de uso del certificado 7

1.1.4 Obligaciones de los suscriptores 9

1.1.5 Obligaciones de los solicitantes de los certificados de autenticación web 10

1.1.6 Obligaciones de VinCAsign 11

1.1.7 Garantías limitadas y rechazo de garantías 12

1.1.8 Acuerdos aplicables y DPC 14

1.1.9 Política de intimidad 14

1.1.10 Política de privacidad 15

1.1.11 Política de reintegro 15

1.1.12 Ley aplicable, jurisdicción competente, y régimen de reclamaciones y disputas 15

1.1.13 Acreditaciones y sellos de calidad 16

1.1.14 Vinculación con la lista de prestadores 17

1.1.15 Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación 17

Control de cambios

Versión	Partes que cambian	Descripción	Autor	Fecha
1.0	Todas	Creación del documento	FAD	21/05/2020
1.1	1.1.2, 1.1.2.1	Modificación por creación de nueva jerarquía TrustServices	VH	15/02/2022
1.2	1.1.1	Actualización de contacto y revisión anual	RRP	22/02/2023

1 Certificado de autenticación web

TEXTO DIVULGATIVO

APLICABLE A LOS

CERTIFICADOS DE AUTENTICACION WEB

Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación de la Entidad de Certificación vinCAsign.

Este documento sigue la estructura definida en el Anexo A de la norma ETSI EN 319 411-1, de acuerdo con las indicaciones del apartado 4.3.4 de la norma ETSI EN 319 412-5.

1.1.1 Información de contacto

1.1.1.1 Organización responsable

La Entidad de Certificación vinCAsign, en lo sucesivo "vinCAsign", es una iniciativa de:

VINTEGRIS

CARRER PALLARS, 99

PLANTA 3

OFICINA 33

08018 BARCELONA

ESPAÑA

TEL.: (+34) 934 329 098

1.1.1.2 Contacto

Para cualquier consulta, diríjanse a:

VINCASIGN INFO@VINCASIGN.NET TEL.: (+34) 934 329 098 / (+34) 917 557 645

1.1.1.3 Contacto para procesos de revocación

Para cualquier consulta, diríjanse a:

VINCASIGN INFO@VINCASIGN.NET TEL.: (+34) 934 329 098 / (+34) 917 557 645

1.1.2 Tipo y finalidad de los certificados de autenticación web

Los certificados de autenticación web son certificados cualificados de acuerdo con el Anexo IV del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por los requerimientos del CA/Browser Forum establecidos en la última versión del *"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"***.**

Estos certificados se emiten para la identificación inequivoca de paginas web y sedes electrónicas del sector público ante servicios y aplicaciones informáticas y cifrado del canal de los datos transmitidos, así como para dotarlas de capacidades SSL/TSL.

VinCAsign emite tres tipos de certificados de autenticación web:

- Certificado de Sede Electrónica: estos certificados se expiden al sector público, de acuerdo con lo establecido en el artículo 38 de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

Los certificados de sede electrónica se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 8 del documento "Perfiles de Certificados electrónicos" de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

- Certificado de SSL OV (Organization Validation): estos certificados se expiden a entidades públicas, privadas, entidades comerciales, entidades no comerciales y a marcas registradas y nombres comerciales, garantizando que el dominio al que hace referencia el certificado pertenece a la organización solicitante del mismo.
- Certificados de SSL EV (Extended Validation): muestran un nivel de seguridad adicional al estar expedido de acuerdo con una serie de criterios específicos de verificación de la identidad de la organización a la que hace referencia.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

    a. Firma digital (para realizar la función de autenticación)

    b. Content commintment (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:

    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) El campo "User Notice" describe el uso de este certificado.

Estos certificados disponen de los OID siguientes:

- Sede electrónica:
    - 1.3.6.1.4.1.47155.1.13.1(si emitido por jerarquía vinCAsign)
    - 1.3.6.1.4.1.47155.2.13.1 (si emitido por jerarquía Vintegris TrustServices)
    - 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(si emitido por jerarquía vinCAsign)
    - 1.3.6.1.4.1.47155.2.14.1 (si emitido por jerarquía Vintegris TrustServices)
    - 0.4.0.194112.1.4
- SSL EV:
    - 1.3.6.1.4.147155.1.14.2 (si emitido por jerarquía vinCAsign)
    - 1.3.6.1.4.1.47155.2.14.2 (si emitido por jerarquía Vintegris TrustServices)
    - 0.4.0.194112.1.4

1.1.2.1 Entidad de Certificación emisora

Los certificados de autenticación de web son emitidos por VinCAsign, identificada mediante los datos indicados anteriormente.

1.1.3 Límites de uso del certificado

1.1.3.1 Límites de uso dirigidos a los solicitantes de los certificados de autenticación web

El solicitante del certificado de sede electrónica o de SSL ha de utilizar el servicio de certificación de certificados de autenticación web prestado por VinCAsign exclusivamente para los usos autorizados en el contrato firmado entre VINTEGRIS y el SUSCRIPTOR, y que se reproducen posteriormente (sección “obligaciones de los solicitantes de certificados de autenticación web”).

Asimismo, el solicitante del certificado de sede electrónica o de SSL se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por VinCAsign.

El solicitante del certificado de sede electrónica o de SSL ha de cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.

El solicitante del certificado de sede electrónica o de SSL no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de vinCAsign, sin previo permiso expreso.

1.1.3.2 Límites de uso dirigidos a los verificadores

Los certificados de autenticación web emitidos por VinCAsign se emplean como mecanismo de identificación de sitios web y para dotar a dichos sitios web de capacidades SSL/TSL. Por ello, estos certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de VinCAsign (https://www.vincasign.net)

El empleo de los certificados digitales en operaciones que contravienen este texto de divulgación, o los contratos con los suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a VinCAsign, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el solicitante del certificado de autenticación web o cualquier tercero.

VinCAsign no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de VinCAsign emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, como la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización de este fuera de los límites y condiciones de uso recogidas en este texto de divulgación, o en los contratos con los suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.1.4 Obligaciones de los suscriptores

1.1.4.1 Generación de claves

El solicitante generará las claves de firma en sus aplicaciones, cumpliendo los estándares de PKI, y debiendo ser claves RSA con una longitud de 2048 bits.

1.1.4.2 Solicitud de certificados

El solicitante se obliga a realizar las solicitudes de certificados de autenticación web de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados por VinCAsign, de conformidad con lo que se establece en la declaración de prácticas de certificación (DPC) y en la documentación de operaciones de VinCAsign.

1.1.4.3 Veracidad de la información

El suscriptor se responsabiliza de que toda la información incluida en su solicitud del certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

VinCAsign realizará la validación técnica de dicha solicitud, así como la validación de los datos contenidos en la misma.

El suscriptor tiene que informar inmediatamente a VinCAsign de cualquier inexactitud detectada en el certificado una vez se haya emitido, así como de los cambios que se produzcan en la información aportada y/o registrada para la emisión del certificado.

1.1.4.4 Obligaciones de custodia

El suscriptor se obliga a custodiar toda la información que genere en su actividad como entidad de registro.

1.1.5 Obligaciones de los solicitantes de los certificados de autenticación web

1.1.5.1 Obligaciones de custodia

El solicitante del certificado de autenticación web se obliga a custodiar el código de identificación personal o cualquier soporte técnico entregado por VinCAsign, las claves privadas y, si fuese necesario, las especificaciones propiedad de VinCAsign que le sean suministradas.

En caso de pérdida o robo de la clave privada del certificado, o en caso de que el solicitante del certificado sospeche que la clave privada ha perdido fiabilidad por cualquier motivo, dichas circunstancias han de ser notificadas inmediatamente a VinCAsign.

1.1.5.2 Obligaciones de uso correcto

El solicitante del certificado de sede electrónica o de SSL tiene que utilizar el servicio de certificación de certificados de autenticación web prestado por VinCAsign, exclusivamente para los usos autorizados en la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

El solicitante del certificado tiene que cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas empleadas.

El solicitante del certificado no podrá adoptar medidas de inspección, alteración o descompilación de los servicios de certificación digital prestados.

El solicitante del certificado debe dejar de emplear la clave privada en caso de compromiso de dicha clave, de revocación, o de compromiso de las claves de la CA.

1.1.5.3 Transacciones prohibidas

El solicitante del certificado de autenticación web se obliga a no utilizar sus claves privadas, los certificados o cualquier otro soporte técnico entregado por VinCAsign en la realización de transacción alguna prohibida por la ley aplicable.

Los servicios de certificación digital prestados por VinCAsign no han sido diseñados ni permiten su utilización o reventa como equipos de control de situaciones peligrosas, o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de

control de tráfico aéreo o sistemas de control de armamento, en las que un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

1.1.6 Obligaciones de VinCAsign

1.1.6.1 En relación con la prestación del servicio de certificación digital

vinCAsign se obliga a:

a) Emitir, entregar, administrar, suspender, revocar y renovar certificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPC de vinCAsign.

b) Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPC.

c) Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPC, en los aspectos técnicos, operativos y de seguridad.

d) Notificar al suscriptor, con anterioridad a la fecha de expiración de los certificados, de la posibilidad de renovarlos, así como la suspensión, alzamiento de esta suspensión o revocación de los certificados, cuando se produzcan dichas circunstancias.

e) Comunicar a las terceras personas que lo soliciten, el estado de los certificados, de acuerdo con lo que se establece en la DPC para los diferentes servicios de verificación de certificados.

1.1.6.2 En relación con las comprobaciones del registro

VinCAsign se obliga a la emisión de certificados en base a los datos suministrados por el suscriptor, por lo cual podrá realizar las comprobaciones que considere oportunas respecto de la identidad y otras informaciones personales y complementarias de los suscriptores.

Estas comprobaciones podrán incluir la justificación documental aportada por el solicitante del certificado, si VinCAsign lo considera necesario, y cualquier otro documento e información relevantes facilitados por el suscriptor.

VinCAsign verificará que el solicitante tiene el control sobre el dominio para el que se solicita el certificado, utilizando uno de los métodos establecidos en la DPC.

Todas las comprobaciones se realizarán previamente a la aprobación de la emisión del certificado.

En el caso que VinCAsign detecte errores en los datos que se deben incluir en los certificados o que justifican estos datos, podrá realizar los cambios que considere necesarios antes de emitir el certificado o suspender el proceso de emisión y gestionar con el suscriptor la incidencia correspondiente. En caso de que VinCAsign corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

VinCAsign se reserva el derecho a no emitir el certificado, cuando considere que la justificación documental resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del solicitante del certificado.

1.1.7 Garantías limitadas y rechazo de garantías

1.1.7.1 Garantía de VinCAsign por los servicios de certificación digital

VinCAsign garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en su creación.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la DPC.
- Que los servicios de revocación y el empleo del depósito cumplen con todos los requisitos materiales establecidos en la DPC.

VinCAsign garantiza al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.

- En caso de certificados publicados en el depósito, que el certificado ha sido emitido al dominio identificado en el mismo y que el certificado ha sido aceptado.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la DPC.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y depósito.

Adicionalmente, VinCAsign garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones a que se refiere el Anexo IV del Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014, en relación a los certificados cualificados de autenticación web.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan. En ningún caso VinCAsign responderá por caso fortuito y en caso de fuerza mayor.

1.1.7.2 Exclusión de la garantía

VinCAsign rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

Específicamente, VinCAsign no garantiza software alguno utilizado por cualquier persona para firmar, verificar firmas, cifrar, descifrar, o utilizar de otra forma certificado digital alguno emitido por vinCAsign, excepto en los casos en que exista una declaración escrita en sentido contrario.

1.1.8 Acuerdos aplicables y DPC

1.1.8.1 Acuerdos aplicables

Los acuerdos aplicables al certificado de autenticación web son los siguientes:

- Contrato de servicios de certificación, que regula la relación entre vinCAsign y la empresa suscriptora de los certificados.
- Condiciones generales del servicio incorporadas en el texto de divulgación del certificado o PDS.
- DPC, que regulan la emisión y utilización de los certificados.

1.1.8.2 DPC

Los servicios de certificación de VinCAsign se regulan técnica y operativamente por la DPC de VinCAsign, por sus actualizaciones posteriores, así como por documentación complementaria.

La DPC y la documentación de operaciones se modifica periódicamente en el Registro y se puede consultar en la página de Internet: https://policy.vincasign.net

1.1.9 Política de intimidad

VinCAsign no puede divulgar ni puede ser obligada a divulgar información confidencial alguna en lo referente a certificados sin una solicitud específica previa que provenga de:

a) La persona con respecto a la cual VinCAsign tiene el deber de mantener la información confidencial, o

b) Una orden judicial, administrativa o cualquier otra prevista en la legislación vigente.

Sin embargo, el suscriptor acepta que determinada información, personal y de otro tipo, proporcionada en la solicitud de certificados, sea incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados, y que la información mencionada no tenga carácter confidencial, por imperativo legal.

VinCAsign no cede a ninguna persona los datos entregados específicamente para la prestación del servicio de certificación.

1.1.10 Política de privacidad

VinCAsign dispone de una política de privacidad según se indica en el apartado 9.4 de la DPC, y regulación específica de la privacidad en relación con el proceso de registro, la confidencialidad del registro, la protección del acceso a la información personal, y el consentimiento del usuario.

Asimismo, se contempla que la documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado, incluso todo en caso de pérdida anticipada de vigencia por revocación.

1.1.11 Política de reintegro

VinCAsign no reintegrará el coste del servicio de certificación en ningún caso.

1.1.12 Ley aplicable, jurisdicción competente, y régimen de reclamaciones y disputas

Las relaciones con vinCAsign se regirán por la ley española en materia de servicios de confianza vigente en cada momento, así como por la legislación civil y mercantil en lo que sea de aplicación.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

En caso de discrepancia entre las partes, las partes intentarán la previa resolución amistosa. A tal fin, las partes deberán dirigir una comunicación a vinCAsign por cualquier medio que deje constancia a la dirección de contacto indicada en el punto 1.1.1.2 de esta PDS.

Si las partes no alcanzasen un acuerdo al respecto, cualquiera de ellas podrá someter el conflicto a la jurisdicción civil, con sujeción a los Tribunales del domicilio social de vinCAsign.

Una ampliación de la información de resolución de disputas se encuentra disponible en la dirección de internet www.vintegris.com.

1.1.13 Acreditaciones y sellos de calidad

VinCAsign dispone, en cuanto a la certificación de los sistemas confiables, de la acreditación correspondiente a la solución CryptoSec Openkey CA de Realia Technologies, HSM Cryptosec PCI: certificaciones FIPS 140 level 3 o Common Criteria EAL 4+ (con la aumentación ALC_FLR.1).

Víntegris dispone de la certificación UNE-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI) con el alcance: "Sistemas de Información y todos los procesos internos de negocio que dan soporte a los servicios integrales de: Consultoría Estratégica de Seguridad de la Información, Diseño, Implantación y Gestión de Arquitecturas de Seguridad de la Información; gestión del ciclo de vida de los certificados digitales (emisión, validación, renovación y revocación); de acuerdo con la declaración de aplicabilidad vigente".

Víntegris dispone de la certificación "eIDAS-compliant" para los siguientes servicios:

- Servicio de expedición de **certificados electrónicos cualificados de firma electrónica**, de acuerdo con la norma ETSI EN 319 411-2: [QCP-n], [QCP-n-qscd]

- Servicio de expedición de **certificados electrónicos cualificados de sello electrónico**, de acuerdo con la norma ETSI EN 319 411-2: [QCP-l], [QCP-l-qscd]

- Servicios de expedición de certificados electrónicos cualificados de las Administraciones Públicas – **Certificados electrónicos cualificados de Empleado Público**, de acuerdo con la norma ETSI EN 319 411-2: [QCP-n] – Nivel Medio, [QCP-n-qscd] – Nivel Alto

- Servicios de expedición de certificados electrónicos cualificados de las Administraciones Públicas – **Certificados cualificados de Sello electrónico de la Administración Pública**, de acuerdo con la norma ETSI EN 319 411-2: [QCP-l] – Nivel Medio, [QCP-l-qscd] – Nivel Alto

- Servicio de creación de firmas electrónicas / sellos electrónicos cualificados - **Servicio de confianza que proporciona firma en servidor** (TW4S), de acuerdo con la norma CEN TS 419 241-1

1.1.14 Vinculación con la lista de prestadores

vinCAsign está incluida en la lista de **Prestadores cualificados** de servicios electrónicos de confianza, del Ministerio de Economía y Empresa del Reino de España:

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

vinCAsign está incluida en la "Trust List" de la Unión Europea como **Prestador cualificado** de servicios electrónicos de confianza:

- https://webgate.ec.europa.eu/tl-browser/#/tl/ES/26

1.1.15 Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación

Las cláusulas del presente texto de divulgación son independientes entre sí, motivo por el cual si cualquier cláusula es considerada inválida o inaplicable, el resto de cláusulas de las seguirán siendo aplicables, excepto acuerdo expreso en contrario de las partes.

Los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad) de la DPC de vinCAsign continuarán vigentes tras la terminación del servicio.

Este texto contiene la voluntad completa y todos los acuerdos entre las partes.

Las partes se notifican hechos mutuamente mediante un procedimiento envío email a la dirección info@vincasign.net