1. Certificado de sello de órgano nivel alto

TEXTO DIVULGATIVO

APLICABLE A LOS

CERTIFICADOS DE SELLO DE ÓRGANO NIVEL ALTO

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

1.1 Información de contacto

1.1.1 Organización responsable

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

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 Contacto

Para cualquier consulta, diríjanse a:

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

1.1.3 Contacto para procesos de revocación

Para cualquier consulta, diríjanse a:

VINCASIGN

INFO@VINCASIGN.NET

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

FAX. +34 934 329 344

1.2 Tipo y finalidad del certificado de sello de órgano nivel alto

Los certificados de sello electrónico de órgano nivel alto, son certificados reconocidos de acuerdo con lo establecido en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Estos certificados se emiten para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada de acuerdo con el artículo 18.1 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Los certificados de sello electrónico de órgano nivel alto se emiten de acuerdo con el Esquema de identificación y firma electrónica de las Administraciones públicas en su versión vigente a fecha de este documento.

Estos certificados no son emitidos al público en ningún caso.

Estos certificados garantizan la identidad del subscriptor, del organismo público y la persona responsable incluidos en el certificado.

El nivel alto corresponde a una configuración de mecanismos de seguridad apropiada para las aplicaciones que precisan medidas adicionales, en atención al análisis de riesgo realizado.

Estos certificados no permiten el cifrado de documentos propios. En todo caso, vinCAsign no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado nos 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 reconocido.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo “User Notice” nos describe el uso de este certificado.

Este certificado dispone del OID 1.3.6.1.4.1.47155.1.5.1

1.2.1 Entidad de Certificación emisora

Los certificados de sello de órgano nivel alto son emitidos por vinCAsign, identificada mediante los datos indicados anteriormente.

1.3 Límites de uso del certificado

1.3.1 Límites de uso dirigidos a los firmantes

El firmante ha de utilizar el servicio de certificación de certificados de sello de órgano nivel alto 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 firmantes”).

Asimismo, el firmante se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por vinCAsign.

El firmante ha de cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.

El firmante no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de vinCAsign, sin previo permiso expreso.

1.3.2 Límites de uso dirigidos a los verificadores

Los 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 firmante 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, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo 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.

1.4 Obligaciones de los suscriptores

1.4.1 Generación de claves

El suscriptor autoriza a vinCAsign a generar las claves, privada y pública, para la identificación y la firma electrónica de los firmantes, y solicita en su nombre la emisión del certificado de sello de órgano nivel alto.

1.4.2 Solicitud de certificados

El suscriptor se obliga a realizar las solicitudes de certificados de sello de órgano nivel alto 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.

1.4.3 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.

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.

1.4.4 Obligaciones de custodia

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

1.5 Obligaciones de los firmantes

1.5.1 Obligaciones de custodia

El firmante 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. El firmante se obliga a custodiar el código de identificación personal (PIN).

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

1.5.2 Obligaciones de uso correcto

El firmante tiene que utilizar el servicio de certificación de certificados de sello de órgano nivel alto prestado por vinCAsign, exclusivamente para los usos autorizados en la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

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

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

El firmante reconocerá:

a) Que cuando utilice cualquier certificado, y mientras el certificado no haya expirado ni haya sido suspendido o haya sido revocado, habrá aceptado dicho certificado y estará operativo.

b) Que no actúa como entidad de certificación y, por lo tanto, se obliga a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados con el propósito de firmar certificado alguno.

1.5.3 Transacciones prohibidas

El firmante 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.

1.6 Obligaciones de los verificadores

1.6.1 Decisión informada

VinCAsign informa al verificador que tiene acceso a información suficiente para tomar una decisión informada en el momento de verificar un certificado y confiar en la información contenida en dicho certificado.

Adicionalmente, el verificador reconocerá que el uso del Registro y de las Listas de Revocación de Certificados (en lo sucesivo, "las LRCs" o "las CRLs) de vinCAsign, se rigen por la DPC de vinCAsign y se comprometerá a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

1.6.2 Requisitos de verificación de la firma electrónica

La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC, con los siguientes requisitos:

- Es necesario utilizar el software apropiado para la verificación de una firma digital con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa la firma electrónica a verificar, ya que la firma electrónica se verifica utilizando esta cadena de certificados.

- Es necesario asegurar que la cadena de certificados identificada es la más adecuada para la firma electrónica que se verifica, ya que una firma electrónica puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse el uso de la cadena más adecuada para verificarla.

- Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada al Registro de vinCAsign (con LRCs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede considerarse correctamente verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.

- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado y el firmante, ya que existe la posibilidad de que alguno de los certificados incluya límites de uso que impidan confiar en la firma electrónica que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.

- Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado por el firmante.

1.6.3Confianza en un certificado no verificado

Si el verificador confía en un certificado no verificado, asumirá todos los riesgos derivados de esta actuación.

1.6.4 Efecto de la verificación

En virtud de la correcta verificación de los certificados de sello de órgano nivel alto, de conformidad con este texto divulgativo, el verificador puede confiar en la identificación y, en su caso, clave pública del firmante, dentro de las limitaciones de uso correspondientes, para generar mensajes cifrados.

1.6.5 Uso correcto y actividades prohibidas

El verificador se obliga a no utilizar ningún tipo de información de estado de los certificados o de ningún otro tipo que haya sido suministrada por vinCAsign, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de vinCAsign, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de certificación de vinCAsign.

Los servicios de certificación digital prestados por vinCAsign no han sido diseñados ni permiten la 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, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

1.6.6 Cláusula de indemnidad

El tercero que confía en el certificado se compromete a mantener indemne a vinCAsign de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

1.7 Obligaciones de vinCAsign

1.7.1 En relación a 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.

1.7.2 En relación a 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 y, cuando resulte procedente, de los firmantes.

Estas comprobaciones podrán incluir la justificación documental aportada por el firmante por medio del suscriptor, si vinCAsign lo considera necesario, y cualquier otro documento e información relevantes facilitados por el suscriptor y/o el firmante.

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 firmante.

Las anteriores obligaciones quedarán en suspenso en los casos en que el suscriptor actúe como autoridad de registro y disponga de los elementos técnicos correspondientes a la generación de claves, emisión de certificados y grabación de dispositivos de firma corporativos.

1.8 Garantías limitadas y rechazo de garantías

1.8.1 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 la creación del mismo.

- 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 suscriptor y firmante 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 que debe contener un certificado reconocido, de acuerdo con el artículo 11 de la Ley 59/2003, de 19 de diciembre.

- 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.

1.8.2 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.

1.9 Acuerdos aplicables y DPC

1.9.1 Acuerdos aplicables

Los acuerdos aplicables al certificado sello de órgano nivel alto 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.

1.9.2 DPC

Los servicios de certificación de vinCAsign se regulan técnicamente 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

1.10 Reglas de confianza para firmas longevas

El punto b.2 del artículo 18 de la Ley 59/2003, de 19 de diciembre, de firma electrónica hace referencia a la obligación de las entidades de certificación de informar a los solicitantes de los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

VinCAsign informa a los solicitantes de los certificados de sello de órgano nivel alto que no ofrece un servicio que garantice la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

VinCAsign recomienda, para la fiabilidad de la firma electrónica de un documento a lo largo del tiempo, el uso de los estándares indicados en el apartado 7.3 (reglas de confianza para firmas longevas) de la Guía de Aplicación de la Norma Técnica de Interoperabilidad "Política de Firma Electrónica y de certificados de la Administración".

Las consideraciones generales para las reglas de confianza de firmas longevas se recogen en el subapartado IV.3 de la NTI de firma electrónica.

1.11 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.

1.12 Política de privacidad

VinCAsign dispone de una política de privacidad en el apartado 9.4 de la DPC, y regulación específica de la privacidad en relación al 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.

1.13 Política de reintegro

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

1.14 Ley aplicable y jurisdicción competente

Las relaciones con vinCAsign se regirán por las leyes españolas, y, en concreto para la Ley 59/2003, de 19 de diciembre, de firma electrónica, así como por la legislación civil y mercantil aplicable.

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

1.15 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 Realtec, HSM Cryptosec PCI: certificaciones FIPS 140 level 3 o Common Criteria EAL 4+ (con la aumentación ALC_FLR.1).

1.16 Vinculación con la lista de prestadores

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

1.17 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 **¡Error! No se encuentra el origen de la referencia.** (Obligaciones y responsabilidad), **¡Error! No se encuentra el origen de la referencia.** (Auditoría de conformidad) y **¡Error! No se encuentra el origen de la referencia.** (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 las siguientes direcciones: