Política del Servicio de Firma Electrónica remota

Índice

Índice 2

Control documental 5

Estado formal 5

Control de versiones 6

1 Introducción y alcance 7

1.1 Introducción 7

1.2 Alcance 7

2 Referencias normativas 8

3 Términos, siglas y abreviaturas 9

4 Conceptos generales 11

4.1 Relación entre el PSC y el Servicio de Firma Remota 11

4.2 Documentación aplicable al SSASC 11

4.2.1 Declaración de Prácticas del SSASC 11

4.2.2 Política del SSASC 12

4.2.3 Términos y condiciones 12

4.2.4 Subcomponentes del servicio de firma remota en servidor SSASC 12

5 Disposiciones generales de la Política y Declaración de Prácticas 14

5.1 Requisitos generales de la Política 14

5.1.1 IDENTIFICACIÓN DEL PSC Y DATOS DE CONTACTO 14

5.2 Nombre del documento e identificación 15

5.3 Participantes 15

5.3.1 Proveedor del servicio de Firma Remota (SSASP) 15

5.3.2 Suscriptor y firmante 15

6 Prácticas de Proveedor de Servicios de Confianza 17

6.1 Responsabilidades de publicación y depósito 17

6.2 Inicialización de las claves de firma 17
6.2.1 Generación y protección de las claves de firma 17
6.2.2 Utilización de las claves de firmantes en el servicio de firma remota 19
6.2.3 Asociación de los medios de identificación electrónica del firmante 20
6.2.4 Asociación del certificado del firmante 21
6.2.5 Provisión de los medios de identificación del firmante 21
6.3 Requisitos operacionales del ciclo de vida de las claves de firma 22
6.3.1 Activación de las claves de firma 22
6.3.2 Gestión de los datos de activación de firma 23
6.3.3 Borrado de las claves de firma 24
6.3.4 Copia de seguridad y restauración de las claves de firma 25
6.4 Controles de seguridad física, de gestión y de operaciones 25
6.4.1 Controles generales 26
6.4.2 Controles de seguridad física 26
6.4.3 Controles de procedimientos 26
6.4.4 Controles de personal 26
6.4.5 Procedimientos de auditoría de seguridad 27
6.4.6 Archivos de registros 28
6.4.7 Cambio de claves 28
6.4.8 Compromiso de claves y recuperación de desastre 29
6.4.9 Terminación del servicio 29
6.5 Controles de seguridad técnica 29
6.5.1 Gestión de los sistemas y de la seguridad 29
6.5.2 Operaciones y Sistemas 30
6.5.3 Controles de seguridad informática 30
6.5.4 Controles técnicos del ciclo de vida 30
6.5.5 Controles de seguridad de red 31

6.6 Auditoría de conformidad 31
6.7 Requisitos comerciales y legales 31
6.7.1 Tarifas 31
6.7.2 Capacidad financiera 31
6.7.3 Confidencialidad 31
6.7.4 Protección de datos personales 31
6.7.5 Derechos de propiedad intelectual 31
6.7.6 Declaraciones y garantías 32
6.7.7 Renuncias a las garantías 32
6.7.8 Limitaciones de responsabilidad 32
6.7.9 Indemnizaciones 32
6.7.10 Duración y terminación 32
6.7.11 Avisos y comunicaciones individuales de los participantes 32
6.7.12 Modificaciones 32
6.7.13 Disposiciones para la resolución de litigios 32
6.7.14 Legislación aplicable 33
6.7.15 Cumplimiento de la legislación aplicable 33
6.7.16 Miscelánea 33
6.7.17 Otras disposiciones 33
7 REFERENCIAS 34

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	
Versión:	1.1
Fecha edición:	27/02/2024
Fichero:	Víntegris_Política _del _Servicio de _Firma electrónica_ remota
Formato:	Office 365
Autores:	Víntegris

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: RR Fecha:27/02/2024	Nombre: VH Fecha: 27/02/2024	Nombre: VH Fecha: 27/02/2024

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Todas	Creación del documento	VH	12/12/2022
1.1		Actualización con SAM Entrust	RR	27/02/2024

1 Introducción y alcance

1.1 Introducción

El presente documento describe la Política del servicio de firma remota en servidor de VinCAsign (entidad de certificación de Vintegris S.L.U). Este servicio se ofrece a través de la aplicación denominada "nebulaSIGN", que se encuentra integrada dentro del concepto "NebulaSUITE", que engloba varias soluciones digitales.

En virtud de este servicio de firma remota en servidor (reconocido como SSASC por sus siglas en inglés), VinCAsign permite al firmante la generación de una firma electrónica a distancia, garantizándole además el control exclusivo sobre sus claves de firma. Para ello gestiona los componentes de su aplicación "nebulaCERT", asociados a un dispositivo cualificado de creación de firma remota (rQSCD por sus siglas en inglés), que permiten generar la firma de referencia en un contexto de seguridad.

Por lo general, un rQSCD queda definido por uno o varios dispositivos físicos que permiten al firmante actuar de manera remota y segura sobre su clave (siguiendo la norma CEN EN 419 241).

1.2 Alcance

El presente documento define la Política del servicio de firma electrónica remota que VinCAsign utiliza para la operación de los componentes que gestionan dispositivos de creación de firma remota en nombre del firmante.

Conforme a esta Política, los componentes del servicio consisten en una aplicación de firma "NebulaSign" y un dispositivo de creación de firma que podrá tener el carácter de cualificado (conocido por sus siglas en inglés QSCD) de acuerdo con la definición del Anexo II del Reglamento (UE) 910/2014 eIDAS.

La presente Política es aplicable a la emisión de los certificados de firma electrónica remota o a distancia emitidos por VinCAsign, que se definen en la Declaración de Prácticas de Certificación.

2 Referencias normativas

La prestación de este servicio se realiza de acuerdo con el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, "Reglamento eIDAS").

Igualmente, este documento se ha redactado siguiendo las directrices definidas en las siguientes especificaciones técnicas:

- ETSI TS 119 431 – 1 "*Firmas electrónicas e infraestructuras (ESI); Requisitos de política y seguridad para los proveedores de servicios de confianza; Parte 1: componentes de servicio del PSC que operan un QSCD / SCDev en remoto*".
- ETSI TS 119 431-2 "*Firmas Electrónicas e Infraestructuras (ESI); Requisitos de política y seguridad para prestadores de servicios de confianza; Parte 2: componentes del servicio del PSC que admiten la creación de firmas digitales AdES."*
- ETSI TS 119 432 *"Firmas e Infraestructuras Electrónicas (ESI); Protocolos para la creación remota de firmas digitales".*
- CEN - EN 419 241-1 *"Sistemas confiables que admiten la firma de servidores - Parte 1: Requisitos generales de seguridad del sistema".*
- CEN - EN 419 241-2 *"Sistemas confiables que admiten la firma del servidor Parte* 2, Perfil de protección para QSCD para la firma del servidor".
- CEN EN 419221-5 Perfiles de protección para módulos criptográficos TSP - Parte 5: Módulo criptográfico para servicios de confianza
- ETSI EN 319 401: Firmas e Infraestructuras Electrónicas (ESI); Requisitos generales de la política para proveedores de servicios de confianza
- EN 319 411-2: Firmas e Infraestructuras Electrónicas (ESI); Política y requisitos de seguridad para los Proveedores de Servicios de Confianza que emiten certificados; Parte 2: Requisitos para los proveedores de servicios de confianza que expidan certificados cualificados de la UE
- Declaración de Prácticas de Confianza de VinCAsign

3 Términos, siglas y abreviaturas

La presente Política utiliza los siguientes términos y abreviaturas tal y como se definen en la ETSI TS 119 431 -1:

- **Referencia a medios de identificación electrónica:** datos usados en el SSASC como referencia a unos medios de identificación electrónica que permiten autenticar a un firmante.
- **Autenticación:** un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
- **Aplicación de firma de servidor (SSA):** Una aplicación que, asociada a un dispositivo de creación de firma (QSCD/SCDev) o un dispositivo de creación de firma en remoto (QSCD/SCDev remoto), permite generar una firma electrónica. En este caso las siglas SSA identifican a la aplicación NebulaSign de VinCAsign.
- **Identificación electrónica (eID)** el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.
- **Medios de identificación electrónica:** una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.
- **Dispositivo cualificado de creación de firma / sello electrónico (QSCD):** dispositivo de creación de firma que cumple con los requisitos del Anexo II del Reglamento (EU) No 910/2014.
- **QSCD remoto (rQSCD)**: es un SCDev ampliado con control remoto proporcionado por un Módulo de Activación de Firma (SAM) ejecutado en un entorno protegido contra manipulaciones. Este módulo utiliza los datos de activación de firma (SAD), recogidos a través de un protocolo de activación de firma (SAP), para garantizar con un alto nivel de confianza que las claves de firma se utilizan bajo el control exclusivo del firmante.
- **Módulo de Activación de Firma (SAM)**: Elemento del rQSCD, que consiste en el software que lleva a cabo el protocolo de activación de firma en el QSCD. Realiza

tareas tales como gestión de usuarios, recepción de un canal seguro de comunicación con el usuario, gestión de las claves de firma y gestión del proceso de firma, entre otros.

- **Dispositivo seguro criptográfico (SCDev):** Elemento del rQSCD; es el soporte hardware que garantiza protección frente a manipulaciones en el momento de realizar operaciones criptográficas tales como la generación de números aleatorios, algoritmos de hash y firma electrónica, entre otros.
- **Componente de servicio de aplicación de firma en servidor (SSASC):** componente de servicio operado por un PSC, compuesto de una aplicación de firma en servidor (SSA) y un QSCD / SCDev, empleado para la creación de firmas electrónicas cualificadas en nombre del firmante.
- **Proveedor de servicio de aplicación de firma en servidor (SSASP)**: PSC que opera un SSASC.
- **Servicio de confianza:** servicio electrónico consistente en la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo, servicios de entrega electrónica certificada y certificados de estos servicios; o la creación, verificación y validación de certificados ara la autenticación de sitios web; o la preservación de firmas, sellos o certificados electrónicos.
- **Proveedor de servicios de confianza (PSC):** entidad que provee de servicios de confianza. En este caso hace referencia a VinCAsign.

4 Conceptos generales

4.1 Relación entre el PSC y el Servicio de Firma Remota

VinCAsign es una Autoridad de Certificación y un Prestador de servicios de confianza cualificado que, entre otros servicios, emite certificados y sellos electrónicos cualificados de acuerdo con la legislación vigente.[1]

El servicio de SSASC forma parte de los servicios llevados a cabo por VinCAsign y permite prestar el servicio de firma electrónica remota a aquellos firmantes que cuenten con certificados electrónicos cualificados centralizados, tal y como se indica en la Declaración de Prácticas de Confianza de VinCAsign.

4.2 Documentación aplicable al SSASC

4.2.1 Declaración de Prácticas del SSASC

VinCAsign, en calidad de prestador del servicio de firma remota en servidor (SSASP por sus siglas en inglés), es la encargada del desarrollo, implementación, pruebas y puesta en marcha del servicio. Además, garantiza el cumplimiento, actualización y revisión del presente documento (Política del Servicio de Firma Remota).

Las prácticas relacionadas con el servicio de firma remota en servidor SSASC, se adaptan a la estructura organizativa, los procedimientos operativos, las instalaciones y el entorno informático de VinCAsign.

La Declaración de Prácticas de SSASC, es una declaración de prácticas de un servicio de confianza tal y como se define en la norma ETSI EN 319 401, y está publicada en la web del Prestador de Servicios de Confianza vinCAsign (https://www.vincasign.net) [OVR-5.1-03]

[1] OVR-A.1-01 de la ETSI TS 119 431-1

4.2.2 Política del SSASC

El presente documento describe la política aplicable al Servicio del Componente de servicio de aplicación de firma en servidor.

4.2.3 Términos y condiciones

Como parte del servicio de firma remota en servidor, VinCAsign publica términos y condiciones específicos que son vinculantes para los usuarios finales al igual que la presente Política y la Declaración de Prácticas.

Los destinatarios de los términos y condiciones son los suscriptores y las partes usuarias.

4.2.4 Subcomponentes del servicio de firma remota en servidor SSASC

El servicio de firma remota en servidor que provee VinCAsign se corresponde con la suite de producto nebulaSUITE. En concreto, el producto fundamental que lo gestiona es nebulaCERT.

Según la definición de subcomponentes establecida en TS 119-341-1, se indican a continuación las funcionalidades que nebulaCERT (apoyado por otros componentes y sistemas):

- **Servicio de generación de claves de firma**: genera claves de firma en el dispositivo remoto. La prueba de posesión de claves de firma generadas se transmite al servicio de registro de VinCAsign que emite el certificado asociado.
- **Servicio de vinculación de certificados:** vincula los certificados generados por el servicio de generación de certificados de VinCAsign con las claves de firma correspondientes alm.
- **Servicio de vinculación de medios de identificación electrónica (eID)**: vincula las referencias de medios de identificación electrónica con las correspondientes claves de firma para proporcionar un único control. El servicio sólo puede utilizarse con certificados emitidos por el servicio de Registro de VinCAsign.
- **Servicio de activación de la firma**: verifica los datos de activación de la firma y activa la clave de firma correspondiente para crear una firma digital.
- **Servicio de supresión de la clave de firma**: destruye las claves de firma de forma que se garantice que las claves de firma no puedan volver a utilizarse.

- **Servicio de provisión de medios de identificación electrónica (eID) (opcional):** prepara y proporciona o pone a disposición de los firmantes los medios de identificación electrónica. VinCAsign no proporciona dicho servicio.

5 Disposiciones generales de la Política y Declaración de Prácticas

5.1 Requisitos generales de la Política

La presente Política y otra documentación relevante está disponible en https://www.vincasign.net/historico.html las 24 horas del día, los 7 días a la semana.

En caso de fallo del sistema, del servicio o de otros factores que no estén bajo el control del Vintegris, éste hará todo lo posible para garantizar que este servicio de información vuelva a estar disponible en máximo 72 horas. Vintegris podrá disponer otras vías de divulgación de esta información durante la gestión de la incidencia.

En los apartados 6.2.1 y 6.2.2 de la presente Política se definen los algoritmos y parámetros de firma aplicados para la generación del par de claves y otros algoritmos y parámetros críticos para la seguridad de las operaciones del SSASC.

5.1.1 IDENTIFICACIÓN DEL PSC Y DATOS DE CONTACTO

Razon Social	VÍNTEGRIS S.L.U.
CIF	B62913926
Domicilio Social	Carrer Pallars, 99 Planta 3, Oficina 33, 08018, Barcelona
Teléfono	93 432 90 98
Email de contacto	info@vincasign.net
Nombre comercial	VinCAsign

Cualquier cambio que se realice sobre los anteriores datos quedarán debidamente reflejados en la página web www.vincasign.net, que VinCAsign actualiza en el momento en el que se produzca cualquier cambio que deba comunicarse públicamente.

Igualmente, la presente Política puede ser modificada en cualquier momento por vinCAsign. De no aceptar cualquiera de los suscriptores con certificado en vigor, alguna

de las modificaciones acordadas puede solicitar la revocación de su certificado y destrucción de sus claves.

La revisión y aprobación de la presente Política queda encargada a la Dirección de VinCAsign.

5.2 Nombre del documento e identificación

Este documento es la "Política del Servicio de Firma electrónica remota" de VinCAsign, y tiene asignado el OID 1.3.6.1.4.1.47155.0.1.1

Para el servicio SSASC, VinCAsign ha definido dos políticas en este documento:

- Política de SSASC avanzado (Normalized SSASC Vintegris Remote Signature Policy), en el que se opera un SCDev remoto, y tiene asignado el OID: 1.3.6.1.4.1.47155.0.1.1.1 - Es conforme con la política "NSCP: Normalized SSASC Policy" definida en ETSI TS 119 431-1 v1.2.1 (2021-05), con OID: 0.4.0.19431.1.1.2.
- Política de SSASC cualificado (Qualified SSASC Vintegris Remote Signature Policy), en el que se opera un QSCD remoto y tiene asignado el OID: 1.3.6.1.4.1.47155.0.1.1.2. Es conforme con la política "EUSCP: EU SSASC Policy" definida en ETSI TS119 431 v1.2.1 (2021-05), con OID: 0.4.19431.1.1.3

VinCAsign revisa periódicamente la conformidad de sus políticas con respecto a la norma ETSI TS 119 431-1 y cambiará el identificador de sus políticas ante cualquier cambio en las políticas definidas en la sección 4.3.2 y 5.2 de dicha norma.

5.3 Participantes

5.3.1 Proveedor del servicio de Firma Remota (SSASP)

VinCAsign actúa como SSASP y no delega a entidades terceras ninguna parte del servicio.

5.3.2 Suscriptor y firmante

En el contexto de este documento el firmante asociado con una clave de firma puede ser:

- Una persona física.
- Una persona física representando a una persona jurídica.

- Una persona jurídica.
- Un dispositivo o sistema operado por o en nombre de una persona física o jurídica.

En todos los casos, las relaciones entre los suscriptores y los firmantes quedan definidas en la Declaración de Prácticas de Certificación de vinCAsign.

6 Prácticas de Proveedor de Servicios de Confianza

6.1 Responsabilidades de publicación y depósito

Según lo especificado en la sección 2 “Publicación de información y repositorios” de la Declaración de Prácticas de Certificación de VinCAsign.

En este apartado se incluirá esta política específica y los términos y condiciones relativos al uso de las claves de firma. Estos términos y condiciones serán identificables fácilmente para una determinada clave de firma o para el certificado asociado.

6.2 Inicialización de las claves de firma

6.2.1 Generación y protección de las claves de firma

vinCAsign define dos versiones del SSASC:

- SSASC vinCAsign
    - Utiliza como SSA la aplicación nebulaCERT (basada en la aplicación VinCertcore) en combinación con un módulo criptográfico (HSM) que actúa como QSCD. La combinación está certificada de acuerdo con los requerimientos del Anexo 2 del Reglamento (UE) 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 [SRA_SKM.1.1].
        - HSM nShield Connect XC en versión 12.60.15
            - Certificación FIPS 140-2 L3 y Common Criteria EAL4+ (AVA_VAN.5) [SRG_KM.1.1] [GEN-A.4-01]
    - Las claves del firmante en el SSA son creadas por vinCAsign bajo estricto control único del firmante por medio del PIN de activación de firma.
        - Estas claves se protegen mediante el PIN de activación de firma, sobre el que se aplica el algoritmo PBKDF2 para derivación de claves.

- SSASC TrustServices
    - Utiliza como SSA el dispositivo Entrust Signature Activation Module en combinación con un módulo criptográfico (HSM) que actúa como QSCD. La combinación está certificada de acuerdo con los requerimientos del Anexo 2 del Reglamento (UE) 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 [SRA_SKM.1.1]
        - Entrust SAM en versión 1.0.4
            - Las operaciones de administración y de seguridad son restringidas al uso de control dual [GEN-6.2.1-08]
        - HSM nShield Connect XC en versión 12.60.15
            - Certificación Common Criteria EAL4+ (conforme a EN 419 221-5) [SRG_KM.1.1] [GEN-A.4-01]
    - Las claves del firmante en el SSA son creadas por vinCAsign bajo estricto control único del firmante por medio de la delegación de las funciones de proveedor de identidad (IdP) y de servidor de autenticación (AS) a nebulaSUITE.

En ambos casos:

- Las claves de los firmantes son generadas usando el algoritmo de clave pública RSA con una longitud de 2048 bits, aunque el sistema está preparado para generar claves de longitud superior.
- Las claves se almacenan fuera de los HSM en Base de Datos de nebulaCERT, cifradas con algoritmo AES de 128 bits de longitud de clave. [SRG_KM.1.3]
    - Las claves no son intercambiables ni pueden ser migradas de una versión de SSASC a otra.
- Las operaciones de administración de los HSM son restringidas al uso de control dual [GEN-6.2.1-08]
- El proceso de generación de claves se divide en dos fases:
    - En la primera fase del proceso de emisión del certificado electrónico del firmante, se genera el par de claves asociado en el dispositivo criptográfico o HSM en unos segundos.

        - Durante este proceso, el par de claves se encuentra desactivado y no se permite su uso a través de la aplicación SSA. [GEN-6.2.1-07]
    - En la segunda fase del proceso, la aplicación SSA genera una petición de certificado en base a los datos proporcionados por la Autoridad de Registro en formato PKCS#10, que es enviado a la Autoridad de Certificación para finalizar la emisión del certificado asociado al par de claves.
        - La petición de certificado en PKCS#10 actúa como prueba de posesión de la clave privada del firmante. [GEN-6.2.1-08]
- Todas las claves generadas por los SSASC de vinCAsign se asocian a certificados emitidos por la Autoridad de Certificación de vinCAsign.

6.2.2 Utilización de las claves de firmantes en el servicio de firma remota

Los algoritmos permitidos en el servicio de firma remota de VinCAsign para su uso por las claves generadas a través del servicio de firma remota son[2] :

- SSASC vinCAsign:
    - RSA-PKCS#1v1_5
    - RSA-PSS
    - sha256-with-rsa
    - sha512-with-rsa
- SSASC TrustServices:
    - RSA-PKCS#1v1_5
    - sha256-with-rsa
    - sha512-with-rsa

[2] Según la ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

6.2.3 Asociación de los medios de identificación electrónica del firmante

La Autoridad de Registro validará la identidad del firmante de acuerdo con los requisitos establecidos en la Declaración de Prácticas de Certificación del certificado solicitado por el firmante con un nivel de garantía alto según los requisitos establecidos en el Reglamento UE 2015/1502. **[**LNK-6.2.2-01] [LNK-6.2.2-02].

La identificación y autenticación del firmante se delega en nebulaSUITE, que realiza las funciones de IdP y AS. Los firmantes deben estar registrados previamente en la plataforma, y deben haber sido identificados previamente mediante alguno de los mecanismos recogidos en la Declaración de Prácticas de vinCAsign.

La Autoridad de Registro (nebulaSUITE) se encarga de solicitar la creación del par de claves al SSA, y de vincular dicho par de claves a la identidad del firmante [LNK-6.2.2-03]:

- En el caso del SSASC vinCAsign, se solicita el establecimiento de un PIN de activación de firma obligatorio por parte del firmante.
- En el caso del SSASC TrustServices, la introducción de un PIN de activación de firma es opcional (dependiendo de la configuración de seguridad del entorno)[3].

Una vez creado el par de claves, la Autoridad de Registro solicita la emisión del certificado electrónico asociado al par de claves mediante la prueba de posesión de la clave privada generada en el SSA. Tras la emisión, la Autoridad de Registro vincula el certificado emitido con el par de claves del firmante [LNK-6.2.2-05].

Tras la emisión del certificado, el SSA almacena en base de datos propia las claves de los firmantes de manera íntegra y segura [LNK-6.2.2-10]:

- En el caso del SSASC vinCAsign, se guardan las claves cifradas por el HSM acompañadas de los datos de activación (que se derivan del PIN del firmante)
- En el caso del SSASC TrustServices, se guardan las claves generadas directamente por el SAM (firmadas electrónicamente).

En ambos casos, la base de datos está protegida ante modificaciones no autorizadas.

[3] CEN EN 419 241-1. Apartado 5.7.1.2, 5.7.2.2 y 5.7.4.2

6.2.4 Asociación del certificado del firmante

Una vez el proceso de registro y emisión del certificado del firmante se ha completado, el certificado del firmante es importado en el SSASC.

El SSAC verifica que la clave pública en el certificado del firmante y la almacenada en el sistema se corresponden. [LNK-6.2.3-01]. En el caso de que ambas claves públicas coincidan, el certificado queda vinculado al par de claves del firmante.

La clave del firmante es marcada como activa, y queda a partir de este momento operativa para realizar operaciones de firma [LNK-6.2.3-02].

El SSASC protege la integridad de las claves de los firmantes y sus metadatos asociados mediante el cómputo de una función criptográfica que permita la verificación de la integridad. [LNK-6.2.3-03]

6.2.5 Provisión de los medios de identificación del firmante

Las claves privadas de los firmantes se encuentran debidamente protegidas por los dispositivos cualificados de creación de firma (QSCD), gestionados por vinCAsign y sin delegación en terceros.

El proceso de identificación y autenticación del firmante se delega en la plataforma nebulaSUITE, que proporciona un nivel de aseguramiento suficiente (al menos sustancial[4]) mediante un esquema de autenticación multifactor de dos canales diferentes.

Los canales autorizados son una combinación de:

- Usuario/password ó token SAML y,
- SMS OTP, email OTP, Autenticador TOTP, tarjeta de coordenadas
- En el caso del SSASC vinCAsign, y en el del SSASC TrustServices en los entornos que no lo permitan, PIN de activación de firma adicional.

vinCAsign no genera ninguno de los medios de identificación del firmante.

[4] CEN EN 419 241-1. Apartado 5.7.4.2

6.3 Requisitos operacionales del ciclo de vida de las claves de firma

6.3.1 Activación de las claves de firma

El protocolo de activación de firma (SAP) requiere que el firmante complete un proceso de identificación y autenticación previo al momento del uso de su clave de firma, mediante el uso de los datos de activación de firma (SAD) [SIG-6.3.1-01] [SIG-6.3.1-05].

- En el caso del SSASC vinCAsign:
    - Las claves del firmante sólo pueden ser activadas dentro de los HSM asociados al SSASC **[SIG-A.5-02]** y sólo si el PIN de activación de firma es correcto [SIG-6.3.1-09]**.**
    - El SAP requiere de:
        - Autenticación multifactor correcta.
        - PIN introducido por el usuario correcto.
        - SAD firmado electrónicamente.
    - El SAP establece mecanismos de protección contra robo o suplantación de sesión, duplicación, *phishing*, adivinación online u offline, *man-in-the-middle* y robo de credenciales; basados en el uso de funciones criptográficas (cifrado, firma electrónica), en el uso de conexiones seguras, y en mecanismos de autenticación multifactor [SIG-6.3.1-06] [SIG-A.5-04]
    - El usuario firmante dispone de un número de intentos máximo para la introducción del PIN. Tras
- En el caso del SSASC TrustServices:

El firmante, para poder usar su clave de firma, ha de proveer un mensaje de activación de firma (SAD) mediante el protocolo de activación de firma (SAP), que está diseñado para prevenir ataques. El mensaje ha de contener dos factores de autenticación de diferente tipo y un testigo de sesión. Para obtener un testigo de sesión, el SSASC requiere que el firmante se identifique previamente con su usuario y al menos un factor de autenticación. **[SIG-6.3.1-01] [SIG-6.3.1-05].** Si el firmante introduce erróneamente 3 veces consecutivas el factor de activación de acceso a la clave remota queda bloqueado. La clave bloqueada

únicamente podrá ser desbloqueada por el firmante introduciendo el código PUK asociado

Las claves del firmante solo se pueden activar dentro del módulo HSM. **[SIG-A.5-02]**

La clave de un firmante solo es activable si el firmante completa el protocolo de activación (SAP) y el PIN de activación enviado en el SAD es el correcto. **[SIG-6.3.1-09]**

El mensaje de activación de activación de firma (SAD) vincula el resumen criptográfico de los datos a firmar con los datos de activación del firmante mediante la firma electrónica del mensaje de activación con la clave de activación del firmante. **[SIG-6.3.1-04]**

Los controles de acceso implementados en el SSAC garantizan que un firmante no tiene acceso las claves de otros firmantes ni a otros objetos y funciones del sistema que no sean las funciones de firma **[SIG-6.3.1-03]**

Una vez se activa la clave del firmante el SSASC solo permite su uso para firmar el resumen criptográfico contenido en el mensaje SAD utilizado para la activación. **[SIG-6.3.1-07]**. Una vez se realiza la operación de firma solicitada con el SAD el SSASC desactiva la clave del firmante, requiriendo de un nuevo SAD para una nueva firma.

El SSASC almacena en los metadatos del par de claves del firmante la fecha de caducidad del certificado asociado. Antes del uso de una clave de firma el SSASC comprueba tanto la fecha de caducidad del certificado así como su estado (no revocado, suspendido, ni caducado), y deniega la operación acorde al estado del certificado. **[SIG-6.3.1-08]**

Las claves de firma serán utilizables sólo en los casos en que se haya obtenido el consentimiento del firmante. SIG-6.3.1-09:

El SSASC permite generar firmas electrónicas con el algoritmo RSA PKCS#1 v1.5 y algoritmo resumen SHA-256 y SHA-512. **[SIG-6.3.1-10]**

Se emplea un par de claves RSA de 2048 bits controlado por el SSA para el cifrado en transporte de una clave AES 128 bits de un solo uso con la que se cifra el PIN de activación en cada mensaje de activación SAD. **[SIG-A.5-03]**

6.3.2 Gestión de los datos de activación de firma

El mensaje con los datos de activación de firma (SAD) es generado en la aplicación SAA, instalada por el firmante. **[SIG-A.6-02]**

El mensaje del SAD contiene el resumen(es) criptográfico(s) de los datos a firmar, referencias que permiten identificar la clave seleccionada e identificar al firmante, el PIN

de activación de firma cifrado. Todo el mensaje del SAD se firma con la clave privada de activación de firma en la aplicación SAA para autenticar al firmante. **[SIG-A.6-01] [SIG-A.6-03] [SIG-A.6-06]**

El SSASC solo permite que el firmante pueda utilizar su clave de activación de firma desde un único dispositivo para evitar que se duplique. **[SIG-A.6-06]**

La combinación de dos factores de autenticación de diferente naturaleza, la clave de activación y el PIN de activación, aseguran que el firmante tiene control exclusivo de sus datos de activación de firma. **[SIG-A.6-07]**

El SAP consiste en la transmisión de un solo mensaje SAD a través de un canal seguro hasta el SSA. El módulo de activación de firma (SAM) es un sub-modulo del SSA. **[SIG-A.6-05]**

El nivel AVA_VAN.5 de evaluación de la solución SSA ha considerado atacantes de potencial alto en las pruebas de seguridad con el fin de asegurar que el mecanismo de autenticación para activar los datos de creación de firma no puede ser alterado. **[SIG-A.6-08]**

6.3.3 Borrado de las claves de firma

Mediante un proceso automático y periódico, las claves de firmantes generadas a través del SSASP cuyo certificado electrónico haya expirado son eliminadas puntualmente [DEL-6.3.2-01].

Bajo cualquiera de las causas y formas de revocación de certificados (establecidas en la Declaración de Prácticas de Certificación de vinCAsign), las claves criptográficas de firmantes cuyo certificado asociado haya sido revocado son eliminadas puntualmente [DEL-6.3.2-02].

La ejecución del proceso automático de eliminación de claves bajo cualquiera de las causas que lo provoque se realiza con una periodicidad inferior a 30 minutos.

Las claves criptográficas no abandonan el dispositivo criptográfico del SSASC en claro, y residen en base de datos. Cualquier operación criptográfica relacionada con la clave del usuario requiere de un posterior borrado de la misma del SSASC [DEL-6.3.2-03]

- Durante la generación de las claves y la emisión del certificado, la clave de firma se encuentra dentro del SSASC. Una vez este proceso haya finalizado, las claves

del firmante se trasladan a la base de datos y se elimina la clave cargada en el dispositivo criptográfico.

Durante el momento de activación de la firma, la clave de firma es copiada al SSASC. Una vez el proceso haya finalizado, la copia de la clave utilizada en el SSASC se elimina del dispositivo criptográfico.

6.3.4 Copia de seguridad y restauración de las claves de firma

Las claves de los firmantes están protegidas por la clave maestra del módulo criptográfico, pudiéndose utilizar solo cuando este módulo está activo. Las claves de infraestructura del SSASC son almacenadas en contenedores cifrados.

Las claves criptográficas de los firmantes quedan guardadas en la base de datos del SSASC [GEN-6.3.3-01] [GEN-6.3.3-02]:

- En el caso del SSASC vinCAsign, las claves quedan protegidas mediante la clave criptográfica maestra del HSM y el PIN del firmante, y utilizando algoritmo AES con 128 bits de longitud de clave.
- En el caso del SSASC TrustServices, las claves quedan protegidas mediante mecanismo criptográfico establecido por el SAM, utilizando algoritmo AES.

Los componentes criptográficos que componen los SSASC son administrados con restricciones de control dual. Ninguna clave criptográfica generada en los mismosqueda expuesta sin cifrar [GEN-6.3.3-03].

Se mantienen copias de seguridad periódicas de la base de datos del SSASC, donde se encuentra las claves de los firmantes, y del resto de claves de infraestructura necesarias para garantizar la continuidad del servicio en caso de incidente. El número de copias de seguridad es el mínimo para garantizar la continuidad del servicio [GEN-6.3.3-04].

VinCAsign ha desplegado una función de recuperación capaz de restaurar el estado del sistema a partir de una copia de seguridad. Esa se llevará a cabo por el personal administrativo en el rol de confianza designado y en condiciones que garanticen la seguridad del proceso. [SRG_BK.2.1 y SRG_BK.2.2].

6.4 Controles de seguridad física, de gestión y de operaciones

6.4.1 Controles generales

6.4.1.1 Gestión y análisis de riesgos

vinCAsign elabora, mantiene y revisa un procedimiento de Gestión de Riesgos para identificar, evaluar y analizar los riesgos que afectan a los servicios cubiertos por esta política.

Este procedimiento de Gestión de Riesgos conlleva análisis periódicos (al menos anuales) o motivados por cambios en el servicio, y está aprobado por la Dirección de vinCAsign.

6.4.1.2 Política de Seguridad de la Información

vinCAsign dispone de una Política de Seguridad de la Información que describe la gestión de la seguridad aprobada por la Dirección de vinCAsign.

6.4.1.3 Gestión de Activos

vinCAsign dispone de un procedimiento de gestión de activos, así como una clasificación en base al procedimiento de Gestión de Riesgos y a la clasificación de la información que alberga o provee el activo en cuestión.

Los dispositivos que almacenan información de vinCAsign están catalogados según la Política de Clasificación de Información de vinCAsign, y existen procedimientos definidos en cuanto al borrado o destrucción segura según dicha clasificación.

6.4.2 Controles de seguridad física

Los definidos en la sección 5.1 “Controles de seguridad física” de la Declaración de Prácticas de Confianza de VinCAsign.

6.4.3 Controles de procedimientos

Los definidos en la sección 5.2 “Controles de Procedimientos” de la Declaración de Prácticas de Confianza de VinCAsign.

6.4.4 Controles de personal

Los definidos en la sección 5.3 “Controles de personal” de la Declaración de Prácticas de Confianza de VinCAsign.

6.4.5 Procedimientos de auditoría de seguridad

Los definidos en la sección 5.4 “Procedimientos de auditoría de seguridad” de la Declaración de Prácticas de Confianza de VinCAsign [OVR-6.4.5-01] [OVR-6.4.5-02].

Los tipos de eventos registrados están previstos en el apartado 5.4.1 de la Declaración de Prácticas de Confianza de VinCAsign.

Se registrarán todos los eventos de seguridad, incluyendo los cambios relacionados con la política de seguridad, el arranque y el apagado del sistema, caídas del sistema y fallos de hardware, actividades del firewall y del router e intentos de acceso al sistema SSASC. [OVR-6.4.5-02]

El SSASC guarda registro, al menos, de los siguientes eventos:

- Inicialización de sistema, arranque, parada y cambios de configuración.
- Eventos de gestión de claves del firmante (generación, activación, uso, desactivación y destrucción)
- Uso de claves de los firmantes.
    - Los eventos de firma del usuario incluyen el certificado asociado a la clave de firma.
- Autenticación de los firmantes (incluyendo intentos fallidos).
- Gestión de los datos de activación de firma del firmante (cambios de PIN)
- Arranque y parada de las funciones de auditoría.
- Cambio de la configuración de las funciones de auditoría.
- Accesos al sistema por parte de los usuarios administradores.

El SSASC deja de procesar de forma automática peticiones en el caso de que sus funciones de auditoría no estén disponibles. [OVR-6.4.5-03]

El SSASC no permite la eliminación o modificación de eventos anteriores, sólo el añadido de nuevos elementos.

El SSASC protege los eventos del registro de auditoría [OVR-6.4.5-04]:

- En el caso del SSASC vinCAsign, los registros se protegen a nivel de tabla, de forma que las modificaciones no autorizadas invalidan la tabla completa, provocando la desactivación del sistema de auditoría.

- En el caso del SSASC TrustServices, el registro de auditoría se realiza en sistema syslog externo, manteniendo la integridad mediante firma electrónica.

Todos los registros de eventos del registro de auditoría del SSA incluyen la siguiente información:

- Fecha y hora del evento.
- Tipo de evento.
- Identidad de la entidad (firmante, administrador o proceso) responsable de la acción.
- Resultado del evento (éxito o error) [OVR-6.4.5-05]

En cuanto a la comprobación periódica de integridad [OVR-6.4.5-06]:

- En el caso del SSASC vinCAsign, el SSASC comprueba en el arranque y periódicamente la integridad del registro de auditoría para detectar el borrado o modificación, y dispone de una funcionalidad para verificar la integridad del registro de auditoría.
- En el caso del SSASC TrustServices, la comprobación de integridad queda delegada por el SAM en el SSA.

Para garantizar la precisión de la fecha y hora de los eventos de auditoría el reloj de los sistemas se encuentra sincronizado por NTP utilizando como referencia el ROA (Real Observatorio de la Armada). Existen controles para detectar problemas que puedan comprometer la sincronización. [OVR-6.4.5-07].

El SSASC denegará por defecto a todos los usuarios el acceso de lectura a los registros de auditoría, excepto a los usuarios a los que se les haya concedido acceso de lectura explícito (por ejemplo, los que tengan el rol de Auditor del Sistema). [SRG_AA.5.1].

6.4.6 Archivos de registros

Los definidos en la sección 5.5 “Archivos de registros” de la Declaración de Prácticas de Confianza de VinCAsign

6.4.7 Cambio de claves

Los definidos en la sección 5.6 “Cambio de claves” de la Declaración de Prácticas de Confianza de VinCAsign.

6.4.8 Compromiso de claves y recuperación de desastre

Los definidos en la sección 5.7 “Compromiso de claves y recuperación de desastre” de la Declaración de Prácticas de Confianza de VinCAsign.

6.4.9 Terminación del servicio

Los definidos en la sección 5.8 “Terminación del servicio” de la Declaración de Prácticas de Confianza de VinCAsign.

6.5 Controles de seguridad técnica

6.5.1 Gestión de los sistemas y de la seguridad

El SSA implementa los siguientes roles de gestión con diferentes privilegios:

- **Auditor del sistema:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a vinCAsign, reportando tanto a ésta como a la dirección técnica. Están autorizados a ver los archivos y registros de auditoria del servicio SSASC con el fin de auditar las operaciones del sistema de acuerdo con la Política de Seguridad.
- **Administrador del sistema:** Responsable del funcionamiento correcto del hardware y software soporte de la plataforma. Está autorizado a instalar, configurar y mantener el servicio activo, pero con acceso controlado a la información relacionada con la seguridad.
- **Operador del sistema**: es el responsable de la operación del día a día del servicio de firma remota, y de las operaciones de copia de seguridad y restauración.
- **Responsable de seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas y prácticas de seguridad de VinCAsign. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Los responsables de seguridad y los administradores de sistemas son usuarios privilegiados del sistema.

Los operadores del sistema y los auditores del sistema tienen funciones privilegiadas, pero no pueden administrar ni configurar el servicio SSASC.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Estas personas realizarán sus funciones basándose en el principio de menor privilegio.

VinCAsign asigna estos roles a personal designado y cualificado e implementa todos los controles de segregación de funciones definidos en la sección 6.2.1.2 de la norma CEN EN 419 241-1. [OVR-6.5.1-01]

6.5.2 Operaciones y Sistemas

La entidad dispone de procedimientos para operar de forma correcta y segura el SSASC. **[OVR-6.5.2-01]**

Tanto los componentes SSA como los HSM son operados de acuerdo con sus manuales para su instalación, administración y operación para cumplir con los objetivos de seguridad definidos en la Declaración de Seguridad de su certificación Common Criteria. **[OVR-6.5.2-02] [GEN-A.4-02] [GEN-A.5-02]**

6.5.3 Controles de seguridad informática

Todos los definidos en la sección 6.5 “Controles de seguridad informática” de la Declaración de Prácticas de Confianza de vinCAsign.

El SSASC se encuentra monitorizado y se generan alertas que son enviadas a los administradores del sistema cuando se detectan eventos que pueden impactar en su disponibilidad o comprometer su seguridad **[OVR-6.5.3-02]**

Adicionalmente el sistema de monitorización permite generar alertas basadas en reglas de correlación para detectar comportamientos que pueden denotar un potencial ataque.

6.5.4 Controles técnicos del ciclo de vida

Todos los definidos en la sección 6.6 “Controles técnicos del ciclo de vida” de la Declaración de Prácticas de Confianza de VinCAsign.

6.5.5 Controles de seguridad de red

Todos los definidos en la sección 6.7 “Controles de seguridad de red” de la Declaración de Prácticas de Confianza de VinCAsign.

6.6 Auditoría de conformidad

Según lo estipulado en la sección 8 “Auditorías de cumplimiento y otras evaluaciones” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7 Requisitos comerciales y legales

Todos los definidos en la sección 9 “Requisitos comerciales y legales” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.1 Tarifas

Según lo definido en la sección 9.1 “Tarifas” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.2 Capacidad financiera

Según lo definido en la sección 9.2 “Capacidad financiera” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.3 Confidencialidad

Según lo definido en la sección 9.3 “Confidencialidad” de la Declaración de Prácticas de Confianza de VinCAsgin.

6.7.4 Protección de datos personales

Según lo definido en la sección 9.4 “Protección de datos personales” de la Declaración de Prácticas de Confianza de VinCAsgin.

6.7.5 Derechos de propiedad intelectual

Según lo definido en la sección 9.5 “Derechos de propiedad intelectual” de la Declaración de Prácticas de Confianza de VinCAsgin.

6.7.6 Declaraciones y garantías

Según lo definido en la sección 9.6 “Declaraciones y garantías” de la Declaración de Prácticas de Confianza de VinCAsgin.

6.7.7 Renuncias a las garantías

Según lo definido en la sección 9.7 “Renuncias a las garantías” de la Declaración de Prácticas de Confianza de VinCAsgin.

6.7.8 Limitaciones de responsabilidad

Según lo definido en la sección 9.8 “Limitaciones de responsabilidad” de la Declaración de Prácticas de Confianza de VinCAsgin.

6.7.9 Indemnizaciones

Según lo definido en la sección 9.9 “Indemnizaciones” de la Declaración de Prácticas de Confianza de VinCAsgin.

6.7.10 Duración y terminación

Según lo definido en la sección 9.10 “Duración y terminación” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.11 Avisos y comunicaciones individuales de los participantes

Según lo definido en la sección 9.11 “Avisos y comunicaciones individuales de los participantes” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.12 Modificaciones

Según lo definido en la sección 9.12 “Modificaciones” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.13 Disposiciones para la resolución de litigios

Según lo definido en la sección 9.13 “Disposiciones para la resolución de litigios” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.14 Legislación aplicable

Según lo definido en la sección 9.14 “Legislación aplicable” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.15 Cumplimiento de la legislación aplicable

Según lo definido en la sección 9.15 “Cumplimiento de la legislación aplicable” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.16 Miscelánea

Según lo definido en la sección 9.16 “Miscelánea” de la Declaración de Prácticas de Confianza de VinCAsign.

6.7.17 Otras disposiciones

Según lo definido en la sección 9.17 “Otras disposiciones” de la Declaración de Prácticas de Confianza de VinCAsign.

7 REFERENCIAS

VinCAsign establece, en el contrato de suscriptor y en el PDS, que la legislación aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española. VinCAsign asume la aplicación de la normativa siguiente para el Servicio de firma remota descrito en la presente Política:

- Reglamento (UE) No 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 999/93/CE (Reglamento eIDAS).
- Declaración de Prácticas de Confianza de VinCAsign. (Accesible en https://www.vincasign.net)
- ETSI EN 319 401 v2.3.1 (Mayo 2021): General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1 v.1.4.1 (Octubre 2023): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- EN 319 411-2 v2.4.1 (Noviembre 2021): Requirements for trust service providers issuing EU qualified certificates.
- ETSI TS 119 431-1 v 1.2.1 (Mayo 2021): TSP service components operating a remote QSCD/SCDev (remote signing).
- ETSI TS 119 431-2 "*Requisitos de política y seguridad para prestadores de servicios de confianza; Parte 2: componentes del servicio del PSC que admiten la creación de firmas digitales AdES.*"
- ETSI TS 119 432 *"Firmas e Infraestructuras Electrónicas (ESI); Protocolos para la creación remota de firmas digitales"*.
- CEN - EN 419 241-1 *"Sistemas confiables que admiten la firma de servidores - Parte 1: Requisitos generales de seguridad del sistema".*
- CEN - EN 419 241-2 *"Sistemas confiables que admiten la firma del servidor Parte 2, Perfil de protección para QSCD para la firma del servidor".*
- *CSN EN 419 221-5 Perfiles de protección para módulos criptográficos TSP - Parte 5: Módulo criptográfico para servicios de confianza*