PÚBLICO

POLÍTICA Y DECLARACIÓN DE PRÁCTICAS DEL SERVICIO DE FIRMA EN SERVIDOR

CENTRO TECNOLÓGICO DEL NOTARIADO

Título del documento:	Política y declaración de prácticas del servicio de firma en servidor
Tipo de documento:	Política
Nombre del fichero:	SSASP PS ES v1.3.docx
Versión:	1.3
Estado:	Aprobado
Confidencialidad:	Público
Fecha:	06/05/2024
Autor:	Oficina de Seguridad

Revisión, Aprobación		
Revisado por:	Director Área de Seguridad y Firma Electrónica	Fecha: 06/06/2024
Aprobado por:	Comité de Seguridad	Fecha: 11/06/2024

Historial de cambios			
Versión	**Fecha**	**Descripción de la acción**	**Páginas**
1.0	05/04/2019	Creación del documento.	
1.1	27/02/2020	Revisión de erratas. Actualización de la versión y el certificado del sistema de firma remota. Se añaden aclaraciones a observaciones del auditor en los puntos 6.3.1 y 6.3.2.	
1.2	13/04/2023	Añadido nuevo componente de servicio basado en la solución Entrust SAM. Actualización de referencias y corrección de imprecisiones.	
1.3	06/05/2024	Se incluye referencia e imagen corporativa del Centro Tecnológico del Notariado. Se permiten claves RSA de longitud superior a 2048 bits.	

1. Índice

2. Introducción

Este documento contiene la Política y Declaración Prácticas del servicio de firma en servidor de la Agencia Notarial de Certificación S.L. Unipersonal (en adelante, Centro Tecnológico del Notariado, CTNotariado o ANCERT indistintamente).

El servicio de firma en servidor es un servicio en que la Agencia Notarial de Certificación S.L. Unipersonal gestiona en nombre del firmante su dispositivo de creación de firma permitiéndole generar firma electrónica a distancia asegurando el control exclusivo sobre sus claves de firma.

El presente documento se estructura de acuerdo a la especificación técnica ETSI TS 119 431[1].

3. Alcance

El presente documento define la Política y la Declaración de Prácticas que la Agencia Notarial de Certificación S.L. Unipersonal, en adelante ANCERT, para la operación de los componentes que gestionan dispositivos de creación de firma a distancia en nombre del firmante.

Los componentes del servicio consisten en la aplicación de creación de firma, el módulo de activación de firma y el dispositivo de creación de firma que podrá tener el carácter de cualificado de acuerdo con la definición del Anexo II del Reglamento (UE) 910/2014.

La presente Política y Declaración de Prácticas es aplicable a las claves de todos los certificados de firma electrónica emitidos por ANCERT que se definan en su Declaración de Prácticas de Certificación como certificados de firma electrónica remota o a distancia.

4. Conceptos generales

4.1. Términos, siglas y abreviaturas

4.1.1 Términos

El presente documento utiliza los siguientes términos y abreviaturas tal y como se definen en [4]:

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

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.

[1] Para facilitar la auditoría y el seguimiento del cumplimiento de los requisitos de seguridad definidos en ETSI TS 119 431 en las secciones 5 en adelante, cada vez que se define un control de seguridad se hace referencia a su numeración en dicha norma.

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.

dispositivo cualificado de creación de firma / sello electrónico (QSCD): dispositivo de creación de firma que cumple con los requisitos del Anexos II del Reglamento (EU) No 910/2014.

dispositivo remoto de creación de firma: dispositivo de creación de firma utilizado a distancia por el firmante y operado en su nombre bajo su control exclusivo de uso.

componente de servicio de aplicación de firma en servidor (SSASC): componente de servicio operado por un TSP, compuesto de una aplicación de firma en servidor (SSA), un módulo de activación de firma (SAM) que puede ser independiente o formar parte del SSA y un QSCD / SCdev, empleado para la creación de firmas electrónicas en nombre del firmante.

proveedor de servicio de aplicación de firma en servidor (SSASP): TSP que opera un SSASC.

dispositivo de creación de firma (SCDev o SCD): un equipo o programa informático configurado que se utiliza para crear una firma electrónica.

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 para la autenticación de sitios web; o la preservación de firmas, sellos o certificados electrónicos.

proveedor de servicios de confianza (TSP): entidad que provee de servicios de confianza.

4.1.2 Relación entre el TSP y el servicio de firma remota

ANCERT es un proveedor de servicios de confianza cualificado que emite certificados y sellos electrónicos cualificados de acuerdo con la legislación vigente. **[OVR-A.1-01]**

El servicio de SSASC forma parte de los servicios operados por ANCERT y permite prestar el servicio de firma electrónica a distancia a los firmantes que cuentan con un certificado electrónico definido para firma remota en su correspondiente Declaración de Prácticas de Certificación.

En el presente documento ANCERT es identificado como el SSASP.

4.1.3 Documentación aplicable al SSASC

Declaración de prácticas del SSASC

ANCERT, en calidad de SSASP, desarrolla, implementa, hace cumplir y actualiza el presente documento que contiene la Declaración de Practicas de SSASC.

La Declaración de Practicas de SSASC, es una declaración de prácticas de un servicio de confianza tal y como se define en la norma ETSI EN 319 401 [2]. **[OVR-5.1-01]**

Política del SSASC

El presente documento también define la política del SSASC.

Términos y condiciones

De manera adicional al presente documento ANCERT puede definir términos y condiciones adicionales del servicio.

5. Disposiciones generales de la política y de la declaración de prácticas

5.1. Requisitos generales de la declaración de prácticas

La presente Declaración de Prácticas y otra documentación relevante está disponible 24x7 en https://www.ancert.com/cps . **[OVR-5.1-03]**

La presente Declaración de Prácticas define en las secciones 6.2.1 y 6.3.1 los parámetros de creación de claves de los firmantes y los algoritmos de firma y sus parámetros utilizables en el SSASC **[OVR-5.1-02]**

ANCERT utiliza dos componentes SSASC para la prestación de los servicios de dispositivo remoto de creación de firma gestionado en nombre del firmante. El componente **SSASC G1** destinado a los certificados con custodia remota de claves de la jerarquía del Consejo General del Notariado y el componente **SSASC G2** dedicado para la custodia de claves de los certificados de firma emitidos para su uso dentro de la Sede Electrónica Notarial.

ANCERT utiliza en el **SSASC G1** su aplicación de firma remota en servidor (SSA) "ANCERT Server Signing Application" que en combinación con el módulo criptográfico conforma el "ANCERT Server Signing System". La solución "ANCERT Server Signing System" está certificada Common Criteria EAL 4+ ALC_FLR.2 + AVA_VAN.5 por el Centro Criptológico Nacional[2] y posee la cualificación de dispositivo cualificado de creación de firma. La declaración de seguridad del SSA está alineada con los requisitos de seguridad definidos en la norma EN 419 241-1.

ANCERT utiliza en el **SSA G2** el componente Entrust Signature Activation Module versión 1.0.3, en adelante Entrust SAM, que está certificado Common Criteria EAL 4+ en el perfil de protección EN 419 241-2 junto con módulo criptográficos Entrust nShield Connect XC también certificados Common Criteria en el perfil de protección EN 419 221-5. El componente Entrust SAM es un dispositivo seguro de creación de firma de acuerdo con los requisitos del Reglamento UE 910/2014.

5.1.1 Administración del documento

[OVR-5.1-01]

Organización que administra el documento

Agencia Notarial de Certificación, S.L. Unipersonal

Calle Campezo 1. Edificio 6, planta 2, 28022 Madrid (España)

[2] https://oc.ccn.cni.es/index.php/es/productos-certificados/productos-certificados/estado/50-evaluacion-finalizada/447-ancert-server-signing-system-v1-0

CIF: B-83395988

Datos de contacto de la organización

Cualquier contacto con la Agencia Notarial de Certificación, referente a esta Declaración de Prácticas puede realizarse por los siguientes medios:

- Vía e-mail a la dirección de correo electrónico ancert@ancert.com.
- Por teléfono al número 912187676.
- Directamente en la sede central de la Agencia Notarial de Certificación: Agencia Notarial de Certificación, S.L. Unipersonal Calle Campezo 1. Edificio 6, planta 2, 28022 Madrid (España)

Las alteraciones que se produzcan sobre los anteriores datos como Web, correo, dirección o teléfono constarán debidamente reflejadas en la página web www.ancert.com que la ANCERT mantiene en vigor en Internet.

Procedimientos de gestión del documento

Quien determina la idoneidad de esta Declaración de Prácticas y se encarga de su aprobación es el Comité de Seguridad de ANCERT.

Existe un procedimiento de creación, revisión y aprobación formal de este documento.

La presente Declaración de Prácticas puede ser modificada en cualquier momento por la Agencia Notarial de Certificación. De no aceptar cualquiera de los suscriptores con certificado en vigor alguna de las modificaciones acordadas puede instar la revocación de su certificado y destrucción de sus claves.

5.2. Nombre del documento e identificación

Este documento es la “Política y declaración de prácticas del servicio de firma en servidor” de la Agencia Notarial de Certificación y tiene asignado el OID: ANCERT.1943.0

El OID de ANCERT es: 1.3.6.1.4.1.18920.

ANCERT ha definido dos políticas para su SSASC:

- **Política de SSASC avanzado**, en el que opera un SCDev remoto, y tiene asignado el OID: ANCERT.1943.1.1.2.
- **Política de SSASC cualificado**, en el que opera un QSCD remoto, y tiene asignado el OID: ANCERT.1943.1.1.3.

La política ANCERT.1943.1.1.2 es conforme a la política “NSCP: Normalized SSASC Policy” definida en ETSI TS 119 431-1 [4] que tiene asignado el siguiente OID: 0.4.0.19431.1.1.2.

La política ANCERT.1943.1.1.3 es conforme a la política “EUSCP: EU SSASC Policy” definida en ETSI TS 119 431-1 [4] que tiene asignado el siguiente OID: 0.4.0.19431.1.1.3.

ANCERT revisa periódicamente la conformidad de sus políticas con respecto a la especificación ETSI TS 119 431-1 [4] y cambiará el identificador de sus políticas ante cualquier cambio en las políticas definidas en la sección 4.3.2 de dicha especificación. **[OVR-5.2-01]**

5.3. Participantes

5.3.1 Proveedor del servicio de firma remota (SSASP)

ANCERT actúa como SSASP y no delega a entidades terceras ninguna parte del servicio. **[OVR-5.3.1-01]**

5.3.2 Subscriptor 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.

La relación entre el subscriptor y el firmante es la que se define en la Declaración de Prácticas de hasta correspondiente al certificado electrónico asociado a la clave de firma.

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 depósito de certificados” de la Política General de Certificación.

6.2. Inicialización de las claves de firma

6.2.1 Generación de las claves de firma

SSASC G1

El **SSASC G1** utiliza la aplicación de firma en servidor (SSA) “ANCERT Server Signing Applicacion” en combinación con un módulo criptográfico (HSM) que actúa como SCDev / QSCD. La combinación de la aplicación SSA y el módulo criptográfico compone el sistema “ANCERT Server Signing System” [8] que está certificado por el Centro Criptológico Nacional[3]. El sistema “ANCERT Server Signing System” es un dispositivo cualificado de creación de firma. **[SRA_SKM.1.1]**

El **SSASC G1** utiliza HSMs con certificación FIPS PUB 140-2 L3 y Common Criteria EAL 4+ AVA_VAN.5 para realizar todas las operaciones criptográficas con las claves de los firmantes. **[SRG_KM.1.1] [GEN-A.4-01]**

[3] https://oc.ccn.cni.es/index.php/es/productos-certificados/productos-certificados/estado/50-evaluacion-finalizada/447-ancert-server-signing-system-v1-0

Fuera del módulo HSM las claves se almacenan cifradas con el algoritmo AES y una longitud de clave de 128 bits. La clave de cifrado es única y se deriva de una clave maestra del módulo HSM y de una clave de firmante derivada del PIN de activación que es transportado cifrado dentro del SAD. **[SRG_KM.1.3]**

SSASC G2

ANCERT utiliza en el **SSASC G2** el componente Entrust Signature Activation Module versión 1.0.3, que está certificado Common Criteria EAL 4+ en el perfil de protección EN 419 241-2. El componente Entrust SAM es un dispositivo seguro de creación de firma de acuerdo con los requisitos del Reglamento UE 910/2014. **[SRA_SKM.1.1]**.

El **SSASC G2** utiliza módulos criptográficos Entrust nShield Connect XC certificados Common Criteria EAL 4+ en el perfil de protección EN 419 221-5 para realizar todas las operaciones criptográficas con las claves de los firmantes. **[SRG_KM.1.1] [GEN-A.4-01]**

Fuera del módulo HSM las claves se almacenan cifradas con el algoritmo AES y una longitud de clave de 128 bits utilizando el formato definido por el componente Entrust SAM **[SRG_KM.1.3]**

Las operaciones de administración sobre el componente Entrust SAM requieren de control dual. **[GEN-6.2.1-08]**

Todos los componentes

Las claves de los firmantes son claves RSA con una longitud de clave de 2048 bits o superior. **[SRG_KM.1.2] [SRC_SKS.1.1]**

Las operaciones de administración del módulo criptográfico requieren de control dual. **[GEN-6.2.1-08]**

Los pares de claves de los firmantes son generados en la primera fase del proceso de emisión del certificado electrónico del firmante. Todo el proceso de generación de claves y emisión del certificado se completa en unos cuantos segundos. Antes de importar el certificado del firmante el par de claves del firmante se encuentran en estado no activo y el SSA y/o el componente SAM no permite su uso. **[GEN-6.2.1-07]** Junto a la clave del firmante el SSA genera una petición de certificado en formato PKCS #10 que sirve como prueba de posesión de la clave privada del firmante en el proceso de registro del certificado y emisión del certificado por parte de la Autoridad de Certificación. **[GEN-6.2.1-08]**

6.2.2 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 UE 2015/1502. **[LNK-6.2.2-01] [LNK-6.2.2-02]**

SSASC G1

La Autoridad de Registro entregará al firmante un código único de registro de un solo uso para completar el proceso de creación del par de claves de firma remota y la emisión del certificado asociado. El periodo de tiempo en el que el código de registro es válido es de una semana.

Los medios de identificación electrónica del firmante (par de claves de activación) y el PIN de activación son generados por el firmante en la aplicación de activación de firma (SAA) instalada en su teléfono inteligente.

La clave pública de activación[4] y el PIN de activación del firmante son enviados junto con el código de registro a la Autoridad de Registro mediante la SAA.

La Autoridad de Registro valida el código de registro del firmante y solicita al SSASC la creación de un par de claves vinculado a los medios de identificación electrónica del firmante recibidos. **[LNK-6.2.2-03]**

La Autoridad de Registro solicita a la Autoridad de Certificación el certificado electrónico vinculado al par de claves generado en el SSASC.

La Autoridad de Registro vincula el certificado emitido al par de claves del firmante en el SSASC. **[LNK-6.2.2-05]**

No se delegan partes del proceso de identificación y autenticación del firmante a terceras partes.

El SSA almacena la clave pública de activación en los metadatos asociados al par ce claves del firmante. El PIN de activación se utiliza como parte para derivar la clave de cifrado con la que se protegen las claves del firmante.

El SSA protege la integridad de las claves de los firmantes y sus metadatos asociados mediante el cómputo de una función HMAC. **[LNK-6.2.2-10]**

SSASC G2

La identificación y autenticación del firmante se delega en un componente que realiza las funciones de proveedor de identidad (IdP) y de servidor de autenticación (AS).

La Autoridad de Registro es la encargada de solicitar al SSA la creación del par de claves del firmante y de vincular éstas con la identidad del firmante. **[LNK-6.2.2-03]**

La Autoridad de Registro solicita a la Autoridad de Certificación el certificado electrónico enviándole un archivo PKCS#10 firmado con el par de claves del firmante que una vez emitido se encarga de vincular al par de claves generado por el SAM en el HSM. **[LNK-6.2.2-05]**

El SSA es el único componente autorizado para interactuar con el SAM y realizar las operaciones de generación de un nuevo par de claves, vincular un par de claves al identificador del firmante, firmar un fichero PKCS#10 y vincular un certificado a un par de claves.

[4] La clave pública es una referencia al medio electrónico de identificación

Las claves de los firmantes y sus metadatos asociados se encuentran firmados con las claves del SAM. **[LNK-6.2.2-10]**

6.2.3 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 SSA / SAM. El SSA / SAM verifica que la clave pública en el certificado del firmante y la almacenada en el sistema se corresponden **[LNK-6.2.3-01]**. En 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 SSA / SAM protege la integridad de las claves de de los firmantes y sus metadatos asociados mediante el cómputo de una función HMAC o una firma digital dependiendo del sistema. **[LNK-6.2.3-03]**

6.2.4 Provisión de los medios de identificación del firmante

ANCERT no genera los medios de identificación del firmante.

SSASC G1

Los medios de identificación del firmante, el par de claves de activación y el PIN de activación son generados por propio el firmante en la aplicación de activación de firma (SAA) instalada en un teléfono inteligente bajo su control.

La clave privada de activación reside en el teléfono inteligente del firmante y se utiliza para firmar los mensajes del protocolo de activación de claves (SAP).

SSASC G2

El SSASC G2 delega todo el proceso de identificación y autenticación del firmante en un componente externo IdP/AS, que debe proporcionar un nivel de aseguramiento al menos substancial requiriendo al firmante de un doble factor de autenticación basado en dos mecanismos de autenticación de diferente naturaleza (por ejemplo, algo que se sabe y algo que se tiene).

En el caso de los certificados de firma de la Sede Electrónica notarial se utiliza el proveedor IdP/AS de dicha sede para autenticar los usuarios. Los medios de autenticación utilizados son usuario y contraseña y un código OTP enviado por SMS al teléfono móvil que el firmante ha registrado en la Sede Electrónica.

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

6.3.1 Activación de las claves de firma

El SSASC requiere que el firmante se identifique y autentique completando de forma satisfactoria para cada uso de su clave de firma el protocolo de activación de firma (SAP) mediante el envío de un mensaje de activación de firma (SAD). **[SIG-6.3.1-01] [SIG-6.3.1-05]**

SSASC G1

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 protocolo de activación de firma (SAP) está diseñado para prevenir ataques de *man-in-the-middle* y *replay* **[SIG-6.3.1-02]**. Además de esto el mensaje SAD incorpora protecciones contra suplantación, robo de sesión, duplicación, robo de credenciales, *phishing* escucha y adivinación, mediante la combinación de técnicas de cifrado, firma electrónica, funciones resumen, incorporación de números aleatorios y uso de dos factores de autenticación de diferente naturaleza (algo que el firmante conoce y algo que firmante posee). Si el firmante introduce erróneamente 3 veces consecutivas el PIN de activación el acceso a la clave remota queda bloqueado. Una clave remota bloqueada solo puede ser desbloqueada por el propio firmante mediante la introducción de un código PUK **[SIG-6.3.1-06] [SIG-A.5-04] [SIG-A.5-06] [SIG-A.5-07]**

El PIN de activación se transporta siempre cifrado con una clave del SSA[5] dentro del mensaje de activación de clave (SAD) **[SIG-A.5-03]**

Los controles de acceso implementados en el SSA 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]**

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]**

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 SSA 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 SSA comprueba que la fecha de

[5] 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 SAD.

caducidad del certificado es válida, y deniega la operación en caso que ésta se haya superado **[SIG-6.3.1-08]**

El SSA 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]**

SSASC G2

Las claves del firmante solo se pueden activar a través del módulo SAM y 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). Para ello es necesario que complete una autenticación de doble factor en un componente IdP/AS autorizado por el SAM. El componente IdP/AS una vez completada la autenticación generará y firmará un mensaje de activación de firma SAD que vincula los datos del resumen criptográfico de los datos a firmar con el identificador de la clave del firmante **[SIG-6.3.1-04]**. Los mensajes SAD son firmados por el IdP/AS con una calve privada cuya parte pública se encuentra registrada y autorizada en el SAM.

El protocolo de activación de firma (SAP) está diseñado para prevenir ataques de *man-in-the-middle* y *replay* **[SIG-6.3.1-02]**. Además de esto el mensaje SAD incorpora protecciones contra suplantación, robo de sesión, duplicación, robo de credenciales, *phishing* escucha y adivinación, mediante la combinación de técnicas de cifrado, firma electrónica, funciones resumen, incorporación de números aleatorios y uso de dos factores de autenticación de diferente naturaleza (algo que el firmante conoce y algo que firmante posee). **[SIG-6.3.1-06] [SIG-A.5-04] [SIG-A.5-06] [SIG-A.5-07]**

Una vez se activa la clave del firmante el SAM 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 se desactiva la clave del firmante, requiriendo de un nuevo SAD para una nueva firma.

El SSA 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 SSA comprueba que la fecha de caducidad del certificado es válida, y deniega la operación en caso que ésta se haya superado **[SIG-6.3.1-08].** El SSA comprueba además para cada petición de firma antes de enviar el SAD al SAM que el certificado asociado a la clave no se encuentra revocado.

El SAM 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]**

Gestión de los datos de activación de firma

SSASC G1

El mensaje con los datos de activación de firma (SAD) es generado en la aplicación SAA instalada en el teléfono inteligente del 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 teléfono inteligente evitando así su duplicado. **[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]**

SSASC G2

El mensaje con los datos de activación de firma (SAD) es generado por el IdP/AS una vez el firmante completa la autenticación con un nivel al menos substancial. **[SIG-A.6-02]**

El mensaje del SAD contiene el resumen(es) criptográfico(s) de los datos a firmar y referencias que permiten identificar la clave seleccionada e identificar al firmante. Todo el mensaje del SAD se firma con una clave del componente IdP/AS autorizada en el SAM. **[SIG-A.6-01] [SIG-A.6-03] [SIG-A.6-06]**

El nivel AVA_VAN.5 de evaluación de la solución Entrust SAM 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]**

6.3.2 Borrado de las claves de firma

Las claves del firmante son borradas de forma inmediata de la base de datos del SSA cuando el certificado del firmante es revocado.

Periódicamente ANCERT ejecuta un proceso de borrado de la base de datos del SSA de aquellas claves de los firmantes cuyo certificado asociado ha caducado. **[DEL-6.3.2-01]**

Los firmantes podrán solicitar la revocación de su certificado electrónico en las Autoridades de Registro por los mecanismos establecidos en la Declaración de Prácticas de Certificación correspondiente. La revocación del certificado supone en todos los casos la destrucción la clave remota asociada. Mediante un procedimiento análogo, los firmantes podrán solicitar la eliminación de su clave remota, lo que a su vez supondrá la revocación del certificado asociado. **[DEL-6.3.2-02]**

El SSA o el SAM según corresponda a cada SSASC carga y activa la clave del firmante en el módulo criptográfico para cada operación de firma remota solicitada por el firmante. Una vez finalizada

la operación de firma solicitada con un mensaje de activación (SAD) el SSA o el SAM destruye automáticamente la clave de la firmante cargada en el módulo criptográfico. **[DEL-6.3.2-03]**

6.3.3 Copia de seguridad y restauración de la claves de firma

Las claves de los firmantes solo se pueden utilizar cuando están cargadas y activadas en el módulo criptográfico.

SSASC G1

Cuando no están cargadas en el módulo criptográfico las claves de los firmantes se almacenan cifradas en la base de datos del SSA utilizando el algoritmo de cifrado AES y una longitud de clave de 128 bits. La clave de cifrado para cada clave y firmante es diferente y se deriva a partir de una clave maestra del módulo criptográfico y el PIN de activación de clave que establece el firmante. **[GEN-6.3.3-01] [GEN-6.3.3-02]**

Se mantienen copias de seguridad periódicas de la base de datos del SSA, 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.

Las claves de infraestructura del SSASC son siempre almacenadas en contenedores cifrados.

El módulo criptográfico que contiene la clave maestra del SSASC que protege las claves de todos los firmantes requiere de control dual para su operación, copia de seguridad y restauración. La clave maestra del SSASC nunca abandona el módulo criptográfico en claro. **[GEN-6.3.3-03]**

El número de copias de seguridad es el mínimo para garantizar la continuidad del servicio. **[GEN-6.3.3-04]**

SSASC G2

Cuando no están cargadas en el módulo criptográfico las claves de los firmantes se almacenan cifradas en la base de datos del SSA en el formato propietario definido por el componente Entrust SAM utilizando el algoritmo de cifrado AES. **[GEN-6.3.3-01] [GEN-6.3.3-02]**

Se mantienen copias de seguridad periódicas de la base de datos del SSA, donde se almacenan las claves de los firmantes ya que el componente SAM no dispone de una base de datos, al igual que del resto de claves de infraestructura necesarias para garantizar la continuidad del servicio en caso de incidente.

Todas las claves de la infraestructura del SSASC son almacenadas en contenedores cifrados. Todas las claves de infraestructura del componente Entrust SAM están protegidas por el módulo HSM, incluidas las de cifrado de las claves del firmante. Para la administración del componente Entrust SAM, incluyendo la restauración del sistema, se requiere de control dual. De forma análoga todas las operaciones de administración del módulo criptográfico también requieren de control dual. Todas las calves de infraestructura del componente Entrust SAM nunca abandonan el módulo criptográfico en claro. **[GEN-6.3.3-03]**

El número de copias de seguridad es el mínimo para garantizar la continuidad del servicio. **[GEN-6.3.3-04]**

6.4. Controles de seguridad física, de gestión y de operaciones

6.4.1 Generales

Gestión de riesgos

ANCERT dispone de un plan de gestión de riesgos para identificar, analizar y evaluar los riesgos que pueden afectar al SSASC.

ANCERT dispone de un plan de tratamiento de riesgos en el que prioriza, selecciona e implementa las medidas de seguridad oportunas para tratar los riesgos identificados en los análisis de riesgos.

ANCERT actualiza el análisis de riesgo con la periodicidad establecida en su plan de gestión de riesgos y cada vez que se producen cambios substanciales en el servicio.

La dirección de ANCERT aprueba formalmente el plan de tratamiento de riesgos resultante de la actividad de gestión de riesgos y acepta el riesgo residual.

Política de seguridad de la información

ANCERT dispone de una política de seguridad de la información, aprobada por su Dirección, que define cómo la organización gestiona la seguridad de la información.

Gestión de activos

ANCERT realiza una gestión adecuada de todos sus activos y les asigna medidas de protección en función de su nivel de riesgo.

En particular, ANCERT dispone de un inventario de activos de información y asigna una clasificación a sus activos de acuerdo con su normativa de clasificación de la información y su análisis de riesgos.

Todos los medios de información son gestionados de forma segura de acuerdo con los requisitos establecidos en la política de seguridad de la información. ANCERT dispone de procedimientos para destruir de forma segura los medios de información que pueden contener información confidencial cuando finaliza su vida útil.

6.4.2 Controles de seguridad física

Los definidos en la sección 5.1 “Controles de seguridad física” de la Política General de Certificación.

6.4.3 Controles de procedimientos

Los definidos en la sección 5.2 “Controles de procedimientos” de la Política General de Certificación.

6.4.4 Controles de personal

Los definidos en la sección 5.3 “Controles de personal” de la Política General de Certificación.

6.4.5 Procedimientos de auditoría de seguridad

Todos los definidos en la sección 5.4 “Procedimientos de auditoría de seguridad” de la Política General de Certificación. **[OVR-6.4.5-01] [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.
- 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.

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]**

SSASC G1

El SSA 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 SSA genera un registro de auditoría continuo en el que solo es posible añadir nuevos eventos y no es posible eliminar o modificar los eventos anteriores.

El SSA protege los eventos del registro de auditoría a nivel de entrada y de todo el registro aplicando una función HMAC que encadena cada registro con el anterior. **[OVR-6.4.5-04]**

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]**

El SSA comprueba en el arranque y periódicamente la integridad del registro de auditoría para detectar el borrado o modificación. Adicionalmente el SSA dispone de una funcionalidad para verificar la integridad del registro de auditoría a petición de un usuario con rol de auditor en el sistema. **[OVR-6.4.5-06]**

SSASC G2

El SAM generar un registro de auditoría en el que solo es posible añadir nuevos eventos y no es posible eliminar o modificar los eventos anteriores.

El SAM protege la integridad de cada registro mediante una firma electrónica. **[OVR-6.4.5-04]**

Todos los registros de eventos del registro de auditoría del SAM 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]**

El SAM ofrece herramientas para validar la integridad y la autenticidad de los registros de auditoría. El SAM delega en el SSA la comprobación periódica de la integridad de los registros de auditoría. **[OVR-6.4.5-06]**

El SAM deja de procesar peticiones de forma automática en caso de detectar un compromiso físico del servidor en el que se ejecuta.

6.4.6 Archivo de informaciones

Según lo especificado en la sección 5.5 “Archivo de informaciones” de la Política General de Certificación. **[OVR-6.4.6-01]**

6.4.7 Cambio de claves

Según lo especificado en la sección 5.6 “Renovación de claves” de la Política General de Certificación.

6.4.8 Compromiso de claves y recuperación de desastre

Según lo especificado en la sección 5.7 “Compromiso de claves y recuperación de desastre” de la Política General de Certificación.

6.4.9 Terminación del servicio

Según lo especificado en la sección 5.8 “Terminación del servicio” de la Política General de Certificación.

6.5. Controles de seguridad técnica

6.5.1 Gestión de los sistemas y de la seguridad

El SSASC implementa los siguientes roles de gestión:

- **Responsable de seguridad** (security officer): tiene la responsabilidad general de administrar e implementar las políticas de seguridad y tiene acceso a la información de seguridad.
- **Administrador del sistema** (system administrators): es el responsable de instalar, configurar y mantener el TW4S pero con acceso controlado a la información de seguridad.
- **Operador del sistema** (system operators): es el responsable de la operación del día a día del TW4S y las operaciones de copia de seguridad y restauración.
- **Auditor del sistema** (system auditor): está autorizado para revisar los archivos y registros de auditoría del TW4S para auditar que las operaciones del sistema están alineadas con la política de seguridad.

ANCERT asigna estos roles a personal 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]**

El componte software SSA, el componente SAM y el módulo 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 Política General de Certificación. **[OVR-6.5.3-01]**

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

Los definidos en la sección 6.6 “Controles técnicos del ciclo de vida” de la Política General de Certificación. **[OVR-6.5.4-01]**

6.5.5 Controles de seguridad de red

Los definidos en la sección 6.7 “Controles de seguridad de red” de la Política General de Certificación. **[OVR-6.5.5-01]**

6.6. Auditoría de conformidad

Según lo especificado en la sección 6 “Auditoría de conformidad” de la Política General de Certificación.

6.7. Requisitos comerciales y legales

6.7.1 Tarifas

Según lo especificado en la sección 9.1 “Tarifas” de la Política General de Certificación.

6.7.2 Capacidad financiera

Según lo especificado en la sección 9.2 “Capacidad financiera” de la Política General de Certificación.

6.7.3 Confidencialidad

Según lo especificado en la sección 9.3 “Confidencialidad” de la Política General de Certificación.

6.7.4 Protección de datos personales

Según lo especificado en la sección 9.4 “Protección de datos personales” de la Política General de Certificación.

6.7.5 Derechos de propiedad intelectual

Según lo especificado en la sección 9.5 “Derechos de propiedad intelectual” de la Política General de Certificación.

6.7.6 Representaciones y garantías

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.7 Rechazo de otras garantías

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.8 Limitación de responsabilidades

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.9 Cláusulas de indemnidad

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.10 Caso fortuito y fuerza mayor

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.11 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.12 Enmiendas

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.13 Resolución de conflictos

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.14 Ley aplicable

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.15 Cláusula de jurisdicción competente

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

6.7.16 Otras provisiones

Según lo especificado en la sección 9.6 “Obligaciones y responsabilidad civil” de la Política General de Certificación.

7. Referencias

[1] Reglamento EU 910/2014.

[2] ETSI EN 319 401 v2.3.1 (Mayo 2021): General Policy Requirements for Trust Service Providers.

[3] EN 319 411-2 v2.4.1 (Octubre 2021): Requirements for trust service providers issuing EU qualified certificates.

[4] ETSI TS 119 431-1 v1.2.1 (Mayo 2021): TSP service components operating a remote QSCD/SCDev (remote signing).

[5] CEN EN 419 241-1 (Julio 2018): Trustworthy Systems Supporting Server Signing – Part 1: General System Requirements.

[6] Política General de Certificación de la Agencia Notarial de Certificación.

[7] ANCERT Server Signing Application v1.1.8 Security Target.

[8] ANCERT Server Signing System v1.0.0 Security Target

[9] Security Target – Entrust Signature Activation Module, version 2.1.

[10] CEN EN 419221-5 – Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services