# Guía de Seguridad de las TIC
# CCN-STIC 140

## Taxonomía de productos STIC-
## Anexo E5: Herramientas para firma electrónica

Febrero 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.02.27 09:36:44 +01'00'


NIPO: 083-19-053-9.

Fecha de Edición: febrero de 2019

**LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

**AVISO LEGAL**

# ÍNDICE

# 1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia de **Herramientas para firma electrónica** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a las que sea de aplicación el Esquema Nacional de Seguridad (ENS). Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
   - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia de **Herramientas para firma electrónica** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.
6. Esta familia de productos estará formada por dos tipos de productos: Dispositivos de creación de firma electrónica remota y Dispositivos seguro de creación de firma electrónica.

# 2. DISPOSITIVOS DE CREACIÓN DE FIRMA ELECTRÓNICA REMOTA

7. La funcionalidad de un dispositivo de creación de firma electrónica remota es la de producir una firma digital creada en nombre de y bajo el único control de una persona física o jurídica.

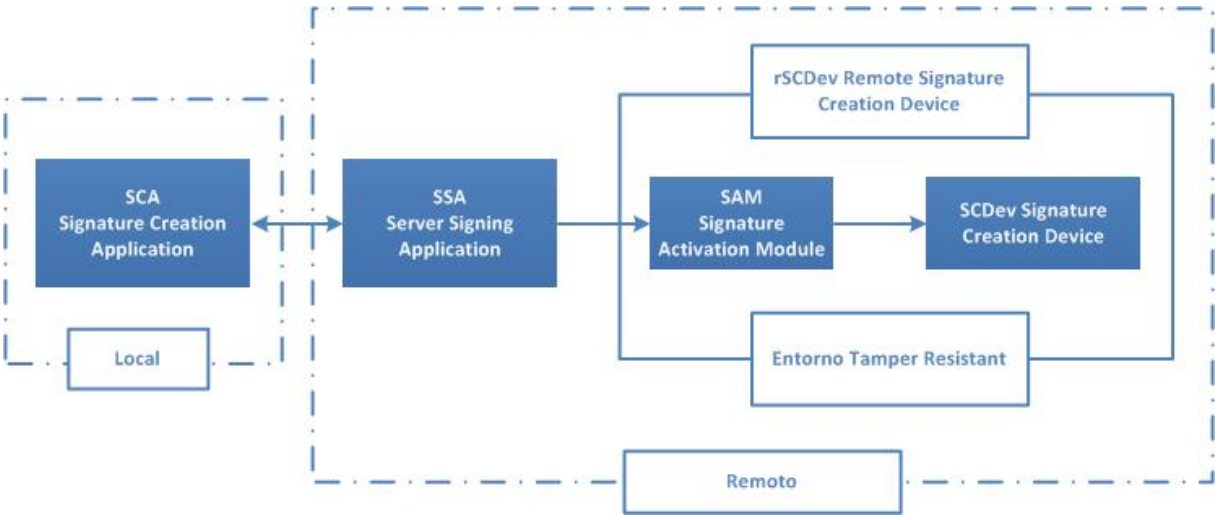
8. Los dispositivos que cumplan los requisitos establecidos en el presente documento podrán generar firmas reconocidas como Firma electrónica cualificada, tal como se define en el reglamento eIDAS [1].

## 2.1 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

9. Un sistema de confianza para firma electrónica o, como se denomina en inglés, *Trustworthy System Supporting Server Signing* (TW4S) puede consistir en un entorno local y remoto. El firmante está en el entorno local e interactúa, a través de una aplicación local, con la aplicación de firma de servidor o *Server Signing Application* (SSA).

10. Para asegurar que el firmante tiene el control único de las claves de firma, la operación de firma tiene que ser autorizada. Esta operación la realiza el módulo de activación de firma o *Signature Activation Module* (SAM), que puede obtener y activar la clave de firma dentro de un dispositivo de creación de firma *Signature Creation Device* (SCDev), normalmente implementado como módulo criptográfico. El SCDev y el SAM deben estará localizados dentro de un entrono *tamper resistant* común que puede ser considerado como el dispositivo de creación de firma remota o *Remote Signature Creation DEVice* (rSCDev).

11. El rSCDev, en combinación con el SSA, son la base del TW4S, que necesita ser operado de una manera segura y debe reunir algunos requisitos para el sistema.




## 2.2 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

12. Hasta el establecimiento, por parte de la Comisión Europea, de una lista de estándares para la evaluación de la seguridad de los productos de las

tecnologías de la información que aplican a la certificación de dispositivos de creación de firma electrónica cualificada, donde un proveedor de servicios de confianza cualificados gestiona los datos de creación de firma electrónica de parte de un signatario, la certificación de tales productos debe estar basada en un proceso que, de conformidad con el Artículo 30(3)(b), utilice niveles de seguridad comparables con aquellos requeridos en el Artículo 30(3)(a) y que sea notificado a la Comisión por el organismo público o privado referido en el párrafo 1 del artículo 30 de la reglamento (EU) 910/2014 [1].

13. La certificación de un dispositivo de creación de firma electrónica cualificada remoto por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) deberá de estar basada en los siguientes requisitos:

    a) Los productos que declaren funcionalidades SAM y/o SCDev estarán evaluados y certificados de acuerdo a los criterios de evaluación definidos en ISO/IEC 15408 [2], y con la metodología de evaluación establecidas en ISO/IEC 18045 "*Methodology for IT security evaluation*" [3], con un mínimo de nivel de aseguramiento de EAL4+ AVA_VAN.5.

    b) Los Productos que declaren funcionalidad SAM y/o SCDev deberán tener una Declaración de Seguridad definida para su evaluación que esté basada en los RFS especificados en este documento. El cumplimiento propio y técnicamente correcto de estos RFS serán analizados por el ENECSTI antes de aceptar el requisito de certificación del producto.

    c) No hay reglas de diseño preconcebidas relativas a implementaciones SAM y/o SCDev, que van desde un único producto o componente que cumple los requisitos de seguridad aplicables hasta una combinación de productos cuya composición cumple los requisitos.

       En el caso de se requieran dos o más productos o componentes para cumplir la funcionalidad de SAM y SCDev, existe una necesidad adicional de evaluar la seguridad de su composición, considerando sus interacciones y asegurando que el interfaz entre los componentes ha sido evaluado. También debería desarrollarse un análisis de vulnerabilidades para considerar la posible introducción de vulnerabilidades como resultado de la composición de componentes.

       La composición de productos o componentes requeridos en combinación con cumplir las funcionalidades de SAM y SCDev serán evaluadas y certificadas de acuerdo a los criterios de evaluación especificados en ISO/IEC 15408 [2] y con la metodología de evaluación establecida en la ISO/IEC 18045 "Methodology for IT security evaluation" [3], aplicando el CAP-C (Composition Assurance Package).

    d) Los procesos de evaluación de la seguridad requeridos a un producto que únicamente cumpla las funcionalidades de SAM o SCDev deberán

incluir en sus declaraciones de seguridad los RFS especificados para cada parte, aunque no podrán ser considerados por sí mismos un rSCDev.

## 2.3 SAM: REQUISITOS FUNDAMENTALES DE SEGURIDAD

14. El dispositivo será capaz de crear de forma segura una representación de un firmante y proteger los atributos de la representación del firmante asociados tanto a la integridad como a la confidencialidad si ésta fuese necesaria (QSCD-SIGNER-REPRESENTATION).
15. El dispositivo será capaz de utilizar de manera segura el módulo criptográfico para generar pares de claves de firma y asignarlas a la representación del firmante, protegiendo la integridad y la confidencialidad de las claves tal como se requiere (QSCD-CK GENERATION).
16. El dispositivo deberá asegurar que un administrador con un rol privilegiado es autenticado antes de realizar ninguna acción. También deberá asegurarse de que cualquier modificación a los datos de representación del firmante, claves o atributos de autenticación se realiza bajo el control de un rol de confianza o bajo el propio firmante. (QSCD-ATTR MODIFICATION).
17. El dispositivo deberá asegurar que el firmante está fuertemente autenticado antes de realizar ninguna acción. El dispositivo deberá implementar un protocolo de activación de firma, que también realizará un control de integridad de la representación transmitida del documento a firmar y de los datos de activación de firma, y controlará la confidencialidad de al menos los elementos que contengan información sensible y protección contra replicación de firma (QSCD-SIGNER AUTH).
18. El dispositivo deberá asegurar que el almacenamiento y la transmisión de datos críticos del firmante al dispositivo, como la representación del documento a firmar o los datos de autenticación, están protegidos frente ataques, modificaciones o divulgación no autorizada (QSCD-TRUSTED-PATH)
19. El dispositivo deberá asegurar también que ningún dato o atributo de firma, ni representación de documento a firmar o firmas son modificadas o divulgadas mientras se encuentren dentro del dispositivo (QSCD-INTEGRITY).
20. El dispositivo generará un registro de auditoría de los eventos de seguridad relevantes. El dispositivo deberá asegurar que las modificaciones a esta auditoría pueden ser detectadas (QSDC-AUDIT).

## 2.4 SCDEV REQUISITOS FUNDAMENTALES DE SEGURIDAD

21. El valor de texto claro de las claves secretas no deberán estar disponibles fuera del módulo criptográfico (CM-NO PLAINTEXT).
22. El módulo criptográfico ofrecerá funciones de generación de claves y otras funciones criptográficas provistas por usuarios que son aprobadas por autoridades reconocidas (CM-CRYPTO QUALITY).

23. El módulo criptográfico deberá proteger la integridad de los valores y los atributos críticos de las claves (secretas o públicas) frente a modificaciones no autorizadas. En este contexto, los atributos críticos están definidos como aquellos atributos de clave a nivel de implementación que podrían ser utilizados por un atacante para causar el equivalente a una modificación del valor de la clave por otros medios (CM-KEY INTEGRITY).
24. El módulo criptográfico deberá llevar a cabo una autenticación o chequeo de autorización de todos los sujetos antes de permitir su uso. En particular, deberá requerir siempre autorización antes de utilizar una clave secreta (CM-AUTHORISATION).
25. Cualquier clave (secreta o pública) deberá tener una definición no ambigua de las funciones criptográficas y operaciones (ej.: cifrado o firma) para los cuales está permitido su uso. El módulo criptográfico deberá rechazar todo intento de usar la clave para un propósito no permitido (CM-KEY PURPOSE).
26. El módulo criptográfico deberá tener una definición no ambigua de los sujetos a los que se debe permitir acceder a la clave (y los propósitos para los cuales puede usarse este acceso) y deberá permitirlo con una granularidad de un sujeto individual. (CM-KEY ACCESS).
27. El módulo criptográfico deberá definir y establecer claramente los límites en los cuales se requiere la autorización y la reautorización a la hora de utilizar una clave secreta. (CM-KEY REAUTH).
28. El módulo criptográfico deberá establecer canales seguros con las aplicaciones cliente que puedan ser usados para proteger la confidencialidad de datos sensibles durante su transmisión. También establecerá canales seguros entre partes separadas del módulo criptográfico cuando la transmisión se produzca a través de un entorno inseguro. (CM-PATH CONFIDENTIALITY).
29. El Módulo Criptográfico proveerá canales seguros a las aplicaciones cliente que pueden ser usadas para proteger la integridad de datos sensibles durante la transmisión entre la aplicación cliente y el Módulo Criptográfico. (CM-PATH INTEGRITY).
30. El módulo criptográfico deberá permitir importar y exportar claves secretas únicamente si se utiliza un método seguro que proteja la confidencialidad y la integridad del dato durante la transmisión. Las claves secretas solo deberán ser exportadas de forma cifrada. (CM-KEY SECURE EXPORT/IMPORT).
31. El módulo criptográfico deberá permitir que claves secretas individuales bajo su control sean identificadas como no exportables, en cuyo caso cualquier intento de exportarlas deberá ser rechazado automáticamente. Las claves públicas puede ser importadas y exportadas de manera que protejan la integridad de los datos durante la transmisión. (CM-NO EXPORT).
32. Cualquier método provisto por el módulo criptográfico para copia de seguridad de datos de usuario, incluyendo claves secretas, deberá preservar la seguridad de los datos y ser controlado solamente por administradores autorizados. El

proceso de *backup* seguro deberá preservar la confidencialidad y la integridad de los datos durante la creación, transmisión, almacenamiento y restauración de la copia. Los *backups* también deberán preservar la integridad de los atributos de las claves. (CM-BACKUP).

33. Los números aleatorios generados y suministrados a las aplicaciones cliente para su uso como claves, datos de autenticación y autorización, o semillas para otro generador de números aleatorios que sea usado para estos propósitos, deberán cumplir la métrica de calidad definida para asegurar que poseen la suficiente entropía (CM-RNG).
34. El módulo criptográfico deberá proteger sus funciones de seguridad contra *tamper*. En particular, deberá permitir cualquier manipulación física dentro del alcance de entrono detectable por los administradores del módulo. (CM-ANTITAMPER).
35. El módulo criptográfico deberá detectar faltas o errores que puedan causar que alguna propiedad de seguridad se debilite o falle, incluyendo las condiciones medioambientales fuera del rango operativo normal, potencia o temperatura, fallos críticos de componentes hardware del módulo criptográfico, del generador de números aleatorios, corrupción del software del módulo criptográfico, etc. Cuando se detecte un fallo, el módulo criptográfico tomará acciones para mantener su seguridad y la seguridad de los datos que contiene y controla. (CM-FAULT DETECTION).
36. El módulo criptográfico deberá crear y auditar registros de auditoría para eventos de seguridad relevantes, guardando los detalles del evento y el sujeto asociado al evento. El módulo criptográfico deberá asegurar que los registros de auditoría están protegidos contra borrado malicioso o modificación, para lo cual proveerá de protección anti-*tamper* (prevención o reacción) del registro de auditoría. (CM-AUDIT).

## 3. DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA ELECTRÓNICA

37. Los Dispositivos Seguros de Creación de Firma deberán estar certificados, dependiendo de las funcionalidades que implementen, contra alguno de los siguientes Perfiles de Protección:

| PERFILES DE PROTECCIÓN | | | |
|---|---|---|---|
| **Perfil de protección** | **Versión** | **Fecha** | **Organismo responsable** |
| *Protection Profiles for secure signature creation device – Part 2: Device with key generation* | 2.0.1 | 23/01/2012 | CEN/ISSS |
| *Protection Profiles for secure signature creation device – Part 3: Device with key import* | 1.0.2 | 24/07/2012 | CEN/ISSS |
| *Protection Profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application* | 1.0.1 | 14/11/2012 | CEN/ISSS |
| *Protection Profiles for secure signature creation device – Part 5: Extension for Device with key generation and trusted communication with signature creation application* | 1.0.1 | 14/11/2012 | CEN/ISSS |
| *Protection Profiles for secure signature creation device – Part 6: Extension for Device with key import and trusted communication with signature creation application* | 1.0.4 | 03/04/2013 | CEN/ISSS |

## 4. REFERENCIAS

[1] Reglamento (EU) 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.

[2] ISO/IEC IS 15408 Information Technology – Security Techniques – Evaluation Criteria for IT Security.

[3] ISO/IEC IS 18045 Information Technology – Security Techniques – Methodology for IT security evaluation.

[4] Orden Presidencial PRE/2740/2007, de fecha 19 de Septiembre de 2007, por el cual se aprueba la Regulación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información..

[5] Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016.

## 5. ABREVIATURAS

| | |
|---|---|
| **CC** | Criterios Comunes / Common Criteria |
| **CCN** | Centro Criptológico Nacional |
| **CPSTIC** | Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación |
| **ENECSTI** | Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. |
| **ENS** | Esquema Nacional de Seguridad |
| **ISSS** | Information Society Standardisation System |
| **PP** | Perfil de Protección |
| **RD** | Real Decreto |
| **RFS** | Requisitos Fundamentales de Seguridad |
| **RSCDev** | Remote Signature Creation Device |
| **SAM** | Signature Activation Module |
| **SCDev** | Signature Creation Device |
| **SSA** | Server Signing Application |
| **ST** | Security Target / Declaración de Seguridad |
| **STIC** | Seguridad de las Tecnologías de la Información y la Comunicación |
| **TIC** | Tecnologías de la Información y la Comunicación |
| **TW4S** | Trustworthy System Supporting Server Signing |