centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo E.2: Dispositivos/Herramientas de cifrado offline

Diciembre 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.12.27 13:21:14 +01'00'

NIPO: 083-19-053-9.

Fecha de Edición: diciembre 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 **Dispositivos/Herramientas de cifrado *offline*** 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 **Dispositivos/Herramientas de cifrado *offline*** 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.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. Los dispositivos o herramientas de cifrado fuera de línea u offline son productos que permiten el cifrado de información para su posterior almacenamiento o transporte cuando no se dispone de una infraestructura de comunicaciones o de intercambio de información segura.

2.2 CASO DE USO

7. Solamente se contempla un caso de uso para el producto considerado.
8. La herramienta o dispositivo offline realiza un cifrado de ficheros "fuera de línea", es decir, los ficheros se cifran localmente, desde la plataforma ala que está conectado (dispositivo) o desde la que se ejecuta (herramienta), para después ser almacenados, enviados o transportados utilizando un medio no seguro.

2.3 ENTORNO DE USO

9. Para la utilización en condiciones óptimas de seguridad de los dispositivos/herramientas de cifrado offline, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:
    - **Administración confiable:** El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la administración/empresa. Por ello se asume que dicha persona estará capacitada y formada.
    - **Plataforma confiable:** La plataforma en la que reside la herramienta o a la que se conecta el dispositivo deberá ser confiable, libre de malware que pudiese interferir en la correcta operación del producto.
    - **Criptografía confiable:** toda la criptografía implementada por el entorno operacional que vaya a ser utilizada por el producto deberá cumplir los requisitos descritos en este documento. Esto incluye la generación de factores de autenticación externos.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

10. Este tipo de productos suele presentarse en dos formatos:
    - Software instalable que se carga en la RAM[1] del equipo informático desde el que se realizarán las operaciones de cifrado de datos.
    - Dispositivo hardware (típicamente conectado mediante USB[2]) con un firmware embebido que realizará las operaciones de cifrado de datos en el propio chip del producto.

[1] *Random Access Memory*

11. En el caso en el que el producto sea un dispositivo hardware, también suele ir acompañado por una aplicación software que se instala en el ordenador al que se conecta y desde el que se realizan las operaciones.
12. La siguiente figura muestra un esquema de la arquitectura lógica de este tipo de productos.

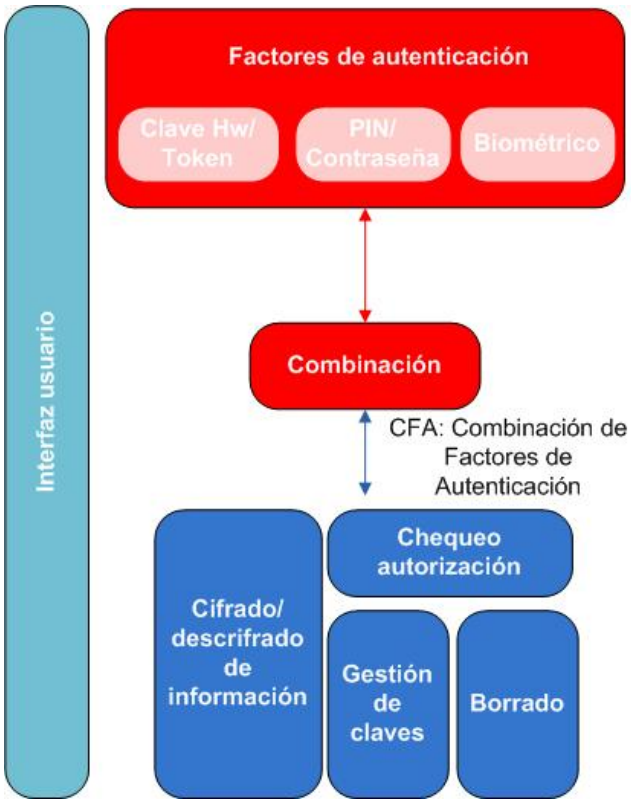

Figura 1 – Arquitectura lógica del sistema

13. A lo largo de este documento denominaremos Combinación de Factores de Autenticación (CFA) al valor resultante de combinar los distintos factores de autenticación utilizados.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

14. No se utilizará ningún perfil de protección *Common Criteria* como referencia para esta familia de productos.
15. El nivel de confianza EAL (*Evaluation Assurance Level*) conforme a CC, al que deben ser evaluados los Requisitos Fundamentales de Seguridad descritos en este documento debería ser **EAL2 o superior.**

[2] *Universal Serial Bus*

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

16. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:

    - Claves y material de cifra.
    - Datos que vayan a ser cifrados por el usuario.
    - Datos de configuración del producto.
    - Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

17. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

    - **Acceso no autorizado:** Un atacante consigue acceder al dispositivo/herramienta y a los datos contenidos en este.
    - **Compromiso del material de cifra:** Un atacante consigue acceder a claves, factores de autenticación, números aleatorios o cualquier otro factor que contribuya a crear las claves o factores de autenticación. Esto le permitirá al atacante el acceso a los datos almacenados.
    - **Obtención de claves:** Un atacante podría llegar a conseguir factores de autenticación como contraseñas o pin mediante la ejecución repetida de aplicaciones software, lo que podría facilitar el acceso a las claves de cifrado y por lo tanto a la información. Esto se produce cuando se eligen algoritmos débiles o con un reducido espacio de claves.
    - **Acceso a información en claro:** Un atacante podría tener acceso a zonas de memoria que contengan texto plano y que no hayan sido correctamente borradas o zonas conocidas donde se aloje código ejecutable.
    - **Acceso a información en claro elegida:** un atacante puede forzar que un usuario autorizado cifre algún fichero conocido en el dispositivo. La elección de algoritmos débiles o de vectores de inicialización podría provocar que el atacante pudiese obtener la clave de cifrado de datos.
    - **Actualizaciones / modificaciones no autorizadas.** Un atacante puede intentar realizar una actualización/modificación del producto que comprometa sus funcionalidades de seguridad instalando software o firmware que lo permitan o que contengan código dañino.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

18. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 REQUISITOS CRIPTOGRÁFICOS

19. **REQ. 1** NOTA: Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 (Categoría ALTA).
20. **REQ. 2** Las claves utilizadas por los algoritmos criptográficos empleados por el producto deberán tener una fortaleza de seguridad de 128 bits o superior.
21. **REQ. 3** Generador de bits aleatorios. En caso de requerir un servicio de generación de bits aleatorios (RBG) determinísticos, el producto deberá:
    a. *Utilizar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).*
    b. Usar una semilla de al menos una fuente de entropía que acumule entropía de varias fuentes o disponer de una fuente de entropía estudiada, con un mínimo de bits de entropía al menos igual a la mayor fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.
22. **REQ. 4** Algoritmos HASH. Las funciones HASH que utilice el producto deberán utilizar los algoritmos SHA-2 y SHA-3 de longitud mayor o igual a 256.
23. **REQ. 5** Verificación de firma: Para los servicios de verificación de firma digital, el producto deberá utilizar uno de los siguientes algoritmos:
    a. *Digital Signature Algorithm* (DSA) con una longitud de clave de 3072 bits o superior.
    b. *Elliptic Curve Digital Signature Algorithm* (ECDSA) con una longitud de clave de 256 o superior.
    c. RSA con una longitud de clave de 3072 o superior.
24. **REQ. 6** Autenticación de mensajes. Para los servicios de autenticación de mensajes, el producto podrá utilizar:
    a. HMAC-SHA-256, 384 o 512.
    b. CMAC-AES-128 o 256.

    y claves criptográficas de longitud 128 bits o superior.

25. **REQ. 7** Envoltura digital de claves. Para la implementación de envoltura digital de claves, el producto podrá utilizar AES en los modos KW, KWP, GCM, CCM, con longitud de claves de 128 bits o superior.

26. **REQ. 8** Transporte de claves. Para el transporte de claves, se utilizará:

    c. RSA en los modos KTS-OAEP o KTS-KEM-KWS, con longitud de clave de 3072 o superior.

    d. AES-128 o superior.

    e. Curvas elípticas con una longitud de clave de 256 o superior.

27. **REQ. 9** Generación de *salt, nonce* y vector de inicialización.

    a. Las *salt* utilizadas por el producto serán generadas por un DRBG propio o suministrado por la plataforma.

    b. En el caso de que el producto utilice *nonce*, éstos deberán ser únicos y con una longitud mínima de 64 bits.

    c. El producto creará los vectores de inicialización de la siguiente manera:

        - Para el modo CBC: los vectores de inicialización deberán ser no repetidos e impredecibles.
        - Para el modo CCM: los *nonce* deberán ser no repetidos e impredecibles.
        - XTS: No utilizará vectores de inicialización. Los Tweak Values deberán ser enteros no negativos, asignados consecutivamente y comenzando por un entero no negativo arbitrario.
        - GCM: Los vectores de inicialización deberán ser no repetidos. El número de invocaciones de GCM no excederá de 2^32 para una clave secreta dada.

28. **REQ. 10** Derivación de claves. Para la derivación de claves, el producto podrá aceptar:

    a. una submáscara generada por un RBG de acuerdo a lo especificado anteriormente.

    b. una submáscara condicionada por contraseña.

    c. una submáscara importada.

    para derivar en una clave intermedia utilizando las funciones hash especificadas, de forma que el resultado tenga una fortaleza de seguridad equivalente a 128 bits o superior.

29. **REQ. 11** Combinación de claves. En caso de utilice este método para la generación de claves, el producto combinará diferentes submáscaras utilizando una OR exclusiva (XOR), SHA-256 o superior para generar una clave intermedia o una clave de cifrado de disco.

30. **REQ. 12** Cifrado de datos en disco. El producto deberá cifrar los datos de disco utilizando AES CBC, GCM, CCM, XTS sin necesidad de intervención por parte del usuario.
31. **REQ. 13** Cifrado de claves. El producto implementará cifrado de claves de acuerdo con el algoritmo AES los modos CBC, GCM y longitud de claves 128 bits o superior.
32. **REQ. 14** Generación de claves simétricas. Las claves simétricas generadas por el producto se obtendrán utilizando el RBG especificado, con longitud mayor o igual a 128 bits.
33. **REQ. 15** Generación de claves asimétricas. El producto podrá importar o generar claves asimétricas para la envoltura digital de claves. Para ello, podrán utilizarse los siguientes algoritmos de generación de claves:
    a. Esquemas RSA con longitud de clave mayor o igual a 3072 bits.
    b. Esquemas ECC de longitud de clave mayor o igual a 256.
34. **REQ. 16** Para la obtención de claves de cifrado, el producto podrá utilizar uno de los siguientes métodos:
    a. Generar la clave simétrica.
    b. Aceptar la clave a partir del RBG suministrado por la plataforma.
    c. Aceptar una clave envuelta digitalmente.
35. **REQ. 17** El producto deberá implementar los siguientes métodos de borrado de claves:
    a. Para memoria volátil, la destrucción podrá ser realizada utilizando los siguientes métodos:
        - Un patrón de sobrescritura de una pasada utilizando un patrón pseudoaleatorio generado por el RBG del producto, ceros, unos, un nuevo valor de clave o algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
        - Apagado de la alimentación de la memoria.
        - Destrucción de la referencia a la clave directamente seguida por una llamada al “recolector de basura” de la memoria.
    b. Para memoria no volátil:
        - Que emplee un algoritmo de *wear-leveling*, la destrucción deberá consistir en alguno de los siguientes métodos:
            1. Una sola pasada de sobrescritura consistente en ceros, unos, un nuevo valor de clave de la misma longitud u otro valor que no contenga ningún PSC.
            2. Borrado de bloque.

- Que no emplee un algoritmo *wear-leveling*, la destrucción deberá ejecutarse por:
    1. Una o más pasadas de sobrescritura consistente en ceros o algún valor que no contenga ningún CSP seguidos de una lectura de verificación.
    2. Una o varias pasadas de sobrescritura consistente en todos unos seguidos de una lectura de verificación, sobrescrito con un nuevo valor de una clave con la misma longitud seguido por una lectura de verificación.
    3. Borrado de bloque.

Y si la lectura de verificación de los datos sobrescritos falla, el proceso deberá ser repetido de nuevo hasta alcanzar un número N (N>1) de intentos en el cual se devuelva un error.

36. **REQ. 18** Destrucción del material criptográfico. Todos los parámetros intermedios y claves criptográficas serán destruidas cuando finalice su uso, utilizando los métodos de borrado seguro establecidos.
37. **REQ. 19** El producto deberá destruir (o indicar al entorno operacional que destruya) el material criptográfico o factores de autenticación contenidos en claro cuando se encuentren en memoria y se reinicie o apague el sistema, se encuentre en inactividad o el usuario administrador, tanto local como remoto, así lo soliciten.
38. **REQ. 20** Protección de las claves y el material de cifra. El producto no deberá almacenar claves en memoria no volátil. Sólo podrá hacerlo cuando esté envuelta digitalmente o cifrada, o cuando reúna alguno de los siguientes criterios:
    a. La clave no cifrada no es parte de la cadena de claves.
    b. La clave no cifrada no permita acceso a los datos cifrados tras la utilización inicial.
    c. La clave no cifrada se grabe en un dispositivo de almacenamiento externo para ser utilizada como factor de autenticación.
39. **REQ. 21** Validación:
    a. Se realizará una validación del CFA utilizando alguno de los siguientes métodos:
        - Envoltura digital de clave.
        - Hash del CFA, submáscara o clave intermedia comparado con el hash del CFA, submáscara o clave intermedia almacenado.
        - Descifrado de un valor conocido usando submáscara, clave intermedia o CFA y comparándolo con un valor conocido almacenado.

b. El producto requerirá que se valide el CFA, submáscara o clave intermedia antes de que se permita el acceso al usuario a cualquier dato protegido.

c. El producto deberá permitir alguna de estas opciones:

- Forzar un retardo tal que solamente se puedan realizar un número de intentos N (N>1) en un periodo de 24 horas.
- Que se bloquee el proceso de validación tras un número N (N>1) de intentos de validación consecutivos.
- Requerir reiniciar el producto tras un número N (N>1) de intentos de acceso fallidos consecutivos.

40. **REQ. 22** El producto requerirá una nueva autenticación después de un estado apagado, suspensión o hibernación.
41. **REQ. 23** Todos los procesos de ejecución de mecanismos criptográficos correrán de manera independiente.

4.2 ADMINISTRACIÓN DEL PRODUCTO

42. **REQ. 24** El producto presentará al menos dos tipos de perfiles: administradores y usuarios, a los que se asociarán diferentes permisos.
43. **REQ. 25** La administración del producto sólo podrá ser realizada por un perfil de administrador.
44. **REQ. 26** El producto deberá ser capaz de implementar las siguientes funciones de gestión:
    a. Modificación de la clave de cifrado de disco.
    b. Borrado de la clave de cifrado de disco.
    c. Modificación de los factores de autenticación usados por parte de los usuarios autorizados.
    d. Actualización del firmware/software del producto.
    e. Gestionar usuarios, incluyendo su creación y asignación de privilegios, así como la baja o supresión de aquellos.

4.3 ADMINISTRACIÓN DEL PRODUCTO

45. **REQ. 27** El producto deberá implementar:
    a. Auto chequeos de arranque, donde se verifique la integridad del software o firmware, los mecanismos criptográficos y de funciones críticas, si procede.
    b. Auto chequeos condicionales: Comprobación de los parámetros de seguridad sensibles (PSS) durante su establecimiento y entrada y salida.

Verificación de la integridad y autenticidad del software o firmware durante su carga. Test periódico de los mecanismos criptográficos.

46. **REQ. 28** El producto deberá tener la capacidad de verificar las actualizaciones del software/firmware utilizando firma digital con anterioridad a la instalación de estas actualizaciones. Solo permitirá la actualización en el caso de que la verificación de la firma haya sido correcta.

4.4 SEGURIDAD FÍSICA

47. **REQ. 29** En el caso en que el producto tenga componentes hardware, éste deberá:

    a) Implementar mecanismos *tamper-evidence* ante un intento de acceso no autorizado.

    b) Implementar encapsulado opaco que impida la observación directa o manipulación del módulo criptográfico.

    c) Distinguir lógicamente entre entrada de datos y de control, y salida de datos, control y estado.

5. ABREVIATURAS

AES	*Advanced Encryption Standard*
CBC	*Cipher Block Chaining*
CC	*Common Criteria*
CCM	*Counter with CBC-MAC*
CCN	*Centro Criptológico Nacional*
CD	*Compact Disk*
CMAC	*Cipher-Based Message Authentication Code*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
DSA	*Digital Signature Algorithm*
EAL	*Evaluation Assurance Level*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ENS	*Esquema Nacional de Seguridad*
GCM	*Galois/Counter Mode*
HMAC	*Hash-based message authentication code*
KEM	*Key-Encapsulation Mechanism*
KTS	*Key Transport Scheme*
KW	*Key Wrap*
KWP	*Key Wrap with Padding*
KWS	*Key-Wrapping Scheme*
MAC	*Message Authentication Code*
OAEP	*Optimal Asymmetric Encryption Padding*
PSC	*Parámetros de Seguridad Críticos*
PSS	*Parámetros de Seguridad Sensibles*
RAM	*Random Access Memory*
RBG	*Random Bit Generator*
RFS	*Requisitos Fundamentales de Seguridad*
RSA	*Rivest, Shamir y Adleman*
SHA	*Secure Hash Algorithm*
USB	*Universal Serial Bus*
XOR	*eXclusive OR*