centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo O.1M: Estaciones de carga de vehículos eléctricos

Septiembre de 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.10.03 16:53:45 +02'00'

NIPO: 083-23-071-5
Fecha de Edición: septiembre de 2023

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 **Estaciones de carga de vehículos eléctricos** 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 los que sea de aplicación el **Esquema Nacional de Seguridad (ENS), categoría MEDIA**. 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 **Estaciones de carga de vehículos eléctricos**, 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. Una estación de carga permite proveer la recarga rápida de las baterías de los vehículos eléctricos mediante la conexión directa a la red eléctrica.

2.2 CASOS DE USO

7. Dada la naturaleza y el objetivo de este tipo de productos, se contemplan dos (2) casos de uso para esta familia, tal y como se indica a continuación.

2.2.1. CASO DE USO 1: SIN BACKEND

Estaciones de recarga que cuentan con supervisión local. En esta situación el producto puede funcionar con autenticación local o sin autenticación local.

2.2.2. CASO DE USO 2: CON BACKEND

Estaciones de carga conectadas a un sistema de supervisión para asegurar el monitoreo remoto.

2.3 ENTORNO DE USO

8. Por lo general, estos dispositivos se utilizan en grandes o medianas empresas y en redes del sector público, junto con otras medidas de seguridad complementarias, formando parte de una arquitectura de defensa en profundidad que busca proteger el entorno de comunicación.
9. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones:
   - **Administración confiable:** El administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención maliciosa al administrar el producto.
   - **Actualizaciones periódicas:** El producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
   - ***Backend* seguro:** El *Backend* está configurando de forma correcta para establecer canales de comunicación seguros y para proveer, en caso necesario, información al usuario final de forma segura.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

10. Este tipo de productos se presenta en formato de *appliance* dedicado.

11. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, estas quedan fuera del alcance analizado, y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 CERTIFICACIÓN LINCE

12. Para que un producto de esta familia pueda ser incluido en el CPSTIC como producto cualificado categoría MEDIA, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[1] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.

[1] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.es)

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

13. Los recursos que deben protegerse mediante el uso de estos productos incluyen:

- **AC.Administración**. Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos, que debe ser protegida en Confidencialidad, Trazabilidad, Autenticidad e Integridad.
- **AC.PSS**. Datos de configuración, registros auditoría y [asignación: listado de datos definidos por el fabricante] que deben ser protegidos en Integridad.
- **AC.PSC**. [selección: credenciales; claves; [asignación: listado de datos definidos por el fabricante] que deben ser protegidos en Confidencialidad e Integridad.
- **AC.Actualizaciones**. Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.
- **AC.Comunicaciones**. Comunicaciones del producto, establecidas entre sus propios componentes y con [**asignación**: *listado de entidades autorizadas*] que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.
- **AC. Suministro:** El suministro eléctrico que el producto es capaz de proveer a un vehículo eléctrico durante el proceso de carga.

3.2 AMENAZAS

14. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo al caso de uso expuesto en la sección 2.1, serían:

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.
- **A.CRYPTO Mecanismos criptográficos débiles:** Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Protocolos de comunicación no autorizados:** Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto.
- **A.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades del producto.

- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.
- **A.PSC y A.PSS Compromiso de parámetros de seguridad críticos y/o sensibles:** un atacante puede comprometer los parámetros de seguridad críticos y/o sensibles y acceder de forma continuada al producto y a sus datos críticos y/o sensibles.
- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **A.NOAUTUSR Acceso no autorizado de usuario:** Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso de credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.

3.3 TRAZABILIDAD AMENAZAS/ REQUISITOS DE SEGURIDAD

15. En la siguiente tabla se trazan que Requisitos Fundamentales de Seguridad definidos en el apartado 4 cubren las amenazas definidas:

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSS	A.PSC	A.FUN	A.NOAUTUSR	A.CRE
ADM.1	X									
ADM2	X									
ADM.3	X									
IAU.1	X								X	
IAU.2										X
IAU.3										X
IAU.4	X									
COM.1		X	X							
COM.2			X							
COM.3			X							
COM.4		X	X							
ACT.1				X						
ACT.2				X						
ACT.3				X						
AUD.1					X					
AUD.2					X					

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSS	A.PSC	A.FUN	A.NOAUTUSR	A.CRE
AUD.3					X					
AUD.4					X					
AUD.5					X					
AUD.6					X					
PSC.1							X			
PSC.2							X			
PRO.1								X		
CIF.1		X	X							
CIF.11		X	X							
CAR.1								X		
CAR.2								X		
CAR.3								X		
CAR.4								X		

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

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

4.1 ADMINISTRACIÓN CONFIABLE

17. Podrán ser cubiertas por el TOE o por su entorno operacional.

ADM.1 El TOE debe definir, al menos, el perfil de administrador y ser capaz de asociar usuarios a perfiles.

ADM.2 El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:

- Administración del producto [**selección***: local; remota*].
- [**asignación**: *otras funcionalidades administrables del producto*].

ADM.3 El TOE deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones descritas en ADM.2.

Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionalidades para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

IAU.1 El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación**: *otros usuarios del producto*] antes de otorgar acceso, salvo para las siguientes funcionalidades [**asignación**: *listado funcionalidades*].

IAU.2 El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

IAU.3 El TOE deberá disponer de la capacidad de gestión de las contraseñas:

a) La contraseña debe poder configurarse con una longitud mínima o igual a 12 caracteres.
b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “]

Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

IAU.4 El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación****: tiempo de inactividad*] de inactividad.

4.3 CANALES SEGUROS

COM.1 Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección***: IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

COM.2 El TOE debe permitir que los canales de comunicación definidos en COM.1 sean iniciados por él mismo o por las entidades autorizadas.

COM.3 El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en COM.1.

COM.4 Protección de la información del canal de administración. El TOE deberá establecer canales seguros cuando intercambie información con el administrador remoto, usando [**selección**: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

4.4 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

ACT.1 El TOE ofrecerá la posibilidad de consultar la versión actual del *firmware/software* y podrá [**selección***: actualizarse automáticamente; iniciar actualizaciones manualmente*] y [***selección****: comprobar si existen nuevas actualizaciones disponibles; ningún otro*].

ACT.2 El TOE deberá utilizar [**selección***: hashes publicados; firma digital*] que estén autorizados en la guía CCN-STIC-807 para autenticar las actualizaciones *firmware/software* antes de instalarlas.

ACT.3 La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.5 AUDITORÍA

AUD.1 El TOE debe generar registros de auditoría y cuando se produzca alguno de los siguientes eventos:

a) Al inicio y finalización de las funciones de auditoría.
b) *Login* y *logout* de usuarios.
c) Cambio en las credenciales de usuarios.

d) Cambios en la configuración del producto [**asignación***: listado de cambios*].
e) Eventos relativos a la funcionalidad del producto [**asignación***: listado de eventos*]
f) Si el TOE gestiona claves criptográficas, [**selección***: generación; importación; cambio; eliminación de claves criptográficas; ningún otro*].

AUD.2 Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento.

AUD.3 A los registros de auditoría se aplicará la siguiente política de acceso:

a) Lectura: solo usuarios autorizados.

b) Modificación: ningún usuario.

c) Borrado: [**selección***: solo administradores; ningún usuario*]

AUD.4 El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección***: transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada*].

AUD.5 El TOE deberá [**selección***: sobreescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC*] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

AUD.6 El producto debe ser capaz de proveer registros de auditoría con una fecha y hora de una fuente confiable.

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

PSC.1 En el caso en que el TOE almacene [***selección****: credenciales; claves privadas; [**asignación***: otros parámetros de seguridad críticos*] estos no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con CIF.1.

PSC.2 Destrucción de PSC. El TOE deberá borrar todos los PSC que utilice una vez finalice su uso implementando uno de los siguientes métodos de borrado.

a) Para memoria volátil, la destrucción podrá ser realizada utilizando los siguientes métodos:

i. Una pasada de sobrescritura utilizando alguno de los siguientes métodos:

- Un patrón pseudoaleatorio generado por el RBG.

- Todo cero o uno.
- Algún valor que no contenga ningún parámetro de seguridad crítico (PSC).

ii. Destrucción de la referencia a la clave directamente seguida por una llamada al "recolector de basura" de la memoria.

iii. Apagado de la memoria.

b) Para memoria no volátil:

i. Que emplee un algoritmo de *wear-leveling*, la destrucción deberá consistir en alguno de los siguientes métodos:

- Una sola pasada de sobrescritura consistente en ceros, unos u otro valor que no contenga ningún PSC.
- Borrado de bloque.

ii. Que no emplee un algoritmo *wear-leveling*, la destrucción deberá ejecutarse por:

- Una o más pasadas de sobrescritura consistente en ceros, unos o algún valor que no contenga ningún CSP seguidos de una lectura de verificación.
- 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.

4.7 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

PRO.1 El TOE deberá ser capaz de realizar un test durante el arranque o encendido del producto, [**selección***: periódicamente durante la operación normal del producto; a petición de un usuario autorizado; ninguna*] para verificar la integridad del software/firmware, [***selección****: el correcto funcionamiento de los mecanismos criptográficos; [**asignación**: otros]; ninguno*].

4.8 CRIPTOGRAFÍA

CIF.1 El TOE permitirá exclusivamente el empleo de mecanismos criptográficos: [***asignación****: listado de mecanismos*] autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría MEDIA del ENS, y de acuerdo al nivel de amenaza establecido.

CIF.11 El producto permitirá destruir (u ordenar la destrucción al entorno operacional) los parámetros de servicios criptográficos (material criptográfico, factores de autenticación, etc…) almacenados en texto claro cuando en almacenamiento volátil, y:

a) El sistema es reiniciado, apagado o inactivado.

b) El administrador (remoto o local) lo solicita.

4.9 CARGADOR ELÉCTRICO

CAR.1 El producto sólo podrá ser utilizado en una sesión de carga por usuarios autorizados mediante [una tarjeta sin contacto (RFID), código QR, tarjeta de crédito] o autorización remota.

> Nota de aplicación: la norma ISO 15118 podrá ser utilizada por el producto para permitir un medio de pago seguro al usuario final.

CAR.2 El producto debe permitir el acceso a usuario autorizados utilizando una lista blanca que permita una operación de carga completa si ocurriera un fallo en las comunicaciones (modo offline).

CAR.3 El producto debe tener mecanismos para detectar un acceso físico a sus componentes internos.

CAR.4 El producto deberá utilizar el protocolo OCPP (OCPP v1.6 o superior) configurado de forma segura para transmitir información dentro de la red interna del proveedor del suministro eléctrico.

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
ENS	Esquema Nacional de Seguridad
OCPP	*Open Charge Point Protocol*
RFS	Requisitos Fundamentales de Seguridad
TOE	*Target of Evaluation*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL