centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC
Anexo A.4: Servidores de Autenticación

Octubre 2021

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.03.21 15:58:22 +01'00'

NIPO: 083-21-130-1

Fecha de Edición: Octubre 2021

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 **Servidores de autenticación** 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 ALTA.** 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 **Servidores de autenticación** 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 productos asociados a esta familia están orientados a verificar la identidad de un usuario o dispositivo, en función de uno o varios factores, dentro de una arquitectura de red protegida. Estos productos suelen situarse justo delante de los servicios de una organización para asegurar que son utilizados únicamente por aquellas identidades autorizadas de acuerdo a la política de seguridad de la organización.

7. En este contexto, las funciones básicas de seguridad que proporcionan esta familia de productos son las siguientes:

    - **Identificación y autenticación de usuarios**. Permiten la aplicación de una política de seguridad centralizada y común para el control de acceso a servicios o sistemas de diferente naturaleza interconectados con el producto, además de proporcionar mayor transparencia al usuario en el proceso de autenticación a los servicios o sistemas a los que el producto le habilite el acceso, en función de sus permisos.

    - **Autenticación multifactor**. Permiten utilizar conjuntamente diferentes formas de autenticación (p.ej. contraseña conocida por el usuario y código de seguridad enviado a un dispositivo móvil que posee el usuario) para confirmar con mayor fiabilidad la identidad de un usuario.

    - **Ruptura del protocolo de autenticación**. Todos los procesos de autenticación requeridos por los servicios utilizados en la organización pasan por el servidor de autenticación, que está diseñado e implementado de forma segura para evitar numerosos ataques frente a los que los servicios que protegen pueden ser vulnerables.

8. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej. control de acceso a red) no específicamente contempladas en este documento.

2.2 CASOS DE USO

9. Para esta familia de productos tan sólo se contempla un caso de uso, en el que el servidor de autenticación hace de medio de identificación y autenticación para el acceso a los servicios de la organización. Existe la posibilidad de que la forma de autenticación varíe (multifactor, credenciales, biometría, etc.) pero la implementación y funcionalidad del producto sigue siendo idéntica.

2.2.1. CASO DE USO 1 – PASARELA DE IDENTIFICACIÓN Y AUTENTICACIÓN A LOS SERVICIOS

10. El servidor de autenticación se sitúa entre los servicios que ofrece una red y los usuarios de ésta, actuando como una frontera entre ambos. Una vez se identifica y autoriza un acceso, el servidor de autenticación se limita a mantener la sesión activa y delega el control de acceso a los servicios que se encuentran tras él.

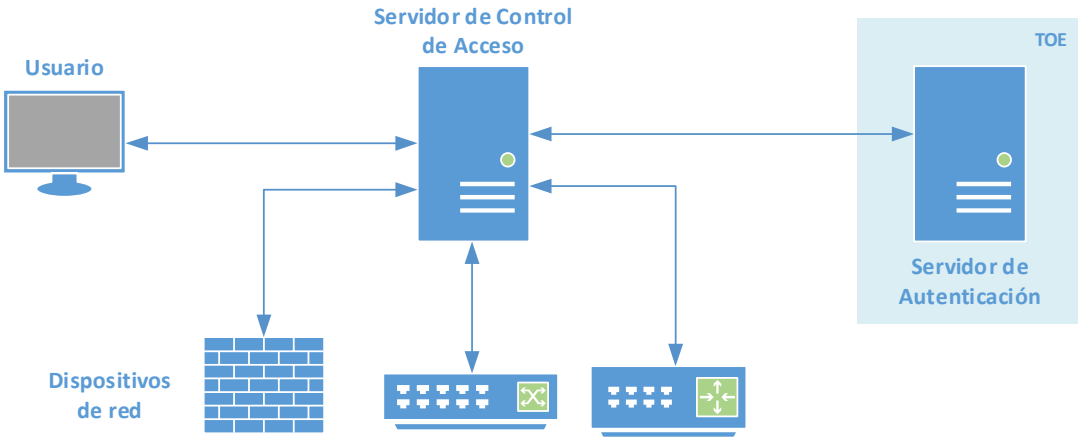

Figura 1 - Ejemplo de Caso de Uso 1: Pasarela de autenticación a los servicios

2.3 ENTORNO DE USO

11. 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 asegurar el entorno de comunicación.

12. 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 usuario administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la organización. Por ello, se asume que dicha persona estará altamente capacitada y carecerá de cualquier intención dañina al administrar estos dispositivos.
    - **Actualizaciones periódicas**. El producto será puesto al día conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Protección física.** El producto debe estar instalado en una localización física segura a la que solo pueden tener acceder los administradores autorizados.

- **Funcionalidad limitada:** El producto deberá utilizarse únicamente como servidor de autenticación y no proporcionar ninguna otra funcionalidad que no sea estrictamente necesaria para el desempeño de este cometido.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

13. Este tipo de productos se presenta en formato de *appliance* dedicado, que proporciona la funcionalidad que deberá tener la capacidad de soportar y manejar multitud de conexiones simultáneas, ya que actúa como punto intermedio entre los usuarios y los servicios.
14. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, éstas quedan fuera del alcance analizado, y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

15. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
16. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad independientes de la implantación.
17. Los productos dentro de esta familia deberán cumplir con los RFS reflejados en el apartado 4 y con los SFR (*Security Functional Requirements*) que se especifican en los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria*:

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Device[1] (o una actualizacion de este)	1.0	27/02/2015	CCDB
Extended Package for Authentication Servers.[2]	1.0	07/08/2015	NIAP

Tabla 1. Perfiles de protección

18. En caso de que el producto no esté certificado contra los perfiles indicados, la declaración de seguridad deberá contener al menos los SFR de éstos con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

[1] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[2] https://www.niap-ccevs.org/pp/pp_ndcpp_app_authsvr_ep_v1.0.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

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

- **AC. Administración:** Interfaces de gestión del producto e información transmitida a través de ellas, en ambos sentidos.
- **AC. Datos:** Datos de configuración del producto y de auditoría generados por este. Información que atraviesa el producto entre sus interfaces de red. Datos de identidades, atributos y credenciales de usuario gestionados y/o almacenados por el producto.
- **AC. Actualizaciones:** Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.
- **AC. Recursos:** Recursos a los que es posible acceder tras el proceso de autenticación.

3.2 AMENAZAS

20. 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:

3.2.1. COMUNICACIONES CON EL PRODUCTO

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso cómo administrador del producto haciéndose pasar por un administrador ante el producto, por el producto ante un administrador, reproduciendo una sesión de administración, realizando ataques del hombre en medio.
- **A.CIFRA Cifrado débil:** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Canales de comunicación no confiables:** Mala implementación de protocolos estándar o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo.
- **A.AUT Autenticación débil de los nodos:** Un producto puede utilizar protocolos de autenticación seguros que utilicen métodos de autenticación débiles (contraseñas no robustas, contraseñas cómo texto en claro, contraseñas precompartidas) para hacerse pasar por un usuario administrador u otro nodo para realizar un ataque de hombre en el medio.

3.2.2. ACTUALIZACIONES VÁLIDAS

- **A.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que debilite las funcionalidades de seguridad del producto.

3.2.3. AUDITORÍA

- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.

3.2.4. INFORMACIÓN Y CREDENCIALES

- **A.CRED Funcionalidades de seguridad comprometidas:** un atacante puede comprometer las credenciales o información del producto permitiendo un acceso continuado al producto y a su información sensible.
- **A.CON Contraseñas débiles:** Un atacante puede aprovecharse del uso contraseñas débiles para acceder con acceso privilegiado al dispositivo.

3.2.5. FALLO DEL PRODUCTO

- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

21. 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 PERFIL DE PROTECCIÓN

22. **REQ.1.** Los productos deberán estar certificados con los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Device[3] (o una actualizacion de este)	1.0	27/02/2015	CCDB
Extended Package for Authentication Servers	1.0	07/08/2015	NIAP

Tabla 2. Perfiles de protección

23. **REQ.2.** En caso de que no esté certificado contra los perfiles indicados, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de éstos con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

24. **REQ.3.** 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 Criptología de empleo en el ENS (Categoría ALTA).

[3] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf

5. ABREVIATURAS

CC	*Common Criteria*
CCDB	*Common Criteria Development Board*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y la Comunicación
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*

PUBLICACIONES DE DEFENSA

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