

Guía de Seguridad de las TIC CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo A.4: Servidores de Autenticación



Noviembre 2017

Edita:



© Centro Criptológico Nacional, 2017

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017

ISDEFE ha participado en el desarrollo del presente documento.

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO	4
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS	5
2.1 FUNCIONALIDAD	5
2.2 CASOS DE USO.....	5
2.2.1. CASO DE USO 1 – PASARELA DE IDENTIFICACIÓN Y AUTENTICACIÓN A LOS SERVICIOS	6
2.3 ENTORNO DE USO	6
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO.....	7
2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)	7
3. ANÁLISIS DE AMENAZAS	9
3.1 RECURSOS QUE ES NECESARIO PROTEGER.....	9
3.2 AMENAZAS	9
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS).....	11
4.1 PERFIL DE PROTECCIÓN	11
4.2 REQUISITOS CRIPTOGRÁFICOS.....	11
5. ABREVIATURAS	12

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). 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, biométrica, 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.

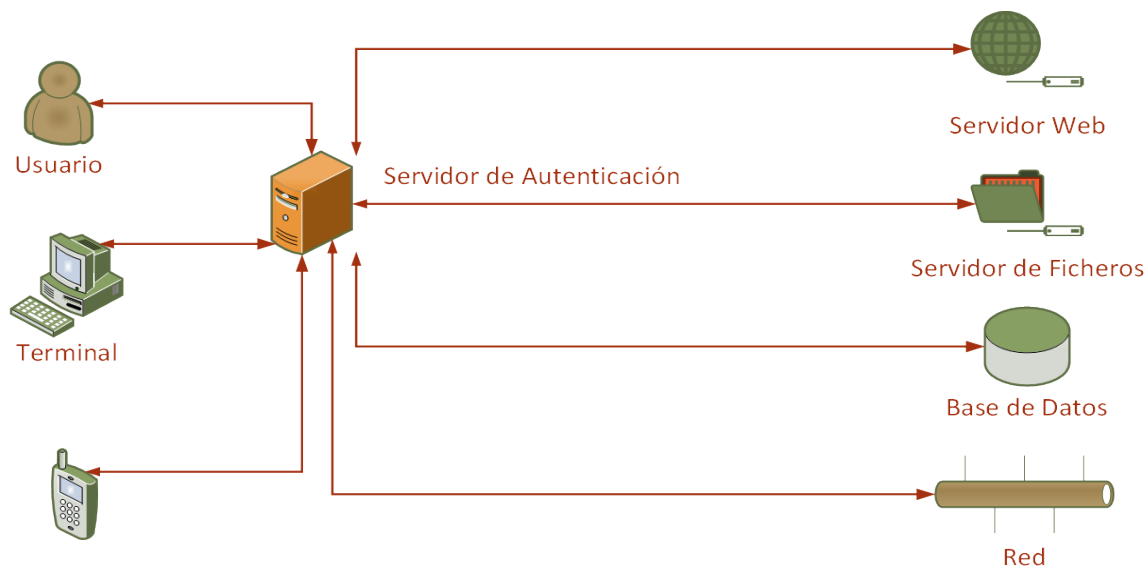


Figura 1 - Ejemplo de Caso de Uso 1: Pasarela de autenticación a los servicios

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.
- **Protección de las credenciales.** Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
- **Política de seguridad de la información.** Una política de seguridad deberá recoger el conjunto de principios, organización y procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

13. Este tipo de productos se presenta en formato de paquete software, generalmente instalado sobre un servidor hardware dedicado a proporcionar esta 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
<i>Collaborative Protection Profile for Network Devices.</i> ¹	1.0	27/02/2015	CCDB
<i>Extended Package for Authentication Servers.</i> 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**.

¹https://www.commoncriteriaportal.org/files/ppfiles/PPP_ND_V1.0.pdf

²https://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:
- Credenciales de usuarios y de administrador, tanto si se encuentran almacenadas en el propio servidor como si se transmiten a través de la red.
 - Servicios a los que es posible acceder tras el proceso de autenticación.
 - Información sensible que pueda almacenar el producto en su configuración o en el dispositivo hardware donde haya sido desplegado.
 - Interfaces de gestión del producto e información transmitida a través de ellas, en ambos sentidos.
 - Datos de configuración del producto y de auditoría generados por éste.
 - Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

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:
- **Acceso no autorizado:** Un atacante consigue acceder a información, intercambiada a través del producto, así como generada o almacenada en él, para la que no estaba autorizado (p.ej.: información almacenada en memoria) o bien consigue que el producto le proporcione acceso a servicios autenticados para los que no tiene la debida autorización.
 - **Cifrado débil:** Utilización en el producto de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
 - **Utilización de algoritmos de autenticación de usuarios débiles:** un atacante podría aprovechar que el producto utiliza métodos de autenticación débiles (contraseñas débiles o transportadas en claro), y que esto le permita suplantar esa identidad e introducirse en la red.
 - **Uso de canales de comunicación inseguros:** 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 producto.
 - **Compromiso o fallo de la funcionalidad de seguridad del producto:** Un atacante o un fallo en la herramienta compromete la funcionalidad de seguridad, permitiendo modificarla o desactivarla de manera no conforme a

las políticas de seguridad (p.ej.: instalación de actualizaciones maliciosas o administración no autorizada de la herramienta).

- **Actividad no auditada:** un agente de amenaza podrá intentar acceder, cambiar y/o modificar la funcionalidad de seguridad del dispositivo sin que el administrador lo detecte.
- **Suplantación de identidad:** un agente de amenaza podrá suplantar al servidor de autenticación frente al servidor de control de acceso o viceversa y conseguir que el producto opere de una manera insegura o extraer datos de seguridad relevantes del producto o de su entorno operacional.
- **Usuarios inválidos:** un agente de amenaza podría suministrar credenciales incorrectas o solicitudes de autenticación inválidas que sean aprobadas o ignoradas por el producto causando un acceso no autorizado a recursos protegidos del su entorno operacional.

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 Devices.	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).

5. ABREVIATURAS

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