Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC
Anexo A.4M: 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 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
2022.03.21 15:58:57 +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 de **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 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 **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 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 contempladas específicamente 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 la misma.

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 esta, 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.

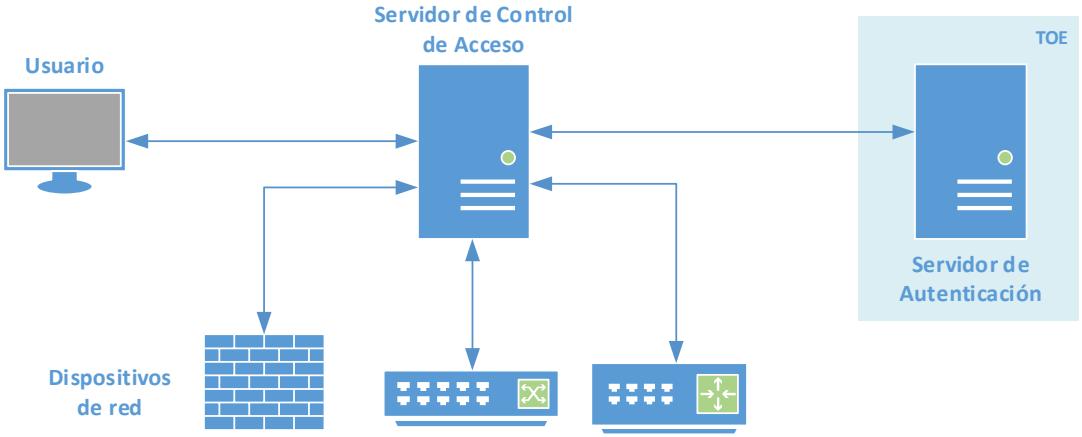

Figura 1 - Ejemplo de Caso de Uso 1: Pasarela de autenticación a los servicios

11. El servidor de control de acceso es opcional y su funcionalidad podría ser implementada por el servidor de autenticación. En cualquier caso, dicha funcionalidad deberá ser cualificada de forma independiente (ver *Anexo A1 Dispositivos de Control de Acceso a red*).

2.3 ENTORNO DE USO

12. 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.

13. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones:

    - **Protección física:** El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
    - **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.
- **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

14. 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.
15. 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

16. 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

17. 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

18. 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)

19. 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

20. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles (A.NOAUT).
21. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades: (A.NOAUT).
    - Administración del producto de forma local y remota.
    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
    - Configuración del secreto compartido RADIUS.
    - Otros parámetros de configuración del producto.
22. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas (ADM.2) (A.NOAUT).

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

23. **IAU.1** El producto debe de identificar y autenticar a cada usuario antes de permitir acciones que modifiquen la configuración del producto (A.NOAUT).
24. **IAU.2** El producto debe implementar mecanismos que impidan ataques de autenticación por fuerza bruta. (A.CON).
25. **IAU.3** El producto debe proteger contra lectura y modificación no autorizadas las credenciales de autenticación (A.CRED).
26. **IAU.4** El producto debe disponer de la capacidad de gestión de las contraseñas (A.CON, A.AUT):
    a) La contraseña debe de 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 [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]
27. **IAU.5** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad (A.NOAUT).

4.3 CANALES DE COMUNICACIÓN CONFIABLES

28. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo a lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.) (A.NOAUT, A.CIFRA, A.AUT).
29. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas. (A.COM).
30. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos (A.COM, A.AUT).

4.4 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

31. **ACT.1** El producto debe ofrecer la posibilidad de consultar la versión actual del software (A.ACT).
32. **ACT.2** El producto debe ofrecer mecanismos (conforme a la criptografía de empleo en el ENS) a través de hashes o firma digital para autenticar las actualizaciones de software antes de instalarlas (A.ACT).
33. **ACT.3.** La actualización del software se permitirá únicamente a usuarios con rol de administrador (A.ACT).
34. **ACT.4** El producto debe ofrecer la posibilidad de iniciar actualizaciones de forma manual y de comprobar si existen nuevas actualizaciones disponibles (A.ACT).

4.5 AUDITORÍA

35. **AUD.1** El producto debe generar información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos (A.AUD):
    a) *Login* y *logout* de usuarios registrados.
    b) Cambio en las credenciales de usuarios
    c) Cambios en la configuración del producto.
    d) Eventos relativos a la funcionalidad del producto.
    e) Generación, importación, cambio o eliminación de claves criptográficas.
36. **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 (si aplica) (A.AUD).
37. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: usuarios autorizados.
    b) Modificación: ningún usuario.

c) Borrado: administradores.

38. **AUD.4** El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa (A.AUD).
39. **AUD.5** El producto debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno (A.AUD).

4.6 PROTECCIÓN CONTRA FALLOS

40. **PRO.1** El producto deberá ser capaz de realizar un *test* (durante el arranque o encendido del producto, periódicamente durante la operación normal del producto y a petición de un usuario autorizado) para demostrar el funcionamiento correcto del producto determinado previamente (A.FUN).

4.7 REQUISITOS CRIPTOGRÁFICOS

41. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría MEDIA del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
42. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.8 REQUISITOS SERVIDOR DE AUTENTICACIÓN

43. **SRVAUT.1** El producto deberá implementar los protocolos RADIUS (RFC 2865, RFC 2869) con EAP-TLS (RFC 5216) para poder gestionar solicitudes de autenticación de otro componente del entorno (Servidor de acceso a red).
44. **SRVAUT.2** El producto deberá verificar la corrección e integridad de los paquetes en los que se incluyen las solicitudes de autenticación de los usuarios o entidades finales. Para ello deberá implementar el protocolo RADIUS (RFC 2865, RFC 2869).
45. **SRVAUT.3** El producto deberá de autenticar identidades basándose en los credenciales que recibe. El producto podrá tomar diferentes resultados de autenticación basándose en información contextual cómo la fecha y hora, el tipo de credencial utilizado u otro atributos asignados.

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
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