GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo A.3: Dispositivos Single Sign-On

Noviembre 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.11.27 11:09:49 +01'00'

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017
ISDEFE ha participado en el desarrollo del presente documento y sus anexos.

ÍNDICE

1. INTRODUCCIÓN 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 DISPOSITIVO EN ALCANCE 7
2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA) 7
3. ANÁLISIS DE AMENAZAS 9
3.1 RECURSOS A PROTEGER 9
3.2 AMENAZAS 9
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) 11
4.1 PERFIL DE PROTECCIÓN 11
4.2 REQUISITOS CRIPTOGRÁFICOS 11
4.3 PROTECCIÓN DE LA COMUNICACIONES 11
5. ABREVIATURAS 12

1. INTRODUCCIÓN

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia de **Dispositivos *Single Sign-On*** 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 *Single Sign-On*** 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 habilitar el acceso a varios sistemas dentro de una organización solicitando una única vez al usuario sus credenciales de Identificación, es decir, no es necesario repetir el proceso de Identificación para cada servicio, sino que basta con tan sólo un acceso/cuenta.

7. Para ello proporcionan las siguientes funciones básicas de seguridad:

   - **Identificación y Autenticación de usuarios**. Permite 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, proporcionando adicionalmente mayor transparencia al usuario en el proceso de Identificación a los servicios o sistemas a los que el producto le habilite el acceso, en función de sus permisos.

   - **Autenticación multifactor**. Es posible implementar conjuntamente diferentes mecanismos de autenticación para confirmar con mayor fiabilidad la identidad de un usuario, mediante la utilización de una combinación de dos o más componentes diferentes (p.ej. contraseña conocida por el usuario y código de seguridad enviado a un dispositivo móvil que posee el usuario).

   - **Reducción de accesos con credenciales**. Los usuarios pueden moverse entre servicios de forma segura e ininterrumpida sin especificar sus credenciales cada vez. Esta situación provoca que un atacante que se encuentre monitorizando la red tenga muchas menos posibilidades de interceptar tráfico que transporte información sensible relacionada con la identificación y autenticación de los usuarios.

   - **Ruptura del protocolo de autenticación.** Todos los procesos de autenticación para todos los servicios utilizados en la organización pasan antes por el servidor *single sign-on*, el cual 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. En el caso de los productos *Single Sign-On* tan sólo se contempla un caso de uso haciendo 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 (credenciales, biometría, multifactor, etc.) pero la implementación y funcionalidad del producto *Single Sign-On* sería semejante.

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

10. El dispositivo *Single Sign-On* se establece por delante de los servicios de la organización actuando como un puente de conexión hacia los mismos por el que todos los usuarios de los servicios deben pasar para poder acceder a su uso. Una vez el usuario logra identificarse y autenticarse correctamente, el dispositivo *Single Sign-On* establece la conexión con el servicio que desee el usuario autenticándole en él de manera transparente, conforme a los permisos asignados en el producto, o también en algunos casos establece la conexión con un dispositivo de control de acceso que es el encargado final de establecer las conexiones con los servicios o recursos de dicho usuario.

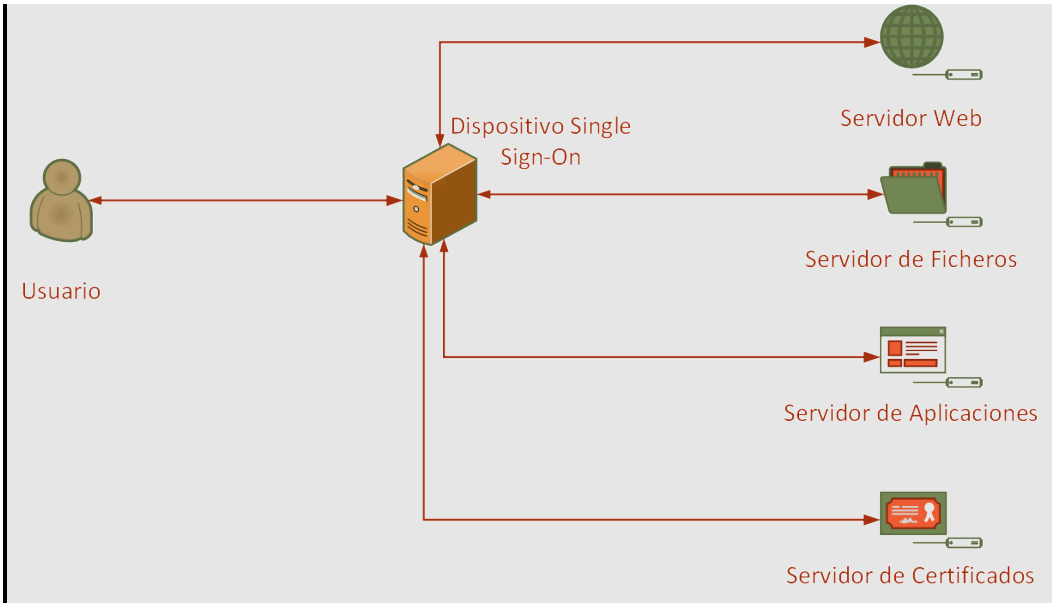

Figura 1 Ejemplo de Caso de Uso 1: Pasarela de identificación y autenticación a los servicios

2.3 ENTORNO DE USO

11. Por lo general estas herramientas se encuentran en grandes o medianas empresas, así como en redes del sector público como parte de una arquitectura de defensa en profundidad, con la finalidad de homogeneizar y reforzar el control de los accesos a múltiples servicios y sistemas de diferente naturaleza conforme a una política de control de accesos organizativa haciendo al mismo tiempo el proceso más transparente para el usuario.

12. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración 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 empresa/administración. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención dañina.

- **Actualizaciones periódicas**: El producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Protección de las comunicaciones**: Deberán habilitarse los mecanismos necesarios que permitan una comunicación segura entre los productos y las redes bajo control de la organización a las que estos se conecten (p.ej.: terminadores VPN[1]/SSH[2], puntos de acceso WLAN[3] seguros, etc.).
- **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 DISPOSITIVO EN ALCANCE

13. Este tipo de productos se presentan en formato de paquete software, generalmente instalado sobre equipamiento hardware en forma de servidor dedicado a proporcionar esta funcionalidad, debiendo tener la capacidad de soportar y manejar multitud de conexiones simultáneas ya que actúan como punto intermedio entre los usuarios y los servicios.
14. El presente documento describe los RFS para dictaminar un dispositivo *Single Sign-On* que se despliega como punto único de identificación y autenticación para unos servicios determinados de una organización. En caso de que el producto pueda ofrecer funcionalidades adicionales a las definidas en la sección2.1, éstas quedan fuera del alcance analizado, debiendo 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, tanto funcionales como de evaluación, independientes de la implantación.

[1] *Virtual Private Network*Red Privada Virtual
[2] *Secure Shell*.Interprete de órdenes seguro
[3] *Wireless Local Area Network.* Red de Área local inalámbrica

17. Los productos dentro de esta familia deberán cumplir con los requisitos Fundamentales de Seguridad reflejados en el apartado 4 y con los SFR (*Security Functional Requirements*) que se especifica en el siguiente perfil de protección certificado de acuerdo a la norma *Common Criteria*:

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Standard Protection Profile for Enterprise Security Management - Identity and Credential Management.[4]	2.1	21/11/2013	NIAP

Tabla 1. Perfiles de protección

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

[4] https://www.commoncriteriaportal.org/files/ppfiles/pp_esm_icm_v2.1.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS A PROTEGER

19. Los recursos a proteger mediante el uso de estos productos, así como para su correcto funcionamiento, incluyen:

    - Credenciales de los usuarios y los servicios a los que es posible acceder tanto estando almacenadas en los mismos como cuando se transmiten como tráfico de red.
    - Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
    - Información sensible que pueda almacenar el producto en su configuración o en el dispositivo hardware donde haya sido desplegado.
    - Datos de configuración del producto y de auditoría generados por éste.
    - Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

20. Las principales amenazas deliberadas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos conforme a la sección 2.2, serían:

    - **Divulgación de información no autorizada:** Un atacante consigue recopilar información no autorizada del producto (p.ej. servicios de la organización, credenciales, etc.).
    - **Escucha de red:** Un atacante se coloca en una conexión inalámbrica o en otro lugar de la infraestructura de red. El atacante puede supervisar y obtener acceso a la comunicación y/o los datos intercambiados (p.ej. credenciales de usuarios) entre el producto y otros puntos finales de la red.
    - **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 memoria).
    - **Cifrado débil**: Utilización en el producto de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
    - **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 de la funcionalidad 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).

21. Un atacante que quisiera comprometer estos productos, atendiendo al entorno de uso en el que se concibe su implementación conforme a la sección 2.3, requeriría:

    - Una cantidad arbitraria de tiempo para analizar los flujos de información intercambiados a través del producto.
    - Acceso ya sea a ejemplar(es) del producto donde llevar a cabo pruebas/intentos de ataque, o al propio producto una vez instalado.
    - Equipamiento comercial/abierto y conocimiento de su uso (p.ej.: herramientas de análisis de red, de explotación de vulnerabilidades, etc.).
    - Conocimiento sobre técnicas criptográficas y de criptoanálisis que permitan descifrar la información que utiliza y pasa por el producto o descifrar y/o averiguar credenciales de los usuarios para poder acceder a los servicios que se quieren proteger.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

22. 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

23. **REQ.1.** Los productos deberán estar certificados con el siguiente perfil de protección certificado de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Standard Protection Profile for Enterprise Security Management - Identity and Credential Management.[5]	2.1	21/11/2013	NIAP

Tabla 2. Perfiles de protección

24. **REQ.2.** En caso de que el producto implemente su propia funcionalidad criptográfica, deberá cumplir con los requisitos marcados apéndice D.1 que contiene el perfil de protección mencionado en la tabla 2.

25. **REQ.3.** En caso de que no esté certificado contra el perfil indicado, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

26. **REQ.4.** 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).

4.3 PROTECCIÓN DE LA COMUNICACIONES

27. **REQ.5.** El producto cifrará toda transmisión de datos sensibles, tales como las credenciales de usuario, con al menos uno de los siguientes protocolos: HTTPS[6], TLS[7] 1.2 o IPSEC[8].

[5] https://www.commoncriteriaportal.org/files/ppfiles/pp_esm_icm_v2.1.pdf
[6] *Hypertext Transfer Protocol Secure*. Protocolo Seguro de Transferencia de Hipertexto

5. ABREVIATURAS

CC	*Common Criteria*
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
EAL	*Evaluation Assurance Level*
HTTPS	*Hypertext Transfer Protocol Secure*
IPSEC	*Internet Protocol SECurity*
NIAP	*National Information Assurance Partnership*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*
SSH	*Secure Shell*
TLS	*Transport Layer Security*
VPN	*Virtual Private Network*
WLAN	*Wireless Local Area Network*

[7] *Transport Layer Security*. Seguridad en la capa de transporte
[8] *Internet Protocol Security*. Protocolo seguro de Internet