GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo D.9: Herramientas para comunicaciones móviles seguras

Julio 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

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
2018.07.10 12:17:00 +02'00'

NIPO: 785-18-034-0.
Publicación incluida en el programa editorial del suprimido Ministerio de la Presidencia y para la Administraciones Territoriales (de acuerdo con la reestructuración ministerial establecida por Real Decreto 355/2018, de 6 de junio).

Fecha de Edición: julio 2018
Isdefe ha participado en el desarrollo del presente documento y sus anexos.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Herramientas para comunicaciones móviles seguras** 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 **Herramientas para comunicaciones móviles seguras** 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 permiten establecer comunicaciones de forma segura cómo voz y video sobre IP (VVoIP) o mensajería instantánea.

2.2 CASOS DE USO

2.2.1. CASO DE USO 1 – VOZ Y VIDEO SOBRE IP

7. La herramienta para comunicaciones móviles seguras tendrá la funcionalidad de trasmitir voz y video sobre IP a través de túneles seguros con servidores remotos.

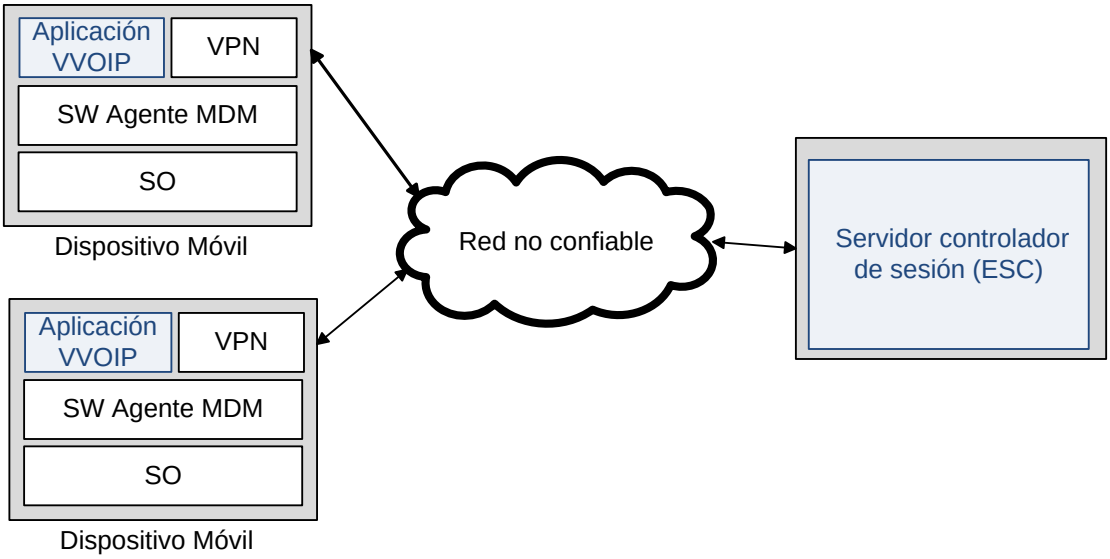

Figura 1 Ejemplo de Caso de Uso 1: Comunicación de Video y Voz sobre IP

8. Una aplicación VVOIP ejecutada sobre un dispositivo móvil establece un túnel seguro con un servidor controlador de sesión (ESC) o con otra aplicación VVOIP ejecutada sobre un dispositivo móvil.

2.3 ENTORNO DE USO

9. Estas herramientas pueden encontrarse tanto en empresas de diferente naturaleza, así como en redes de las Administraciones Públicas como parte de una arquitectura de defensa en profundidad que busca asegurar el entorno de comunicación para evitar escuchas o exfiltraciones de información, existiendo medidas complementarias en diferentes capas de protección.

10. 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:

- **Entorno de ejecución seguro:** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
- **Administración confiable**: El usuario 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 altamente capacitada y carecerá de cualquier intención maliciosa al administrar los dispositivos pasarelas. El producto no será capaz de defenderse contra un usuario administrador con malas intenciones.
- **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/, puntos de acceso WLAN 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 definidos por la 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

11. Este tipo de productos se presentan en formato de paquete **Software** que se instala sobre un entorno de ejecución seguro.
12. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 ALINEAMIENTO CON COMMON CRITERIA

13. 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).
14. 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. En el apartado 4 se indican los perfiles de protección aplicables a cada caso.

3. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

15. 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.

3.1 REQUISITOS CRIPTOGRÁFICOS

16. **REQ. 1** 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).

3.2 VOZ Y VIDEO SOBRE IP

17. **REQ. 2** El producto debe estar certificado contra los siguientes perfiles de protección:

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Extended Package for Voice and Video over IP (VVoIP)[1]	1.0	28/09/2016	NIAP
Protection Profile for Application Software.[2]	1.2	25/04/2016	NIAP

Tabla 1. Perfiles de protección VVoIP

18. **REQ. 3** El producto debe poder ejecutarse sobre un dispositivo móvil cualificado, es decir, que esté cualificado en la familia de dispositivos móviles.
19. **REQ. 4** El producto deberá estar certificado o formar parte de una arquitectura con un producto certificado contra uno de los siguientes perfiles de protección:

[1] https://www.niap-ccevs.og/pp/ep_vvoip_v1.0.pdf
[2] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Extended Package for Enterprise Session Controller (ESC)[3]	1.0	25/10/2016	NIAP
Collaborative Protection Profile for Network Devices.[4]	1.0	27/02/2015	*CCDB*
Extended Package for SIP Server[5]	2.0	01/12/2015	NIAP
Collaborative Protection Profile for Network Devices.[4]	1.0	27/02/2015	CCDB

Tabla 2. Perfiles de protección servidor

[3] https://www.niap-ccevs.og/pp/ep_esc_v1.0.pdf
[4] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[5] https://www.commoncriteriaportal.org/files/ppfiles/pp_ndcpp_sip_ep_v2.0.pdf