centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo D.9A: Herramientas de voz y vídeo por IP (VVoIP)

Septiembre de 2023

MINISTERIO DE DEFENSA

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

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
2023.10.03 16:51:20 +02'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

NIPO: 083-23-071-5
Fecha de Edición: septiembre de 2023

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Herramientas de voz y vídeo por IP (VVoIP)** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos y Servicios STIC (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 para 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 **Herramientas de voz y Vídeo por IP (VVoIP)** 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. Se considera Herramienta de comunicaciones VoIP/VVoIP a todo producto que permita a dos o más dispositivos, establecer comunicaciones seguras de Voz (VoIP) o Voz y Vídeo (VVoIP) a través de conexiones de datos basadas en redes IP.

7. Los componentes que integran este tipo de productos son de dos tipos:

    - **VVoIP endpoint,** que puede consistir en un dispositivo hardware dedicado con capacidad VVoIP, o puede tratarse de una aplicación VVoIP que se ejecuta en un dispositivo hardware de propósito general, como un smartphone, tablet o PC.
    - **Servidor de control de llamadas (SCL),** que puede consistir en un *appliance* dedicado con un firmware no modificable, o puede tratarse de un servidor de propósito general que proporciona la funcionalidad de control de llamadas.

8. El VVoIP endpoint puede actuar como un cliente que se comunica con un servidor de control de llamadas, o puede actuar como su propio servidor de control de llamadas cuando se implementa una arquitectura extremo a extremo (P2P). El VVoIP endpoint debe ser capaz de: descargar de forma segura sus ficheros de actualización de firmware/software desde un servidor interno de la organización (el SCL u otro), establecer una comunicación segura para el control de llamada con el servidor de control de llamadas, y transmitir de forma segura voz/vídeo a otros dispositivos.

9. Para la viabilidad de las comunicaciones VVoIP, estos productos deben proporcionar dos funciones básicas:

    - Control de llamadas (*Call Control Processing*): señalización para el establecimiento, procesamiento y finalización de las llamadas VVoIP.
    - Transmisión de los datos de voz/vídeo (*Streaming media*).

10. Generalmente la función de control de llamadas la proporciona un Servidor de control de llamadas (SCL), comúnmente llamado ESC (*Entrerprise Session Controller*) o *Call-Processing Server*.

    La función principal del SCL es el establecimiento, procesamiento y finalización de las llamadas VVoIP. Para ello utiliza protocolos de procesado de llamadas (*Call processing protocols*), como H.323 o SIP. El protocolo más extendido es SIP (*Session Initiation Protocol*) por lo que, en muchos casos, este servidor es también referido como ***SIP Server***. Es también misión del SCL proteger esta señalización con un protocolo seguro que proporcione autenticación y cifrado, por ejemplo, TLS (*Transport Layer Security*).

    Dentro de las capacidades de control de llamadas deberá llevarse a cabo el registro de los detalles de cada llamada (CDRs, *Call Details Records*).

El SCL también se comunica con otra serie de servicios que proporcionan otros componentes de la infraestructura de la organización, como servicios de buzón de voz, conferencia, NTP (*Network Time Protocol*), DNS (*Domain Name System*) y en muchos casos, almacena las actualizaciones de software/ firmware para su distribución a los VVoIP endpoints.

11. Respecto a la transmisión de voz/vídeo (*streaming media*), generalmente se lleva a cabo directamente entre los **VVoIP endpoints**, aunque dependiendo de la arquitectura del producto, el SCL también puede actuar como intermediario redireccionando esta comunicación entre los VVoIP endpoints.

    Es también misión del VVoIP endpoint, proteger estos datos con un protocolo seguro que proporcione autenticación y cifrado, por ejemplo, SRTP (*Secure Real-time Transport Protocol*).

2.2 CASOS DE USO

12. Dada la naturaleza y el objetivo de este tipo de productos, se contemplan dos casos de uso para esta familia, tal y como se indica a continuación.

2.2.1. CASO DE USO 1 – ARQUITECTURA CLIENTE-SERVIDOR SCL

13. El VVoIP endpoint es un cliente que interactúa con un Servidor de control de llamadas (SCL), encargado de establecer, procesar y finalizar las llamadas entre los VVoIP endpoints utilizando para ello un protocolo de control de llamadas (SIP o H.323).

14. En este caso de uso, es el servidor de control de llamadas (SCL) el encargado de las funciones de auditoría del sistema, incluido el registro de los detalles de las llamadas o CDRs (*Call Details Records*).

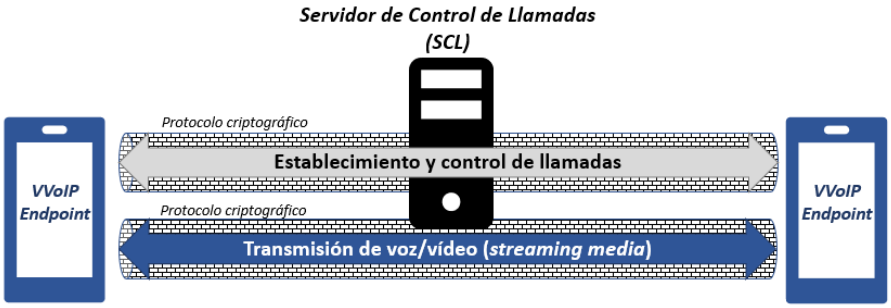

Figura 1 – Arquitectura cliente-servidor.

2.2.2. CASO DE USO 2 – ARQUITECTURA P2P

15. La arquitectura del producto es extremo a extremo (P2P, peer-to-peer). Cada VVoIP endpoint interactúa directamente con otros VVoIP endpoints sin necesidad de utilizar ningún Servidor de control de llamadas de intermediario, ya que esta función la proporciona el propio VVoIP endpoint.

16. En este caso de uso, es el VVoIP endpoint el encargado de las funciones de auditoría del sistema, incluido el registro de los detalles de las llamadas o CDRs (*Call Details Records*).

Figura 2 – Arquitectura P2P.

2.3 ENTORNO DE USO

17. Para la utilización en condiciones óptimas de seguridad de la Herramienta de comunicaciones VoIP/VVoIP, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

- **Protección física**. El producto debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.
- **Administración confiable:** Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
- **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de control de llamadas y transmisión de voz/vídeo, como función principal y no debe proporcionar ninguna otra funcionalidad o servicio.
- **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.

- **Plataforma confiable.** En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

18. Este tipo de productos se presentan:

    a) El VVoIP endpoint puede presentarse como un dispositivo hardware dedicado con capacidad VVoIP, o como una aplicación VVoIP que se ejecuta en un dispositivo hardware de propósito general.

    b) El Servidor de control de llamadas (SCL) puede presentarse como un dispositivo dedicado con un firmware no modificable, o como un servidor de propósito general que proporciona la funcionalidad de control de llamadas.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

19. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TIC (Tecnologías de la Información y de las Comunicaciones).

20. 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.

21. Los productos dentro de esta familia deberán estar certificados de acuerdo a la norma *Common Criteria.* Dicha certificación deberá evidenciar el problema de seguridad definido en el presente documento e incluir los requisitos fundamentales de seguridad recogidos en el apartado 4.

22. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:

    - **El determinado por el perfil de protección** para aquellos SFR incluidos en los perfiles exigidos cuando los productos se encuentren certificados contra alguno de los perfiles anteriormente descritos.

    - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.

23. En caso de que alguno de los requisitos indicados en el apartado 4 no se encuentre recogido en la declaración de seguridad del producto, pero este sí implemente esa función de seguridad, se podrá llevar a cabo una evaluación **STIC complementaria**, cuyo objetivo será verificar el cumplimiento de esos requisitos.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

24. La convención utilizada en las descripciones es la siguiente:

    - Selección**:** se deberá seleccionar al menos una opción de las indicadas y se incluirá en la declaración de seguridad. Ejemplo:

      AC.PSC. [**selección**: credenciales; claves] que deben ser protegidos en Confidencialidad e Integridad.

      DS: **AC.PSC**. credenciales que deben ser protegidos en Confidencialidad e Integridad.

    - Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

      AC.PSS. Datos de configuración, registros de auditoría y [**asignación**: listado de datos definidos por el fabricante] que deben ser protegidos en Integridad.

      DS: **AC.PSS**. Datos de configuración, registros de auditoría que deben ser protegidos en Integridad.

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

    - **AC.Administración**. Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos, que debe ser protegida en Confidencialidad, Trazabilidad, Autenticidad e Integridad.
    - **AC.PSS**. Datos de configuración, registros de auditoría y [**asignación**: *listado de datos definidos por el fabricante*] que deben ser protegidos en Integridad.
    - **AC.PSC**. [**selección**: credenciales; claves; [**asignación**: *listado de datos definidos por el fabricante*] que deben ser protegidos en Confidencialidad e Integridad.
    - **AC.Actualizaciones**. Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.
    - **AC.Comunicaciones**. Comunicaciones del producto, establecidas entre sus propios componentes y con [**asignación**: *listado de entidades autorizadas*] que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.

3.2 AMENAZAS

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

    - **A.NOAUT Acceso no autorizado de administrador**: Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un

administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.

- **A.CRYPTO Mecanismos criptográficos débiles**: Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Protocolos de comunicación no autorizados**: Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto.
- **A.ACT Actualización maliciosa**: un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades del producto.
- **A.AUD Actividades no detectadas**: Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.
- **A.PSC Compromiso de parámetros de seguridad críticos**: Un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.
- **A.FUN Fallo de las funcionalidades de seguridad**: Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **A.NOAUTUSR Acceso no autorizado de usuario**: Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CRE Compromiso de credenciales**: Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.
- **A.VVoIP Endpoints no autorizados**: Un atacante puede intentar registrar un VVoIP endpoint no autorizado, con el propósito de suplantar a un usuario legítimo y establecer conexiones no autorizadas con otros VVoIP endpoints o con llamadas activas.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

27. 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.

28. La convención utilizada en las descripciones de los RFS es la siguiente:

    - Selección**:** se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

      RFS: Administración del producto [**selección***: local; remota*]

      DS: Administración del producto local y remota

    - Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

      RFS: El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación:** otros usuarios del producto] antes de otorgar acceso.

      DS: El TOE deberá identificar y autenticar a cada usuario administrador, auditor y usuario avanzado antes de otorgar acceso.

29. El apartado 4.1 indica los requisitos que debe cumplir el **VVoIP endpoint**. El apartado 4.2 indica los requisitos que debe cumplir el **servidor de control de llamadas** para los casos de arquitecturas cliente-servidor (caso de uso 1).

4.1 VVOIP ENDPOINT

4.1.1. PERFIL DE PROTECCIÓN

30. **REQ. 1**. El producto deberá estar certificado con el siguiente perfil de protección de acuerdo a la norma Common Criteria:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
PP-Module for Voice and Video over IP (VVoIP)	*1.0*	*28/10/2020*	*NIAP*

a) En caso de que el producto sea un dispositivo de red, de forma adicional deberá estar certificado con alguno de los siguientes perfiles de protección de acuerdo a la norma Common Criteria:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
collaborative Protection Profile for Network Devices	2.2e	27/03/2020	CCDB
collaborative Protection Profile for Network Devices	*2.1*	*11/03/2019*	*CCDB*
collaborative Protection Profile for Network Devices	*2.0 + Errata 20180314*	14/03/2018	*CCDB*

b) En caso de que el producto sea una aplicación software, de forma adicional deberá estar certificado con los siguientes perfiles de protección de acuerdo a la norma Common Criteria:

i. Perfil de Protección de Aplicaciones Software:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software	*1.4*	*18/10/2021*	*NIAP*
Protection Profile for Application Software	*1.3*	*01/03/2019*	*NIAP*

ii. Paquete Funcional para TLS:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Functional Package for TLS	*1.1*	*01/03/2019*	*NIAP*
Functional Package for TLS	*2.0*	*19/12/2022*	*NIAP*

31. **REQ. 2**. En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de los perfiles indicados en el REQ.1, con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2** o superior.

4.1.2. REQUISITOS CRIPTOGRÁFICOS

32. **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).

4.2 SERVIDOR DE CONTROL DE LLAMADAS (SCL)

4.2.1. PERFIL DE PROTECCIÓN

33. **REQ. 4**. El producto deberá estar certificado con el siguiente perfil de protección de acuerdo a la norma Common Criteria:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
PP-Module for Enterprise Session Controller (ESC)	*1.0*	*20/11/2020*	*NIAP*

De forma adicional, el producto deberá estar certificado también con alguno de los siguientes perfiles de protección de acuerdo a la norma Common Criteria:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
collaborative Protection Profile for Network Devices	*2.2e*	*27/03/2020*	*CCDB*
collaborative Protection Profile for Network Devices	*2.1*	*11/03/2019*	*CCDB*
collaborative Protection Profile for Network Devices	*2.0 + Errata 20180314*	14/03/2018	*CCDB*

34. **REQ. 5**. En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de los perfiles indicados en el REQ.1, con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2** o superior.

4.2.2. REQUISITOS CRIPTOGRÁFICOS

REQ. 6. 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 NOTAS DE APLICACIÓN

35. En el Caso de Uso 1 – Arquitectura cliente-servidor SCL, los requisitos deberán aplicarse tanto al Cliente como al servidor de control de llamadas (SCL). Por tanto, el alcance de la certificación deberá incluir ambos: el Cliente y el servidor de control de llamadas (SCL).

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
SCL	Servidor de Control de Llamadas
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
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