REF: 2014-17-INF-1476 v1	Creado: CERT10
Difusión: Expediente	Revisado: CALIDAD
Fecha: 01.07.2015	Aprobado: TECNICO

INFORME DE CERTIFICACIÓN

Expediente: 2014-17 Enigmedia App SDK v1.10.4

Datos del solicitante: B75058503 Enigmedia S.L.

Referencias:

[EXT-2448] Solicitud de Certificación

[EXT-2769] Informe Técnico de Evaluación

La documentación del producto referenciada en los documentos anteriores.

Informe de Certificación del producto Enigmedia App SDK, versión 1.10.4, según la solicitud de referencia [EXT-2448], de fecha 28/03/2014, evaluado por el laboratorio Epoche & Espri S.L.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación, con referencia [EXT-2769], recibido el pasado 16/01/2015.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

ÍNDICE

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto Enigmedia App SDK, versión 1.10.4.

El TOE es una SDK para dispositivos móviles orientada a las comunicaciones seguras de VoIP (Voz sobre IP) con audio/vídeo. Como tal, el TOE proporciona servicios a aplicaciones Android, de tal manera que dichas aplicaciones incluirán en su interior al TOE (entre ellas la aplicación Enigmedia App).

Fabricante: Enigmedia S.L.

Patrocinador: Enigmedia S.L.

Organismo de Certificación: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

Laboratorio de Evaluación: Epoche & Espri S.L.U.

Perfil de Protección: Ninguno.

Nivel de Evaluación: Common Criteria v3.1 R4. EAL1.

Fecha de término de la evaluación: 16/01/2015.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1 presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Epoche & Espri S.L.U. asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL1, definidas por los criterios de evaluación [CC_P3] y la metodología de evaluación [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Enigmedia App SDK, versión 1.10.4, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El TOE es una SDK para dispositivos móviles orientada a las comunicaciones seguras de VoIP (Voz sobre IP) con audio/vídeo. Como tal, el TOE proporciona servicios a aplicaciones Android, de tal manera que dichas aplicaciones incluirán en su interior al TOE (entre ellas la aplicación Enigmedia App).

Esta SDK consta de un conjunto de librerías software multiplataforma que implementan la siguiente funcionalidad de seguridad:

- Funcionalidad criptográfica asociada la gestión y cifrado de las comunicaciones VoIP haciendo uso del algoritmo KVC.
- Funcionalidad criptográfica asociada a la gestión y cifrado del fichero de configuración de cada instancia del TOE, haciendo uso del algoritmo AES-CBC con clave de 256 bits.
- Importación tanto de los datos para el fichero de configuración durante la primera fase de operación del TOE como de la clave KVC utilizada para cifrar cada comunicación VoIP.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- Mantenimiento interno del ID de usuario asociado al dispositivo donde el TOE opera.
- Mantenimiento de dos canales seguros de comunicación: uno con la centralita SIP (o servidor MediaProxy en su defecto) y otro con el servidor Web del Frontend.

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL1, según Common Criteria v3.1 R4.

Clases	**Componentes**
ADV Development	ADV_FSP.1 Basic functional specification
AGD Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definitions
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE Tests	ATE_IND.1 Independent testing - conformance
AVA Vulnerability Assessment	AVA_VAN.1 Vulnerability survey

REQUISITOS FUNCIONALES DE SEGURIDAD

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, según Common Criteria v3.1 R4.

Requisitos funcionales de seguridad del TOE	**Descripción**
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4/AES	Cryptographic key destruction/AES
FCS_CKM.4/KVC	Cryptographic key destruction/KVC

FCS_COP.1/AES	Cryptographic operation/AES
FCS_COP.1/KVC	Cryptographic operation/KVC
FDP_ITC.1	Import of user data without security attributes
FDP_ITC.2	Import of user data with security attributes
FIA_ATD.1	User attribute definition
FTP_ITC.1/SIP	Inter-TSF trusted channel/SIP
FTP_ITC.1/WEB	Inter-TSF trusted channel/WEB

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

IDENTIFICACIÓN

Producto: Enigmedia App SDK, versión 1.10.4.
Declaración de Seguridad: Declaración de Seguridad Enigmedia App SDK v1.2, Noviembre 2014.
Perfil de Protección: Ninguno.
Nivel de Evaluación: Common Criteria v3.1 R4. EAL1.

FUNCIONALIDAD DEL ENTORNO

Se relacionan, a continuación, los objetivos que se deben cubrir por el entorno de uso del TOE.

Objetivo entorno 01: OE.INSTALLATION

El entorno es el encargado de verificar la identidad del usuario a través de una confirmación con envío de SMS, generación de la configuración de la App en sus servidores e inserción de los datos del usuario final en el sistema (LDAP) una vez verificado.

Objetivo entorno 02: OE.SYNC

El entorno permite el uso de canales seguros entre la aplicación y los servidores, con los que sincronizar los datos de usuario final.

Objetivo entorno 03: OE.SIGNAL_ENCRYP

El entorno proporciona un servidor de señalización SIP, con capacidad para validar a los usuarios finales mediante certificados.

Objetivo entorno 04: OE.MEDIA_ENCRYP

Es el entorno el que genera las claves del algoritmo KVC que más tarde se van a usar para cifrar la voz y el vídeo y las distribuye a las dos partes que van a establecer una comunicación o llamada.

ARQUITECTURA

ARQUITECTURA LÓGICA

Desde el punto de vista del ámbito lógico del TOE, se cuentan con las siguientes características de seguridad:

Seguridad en las comunicaciones
Las comunicaciones de señalización (registro en el sistema, inicio de llamada, intercambio de claves, negociación de codecs) hacen uso de autenticación mutua a través de TLSv1.0. Se utiliza una cipherSuite Openssl High con certificados de 4096 bits y cifrados con 3DES mediante una passphrase de 40 bytes. Estos certificados son únicos por usuario final y son generados y cifrados en servidor haciendo uso de

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Email: organismo.certificacion@cni.es

una passphrase aleatoria. Una vez generados son enviados a la aplicación que integra al TOE durante el uso del asistente de configuración inicial a través de un canal TLSv1.0. De esta forma no sólo se cifra la comunicación sino que también se autoriza y autentica al usuario final, permitiendo tener en todo momento un control de los usuarios finales registrados, así como la caducidad y revocación de certificados.

Además de las comunicaciones de señalización, se llevan a cabo comunicaciones con un servidor web Apache desplegado en el Frontend. Las comunicaciones con este servidor se realizan a través de HTTPS.

Almacenamiento cifrado
El almacenamiento de la configuración, agenda e historial de llamadas se realiza mediante el cifrado de un fichero de configuración usando AES CBC de 256 bits. La clave AES de 256 bits utilizada para el cifrado y descifrado de dicho archivo es generada mediante key derivation a partir de un PIN que el usuario final de la aplicación que integra al TOE introduce durante la instalación.
El TOE ofrece facilidades de almacenamiento seguro de los mensajes, mediante SQLite y un cipher AES CBC de 256 bits cuya clave se genera aleatoriamente durante el proceso de instalación y se almacena en el fichero de configuración.

VoIP con algoritmo KVC
Las comunicaciones VoIP se cifran haciendo uso del algoritmo propietario KVC y con una autenticación y comprobación de integridad HMAC-SHA1 de 80 bits en cada paquete de datos enviado.

Importación segura de datos
Tanto la configuración de la aplicación una vez que un usuario final se ha dado de alta, como la clave del algoritmo KVC utilizada en cada comunicación VoIP son importadas de manera segura en el TOE, a través de los canales seguros de comunicación.
La generación de las claves del algoritmo KVC se realiza en servidor, usando para ello hardware de generación de entropía certificado como FIPS 140-2.

Gestión de la identidad del usuario
Una vez que el usuario final se ha dado de alta en los servidores, su identidad se almacena en el dispositivo desde el que se ha dado de alta, así como su configuración.

Borrado de seguridad
Las claves asociadas a los algoritmos criptográficos que implementa el TOE son borradas de memoria una vez utilizados.

ARQUITECTURA FÍSICA

El TOE es una SDK para dispositivos móviles que es utilizada por aplicaciones Android. Los usuarios del TOE son los desarrolladores que crearán GUIs que, al integrarlos con el TOE, darán como resultado dichas aplicaciones Android.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Por tanto, los componentes de que consta el TOE y que se hacen llegar a los usuarios son:

Elemento	Formato	Nota
TOE	Ficheros de código fuente C y JAVA	El TOE se proporciona al desarrollador a modo de conjunto de librerías
Especificación funcional del TOE	PDF y HTML	Está formada por los siguientes documentos: - Doxygen Enigmedia App SDK, v1.7 - libSRTP Overview and Reference Manual, v1.3 - Web Services Client Android, version 1.10.4

DOCUMENTOS

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

- Declaración de seguridad de Enigmedia App SDK 1.10.4, versión 1.2. Noviembre 2014.
- Manual Enigmedia App versión Android, versión 1.10.4, Noviembre 2014.

PRUEBAS DEL PRODUCTO

El evaluador ha seleccionado un subconjunto de pruebas y una estrategia apropiada para el TOE entregado por el fabricante. La documentación describe el comportamiento de las TSFIs y el evaluador ha aplicado esa información a la hora de desarrollar sus pruebas.
El principal objetivo de las pruebas realizadas por el evaluador ha sido comprobar el cumplimiento de los requisitos especificados en la declaración de seguridad [ST12] a través de las interfaces TSFIs.

CONFIGURACIÓN EVALUADA

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Así, para el funcionamiento del producto Enigmedia App SDK, versión 1.10.4 es necesario disponer de los siguientes componentes software:

Componentes locales

Se consideran componentes locales a aquellos que se ejecutan dentro del propio dispositivo móvil donde el TOE está instalado.

- Sistema Operativo: El TOE se ejecuta sobre Android versión 4.0 o superior (aunque existe una versión del TOE para iOS, la única versión evaluada es la

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Email: organismo.certificacion@cni.es

que se despliega en Android). La versión de Android debe ser oficial y no encontrarse rooteada o modificada para ejecutar acciones no permitidas por defecto.

- GUI: El TOE precisa para su operación (por parte de usuarios finales del dispositivo móvil) de un interfaz de usuario, el cual será el encargado de interaccionar con las funcionalidades que ofrece el TOE.

Componentes externos

Se consideran componentes externos a aquellas entidades (hardware o software) que ejecutan su funcionalidad fuera del propio dispositivo móvil donde el TOE está instalado.

Servidores del frontend:

- Centralita SIP: Es un servidor OpenSIPS 1.9.1.
- MediaProxy: Es un servidor OpenSIPS 1.9.1 con el módulo MediaProxy 2.6.1 activo.
- Servidor web: Es un servidor Apache 2.2.22.
- DNS público: Bind 9.8.4.

Servidores del backend:

- Servidor de aplicaciones: Tomcat 7.0.28.
- Servidor de usuarios: OpenLDAP 2.4.31.
- DNS privado: Bind 9.8.4.
- Servidor BBDD: PostgreSQL 9.1.14.

RESULTADOS DE LA EVALUACIÓN

El producto Enigmedia App SDK, versión 1.10.4 ha sido evaluado en base a la Declaración de Seguridad Enigmedia App SDK v1.2, Noviembre 2014.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1 presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Epoche & Espri S.L.U. asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL1, definidas por los criterios de evaluación [CC_P3] y la metodología de evaluación [CEM].

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

- Es especialmente trascendente hacer cumplir la premisa que se incluye en la declaración de seguridad [ST12], en la que se indica que el dispositivo Android donde el TOE se ejecute NO DEBE estar "rooteado", pues de lo contrario no se puede asegurar que las capacidades de seguridad del TOE se mantengan.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Email: organismo.certificacion@cni.es

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Enigmedia App SDK, versión 1.10.4, se propone la resolución estimatoria de la misma.

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

- [CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, Sept. 2012.
- [CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.
- [CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.
- [CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

DECLARACIÓN DE SEGURIDAD

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación: Declaración de Seguridad Enigmedia App SDK v1.2, Noviembre 2014.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es