REF: 2016-45-INF-2360 v1	Creado: CERT10
Difusión: Público	Revisado: CALIDAD
Fecha: 23.05.2018	Aprobado: TECNICO

INFORME DE CERTIFICACIÓN

Expediente: 2016-45 ISTRIA IS101 v1.01

Datos del solicitante: A-87050423 ISTRIA Soluciones de Criptografía

Referencias:

[EXT-3177] Solicitud de Certificación de ISTRIA IS101 v1.01

[EXT-3927] Informe Técnico de Evaluación de ISTRIA IS101 v1.01

La documentación del producto referenciada en los documentos anteriores.

Informe de Certificación del producto IS101 v1.01, según la solicitud de referencia [EXT-3177] recibida el 27/10/2016, evaluado por el laboratorio Epoche & Espri S.L.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación [EXT-3927], recibido el pasado 26/04/2018.

ÍNDICE

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto IS101 v1.01.

El IS101 es un dispositivo de altas prestaciones que integra una plataforma hardware segura con un FW/SW específico y permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada).

Fabricante: ISTRIA Soluciones de Criptografía.

Patrocinador: ISTRIA Soluciones de Criptografía.

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: CC v3.1 R4 – EAL4 + ALC_FLR.1.

Fecha de término de la evaluación: 26/04/2018.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 (aumentado con ALC_FLR.1) 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 EAL4 + ALC_FLR.1, definidas por Common Criteria v3.1 R4 y CEM v3.1 R4.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto IS101 v1.01, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El IS101 es un dispositivo de altas prestaciones que integra una plataforma hardware segura con un FW/SW específico y permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada).

Los principales servicios y características de seguridad ofrecidos por el

TOE incluyen:

- Control robusto del procesamiento y manejo del tráfico de datos de usuario, limitando el tráfico que está permitido que atraviese el equipo a aquellos flujos determinados por las políticas de seguridad IPsec configuradas en cada momento.
- Identificación y Autenticación de usuarios y establecimiento de canales seguros para aquellos usuarios conectados de forma remota.

- Control de acceso a las operaciones de administración, gestión y configuración mediante perfiles de usuario y esquemas de permisos.
- Protecciones físicas y lógicas (activas y pasivas).
- Almacenamiento seguro de ciertos datos sensibles en el supervisor de seguridad (necesarios para el arranque del equipo), permitiendo verificar su integridad en cada arranque, y chequeos periódicos (auto-tests) del estado de los sensores y mecanismos anti-tamper.
- Trazabilidad de los eventos más relevantes desde el punto de vista de seguridad.

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL4, más las requeridas para el componente adicional ALC_FLR.1, según Common Criteria v3.1 R4.

Class	Family/Component
ASE: Security Target Evaluation	ASE_INT.1. ST Introduction
	ASE_CCL.1. Conformance claims
	ASE_SPD.1. Security problem definition
	ASE_OBJ.2. Security objectives
	ASE_ECD.1. Extended component definition
	ASE_REQ.2. Derived security requirements
	ASE_TSS.1. TOE summary specification
ADV: Development	ADV_ARC.1. Security architecture description
	ADV_FSP.4. Complete functional specification
	ADV_IMP.1. Implementation representation of the TSF
	ADV_TDS.3. Basic modular design
AGC: Guidance documents	AGD_OPE.1. Operational user guidance
	AGD_PRE.1. Preparative procedures
ALC: Life cycle support	ALC_CMC.4. Production support, acceptance procedures and automation
	ALC_CMS.4. Problem tracking CM coverage
	ALC_DEL.1. Delivery procedures

	ALC_DVS.1. Identification of security measures
	ALC_FLR.1. Flaw remediation
	ALC_LCD.1. Developer defined life-cycle model
	ALC_TAT.1. Well-defined development tools
ATE: Tests	ATE_COV.2. Analysis of coverage
	ATE_DPT.1. Testing: basic design
	ATE_FUN.1. Functional tests
	ATE_IND.2. Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3. Focused vulnerability analysis

REQUISITOS FUNCIONALES DE SEGURIDAD

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

Requirement Class	Requirement Component
Security Audit (FAU)	FAU_ARP.1 Security Alarms
	FAU_GEN.1 Audit Data Generation
	FAU_GEN.2 User Identity Association
	FAU_SAA.1 Potential Violation Analysis
	FAU_SAR.1 Audit Review
	FAU_SAR.3 Selectable Audit Review
	FAU_SEL.1(AR) Selective Audit
	FAU_SEL.1(SNMP) Selective Audit
	FAU_STG.2 Guarantees of Audit Data Availability
	FAU_STG.4 Prevention of Audit Data Loss
User Data Protection (FDP)	FDP_ACC.1(INY) Subset Access Control
	FDP_ACC.1(USR) Subset Access Control
	FDP_ACF.1(INY) Security Attribute Based Access Control
	FDP_ACF.1(USR) Security Attribute Based Access Control
	FDP_IFC.1 Subset Information Flow Control
	FDP_IFF.1 Simple Security Attributes
Identification & Authentication (FIA)	FIA_AFL.1(INY) Authentication Failure Handling
	FIA_AFL.1(USR) Authentication Failure Handling
	FIA_ATD.1 User Attribute Definition
	FIA_SOS.1(INY) Verification of Secrets
	FIA_SOS.1(USR) Verification of Secrets
	FIA_UAU.1(INY) Timing of Authentication
	FIA_UAU.1(USR) Timing of Authentication
	FIA_UAU.2 User Authentication Before any Action
	FIA_UAU.5 Multiple Authentication Mechanisms
	FIA_UID.1(INY) Timing of Identification

	FIA_UID.1(USR) Timing of Identification
	FIA_UID.2 User Identification Before Any Action
Security Management (FMT)	FMT_MSA.1(IFC) Management of Security Attributes
	FMT_MSA.1(INY) Management of Security Attributes
	FMT_MSA.1(USR1) Management of Security Attributes
	FMT_MSA.1(USR2) Management of Security Attributes
	FMT_MSA.3(IFC) Static Attribute Initialisation
	FMT_MSA.3(INY) Static Attribute Initialisation
	FMT_MSA.3(USR1) Static Attribute Initialisation
	FMT_MSA.3(USR2) Static Attribute Initialisation
	FMT_MTD.1 Management of TSF data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles
Protection of the TSF (FPT)	FPT_FLS.1 Failure with Preservation of Secure State
	FPT_ITK.1 Import of TSF Data from Outside of the TOE
	FPT_PHP.3 Resistance to Physical Attack
	FPT_RCV.1 Manual Recovery
	FPT_STM.1 Reliable Time Stamps
	FPT_TST.1 TSF Testing
TOE Access (FTA)	FTA_SSL.3 TSF-Initiated Termination
	FTA_SSL.4 User-Initiated Termination
Trusted Path/Channels (FTP)	FTP_ITC.1 Inter-TSF Trusted Channel

IDENTIFICACIÓN

Producto: IS101 v1.01.

Declaración de Seguridad: IS101. Declaración de Seguridad (IS251101ZZ01), ED10/Rev. 27. 23/04/2018.

Perfil de Protección: ninguno.

Nivel de Evaluación: CC v3.1 R4 – EAL4 + ALC_FLR.1

POLÍTICA DE SEGURIDAD

El uso del producto debe implementar una serie de políticas organizativas que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de estas políticas se encuentra en la Declaración de Seguridad en el apartado 5.3.

HIPÓTESIS Y ENTORNO DE USO

Las hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas. Por tanto, para garantizar el uso seguro del TOE, se parte de las siguientes hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

El detalle de estas hipótesis se encuentra en la Declaración de Seguridad en el apartado 5.4.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a *enchanced basic* de EAL4, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Las amenazas cubiertas por las propiedades de seguridad del TOE se detallan en el apartado 5.2 de la Declaración de Seguridad.

FUNCIONALIDAD DEL ENTORNO

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

Los objetivos que se deben cubrir por el entorno de uso del TOE se encuentran indicados en el apartado 6.2 de la Declaración de Seguridad.

ARQUITECTURA

ARQUITECTURA LÓGICA

El TOE incluye e integra componentes HW y SW/FW, implementando los siguientes protocolos, funcionalidades y mecanismos:

- control y filtrado robusto del tráfico,
- sistema de control de acceso para la gestión del IS101, de acuerdo a una serie de perfiles de usuario,
- Mecanismos anti-tamper pasivos,
- Mecanismos anti-tamper activos,
- Almacenamiento seguro de ciertos datos sensibles en el supervisor de seguridad,
- Monitorización de los eventos de seguridad más relevantes que se producen en el equipo,
- Establecimiento de canales seguros para la comunicación con dispositivos IT confiables externos al TOE.

ARQUITECTURA FÍSICA

El TOE se suministra como un único equipo ya programado (HW + SW/FW embebido), empaquetado y etiquetado conforme a los procedimientos de entrega establecidos para el equipo. La fuente de alimentación del equipo así como el cable de consola estándar, son elementos auxiliares que, aunque no forman parte del TOE, se suministran junto con el mismo.

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.

- IS101. Manual de Usuario (IS240101ZZ01) en formato PDF.

PRUEBAS DEL PRODUCTO

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todas las pruebas han sido realizadas por el fabricante, en sus instalaciones, con resultado satisfactorio.

Durante el proceso de evaluación se han verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas, acorde a la arquitectura identificada en la Declaración de Seguridad.

Para verificar los resultados de las pruebas del fabricante, el laboratorio ha repetido una serie de pruebas suficiente para permitirle verificar la principal funcionalidad de seguridad del TOE. Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

CONFIGURACIÓN EVALUADA

El entorno de pruebas utilizado por el evaluador sigue el mismo esquema que el entorno operacional y lo componen los siguientes elementos:

- TOE IS101 (para la red roja).
- TOE IS101 (para la red negra).
- Host1: Máquina del entorno: Consiste en una máquina con sistema operativo Linux (Debian) instalado, incluyendo a su vez un servidor FTP, servidor PKI y servidor DHCP. Se encuentra conectada a la red roja (protegida) del IS101.
- Host2: Máquina de Entorno: Consiste en una máquina con sistema operativo Linux (Debian) instalado. Conectada a la red roja (protegida) del IS101.
- Host3: Máquina de Entorno utilizada también por el evaluador para hacer las pruebas correspondientes. Esta contiene un sistema Kali Linux (Debian) corriendo sobre la máquina.

Todas las máquinas y elementos se encuentran conectados entre sí a través de switches y cableado Ethernet.

Además se han utilizado varios scripts y herramientas desarrolladas por el evaluador para la ejecución de las pruebas.

RESULTADOS DE LA EVALUACIÓN

El producto IS101 v1.01 ha sido evaluado en base a la Declaración de Seguridad: “IS101. Declaración de Seguridad (IS251101ZZ01), ED10/Rev. 27. 23/04/2018”.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 + ALC_FLR.1 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 EAL4 + ALC_FLR.1, definidas por Common Criteria v3.1 R4 y CEM v3.1 R4.

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.

- El cumplimiento de las hipótesis indicadas por la Declaración de Seguridad son una pieza fundamental en la seguridad del TOE ya que implica configuraciones del entorno del TOE que dejan algunas vulnerabilidades fuera del alcance de la certificación.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto IS101 v1.01, 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
FW	Firmware
HW	Hardware
OC	Organismo de Certificación
SW	Software
TOE	Target Of Evaluation

BIBLIOGRAFÍA

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

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R3 Final, July 2009.

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 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:

- IS101. Declaración de Seguridad (IS251101ZZ01), ED10/Rev. 27. 23/04/2018

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for assurance components up to EAL4.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-

certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.