Referencia: 2017-9-INF-2840-v1
Difusión: Público
Fecha: 06.09.2019

Creado por: CERT11
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente #	**2017-9**
TOE	**AUTEK PSTdiode ATKDDL versión 1.0.0**
Solicitante	**B82015181 - Autek Ingenieria S.L.**
Referencias	

[EXT-3311] Solicitud Certificación Autek Data Diode

[EXT-5170] Informe Técnico de Evaluación, versión 3.0.

Informe de Certificación del producto AUTEK PSTdiode ATKDDL versión 1.0.0, según la solicitud de referencia [EXT-3311], de fecha 23/02/2017, evaluado por el laboratorio Epoche & Espri S.L.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-5170], recibido el pasado 25/07/2019.

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto AUTEK PSTdiode ATKDDL versión 1.0.0.

El TOE es un conjunto de hardware (dos tarjetas PCI-Express) que constituye el núcleo sobre el que construir un sistema de transmisión unidireccional entre dos redes no conectadas por otros medios.

El TOE ha sido diseñado para ser instalado en sendos PCs estándar. El uso previsto del TOE es la transmisión unidireccional de datos desde el PC en el que esté instalada la tarjeta TX hasta el PC en el que esté instalada la tarjeta RX. El diseño del TOE garantiza que no existe flujo de información en el otro sentido, por lo que es adecuado para todos los usos en los que haya necesidad de transmisión de información en un único sentido, con garantía física de unidireccionalidad.

El producto PSTdiode ATKDDL v.1.0.0 está formado por una tarjeta emisora TX (ATKDDL_TX v.1.0.0), una tarjeta receptora RX (ATKDDL_RX v.1.0.0).

Fabricante: Autek Ingenieria S.L..

Patrocinador: Autek Ingenieria S.L..

Organismo de Certificación: Centro Criptológico Nacional (CCN).

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

Perfil de Protección: No aplica.

Nivel de Evaluación: CC v 3.1 R5 EAL 4 + ALC_FLR.3 + AVA_VAN.5.

Fecha de término de la evaluación: 25/07/2019.

Todos los componentes de garantía requeridos por el nivel de evaluación CC v 3.1 R5 EAL 4 + ALC_FLR.3 + AVA_VAN.5 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 CC v 3.1 R5 EAL 4 + ALC_FLR.3 + AVA_VAN.5, definidas por *Common Criteria version 3.1 release 5* y la metodología de evaluación [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto AUTEK PSTdiode ATKDDL versión 1.0.0, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El TOE es un conjunto de hardware (dos tarjetas PCI-Express) que constituye el núcleo sobre el que construir un sistema de transmisión unidireccional entre dos redes no conectadas por otros medios.

El TOE ha sido diseñado para ser instalado en sendos PCs estándar. El uso previsto del TOE es la transmisión unidireccional de datos desde el PC en el que esté instalada la tarjeta TX hasta el PC en el que esté instalada la tarjeta RX. El diseño del TOE garantiza que no existe flujo de información en

el otro sentido, por lo que es adecuado para todos los usos en los que haya necesidad de transmisión de información en un único sentido, con garantía física de unidireccionalidad.

El sistema de transmisión unidireccional construido usando como base el TOE es de aplicación a varios escenarios de intercambio seguro de información. Los dos casos de uso más típicos son los que se describen a continuación. En todos los escenarios de uso el sistema de transmisión unidireccional debe ser el único punto de intercambio de información entre los dominios de seguridad separados.

El primer escenario de uso es el de redes clasificadas que se consigue a través de la entrada de información en una red de mayor grado de clasificación que la red de origen. Se garantiza de que no hay flujo de información en el sentido inverso, es decir de la red de mayor clasificación o nivel de seguridad hacia la de menor.

El segundo escenario de uso es el de redes de control aisladas que se consigue a través de la salida de información para monitorización de una instalación de control industrial aislada. Garantía de que no entra malware que pueda afectar a la integridad o disponibilidad de la red de control aislada.

El producto PSTdiode ATKDDL v.1.0.0 está formado por una tarjeta emisora TX (ATKDDL_TX v.1.0.0), una tarjeta receptora RX (ATKDDL_RX v.1.0.0).

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL 4 + ALC_FLR.3 + AVA_VAN.5 según Common Criteria [CC_P3].

Clase	Familia/Componente
ASE	INT.1
	CCL.1
	SPD.1
	OBJ.2
	ECD.1
	REQ.2
	TSS.1
AGD	OPE.1
	PRE.1
ALC	CMC.4
	CMS.4
	DEL.1

	DVS.1 LCD.1 TAT.1 FLR.3 (aumento)
ADV	FSP.4 ARC.1 TDS.3 IMP.1
ATE	COV.2 DPT.1 FUN.1 IND.2
AVA	VAN.5 (aumento)

REQUISITOS FUNCIONALES DE SEGURIDAD

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, según según [CC_P2].

Clase	Familia/Componente
FDP	IFC.1 IFF.1

IDENTIFICACIÓN

Producto: AUTEK PSTdiode ATKDDL versión 1.0.0.

Declaración de Seguridad: Declaración de seguridad de PSTdiode ATKDDL. 27/06/2019. Ref. 0555-01 R1.3.

Perfil de Protección: No aplica.

Nivel de Evaluación: Common Criteria v3.1 R5, EAL4 + ALC_FLR.3 + AVA_VAN.5.

POLÍTICA DE SEGURIDAD

El producto AUTEK PSTdiode ATKDDL versión 1.0.0 no implementa ninguna política de seguridad organizativa.

HIPÓTESIS Y ENTORNO DE USO

Las siguientes 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.

Hipótesis 01: A.PHYSEC

Cada uno de los dos PCs (emisor y receptor) donde se instalan las respectivas tarjetas que constituyen el hardware del TOE se deben situar dentro de un entorno físicamente controlado.

Hipótesis 02: A.LOCNOEVIL

Los administradores autorizados y con acceso físico al TOE no van a intentar circunvalar la funcionalidad de seguridad del mismo.

Hipótesis 03: A.SINGLECHAN

No existen otros canales, a parte del TOE, por los que pueda circular la información, entre los dos PCs donde se instalan las tarjetas emisora y receptora.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto AUTEK PSTdiode ATKDDL versión 1.0.0, aunque los agentes que realicen ataques tengan potencial de ataque **Alto** correspondiente al nivel de garantía EAL4 + ALC_FLR.3 + AVA_VAN.5, 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 relacionan a continuación.

Amenaza 01: T.R_TO_T_TRANSFER

Un usuario remoto (sin acceso físico al PC donde está instalada la tarjeta emisora, pero con conectividad de red hasta dicho PC), consigue obtener, a través del sistema, información perteneciente al PC receptor u otros sistemas conectados a él.

Un usuario remoto (sin acceso físico al PC donde está instalada la tarjeta receptora, pero con conectividad de red hasta dicho PC), consigue transmitir cualquier tipo de información a través del sistema, desde el PC receptor hasta el PC emisor.

FUNCIONALIDAD DEL ENTORNO

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

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

Objetivo entorno 01: OE.PHYSEC

El acceso físico al hardware de los PCs dónde se instalan las tarjetas emisora y receptora estará limitado y controlado. Las maneras obvias de circunvalar el sistema (como por ejemplo conectar ambos equipos directamente mediante un cable de red) quedan descartadas por medidas físicas u organizativas de los entornos de explotación.

Objetivo entorno 02: OE.LOCNOEVIL

Los administradores autorizados y con acceso físico al TOE, instalarán y administrarán el TOE de acuerdo a los procedimiento de uso seguro del TOE.

Objetivo entorno 03: OE.TOPOLOGY

La única manera de conectar los dos PCs (emisor y receptor) entre sí es a través de TOE.

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad) o de los requisitos de seguridad del TOE se encuentran en la correspondiente Declaración de Seguridad.

ARQUITECTURA

ARQUITECTURA LÓGICA

El TOE proporciona la siguiente funcionalidad:

- Carácter unidireccional de la información transmitida. Es decir, garantía de que toda información transferida entre las tarjetas emisora y receptora circula en un único sentido, desde la tarjeta emisora a la receptora.

ARQUITECTURA FÍSICA

Los componentes que forman parte del TOE son entregados en mano por personal de Autek Ingeniería S.L.

El TOE está formado por los siguientes componentes:

- Tarjeta emisora TX (ATKDDL_TX 1.0.0)
- Tarjeta receptora RX (ATKDDL_RX 1.0.0)

Y por el CD-ROM 'Software y documentación', que contiene:

- Manual de instalación y uso en formato PDF (um_0555-10_r4).

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.

- Manual de instalación y uso en formato PDF (um_0555-10_r4).

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 satisfactorios.

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.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Para verificar los resultados de las pruebas del fabricante, el laboratorio ha repetido todas las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación.

Adicionalmente, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados, así obtenidos, son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no representa un problema para la seguridad, ni supone una merma en la capacidad funcional del producto.

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 AUTEK PSTdiode ATKDDL versión 1.0.0 es necesario disponer de los siguientes componentes software:

- El sistema operativo (que no forma parte del TOE) de los ordenadores puede ser Windows (7 ó superior) o Linux (se recomienda Debian 9 ó superior).
- Es necesario el uso de como mínimo dos componentes software desarrollados específicamente para construir un sistema que permita la transmisión y la recepción de datos mediante el TOE.

En cuanto a los componentes hardware:

- El TOE necesita dos ordenadores estándar (que no forman parte del TOE) con bus PCI-Express 2.1 o superior.

RESULTADOS DE LA EVALUACIÓN

El producto AUTEK PSTdiode ATKDDL versión 1.0.0 ha sido evaluado en base a la Declaración de Seguridad *"Declaración de seguridad de PSTdiode ATKDDL. 27/06/2019. Ref. 0555-01 R1.3"*.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 + ALC_FLR.3 + AVA_VAN.5 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.3 + AVA_VAN.5, definidas por Common Criteria [CC_P3] y [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.

El uso del TOE es recomendado dado que no existen vulnerabilidades explotables en el entorno operacional. De todos modos, se proporcionan las siguientes recomendaciones de uso:

- El cumplimiento de las hipótesis indicadas en la declaración de seguridad es un punto clave ya que implica configuraciones en el entorno del TOE que dejan algunas vulnerabilidades fuera de alcance.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto AUTEK PSTdiode ATKDDL versión 1.0.0, 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, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

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 de PSTdiode ATKDDL. 27/06/2019. Ref. 0555-01 R1.3.

La version pública de este document constituye la "Declaración de Seguridad LITE" que ha sido revisada siguiendo el documento con código [CCDB-2006-04-004], y se publica con el informe de certificación en las webs del CCRA y del OC. El identificador de la "Declaración de Seguridad LITE" es:

- PSTdiode ATKDDL Security Target Lite. 27/06/2019. Ref. 0555-24 R1.3

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.