Referencia: 2018-6-INF-2529-v1
Difusión: Público
Fecha: 15.10.2018

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

INFORME DE CERTIFICACIÓN

Expediente #	**2018-6**
TOE	**Savvy M2C Communications versión 1.3**
Solicitante	**B-75092114 - Savvy Data Systems S.L.**
Referencias	

[EXT-3826] Solicitud de certificación

[EXT-4255] Informe Técnico de Evaluación

Informe de Certificación del producto Savvy M2C Communications versión 1.3, según la solicitud de referencia [EXT-3826], de fecha 28/02/2018, evaluado por el laboratorio Epoche & Espri S.L.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-4255], recibido el pasado 31/08/2018.

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto Savvy M2C Communications versión 1.3.

El TOE es el modelo de comunicación captador-Cloud / Cloud-usuario, es decir cómo se conectan de forma segura los dispositivos captadores con el Cloud (servidores DataFrontend, DF), cómo se gestiona esa conexión desde estos servidores y cómo se conecta un cliente de manera segura a través de la interfaz web para visualizar datos, configurar captadores y/o gestionar la plataforma con el servidor web.

Fabricante: Savvy Data Systems S.L..

Patrocinador: Savvy Data Systems S.L..

Organismo de Certificación: Centro Criptológico Nacional (CCN).

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

Perfil de Protección: No declarado.

Nivel de Evaluación: Common Criteria versión 3.1 release 5 - EAL1.

ISO/IEC 15408:2009 – EAL1.

Fecha de término de la evaluación: 31/08/2018.

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 las metodologías Common Criteria versión 3.1 release 5 e ISO/IEC 15408:2009 y Common Evaluation Methodology version 3.1 release 5 e ISO/IEC 18045:2008/2014-01.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Savvy M2C Communications versión 1.3, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El TOE es el modelo de comunicación captador-Cloud / Cloud-usuario, es decir cómo se conectan de forma segura los dispositivos captadores con el Cloud (servidores DataFrontend, DF), cómo se gestiona esa conexión desde estos servidores y cómo se conecta un cliente de manera segura a través de la interfaz web para visualizar datos, configurar captadores y/o gestionar la plataforma con el servidor web.

En el caso del captador se trata de una aplicación Java corriendo en una máquina Ubuntu. Los servidores Data Frontend también se tratan de una aplicación en Java corriendo sobre una máquina

Ubuntu, que se encuentran en un Data Center contratado a una compañía externa. La interfaz web corre en una máquina Ubuntu sobre Apache también en el Data Center contratado.

Aunque el tipo de producto que ofrece Savvy Data Systems se trata tanto de hardware como software, el TOE únicamente consiste en la gestión de las comunicaciones entre captador- Cloud y el acceso a la interfaz web (comunicación con el usuario). Por lo tanto, se define como tipo: "Canales de comunicaciones".

Todos los canales de comunicación mencionados anteriormente utilizan TLS v1.2. Los captadores solo se pueden conectar con el Cloud debido a que comprueban la firma del certificado y además deben acreditarse a la hora de establecer la conexión, sin posibilidad de fallo (conlleva bloqueo inmediato).

El uso del TOE por parte del usuario, dada su naturaleza, solo puede darse en la interfaz web. Tiene un mecanismo de autenticación en dos pasos en la que se verifican los dispositivos desde los que se accede y bloqueos en función del número de intentos fallidos en el login.

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 versión 3.1 release 5 e ISO/IEC 15408:2009.

Assurance Class	Assurance components
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 definition
	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 versión 3.1 release 5 e ISO/IEC 15408:2009.

TOE Security Functional Requirements	Description
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ITT.1	Basic internal transfer protection
FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
FPT_ITT.1	Basic internal TSF data transfer protection
FTA_SSL.4	User-initiated termination
FTA_TSE.1	TOE session establishment

IDENTIFICACIÓN

Producto: Savvy M2C Communications versión 1.3.

Declaración de Seguridad: ST-EAL1 Savvy M2C Communications, versión 1.5. 12/07/2018.

Perfil de Protección: No declarado.

Nivel de Evaluación: Common Criteria versión 3.1 release 5 – EAL 1

ISO/IEC 15408:2009 - EAL1.

POLÍTICA DE SEGURIDAD

El TOE no define en su Declaración de Seguridad ninguna Política de Seguridad.

HIPÓTESIS Y ENTORNO DE USO

De acuerdo al nivel de garantía declarado (EAL1), el TOE no declara un problema de seguridad en su Declaración de Seguridad, por lo que no existe una declaración de hipótesis específica. El fabricante conforme a lo marcado por Common Criteria tan sólo define una serie de objetivos de seguridad para el entorno operacional en la sección 3.1 de [ST] que deben ser observados por los potenciales consumidores del TOE.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

De acuerdo al nivel de garantía declarado (EAL1), el TOE no declara un problema de seguridad en su Declaración de Seguridad, por lo que no existe una declaración de hipótesis específica. El fabricante conforme a lo marcado por Common Criteria tan sólo define una serie de objetivos de seguridad para el entorno operacional en la sección 3.1 de [ST] que deben ser observados por los potenciales consumidores del TOE.

FUNCIONALIDAD DEL ENTORNO

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

Los detalles de la definición del entorno del TOE se encuentran en la correspondiente Declaración de Seguridad [ST] en su sección 3.1.

La relación de los objetivos para el entorno operacional es la siguiente:

- **OE.1 Acceso físico al captador protegido**: el acceso físico está restringido a personal autorizado de confianza.

- **OE.2 Administrador de confianza en el captador**: el usuario no tiene permisos de root sobre el captador para la ejecución de comandos, únicamente tiene permisos de root el personal autorizado de confianza de Savvy Data Systems.
- **OE.3 Acceso físico al Cloud protegido**: el acceso físico está impedido por la propia seguridad perimetral del Data Center contratado.
- **OE.4 Cloud protegido por firewall**: firewall seguro que únicamente permite conexiones externas mediante SSH desde la oficina de Savvy Data Systems (personal de confianza). El puerto 443 está abierto al exterior en servidores DF y Web.
- **OE.5 Navegador web TLS v1.2**: el servidor web solo acepta peticiones de navegadores que usan TLS v1.2.
- **OE.6 Administrador de confianza en la plataforma**: Los usuarios administradores de la plataforma únicamente son personal de confianza de Savvy Data Systems.

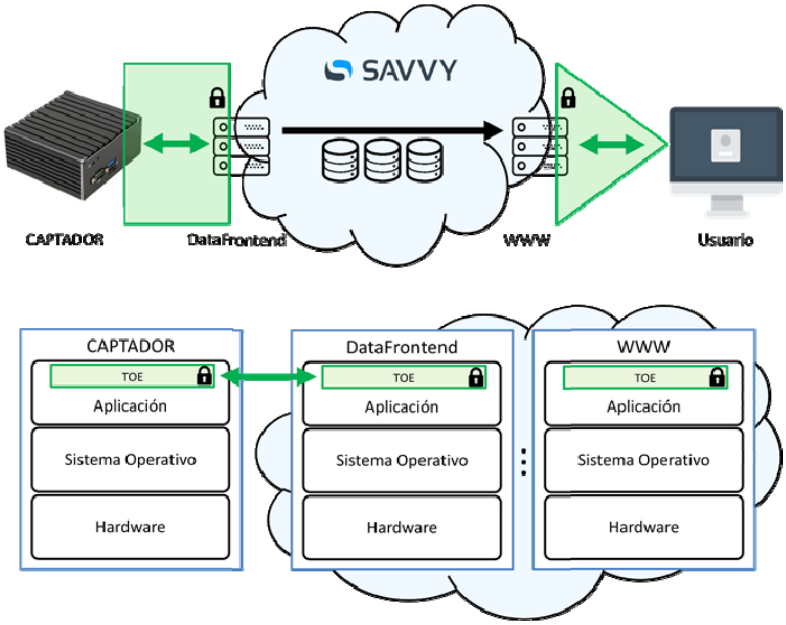
ARQUITECTURA

ARQUITECTURA LÓGICA

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

- Conexión de los dispositivos captadores con el Cloud: el software en Java residente en los captadores abre una serie de conexiones de forma segura contra el servicio Cloud usando TLS v1.2, comprobando la identidad del servidor al que se conecta (certificados pinneados) y autenticándose con su código y clave de dispositivo, pudiéndose autenticar únicamente los dispositivos autorizados por Savvy Data Systems (en caso de fallo, supone bloqueo automático).
- Gestión de la conexión con los captadores desde el Cloud: los servidores gestionan la identificación y autorización de las conexiones de los captadores. Realizan la recepción de datos a través de TLS v1.2. Se ha desarrollado un mecanismo de rotación y revocación de certificados sin necesidad de parada y evitando la necesidad de validación de la cadena de certificación y de entidades externas, para tener una mayor seguridad y precisión.
- Gestión del login en la interfaz web: siempre se redirecciona a HTTPS, contando con un certificado válido emitido por COMODO RSA DomainValidationSecure Server CA. Para acceder a cualquier apartado de la interfaz web, es necesario identificarse y autenticarse. Además, se cuenta con un proceso de autenticación en dos pasos para verificar el dispositivo desde el que se conecta. Se tiene también un sistema de desafío para prevenir ataques replay y un sistema de bloqueo por IP.

El TOE consiste en la parte del firmware (marcada en verde) encargada de gestionar las comunicaciones. Ambas figuras representan el mismo concepto, solo que cada una representa un punto de vista diferente.



ARQUITECTURA FÍSICA

La parte del TOE correspondiente al captador se entrega instalado junto con el captador. Se encuentra dentro de un archivo en Java, un .jar, llamado “clienteIC.jar”.

En cuanto a la parte del TOE correspondiente al Cloud, no se entrega nada al usuario. Se encuentra dentro de un conjunto de archivos compilados en Java. La parte web del TOE es accesible por Internet y al usuario se le envía un email en el que se le informa de que se le ha creado una cuenta de usuario con su cuenta de correo y que debe establecer una contraseña a través del enlace incluido también en el mensaje. La parte web se trata de un conjunto de archivos PHP. Los captadores no requieren de la interacción del usuario, únicamente para su instalación y configuración de red, por lo que se ofrece una guía que detalla estos pasos, en formato papel entregada junto con el captador (Ficha de captador – CER20180419_HW001 - Versión 1.3 [FC13]).

Para la interfaz web se entrega una pequeña guía (Guía de acceso web – Versión 1.3 [GBAW13]) que describe las interfaces del TOE accesibles por el usuario y los diferentes roles vía email en formato pdf y además se ofrecen formaciones presenciales personalizadas.

DOCUMENTOS

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

- [FC13] Código captador CER20180419_HW001, versión 1.3.

- [GBAW13] Guía básico acceso web, versión 1.3.
- [ADC12] Aspectos Datacenter, versión 1.2.

PRUEBAS DEL PRODUCTO

El evaluador ha definido las pruebas teniendo en cuenta los requisitos de seguridad definidos en la [ST] y las interfaces externas, considerando la documentación proporcionada por el desarrollador.

El evaluador ha realizado los pasos indicados para obtener la versión del TOE, siendo la versión entregada para las pruebas la misma que la descrita en la declaración de seguridad (Savvy M2C Communications versión 1.3).

El manual [FC13] indica que el fabricante entrega el TOE instalado, y solo es necesario configurar la red del captador para su conexión a internet de acuerdo con la declaración de seguridad [ST].

Dicha configuración se considera válida para la realización de las pruebas ya que el TOE está desplegado y configurado conforme a la declaración de seguridad y se encuentra en un estado conocido.

El principal objetivo de las pruebas realizadas por el evaluador ha sido comprobar el cumplimiento de los requisitos especificados en la declaración de seguridad [ST] a través de las interfaces TSFIs, para ello el evaluador diseño un conjunto de pruebas siguiendo una estrategia adecuada para el tipo de TOE. No se ha realizado ningún tipo de muestreo, por lo que se han probado todos los SFRs a través de las correspondientes TSFIs.

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

El TOE se define por su nombre y versión como Savvy M2C Communications versión 1.3.

El evaluador ha empleado una configuración consistente con lo descrito en las guías de preparación y operación del TOE (referenciadas en la sección DOCUMENTOS).

Adicionalmente los elementos empleados en el entorno operacional para evaluar el TOE ha sido los siguientes:

- Software cliente residente en el Captador (PC Industrial con Intel(R) Celeron(R) CPU N2930 @ 1.83GHz y 4 GB de RAM):
    - Ubuntu Server
    - Java JDK
    - OpenSSL

- Servidores DataFrontend (DF): Se trata de una granja de servidores con base Linux, en los que se ejecuta el código de recepción de datos desde los captadores. Los requisitos de seguridad del entorno que deben satisfacer el proveedor de la granja de servidores se define en [ADC12] Aspectos Datacenter, versión 1.2. Los elementos que componen estos servidores son:
    - Ubuntu Server
    - Java
    - OpenSSL
- Servidores Web (servidor):
    - Ubuntu Server
    - Apache server
    - PHP server
    - Apache / Mod Security
    - OpenSSL
    - Fail2Ban

El consumidor del TOE puede verificar la configuración incluida en el TOE siguiendo el procedimiento de verificación definido en la sección "Comprobación de versión del TOE" en la guía [GBAW13] Guía básico acceso web, versión 1.3.

RESULTADOS DE LA EVALUACIÓN

El producto Savvy M2C Communications versión 1.3 ha sido evaluado en base a la Declaración de Seguridad ST-EAL1 Savvy M2C Communications, versión 1.5. 12/07/2018.

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 Common Criteria versión 3.1 release 5 e ISO/IEC 15408:2009 y Common Evaluation Methodology version 3.1 release 5 e ISO/IEC 18045:2008/2014-01.

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 equipo evaluador recomienda el uso del TOE compuesto ya que no presenta vulnerabilidades explotables en su entorno operacional.

Se proporciona la siguiente recomendación adicional que debe ser tenida en cuenta por los posibles consumidores del TOE:

- Los potenciales consumidores deben seguir estrictamente de los pasos proporcionados para el establecimiento de los canales seguros implementados por el TOE es crucial para satisfacer la configuración evaluada.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Savvy M2C Communications versión 1.3, se propone la resolución estimatoria de la misma.

El certificador recomienda que los posibles consumidores observen los objetivos de seguridad que debe satisfacer el entorno operacional (ver sección 3.1 de la declaración de seguridad), además de seguir lo especificado en las guías de seguridad relacionadas en la sección DOCUMENTOS de este informe de certificación.

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:

[ADC12] Aspectos Datacenter, versión 1.2. Savvy Data Systems S.L.

[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.

[FC13] Código captador CER20180419_HW001, versión 1.3. Savvy Data Systems S.L.

[GBAW13] Guía básico acceso web, versión 1.3. Savvy Data Systems S.L.

[ISO15408-1] ISO/IEC 15408:2009-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.

[ISO15408-2] ISO/IEC 15408:2009-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security Functional Components.

[ISO15408-3] ISO/IEC 15408:2009-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security Assurance Components.

[ISO18045] ISO/IEC 18045:2008/2014-01 Information technology - Security techniques - Methodology for IT security evaluation.

[ST] ST-EAL1 Savvy M2C Communications, versión 1.5. 12/07/2018. Savvy Data Systems S.L.

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:

- ST-EAL1 Savvy M2C Communications, versión 1.5. 12/07/2018.

ACUERDOS DE RECONOCIMIENTO MUTUO DEL CERTIFICADO

El certificado emitido como consecuencia de la evaluación técnica y el proceso de certificación realizado cuenta con reconocimiento mutuo teniendo en cuenta los acuerdos de reconocimiento mutuos firmados por el Centro Criptológico Nacional. A continuación se incluyen los términos y alcance de reconocimiento de dichos acuerdos de reconocimiento mutuo.

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 all assurance components selected.

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 selected.