# ST-EAL1 Savvy M2C Communications


Versión del documento: 1.6

Fecha: 22/02/2019

Savvy Data Systems S.L.

C.I.F. B-75092114

C/ Portuetxe 45-A 4-4

20018 San Sebastián-Donostia (Gipuzkoa)

Telephone: +34 943 317 074

# CONTENIDO





SAVVY

SAVVY

# 1 INTRODUCCIÓN

## 1.1 Referencia a la declaración de seguridad

**Título:** ST-EAL1 Savvy M2C Communications

**Versión:** 1.6

**Autor:** Savvy Data Systems S.L.

**Fecha de publicación:** 12/07/2018

## 1.2 Referencia del TOE

**Nombre:** Savvy M2C Communications

**Versión**: 1.3

**Desarrollador:** Savvy Data SystemsS.L.

## 1.3 Resumen del producto

La solución M2C que ofrece Savvy Data Systems está pensada para ser desplegada en plantas de fabricación. El dispositivo captador (o *Savvy Smart Box*) se conecta a la máquina (o máquinas) a través de la red de planta, realiza un mecanismo de autodespliegue por el cual es capaz de establecer una conexión automática a través de la red de Internet contra el Cloud de Savvy Data Systems, comenzará a captar datos de diversos orígenes y serán enviados al Cloud a través de un canal cifrado por TLS v1.2. Desde la interfaz web, los usuarios autorizados pueden realizar la configuración del captador, la gestión de la plataforma y la consulta de los datos recogidos por el captador en tiempo real.

## 1.4 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.

### *1.4.1 Tipo de TOE*

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”.

### 1.4.2 Uso del TOE

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.

### 1.4.3 Características de seguridad del TOE

Las características de seguridad que implementa el TOE son las siguientes:

- **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.

### 1.4.4 Software y hardware requerido por el TOE para su operación

Captador: PC Industrial con Intel(R) Celeron(R) CPU N2930 @ 1.83GHz y 4 GB de RAM. Puede correr sobre Ubuntu Server 14.04 LTS, Ubuntu Server 16.04 LTS o Ubuntu Server 18.04 LTS y puede utilizar Java 7 o Java 8.

Servidor DF: Servidor virtualizado en el Data Center contratado con Intel(R) Xeon(R) CPU E5-2683 v3 @ 2.00GHz, 2 cores y 4 GB de RAM. Puede correr sobre Ubuntu Server 14.04 LTS, Ubuntu Server 16.04 LTS o Ubuntu Server 18.04 LTS y puede utilizar Java 7 o Java 8.

Servidor Web: Servidor virtualizado en el Data Center contratado con Intel(R) Xeon(R) CPU E5-2683 v3 @ 2.00GHz, 4 cores y 8 GB de RAM. Puede correr sobre Ubuntu Server 14.04 LTS, Ubuntu Server 16.04 LTS o Ubuntu Server 18.04 LTS, puede utilizar Java 7 o Java 8, PHP 5.5.9 o PHP 7.2 y Apache (se mantiene actualizado a nuevas versiones por actualizaciones de seguridad).

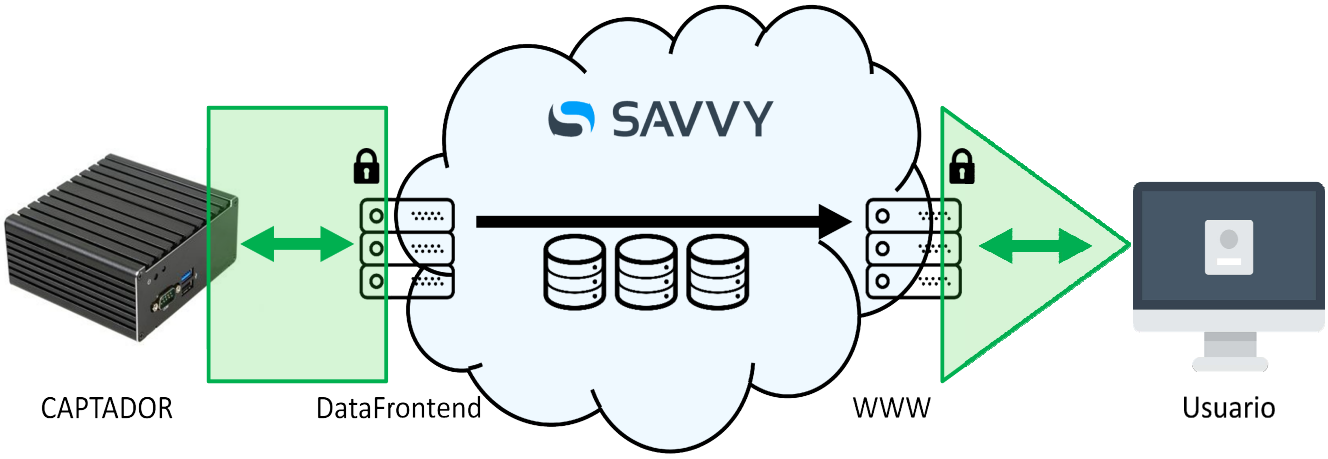
**Plataforma de pruebas utilizada en la evaluación de seguridad.**

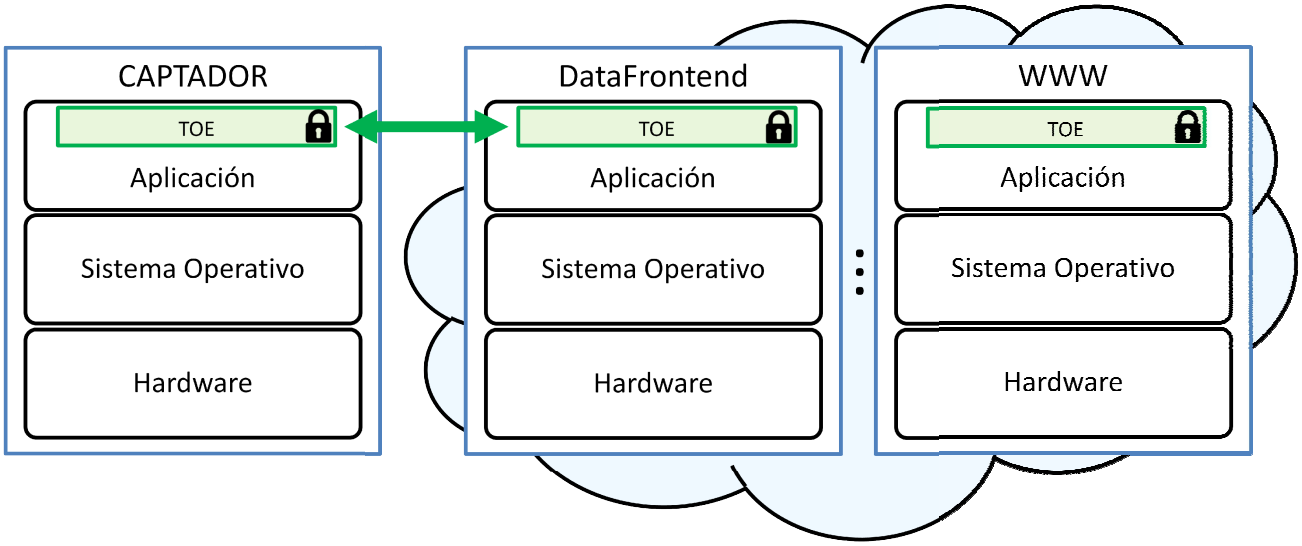
Para la evaluación se ha utilizado la siguiente plataforma de pruebas, todo bajo TLS v1.2:

Captador: PC Industrial con Intel(R) Celeron(R) CPU N2930 @ 1.83GHz y 4 GB de RAM, con Ubuntu Server 14.04 LTS y Java 7.

Servidor DF: Servidor virtualizado en el Data Center contratado con Intel(R) Xeon(R) CPU E5-2683 v3 @ 2.00GHz, 2 cores y 4 GB de RAM, con Ubuntu Server 14.04 LTS y Java 7.

Servidor Web: Servidor virtualizado en el Data Center contratado con Intel(R) Xeon(R) CPU E5-2683 v3 @ 2.00GHz, 4 cores y 8 GB de RAM, con Ubuntu Server 14.04 LTS, Java 7, PHP 5.5.9 y Apache 2.4.7.




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.

## 1.5 Descripción del TOE

### *1.5.1 Ámbito físico del TOE: Componentes*

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 – XXXXXXXX - Versión 1.3). Para la interfaz web se entrega una pequeña guía (Guía de acceso web – Versión 1.3) 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.

### *1.5.2 Ámbito lógico del TOE*

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 abre una serie de conexiones seguras contra el servicio Cloud denominadas canales. Normalmente la salida se consigue a través del puerto 443, aunque se puede trabajar con un gran número de puertos o vía proxy. Estos canales son sockets TCP abiertos desde Java utilizando TLS v1.2. El captador entonces verifica la huella digital del certificado del servidor, el firmware del cliente cuenta con un keystore con 5 certificados que se utilizan para probar la identidad del servidor y aceptar la conexión con uno de los 5 certificados del servidor. Se explica con mayor detalle en el siguiente punto. Una vez establecido el canal seguro de comunicación, el dispositivo debe autenticarse utilizando un código y una clave de dispositivo. Si se autentica incorrectamente, se bloquea inmediatamente.
- **Gestión de la conexión de los captadores desde el Cloud:** se trata de una granja de servidores, en los que se ejecuta el código en Java de recepción de datos. Todos tienen el mismo código y la carga es gestionada mediante un algoritmo de balanceo distribuido, que los servidores administran de forma colaborativa. Cada DF abre un puerto de escucha, al que se conectan los dispositivos de captura y validan la conexión del dispositivo. La escucha se hace mediante un socket tipo servidor que se crea mediante un contexto TLS v1.2, cargando el certificado que en ese momento esté vigente. Para rotar y revocar certificados, se ha desarrollado un mecanismo que permite la rotación y la revocación sin necesidad de parada y evitando la necesidad de validación de la cadena de certificación y de entidades externas. Los certificados son creados en una máquina virtual controlada en las instalaciones de Savvy Data Systems. Se crean 5 certificados autofirmados, ya que el objetivo de los mismos no es permitir a los captadores la validación de la cadena

de certificación hasta una entidad firmante superior. En su lugar, los captadores validan la clave pública del certificado contra el almacén local de claves públicas válidas que tienen instalado. Cada uno de ellos utiliza un mecanismo criptográfico diferente. Se crean dos almacenes de claves diferentes. El primero irá instalado en los captadores, y contiene las 5 claves públicas. El segundo irá instalado en los DFs, y contiene únicamente el par de claves pública y privada que está vigente en este momento. También se crean 12 sobres sellados "ICE" (In Case of Emergency), siendo tres copias impresas de cada una de las 4 claves privadas de rotación/revocación. Cada uno de los sobres ICE indica su número de sobre y los mecanismos criptográficos utilizados. Las tres copias (cuatro sobres por copia) son entregadas a tres personas de alto cargo en la empresa (Director Gerente, Responsable de Área de Negocio, y Director Técnico), quienes las guardan en lugar seguro y secreto. Los sobres están debidamente codificados para que nadie ajeno a este procedimiento conozca su razón de ser ni su forma de aplicación. Por tanto, el almacén de claves de los captadores tiene cargadas las claves públicas firmadas de 5 certificados diferentes, siendo uno de ellos es el que está vigente (en uso por los servidores DF), y los otros 4 son usados para los casos en los que sea necesario ejecutar una rotación y/o revocación.

- **Gestión del login en la interfaz web:** siempre se redirecciona a HTTPS, aunque si bien el servidor web escucha en el puerto 80, solo se mantiene por compatibilidad. Se cuenta con un certificado válido emitido por COMODO RSA DomainValidationSecure Server CA. La clave es RSA de 2048 bits y el algoritmo usado para la firma es SHA256. Por otro lado, el servidor web solo acepta conexiones TLS v1.2. Para acceder a la información y a la gestión, se requiere de un acceso mediante login. El proceso de autenticación en dos pasos se encarga de verificar el dispositivo cuando un usuario se intenta identificar desde un dispositivo nuevo, enviándole un email a su cuenta de correo con un código. En caso de fallo en el código de verificación, se permiten tres intentos. Una vez superados, es necesario volver a comenzar con el proceso. Además, desde la propia plataforma, un usuario tiene la posibilidad de controlar y eliminar los dispositivos autorizados asociados a su cuenta. Tras 30 días sin conectarse desde un dispositivo, éste necesitará una nueva verificación. Una vez validadas las credenciales del usuario se envía un email con un código que hay que insertar para completar la verificación del dispositivo. La validación del login sigue dos pasos, primero se envía el usuario junto con un desafío creado en el formulario vía Ajax para evitar ataques tipo replay y se comprueba que existe en la base de datos. A continuación se comprueba que la clave enviada en el formulario coincide con la clave del usuario que ha devuelto en la consulta anterior. Las claves se almacenan en base de datos tras un proceso criptográfico con una salt aleatoria que es almacenada también. En caso de fallo al intentar identificarse o autenticarse, no se aporta más información que credenciales inválidas. Se tiene establecido un mecanismo de bloqueo por IP en el que tras múltiples fallos se bloquea dicha IP. En caso de que se haya realizado un bloqueo, el mensaje sigue siendo de credenciales inválidas, nunca se da más

información. Solo pueden eliminar los bloqueos los usuarios administradores de la plataforma.



SAVVY

# 2 DECLARACIONES DE CONFORMIDAD

## 2.1 Conformidad respecto a la norma CC

Esta Declaración de Seguridad cumple con lo indicado en la norma Common Criteria versión 3.1, Parte 2 release 5, y Parte 3 release 5, para un nivel de evaluación EAL1.

## 2.2 Conformidad respecto a Perfiles de Protección

Esta Declaración de Seguridad no declara el cumplimiento de ningún Perfil de Protección.

# 3 OBJETIVOS DE SEGURIDAD

## 3.1 Objetivos de seguridad para el entorno operacional

- 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.

# 4 DEFINICIÓN DE COMPONENTES EXTENDIDOS

No se definen componentes extendidos



SAVVY

# 5 REQUISITOS DE SEGURIDAD DEL TOE

## 5.1 Requisitos funcionales de seguridad

### *Class FDP*

- FDP_IFC Information Flow Control Policy
  - FDP_IFC.1 Subset information flow control, requires that each identified information flow control SFPs be in place for a subset of the possible operations on a subset of information flows in the TOE.
    - FDP_IFC.1.1 The TSF shall enforce the [**Savvy M2C information flow control SFP**] on [
      **Subjects: Savvy Smart Boxes**
      **Information: network packets of the communication established between the Savvy Smart Boxes and the cloud of Savvy Data Systems**
      **Operations: allow, deny**
      ].
- FDP_IFF Information Flow Control Functions
  - FDP_IFF.1 Simple security attributes, requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function, and describes how security attributes are derived by the function.
    - FDP_IFF.1.1 The TSF shall enforce the [**Savvy M2C information flow control SFP**] based on the following types of subject and information security attributes:
      [
      **Subject - Savvy Smart Boxes with security attributes: ID, password**
      **Information - network packets with security attributes: source IP address**
      **].**
    - FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**if the source IP address of the packets coming from the Savvy Smart Box is not blocked in the cloud and the ID and passwords of the Savvy Smart Box are correct, then the communication is allowed. Otherwise, the communication is denied**].
    - FDP_IFF.1.3 The TSF shall enforce the [**no additional rules**].
    - FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**no additional rules rules**].
    - FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**no additional rules**].

- FDP_ITT Internal TOE transfer
    - FDP_ITT.1 Basic Internal transfer protection, requires that user data be protected when transmitted between parts of the TOE.
        - FDP_ITT.1.1: The TSF shall enforce the [**Savvy M2C information flow control SFP**] to prevent the [**disclosure and modification**] of user data when it is transmitted between physically-separated parts of the TOE.

### *Class FIA*

- FIA_AFL Authentication failures
    - FIA_AFL.1 Authentication failure handling requires that the TSF be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry (e.g. workstation) from which the attempts were made until an administrator-defined condition occurs.
        - FIA_AFL.1.1: The TSF shall detect when [**five (5)**] unsuccessful authentication attempts occur related to [**failed login attemps**].
        - FIA_AFL.1.2: When the defined number of unsuccessful authentication attempts has been [**met**], the TSF shall [**block the IP address**].
- FIA_UAU User authentication
    - FIA_UAU.2 User authentication before any action, requires that users are authenticated before any other action will be allowed by the TSF.
        - FIA_UAU.2.1: The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
    - FIA_UAU.7 Protected authentication feedback, requires that only limited feedback information is provided to the user during the authentication.
        - FIA_UAU.7.1: The TSF shall provide only [**the character '*' for each character of the password**] to the user while the authentication is in progress.
- FIA_UID User identification
    - FIA_UID.2 User identification before any action, requires that users identify themselves before any other action will be allowed by the TSF.
        - FIA_UID.2.1: The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

### *Class FPT*

- FPT_ITT Internal TOE TSF data transfer
    - FPT_ITT.1 Basic internal TSF data transfer protection, requires that TSF data be protected when transmitted between separate parts of the TOE.

- The TSF shall protect TSF data from [**disclosure and modification**] when it is transmitted between separate parts of the TOE.

*Class FTA*

- FTA_SSL Session locking and termination
  - FTA_SSL.4 User-initiated termination, provides capabilities for the user to terminate the user's own interactive sessions.
    - FTA_SSL.4.1: The TSF shall allow user-initiated termination of the user's own interactive session.
- FTA_TSE TOE session establishment
  - FTA_TSE.1 TOE session establishment, provides requirements for denying users access to the TOE based on attributes.
    - FTA_TSE.1.1: The TSF shall be able to deny session establishment based on [**blocked IP and valid credentials**].

## 5.2 Requisitos de garantía de seguridad

El desarrollo y evaluación del TOE se realizará conforme al siguiente nivel de garantía:

- EAL1

| 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 |

## 5.3 Justificación de los Requisitos de garantía de seguridad

La garantía de seguridad deseada para este tipo de TOE según las exigencias del mercado es la proporcionada por el nivel de evaluación equivalente EAL1.

## 5.4 Dependencias de los Requisitos funcionales de seguridad

Todas las dependencias, tanto en los requisitos funcionales de seguridad como los de garantía se han satisfecho, salvo la dependencia del requisito de FDP_IFF.1 con FMT_MSA.3. El

TOE no implementa funcionalidad de gestión asociada a los atributos de seguridad de la política de control de flujo definida en FDP_IFF.1/FDP_IFC.1. Estos atributos de seguridad son establecidos por personal de Savvy en la fase previa de instalación y no son modificados durante la operación habitual del TOE.

# 6 ESPECIFICACIÓN RESUMIDA DEL TOE

A continuación se indica, para cada uno de los requisitos funcionales de seguridad, cómo son implementados por el TOE.

### *FDP_IFC.1 y FDP_IFF.1*

Cuando un captador se conecta contra el Cloud, éste envía sus credenciales de conexión (ID y password) únicas asignadas y dadas de alta en el sistema por el personal técnico de confianza de Savvy Data Systems durante el montaje del captador. El Cloud comprueba que la dirección IP del captador no está bloqueada y que las credenciales recibidas están dadas de alta en el sistema y son correctas. Si esto se cumple, se permite la comunicación entre el Cloud y el captador. En caso de que las credenciales sean incorrectas, se bloquea automáticamente dicha dirección IP. No se permite ningún fallo o intento adicional.

### *FDP_ITT.1 y FPT_ITT.1*

La comunicación entre captador y Cloud se realiza utilizando TLS v1.2. La comunicación Cloud-usuario se realiza también a través de TLS v1.2. Para FDP_ITT, se ha definido una nota de aplicación que explica cómo se controla la conexión.

### *FIA_AFL.1*

Tras 5 intentos fallidos de acceso desde la misma dirección IP, se bloquea dicha dirección IP desde la que se intenta acceder.

### *FIA_UAU.2*

Cuando se entra a la interfaz web, tanto a gestión como a presentación, lo primero que se solicita es el login (si tiene la opción de recordar credenciales, se entra directamente). En caso de que sea la primera vez que se entra desde ese dispositivo, se necesita validarlo mediante el mecanismo de autenticación en dos pasos.

### *FIA_UAU.7*

En caso de fallo en la autenticación o de estar bloqueado, el mensaje que se muestra siempre es el mismo: Invalid credentials.

### *FIA_UID.2*

Cuando se entra a la interfaz web, tanto a gestión como a presentación, lo primero que se solicita es el login (si tiene la opción de recordar credenciales, se entra directamente). En caso de que sea la primera vez que se entra desde ese dispositivo, se necesita validarlo mediante el mecanismo de autenticación en dos pasos.

### *FTA_SSL.4*

El usuario, tanto usuario común como usuario administrador, a través de la plataforma, puede eliminar un dispositivo autorizado desde el que ha accedido, incluido el dispositivo desde el

que está conectado. En ese caso, se le cerrará su sesión y será necesario que se acredite de nuevo.

### *FTA_TSE.1*

Para denegar el establecimiento de sesión, se comprueba si una IP está bloqueada o no. También se comprueba si las credenciales de acceso son válidas.



SAVVY