AuthenTest©

Declaración de Seguridad

Índice

Introducción a la declaración de seguridad

Referencia de la declaración de seguridad

Documento A_clt_01_v06_Declaracion de seguridad, numero de versión 06, fecha 10/05/2010.
Autor Authenware

Referencia del TOE

Nombre del producto: Authentest Server

Version: 1.2.6

Introducción al TOE

Uso del TOE

El TOE es un conjunto de funcionalidades y subsistemas que provee Authentest para proteger al servicio de verificación biométrica de ataques que impidan su normal funcionamiento.

Las funcionalidades del TOE incluyen:

- la capacidad de repeler los ataques de denegación de servicio y de repetición ilegítima de ingresos ya recibidos (ataques de repetición o replay attacks)
- la capacidad de controlar el acceso al servicio web de verificación biométrica desde software externo que se conecte con el certificado digital adecuado.
- la capacidad de importar los certificados digitales que serán tomados como válidos en el momento de acceso.
- la capacidad de cifrar los patrones biométricos mediante la utilización del algoritmo AES con el fin de preservar su confidencialidad.
- la capacidad de generar registros de auditoría sobre las operaciones críticas del producto.
- la capacidad de consultar los registros de auditoría para su adecuado análisis.
- la capacidad de almacenar afuera del TOE tanto la base de datos de patrones biométricos de comportamiento e ingreso como los registros de auditoría, permitiendo así al cliente aplicar su infraestructura y políticas de seguridad y auditoria vigentes.

El producto: Authentest provee un servicio de verificación de identidad mediante biometría comportamental basada en el ritmo de tipeo de los usuarios que operan a través de aplicaciones externas al TOE. Si bien su principal aplicación es la validación biométrica al momento de la autenticación mediante nombre de usuario y contraseña, Authentest está preparado para trabajar con cualquier dato o campo que se desee validar biométricamente. Por ejemplo, frases de paso, solo el nombre de usuario, etc.

Authentest devuelve, a través de la consulta a un servicio web estándar, si la persona que ha tipeado es quien dice ser o no (0 o 1) acompañado por el porcentaje de confianza sobre esta afirmación. Para tomar esta decisión, Authentest compara el ingreso actual contra un patrón biométrico comportamental que incluye tres dimensiones principales:

El ritmo de tipeo (Tiempos de intervalo entre dos teclas y tiempos de detención de cada una)

Información del entorno habitual (IP, Sistema operativo, Navegador, etc.)

Comportamiento oculto o inconsciente tales como si el usuario legítimo utiliza la tecla <Tab> o el mouse para pasar del campo usuario a la contraseña, que días de la semana y a qué hora es esperable su ingreso, etc.

Las características principales de seguridad del producto son las siguientes: los clientes lo utilizarán como segundo factor de autenticación debido a que la validación biométrica con Authentest se realizará luego de haber verificado contra algún servicio de directorio o base de datos que los datos tipeados coincidan. Por ejemplo, se verifica que el nombre de usuario y contraseña coincidan (primer factor) y luego se verifica biométricamente (segundo factor).

Gracias a su diseño, Authentest no requiere conocer el nombre real del usuario ni su contraseña. Authentest no almacena ni manipula estos datos sensibles del cliente, no aumentando así las vulnerabilidades referidas a la confidencialidad e integridad de estos datos.

Por tratarse de un segundo factor de autenticación y por como Authentest ha sido diseñado, permite que en caso de fallo de Authentest, este no interferirá con la operatividad del sistema y/o del negocio si las reglas de negocio fueron correctamente expresadas.

Adicionalmente, Authentest ha sido diseñado para adecuarse a cinco niveles de seguridad que pueden ser configurados de manera jerárquica partiendo desde el nivel de sistema, por aplicación del cliente, por usuario, y por transacción específica.

Nota: los ratios de efectividad del algoritmo de autenticación (FAR, FRR, EER, etc.) han sido oportunamente evaluados y certificados por el International Biometric Group (www.biometricgroup.com) y no son objeto de esta evaluación, sino que sí lo son los mecanismos que permiten que funcione de manera correcta y segura como la confidencialidad e integridad del patrón de comportamiento y la integridad de los parámetros de configuración.

Tipo de TOE:

El TOE es un conjunto de funcionalidades y subsistemas que provee Authentest para la protección del servicio de verificación biométrica contra ataques que impidan su normal funcionamiento.

Hardware y software requerido por el TOE

El TOE necesita de los siguientes elementos de software para su correcta y segura ejecución:

- RedHat Enterprise 5.4
- Openssh Server 4.3
- JAVA 1.6.0_07

Una configuración compatible de Hardware con los requerimientos anteriores como por ejemplo la siguiente:

- Procesador doble núcleo 1.5 GHz o superior
- 4 GB de memoria
- HDD 40 GB o más, SCSI, SATA o SAS.
- Placa de Red compatible con RedHat Enterprise 5.4
- Lector DVD

También se requiere un servidor de base de datos que cuente con Mysql 5.0 y otro servidor de logs compatible con syslogd 1.4.1 o superior. Ambos de de configuraciones de hardware similares a la anteriormente descripta.

Descripción del TOE

El siguiente esquema muestra el TOE con los elementos de entorno:

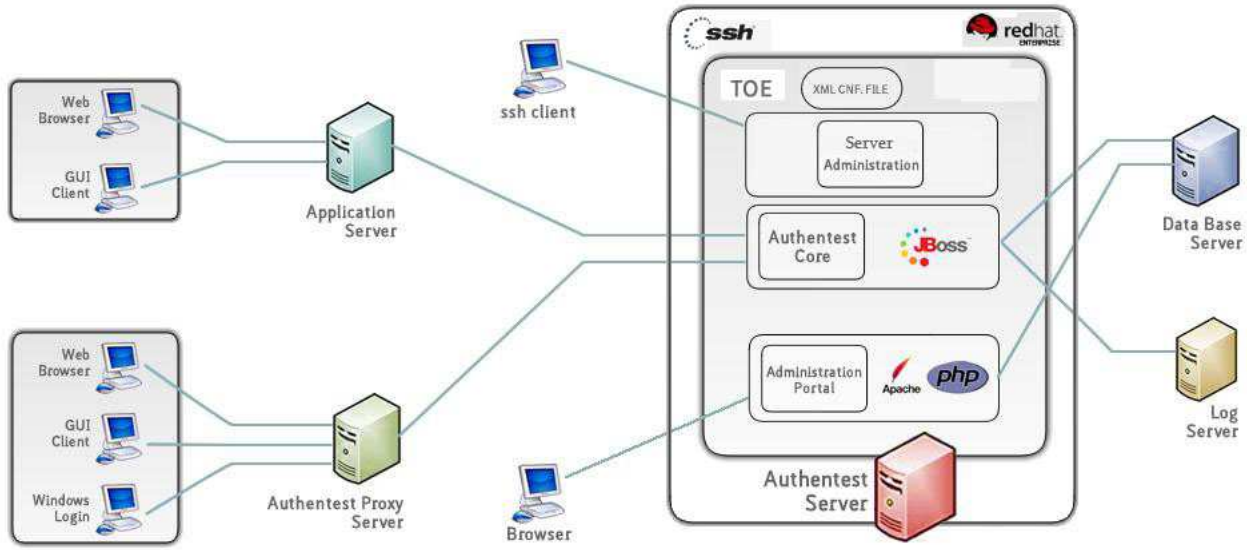

Figura - Descripción del TOE (Componentes: JBoss 4.2.3 GA, Apache 2.2.3-31, Php 5.2.10.1, Authentest Core, Administration Portal, Server Administration)

Los componentes que conforman al TOE son los siguientes:

- JBoss 4.2.3 GA: Servidor de Aplicaciones que utiliza Authentest Server para ejecutar sus servicios web.
- Apache 2.2.3-31: Servidor Web que utiliza Authentest Server para ejecutar su portal de administración.
- PHP 5.2.10.1: Lenguaje de scripts para aplicaciones web utilizado en el portal de administración.
- Authentest Core: Implementa los servicios web desplegados por Authentest Server. Este componente es un .war instalado en el servidor JBoss.
- Administration Portal: Implementa las funcionalidades del portal web de administración de Authentest Server. Este componente es un conjunto de scripts .php desplegados en el servidor Apache.
- Server Administration: Implementa la funcionalidad de administración, a nivel de servidor, de Authentest Server. Este componente es un archivo ejecutable binario, desarrollado en Python, con interfaz carácter, ejecutable desde SSH.

Como repositorios de los patrones de comportamiento y los datos de auditoría se utilizaran sendos servidores remotos de base de datos y de syslog, sin que la confidencialidad de los patrones dependa de la seguridad de la base de datos o del log, debido a que los patrones son previamente cifrados.

Relación de características de seguridad

Para garantizar la seguridad del servicio de autenticación basado en el comportamiento, el TOE implementa los siguientes mecanismos de seguridad:

Control de acceso al portal de administración

Autenticación fuerte basada en PKI para acceso a los web-services

De manera adicional Authentest registra los eventos principales relativos a la seguridad del servicio.

Cifrado de los patrones de comportamiento, como garantía de su confidencialidad.

Autenticación del administrador de la máquina, para la segura y correcta activación y posteriores cambios de configuración, se delega al Sistema Operativo y se accede a través de SSH, por lo tanto es una característica de seguridad que proporciona el entorno, sistema operativo y ssh.

Declaración de Conformidad

Conformidad con respecto a Common Criteria

Esta declaración de seguridad es conforme a la norma Common Criteria versión 3.1 release 3 partes 2 y 3. No se han utilizado componentes extendidos.

Cumplimiento de perfiles de protección

Esta declaración de seguridad no reclama cumplimiento de ningún perfil de protección al ajustarse a las propiedades específicas del producto y no existir perfil de protección aplicable.

Cumplimiento de paquetes de garantía

Esta declaración de seguridad declara cumplir con el paquete EAL2 aumentado con el componente ALC_FLR.1.

Definición del problema de seguridad

Activos

A1. La confidencialidad del patrón de comportamiento biométrico. Un patrón de comportamiento biométrico es la síntesis de los últimos n ingresos positivos de un usuario con un determinado conjunto de campos (Ej. usuario y contraseña). Este patrón es la referencia biométrica dinámica contra la que se compara cada ingreso permitiendo determinar la legitimidad del usuario con un nivel de confianza determinado.

A2. La confidencialidad de los parámetros de configuración del algoritmo de reconocimiento y de los ficheros de configuración del servicio Authentest. Estos parámetros son:

Nivel de seguridad: Ajusta el nivel de seguridad/sensibilidad dentro de 5 posibilidades:

High operative (1): Para aplicaciones con bajos requerimientos de seguridad pero con alta necesidad de operatividad. Esto implica mayor tasa de falsos positivos y menor tasa de falsos negativos

Operative (2): Este nivel es un punto intermedio entre el nivel anterior y el siguiente.

Secure (3): En este nivel la probabilidad de falsos positivos y falsos negativos está balanceada. Recomendado para la mayoría de las aplicaciones tradicionales.

High secure (4): Este nivel es un punto intermedio entre el nivel anterior y el siguiente.

Paranoid (5): Para aplicaciones con altos requerimientos de seguridad pero con baja necesidad de operatividad. Esto implica menor tasa de falsos positivos y mayor tasa de falsos negativos.

Modo de operación: Determina el modo de operación, este puede ser stealth (oculto) o normal. Si se selecciona stealth el servicio getTrust responderá siempre de manera positiva pero registrará los resultados reales, que podrán visualizarse en el portal de administración.

Fuentes de Datos: Parametriza los orígenes de datos necesarios para leer y almacenar los patrones de comportamiento biométricos y otros datos requeridos para la ejecución de los servicios.

A3. La disponibilidad del servicio frente a ataques lógicos provenientes de fuentes no confiables externas.

Amenazas

T1. Un agente externo a la administración del sistema no autorizado, compromete la confidencialidad del patrón de comportamiento biométrico.

T2. Un agente externo a la administración del sistema no autorizado, compromete la confidencialidad de los parámetros de configuración del TOE degradando la seguridad del mismo en su servicio.

T3. Un agente externo en una red no confiable deniega el servicio de identificación basado en el comportamiento utilizando técnicas y ataques de denegación de servicios remotas, imposibilitando el acceso al servicio por parte de los usuarios de Authentest, utilizando firmas de comportamiento falsas o mediante replay attack.

Políticas organizativas de seguridad

P1. El entorno de uso del TOE garantizara la existencia de los siguientes roles y capacidades:

Administrador de consola: puede realizar la activación del producto y su configuración básica.

Usuario Authentest: puede realizar la configuración de los parámetros del entorno de red, arrancar o detener el servicio JBoss, configurar el URL del web-service, configurar la distribución de teclado del sistema operativo del TOE, cambiar su propia password, cambiar las reglas de firewall y administrar los certificados digitales utilizados por el web-service.

Aplicación web-service remota: invoca la funcionalidad de autenticación basada en el comportamiento humano a través de los métodos del servicio web ofrecidos por el TOE así como el resto de los métodos que permiten la gestión de los usuarios de las aplicaciones remotas y sus respectivos patrones biométricos. Puede ser cualquier entidad externa, como un servidor de aplicaciones o un proxy, que en todo caso se autentica por certificado e invoca los servicios web.

Roles para el portal web:

Administrador de grupo: cuenta con los privilegios necesarios para administrar usuarios y aplicaciones que pertenezcan al grupo de aplicaciones que administra.

Administrador de portal: este usuario es el que cuenta con los privilegios para crear grupos de aplicaciones, usuarios administradores de grupo, otros usuarios administradores de portal, lectura de toda la actividad, ver registros de auditoría del portal, cambiar el nivel de seguridad de Authentest Server , aplicaciones y usuarios, y activar o desactivar el modo de funcionamiento silencioso.

P2. El TOE generará trazas de auditoría de actividad del servicio de autenticación y relativas a la funcionalidad del TOE, para la integración en los sistemas de gestión del usuario con el TOE.

P3. El TOE identificará su versión y la condición de producto certificado en la consola y página principal del portal web, así como advertirá de las responsabilidades sobre el uso del producto utilizado o configurado de manera insegura.

Hipótesis

H1. Como todos los métodos biométrico comportamentales (Por ej.: reconocimiento de la voz o la firma) la fiabilidad del algoritmo, en lo que a falsos negativos o rechazos erróneos se refiere, depende fuertemente de la colaboración del usuario de la aplicación remota, que deberá seguir las siguientes recomendaciones equivalentes a cuando se va a firmar un cheque y se quiere evitar el rechazo del banco por no reconocer la firma como legitima:

Tipear naturalmente, evitando forzar una velocidad mayor o menor a la habitual durante el entrenamiento del patrón biométrico y en los sucesivos ingresos.

En el momento de ingresar los datos observados biométricamente evitar realizar otra actividad que pueda alterar la naturalidad del ritmo habitual (hablar por teléfono, tipear con una sola mano, etc.)

Utilizar palabras que resulten naturales y reconocidas que impliquen un tipeo natural.

En caso de utilizar números tener presente que el patrón biométrico de tipeo varía si se utiliza una vez el teclado numérico y otra vez los números arriba de las letras.

Siempre que sea posible, utilizar la misma máquina y entorno. Mismo teclado, sistema operativo, navegador (en caso de aplicaciones Web), etc.

H2. La generación y distribución de los certificados y claves para el servidor de aplicaciones se realiza mediante una tercera entidad externa de confianza, con el nivel de seguridad acorde a cada instalación en particular.

H3. Los servidores de aplicación remotos que consumen los servicios de Authentest son responsables de garantizar la confidencialidad e integridad de los certificados con los que se realiza la autenticación.

H4. La fiabilidad en el uso e integración de los servicios de Authentest en los servidores de aplicaciones remotos dependen de la seguridad y buenas prácticas de dichas entidades externas. Por lo anterior se considera como confiables a los servidores de aplicación remotos.

H5. El acceso físico al servidor está restringido a los administradores de Authentest, usuario administrador de consola y usuario Authentest, que son considerados como usuarios confiables en todas sus operaciones. Así también los usuarios administradores de Authentest, usuario administrador del portal y usuario administrador de grupo, que ingresan a través del portal de administración, son considerados como usuarios confiables en todas sus operaciones.

H6. La fiabilidad en el uso de Authentest depende de la seguridad y buenas prácticas implementadas en el sistema de gestión de bases de datos externo, en donde se almacenan los patrones de comportamiento biométrico. Por lo anterior se considera que dicho sistema es confiable y está bien configurado.

H7. El sistema operativo deberá estar configurado de manera que realice correctamente la política de control de acceso a la aplicación “Server Administration”.

Objetivos de Seguridad

Objetivos de seguridad para el TOE

OT1. El TOE protegerá mediante los mecanismos de cifrado apropiados, la confidencialidad de los patrones de comportamiento cuando estos sean exportados a su repositorio externo.

OT2. El TOE implementara los roles y capacidades expresados por la política de seguridad P1, mediante la correspondiente política y funciones de control de acceso, gestión de la seguridad, y demás funciones requeridas.

OT3. El TOE protegerá la confidencialidad frente a agente no autorizados de los parámetros del sistema.

OT4. El TOE establecerá los sistemas de medida y distribución de la carga de los servicios web ofrecidos para evitar ataques de denegación de servicio y detección de replay attacks.

OT5. El TOE generará trazas de auditoría de actividad del servicio de autenticación, y relativas a la funcionalidad del TOE, para la integración en los sistemas de gestión del usuario del TOE.

OT6. El TOE identificará su versión y la condición de producto certificado en la consola y página principal del portal web, así como advertirá de las responsabilidades sobre el uso del producto utilizado o configurado de manera insegura.

Objetivos de seguridad para el entorno operacional

OE1. El entorno de uso deberá garantizar la fiabilidad del algoritmo de autenticación basado en el comportamiento, comunicando fehacientemente a todos los usuarios las siguientes recomendaciones:

Tipear naturalmente, evitando forzar una velocidad mayor o menor a la habitual durante el entrenamiento del patrón biométrico y en los sucesivos ingresos.

En el momento de ingresar los datos observados biométricamente evitar realizar otra actividad que pueda alterar la naturalidad del ritmo habitual (hablar por teléfono, tipear con una sola mano, etc.)

Utilizar palabras que resulten naturales y reconocidas que impliquen un tipeo natural.

En caso de utilizar números tener presente que el patrón biométrico de tipeo varía si se utiliza una vez el teclado numérico y otra vez los números arriba de las letras.

Siempre que sea posible, utilizar la misma máquina y entorno. Mismo teclado, sistema operativo, navegador (en caso de aplicaciones Web), etc.

OE2. El entorno de uso deberá garantizar la generación y distribución de los certificados y claves para el servidor de aplicaciones que se realiza mediante una tercera entidad externa de confianza, con el nivel de seguridad acorde a cada instalación en particular.

OE3. El entorno de uso deberá garantizar la confidencialidad e integridad de los certificados con los que se realiza la autenticación. El cliente deberá garantizar la generación de los certificados con herramientas externas al TOE y copiarlos al TOE utilizando protocolo SSH. El cliente deberá garantizar la generación y distribución segura de de los certificados necesarios para invocar el web-service del TOE.

OE4. El TOE deberá tener comunicación con el cliente que consumirá el web-service en una red de datos separada de la red del cliente. En caso de no contar con una red separada debe de aislarse en un segmento de VLAN. A esta red de datos podrá también conectarse el servidor de base de datos, servidor de log (syslog) remoto y el equipo desde donde se podrá administrar el TOE mediante ssh

y/o Portal de Administración. El acceso al TOE para su administración deberá realizarse desde un equipo conectado a la red de datos. En todos los casos se recomienda disponer de un solo punto de acceso a la red, sea la red de cliente o red de datos, e implementar mecanismos de filtrado que se basen en una política de denegación por defecto.

OE5. El cliente deberá garantizar que el acceso físico al servidor está restringido a los administradores de Authentest, como así también que estos puedan ser considerados como usuarios confiables (usuario administrador de consola, usuario Authentest, usuario administrador del portal y usuario administrador de grupo).

OE6. El entorno de uso deberá garantizar que el sistema de gestión de bases de datos externos, en donde se almacenan los patrones de comportamiento biométrico sea confiable y este bien configurado.

OE7. El entorno de uso deberá garantizar que el sistema operativo este configurado de manera que realice correctamente la política de control de acceso a la aplicación “Server Administration”.

Justificación de los objetivos

La correspondencia entre los objetivos de seguridad para el TOE y las amenazas y políticas de seguridad son las siguientes:

	OT1	OT2	OT3	OT4	OT5	OT6
T1	X					
T2			X			
T3				X		
P1		X				
P2					X	
P3						X

El objetivo OT1 permite garantizar la confidencialidad de los patrones de comportamiento cuando se exportan a una base de datos externa al TOE, impidiendo la amenaza T1, que queda fuera del potencial de ataque aplicable.

El objetivo OT2 permite implementar los roles y capacidades expresados por la política organizativa de seguridad P1, mediante la correspondiente política y funciones de control de acceso, gestión de la seguridad, y demás funciones requeridas.

El objetivo OT3 permite proteger la confidencialidad frente a agentes no autorizados de los parámetros impidiendo las amenazas T2, quedando estas fuera del potencial de ataque aplicable.

El objetivo OT4 permite establecer los sistemas de medida y distribución de la carga de los servicios web, impidiendo la amenaza T3, quedando esta fuera del potencial de ataque aplicable.

El objetivo OT5 permite generar trazas de auditoría de actividad del servicio de autenticación, así como las relativas a la funcionalidad para los sistemas de gestión del usuario del TOE, cumpliendo con la política organizativa P2 de generación de trazas.

El objetivo OT6 permite la identificación de la versión del TOE, condiciones de producto certificado en la consola y página principal del portal de administración y advertir sobre las responsabilidades en el uso del producto utilizado o configurado de manera insegura, permitiendo cumplir con la política de organizativa P3

La correspondencia entre los objetivos de seguridad del entorno y las hipótesis de seguridad son las siguientes:

	OE1	OE2	OE3	OE4	OE5	OE6	OE7
H1	X						
H2		X					
H3			X				
H4				X			
H5					X		
H6						X	
H7							X

La correspondencia entre las hipótesis de entorno y los correspondientes objetivos de seguridad es trivial.

El objetivo de seguridad del entorno OE1 soporta directamente la suposición H1.

El objetivo de seguridad del entorno OE2 soporta directamente la suposición H2.

El objetivo de seguridad del entorno OE3 soporta directamente la suposición H3.

El objetivo de seguridad del entorno OE4 soporta la suposición H4 ya que el colocar los servidores en una red separada de la red del cliente es una buena práctica para garantizar la fiabilidad en el uso e integración de los servidores de Authentest con los servidores de aplicaciones remotas.

El objetivo de seguridad del entorno OE5 soporta directamente la suposición H5.

El objetivo de seguridad del entorno OE6 soporta directamente la suposición H6.

El objetivo de seguridad del entorno OE7 soporta directamente la suposición H7.

Requisitos de seguridad

Requisitos funcionales de seguridad

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 **The TSF shall be able to generate an audit record of the following auditable events:**

1. **Start-up and shutdown of the audit functions;**
2. **All auditable events for the [selection, choose one of: not specified] level of audit; and**
3. **[assignment:**

Funcionalidad	Eventos
WEBSERVICE	**getTrust**
PORTAL ADMINISTRACION	**ApplicationCreate** **ApplicationUpdate** **ApplicationDelete** **UserCreate** **UserUpdate** **UserDelete** **UserChangePassword** **GroupOfApplicationsCreate** **GroupOfApplicationsUpdate** **GroupOfApplicationsDelete** **FieldCreate** **FieldUpdate** **FieldDelete** **SecurityLevelChange** **ModeChange**
INTEGRITY CONTROLLER	**CheckIntegrity**

].

FAU_GEN.1.2 **The TSF shall record within each audit record at least the following information:**

1. **Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and**

2. **For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information***

Funcionalidad	Datos auditados
WEBSERVICE	**date/time, user, application, field, trust identity rate, quality personal record, pattern id, result, ip, isp, time zone, use tab, use enter**
PORTAL ADMINISTRACION	**date/time, ip, user, event**
INTEGRITY CONTROLLER	**date/time, type, error**

].

FAU_SAR.1_WEB-SERVICES Audit review

FAU_SAR.1.1 **The TSF shall provide [assignment: todos los usuarios del portal web] with the capability to read [assignment: registro de auditoría de la actividad de autenticación del grupo de aplicaciones asociada al usuario] from the audit records.**

FAU_SAR.1.2 **The TSF shall provide the audit records in a manner suitable for the user to interpret the information.**

FAU_SAR.1_ADMIN Audit review

FAU_SAR.1.1 **The TSF shall provide [assignment: Administrador del portal de administración] with the capability to read [assignment: registro de auditoría de la actividad de uso de las funcionalidades del portal de administración por parte de los usuarios del portal de administración] from the audit records.**

FAU_SAR.1.2 **The TSF shall provide the audit records in a manner suitable for the user to interpret the information.**

FAU_SAR.1_SSH Audit review

FAU_SAR.1.1 **The TSF shall provide [assignment: usuario Authentest y usuario administrador de consola] with the capability to read [assignment: registro de auditoría de la actividad del chequeo de integridad al arranque] from the audit records.**

FAU_SAR.1.2 **The TSF shall provide the audit records in a manner suitable for the user to interpret the information.**

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 **The TSF shall provide the ability to apply [assignment: ordenación y filtro por campos] of audit data based on [assignment: valores del juego de caracteres].**

FDP_ACC.2_WEB-SERVICES Complete access control

FDP_ACC.2.1 The TSF shall enforce the [assignment: **Política de acceso a los web-services**] on [assignment:

Sujetos: Servidores de aplicaciones remotos
Objetos: Servicios exportados como web-service

] and all operations among subjects and objects covered by the **SFP.**

FDP_ACC.2.2 **The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.**

FDP_ACC.2_PORTAL_ADMINISTRACION Complete access control

FDP_ACC.2.1 The TSF shall enforce the [assignment: **Política de acceso al portal de**

administración] on [assignment:

Sujetos: usuarios del portal web
Objetos: portal de administración

] and all operations among subjects and objects covered by the **SFP.**

FDP_ACC.2.2 **The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.**

FDP_ACF.1_WEB-SERVICES Security attribute based access control

FDP_ACF.1.1 **The TSF shall enforce the [assignment: Política de acceso a los web-services] to objects based on the following: [assignment:**

Sujetos: Servidores de aplicaciones remotes, atributos: identidad del servidor de aplicación basada en su certificado.
Objetos: Servicios exportados como web-service, atributos el nombre de método.]

FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:**

1- **La aplicación remota podrá invocar web-services tras su autenticación mediante el certificado.**
2- **El resultado de la invocación de cada web-service particular se atiene a la funcionalidad de cada uno de ellos.]**

FDP_ACF.1.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: ninguna].**

FDP_ACF.1.4 **The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Cualquier otra combinación].**

FDP_ACF.1_PORTAL_ADMINISTRACION Security attribute based access control

FDP_ACF.1.1 **The TSF shall enforce the [assignment: Política de acceso al portal de administración] to objects based on the following: [assignment:**

Sujetos: usuarios del portal de administración, atributos: rol y grupo de aplicaciones autorizadas.
Objetos: Funcionalidad y datos del portal de administración, atributos: la identidad de la pantalla, la identidad del grupo de aplicaciones y el rol.]

FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:**

1- **El usuario podrá acceder a las pantallas del portal autorizadas por rol.**
2- **El usuario podrá accede a la información del portal, filtrada por el grupo de la aplicación a la que tenga acceso.]**

FDP_ACF.1.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: ninguna].**

FDP_ACF.1.4 **The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Cualquier otra combinación].**

FMT_MSA.1_PORTAL_ADMINISTRACION Management of security attributes

FMT_MSA.1.1 **The TSF shall enforce the [assignment: Política de acceso al portal de administración [selection: alta y baja] the security attributes [assignment: identidad y rol de cualquier usuario del portal de administración (1), identidad y rol de administradores del mismo grupo del portal de administración (2)] to [assignment: administrador del portal de administración para (1), administrador de grupo del portal de administración para (2)].**

FMT_MSA.1_WEB-SERVICES Management of security attributes

FMT_MSA.1.1 **The TSF shall enforce the [assignment: Política de acceso a los servicios web[selection: alta y baja] the security attributes [assignment: certificado raíz para la autenticación de las aplicaciones web to [assignment: el usuario Authentest y el administrador de consola a través de la consola ssh].**

FMT_MSA.3_PORTAL_ADMINISTRACION Static attribute initialization

FMT_MSA.3.1 **The TSF shall enforce the [assignment: Política de control de acceso al portal de administración] to provide [selection, choose one of: restrictive] default values for security attributes that are used to enforce the SFP.**

FMT_MSA.3.2 **The TSF shall allow the [assignment: administradores del portal] to specify alternative initial values to override the default values when an object or information is created.**

FMT_MSA.3_WEB-SERVICES Static attribute initialization

FMT_MSA.3.1 **The TSF shall enforce the [assignment: Política de control de acceso a servicios web] to provide [selection, choose one of: restrictive] default values for security attributes that are used to enforce the SFP.**

FMT_MSA.3.2 **The TSF shall allow the [assignment: el administrador de consola y el usuario Authentest] to specify alternative initial values to override the default values when an object or information is created.**

FMT_SMR.1 Security roles

FMT_SMR.1.1 **The TSF shall maintain the roles [assignment:**

Administrador de consola: puede realizar la activación del producto y su configuración básica.

Usuario Authentest: puede realizar la configuración de los parámetros del entorno de red , arrancar o detener el servicio JBoss, configurar el URL del endpoint del web-service, configurar el layout de teclado, cambiar su propia password, cambiar las reglas de firewall y administrar los certificados digitales utilizados el web-service.

Aplicación Web-service remota: invoca la funcionalidad de autenticación basada en el comportamiento humano a través de los métodos del web-service exportados por el TOE así como el resto de los métodos que permiten la gestión de los usuarios de las aplicaciones remotas y sus respectivos patrones biométricos.

Roles para el portal web:

Administrador de grupo: cuenta con los privilegios necesarios para administrar usuarios y aplicaciones que pertenezcan al grupo de aplicaciones que administra. También visualizar los registros de auditoría de solicitudes de autenticación biométrica en las aplicaciones incluidas en el grupo que administra.

Administrador de portal: este usuario es el que cuenta con los privilegios para crear grupos de aplicaciones, usuarios administradores de grupo, otros usuarios administradores de portal, lectura de toda la actividad, visualizar todos los registros de auditoría de solicitudes de autenticación biométrica, ver registros de auditoría de uso del portal, cambiar el nivel de seguridad de Authentest Server y el activar o desactivar el modo de funcionamiento silencioso.

FMT_SMR.1.2 **The TSF shall be able to associate users with roles.**

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 **The TSF shall be capable of performing the following management functions: [assignment:**

1- **Gestión de parámetros de configuración del TOE, conforme a la Política de control de acceso a la consola, cuya lógica se delega en el entorno, sistema operativo y ssh.**
2- **Gestión de roles y capacidades, conforme a la Política de control de acceso al portal.**

Nota: No existen funciones de gestión del TOE a través de web-services

FIA_UAU.2_ WEB-SERVICES User authentication before any action

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.1_PORTAL_ADMINISTRACION Timing of authentication

FIA_UAU.1.1 **The TSF shall allow [assignment: acceso a la pantalla ServiceStatus] on behalf of the user to be performed before the user is authenticated.**

FIA_UAU.1.2 **The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.**

FIA_UID.2_WEB-SERVICES User identification before any action

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.

FIA_UID.1_PORTAL_ADMINISTRACION Timing of identification

FIA_UID.1.1 **The TSF shall allow [assignment: acceso a la pantalla ServiceStatus] on behalf of the user to be performed before the user is identified.**

FIA_UID.1.2 **The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.**

FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 **The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product (Servicio de almacenamiento de patrones de comportamiento) from unauthorised disclosure during transmission.**

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 **The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.**

FTP_ITC.1.2 **The TSF shall permit [selection: el servidor de aplicaciones remoto] to initiate communication via the trusted channel.**

FTP_ITC.1.3 **The TSF shall initiate communication via the trusted channel for [assignment: acceso a los web-services].**

FPT_RPL.1 Replay detection

FPT_RPL.1.1 **The TSF shall detect replay for the following entities: [assignment: solicitudes de autenticación getTrust() sobre web-services, detectando la igualdad de la firma suministrada con respecto a la lista de las firmas anteriores, de número configurable durante la instalación].**

FPT_RPL.1.2 **The TSF shall perform [assignment: el servicio devuelve un código de error con la identificación de la condición anómala] when replay is detected.**

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 **The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: generación de una firma de la plataforma del TOE] and specified cryptographic key sizes [assignment: 256bits] that meet the following: [assignment: la firma es generada a partir de las características del hardware del servidor y es utilizada para cifrar con AES el sistema de archivos donde se encuentran los parámetros de configuración].**

FDP_ITC.1_IMPORTACION_CERTIFICADOS Import of user data without security attributes

FDP_ITC.1.1 **The TSF shall enforce the [assignment: Política de control de acceso a la consola] when importing user data, controlled under the SFP, from outside of the TOE.**

FDP_ITC.1.2 **The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.**

FDP_ITC.1.3 **The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: importación de certificados conforme a los mecanismos y formato del servidor de aplicaciones jBoss].**

NOTA DE APLICACIÓN 1:

La política que se referencia en el requisito, la ejercita el sistema operativo fuera del TOE y es necesaria para que el usuario administrador de consola y el usuario Authentest se les conceda el acceso que les permitirá ejercitar la funcionalidad importación de certificados, implementada en el TOE. Razón por la cual no se satisface la dependencias FDP_ACC.1 y FMT_MSA.1

FDP_ITC.1 CIFRADO_PATRONES_BIOMETRICOS Import of user data without security attributes

FDP_ITC.1.1 **The TSF shall enforce the [assignment: Política de control de acceso a la consola] when importing user data, controlled under the SFP, from outside of the TOE.**

FDP_ITC.1.2 **The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.**

FDP_ITC.1.3 **The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: importación de clave de cifrado AES en el momento de la instalación].**

NOTA DE APLICACIÓN 2:

La política que se referencia en el requisito, la ejercita el sistema operativo fuera del TOE y es necesaria para que el usuario administrador de consola y el usuario Authentest se les conceda el acceso que les permitirá importar la clave de cifrado AES en el momento de la instalación, implementada en el TOE. Razón por la cual no se satisface la dependencias FDP_ACC.1 y FMT_MSA.1

FCS_COP.1_AES _CIFRADO_SISTEMA_FICHEROS Cryptographic operation

FCS_COP.1.1 **The TSF shall perform [assignment: cifrado y descifrado de los activos A2] in accordance with a specified cryptographic algorithm [assignment: AES] and cryptographic key sizes [assignment: 256bits] that meet the following: [assignment: none].**

FCS_COP.1_AES _CIFRADO_PATRONES_BIOMETRICOS Cryptographic operation

FCS_COP.1.1 **The TSF shall perform [assignment: cifrado y descifrado de los activos A1] in accordance with a specified cryptographic algorithm [assignment: AES] and cryptographic key sizes [assignment: 256bits] that meet the following: [assignment: none].**

FCS_COP.1_RSA Cryptographic operation

FCS_COP.1.1 **The TSF shall perform [assignment: cifrado y descifrado asimétrico del canal de comunicación con los webservices del producto] in accordance with a specified cryptographic algorithm [assignment: RSA] and cryptographic key sizes [assignment: 4096bits] that meet the following: [assignment: none].**

FPT_TST.1 TSF testing

FPT_TST.1.1 **The TSF shall run a suite of self tests [selection: at the request of the authorised user] to demonstrate the correct operation of [parts of TSF]].**

FPT_TST.1.2 **The TSF shall provide authorised users with the capability to verify the integrity of [selection: none].**

FPT_TST.1.3 **The TSF shall provide authorised users with the capability to verify the integrity of [selection: none].**

FTA_TAB.1_PORTAL_ADMINISTRACION Default TOE access banners

FTA_TAB.1.1 **Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.**

FRU_RSA.1 Maximum quotas

FRU_RSA.1.1 **The TSF shall enforce maximum quotas of the following resources: [assignment: *solicitudes web-services*] that [selection: *aplicaciones web-service remotas*] can use [selection: *simultaneously*].**

Requisitos de garantía de seguridad

El TOE se evaluará conforme a los requisitos de garantía de seguridad EAL2+ALC_FLR.1.

Assurance Class	Assurance components
ADV	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA	AVA_VAN.2 Vulnerability analysis
ALC	ALC_FLR.1 Flaw remediation

Justificación de los requisitos

La siguiente tabla establece la correspondencia entre los objetivos de seguridad a satisfacer por el TOE y los requisitos funcionales de seguridad aplicables.

	OT1	OT2	OT3	OT4	OT5	OT6
FAU_GEN.1 AUDIT					X	
FAU_SAR.1_WEB-SERVICES					X	
FAU_SAR.1_ADMIN					X	
FAU_SAR.1_SSH					X	
FAU_SAR.3					X	
FDP_ACC.2_WEB-SERVICES		X				
FDP_ACC.2_PORTAL_ADMINISTRACION		X				
FDP_ACF.1_WEB-SERVICES		X				
FDP_ACF.1_PORTAL_ADMINISTRACION		X				
FMT_MSA.1_PORTAL_ADMINISTRACION		X				
FMT_MSA.1_WEB-SERVICES		X				
FMT_MSA.3_PORTAL_ADMINISTRACION		X				
FMT_MSA.3_ WEB-SERVICES		X				
FMT_SMR.1		X				
FMT_SMF.1		X				
FIA_UAU.2_WEB-SERVICES		X				
FIA_UAU.1_PORTAL_ADMINISTRACION		X				
FIA_UID.2_WEB-SERVICES		X				
FIA_UID.1_PORTAL_ADMINISTRACION		X				
FPT_ITC.1	X					
FTP_ITC.1		X				
FPT_RPL.1				X		
FCS_CKM.1			X			
FDP_ITC.1_IMPORTACION_CERTIFICADOS		X				
FDP_ITC.1_CIFRADO_PATRONES_BIOMETRICOS	X					
FCS_COP.1_ AES _CIFRADO_SISTEMA_FICHEROS			X			
FCS_COP.1_ AES_CIFRADO_PATRONES_BIOMETRICOS	X					
FCS_COP.1_RSA		X				
FPT_TST.1			X			
FTA_TAB.1_PORTAL_ADMINISTRACION						X
FRU_RSA.1				X		

El objetivo OT1 permite garantizar la confidencialidad de los patrones de comportamiento cuando se exportan a una base de datos externa al TOE, y se implementará conforme a lo indicado en los requisitos funcionales FPT_ITC.1, que protege la comunicación con el sistema de almacenamiento de patrones, FDP_ITC.1_CIFRADO_PATRONES_BIOMETRICOS, que importa la clave de cifrado (La política sobre la cual se importa la clave de cifrado, es la de acceso al consola y se delega en el entorno, sistema operativo y ssh), y FCS_COP.1_AES_CIFRADO _PATRONES_BIOMETRICOS, que realiza el cifrado simétrico de dichos patrones.

El objetivo OT2 permite implementar los roles y capacidades que tendrán los usuarios:

- En el caso de la consola SSH se implementará conforme a lo indicado en los requisitos funcionales FMT_SMR.1, indicando que los parámetros de configuración del TOE serán accedidos según la política de control de acceso a consola y FMT_SMF.1 que como ya se menciono anteriormente se delega en el entorno, sistema operativo y ssh, la política de control de acceso a la consola.
- Para los servicios web se implementará conforme a lo indicado en los requisitos funcionales FDP_ACC.2_WEB-SERVICES, que especifica que serán controladas las operaciones sobre los servicios exportados como web-services cifrándolas en un canal seguro, FTP_ITC.1, mediante un algoritmo de clave pública RSA, FCS_COP.1_RSA, cuya identificación está basada en certificados, FDP_ACF.1_WEB-SERVICES, dichos certificados podrán ser administrados desde la consola ssh, FMT_MSA.1_WEB-SERVICES, siendo importados desde la misma, FDP_ITC.1_IMPORTACION_CERTIFICADOS , pudiendo asignar los valores iniciales mediante el usuario Authentest (La política sobre la cual se importan los certificados, es la de acceso al consola y se delega en el entorno, sistema operativo y ssh), FMT_MSA.3_ WEB-SERVICES , requiriendo la identificación, FIA_UID.2_WEB-SERVICES y autenticación, FIA_UAU.2_WEB-SERVICES , antes de poder realizar cualquier acción.
- En el caso del portal de administración se implementará conforme a lo indicado en los requisitos funcionales FDP_ACC.2_PORTAL_ADMINISTRACION, que especifica que serán controladas las operaciones posibles a realizar sobre el portal de administración web limitando el acceso a las funcionalidades y datos, FDP_ACF.1_ PORTAL_ADMINISTRACION, mediante la implementación de roles y grupos, FMT_MSA.1_ PORTAL_ADMINISTRACION, permitiendo al administrador del portal asignar los valores iniciales , FMT_MSA.3_PORTAL_ADMINISTRACION , controlando las acciones permitidas para cada rol, FMT_SMR.1, gestionando los roles y capacidades conforme a la política de acceso al portal web, FMT_SMF.1, permitiendo el acceso sin, FIA_UID.1_PORTAL_ADMINISTRACION, ni autenticación, FIA_UAU.1_PORTAL_ADMINISTRACION, identificación a la pantalla ServiceStatus

El objetivo OT3 permite al TOE garantizar la confidencialidad frente a agentes no autorizados de los parámetros del sistema, y se implementará almacenando los parámetros en un sistema de archivos cifrado mediante una clave simétrica en el momento de la instalación, FCS_CKM.1, que genera la clave de cifrado final a partir de un valor firma de la plataforma del TOE, FCS_COP.1_AES_CIFRADO_SISTEMA_FICHEROS que realiza el cifrado simétrico de los parámetros del sistema. Además, bajo demanda de un usuario autorizado, se comprobará la correcta operación de partes del TOE para determinar si las funciones de seguridad del mismo han sido alteradas, FPT_TST.1.

El objetivo OT4 permite establecer los sistemas de medida y distribución de la carga en los servicios web impidiendo ataques de denegación de servicio, y se implementará conforme a los indicado en los requisitos funcionales FPT_RPL.1, que detecta la igualdad en la firma suministrada con res-

pecto a la lista de firmas anteriores y el requisito FRU_RSA.1 limitando la cantidad de pedidos simultáneos desde aplicaciones remotas.

El objetivo OT5 permite generar trazas de auditoría de actividad del servicio de autenticación, así como las relativas al uso del portal de administración, y se implementará conforme a lo indicado en los requisitos funcionales FAU_GEN.1. Permitiendo que sean examinados según lo indicado en el requisito funcional FAU_SAR.1_WEB-SERVICES, FAU_SAR.1_ADMIN y FAU_SAR.1_SSH respectivamente, pudiendo ser seleccionados según FAU_SAR.3

El objetivo OT6 permite la identificación de la versión del TOE, condiciones de producto certificado en la consola y página principal del portal de administración, advirtiendo las responsabilidades en el uso del producto utilizado o configurado de manera insegura, y se implementará conforma a lo indicado en el requisito funcional FTA_TAB.1_PORTAL_ADMINISTRACION

La dependencia de los requisitos de generación de auditoría con respecto al componente FPT_STM.1 sugiere su inclusión en la declaración de seguridad. Sin embargo, la fuente de tiempo, para la generación de la auditoría, es el sistema y no forma parte del TOE.

Las dependencias con FDP_ACC.1 y FMT_MSA.1 de los requisitos de importación de certificados FDP_ITC.1_IMPORTACION DE CERTIFICADOS y de cifrado de patrones FDP_ITC.1_CIFRADO_PATRONES_BIOMETRICOS no se cumplen porque la identificación de acceso la realiza el sistema operativo, por esta razón se menciona la política de acceso a la consola en el requisito pero no la ejercita el TOE.

En cuanto a la gestión de claves criptográficas, el TOE las importa y crea para su uso en el cifrado del sistema de archivos y de los patrones de comportamiento biométrico, pero no gestiona su destrucción, no siendo de aplicación el requisito funcional de seguridad FCS_CKM.4.

La elección de los requisitos de garantía de seguridad se basó en razones de mercado y en conformidad con EAL2+ALC_FLR.1.

Síntesis de la especificación del TOE

Síntesis de la especificación del TOE

FAU_GEN.1 AUDIT - DATA GENERATION

El TOE incluye un módulo de registro de datos de auditoría tanto en el subsistema JBoss como en el portal web. En ambos de los casos, los datos de auditoría se almacenan en un servidor externo. Por otra parte existe el almacenamiento de datos de auditoría en archivos internos referidos a los test de integridad del TOE.

FAU_SAR.1_WEB-SERVICES - AUDIT REVIEW

Mediante el portal web se puede visualizar los datos de auditoría generados a partir de las llamadas al método getTrust del web-service. Estos datos pueden ser visualizados por cualquier usuario, pero verá solo los datos del grupo de aplicaciones que tiene asignado.

FAU_SAR.1_ADMIN - AUDIT REVIEW

El usuario administrador del portal podrá visualizar la actividad de los usuarios del portal, realizada dentro del portal, mediante una pantalla que muestra todos los eventos realizados por los otros usuarios del portal. Esta funcionalidad se encuentra en la opción Admin-Audit dentro del portal.

FAU_SAR.1_SSH - AUDIT REVIEW

Mediante la aplicación “Server Administration” se puede visualizar los datos de auditoría generados por el integrity controller al arranque del TOE. Estos datos pueden ser visualizados por el usuario Authentest o el usuario administrador de consola.

FAU_SAR.3 - SELECTABLE AUDIT REVIEW

Los usuarios del portal contarán con las capacidades de ordenamiento y filtros sobre los datos auditados. Estos filtros cuentan como mínimo un filtro por rango de fechas y uno por usuario.

Política de Control de Acceso a Web-Services (FDP_ACC.2_WEB-SERVICES - COMPLETE ACCESS CONTROL y FDP_ACF.1_WEB-SERVICES - SECURITY ATTRIBUTE BASED ACCESS CONTROL

El control de acceso a los servicios web esta implementado a través de los mecanismos de autenticación, mediante certificados digitales importados desde la consola ssh. Dichos mecanismos son provistos por el servidor de aplicaciones JBoss.

Solo podrán acceder a los servicios web aquellos servidores de aplicación remotos que puedan autentificarse mediante un certificado válido.

Política de Control de Acceso al Portal de Administración (FDP_ACC.2 _PORTAL_ ADMINISTRACION - COMPLETE ACCESS CONTROL y FDP_ACF.1_PORTAL_ADMINISTRACION - SECURITY ATTRIBUTE BASED ACCESS CONTROL)

Se controlará el acceso al portal de administración mediante la autenticación por usuario y contraseña.

El portal de administración impedirá el acceso a las pantallas y datos mediante la restricción en las opciones de menú y opciones de filtro disponibles según las reglas definidas en la política organizativa P1

FMT_MSA.1_PORTAL_ADMINISTRACION - MANAGEMENT OF SECURITY ATTRIBUTES

El usuario administrador del portal puede modificar, mediante las pantallas de administración de usuarios, el rol y el grupo de aplicaciones a la que pertenece cualquier usuario del portal de administración. Por otra parte los usuarios administradores de grupo del portal solo pueden modificar los usuarios de su grupo de aplicaciones del portal.

FMT_MSA.1_WEB-SERVICES - MANAGEMENT OF SECURITY ATTRIBUTES

El usuario Authentest y el administrador de consola podrán agregar o eliminar certificados del repositorio de certificados de JBoss permitiendo controlar las aplicaciones que tienen acceso a los WebServices.

FMT_MSA.3_PORTAL_ADMINISTRACION - STATIC ATTRIBUTE INITIALISATION

El TOE permite modificar a través del portal de administración los siguientes valores:

- Aplicaciones y campos para los que podrá ser utilizado el servicio de identificación
- Usuario y Grupos de aplicaciones para la administración web.
- Reinicio de patrones de identificación.
- Niveles de seguridad para el algoritmo de identificación
- Establecer modo silencioso para el algoritmo de identificación.

FMT_MSA.3_ WEB-SERVICES - STATIC ATTRIBUTE INITIALISATION

El TOE permite la importación de certificados para el acceso a los webservices desde la consola SSH con el usuario Authentest y el administrador de consola.

FMT_SMR.1 - SECURITY ROLES

Los roles de seguridad serán los siguientes

- Administrador de consola: Se crea al momento de la instalación y se controla su acceso mediante los mecanismos generales del sistema operativo mediante usuario y contraseña.
- Usuario Authentest: Se crea al momento de la instalación y se controla su acceso mediante los mecanismos generales del sistema operativo mediante usuario y contraseña.
- Aplicación Web-service remota: Se crean mediante la administración de certificados digitales, desde la consola por el usuario Authentest, que le permiten acceder a los servicios web expuestos por el TOE.

Roles para el portal web:

- Administrador de portal: Se crea uno al momento de la instalación y se controla su acceso mediante usuario, contraseña y patrón de comportamiento biométrico. Posteriormente se puede asignar este rol a otros usuarios del portal.
- Administrador de grupo: Los crea el administrador del portal u otro administrador de grupo para ese mismo grupo y se controla su acceso mediante usuario, contraseña y patrón de comportamiento biométrico.

FMT_SMF.1 - SPECIFICATION OF MANAGEMENT FUNCTIONS

La gestión de parámetros del TOE se realizan mediante la consola, la aplicación “Server Administration” a estas dos pueden acceder los usuario administrador de consola y usuario Authentest, este último con permisos restringidos para la consola.

El resto de los parámetros y roles se administran desde el portal web, a este pueden acceder los usuarios que sean administrador de portal, administrador de grupos o usuario normal.

FIA_UAU.2_WEB-SERVICES - USER AUTHENTICATION BEFORE ANY ACTION

Los servidores de aplicación remoto no podrán realizar ninguna llamada a los servicios web publicados por el TOE si antes no se han autenticado exitosamente mediante el uso de certificados digitales.

FIA_UAU.1_PORTAL_ADMINISTRACION- TIMING OF AUTHENTICATION

Los usuarios del portal web solo podrán acceder a la pantalla “Service Status” sin necesidad de autenticarse. Si deberán hacerlo para el resto de las funcionalidades del mismo.

FIA_UID.2_WEB-SERVICES - USER IDENTIFICATION BEFORE ANY ACTION

Los servidores de aplicación remoto no podrán realizar ninguna llamada a los servicios web publicados por el TOE si antes no se han identificado exitosamente mediante el uso de certificados digitales.

FIA_UID.1_PORTAL_ADMINISTRACION- TIMING OF IDENTIFICATION

Los usuarios del portal web solo podrán acceder a la pantalla “Service Status” sin necesidad de identificarse. Si deberán hacerlo para el resto de las funcionalidades del mismo.

FPT_ITC.1 - INTER-TSF CONFIDENTIALITY DURING TRANSMISSION

El almacén de patrones de comportamiento se cifran con algoritmo AES antes de ser almacenados en la base de datos externa al TOE, cuando el servicio requiere acceder a los datos son leídos de la base de datos y luego descifrados por el servicio web en el TOE.

FTP_ITC.1 - INTER-TSF TRUSTED CHANNEL

La comunicación entre el TOE y los servicios web externos se asegura a través de un canal seguro SSL con certificados digitales generados y distribuidos de forma segura tanto en el TOE como la aplicación remota que consume el servicio.

FPT_RPL.1 - REPLAY DETECTION

El TOE cuenta con la capacidad de detectar solicitudes de autenticación getTrust() sobre webservices, detectando la igualdad de la firma suministrada con respecto a la lista de las firmas anteriores, de número configurable.

FCS_CKM.1 - CRYPTOGRAPHIC KEY GENERATION

Por cada instalación se importa una clave que sirve para cifrar la información almacenada en la base de datos externa al TOE, también se genera una firma de hardware que será utilizada como clave para cifrar el sistema de archivos donde se encuentra el algoritmo de reconocimiento y parámetros del TOE. Los datos de la base de datos y el sistema de archivos se cifran con algoritmo AES.

FDP_ITC.1_IMPORTACION_CERTIFICADOS 1 - IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES

La importación de los certificados generados externamente en formato Jboss serán importados al TOE mediante la aplicación “Server Administration”, utilizando el usuario Authentest o el usuario administrador de consola. La importación se realiza bajo política de acceso a la consola que se delega al entorno, sistema operativo y ssh.

FDP_ITC.1 CIFRADO_PATRONES_BIOMETRICOS - IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES

La importación de la clave final de cifrado AES para la encriptación de los patrones biométricos se realizará durante el proceso de instalación. La importación se realiza bajo la política de acceso a la consola que se delega al entorno, sistema operativo y ssh.

FCS_COP.1_AES_CIFRADO_SISTEMA_FICHEROS - CRYPTOGRAPHIC OPERATION

El algoritmo AES es utilizado para el cifrado y descifrado del sistema de ficheros
En el cifrado y descifrado de datos con algoritmo AES se usa una llave de 256 bits, que es generada a partir de datos tomados del entorno.

FCS_COP.1_AES_ CIFRADO_PATRONES_BIOMETRICOS - CRYPTOGRAPHIC OPERATION

El algoritmo AES es utilizado para el cifrado y descifrado de los patrones almacenados en la base de datos externa al TOE.
En el cifrado y descifrado de datos con algoritmo AES se usa una llave de 256 bits, que es importada al momento de la instalación.

FCS_COP.1_RSA - CRYPTOGRAPHIC OPERATION

En el cifrado y descifrado con certificados digitales utilizados en FTP_ITC.1 - INTER-TSF TRUSTED CHANNEL que utilizan claves RSA con una llave de 4096 bits.

FPT_TST.1 - TSF TESTING

Mediante la aplicación “Server Administration” los usuarios autorizados podrán verificar el correctos funcionamiento de los servicios web publicados por el TOE. Se realizará una serie de pruebas a fin de determinar que los servicios web estén accesibles y respondan según lo esperado.

FTA_TAB.1_PORTAL_ADMINISTRACION - DEFAULT TOE ACCESS BANNERS

En la pantalla inicial del sitio de administración web se presenta un texto advirtiendo acerca del uso no autorizado de la herramienta.

FRU_RSA.1 - MAXIMUM QUOTAS

El TOE permite controlar la cantidad de conexiones máxima de clientes que JBoss puede atender simultáneamente.