centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1521

Procedimiento de Empleo Seguro
SIAVAL SafeCert Server Signing System (QSCD) 3.1

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:28:54 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. ***SIAVAL SafeCert Manager*** es un software de firma electrónica en servidor, que asegura el control exclusivo de las claves de firma por parte del firmante utilizando un módulo ***Thales Luna K7 Cryptographic Module***. La composición de estos dos componentes forma el producto objetivo de la evaluación denominando **SIAVAL SafeCert Server Signing System (QSCD)**.

2. El conjunto de componentes que conforman el producto SIAVAL SafeCert Server Signing System (QSCD) posibilita la generación de firmas en servidor, de manera que una organización pueda fácilmente establecer un sistema de firma seguro, centralizando los procesos de firma de documentos de sus usuarios. Facilita la gestión del ciclo de vida de las claves, su asociación entre los usuarios, así como el cumplimiento del propósito de uso de dichas claves.

3. Se establece en todo momento el control exclusivo por parte de los usuarios de sus claves de firma, asegurando el vínculo entre usuario y claves, protegiendo la clave privada de firma de forma tal que únicamente pueda ser utilizada dentro del entorno operativo y por su propietario legítimo. Para ello, el SIAVAL SafeCert Server Signing System (QSCD) dispone del componente criptográfico Thales Luna K7 Cryptographic Module que se encargará de realizar las operaciones criptográficas necesarias para generar claves con funciones *"endorsed"* y algoritmos que aseguren en todo momento su fortaleza y a su vez protegerlas estableciendo el control exclusivo de uso por parte de su titular. Así mismo, será utilizado para aplicar el protocolo de activación de las claves de firma cuando se solicite una operación de firma/autenticación o cambio de contraseña por parte del titular de la clave.

4. La forma de interactuar con el SIAVAL SafeCert Server Signing System (QSCD) es mediante dos interfaces vía webservices, una de uso administrativo y otra de firma, a través de las cuales las aplicaciones invocarán a las operaciones. Estas interfaces aseguran el control de acceso mediante la autenticación, en todo momento, de los usuarios que acceden a dichos servicios y realizando la autorización en función de perfiles que determinarán el ámbito y uso de las operaciones.

5. La interfaz WebService vía SOAP de uso administrativo, se utilizará para el aprovisionamiento y activación de las cuentas de los usuarios firmantes en el sistema. De manera que, a través de esta interfaz, la organización establecerá y gestionará a los usuarios firmantes, así como sus claves activas en el sistema.

6. A la interfaz de firma WebService vía SOAP y mediante mensajes binarios Hessian, se accederá desde aquellas aplicaciones de creación de firma de la organización que se integren con el sistema para posibilitar la firma de documentos. El acceso a estos servicios se accederá autenticando a las aplicaciones solicitantes de la firma, de manera que se establezca un canal seguro entre la aplicación de firma y el SIAVAL SafeCert Server Signing System (QSCD). A través de este canal seguro, el usuario, en el momento de la firma, establecerá las credenciales de autenticación a su clave de firma a través de un sistema multicanal, proporcionando una clave secreta que únicamente él conoce, y un segundo factor de autenticación como por ejemplo una contraseña dinámica de un solo uso o sus credenciales biométricas.

7. El uso del componente criptográfico Thales Luna K7 Cryptographic Module, que contiene el SIAVAL SafeCert Server Signing System (QSCD), se realizará exclusivamente mediante peticiones a través de los interfaces anteriormente descritos del módulo SIAVAL SafeCert

Manager, no habiendo ningún interfaz directo entre los usuarios o aplicaciones de firma con el componente criptográfico, siendo el módulo SIAVAL SafeCert Manager el que realiza el acceso al módulo criptográfico a través de su interfaz PKCS#11 para realizar las operaciones criptográficas necesarias en función de la solicitud recibida a través de los interfaces webservices públicos.

8. Los usuarios firmantes podrán tener asociadas varias claves, de manera que podrán utilizar en cada aplicación de creación de firma la clave requerida en cada momento.
9. En el SIAVAL SafeCert Server Signing System (QSCD), mediante configuración, se podrán establecer diferentes políticas sobre diferentes aspectos de seguridad, estas políticas engloban ámbitos tanto del componente dependiente SIAVAL Safecert Manager, como del componente base Thales Luna K7 Cryptographic Module:
    - Bloqueo/suspensión de las claves tras n fallos de intentos de autenticación en el momento de la firma o cambio de contraseña por parte del usuario firmante.
    - Activación del uso de las claves durante periodos de tiempo.
    - Se establecen en el hardware criptográfico los algoritmos y tamaños que aseguran la fortaleza necesaria de las claves y operaciones criptográficas utilizadas en el sistema.
    - Se establecen los atributos de seguridad necesarios para determinar que las claves no puedan ser exportadas del hardware criptográfico sin estar debidamente protegidas.
10. Las características de seguridad fundamentales del SIAVAL SafeCert Server Signing System (QSCD) se resumen en:
    - **Control de Acceso**: Se establece control de acceso para todas las operaciones realizadas en el SIAVAL SafeCert Server Signing System (QSCD) de manera que solamente los usuarios autorizados puedan realizar las operaciones para las que tienen permisos.
    - **Protección de las claves de firma**: Se asegura en todo momento la protección de las claves de firma de los firmantes, de manera que solamente puedan ser utilizadas dentro del entorno operativo del SIAVAL SafeCert Server Signing System (QSCD) y no puedan ser divulgadas para su uso ilegítimo.
    - **Control Exclusivo de la clave de firma**: La clave de firma se asocia al firmante de manera que éste tenga el control exclusivo para su activación en el momento de la firma.
    - **Firma segura**: Se asegura todo el ciclo del proceso de firma, desde el momento en que desde la aplicación de creación de firma se solicita al SIAVAL SafeCert Server Signing System (QSCD) una firma, tanto en la transmisión de los datos a firmar al SIAVAL SafeCert Server Signing System (QSCD), como en la generación de la firma, así como en la devolución de la firma a la aplicación. Así mismo, la firma generada tiene la fortaleza necesaria para que pueda verificarse su integridad.
    - **Utilización de algoritmos y tamaños de claves adecuados**: Se establece la utilización de un módulo criptográfico certificado Common Criteria EAL4+ para asegurar la fortaleza de las claves y operaciones criptográficas utilizadas en el sistema.
11. El SIAVAL SafeCert Server Signing System (QSCD) está formado por dos componentes, cada uno de ellos certificado Common Criteria con los siguientes niveles de aseguramiento:

- Thales Luna K7 Cryptographic Module certificado Common Criteria EAL4+ (ALC_FLR.2 y AVA-VAN.5)
- SIAVAL SafeCert Manager certificado Common Criteria EAL4+ (ALC_FLR.1 y AVA-VAN.5)

12. El Componente Base de la composición es el módulo criptográfico Thales Luna K7 Cryptographic Module y el Componente Dependiente es el SIAVAL SafeCert Manager.
13. El SIAVAL SafeCert Server Signing System (QSCD) es un subconjunto de los componentes que conforman la solución global aportada por el producto.
14. Los componentes lógicos incluidos en el SIAVAL SafeCert Server Signing System (QSCD) son:

    - **Módulo de firma**: Software que proporciona los servicios de firma, importación de claves mediante PKCS#12 y cambio de PIN de activación de la clave privada a través de Servicios Web convencionales y mediante el uso del API de Integración Java.
    - **Módulo criptográfico**: Que invoca al componente Base para realizar las operaciones criptográficas de protección de las claves y firma electrónica.
    - **Software Cliente Thales Luna K7 Cryptographic Module**: para la comunicación entre el componente SIAVAL SafeCert Manager y el HSM.
    - **Servicios web de administración**: Que actúan sobre el módulo de administración donde se realiza las operaciones de alta de titulares y creación de par de claves a través de la RA correspondiente.
    - **Módulo de gestión de Segundo Factor de Autenticación** (interno).
    - **Componentes de integración con *Plataformas de envío de OTPs*** a los titulares.
    - **Componentes de integración con *Plataformas de Segundo Factor de Autenticación***.
    - **Ficheros de configuración y claves** para la generación y comprobación de la autoría de los datos.
    - **Hardware criptográfico** instalado en la máquina a través del interfaz PCI.

15. En la siguiente ilustración se representa la arquitectura lógica de los componentes que constituyen la solución completa, distinguiendo entre los que pertenecen al SIAVAL SafeCert Server Signing System (QSCD) y aquellos componentes que no forman parte del SIAVAL SafeCert Server Signing System (QSCD) y son externos a él pero que son necesarios para su correcto funcionamiento:

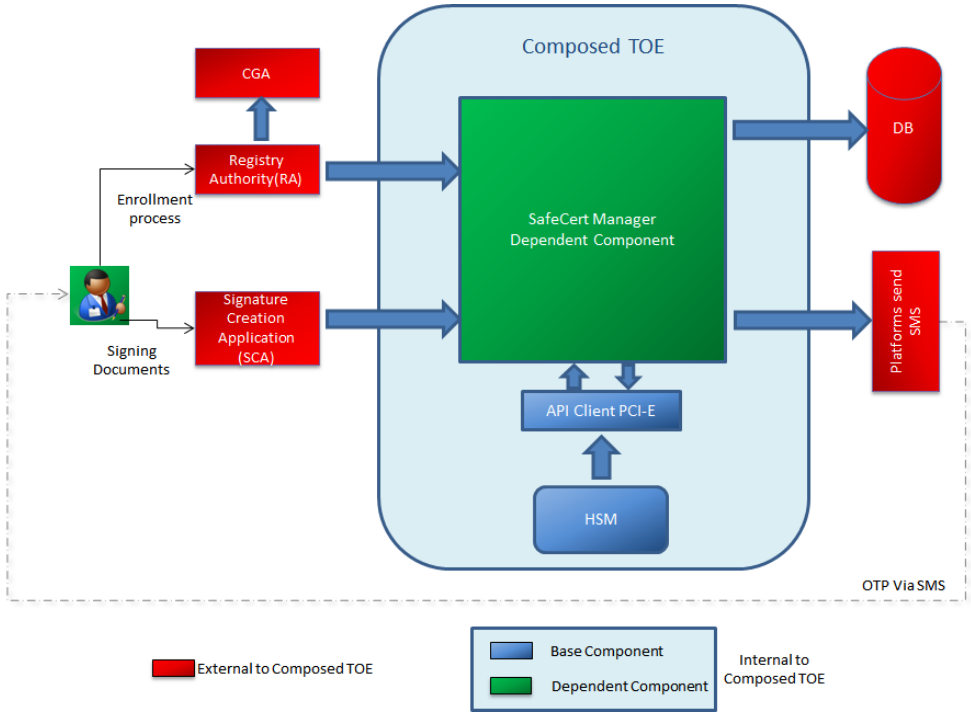

Ilustración 1: Arquitectura lógica del SIAVAL SafeCert Server Signing System (QSCD)

2 OBJETO Y ALCANCE

16. El objetivo de este documento es servir de guía para la instalación y configuración segura del producto SIAVAL SafeCert Server Signing System (QSCD) versión 3.1, incluyendo todos los componentes que lo conforman.

17. El producto SIAVAL SafeCert Server Signing System (QSCD) ha sido incluido en el catálogo de productos y servicios STIC (CPSTIC). Para conocer el listado, categoría o nivel y familia de éste, consulte: https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic .

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

4.1.1 ENTREGA SEGURA DEL PRODUCTO

18. El producto se entrega integrado en un *appliance*, con una infraestructura hardware y un software base securizado y previamente instalado, que incorpora los siguientes componentes:
    - SIAVAL SafeCert Manager 3.
    - Thales Luna PCI Modelo K7 Cryptographic Module con PED correctamente instalada con software de cliente.
    - Software de administración y operación correctamente instalado (Webmin).
19. Se ha definido un procedimiento de entrega segura con el que se podrá validar que se entregan todos los componentes indicados, que se encuentran operativos y que se mantiene la integridad de los componentes software del producto desplegados, es decir, que no han sufrido modificaciones durante el proceso de entrega y coinciden con los liberados por el fabricante. Este procedimiento de entrega consta de los siguientes pasos:
    - Entrega de *appliance* físico empaquetado, con los componentes ya instalados, junto con un albarán de entrega en el que se identifica el *appliance* entregado con su número de serie y la versión del producto en él desplegada.
    - Verificación de las medidas físicas: La caja en la que se entrega el *appliance* físico debe encontrarse con el embalaje sellado y el albarán de entrega cerrado correctamente. De igual forma, una vez desempaquetada la máquina, ésta debe llevar las pegatinas anti-tampering correctamente colocadas y sin evidencias de apertura.
    - Verificación de componentes *software* instalados: En el *appliance*, para el correcto funcionamiento del producto y su administración, deben instalarse una serie de componentes software: El propio producto **SIAVAL SafeCert Server Signing System (QSCD)**, el software cliente del módulo criptográfico **HSM LunaPCI** y la herramienta de administración (**Webmin**). Para verificar que se han instalado estos componentes se puede ejecutar el comando **"Consultar módulos instalados"** desde la opción de menú **"Operación de Sistema => Gestión del Sistema"** de la herramienta Webmin, que muestra el nombre y la versión de los componentes *software* instalados.
20. El acceso a la herramienta Webmin se realiza mediante consola web a través de la URL https://host:55080

```
28-06-2023 00:00:00 I scripts 3.3.00-20230628-0000
28-06-2023 00:00:00 I webmin 3.3.00-20230628-0000
26-10-2023 13:27:48 I lunapci 62.74.104_RL87-20230519
26-10-2023 13:28:53 I Luna PCI-E Hardware version: 808-00055-001
26-10-2023 13:30:02 I Luna PCI-E client version: 10.4.0
31-10-2023 08:05:33 I scripts 3.3.00-20231030-2111
31-10-2023 08:05:42 I webmin 3.3.00-20231030-2111
31-10-2023 08:09:17 I safecert_conf 7.0.90-20200421-1512
31-10-2023 08:09:36 I tomcat 9.0.73
31-10-2023 08:09:40 I proxysfda_conf 7.0.90-20200123-1424
31-10-2023 08:10:49 I proxysfda 3
31-10-2023 08:10:49 I safecert 3
```

Ilustración 2: Chequeo Versiones Instaladas

21. Se visualizarán los componentes instalados indicando la fecha y hora de su instalación y la versión correspondiente.
22. Entre ellos se indicará en la línea con la referencia "safecert" la versión del componente SIAVAL SafeCert Manager que en el caso de la versión certificada será 3.

- Validación del Firmware de Luna K7: Para verificar que en el *appliance* se ha instalado el dispositivo criptográfico (HSM) Thales Luna K7 Cryptographic Module con la versión del Firmware adecuada, se deberá acceder al *appliance* mediante conexión **ssh** con el usuario **adminsia** y seleccionar la opción en el menú **hl1**.

```
Opciones HSM - LUNA

hl1. Gestionar el HSM-Luna (lunacm)
hl2. Crear la MASTERKEY (ckdemo)
hl3. Vincular PED REMOTO (pedClient)
hl4. Activar la particion del HSM - LOCAL
```

Ilustración 3: Opciones HSM LUNA

23. En la pantalla se mostrará el modelo y versión del módulo criptográfico.

```
lunacm (64-bit) v10.4.0-417. Copyright (c) 2021 SafeNet. All rights reserved.


        Available HSMs:

        Slot Id ->              3
        Label ->                HSMPCI
        Serial Number ->        1474304313959
        Model ->                Luna K7
        Firmware Version ->     7.7.2
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning Mode
        Slot Description ->     User Token Slot
        FM HW Status ->         FM Ready

        Slot Id ->              4
        Label ->                LUNAPCI
        Serial Number ->        633209
        Model ->                Luna K7
        Firmware Version ->     7.7.2
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mode
        Slot Description ->     Admin Token Slot
        FM HW Status ->         FM Ready
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           L3 Device


        Current Slot Id: 3
```

Ilustración 4: Firmware Luna K7 Cryptographic Module

24. En la línea con la referencia "Firmware Version ->" se visualizará la versión firmware instalado en el módulo criptográfico, que deberá corresponder con una de las certificadas, en este caso, 7.7.0, 7.7.1 o 7.7.2.

    - Validación de la integridad del producto: En el proceso de liberación del producto se genera un *hash* de cada uno de los componentes del producto liberados y de las librerías comunes utilizadas. Durante la entrega se podrá validar la integridad de los componentes desplegados en el *appliance* ejecutando el comando **"Chequeo de integridad del producto"** desde la herramienta de administración Webmin, que muestra el hash de dichos componentes y que se pueden comparar con los generados durante la liberación del producto. En caso de coincidencia, se puede considerar que los componentes desplegados son los mismos que los liberados por el fabricante.

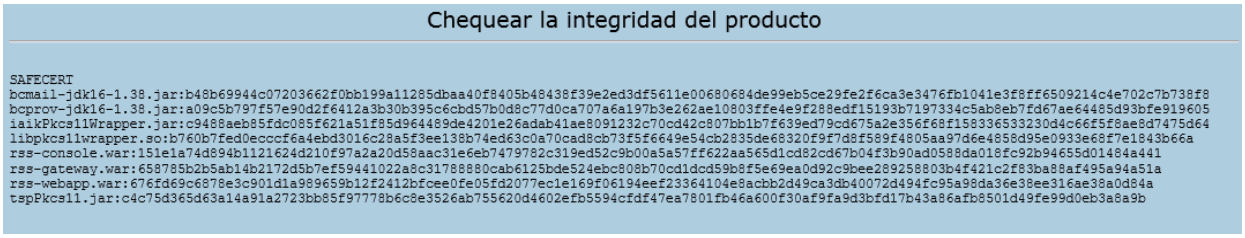

Ilustración 5: Chequeo Integridad

25. Para aplicar esta configuración se debe disponer de los siguientes componentes:

    - LunaPCI PED correctamente instalada con software de cliente.
    - SafeCert correctamente desplegado.
    - Postgre compilado con soporte SSL.

4.1.2 ENTREGA SEGURA DE LOS MANUALES

26. Los manuales en formato pdf se entregan al cliente en el momento de la puesta en marcha de la máquina donde reside el SIAVAL SafeCert Server Signing System (QSCD).
27. El técnico de SIA desplazado a las instalaciones del cliente se encargará de entregarle los siguientes manuales del componente SIAVAL SafeCert Manager:

    - SIAVAL SafeCert - Manual de Administración, Rev. 1.0 [REF1]
    - SIAVAL SafeCert - Manual de Instalación, Rev. 1.0 [REF2]
    - SIAVAL SafeCert - Manual de Integración, Rev. 1.0 [REF3]
    - SIAVAL SafeCert - Manual de Integración ProxySFDA, Rev. 1.0 [REF4]
    - SIAVAL SafeCert - Manual de operaciones, Rev. 1.0 [REF5]
    - SIAVAL SafeCert - Manual de configuración segura, versión. 3.0 [REF6]

28. Igualmente, se entregan las guías de usuario del componente HSM, el módulo criptográfico LUNA K7 Cryptographic Module, proporcionadas por el fabricante.

    - 007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ [REF7]
    - 007-000465-001_K7_CC_User_Guidance_Part2_AGD_OPE_RevK [REF8]
    - 007-000466-001_K7_CC_User_Guidance_Part3_AGD_OPE_RevJ [REF9]

- 007-000467-001_K7_CC_User_Guidance_Part4_AGD_OPE_RevH [REF10]

29. También se hace entrega de la documentación relacionada con la composición de ambos componentes, el SIAVAL SafeCert Manager y el módulo criptográfico LUNA K7 Cryptographic Module:

    - SIAVAL SafeCert - Manual de composición, versión 2.0 [REF11]

30. La entrega de estos documentos es realizada por el técnico desplazado de SIA de manera que los documentos llegan al usuario de manera íntegra.

4.1.3 ENTREGA SEGURA DE LOS SCRIPTS DE BASE DE DATOS

31. Igualmente, los scripts de generación de la estructura de la base de datos se entregan al cliente en el momento de la puesta en marcha del producto.

32. El técnico de SIA desplazado a las instalaciones del cliente se encargará de entregar los scripts de base de datos que, considerando que se trata de una base de datos PostgreSQL, son los siguientes:

    - RSSTablas.sql
    - RSSDatmin.sql
    - RSS_Estadisticas.sql

4.2 ENTORNO DE INSTALACIÓN SEGURO

33. El servidor físico en el que se encuentra desplegado el producto debe de tener su acceso restringido para la preparación del entorno y para la instalación, administración y operación del sistema, de forma que solamente tengan acceso a él un conjunto limitado de usuarios con los permisos necesarios para realizar la función para la que se han creado.

4.3 REGISTRO Y LICENCIAS

34. En las oficinas de SIA, durante el proceso de preparación y montaje del producto en el *appliance* que finalmente se entrega al cliente, se toma nota y se registran, en los sistemas internos, los componentes *hardware* y *software* que finalmente se envían al cliente. En la fase de instalación y configuración del producto en el entorno del cliente no hay que realizar ninguna actividad especial de registro ni de obtención de licencias.

4.4 CONSIDERACIONES PREVIAS

4.4.1 GENERACIÓN DE LA ESTRUCTURA DE LA BASE DE DATOS

35. Previamente a la instalación y configuración del producto, hay que realizar el proceso de generación de la estructura de la base de datos en la que se va a apoyar el funcionamiento del mismo, para lo que se necesita disponer de un usuario con acceso al esquema de datos y con privilegios suficientes para crear, modificar y borrar tablas y otros objetos.

36. La creación del modelo de datos se realiza ejecutando, de forma ordenada, los scripts de base de datos que, considerando que se trata de una base de datos PostgreSQL, son los siguientes:

- RSSTablas.sql
- RSSDatmin.sql
- RSS_Estadisticas.sql

37. La optimización de la base de datos, si procede, en relación a la distribución en tablespaces, generación/ubicación de índices, etc., debe realizarse de manera específica en cada proyecto de despliegue por un administrador de base de datos experto en la solución de base de datos utilizada.

4.4.2 ASEGURAMIENTO DEL DESPLIEGUE DEL MÓDULO CRIPTOGRÁFICO

38. Para asegurar el despliegue del módulo criptográfico, HSM, se tienen que llevar a cabo una serie de actividades y tomar una serie de decisiones que se mencionan a continuación.

4.4.2.1 PROTECCIÓN DE DATOS FUERA DEL CONTROL DEL HSM

39. Cuando las copias de los datos protegidos por el HSM se gestionan fuera del HSM, deben disponer de una protección adecuada para esos datos, considerando los datos en sí y la aplicación o entorno que los contenga. Esto incluye la protección de los datos que se exportan desde el módulo criptográfico Thales Luna K7 o se importan al mismo, como datos de auditoría y claves cifradas.
40. A este respecto, se puede disponer de más información en el documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7], en el apartado *"CHAPTER2: Planning your deployment"* / *"Protection of data outside the HSM"*.

4.4.2.2 PLANIFICACIÓN DEL NÚMERO DE ROLES AUTENTICADOS NECESARIOS

41. Antes de poner en marcha el HSM, la organización donde vaya a funcionar debe revisar y decidir qué roles y métodos de autenticación se van a utilizar.
42. A este respecto, se puede disponer de más información en el documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7], en el apartado *"CHAPTER2: Planning your deployment"* / *"Assigning people to HSM roles"*.

4.4.2.3 DECIDIR SI SE DEBE UTILIZAR EL PED REMOTO

43. Antes de utilizar el PED remoto, el cliente final debe decidir si va a necesitar utilizarlo en su instalación.
44. A este respecto, se puede disponer de más información en el documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7], en el apartado *"CHAPTER2: Planning your deployment"* / *"Using the Thales Luna PED (Remote Configuration)"*.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

45. El entorno sobre el cual el producto SIAVAL SafeCert Server Signing System (QSCD) ha sido verificado que cumple las especificaciones Common Criteria en un nivel de evaluación EAL4 + ALC_FLR.1 + AVA_VAN.5 es el siguiente:

- **Hardware:**

- **Appliance**, donde reside el HSM y SIAVAL SafeCert.

- **Software:**
  - **Sistema operativo en la máquina servidor del Producto**: Rocky Linux release 8.10 de 64 bits.
  - **Servidor de aplicaciones**: Apache Tomcat 9.
  - **Base de Datos**: PostgreSQL.
  - **Cliente HSM**: LUNA PCI-E Cryptographic Module Client 10.
  - **Java Runtime Enviroment en servidor**: OpenJDK 1.8.x.
  - **Consola web de administración**: SIAVAL SafeCert Console 3.
  - **Consola web de administración del entorno**: Webmin.
  - **Componente ProxySFDA**: SIAVAL SafeCert ProxySFDA 3 para la gestión de SFDAs externos y envío de OTPs.

5 FASE DE INSTALACIÓN

46. El producto SIAVAL SafeCert Server Signing System (QSCD) es entregado en modo *appliance*, con todos los elementos que necesita para funcionar previamente instalados, de manera que, para ponerlo en funcionamiento, no se necesita ninguna instalación adicional.

6 FASE DE CONFIGURACIÓN

47. El producto SIAVAL SafeCert Server Signing System (QSCD) se configura considerando los mecanismos criptográficos autorizados para su uso en el ENS, tal como se establece en la guía *"CCN-STIC 807: Criptología de Empleo en Esquema Nacional de Seguridad"* [REF12].

6.1 MODO DE OPERACIÓN SEGURO

6.1.1 PREPARACIÓN DE LOS COMPONENTES HARDWARE /SOFTWARE

48. A continuación, se describen los procedimientos de preparación de los componentes hardware/software del entorno de operación.

6.1.1.1 ACCESO MEDIANTE CERTIFICADO A WEBMIN AL USUARIO "OPERACION"

49. Se trata de uno de los mecanismos de autenticación admitidos en el ENS, tal como se establece en la guía *"CCN-STIC 807: Criptología de Empleo en Esquema Nacional de Seguridad"* [REF12].

50. Se ha de configurar para el usuario *"operacion"* el acceso mediante certificado a la herramienta de configuración Webmin, este usuario será el utilizado por el cliente final para realizar las operaciones básicas en el entorno.

51. Para realizar la configuración de su certificado de autenticación, se accederá mediante el usuario *"admin"* a Webmin y se establecerá el certificado de la CA del cliente que se utilizará para el acceso de su usuario *"operacion"*.

52. Posteriormente, se le asignará al usuario *"operacion"* el DN del certificado con el que se deberá autenticar. Hecho esto, el usuario ya podrá autenticarse a la herramienta Webmin.

6.1.1.2 CONFIGURAR COMUNICACIÓN SSL EN EL SERVIDOR DE APLICACIONES

6.1.1.2.1 Configurar certificado de autenticación de *"admin"* para el acceso inicial

53. La configuración del acceso mediante autenticación con certificados determina que se debe configurar un certificado inicial de autenticación para el usuario superadministrador del sistema SafeCert. De manera que, se accederá inicialmente con la contraseña para establecer en la consola de administración al usuario superadministrador el certificado de autenticación emitido por la CA del cliente.

54. Para ello se accede a la cuenta del usuario superadministrador y se sube el certificado en el concepto **"Certificado de Autenticación"** tal y como se muestra en la pantalla:

Ilustración 6: Certificado superadministrador

55. Una vez configurado el certificado al usuario en el sistema SafeCert, se procederá a configurar la autenticación por certificados en el conector del servidor de aplicaciones, desde ese momento los accesos serán obligatorios realizarlos mediante autenticación con certificado.

6.1.1.2.2 Configurar conector SSL con autenticación de cliente

56. Para configurar el conector mediante protocolo SSL debemos disponer de, al menos, un almacén de certificados y claves de tipo jks. En realidad, Tomcat puede utilizar dos almacenes de este tipo, uno que deberá contener la clave privada y el certificado para el servidor y otro que contendrá los certificados de confianza que se admitirán en las conexiones SSL.
57. Se debe establecer como único protocolo aceptado TLS v1.2 deshabilitando de esta manera la utilización de protocolos con vulnerabilidades conocidas como SSL.
58. El conector deberá quedar similar a como se muestra a continuación, el almacén denominado ***siavalaplliance.jks*** contendrá el certificado y clave privada del servidor que se desee establecer en el sistema, y el almacén denominado ***authCA.jks*** contendrá los certificados de las CA que permitirán autenticarse al servidor.
59. Los valores de los parámetros *"keystorePass"* y *"truststorePass"* corresponden a las contraseñas de sus respectivos almacenes.

```
<Connector port="4443" protocol="org.apache.coyote.http11.Http11Protocol"
        maxThreads="200" maxHttpHeaderSize="8192"
        server="SafeCert Server"
        SSLEnabled="true" scheme="https" secure="true"
        clientAuth="true"
        keystoreFile="/opt/software/eastsp/conf/siavalaplliance.jks"
        keystorePass="xxxxxx"
        truststoreFile="/opt/software/eastsp/conf/authCA.jks"
        truststorePass="xxxxxxx"
        keyAlias="privatekey" keystoreType="JKS" sslEnabledProtocols="TLSv1.2"
        ciphers="TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
        TLS_ECDHE_ECDSA_WITH_AES_256_CCM,
        TLS_ECDHE_ECDSA_WITH_AES_128_CCM,
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" />
```

60. Tanto el protocolo utilizado como los algoritmos indicados en la Cipher Suite para la negociación del canal seguro se encuentran entre los autorizados y recomendados en la guía *"CCN-STIC 807: Criptología de Empleo en Esquema Nacional de Seguridad"* [REF12].

    NOTA: Los algoritmos indicados en la Cipher Suite para la negociación del canal seguro, deberán irse actualizando en función del estado del arte tecnológico, de manera que se

asegure en todo momento la utilización de algoritmos robustos para la comunicación de los datos. Se determina, por tanto, que la configuración de algoritmos distintos a los especificados en la documentación, si estos son considerados más robustos, no serán contrarios a la certificación Common Criteria aprobada del sistema.

6.1.1.3 CONFIGURACIÓN THALES LUNA K7 CRIPTOGRAFIC MODULE

6.1.1.3.1 Inicialización HSM

61. El módulo criptográfico HSM es un elemento esencial en la seguridad del sistema, de manera que éste debe ser inicializado y configurado de acuerdo con las especificaciones del fabricante.

62. En este sentido, el uso en el sistema de SIAVAL SafeCert Server Signing System (QSCD) del HSM Thales Luna K7 Criptographic Module requiere que se sigan los manuales del fabricante, tanto en su proceso de inicialización, como en el de la configuración necesaria para cumplir Common Criteria, así como su posterior operación.

6.1.1.3.2 Configuración Módulo Criptográfico Common Criteria

63. Los manuales del fabricante Thales que deben seguirse para la configuración y operación cumpliendo con su certificación Common Criteria son los siguientes:

    - 007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ [REF7]
    - 007-000465-001_K7_CC_User_Guidance_Part2_AGD_OPE_RevK [REF8]
    - 007-000466-001_K7_CC_User_Guidance_Part3_AGD_OPE_RevJ [REF9]
    - 007-000467-001_K7_CC_User_Guidance_Part4_AGD_OPE_RevH [REF10]

64. Se debe prestar especial atención al apartado *"CHAPTER 5: Rules for CC compliance"* del documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7], donde se especifican las políticas obligatorias que deben configurarse para cumplir con la certificación Common Criteria del módulo criptográfico.

6.1.1.3.3 Registro del HSM en SafeCert

65. Una vez configurado el HSM es necesario registrarlo en SafeCert desde la vista de **"Repositorios HSM"** de la Consola de Administración del producto. Se puede consultar el funcionamiento de la vista en el apartado *"Repositorios de claves HSM"* del *"Manual de Administración"* [REF1].

6.1.1.4 COMUNICACIÓN SEGURA ENTRE SAFECERT Y LA BASE DE DATOS

6.1.1.4.1 Configuración SSL en Postgre

66. Como ya se ha mencionado previamente, es necesario que Postgre tenga instalado soporte SSL.

67. También debemos tener disponibles una clave privada y su correspondiente certificado en formato PEM, así como el certificado de la CA emisora también en formato PEM.

68. Para activar SSL es necesario editar el fichero **postgresql.conf** en directorio data y configurar los parámetros siguientes:

    ssl = on

    ssl_cert_file = 'server.crt'

ssl_key_file = 'server.key'

ssl_ca_file = 'root.crt'

69. Por defecto, Postgre utiliza el protocolo TLS v1.2 que es uno de los recomendados en la guía *"CCN-STIC 807: Criptología de Empleo en Esquema Nacional de Seguridad"* [REF12].
70. Los ficheros **server.crt**, **server.key** y **root.crt** han de situarse en el directorio **data**.
71. El fichero **server.key** debe tener ***chmod og-rwx***.
72. También es necesario editar el fichero **pg_hba.conf** en directorio **data**, en el que definiremos:
    - Comentar las líneas host para evitar las conexiones mediante protocolo http.
    - Añadir la línea: ***hostssl all all all md5***
73. Es posible también especificar las IPs o rangos de IPs desde las cuales se podrán conectar a la base de datos. Para más detalle de las posibilidades de configuración de la base de datos PostgreSQL, ver manual de configuración del producto.
74. Con esta configuración se precisa de conexión SSL para todas las bases de datos y para todos los usuarios desde todas las direcciones.
75. A continuación, se reiniciará el servidor Postgre y ya tendremos la configuración SSL activada.

6.1.1.4.2 Configuración SSL en SafeCert

76. El primer paso es añadir el certificado del servidor Postgre o el de su CA en el almacén de certificados de confianza del entorno de ejecución (ver apartado 6.1.1.8.1 Insertar un nuevo certificado de confianza en almacén de certificados de Tomcat).
77. Añadir el parámetro ***ssl=true*** en la URL jdbc de acceso a Postgre según el ejemplo:

    jdbc:postgresql://host:port/postgres?ssl=true

78. Mediante esta URL solamente se accederá a Postgre mediante protocolo SSL.
79. A partir de la versión 9.6 de PostgreSQL la URL cambia ligeramente quedando de la siguiente manera:

    jdbc:postgresql://host:port/postgres?sslmode=verify-ca

6.1.1.5 CONFIGURACIÓN SEGURA CON PROXYSFDA

80. Insertar certificado de confianza y establecer las credenciales de autenticación al módulo ProxySFDA en la consola de administración de SafeCert.

6.1.1.6 ACTIVACIÓN DE FIREWALL EN EL APPLIANCE

81. El firewall del *appliance* donde resida SIAVAL SafeCert Server Signing System (QSCD) deberá estar habilitado y con la configuración que a continuación se detalla.
82. Para poder validar que el firewall está habilitado y con la configuración adecuada se deberá acceder a través de la herramienta de administración Webmin y acceder a la opción **"SISTEMA/Gestión de Sistema/Configurar iptables"**. En él se podrá visualizar que el firewall está activado y los puertos a los que se permiten conexiones desde el exterior a

través de dicho firewall, de manera que no admitirá la consulta de información relevante a través de dichos puertos.

83. Una configuración tipo se muestra en la siguiente imagen, donde se observan los puertos habilitados en el sistema filtrados por el firewall. Los puertos pueden variar si estos se modifican en función de la instalación en el entorno operativo.

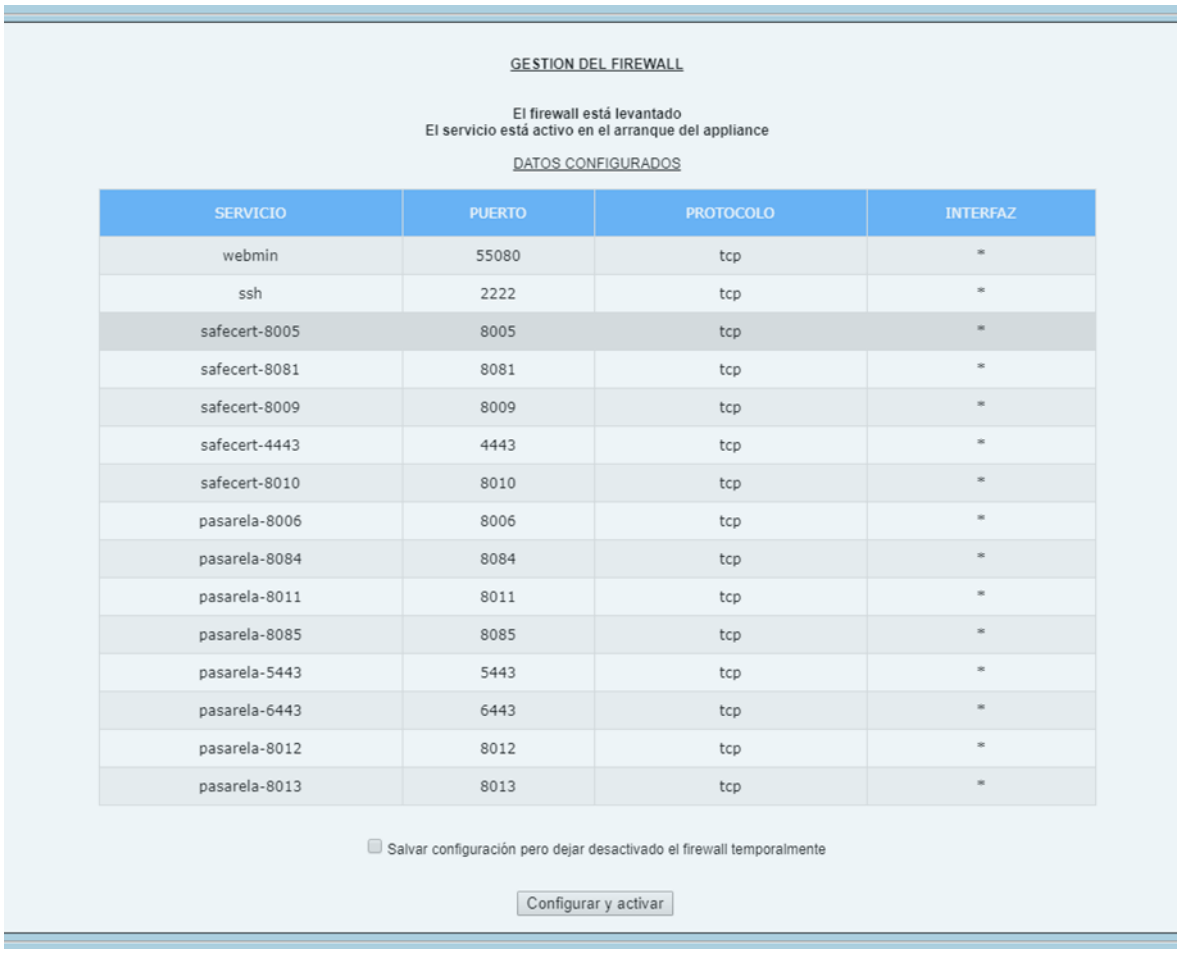

Ilustración 7: Activación Firewall

6.1.1.7 CONFIGURACIÓN SERVICIO DE TIEMPO

84. La gestión y configuración del servicio de tiempo del sistema se realiza accediendo a la opción **"SISTEMA\Gestión del Sistema"**, aparecen dos opciones **"Configurar servicio de tiempo"** y **"Visualizar la hora del sistema"**.

Configurar servicio de tiempo	Configuración de opciones y parámetros del servicio de tiempo
Visualizar la hora del sistema	Permite consultar la hora del sistema y datos relativos al servicio de tiempo

Ilustración 8: Servicio de tiempo

6.1.1.7.1 Configurar servicio de tiempo

85. Esta opción permite configurar varias opciones del servicio de tiempo para la sincronización horaria:

Ilustración 9: Configurar servicio de tiempo

86. Se puede arrancar/parar/reiniciar el servicio de tiempo, seleccionar si se quiere o no arrancar el servicio al reiniciar el *appliance*, seleccionar los servidores de tiempo necesarios.

Ilustración 10: Servidores de tiempo

87. Gestión de la sincronización: Esta opción aparece si el usuario pertenece al grupo Administrador de SIA. Ofrece la posibilidad de activar el chequeo del offset permitiendo configurar el máximo permitido.

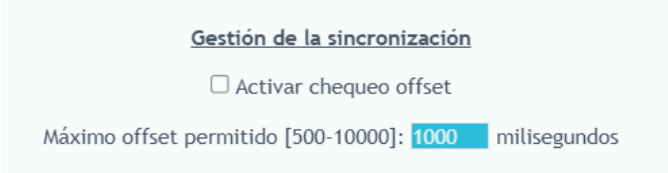

Ilustración 11: Gestión de la sincronización

88. Se pueden activar las estadísticas de sincronización. En la opción **"Visualizar hora del sistema"** se permite ver el contenido de los ficheros obtenidos y en la opción **"Gestión del envío de log vía SCP"** se puede seleccionar la opción para enviar estos ficheros, además del propio del servicio de tiempo, a un servidor remoto.
89. Programar un ajuste de tiempo: El día seleccionado a las 00:00 se forzará el ajuste de tiempo y hasta las 00:10, cada minuto, se dejará constancia en el fichero de log del servicio de tiempo el estado del mismo.
90. El proceso de sincronización horaria no debe dejarse activado constantemente, de esta manera se evita que se produzcan ataques entre el servidor de tiempo y el *appliance*, de manera que un administrador deberá realizar la sincronización horaria en el proceso de puesta en marcha y establecer una política periódica de resincronización, pero sin que quede el servicio de tiempo activado continuamente.
91. **NOTA:** Si se activa la opción **"Gestión de la sincronización"** y/o la **"Programación de un ajuste de tiempo"**, se puede activar la posibilidad de levantar el servicio de tiempo si éste no lo está.

6.1.1.7.2 Visualizar la hora del sistema

92. Esta opción permite visualizar, además de la hora del sistema, los servidores de tiempo configurados, el estado actual de la sincronización. Se indica también si el servicio está activado en el reinicio del *appliance* y permite visualizar el log del propio servicio de tiempo y ver los ficheros generados de estadísticas.

Ilustración 12: Visualizar la hora del Sistema

6.1.1.8 PROCEDIMIENTOS GENERALES PARA LA PREPARACIÓN DE COMPONENTES

6.1.1.8.1 Insertar un nuevo certificado de confianza en almacén de certificados de Tomcat

93. Para validar que un certificado de conexión SSL es de confianza es necesario que éste se encuentre en el almacén de certificados de confianza del Tomcat. Esta validación se puede realizar de dos maneras, insertando el propio certificado del servidor SSL, o insertando el certificado de la CA que emitió el certificado del servidor SSL. La primera forma garantiza que solamente se permitan conexiones con dicho certificado, la segunda evita la actualización del certificado del servidor SSL cuando éste ha caducado, siempre y cuando el nuevo certificado también esté emitido por la misma CA.

94. Java dispone de una utilidad para insertar certificados en el almacén de certificados de confianza. Para ello debemos disponer del certificado, sea el del servidor SSL o el de su CA, en formato PEM o en formato DER.
95. El comando a ejecutar es el siguiente:

    keytool -import -trustcacerts -alias aliasCertificado -file server.cer -keystore certificados_SSL.jks

96. En la inserción del nuevo certificado se solicitará la contraseña del almacén de certificados.
97. Es necesario tener en cuenta que el parámetro *"aliasCertificado"* no debe duplicarse y que para algunas aplicaciones debe tener un valor determinado.
98. Para listar los objetos contenidos en un almacén de certificados se puede ejecutar el comando:

    keytool -list -keystore certificados_SSL.jks

99. Para mostrar el listado de objetos se solicitará la contraseña del almacén de certificados.
100. Es necesario incluir el certificado para SSL de Postgre en el almacén **CACerts**.

6.1.2 CONFIGURACIÓN DEL ENTORNO DE OPERACIÓN

101. Para conseguir securizar SIAVAL SafeCert Server Signing System (QSCD) es necesario configurar una serie de sistemas o módulos tal y como se describe a continuación:

- Configuración SSL Tomcat con TLS v1.2: podemos encontrar toda la información relativa a este punto en el apartado 6.1.1.2.2 Configurar conector SSL con autenticación de cliente.
- Configuración SSL Base de datos: podemos encontrar toda la información relativa a este punto en el apartado 6.1.1.4 Comunicación segura entre SafeCert y la base de datos.
- Autenticación con certificados: podemos encontrar toda la información relativa a este punto en el apartado 6.1.1.2.1 Configurar certificado de autenticación de "admin" para el acceso inicial.
- Configuración segura del envío de OTPs: la gestión y configuración del sistema de envío de OTPs se realizará de manera segura y solamente por las personas autorizadas mediante la configuración de los conectores de SFDA correspondientes. Esta configuración se realiza desde las vistas de **"Conectores de Segundo Factor de Autenticación (SFDA)"** y **"Sistemas de Segundo Factor de Autenticación (SFDA)"** de la Consola de Administración del producto.
- Parámetros de configuración: podemos encontrar toda la información relativa a este punto en el apartado 6.1.5 Configuración del sistema.
- Para conseguir un nivel de seguridad adecuado se exige que las aplicaciones cliente del producto verifiquen el certificado de servidor.
- Activación del Firewall en la máquina *appliance*: El firewall deberá estar habilitado en el sistema tal y como se indica en el apartado 6.1.1.6 Activación de firewall en el appliance.

6.1.3 CONFIGURACIÓN DE LOS AJUSTES DEL HSM

6.1.3.1 VISUALIZAR LAS CARACTERÍSTICAS Y POLÍTICAS DE LA PLATAFORMA

102. Las características y políticas que tiene configuradas el módulo criptográfico se pueden consultar tal como se describe en el apartado *"CHAPTER 4: HSM Configuration" / "Configuring HSM settings" / "Viewing current platform level capabilities and policies"* del documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7].

6.1.3.2 CARACTERÍSTICAS Y POLÍTICA DE LA PARTICIÓN

103. Las características de la partición del módulo criptográfico se pueden consultar tal como se describe en el apartado *"CHAPTER 4: HSM Configuration" / "Configuring HSM settings" / "Partition capabilities and policy"* del documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7].

6.1.3.3 CONFIGURACIÓN DE LAS POLÍTICAS DEL HSM Y DE LA PARTICIÓN

104. La configuración de las políticas, tanto del HSM como de la partición, se puede realizar tal como se indica en el documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7], en el apartado *"CHAPTER 4: HSM Configuration" / "Configuring HSM settings" / "Configuring HSM and partition policies"*.

6.1.3.4 CONFIGURACIONES DEL BLOQUEO DE CUENTAS DEL HSM

105. Se disponen de varias configuraciones diferentes para realizar el bloqueo de cuentas de distintas formas. El comportamiento del producto en este sentido se puede consultar en el apartado *"CHAPTER 4: HSM Configuration" / "Configuring HSM settings" / "Configuring HSM behaviours (account lockout)"* del documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7].

6.1.3.5 REVISIÓN DE LOS SERVICIOS DISPONIBLES

106. Antes de importar o crear claves criptográficas, es importante que se revisen cuáles son las características del HSM que están habilitadas y que su valor esté adecuadamente establecido. Esto se puede realizar tal como se especifica en el apartado *"CHAPTER 4: HSM Configuration" / "Configuring HSM settings" / "Reviewing available services"* del documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7].

6.1.4 CUMPLIMIENTO DE COMMON CRITERIA POR PARTE DEL HSM

107. Se establecen los requisitos mínimos de configuración y las reglas que deben seguirse en una configuración aprobada del HSM Thales Luna que cumpla con las declaraciones de garantía realizadas en la Declaración de Seguridad para el cumplimiento de Common Criteria. Esto se describe en el apartado *"CHAPTER 5: Rules for CC compliance"* del documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7].

108. Entre los requisitos a cumplir por el HSM se requieren los siguientes:

6.1.4.1 ROLES REQUERIDOS

109. Los roles que se requieren para el funcionamiento del HSM en cumplimiento de Common Criteria se describen en el documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7], en el apartado *"CHAPTER 5: Rules for CC compliance" / "Required roles"*.

6.1.4.2 CONFIGURACIÓN DE POLÍTICAS DEL HSM Y DE LA PARTICIÓN

110. La configuración de las políticas del HSM y de la partición que permitan cumplir con la configuración de Common Criteria, se describen en el documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7], en el apartado *"CHAPTER 5: Rules for CC compliance" / "Compliant HSM and partition policy settings"*.

6.1.4.3 LIMITAR EL USO DEL PUERTO USB DEL MÓDULO CRIPTOGRÁFICO

111. Al puerto USB de la placa base del módulo criptográfico no se puede conectar ningún dispositivo USB que no sea un dispositivo específico de Thales diseñado o suministrado para interoperar con el módulo criptográfico Thales Luna K7.

112. La descripción de esta regla se puede consultar en el documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7], en el apartado *"CHAPTER 5: Rules for CC compliance" / "Summary rules that must be followed"*.

6.1.5 CONFIGURACIÓN DEL SISTEMA

113. Existen una serie de parámetros que van a definir el comportamiento del sistema, configurables desde la vista de **"Gestión de la Configuración"** de la Consola de Administración. A continuación, se pueden consultar los valores y efectos de los parámetros más relevantes de cara a la seguridad del sistema:

- Solicitar PIN de certificado al titular.

  VALOR CONFIGURADO: **SI**

- Activación de la Verificación OnLine de la autoría de los datos: En caso de que la verificación de la autoría de los datos se encuentre activada, este parámetro indicará si la verificación se hará en modo OnLine. En caso de seleccionar "SÍ" cada vez que la aplicación requiera el acceso a un registro almacenado en el repositorio de datos, se hará la comprobación de la autoría de dicho registro, alertando al administrador en caso de que haya alguna inconsistencia.

  VALOR CONFIGURADO: **SI**

- Cancelación OnLine de la operación en caso de error de autoría de los datos: En caso de que este parámetro estuviera configurado con el valor "SÍ" y se produjera un error en el acceso a un registro durante el transcurso de una operación, esta operación sería cancelada. Si, por el contrario, el valor fuera "NO", la operación seguiría su curso. En cualquier caso, se notifica al administrador del error de autoría existente.

  VALOR CONFIGURADO: **SI**

- Notificación en base de datos de errores de autoría de datos: En caso de configurar esta entrada con el valor "SÍ", aquellos errores de autoría que se produzcan serán escritos en el log de operaciones.

  VALOR CONFIGURADO: **SI**

- Permitir firmar con certificados caducados: Se puede configurar si, a la hora de realizar una operación de firma, se validará o no la caducidad del certificado.

  VALOR CONFIGURADO: **NO**

- Permitir autenticar con certificados caducados: Se puede configurar si, a la hora de realizar una operación de autenticación, se validará o no la caducidad del certificado.

  VALOR CONFIGURADO: **NO**

- Permitir firmar con certificados con PIN caducado: Se puede configurar si, a la hora de realizar una operación de firma, se validará o no la caducidad del PIN del certificado.

  VALOR CONFIGURADO: **NO**

- Permitir autenticar con certificados con PIN caducado: Se puede configurar si, a la hora de realizar una operación de autenticación, se validará o no la caducidad del PIN del certificado.

  VALOR CONFIGURADO: **NO**

- Permitir el uso de certificados compartidos: Se puede configurar el sistema para que los titulares puedan compartir sus claves.

  VALOR CONFIGURADO: **NO**

- Segundo factor de autenticación obligatorio en certificados personales (no aplica en compartidos):

  VALOR CONFIGURADO: **SI**

- Modo de gestión de logs. Requiere reinicio.

  VALOR CONFIGURADO: **Gestión Interna**

6.1.6 EJECUCIÓN PERIÓDICA DE TAREAS

114. El producto incluye una serie de tareas para facilitar la gestión del sistema y ejecutar la **"Revisión de autoría de los datos"**, la **"Revisión de los certificados caducados"**, etc.

115. Se debe configurar la ejecución periódica de estas tareas desde la vista de **"Gestión de Tareas"** de la Consola de Administración. Se puede consultar más información sobre las tareas disponibles y cómo configurar su ejecución periódica en el apartado *"Tareas"* del *"Manual de Administración"* [REF1] del producto.

6.1.7 AUTORÍA DE LA CONFIGURACIÓN

6.1.7.1 ACTIVACIÓN DE REGISTROS HMAC

116. Como mecanismo de garantía de la autoría de los datos almacenados en la base de datos, el producto dispone de la posibilidad de generar un código HMAC de cada uno de

los registros almacenados en la base de datos de todas o de las tablas y campos que se determinen en la configuración inicial, que se actualiza con cada modificación de los datos.

117. El código HMAC se genera utilizando algoritmos que se encuentran entre los autorizados y recomendados en la guía *"CCN-STIC 807: Criptología de Empleo en Esquema Nacional de Seguridad"* [REF12].

118. Para la activación de este mecanismo es necesario ejecutar el script de inicialización como se indica en el apartado *"Inicialización de la aplicación"* del *"Manual de Instalación"* [REF2] del producto.

119. La configuración HMAC como mínimo debe tener habilitadas las siguientes tablas y campos sin perjuicio que se decida por política habilitar la base de datos completa, además de los campos del titular cifrados:

```
==========================================
INICIO CONFIGURACION HMAC
==========================================
Configuración HMAC habilitada en el sistema.
----------------------------------------------------
Configuracion datos cifrados
Tabla: titular - Campo: dato_personal6 ---> Cifrar: true  Editable: true
Tabla: titular - Campo: dato_personal5 ---> Cifrar: true  Editable: true
Tabla: titular - Campo: dato_personal4 ---> Cifrar: true  Editable: true
Tabla: titular - Campo: dato_personal3 ---> Cifrar: true  Editable: true
Tabla: titular - Campo: dato_personal2 ---> Cifrar: true  Editable: true
Tabla: titular - Campo: dato_personal1 ---> Cifrar: true  Editable: true
Tabla: titular - Campo: email ---> Cifrar: true  Editable: true
Tabla: titular - Campo: dato_personal7 ---> Cifrar: true  Editable: true
----------------------------------------------------
Configuracion de HMAC habilitado por tablas y columnas
Tabla: FuncionalidadPerfil - HMAC: Habilitado
Tabla: CredencialInterna - HMAC: Habilitado
Tabla: Configuration - HMAC: Habilitado
Tabla: Titular - HMAC: Habilitado
Tabla: Operacion - HMAC: Habilitado
Tabla: OTP - HMAC: Habilitado
Tabla: UsuarioPerfilEntidadBase - HMAC: Habilitado
Tabla: AccionFuncionalidad - HMAC: Habilitado
Tabla: CertificadoAuxiliar - HMAC: Habilitado
Tabla: Certificado - HMAC: Habilitado
        Columna: id_certificado - HMAC: Habilitado |
        Columna: id_titular - HMAC: Habilitado |
        Columna: certificado - HMAC: Habilitado |
        Columna: blob_clave - HMAC: Habilitado |
Tabla: UsuarioBase - HMAC: Habilitado
Tabla: OperacionTitular - HMAC: Habilitado
Tabla: AccionFuncPerfil - HMAC: Habilitado
TipoOperacion - HMAC: Habilitado
Tabla: Perfil - HMAC: Habilitado
==========================================
FIN CONFIGURACION HMAC
==========================================
```

120. Esta configuración se podrá consultar exportando la configuración a través de Webmin, mediante la opción **"Exportar Configuración"** y, a través de la herramienta safecert_init, consultar la configuración con la opción **4**:

Gestión de Safecert

Comando	Descripción
Chequear la integridad del producto	Comprobar la integridad de los .war y .jar que integran el producto
	---------- SAFECERT
Iniciar Safecert	Levanta el servicio
Parar Safecert	Para el servicio
Visualizar el estado de SafeCert	Verifica el estado del servicio safecert, si está levantado o no
Ver el estado del HSM y la base de datos	Verifica el estado del HSM y la conexión con la BBDD
Configurar los puertos tcp de Safecert	Permite la edición del fichero de configuración XML de los puertos TCP del servicio
Modificar el almacén de certificados	Permite la modificación del almacén de certificados, clave y alias debido a la caducidad de éste
Configurar los logs de SafeCert Console	Configura el nivel de logs y el fichero que los almacena para la consola
Configurar los logs de SafeCert WebApp	Configura el nivel de logs y el fichero que los almacena para los servicios
Configurar el arranque de SafeCert	Permite la edición del fichero catalina.sh de configuración
Configurar/Chequear la base de datos SafeCert Console	Permite configurar la conexión a la base de datos de la consola y/o chequear si hay comunicación con ésta
Configurar/Chequear la base de datos SafeCert WebApp	Permite configurar la conexión a la base de datos de los servicios y/o chequear si hay comunicación con ésta
Visualizar el log de arranque/parada de SafeCert	Muestra el log de arranque y parada de los servicios
Visualizar log de WS de SafeCert	Muestra los logs de actividad
Visualizar log de la consola de SafeCert	Muestra los logs de la consola
	---------- CONFIGURACION HMAC
Visualizar el estado de la configuración	Permite la consulta del estado de la generación de los ficheros de configuración de hmac
Añadir appliances	Permite gestionar la lista de nombres de appliances que comparten configuración hmac
Exportar configuración	Permite exportar a un fichero .tgz la configuración hmac para poder importarlo en otro/s appliance/s del grupo
Importar configuración	Permite importar la configuración hmac desde un fichero .tgz

Copiar los tres ficheros en la carpeta base de la herramienta safecert-init y ejecutar el comando *rss-hmac.bat* o *.sh* dependiendo el sistema.

Ilustración 13: Configuración HMAC

Seleccionar la opción **4** para visualizar la configuración establecida en el sistema.

6.1.7.2 VERIFICACIÓN DE REGISTROS HMAC

121. Una vez configurado el producto para que genere los códigos HMAC de los datos almacenados en la base de datos es necesario realizar las validaciones correspondientes para garantizar la autoría de dichos datos. Se pueden configurar dos tipos de verificaciones no excluyentes:

- **Verificación *online***: Realiza la verificación de los códigos HMAC en cada acceso a un registro de la base de datos. Para la configuración de este modo de verificación es necesario configurar adecuadamente los parámetros del grupo **"Cancelación OnLine**

de la operación en caso de error de autoría de datos" desde la vista de **"Gestión de la Configuración"** de la Consola de Administración. Se pueden consultar los valores y efectos de cada uno de estos parámetros en el apartado *"Configuración general de SafeCert"* del *"Manual de Administración"* del producto.

- **Verificación *offline***: Realiza la verificación de los códigos HMAC en una tarea independiente denominada **"Revisión de autoría de los datos"** que se puede ejecutar de forma manual desde la vista de **"Gestión de Tareas"** de la Consola de Administración o de forma periódica si se planifica desde esta misma vista. Se puede consultar más información sobre esta tarea y cómo configurar su ejecución periódica en el apartado *"Tareas"* del *"Manual de Administración"* del producto.

6.2 AUTENTICACIÓN

122. Los usuarios se autentican al SafeCert Manager utilizando certificados. Se trata de uno de los mecanismos de autenticación admitidos en el ENS, tal como se establece en la guía *"CCN-STIC 807: Criptología de Empleo en Esquema Nacional de Seguridad"* [REF12].

123. Por otro lado, los usuarios se autentican al *appliance* físico por SSH con un par de claves, pública y privada. El protocolo utilizado es el SSH v2, tal como se recomienda en la guía *"CCN-STIC 807: Criptología de Empleo en Esquema Nacional de Seguridad"* [REF12].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

124. La configuración del SafeCert Manager se realiza de forma remota, utilizando, tanto la Consola de administración del SafeCert Manager, como la herramienta de administración del sistema Webmin.

125. El acceso a la Consola del SafeCert Manager se realiza mediante SSL usando el protocolo TLS v1.2 con autenticación con certificados, siendo este protocolo uno de los autorizados en el ENS, tal cómo se describe en la guía *"CCN-STIC 807: Criptología de Empleo en Esquema Nacional de Seguridad"* [REF12].

126. El acceso al *appliance* que se realiza mediante SSH utiliza SSH v2, que es la única versión de SSH autorizada para su uso en el ENS, tal cómo se describe en la guía *"CCN-STIC 807: Criptología de Empleo en Esquema Nacional de Seguridad"* [REF12].

127. Para la inicialización/configuración del HSM se requiere acceso local, según indican los manuales del fabricante del módulo criptográfico, concretamente en el *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ.pdf"* [REF7].

128. Las operaciones criptográficas que se utilizan en el sistema se realizan en un módulo criptográfico, HSM, certificado Common Criteria.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

129. En el sistema, se restringe el acceso al servidor físico y al servidor de aplicaciones para la preparación del entorno y para la instalación, administración y operación del sistema a un conjunto de usuarios con los permisos necesarios para realizar la función para la que se han creado.

130. Se definen usuarios con acceso al servidor físico y con un nivel de autorización en función de las tareas asignadas a cada uno de ellos. Estos usuarios únicamente podrán ser utilizados por personal de SIA autorizado para llevar a cabo la puesta en marcha y mantenimiento del sistema.

- root: Usuario de sistema operativo con control total sobre el servidor físico. Utilizado para la preparación del entorno y la instalación del producto.
- siauser: Usuario con acceso vía SSH al servidor físico. Utilizado durante la preparación del entorno y la instalación del producto. La conexión vía SSH se realizará mediante autenticación con certificados.
- eastsp: usuario propietario del producto y sus recursos, pero sin permisos de conexión remota al servidor físico.

131. Se definen usuarios con acceso a la aplicación de administración y operación Webmin y con un nivel de autorización en función de las tareas asignadas a cada uno de ellos.

- operacion: Usuario de la herramienta Webmin utilizado por el cliente final para realizar operaciones de monitorización del producto, consulta de Logs del producto y operaciones básicas sobre el servidor de aplicaciones (arranque y parada).
- admin (Webmin): Usuario de la herramienta Webmin utilizado por el instalador para realizar operaciones de configuración del entorno.
- admin (SafeCert): Usuario del sistema SafeCert con acceso a todas las operaciones del producto. Utilizado por el personal encargado de la instalación y actualización del producto.
- audit (SafeCert): Usuario del sistema SafeCert utilizado por el cliente final para realizar operaciones de consulta sobre las vistas de la Consola de Administración, pero sin permisos para la modificación de datos.
- adminConsole (SafeCert): Usuario del sistema SafeCert con acceso a todas las vistas de la Consola de Administración tanto de consulta como de edición.
- adminSafeCertWS (SafeCert): Usuario del sistema SafeCert con permisos para ejecutar todos los servicios de las interfaces del producto (Interfaz_Titular, Interfaz_Admin e Interfaz_Firma).
- userAdmin (SafeCert): Usuario del sistema SafeCert con permisos para ejecutar los servicios de las interfaces Interfaz_Titular e Interfaz_Admin.
- userFirma (SafeCert): Usuario del sistema SafeCert con acceso a ejecutar los servicios del interfaz Interfaz_Firma.

132. También se definen los roles de acceso al módulo criptográfico, HSM, que se describen en el documento *"007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ"* [REF7], en el apartado *"CHAPTER 2: Planning your deployment" / "Assigning people to HSM roles"*.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

133. La configuración de los interfaces de acceso, tanto a la consola de administración, como a los servicios web del producto, se describe en el *"Manual de configuración segura"* [REF6] y se indica en el apartado 6.1.1.2 Configurar comunicación SSL en el servidor de aplicaciones, de este mismo documento, en el que se mencionan los puertos habilitados en el sistema.

6.5 GESTIÓN DE CERTIFICADOS

134. Los certificados utilizados por el sistema se cargan en el *appliance* para ser utilizados por el producto tal como se menciona en el apartado 6.1.1.2 Configurar comunicación SSL en el servidor de aplicaciones.

6.6 SERVIDORES DE AUTENTICACIÓN

135. El sistema no utiliza servidores externos de autenticación.

6.7 SINCRONIZACIÓN

136. La sincronización segura del producto se lleva a cabo tal cómo se especifica en el apartado 6.1.1.7 Configuración servicio de tiempo.

6.8 ACTUALIZACIONES

137. Las actualizaciones del producto se proporcionan de forma segura en ficheros firmados y se despliegan en el *appliance* mediante una opción específica facilitada por la herramienta de administración, Webmin.

6.9 AUTO-CHEQUEOS

138. En el *appliance*, al ir a arrancar el SafeCert Manager, se chequea el estado del módulo criptográfico, HSM, verificando que éste se encuentra operativo.

139. En el caso de que el HSM no se encuentre operativo, se muestra un mensaje de alerta al administrador, para que éste realice la comprobación correspondiente. En cualquier caso, aunque el HSM no se encuentre operativo, se permite el arranque del producto.

140. Bajo demanda, el administrador puede chequear periódicamente la integridad y validez de los hashes de los productos instalados.

141. Si los hashes de los productos instalados no coinciden con los que se esperan, será señal de que los productos habrán sufrido algún cambio desde su instalación segura en el *appliance* y el administrador podrá tomar las acciones que considere oportunas.

6.10 ALTA DISPONIBILIDAD

142. No es necesario configurar nada específico en el SIAVAL SafeCert Server Signing System (QSCD) para que funcione en alta disponibilidad.

143. Si se desea el uso del producto en alta disponibilidad, la configuración se podrá realizar en el entorno de operación mediante balanceadores externos que faciliten acceso a diversas instancias del SIAVAL SafeCert Server Signing System (QSCD), sin necesidad de configurar nada especial en el producto en sí. En las distintas instancias del producto se deberán usar las mismas claves maestras del HSM utilizando el procedimiento del backup/recuperación del módulo criptográfico.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

144. Los eventos de auditoría se registran y su autoría se controla mediante la activación de registros HMAC, tal como se expone en el apartado 6.1.7 Autoría de la configuración.

145. Los registros de auditoría se almacenan en base de datos y pueden ser consultados a través de la herramienta de administración del sistema por los usuarios administradores o auditores, tal como se indica en el *"Manual de Administración"* [REF1], en los apartados *"4.10 Log de operaciones"* y *"4.12 Log de eventos de titular generado por LogManager"*.

146. Los códigos de operación utilizados en el log de auditoría se describen en el *"Manual de Administración"* [REF1] del SIAVAL SafeCert, en los apartados *"5.2 Códigos de operación del sistema (logs de auditoría)"* y *"5.3 Códigos de operación del titular (logs de operaciones del titular)"*.

6.11.2 ALMACENAMIENTO LOCAL

147. Los eventos de auditoría no se almacenan localmente.

148. Localmente se generan ficheros de log que, aunque no son de auditoría, recogen la actividad del sistema y que pueden ser consultados a través de la herramienta de administración del entorno, Webmin

6.11.3 ALMACENAMIENTO REMOTO

149. Los registros de auditoría se almacenan en la base de datos utilizada por el SIAVAL SafeCert Server Signing System (QSCD), que se encuentra en red, y no se envían a ningún sistema externo.

6.12 BACKUP

150. Toda la configuración del SIAVAL SafeCert se almacena en la base de datos utilizada por el producto. Entre ella se encuentran la información de los roles, los usuarios, la información de autenticación y de autorización, etc. En la base de datos también se encuentra la información de auditoría del producto.

151. El backup de la configuración se consigue realizando un backup de la base de datos y se puede llevar a cabo periódicamente, con la frecuencia que se desee.

7 REFERENCIAS

153. La documentación que se ha referenciado a lo largo de la guía es:

REF1	SIAVAL SafeCert - Manual de Administración
REF2	SIAVAL SafeCert - Manual de Instalación
REF3	SIAVAL SafeCert - Manual de Integración
REF4	SIAVAL SafeCert - Manual de Integración ProxySFDA
REF5	SIAVAL SafeCert - Manual de operaciones
REF6	SIAVAL SafeCert - Manual de configuración segura
REF7	007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevJ
REF8	007-000465-001_K7_CC_User_Guidance_Part2_AGD_OPE_RevK
REF9	007-000466-001_K7_CC_User_Guidance_Part3_AGD_OPE_RevJ
REF10	007-000467-001_K7_CC_User_Guidance_Part4_AGD_OPE_RevH
REF11	SIAVAL SafeCert - Manual de composición
REF12	CNN-STIC 807: Criptología de Empleo en el Esquema Nacional de Seguridad

8 ABREVIATURAS

CPSTIC	Catálogo de Productos y Servicios de Seguridad TIC.
ENS	Esquema Nacional de Seguridad.
HMAC	Hash-based Message Authentication Code.
HSM	Hardware Security Module.
MAC	Message Authentication Code.
OTP	One-Time Password.
PKCS	Public-Key Cryptography Standards
QSCD	Qualified Signature Creation Device.
SCP	Secure Copy Protocol.
SFDA	Segundo Factor de Autenticación.
SSH	Secure Shell.
SSL	Secure Sockets Layer.
TLS	Transport Layer Security.