centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1002

Procedimiento de Empleo Seguro
u.trust Anchor v4.49.1



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 3
3 ORGANIZACIÓN DEL DOCUMENTO 4
4 FASE PREVIA A LA INSTALACIÓN 5
4.1 ENTREGA SEGURA DEL PRODUCTO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 6
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 7
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 9
6 FASE DE CONFIGURACIÓN 10
6.1 MODO DE OPERACIÓN SEGURO 10
6.2 AUTENTICACIÓN 10
6.3 ADMINISTRACIÓN DEL PRODUCTO 11
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 11
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 11
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 12
6.5 GESTIÓN DE CERTIFICADOS 12
6.6 SINCRONIZACIÓN 13
6.7 ACTUALIZACIONES 13
6.8 AUTO-CHEQUEOS 13
6.9 AUDITORÍA 14
6.9.1 REGISTRO DE EVENTOS 14
6.9.2 ALMACENAMIENTO LOCAL 15
6.9.3 ALMACENAMIENTO REMOTO 15
6.10 BACKUP 16
7 REFERENCIAS 17
8 ABREVIATURAS 18

ÍNDICE DE TABLAS

Tabla 1: Requisitos de temperatura y humedad del PCI [REF3] 6
Tabla 2: Requisitos de temperatura y humedad del entorno LAN [REF3] 6
Tabla 3. Requisitos del entorno del PCI [REF3] 7
Tabla 4. Requisitos del entorno del LAN [REF3] 7

ÍNDICE DE FIGURAS

Figura 1: Componentes del entorno [REF10] 8

1 INTRODUCCIÓN

u.trust Anchor es un módulo de seguridad de hardware (HSM), con el objetivo principal de proporcionar servicios criptográficos seguros en entornos que requieren altos niveles de protección. Este producto es compatible con APIs criptográficas estandarizadas como: PKCS#11, JCE, OpenSSL, CSP/CNG y EKM, que facilita su integración en múltiples entornos y aplicaciones.

Entre sus capacidades se incluyen: la firma y verificación de datos, el cifrado o descifrado, cálculo MAC, derivación y acuerdo de claves, funciones hash, generación integrada de números aleatorios, generación segura de claves, almacenamiento interno y externo de claves protegidas, además de proveer de un mecanismo de actualización de software seguro y otras funciones de gestión de claves en un entorno no manipulable.

Este producto introduce el concepto de HSM *contenedorizados* (cHSM). *u.trust Anchor* puede desplegar hasta 31 cHSMs en paralelo, cada uno operando de forma independiente y ofreciendo las mismas funcionalidades que un HSM tradicional. *u.trust Anchor*, además de permitir la escalabilidad rápidamente, también permite a los proveedores ofrecer HSM como servicio (HSMaaS) en múltiples casos de uso.

- Este producto garantiza la conformidad con los estándares más estrictos de seguridad y calidad: conformidad con las directrices establecidas en la guía CCN-STIC-140-E5 para la taxonomía especifica de Módulo de seguridad hardware (HSM) 17
- Cumplimiento con la normativa *Common Criteria for Information Technology Security Evaluation*, Versión 3.1, Revisión 5.

2 OBJETO Y ALCANCE

El presente documento tiene por objeto facilitar la configuración y el uso del *u.Trust Anchor* así como proteger el entorno en el que se implanta. Además, se especifica la configuración necesaria para que el producto cumpla con los requisitos de la taxonomía: CCN-STIC-140-E5 17

La versión cualificada para este producto es el *u.trust Anchor* v4.49.1. Este producto viene en forma de PCI plug-in card. PCI P/N CSAR-7.3.0.3.x-PCIe-CC, estando x entre 00 y 99.

u.trust Anchor tiene la capacidad de soportar los siguientes sistemas:

- Linux x64
- Red Hat Enterprise Linux 7/8
- CentOS 7/8
- SUSE Linux Enterprise Server 12/15
- Ubuntu 18.04 LTS / 20.04 LTS

El producto *u.Trust Anchor* ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF8].

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

Las organizaciones interesadas en *u.Trust Anchor* pueden adquirir el producto accediendo a la página web oficial de Utimaco 17

El producto se puede entregar como PCIe o integrado en el Utimaco *u.trust Anchor* LAN. En ambos casos, el equipo se entrega empaquetado con las respectivas medidas de seguridad junto con una pegatina con el número de seguimiento del envío. El embalaje identifica al fabricante Utimaco por su logo, además, los sellos de seguridad no deben encontrarse dañados. Todo el proceso de verificación del paquete se encuentra en el Manual Operativo proporcionado 17, capitulo 4.2 "*Checking the Security Bag and Deliverables*".

Se pueden descargar todos los recursos necesarios para operar el *u.trust Anchor* desde el portal de descarga de Utimaco. Estos recursos son: documentación del usuario, *Global Initial Admin Key*, *Utimaco root certificate* y las herramientas de administración para el dispositivo. Para verificar estos descargables, el checksum SHA-256 del paquete de recursos debe ser el que se especificó en la información del envío.

Además del PCI, este también puede venir integrado en Utimaco *u.trust Anchor* LAN, un dispositivo de red hardware. El dispositivo contiene todo lo necesario para poner en funcionamiento *el u.trust Anchor.* Se debe comprobar que todos los componentes estén completos.

La integridad y la autenticidad de los componentes del *u.trust Anchor* pueden comprobarse e identificarse siguiendo las instrucciones descritas en el capítulo 4.3 "Verifying the Device" del Administrator Manual 17:

- Para dirigirse al dispositivo predeterminado es:

```
/dev/cs2.0
```

- El dispositivo puede integrarse tanto en el ordenador local del operador como en un host remoto. Si se desea dirigirse al dispositivo *u.trust Anchor* que está integrado en tu dispositivo local, se utilizará el parámetro **-d** de la siguiente forma:

```
-d /dev/cs2.0
```

- Para dirigirte a un dispositivo *u.trust Anchor* LAN, permitiendo direccionar el dispositivo, se debe usar:

```
-d HSM6020 -p 4000
```

- Para hosts remotos, el argumento **-p** especifica el puerto TCP al que conectarse. El número de puerto se ignora cuando se usa un nodo de dispositivo.
- Verificar el dispositivo: Antes de integrar el certificado, hay que verificar el dispositivo, siguiendo los pasos detallados a continuación:

NOTA: en los comandos el valor *<device>* será proporcionado por Utimaco.

a) Verificar mediante el comando *gladm*, la versión de los componentes del HSM así como que la información del sistema declara '*u.trust Anchor CC*'

```
gladm -d <device> system-get-info
```

b) Usar el certificado raíz de Utimaco (*Utimaco root certificate)*, que se entrega dentro de los recursos entregados por el fabricante. El comando *gladm system-get-info*, ofrece un parámetro adicional de verificación.

```
gladm -d <device> --vendor=<certificado.cer> -u admin -k giak.pem
system-get-info
```

NOTA: Al usar el parámetro *--vendor=<certificado.cer>* y las credenciales de autenticación, se verifica la integridad del certificado. Si el comando se ejecuta correctamente, el certificado queda verificado. Si el certificado no se verifica, devuelve un error y el comando no se ejecuta. En ese caso, contactar inmediatamente con Utimaco.

4.2 ENTORNO DE INSTALACIÓN SEGURO

U.Trust Anchor solo debe instalarse, utilizarse y almacenarse en un entorno protegido que limite el acceso físico al dispositivo a los administradores autorizados. Este puede ser un Centro de Procesamiento de Datos o un lugar restringido que cumpla los requisitos ambientales y de seguridad que se resumen a continuación.

Los requisitos de temperatura y humedad del PCI son los siguientes:

TEMPERATURA AMBIENTE	En funcionamiento: De +10° C a +40° C (de +50° F a +104° F) En almacenamiento: De -10° C a +55° C (de +14° F a +131° F)
HUMEDAD	Del 10% al 95% de humedad relativa, sin condensación.

Tabla 1: Requisitos de temperatura y humedad del PCI 17

En el caso de utilizar la versión integrada en *u.trust Anchor* LAN, los requisitos son los siguientes:

TEMPERATURA AMBIENTE	En funcionamiento: De +10° C a +50° C (de +50° F a +122° F) En almacenamiento: De -10° C a +55° C (de +14° F a +131° F)
HUMEDAD	Del 10% al 95% de humedad relativa, sin condensación.

Tabla 2: Requisitos de temperatura y humedad del entorno LAN 17

Además, el entorno operativo del *u.trust Anchor* debe cumplir los siguientes requisitos de seguridad:

- El PIN pad es guardado de forma segura y sus precintos no están dañados, tampoco puede ser supervisado ni monitorizado durante la introducción de la contraseña.
- Las tarjetas inteligentes se han guardado de forma segura.
- El ordenador de administración está libre de malwares, es de confianza y sólo se instala y ejecuta en él software de confianza, además solo son posibles los cambios autorizados en el software y en la configuración del dispositivo.
- Sólo las personas de confianza tienen acceso físico y de red al *u.trust Anchor* y al ordenador de administración.
- La administración y la configuración/operación del ordenador de administración deberán ser realizadas exclusivamente por personas verificadas, de confianza, autorizadas y bien formadas.

- Se requieren inspecciones periódicas para disuadir y detectar manipulaciones (incluidos intentos de acceso a canales laterales o a las conexiones entre partes físicamente separadas del *u.trust Anchor*).
- El *u.trust Anchor* debe estar protegido frente a posibles ataques basados en emanaciones, como emanaciones electromagnéticas o ataques de Análisis de Potencia Simple o Análisis de Potencia Diferencial.
- Se recomienda encarecidamente utilizar el ordenador de administración exclusivamente para la operación y administración del *u.trust Anchor*. No debería haber acceso a Internet y la administración remota del equipo debe limitarse al mínimo.
- Sólo las personas de confianza tienen acceso físico y de red al *u.trust Anchor* y al ordenador de administración en el que se instale la tarjeta PCIe y deberá estar situado en una zona de alta seguridad. Las personas no autorizadas no podrán acceder al ordenador de administración y deberá estar protegido por un mecanismo de control de acceso, por ejemplo, contraseña y/o tarjeta inteligente.

4.3 REGISTRO Y LICENCIAS

Cada *u.trust Anchor* se entrega con una única clave asimétrica basada en curvas elípticas, que se genera durante el proceso de fabricación. La clave pública es firmada por el certificado de autoridad (CA) de Utimaco y el certificado resultante se carga en el HSM. Este certificado es un certificado CA y permite al dispositivo firmar a un numero de certificados de entidades finales.

El proceso se explica con más detalle en la "Quick Start Guide" proporcionada 17, capitulo 2.2 "*The chain of trust model*".

4.4 CONSIDERACIONES PREVIAS

Previo al inicio de la instalación y configuración segura del producto, debe tenerse en cuenta las características de los distintos casos de uso: PCI y el entorno LAN.

Para el uso del PCI se detallan los siguientes requisitos

ALTURA DE FUNCIONAMIENTO	Máximo 2000m (6500 pies)
NIVEL DE CONTAMINACIÓN	Máximo 2 (según IEC-60664-1)
CLASE DE PROTECCCIÓN	IP00

Tabla 3. Requisitos del entorno del PCI 17

En el caso de utilizar la versión integrada en *u.trust Anchor* LAN, los requisitos son los siguientes:

ALTURA DE FUNCIONAMIENTO	Máximo 2000m (6500 pies)
NIVEL DE CONTAMINACIÓN	Máximo 2 (según IEC-60664-1)
CLASE DE PROTECCCIÓN	IP20

Tabla 4. Requisitos del entorno del LAN 17

Se necesitará un ordenador con alguno de los sistemas operativos indicados en la sección 2 de este documento.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

Para utilizar el PCI *u.trust Anchor*, debe montarse en el ordenador de administración con una ranura PCI libre o en el *u.trust Anchor* LAN.

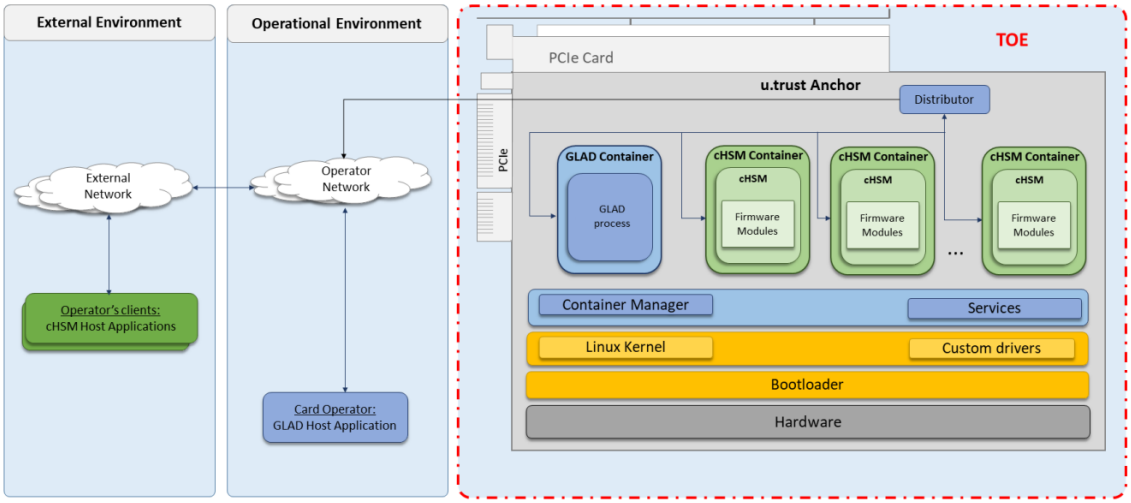


Figura 1: Componentes del entorno 17

El producto PCI tiene que estar alojado en un operador de tarjetas, *GLAD Host Application,* cuyo entorno operacional se considere fiable y seguro, visible en la Figura 1. El entorno de operacional se compone de una *Operator Network,* que actúa como la red interna por la que se comunica la infraestructura del operador, y de la aplicación *Card Operator*, que es la aplicación encargada de interactuar con la tarjeta PCI a través de dicha red.

El operador puede facilitar a los clientes el acceso remoto a los cHSM a través de una red de comunicaciones. Sin embargo, el entorno externo no se encuentra bajo el control ni la responsabilidad directa del operador.

5 FASE DE INSTALACIÓN

Para realizar la instalación del PCI *u.trust Anchor* correctamente se necesitarán las siguientes herramientas:

- En el capítulo 4.1 "*Installing gladm*" del *Administrator Manual* 17.
- En el capítulo 4.2 "*Installing pci driver"* del *Administrator Manual* 17.

Mediante el uso de herramienta *csadm* administraremos los HSM *contenedorizados* (cHSM). Su instalación viene detallada en el capítulo 2 "*Installation*" del *csadm Manual* 17.

Cuando se realice la administración del *u.trust Anchor* LAN, será necesario habilitar el demonio SSH siguiendo los pasos que se detallan en el capítulo 3.4 "*Enable SSH Daemon*" del *u.trust Anchor LAN V5 CC - Quick Start Guide* 17.

La instalación correcta del *u.trust Anchor* LAN vendrá descrita en el capítulo 4 "*Bringing into service"* del Operating Manual 17. En este capítulo primero se detallarán los requisitos previos, los cuales ya se han mencionado anteriormente, el procedimiento para la instalación física, la puesta en marcha del LAN y la identificación de este para asegurar la integridad del dispositivo. Para contrastar información, también se puede revisar en el capítulo 3 "*Getting Started*" del "Quick Start Guide" 17.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

El dispositivo tiene diferentes variantes de configuración, que reflejan distintas capacidades y niveles de flexibilidad en el uso de los HSM *contenedorizados* (cHSMs):

- u.trust Anchor CSAR Premium (con un número flexible de hasta 31 cHSMs)
- u.trust Anchor CSAR Plus (con un número flexible de hasta 16 cHSMs)
- u.trust Anchor CSAR Standard (con un número flexible de hasta 8 cHSMs)
- u.trust Anchor Se40k (con hasta 12 cHSMs, para ser usados en un único clúster)
- u.trust Anchor Se15k (con hasta 4 cHSMs, para ser usados en un único clúster)

Sin embargo, no es necesario activar una configuración específica para que este producto opere en el modo de cumplimiento *common criteria*, ya que este es el único modo de funcionamiento del producto.

6.2 AUTENTICACIÓN

Al registrarse, cada usuario debe elegir su mecanismo de autenticación. El producto ofrece tres mecanismos diferentes para la autenticación:

- **Mecanismo de autenticación de firma RSA**: se realiza con una firma RSA generada utilizando el esquema RSASSA-PKCS1-v1_5 según el estándar [PKCS#1], con longitudes de clave de un mínimo de 2048 y un máximo de 16384 bits. Aunque lo recomendable es usar mínimo 3072 bits.
- **Mecanismo de autenticación de firma ECDSA**: se realiza con una firma ECDSA generada utilizando el esquema, según el estándar [ANSI-X9.62], con longitudes de clave de mínimo 224 bits
- **Mecanismo de autenticación de contraseña HMAC**: La autenticación se realiza con un HMAC, usando la contraseña de autenticación como clave HMAC de acuerdo con el [FIPS 198] y [RFC 2104], con longitudes de entre 4 y 1024 bytes.

Para intercambiar datos sensibles, debe establecerse una sesión de mensajería segura entre el *u.trust Anchor* y la aplicación cliente. Dicha sesión de mensajería segura es obligatoria para cada comando que requiera autenticación del usuario. Este mecanismo garantiza una comunicación confiable para aplicaciones cliente (locales o remotas).

El producto admite la autenticación de usuarios y la mensajería segura mediante generación y verificación de firmas RSA y ECDSA, cálculo de valores hash, derivación de claves, cálculo de HMAC, acuerdo de claves EC Diffie-Hellman, cifrado y descifrado AES, cálculo y verificación de MAC, y generación de números aleatorios mediante un RNG híbrido para el valor de desafío y la clave ECDH efímera.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

Como herramientas de administración tenemos tanto *gladm* como *csadm*. Estas herramientas se complementan entre sí, permitiendo la gestión de certificados y claves, gestión de usuarios, puesta en marcha del dispositivo, supervisión del estado y gestión de los cHSMs. Aunque *gladm* se utilizará principalmente para la gestión del sistema y *csadm* para la gestión de los cHSM.

El *u.trust Anchor* permite conectarse al LAN tanto local como remotamente, para acceder remotamente se podrá acceder mediante SSH haciendo uso de PuTTY o WinSCP en Windows o ssh en Linux.

El *u.trust anchor* LAN posee una pantalla con varias teclas de control, a través de esta se puede acceder a las opciones de menú necesarias para realizar las funciones de administración más importantes, incluida la puesta en servicio y la supervisión del estado.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

El usuario que inicia por primera vez el *u.trust Anchor* obtiene por defecto el usuario ADMIN, cuyo rol es *Global Administrator*. Para las credenciales de este usuario se usará la clave proporcionada por Utimaco (GIAK) en el paquete descargado y solo da acceso a un set limitado de comandos. Esta clave debe ser sustituida por una clave propia (GAAK), para así poder tener acceso a todos los comandos de ADMIN. La clave utilizará RSA y tendrá un mínimo de 3072 bits.

El producto admite los siguientes roles para los distintos usuarios:

- Roles de administrador:
    - *Global Administrator:* Se encarga de la inicialización global del dispositivo, administración del dispositivo y gestión del cHSM.
    - *User Administrator* (rol a nivel de cHSM): Este rol realiza tareas de gestión de usuarios del cHSM, como creación y eliminación de usuarios del cHSM.
    - *cHSM Administrator* (rol a nivel de cHSM): La función principal es la administración general del cHSM, como gestionar la Clave Maestra de Respaldo del cHSM.
    - *Key Manager* (rol a nivel de cHSM): El papel de este rol es llevar a cabo tareas de gestión de claves de los usuarios en el cHSM, como generación de claves, exportación e importación, copia de seguridad y restauración de claves, eliminación de claves.
    - *SO (Security Officer)* (rol a nivel de cHSM): Realiza tareas como la creación, modificación o eliminación de objetos de configuración específicos de grupos de claves e iniciación de un grupo de claves.
- *Key User* (rol a nivel de cHSM): Hace uso del cHSM para servicios criptográficos, como la creación de firmas.
- *Client Application*: Utiliza el *u.trust Anchor* para crear un canal seguro de comunicación; por lo tanto, cada usuario autenticado puede asumir adicionalmente este rol.

Para las contraseñas se aplican las siguientes normas:

- La longitud mínima recomendada de la contraseña es de 12 caracteres.
- La contraseña contendrá letras mayúsculas y minúsculas, al menos dos caracteres especiales y números. Se recomienda el uso de los 4 y al menos un mínimo de 3.
- La contraseña se cambiará periódicamente, al menos cada 60 días.
- El sistema bloqueará la autorización del usuario tras un número bien definido de intentos de autorización fallidos. Se recomienda establecer un umbral de 3 intentos fallidos de autenticación.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

En el caso de utilizar la versión integrada en *u.trust Anchor* LAN, es necesario asignar una dirección IP al *u.trust Anchor* LAN para garantizar que se pueda acceder a él a través de la red. La dirección IP del *u.trust Anchor* LAN puede ser estática o configurarse automáticamente mediante DHCP, en caso de que sea estática, la dirección IP será 10.10.10.10 y estará asignada a la interfaz eth1, por otra parte, en caso de usar la configuración por DHCP, la interfaz eth0 estará configurada por defecto para utilizar esta configuración.

En el documento “u.trust Anchor LAN V5 CC - Administration Manual” encontraremos la siguiente información 17:

- Las instrucciones para configurar una dirección IPv4 estática para la *u.trust Anchor* LAN se encuentran en el capítulo 3.4.1.1 " *Entering a static IPv4 Address With the Front Panel*".
- Para configurar una dirección IPv4 estática para la pasarela de red por defecto podremos seguir la guía se encuentran en el capítulo 3.4.1.2 "*Entering the IPv4 Default Gateway With the Front Panel*".
- En caso de configurar la dirección IPv4 para la *u.trust Anchor* LAN y la pasarela de red por defecto mediante un servidor DHCP se pueden consultar los pasos en el capítulo 3.4.2 "*Setting up Dynamic IPv4 Addresses With the Front Panel*".
- Las instrucciones para configurar la dirección IPv4 haciendo uso de la línea de comandos en lugar del panel central y mediante un servidor DHCP se encuentran en el capítulo 3.4.3 "*Setting up the IPv4 Configuration With a Command-Line*".
- Por defecto la IPv6 viene deshabilitada. Las instrucciones para habilitar y configurar la dirección IPv6 mediante un servidor DHCP se encuentran en el capítulo 3.4.4 "*Setting up the IPv6 Configuration With a Command-Line*".

6.5 GESTIÓN DE CERTIFICADOS

El *u.trust Anchor* soporta los siguientes mecanismos criptográficos en cumplimiento con las especificaciones de la guía CCN-STC-807:

- Cifrado de bloque AES en los modos CBC, CTR y GCM con una longitud de clave de 32 bytes, usado para encriptación y desencriptación.
- AES CMAC y GMAC con una longitud de clave de 32 bytes.
- ECDSA con una longitud de clave de mínimo 256 bits, usado para generación o verificación de firma ECDSA.

- Esquema de encriptación RSA con una longitud de clave de mínimo 3072 bits, usado para encriptación y desencriptación y para generación o verificación de firma RSA.
- Algoritmo Hash SHA3-256, SHA3-384 y SHA3-512.
- Diffie-Hellman (DH) con una longitud de clave de mínimo 3072 bits.
- EC Diffie-Hellman (ECDH) con una longitud de clave de mínimo 256 bits.
- Key derivation basado en HMAC.

El fabricante proporcionará la información necesaria para realizar la configuración de estos mecanismos.

6.6 SINCRONIZACIÓN

La sincronización horaria se establece manualmente mediante la herramienta *gladm* en el ordenador central. Para ello se utilizan los siguientes comandos:

```
gladm -d <device> system-get-time
```

Este comando te devolverá la fecha y hora del dispositivo, habrá que revisar que coincidan con la hora del sistema local, en caso de que difieran hay que realizar el siguiente comando:

```
gladm -d <device> -u admin -k giak.pem system-set-time
```

Se recomienda consultar el capítulo 4.3.1 "*Verifying the Device*" del “u.trust Anchor CC - Administration Manual” 17 para obtener información detallada sobre cómo utilizar los comandos relacionados.

6.7 ACTUALIZACIONES

La actualización del firmware de un dispositivo *u.trust Anchor* se realiza haciendo uso de la herramienta *gladm* mediante paquetes *rauc* junto con un *manifest* dentro de un archivo *squashfs*. El paquete *rauc* está firmado utilizando una firma “Cryptographic Message Syntax” (CMS/PKCS#7).

Las actualizaciones utilizan un esquema A/B, lo que significa que existe una ranura en espera (*standby slot*) que se actualiza mientras la otra está en uso para el arranque.

Para realizar una actualización completa, el procedimiento debe repetirse según se describe en el capítulo 5.3 “*Updating u.trust Anchor*” del “u.trust Anchor CC - Administration Manual”.17 El administrador del producto debe revisar de forma periódica la existencia de nuevas actualizaciones y vulnerabilidades del producto.

6.8 AUTO-CHEQUEOS

u.trust Anchor, para garantizar un funcionamiento correcto, puede ejecutar un conjunto de los siguientes auto-chequeos durante:

El arranque inicial (al encender o reiniciar):

- Prueba de integridad del software/firmware.
- Pruebas de algoritmos criptográficos.
- Pruebas del generador de números aleatorios.

La descarga de firmware:

- Prueba de descarga de firmware (mediante verificación de firma ECDSA).

Cada solicitud de PTRNG:

- Prueba en línea del PTRNG.
- Pruebas continuas de salud.

Cada solicitud de DRBG:

- Prueba condicional de DRBG.

La generación de pares de claves:

- Prueba de consistencia por pares (*pair-wise consistency test*).

Al encenderse, el dispositivo realiza comprobaciones de integridad del firmware durante toda la cadena de arranque. Si alguna de las comprobaciones de integridad del firmware durante el arranque de la imagen operativa principal falla antes de que se haya iniciado cualquier cHSM, el dispositivo puede intentar arrancar la imagen operativa de respaldo en su lugar, incluyendo también las comprobaciones de integridad del firmware de dicha imagen de respaldo durante el arranque. Ambas proporcionan la misma interfaz.

Si alguna comprobación de integridad del firmware de un cHSM falla al iniciar o reiniciar uno de los cHSM, el cHSM que falle será puesto en un "Estado de Error seguro". En este estado de error solo están disponibles los comandos de solicitud de estado, y no se proporciona ningún servicio criptográfico a ningún usuario de ese cHSM. Sin embargo, esto afecta únicamente al cHSM que ha fallado, el resto de cHSM pueden iniciarse correctamente.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

El *u.trust Anchor* registra todos los eventos y acciones relacionados con cuestiones de seguridad que ocurren o se ejecutan mientras está en funcionamiento, en uno o más archivos internos de registro de auditoría. El contenido de estos archivos de auditoría deberá revisarse periódicamente, de acuerdo con la política de seguridad individual del cliente, por uno o más usuarios autorizados.

El producto tiene registro de eventos en diferentes niveles:

- Registro de Auditoría Global de *u.trust Anchor*:

  En este registro de auditoría global se registran eventos globales del dispositivo, como alarmas, errores globales del dispositivo y la ejecución de comandos globales del dispositivo. El *Global Administrator* es responsable de gestionar el registro de auditoría global mediante los comandos *gladm* correspondientes:

```
gladm system-get-audit-log
```

- Registro de Auditoría del cHSM de *u.trust Anchor*:

  En este registro de auditoría del cHSM se registran eventos específicos del cHSM, como la ejecución exitosa o fallida de comandos relevantes para la seguridad. El *cHSM Administrator* es responsable de gestionar el registro de auditoría específico del cHSM mediante los comandos *csadm* correspondientes:

```
csadm GetAuditLog
```

Para ver el formato de los registros log y más información, acuda al capítulo 6.2.2 "*Audit log*" del "utrust AnchorCC cHSM Manual Administrators". 17

El producto es capaz de generar un registro de auditoría de los siguientes eventos auditables:

- Inicio y apagado de las funciones de auditoría.
- Arranque del TOE.
- Generación y destrucción de claves criptográficas
- Fallo del generador de números aleatorios.
- Fallos de autenticación.
- Todos los intentos de importar o exportar claves.
- Todas las modificaciones a los atributos de las claves.
- Copia de seguridad y restauración: uso de cualquier función de copia de seguridad, uso de cualquier función de restauración, restauración fallida debido a detección de modificación de los datos de respaldo.
- Errores de integridad detectados para claves.
- Fallos al establecer canales seguros.
- Finalización de los auto-chequeos.
- Fallos detectados por el *u.trust Anchor*.
- Todas las acciones administrativas.
- Ajuste del reloj interno por parte de un administrador.
- Modificaciones a los parámetros de auditoría (que afecten al contenido del registro de auditoría).

6.9.2 ALMACENAMIENTO LOCAL

El producto almacena los registros localmente en el *Audit Trail*, al cual solo tienen acceso el personal autorizado, cuando el sistema de almacenamiento alcanza su capacidad máxima se implementan medidas de mitigación como el *logrotate,* que aseguran que ningún registro se pierda.

El *audit trail* generado por el dispositivo será recopilado, mantenido y revisado por un auditor del sistema conforme a un procedimiento de auditoría definido para el sistema específico.

6.9.3 ALMACENAMIENTO REMOTO

En caso de usar la versión integrada en *u.trust Anchor* LAN, se tiene la capacidad de hacer el envío de registros a un servidor *syslog*. Para esto, en primer lugar, el servidor syslog debe estar configurado para aceptar inicios de sesión remoto, para ello habrá que iniciar el servicio "*syslogd*" con el parámetro **-r**, usando por defecto el puerto 514 y el protocolo UDP.

La configuración del envío de registros se realiza mediante los siguientes ficheros:

- */etc/csxlan.conf*: La configuración de este fichero viene descrita en el capítulo 6.4.1 "*Configuring the csxlan.conf File*" del "u.trust Anchor LAN V5 CC - Administration Manual" 17.
- */etc/syslog.conf*: La configuración de este fichero viene descrita en el capítulo 6.4.2 "*Configuring the syslog.conf File*" del "u.trust Anchor LAN V5 CC - Administration Manual" 17.

Para que los registros se transmitan correctamente, los valores configurados en *LogFacility* en el fichero *csxlan.conf* deben coincidir con las reglas establecidas en *syslog.conf*.

6.10 BACKUP

Cualquier método proporcionado por el dispositivo para realizar copias de seguridad de los datos de usuario, incluidas las claves secretas, preserva la seguridad de dichos datos y está controlado por administradores autorizados.

Se aplican las siguientes normas para determinar si se permite una operación de copia de seguridad:

- Solo los administradores autorizados podrán realizar cualquier operación de copia de seguridad proporcionada por el dispositivo, ya sea para crear copias de seguridad del estado del dispositivo o para restaurar dicho estado desde una copia de seguridad.
- Garantizar la confidencialidad e integridad de los datos durante la creación, transmisión, almacenamiento y restauración de la copia de seguridad.
- Preservar la confidencialidad e integridad de las claves secretas, así como la integridad de las claves públicas.
- Preservar la integridad de los atributos de las claves y la vinculación de cada conjunto de atributos con su clave correspondiente.

Se recomienda consultar el capítulo 4.7 "*Commands for Managing the Master Backup Keys*" del u.trust AnchorCC cHSM Manual Administrators 17.

7 REFERENCIAS

[REF1] Módulo de seguridad hardware (HSM) (CCN-STIC-140-E5). https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/7420-stic-140-l2-modulo-de-seguridad-hardware-hsm/file?format=html

[REF2] u.trust Anchor LAN V5 CC - Operating Manual

[REF3] u.trust Anchor LAN V5 CC - Quick Start Guide

[REF4] u.trust Anchor CC - Administration Manual

[REF5] u.trust Anchor CC – csadm Manual

[REF6] u.trust Anchor LAN V5 CC – Administration Manual

[REF7] u.trust Anchor CC – Containerized Hardware Security Module (cHSM)- Administration Manual

[REF8] Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN. https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

[REF9] Página web oficial de Utimaco. https://utimaco.com/

[REF10] Declaración de seguridad de Common Criteria. https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-2400107-01-ST-Lite_v1-0-4.pdf

8 ABREVIATURAS

AES	Advanced Encryption Standard.
ANSI	American National Standards Institute.
API	Application Programming Interface.
CA	Certificado de Autoridad.
CBC	Cipher-Block-Chaining.
cHSM	Containerized HSM.
CMAC	Cipher-based Message Authentication Code.
CTR	Counter (Mode).
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman.
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad.
FIPS	Federal Information Processing Standard.
GAAK	Global Admin Authentication Key.
GCM	Galois/Counter Mode.
GIAK	Global Initial Administrator Key.
GMAC	Galois Message Authentication Code.
HMAC	Hash-based Message Authentication Code.
HSM	Hardware Security Module.
HSMaaS	HSM as a Service.
LAN	Local Area Network.
MAC	Message Authentication Code.
PCI	Peripheral Component Interconnect.
PIN	Personal Identification Number.
PKCS	Public-Key Cryptography Standards.
PTRNG	Physical True Random Number Generator.
RFC	Request for Comments.
RSA	Rivest-Shamir-Adleman.
SHA	Secure Hash Algorithm.
SSH	Secure Shell.