centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1513

Procedimiento de Empleo Seguro
CryptoServer CP5

Octubre 2025

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-131-X

Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 10:41:15 +02'00'

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

ÍNDICE

1 INTRODUCCIÓN

1. CryptoServer CP5 es un módulo de seguridad de hardware que proporciona servicios criptográficos seguros como HSM de propósito general.
2. CryptoServer Se-Series Gen2 CP5 es un módulo criptográfico que se utiliza para implementar servicios de firma/sellado local y de servidor de firma.
3. Como parte de un Sistema de Sellado de Tiempo, el CryptoServer CP5 puede utilizarse como módulo criptográfico que crea las firmas digitales de los tokens de sellado de tiempo.

2 OBJETIVO Y ALCANCE

4. El presente documento tiene por objeto facilitar la instalación y configuración seguras del CryptoServer CP5, así como proteger el entorno en el que se implanta. El CryptoServer CP5 puede suministrarse en los siguientes modelos (versiones) de CryptoServer CP5:

    - CryptoServer CP5 Se12 5.1.0.0 o abreviado Se12 es un CryptoServer CP5 sin chip criptoacelerador.
    - CryptoServer CP5 Se52 5.1.0.0 o abreviado Se52 es un CryptoServer CP5 sin chip criptoacelerador.
    - CryptoServer CP5 Se500 5.1.0.0 o abreviado Se500 es un CryptoServer CP5 con un chip criptoacelerador.
    - CryptoServer CP5 Se1500 5.1.0.0 o abreviado Se1500 es un CryptoServer CP5 con un chip criptoacelerador.

5. Todos los modelos CryptoServer CP5 están disponibles en dos variantes de entrega.

    - PCIe Plug-in Card con bus PCIe para su integración en un ordenador.
    - CryptoServer CP5 LAN V5 Network Appliance, que es un dispositivo de red de 19 pulgadas con una tarjeta CryptoServer CP5 PCIe montada en su interior. Puede integrarse fácilmente en una red y ofrece múltiples opciones de administración y supervisión remotas.

6. El producto CryptoServer CP5 ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en la familia “Hardware Security Module (HSM)”.

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

7. El producto se entrega en un paquete con el CryptoServer CP5 sellado y completamente instalado. Además del paquete y por separado, la hoja de información de entrega en formato PDF y el archivo CSXXXXXX.key, que contiene la parte pública de la *HSM Authentication Key* del dispositivo y la guía para la verificación de la entrega se adjuntan a un correo electrónico firmado por Utimaco IS GmbH. El cliente debe comprobar la integridad y la autenticidad del paquete recibido utilizando la hoja de información de entrega, así como todos los demás datos del correo electrónico firmado.
8. El producto se suministra en una de las dos siguientes variantes de entrega. Como tarjeta PCIe o como servidor LAN. Las instrucciones paso a paso sobre cómo se verifica el producto en el lado del cliente para cada variante de entrega se describen en la documentación de orientación operativa (manuales de funcionamiento y administración), que se entrega al cliente en un CD como parte del paquete de entrega.
9. La completitud e integridad del contenido del paquete debe determinarse como se describe en el Manual Operativo proporcionado [REF2] o [REF3], Capítulo 3 *"Checking the Wrapping, Seals and the Completeness of Deliverables".*
10. Para verificar el estado interno del CryptoServer CP5, se instalará la herramienta de línea de comandos ***csadm*** en un ordenador (denominado ordenador de administración). En primer lugar, permite leer el número de serie y el estado interno del CryptoServer CP5, tal como se explica detalladamente en el correspondiente Operating Manual [REF2][REF3], capítulo "*Installing the Host Software for the CryptoServer CP5*". Además, mediante ***csadm*** es posible verificar el firmware instalado en el módulo de seguridad, tal como se describe en el Manual de Administración de CryptoServer CP5 [REF1], Capítulo 8.1 "*Identifying Your CryptoServer CP5".*
11. La integridad y autenticidad de los componentes del CryptoServer pueden comprobarse e identificarse mediante las medidas descritas en la tabla siguiente.

PASO	COMPONENTE	MEDIDA
1	Un CD-R CryptoServer CP5	Comprobar que el contenido de la etiqueta del CD es el especificado en la información de entrega. El checksum del SHA-256 del contenido (archivo CryptoServerCP5InternalSAM-V<versionnumber>.zip) debe ser el especificado en la información de entrega. Para más instrucciones al respecto, se recomienda consultar el capítulo "*Checking the Wrapping, Seals and Completeness of Deliverables*", paso 6 ó 10 respectivamente, del *Operating Manual* [REF2][REF3] correspondiente entregado
2	Un CryptoServer CP5 completamente instalado que contiene los siguientes componentes:	
	■ Tarjeta PCIe	Comprobar que el número de serie de la tarjeta PCIe que está impreso en una etiqueta en el soporte de la ranura de la tarjeta

		PCIe es el que figura en la hoja de información de entrega. Se recomienda consultar las instrucciones detalladas al respecto en el capítulo 3, *"Checking the Wrapping, Seals and Completeness of Deliverables"*, del Operating Manual [REF2][REF3] correspondiente que se entrega en el CD del producto. El archivo **README.txt** proporciona ayuda sobre por dónde empezar. También es posible comprobar el número de serie con el comando **csadm GetState**. Allí aparece como la última entrada en formato **CSXXXXXX** en el campo **adm1**, y debe ser idéntico al número de serie que aparece en la información de entrega. Para la verificación criptográfica de la autenticidad del HSM, se recomienda consultar el capítulo 4.2 de este documento. Para más información, se recomienda consultar las instrucciones detalladas en el capítulo 7.4, "Checking the Authenticity of the CryptoServer CP5" o en el capítulo 6.9, "*Checking the Authenticity of the CryptoServer CP5 LAN*" del *Operating Manual* [REF2][REF3] correspondiente.
	▪ Bootloader y versión de hardware	Comprobar el estado interno del módulo de seguridad, la versión de hardware y el número de versión del gestor de arranque mediante el comando **csadm GetState**. Para más información, se recomienda consultar las instrucciones al respecto en [REF1], capítulo 8.1 "*Identifying Your CryptoServer CP5*", paso 2.
	▪ Lógica de control (FPGA) y controlador sensorial.	Comprobar los números de versión de la lógica de control (FPGA) y del controlador sensorial utilizando el comando **csadm GetBootLog**. Para más información al respecto, se recomienda consultar las instrucciones al respecto en **¡Error! No se encuentra el origen de la referencia.**, capítulo 8.1 "*Identifying Your CryptoServer CP5*", paso 3.
	▪ Paquete de firmware CryptoServer CP5	Comprobar el número de versión y el estado de inicialización de todos los módulos de firmware incluidos en el paquete de firmware CryptoServer CP5 y cargados en la tarjeta plug-in CryptoServer CP5 PCIe mediante el comando **csadm ListFirmware**. Para más información al respecto, se recomienda consultar las instrucciones al respecto en [REF1], capítulo 8.1 "*Identifying Your CryptoServer CP5*", paso 4. Los números de versión de los módulos de firmware serán los que figuran en [REF1], Apéndice A, "*List of Certified Firmware Versions*".

3	Si el producto se ha entregado como CryptoServer CP5 LAN V5	El número de serie del CryptoServer CP5 LAN V5 que figura en la carcasa exterior del aparato LAN debe coincidir con el indicado en la hoja de información de entrega.

Tabla 1. Medidas de comprobación de autenticidad e integridad

12. Si alguna de estas medidas no se cumple, no se continuará con el procedimiento de instalación y se contactará con el fabricante Utimaco IS GmbH.

13. Además, los siguientes entregables también son necesarios para el funcionamiento del producto, por lo que también debe comprobarse que estén completos:

    - Si se ha suministrado un CryptoServer CP5 LAN V5, debe disponerse de dos cables de alimentación.
    - Un Utimaco cyberJack: un PIN pad con soporte, un cable micro USB y un cable alargador USB según se indica en el Manual de instrucciones correspondiente ([REF2] o [REF3], capítulo 1.5, "Deliverables"). Los números del precinto de seguridad y el número de serie del PIN pad serán los mismos que figuran en la hoja de Información de entrega.
    - Diez tarjetas de administración con la clave de administrador predeterminada ADMIN.key almacenada en ellas. Los números de serie de las tarjetas inteligentes serán los que figuran en la hoja de información de entrega.

4.2 ENTORNO DE INSTALACIÓN SEGURO

14. CryptoServer CP5 sólo debe instalarse, utilizarse y almacenarse en un entorno protegido que limite el acceso físico al dispositivo a los administradores autorizados. El entorno protegido puede ser un Centro de Proceso de Datos o un lugar restringido que cumpla los requisitos ambientales y de seguridad que se resumen a continuación.

15. Los requisitos de temperatura y humedad son los siguientes:

TEMPERATURA AMBIENTE	Funcionamiento Tarjeta PCIe: +10 °C a +45 °C Funcionamiento Dispositivo LAN: +10 °C a +50 °C Almacenamiento: de -10 °C a +55 °C
HUMEDAD	10 % a 95% de humedad relativa, sin condensación

Tabla 2. Requisitos de humedad y temperatura

16. En caso de formato *appliance*, es necesario un cable de red RJ45 para conectar el CryptoServer CP5 LAN en la red.

17. Además, el entorno operativo de CryptoServer CP5 (o CP5 LAN) debe cumplir los siguientes requisitos de seguridad:

    - El PIN pad es guardado de forma segura y sus precintos no están dañados.
    - Las tarjetas inteligentes se han guardado de forma segura.
    - El PIN pad no puede ser supervisado durante la introducción del PIN.
    - No se pueden supervisar las entradas de contraseña.
    - El ordenador de administración es de confianza y sólo se instala y ejecuta en él software de confianza.

- Sólo las personas de confianza tienen acceso físico y de red al CryptoServer CP5 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.
- El ordenador de administración en el que se instale la tarjeta CryptoServer CP5 PCIe deberá estar situado en una zona de alta seguridad a la que sólo puedan acceder personas autorizadas. Las personas no autorizadas no podrán acceder al ordenador de administración. Deberá estar protegido por un mecanismo de control de acceso, por ejemplo, contraseña y/o tarjeta inteligente.

18. Las siguientes normas se aplican a las contraseñas:
    - 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.
    - 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.
19. Si se utiliza un ordenador de administración con sistema operativo Windows y ya se ha instalado en él el controlador USB REINER SCT "Base Components", habrá que desinstalar este controlador mediante el Administrador de dispositivos de Windows.
20. Si el CryptoServer CP5 LAN se utiliza en un clúster, debe garantizarse que todos los dispositivos CryptoServer CP5 LAN pertenecientes al mismo clúster estén siempre sincronizados, por ejemplo, que las mismas claves se almacenen en los dispositivos en el mismo estado actualizado.

4.3 REGISTRO Y LICENCIAS

21. CryptoServer CP5 utiliza archivos de licencia firmados (con formato .slf) para controlar el rendimiento de los algoritmos criptográficos RSA y ECDSA y el número de transacciones por segundo sin afectar a la seguridad de dichos algoritmos ni a la seguridad general del HSM.
22. Estos archivos son generados por Utimaco, y son introducidos en el dispositivo antes de su entrega. Durante este proceso, dicha firma es analizada y verificada. Para más información, se recomienda consultar el capítulo "Signed License Files" en [REF1].

4.4 CONSIDERACIONES PREVIAS

23. Se recomienda comprobar el capítulo 3 del manual de instrucciones correspondiente [REF2] o [REF3] en relación con la integridad del producto suministrado antes de la instalación.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

24. En el entorno operativo del producto debe de haber un ordenador de administración con uno de los Sistemas Operativos enumerados en la tabla siguiente.

MICROSOFT WINDOWS (32-BIT AND 64-BIT)	LINUX (32-BIT AND 64-BIT)
Windows Server 2019	Red Hat Enterprise Linux (RHEL) 9.X
Windows Server 2022	

Tabla 3. Sistemas Operativos admitidos para el ordenador de administración

4.5.1 ENTORNO OPERATIVO PARA TARJETA PCIE

25. Para utilizar la tarjeta CryptoServer CP5 PCIe, debe montarse en el ordenador de administración con una ranura PCIe libre y al menos los siguientes componentes del sistema:
    - CPU: Intel x86/x64, AMD x86/x86-64
    - Capacidad del disco duro: al menos 120 Mbytes.
    - RAM: más de 12 Mbytes.
26. El controlador CryptoServer y el software host suministrados en el CD del producto deben instalarse en el ordenador de administración tal y como se describe en los capítulos siguientes.
27. Utimaco no proporciona ningún software que permita el acceso remoto al CryptoServer CP5 con la variante de entrega de la tarjeta CryptoServer CP5 PCIe. Por lo tanto, la tarjeta CryptoServer CP5 PCIe montada sólo puede comunicarse con las herramientas de administración y el software de comunicación suministrados por Utimaco IS GmbH, así como con las aplicaciones instaladas en el ordenador de administración.
28. Sin embargo, el cliente puede utilizar software propio o de terceros, por ejemplo, un *daemon* de comunicación TCP/IP, para acceder remotamente a la tarjeta CryptoServer CP5 PCIe a través de una red. En este caso, se necesitan dos ordenadores: Un ordenador host con una ranura PCIe libre para la tarjeta CryptoServer CP5 PCIe, y un ordenador de administración en el que estén instalados el software de administración y otras aplicaciones que utilicen remotamente la tarjeta CryptoServer CP5 PCIe.
29. El controlador CryptoServer proporcionado por Utimaco en el CD del producto suministrado, y el software de terceros que permite la comunicación remota con el CryptoServer CP5 deben instalarse en el ordenador de administración en el que esté montada la tarjeta CryptoServer CP5 PCIe.
30. Todas las instrucciones contenidas en el presente documento contemplan únicamente el primer escenario de despliegue, con un único ordenador en el que se monta la tarjeta CryptoServer CP5 PCIe y se instala el software de host suministrado.

5 FASE DE INSTALACIÓN

31. En el capítulo 7 "Bringing into Service" del Operating Manual [REF3] se encontrarán las instrucciones para la instalación y puesta en servicio de la tarjeta CryptoServer CP5 PCIe.
32. Para las instrucciones de puesta en servicio de la tarjeta CryptoServer CP5 LAN suministrada, se recomienda consultar el capítulo 6 "Bringing into Service" del Operating Manual [REF2].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

33. No es necesaria una activación de la configuración para utilizar el producto en el modo seguro, ya que este es el único modo de funcionamiento del producto.

34. CryptoServer CP5 se maneja desde el ordenador central mediante una herramienta de línea de comandos denominada ***csadm***. Ha sido diseñada para ser llamada desde una línea de comandos o en un archivo por lotes. Ofrece funciones para administrar CryptoServer CP5 y gestionar las claves de autenticación de usuario.

35. Además, ***csadm*** proporciona todo tipo de funciones de administración general, como la visualización de la información de estado, la configuración del reloj del módulo de seguridad, la gestión de usuarios, etc.

6.2 AUTENTICACIÓN

36. Al registrarse, cada usuario debe elegir un mecanismo de autenticación específico. El equipo ofrece dos mecanismos diferentes de autenticación de usuarios:

    - Uno es el mecanismo de autenticación de firma RSA, que se realiza con una firma RSA generada utilizando el esquema RSASSA-PKCS1-v1_5 según el estándar [PKCS#1], capítulo 8.2.1, con longitudes de clave de un mínimo de 2048 y un máximo de 8192 bits. Se recomienda emplear claves RSA con longitud superior a 3072 bits.
    - El segundo mecanismo de autenticación es el de contraseña HMAC.

37. Además, para el módulo de activación de firma interna (SAM) se utiliza el mecanismo de autenticación de firma. La autenticación se realiza con la ayuda de una firma RSA que debe calcularse sobre el módulo de firmware con la Clave de Firma de Módulo CryptoServer CP5 dedicada, propiedad del fabricante.

38. Para el intercambio de datos sensibles, se establece una sesión de Mensajería Segura, utilizando el acuerdo de Clave Diffie-Hellman, entre el producto y la aplicación host. Esta sesión de mensajería segura es obligatoria para cada comando que requiera la autenticación del usuario.

39. Para más información al respecto, se recomienda consultar el apartado 3.8.2 Authentication Mechanisms del documento [REF1].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

40. El CryptoServer CP5 puede administrarse desde una aplicación host en el ordenador de administración. La tarjeta CryptoServer CP5 PCIe soporta un canal seguro (Secure Messaging) para la comunicación entre esta tarjeta PCIe y la aplicación host.

41. Esta aplicación host no se ejecuta necesariamente en el ordenador en el que se ha montado la tarjeta CryptoServer PCIe.

42. La sesión de mensajería segura se establece utilizando Diffie-Hellman con autenticación mutua y mecanismo AES-CMAC. El CryptoServer CP5 impone el uso de la mensajería segura

para todos los comandos relevantes para la seguridad que transporten datos hacia o desde el CryptoServer CP5.

43. CryptoServer CP5 puede administrarse de las siguientes maneras.

6.3.1.1 HERRAMIENTA DE ADMINISTRACIÓN CLI (*CSADM*)

44. La herramienta de línea de comandos CryptoServer csadm es un programa que puede invocarse desde una línea de comandos o desde un archivo batch desde el ordenador de administración. Con ***csadm*** se pueden administrar tanto las tarjetas CryptoServer CP5 PCIe como CryptoServer CP5 LAN. Con ***csadm*** se pueden llevar a cabo todas las tareas de administración relacionadas con la puesta en funcionamiento del CryptoServer CP5, la supervisión de su estado y la gestión de los usuarios, el firmware, las claves de autenticación de usuario y las claves de sistema utilizadas para la protección de datos.

6.3.1.2 MENÚ DEL CRYPTOSERVER CP5 LAN

45. Si el CryptoServer CP5 está integrado en un CryptoServer CP5 LAN, en la parte frontal del CryptoServer CP5 LAN hay un display y varias teclas de control. A través de este display y de las llaves de control 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, así como a una gama limitada de funciones para la gestión del firmware y de las llaves. Sin embargo, estas opciones de menú no pueden utilizarse para gestionar los datos del usuario.

46. Las opciones de menú de la parte frontal del CryptoServer CP5 LAN permiten administrar tanto el CryptoServer CP5 LAN como la tarjeta CryptoServer CP5 PCIe montada dentro del CryptoServer CP5 LAN.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

47. En todos los CryptoServer CP5 se suministra un usuario por defecto, ADMIN. El usuario ADMIN dispone de permisos para las funciones **Administrador de usuarios** y **Administrador** (22000000). En cada una de las diez tarjetas inteligentes suministradas se almacena inicialmente una clave de autenticación RSA de 2048 bits, ADMIN.key, protegida por el PIN inicial 123456, que también se encuentra en el CD del producto, en el directorio \Software\<Windows|Linux>\<x86-32|x86-64>\Administration\key. Esta clave por defecto puede ser utilizada inicialmente por el usuario ADMIN, y no está protegida por contraseña.

48. Dado que la clave ADMIN.key no es específica del cliente, el cliente deberá cambiarla lo antes posible o sustituir al usuario ADMIN por otros usuarios específicos del cliente con derechos de administración.

49. Si el ADMIN es sustituido por dos o más usuarios, la suma de los permisos de los nuevos usuarios creados utilizando una clave RSA como token de autenticación debe ser como mínimo 21000000. Sólo si se ha alcanzado este permiso, el CryptoServer CP5 permite la supresión del usuario ADMIN por defecto. De este modo, se garantiza que el CryptoServer CP5 siga siendo administrable siempre que se haya producido una alarma en el CryptoServer CP5 o se haya ejecutado el comando "***csadm Clear***". En caso de alarma o de ejecución del comando "**csadm Clear**", todos los usuarios que utilicen la autenticación por contraseña se borrarán de la base de datos de usuarios del CryptoServer CP5. Por lo tanto,

los usuarios restantes deberán poder configurar de nuevo el CryptoServer CP5. En particular, deben quedar suficientes usuarios capaces de autenticar los comandos para restablecer la alarma y crear nuevos usuarios. Pueden crearse usuarios adicionales con permisos de administrador y autentificación de contraseña, pero serán eliminados en caso de alarma.

50. Para más detalles sobre los usuarios y los roles, consulte el capítulo "User Roles and Accessible Functions" del administration manual [REF1].

51. El número establecido de intentos fallidos de autenticación es 5, tras lo que el usuario es bloqueado de futuros intentos de autenticación. Tras alcanzar este límite, el usuario solo podrá ser desbloqueado por el User Administrator.

52. Para más información acerca del número máximo de intentos fallidos de autenticación, consultar el apartado 3.8.4 Maximum of Failed Authentication Attempts del documento [REF1]. Asimismo, también se recomienda consultar el apartado 7.5.2 GetMaxAuthFails [REF1].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

53. En el caso de una variante de entrega de dispositivo LAN, es necesario asignar una dirección IP al CryptoServer CP5 LAN para garantizar que se pueda acceder a él a través de la red. La dirección IP del CryptoServer CP5 LAN puede ser estática o configurarse automáticamente mediante DHCP. Por defecto, la interfaz **eth0** está configurada para utilizar una dirección IP dinámica (DHCP), y la dirección IP estática 10.10.10.10 está asignada a la interfaz **eth1**.

54. La siguiente información se puede encontrar en el Manual de funcionamiento [REF2].

55. Las instrucciones para configurar una dirección IPv4 estática para la LAN CryptoServer CP5 se encuentran en el capítulo "Entering a Static IPv4 Address for the CryptoServer CP5 LAN", del documento CryptoServer Se-Series Gen2 CP5 LAN V5 Operating Manual [REF2].

56. Las instrucciones para configurar una dirección IPv4 estática para la pasarela de red por defecto se encuentran en el capítulo "Entering a Static IPv4 Address for the Default Gateway", del documento CryptoServer Se-Series Gen2 CP5 LAN V5 Operating Manual [REF2].

57. Las instrucciones para configurar la dirección IPv4 para la LAN CryptoServer CP5 y la pasarela de red por defecto mediante un servidor DHCP se encuentran en el capítulo "Setting up Dynamic IPv4 Addresses with DHCP", del documento CryptoServer Se-Series Gen2 CP5 LAN V5 Operating Manual [REF2].

58. Para más información sobre la configuración de las interfaces de red, se recomienda consultar los apartados "Disabling the SSH Daemon (optional)" y "Restricting the Network Access", del documento CryptoServer Se-Series Gen2 CP5 LAN V5 Operating Manual [REF2].

6.5 GESTIÓN DE CERTIFICADOS

59. La tarjeta CryptoServer CP5 PCIe soporta un canal seguro (Secure Messaging) para la comunicación entre esta tarjeta PCIe y la aplicación host. Esta aplicación host no se ejecuta necesariamente en el ordenador en el que se ha montado la tarjeta CryptoServer PCIe. CryptoServer CP5 está configurado para autenticarse ante las aplicaciones host al inicio de una sesión de mensajería segura. Para ello, se utiliza un par de claves RSA de 3072 bits

específico del dispositivo denominado HSM Authentication Key, abreviado HSMAuthKey, para verificar la autenticidad de una sesión de mensajería segura originada en el HSM. Los comandos enviados por la aplicación host al CryptoServer CP5 y las respuestas del CryptoServer CP5 a la aplicación host se cifran y la integridad de los datos se protege mediante un MAC (Message Authentication Code).

60. Para cada conexión entre el CryptoServer CP5 y la aplicación host se genera una nueva clave de sesión aleatoria. Esto impide que los paquetes de datos grabados pertenecientes a una conexión anterior se importen a una nueva conexión. El identificador de sesión único garantiza que cada clave de sesión sea identificable de forma única. Todos los comandos que utilizan la misma clave de sesión y el mismo ID de sesión forman parte de la misma sesión (conexión).

61. Además, en cada sesión se utiliza un contador de secuencias para evitar la repetición de mensajes anteriores dentro de la sesión. Esto garantiza que no se registren comandos dentro de la misma conexión y se envíen de nuevo al CryptoServer CP5. Una vez que se ha solicitado una clave de sesión y se ha establecido una conexión segura entre el host y el CryptoServer CP5, todos los comandos intercambiados dentro de esta sesión son autentificados, encriptados y protegidos contra la manipulación por una MAC.

62. Para más información, consulte los capítulos "HSM Authentication Key" y "Using and Managing Cryptographic Keys" del manual de instrucciones [REF1].

6.6 SINCRONIZACIÓN

63. La sincronización horaria se establece manualmente mediante la herramienta ***csadm*** en el ordenador central. Para ello se utilizan las funciones *SetTime* y *GetTime* de la interfaz externa del CryptoServer CP5. Se recomienda consultar el capítulo "Commands for Administration" del Manual de Administración [REF1] para obtener información detallada sobre cómo utilizar los comandos relacionados.

6.7 ACTUALIZACIONES

64. El paquete de firmware actualizado se entregará al cliente en forma de un nuevo CD de producto CryptoServer CP5, que también irá acompañado de una nueva hoja de información de entrega. Los pasos a seguir para una actualización de firmware segura se describen en el capítulo "Performing a Firmware Update" del Manual de Administración [REF1].

6.8 AUTO-CHEQUEOS

65. El cargador de arranque realiza varias auto pruebas, incluidas pruebas de integridad del firmware, cada vez que se inicia el CryptoServer CP5 para comprobar si determinados componentes de hardware y software funcionan correctamente. Además, cada vez que se inicia CryptoServer CP5 se ejecuta un módulo de firmware dedicado que implementa todas las auto pruebas para todos los algoritmos criptográficos.

66. La lista de autocomprobaciones es la siguiente:

    - Prueba de integridad del software/firmware en el arranque inicial (o encendido o reinicio)
    - Pruebas de algoritmos criptográficos en el arranque inicial (o encendido o reinicio)

- Pruebas de funciones críticas, incluidas pruebas de memoria y pruebas del generador de números aleatorios, en el arranque inicial (o en el encendido o reinicio).
- Prueba de descarga de firmware (mediante verificación de firma RSA) en la descarga de firmware.
- Prueba en línea del PTRNG según [AIS 20/31] para la clase de RNG PTG.2 en cada solicitud de PTRNG.
- Prueba DRBG condicional según [FIPS 140-2] en cada solicitud DRBG:
  - Prueba de coherencia por pares según [FIPS 140-2] durante la generación del par de claves.

67. Si se detecta un error durante la autocomprobación, se interrumpe el arranque y el CryptoServer CP5 pasa al estado operativo DEFECT. Todo módulo de seguridad que se encuentre en estado DEFECT ya no podrá utilizarse para ninguna operación criptográfica ni función administrativa y deberá devolverse al fabricante Utimaco.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

68. CryptoServer CP5 registra en el archivo o archivos de registro de auditoría todos los eventos y acciones relacionados con cuestiones de seguridad que se produzcan o se ejecuten durante su funcionamiento. Los eventos auditables son los siguientes:

    - Gestión de firmware y archivos, incluidos los comandos para cargar o eliminar un archivo o un módulo de firmware.
    - Acciones de gestión de usuarios, incluidos los comandos para añadir o eliminar un usuario o para modificar el token de autenticación del usuario
    - Ajuste del reloj del sistema del CryptoServer CP5
    - Eventos del sistema como una alarma fallo de autotest o arranque y apagado de CryptoServer CP5
    - Gestión del archivo de registro de auditoría, incluida la eliminación del archivo de registro de auditoría
    - Gestión de la Master Backup Key, incluida la creación o importación de la Master Backup Key
    - Gestión de claves, incluidas las funciones de gestión de claves del módulo de firmware CXI
    - Autenticaciones fallidas
    - Operaciones de copia de seguridad y restauración, incluidas la copia de seguridad y la restauración de claves criptográficas individuales y objetos de configuración

69. Para más información al respecto, se recomienda consultar el apartado 3.11 Auditing, del documento [REF1].

6.9.2 ALMACENAMIENTO LOCAL

70. CryptoServer CP5 puede escribir en un máximo de diez archivos de registro de auditoría (de un tamaño máximo de 200KB cada uno) de forma no rotatoria. Esto significa que, una vez llenos todos los archivos de registro de auditoría existentes, CryptoServer CP5 se niega a realizar cualquier función auditable con un mensaje de error. Por lo tanto, es necesario realizar copias de seguridad periódicas del contenido de los ficheros de registro de

auditoría y borrarlos, o bien archivar y borrar al menos uno de ellos para poder volver a utilizar CryptoServer CP5. Para obtener instrucciones paso a paso, se recomienda consultar el apartado 8.12 "Proceeding When All Audit Files Are Full" del Manual de Administración [REF1].

6.10 BACKUP

71. La copia de seguridad de los datos de auditoría se exporta en texto sin formato. El administrador autorizado es responsable de proteger la integridad de los archivos de respaldo de auditoría y almacenarlos en un entorno seguro. El entorno seguro protegerá los datos de auditoría contra pérdida y manipulación de acuerdo con la política de seguridad de auditoría del cliente. Por ejemplo, los archivos de respaldo de auditoría pueden almacenarse en un contenedor de almacenamiento encriptado en una unidad flash USB confiable en una caja fuerte segura a la que solo pueden acceder personas autorizadas.
72. En relación con los procedimientos de backup de claves, se recomienda consultar el capítulo 3.13.4 "Protección de claves en el almacenamiento, copia de seguridad y exportación de claves" del Manual de Administración [REF1].
73. Asimismo, también se recomienda consultar el apartado 3.4.4 “Master Backup Key (MBK)”, del Manual de Administración [REF1].

7 REFERENCIAS

[REF1] CryptoServer Se-Series Gen2 CP5 – Administration Manual / Utimaco IS GmbH

[REF2] CryptoServer Se-Series Gen2 CP5 LAN V5 -- Operating Manual / Utimaco IS GmbH

[REF3] CryptoServer Se-Series Gen2 CP5 PCIe-- Operating Manual / Utimaco IS GmbH

8 ABREVIATURAS

AES-CMAC	Advanced Encryption Standard - Cipher-based Message Authentication Code
AIS 20/31	Application Notes and Interpretation of the Scheme 20/31 (Norma alemana para generadores de números aleatorios)
CXI	CryptoServer eXtended Interface
Diffie-Hellman	Algoritmo de intercambio de claves criptográficas
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS 140-2	Federal Information Processing Standard 140-2
FPGA	Field Programmable Gate Array
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
JRE	Java Runtime Environment
LAN	Local Area Network
MAC	Message Authentication Code
MBK	Master Backup Key
OpenJDK	Open Java Development Kit
PCIe	Peripheral Component Interconnect Express
PKCS#1	Public-Key Cryptography Standards #1
PTRNG	Physical True Random Number Generator
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SHA-256	Secure Hash Algorithm 256-bit

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL