CCN
centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD EN ENTIDAD DE CERTIFICACIÓN SOBRE WINDOWS SERVER 2016

JUNIO 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

© Centro Criptológico Nacional, 2020
NIPO: 083-20-144-0

Fecha de Edición: junio de 2020
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

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.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

junio de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN-STIC-500) siendo de aplicación para la Administración y de obligado cumplimiento para los Sistemas que manejen información clasificada Nacional.

La serie CCN-STIC-500 se ha diseñado de manera incremental. Así que, dependiendo del sistema, se aplicarán consecutivamente varias de estas guías. Por ejemplo, para un servidor de Entidad de Certificación de empresa de Windows Server 2016, las guías que deberán aplicarse son:

a) CCN-STIC-570A Windows Server 2016 - Inst completa, DC o miembro.

b) CCN-STIC-574 Implementación de IIS 10 sobre Windows Server 2016 en servidor miembro del dominio.

c) La presente guía.

Nota: Estas guías están pensadas y diseñadas para entornos de máxima seguridad donde no existirá ningún tipo de conexión con redes consideradas no seguras como puede ser Internet.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para la implementación, establecer la configuración y realizar tareas de administración maximizando las condiciones de seguridad del servidor que actúe como Entidad de Certificación de Microsoft Windows Server 2016 en un servidor miembro de una infraestructura de dominio.

La instalación, así como los procesos de administración, se ha diseñado para que la implementación sea lo más restrictiva posible. Es posible que determinadas funcionalidades del servidor de Entidad de Certificación requieran modificar algunas de las configuraciones que se plantean a través de la presente guía.

Esta guía asume que el servidor de Entidad de Certificación se va a implementar sobre un equipo con Windows Server 2016 de 64 Bits en el cuál se ha seguido el proceso de implementación definido en las guías CCN-STIC-570A y CCN-STIC-574.

Cumpliendo con estos requisitos previos, se puede iniciar la instalación del servidor de Entidad de Certificación basado en Microsoft Windows Server 2016.

Así mismo y por motivos de seguridad y reducción de la superficie de ataque, no se contempla en esta guía la instalación del servicio Web de inscripción de certificados, servicio respondedor en línea u otros servicios que no sean estrictamente necesarios para el adecuado funcionamiento del servicio de la Entidad de Certificación en un entorno privado.

Sin embargo y debido a la necesidad de verificar la revocación de certificados, por parte de los equipos cliente y aplicaciones, será necesario instalar el servicio “Internet Information Services (IIS)” para publicar la lista de revocación de certificados de la Entidad de Certificación. Es por ello que antes de iniciar las tareas de instalación de la presente guía, es necesario aplicar la guía de seguridad “CCN-STIC-574 Implementación de IIS 10 sobre Windows Server 2016 en servidor miembro de dominio”.

4. ALCANCE

La guía ha sido elaborada con el propósito de proporcionar información específica para realizar una implementación del servidor de Entidad de Certificación de Microsoft Windows Server 2016 en una configuración restrictiva de seguridad. Se incluyen, además, operaciones básicas de administración como la gestión de extensiones, creación de plantillas de certificados, gestión de la seguridad de la Entidad de Certificación y control de auditoría, además de aquellas acciones que deben ser llevadas a cabo para el adecuado mantenimiento del servicio.

Esta guía de seguridad contempla dos escenarios de implementación: un primer escenario con una única Entidad de Certificación raíz de tipo “Empresa” instalada en un servidor miembro de un dominio de Directorio Activo y un segundo escenario con una Entidad de Certificación raíz de tipo “Independiente” instalada en un servidor independiente y una Entidad de Certificación subordinada de la primera, de tipo “Empresa” e instalada en un servidor miembro de un dominio de Directorio Activo.

El escenario de una única Entidad de Certificación raíz de empresa tiene las siguientes características técnicas:

a) Un único bosque de Directorio Activo.

b) Un único dominio dentro del bosque de Directorio Activo.

c) Nivel funcional del bosque y del dominio en Windows Server 2016 Standard.

d) Un controlador de dominio basado en Windows Server 2016 Standard.

e) Un servidor miembro del dominio basado en Windows Server 2016 Standard.

f) La instalación del servicio de Entidad de Certificación se realiza en modo limpio, es decir, no se contemplan procedimientos de migración desde versiones anteriores.

g) No se contemplan mecanismos de alta disponibilidad ni balanceo de carga en el escenario planteado.

El escenario de dos entidades de certificación, una entidad raíz y otra subordinada tiene las siguientes características técnicas:

a) Un único bosque de Directorio Activo.

b) Un único dominio dentro del bosque de Directorio Activo.

c) Nivel funcional del bosque y del dominio en Windows Server 2016.

d) Un controlador de dominio basado en Windows Server 2016.

e) Un servidor miembro del dominio basado en Windows Server 2016.

f) Un servidor independiente del dominio basado en Windows Server 2016.

g) La instalación del servicio de Entidad de Certificación se realiza en modo limpio, es decir, no se contemplan procedimientos de migración desde versiones anteriores.

h) No se contemplan mecanismos de alta disponibilidad ni balanceo de carga en el escenario planteado.

Este documento incluye:

a) **Mecanismos para la aplicación de configuraciones.** Se incorporan mecanismos para la implementación, de forma automática, de las configuraciones de seguridad susceptibles de ello.

b) **Mecanismos para la creación de cuentas necesarias para la funcionalidad de la solución.** Tanto los procesos de implementación como de instalación requieren de cuentas específicas; se ha automatizado el proceso de creación de dichas cuentas.

c) **Descripción de la seguridad en el servicio de Entidad de Certificación.** Completa la descripción de los mecanismos de seguridad, autenticación y autorización utilizados en el servicio de Entidad de Certificación de Windows Server 2016, así como las medidas para reforzar dicha seguridad.

d) **Guía paso a paso.** Va a permitir implantar y establecer las configuraciones de seguridad de un servidor de Entidad de Certificación de Windows Server 2016.

e) **Guía de administración.** Va a permitir realizar tareas de administración en el entorno de seguridad establecido.

f) **Lista de comprobación.** Permitirá verificar el grado de cumplimiento de un servidor con respecto a las condiciones de seguridad que se establecen en esta guía.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad es conveniente explicar el proceso de refuerzo de la seguridad que describe y los recursos que proporciona. Este procedimiento constará, a grandes rasgos, de los siguientes pasos:

a) Antes de comenzar a aplicar la guía, además de los requisitos para la instalación del servicio de Entidad de Certificación, será necesario cumplir los requisitos definidos para Windows Server 2016.

b) Así mismo, antes de instalar el rol de servicios de certificados de Directorio Activo, será necesario aplicar la guía de seguridad codificada como CCN-STIC-570A.

c) A continuación, se deberá instalar y configurar el rol de servidor web (IIS) y aplicar la guía de seguridad codificada como CCN-STIC-574.

d) Por último, se deberá instalar y configurar el rol de servicios de certificados de Directorio Activo tal y como se describe en la presente guía.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación a equipos tipo puesto servidor con Sistema Operativo Windows Server 2016, en castellano, con el objetivo de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la CCN-STIC-301. En el caso de llevar a cabo la aplicación de esta guía sobre el Sistema Operativo con una configuración de idioma diferente al castellano, es posible que deba incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

La guía ha sido probada y verificada con la versión de Windows Server 2016 Standard, con los parámetros por defecto de instalación y aplicando la guía “CCN-STIC-570A” para su configuración. No se ha verificado en otros tipos de instalaciones como pudiera ser Windows Server 2016 Datacenter. No obstante, y teniendo en consideración las funcionalidades de ambas versiones de sistema operativo servidor, podría llegar a implementarse la siguiente guía sobre la versión Datacenter. La presente guía no será funcional con la versión Windows Server 2016 Essentials.

Esta guía se ha diseñado para reducir la superficie de exposición de los equipos servidores que cuenten con una implementación de rol Entidad de Certificación en un entorno de dominio de Active Directory.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V de Windows Server 2016 con las siguientes características técnicas:

a) Servidor Dell PowerEdgeTM T320:
   i. Intel Pentium Xeon Quad Core.
   ii. HDD 80 GB.
   iii. 32 GB de RAM.
   iv. Interfaz de Red 1 GB.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de Windows Server 2016. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 bits (x64), con más de 2048 MB de memoria RAM.

Así mismo hay que tener en cuenta que el rol de Entidad de Certificación requiere, para un entorno de producción, un mínimo de requerimientos (2 GB de RAM y 32 GB de espacio de almacenamiento en disco). Oficialmente no se indica ningún requerimiento adicional.

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima en caso de redes clasificadas y la seguridad mínima siguiendo las normas descritas en el ENS. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y por lo tanto pueda ser necesario aplicar acciones adicionales para habilitar servicios o características deseadas en Microsoft Windows Server 2016.

Para garantizar la seguridad de los servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Windows Update. Las actualizaciones por lo general se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que en ocasiones se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse de haber probado en un entorno aislado y controlado donde se han aplicado los test y cambios en la configuración, que se ajustan a los criterios específicos de cada organización.

El espíritu de estas guías no está dirigido a reemplazar políticas consolidadas y probadas de las organizaciones sino a servir como la línea base de seguridad, que deberá ser adaptada a las necesidades propias de cada organización.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del rol de Entidad de Certificación sobre Microsoft Windows Server 2016 dependiendo del entorno sobre el que vaya a ser aplicado:

La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

a) Anexo A: En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter con rol de Entidad de Certificación a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) Anexo B: En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter a las necesidades requeridas en los entornos clasificados donde se quiera instalar el rol de Entidad de Certificación.

Cabe remarcar que en sus respectivos anexos se dotará de la información necesaria y concreta para cada tipo de implementación.

De manera adicional, en cada una de las carpetas “Scripts” que se adjuntan a los documentos, existe un directorio que almacena un informe en formato HTML con cada objeto de directiva de grupo (GPO) o directiva de grupo local (GPL) que se aplica.

6. INTRODUCCIÓN A LOS SERVICIOS DE CIFRADO

Como ya es sabido, las redes públicas no proporcionan mecanismos de seguridad para la transmisión de datos entre sistemas y usuarios. El diseño original de Internet, y por consiguiente de la pila de protocolos TCP/IP, no contemplaba la seguridad en el intercambio de datos.

Es por ello que este tipo de comunicaciones es susceptible de ser interceptada y modificada por terceras personas o sistemas, sin previa autorización.

La criptografía ayuda a proteger los datos que se transmiten en redes públicas y privadas, así como aquellos que están almacenados en bases de datos o sistemas de información.

Los principales objetivos de la criptografía son los siguientes:

a) Confidencialidad. Ayuda a proteger la identidad de un usuario o sistema y evita que se lea la información transmitida.

b) Integridad. Garantiza que la información transmitida no ha sido alterada en el transcurso de la comunicación.

c) Autenticación. Identifica de forma única la identidad del remitente o receptor de la información, para garantizar a la otra parte que es quien dice ser.

d) No repudio o sin rechazo. Evita que una parte involucrada en la comunicación niegue el envío de un mensaje.

Para alcanzar estos objetivos, se puede usar una combinación de algoritmos y prácticas conocidas como primitivas criptográficas para crear un esquema de cifrado.

a) Cifrado de clave secreta (cifrado simétrico). Realiza la transformación de los datos para impedir que puedan ser leídos por terceros. Este tipo de cifrado utiliza una clave secreta compartida para cifrar y descifrar los datos. Los algoritmos de cifrado de clave secreta son muy rápidos (comparados con los de clave pública) y resultan adecuados para realizar transformaciones criptográficas en grandes flujos de datos.

b) Cifrado de clave pública (cifrado asimétrico). Realiza la transformación de los datos para impedir que puedan ser leídos por terceros. Este tipo de cifrado utiliza un par de claves pública y privada para cifrar y descifrar los datos. La clave pública y la clave privada están vinculadas matemáticamente; los datos cifrados con la clave pública solo pueden descifrarse con la clave privada y los datos firmados con la clave privada solo pueden comprobarse con la clave pública.

c) Firmas digitales. Ayudan a comprobar que los datos se originan en una parte específica mediante la creación de una firma digital única para esa parte. En este proceso también se usan funciones hash.

d) Valores hash de cifrado. Los algoritmos hash asignan valores binarios de longitud arbitraria a valores binarios más pequeños de longitud fija, que se denominan valores hash. Un valor hash es una representación numérica de un segmento de datos. Los valores hash son únicos estadísticamente; el valor hash de una secuencia de dos bytes distinta no será el mismo.

6.1 PROVEEDORES DE SERVICIOS DE CIFRADO (CSP)

Un proveedor de servicios de cifrado (CSP) es un programa que ofrece servicios de autenticación, codificación y cifrado para que las aplicaciones basadas en Windows obtengan acceso mediante la interfaz de programación de aplicaciones criptográficas de Microsoft (CryptoAPI).

Cada proveedor contiene la implementación de los algoritmos y funciones de criptografía estándar y como mínimo, consiste en una librería de enlace dinámica (DLL) que implementa las funciones CryptoAPI.

Los proveedores asociados con CryptoAPI implementan tanto algoritmos de cifrado como almacenamiento de claves.

Sin embargo, los proveedores asociados con CNG (Crypto New generation) disponibles a partir de los sistemas operativos Windows Vista y Windows Server 2008, separan la implementación de algoritmos de cifrado del almacenamiento de las claves.

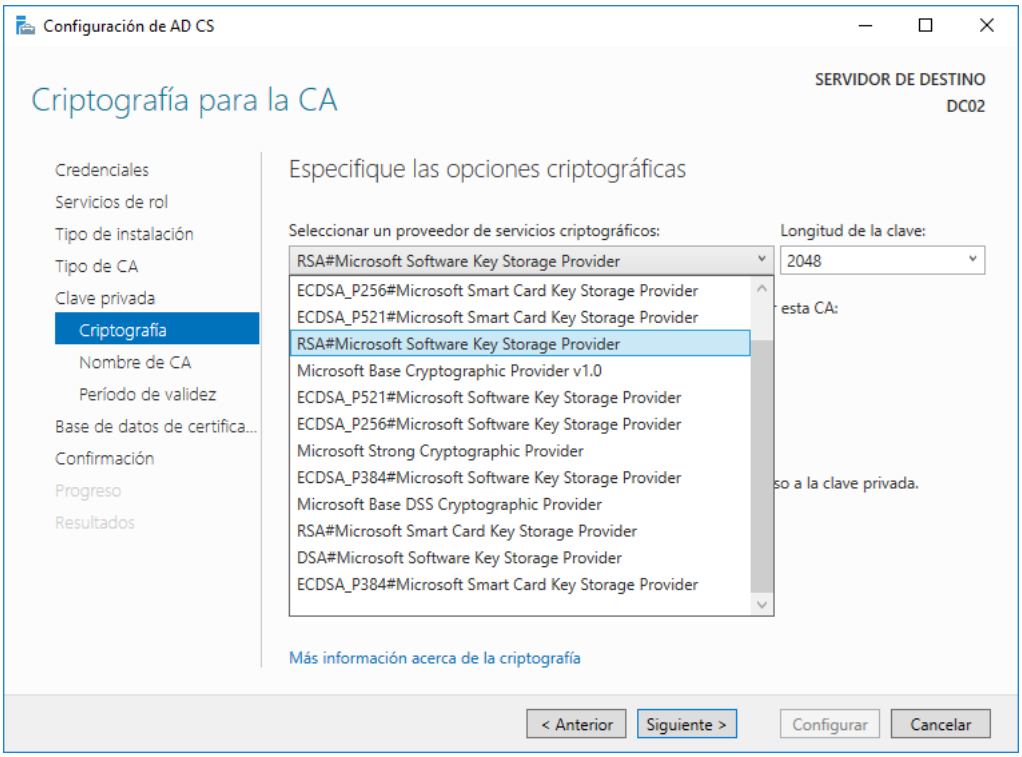
La siguiente lista muestra los proveedores de servicios de cifrado que actualmente están disponibles.

Nota: La información sobre proveedores de servicios de cifrado, así como algoritmos soportados y longitudes de claves, ha sido extraída de la siguiente página Web de Microsoft MSDN https://msdn.microsoft.com/en-us/library/windows/desktop/bb931380(v=vs.85).aspx. Es posible que las actualizaciones de seguridad modifiquen las configuraciones de seguridad predeterminadas de los proveedores de servicios de cifrado o incluso invaliden algoritmos que han sido considerados obsoletos.

Proveedor	Descripción
Microsoft Base Cryptographic Provider	Contiene un conjunto básico de funcionalidades criptográficas. Se distribuye con CryptoAPI v1.0 y v2.0.
Microsoft Strong Cryptographic Provider	Una extensión a “Microsoft Base Cryptographic Provider” disponible a partir de Windows XP y versiones superiores.
Microsoft Enhanced Cryptographic Provider	Basado en “Microsoft Base Cryptographic Provider” con mayor longitud en las claves y algoritmos adicionales añadidos.
Microsoft Enhanced RSA and AES Cryptographic Provider	Proveedor de cifrado mejorado de Microsoft que proporciona soporte de algoritmos de cifrado AES.
Microsoft Base DSS Cryptographic Provider	Proporciona funcionalidades de Hash, firma digital y verificación de la firma utilizando los algoritmos Secure Hash Algorithm (SHA) y Digital Signature Standard (DSS).
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider	Es un súper-conjunto del proveedor de cifrado DSS que además soporta el intercambio de claves Diffie-Hellman, funcionalidad Hash SHA, firma digital DSS y verificación de firma DSS.

Proveedor	Descripción
Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider	Soporta el intercambio de claves Diffie-Hellman (un derivado DES de 40 bits), funcionalidad Hash SHA, firma digital DSS y verificación de firma DSS.
Microsoft DH Schannel Cryptographic Provider	Soporta funcionalidad Hash, firma digital DSS, generación de claves Diffie-Hellman (D-H), intercambio de claves D-H. Además, soporta la derivación de claves para los protocolos SSL 3.0 y TLS 1.0
Microsoft RSA/Schannel Cryptographic Provider	Soporta funcionalidad Hash, firma digital y verificación de firma. El algoritmo CALG_SSL3_SHAMD5 se utiliza para la autenticación de clientes con los protocolos SSL 3.0 y TLS 1.0. Además, soporta la derivación de claves para los protocolos SSL2, PCT1, SSL3 y TLS1
Microsoft Base Smart Card Crypto Provider	Soporta tarjetas inteligentes.

Cuando se instala una Entidad de Certificación, uno de los parámetros más importantes que se debe seleccionar es el proveedor de servicios de cifrado (CSP) que va a utilizar dicha Entidad de Certificación junto con la longitud de la clave pública, tal y como se muestra en la siguiente imagen.



Más adelante, en esta guía, se mostrarán los pasos necesarios para instalar y configurar correctamente un servidor de Entidad de Certificación basado en Windows Server 2016 con los más altos niveles de seguridad.

6.1.1 ALGORITMOS Y LONGITUDES DE CLAVES

6.1.1.1 MICROSOFT BASE CRYPTOGRAPHIC PROVIDER

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
Data Encryption Standard (DES)	Cifrado	Bloque	56/56/56
Hashed Message Authentication Checksum (HMAC)	Hash	Cualquiera	0/0/0
Message Authentication Checksum (MAC)	Hash	Cualquiera	0/0/0
Message Digest 2 (MD2)	Hash	Cualquiera	128/128/128
Message Digest 4 (MD4)	Hash	Cualquiera	128/128/128
Message Digest 5 (MD5)	Hash	Cualquiera	128/128/128
RSA Data Security 2 (RC2)	Cifrado	Bloque	40/40/56
RSA Data Security 4 (RC4)	Cifrado	Bloque	40/40/56
RSA Key Exchange	Intercambio de claves	RSA	512/384/1024
RSA Signature	Firma	RSA	512/384/16384
Secure Hash Algorithm (SHA1)	Hash	Cualquiera	160/160/160
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hash	Cualquiera	288/288/288

6.1.1.2 MICROSOFT STRONG CRYPTOGRAPHIC PROVIDER

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
Data Encryption Standard (DES)	Cifrado	Bloque	56/56/56
Two Key Triple DES	Cifrado	Bloque	112/112/112
Three Key Triple DES	Cifrado	Bloque	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hash	Cualquiera	0/0/0
Message Authentication Checksum (MAC)	Hash	Cualquiera	0/0/0
Message Digest 2 (MD2)	Hash	Cualquiera	128/128/128
Message Digest 4 (MD4)	Hash	Cualquiera	128/128/128
Message Digest 5 (MD5)	Hash	Cualquiera	128/128/128
RSA Data Security 2 (RC2)	Cifrado	Bloque	128/40/128
RSA Data Security 4 (RC4)	Cifrado	Stream	128/40/128

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
RSA Key Exchange	Intercambio de claves	RSA	1024/384/16384
RSA Signature	Firma	RSA	1024/384/16384
Secure Hash Algorithm (SHA1)	Hash	Cualquiera	160/160/160
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hash	Cualquiera	288/288/288

6.1.1.3 MICROSOFT ENHANCED CRYPTOGRAPHIC PROVIDER

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
Data Encryption Standard (DES)	Cifrado	Bloque	56/56/56
Two Key Triple DES	Cifrado	Bloque	112/112/112
Three Key Triple DES	Cifrado	Bloque	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hash	Cualquiera	0/0/0
Message Authentication Checksum (MAC)	Hash	Cualquiera	0/0/0
Message Digest 2 (MD2)	Hash	Cualquiera	128/128/128
Message Digest 4 (MD4)	Hash	Cualquiera	128/128/128
Message Digest 5 (MD5)	Hash	Cualquiera	128/128/128
RSA Data Security 2 (RC2)	Cifrado	Bloque	128/40/128
RSA Data Security 4 (RC4)	Cifrado	Stream	128/40/128
RSA Key Exchange	Intercambio de claves	RSA	1024/384/16384
RSA Signature	Firma	RSA	1024/384/16384
Secure Hash Algorithm (SHA1)	Hash	Cualquiera	160/160/160
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hash	Cualquiera	288/288/288

6.1.1.4 MICROSOFT ENHANCED RSA AND AES CRYPTOGRAPHIC PROVIDER

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
Advanced Encryption Standard 128 (AES128)	Cifrado	Bloque	128/128/128
Advanced Encryption Standard 192 (AES192)	Cifrado	Bloque	192/192/192

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
Advanced Encryption Standard 256 (AES256)	Cifrado	Bloque	256/256/256
Data Encryption Standard (DES)	Cifrado	Bloque	56/56/56
Two Key Triple DES	Cifrado	Bloque	112/112/112
Three Key Triple DES	Cifrado	Bloque	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hash	Cualquiera	0/0/0
Message Authentication Checksum (MAC)	Hash	Cualquiera	0/0/0
Message Digest 2 (MD2)	Hash	Cualquiera	128/128/128
Message Digest 4 (MD4)	Hash	Cualquiera	128/128/128
Message Digest 5 (MD5)	Hash	Cualquiera	128/128/128
RSA Data Security 2 (RC2)	Cifrado	Bloque	128/128/128
RSA Data Security 4 (RC4)	Cifrado	Stream	128/128/128
RSA Key Exchange	Intercambio de claves	RSA	1024/384/16384
RSA Signature	Firma	RSA	1024/384/16384
Secure Hash Algorithm (SHA1)	Hash	Cualquiera	160/160/160
Secure Hash Algorithm (SHA256)	Hash	Cualquiera	256/256/256
Secure Hash Algorithm (SHA384)	Hash	Cualquiera	384/384/384
Secure Hash Algorithm (SHA512)	Hash	Cualquiera	512/512/512
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hash	Cualquiera	288/288/288

6.1.1.5 MICROSOFT BASE DSS CRYPTOGRAPHIC PROVIDER

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
Digital Signature Algorithm (DSA)	Firma	DSS	1024/512/1024
Message Digest 5 (MD5)	Hash	Cualquiera	128/128/128
Secure Hash Algorithm (SHA1)	Hash	Cualquiera	160/160/160

6.1.1.6 MICROSOFT BASE DSS AND DIFFIE-HELLMAN CRYPTOGRAPHIC PROVIDER

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
CYLINK Message Encryption Algorithm	Cifrado	Bloque	40/40/40
Data Encryption Standard (DES)	Cifrado	Bloque	56/56/56
Diffie-Hellman Key Exchange Algorithm	Intercambio de claves	Diffie-Hellman	512/512/1024
Diffie-Hellman Ephemeral Algorithm	Intercambio de claves	Diffie-Hellman	512/512/1024
Digital Signature Algorithm (DSA)	Firma	DSS	1024/512/1024
Message Digest 5 (MD5)	Hash	Cualquiera	128/128/128
RSA Data Security 2 (RC2)	Cifrado	Bloque	40/40/56
RSA Data Security 4 (RC4)	Cifrado	Stream	40/40/56
Secure Hash Algorithm (SHA1)	Hash	Cualquiera	160/160/160

6.1.1.7 MICROSOFT ENHANCED DSS AND DIFFIE-HELLMAN CRYPTOGRAPHIC PROVIDER

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
CYLINK Message Encryption Algorithm	Cifrado	Bloque	40/40/40
Data Encryption Standard (DES)	Cifrado	Bloque	56/56/56
Two Key Triple DES	Cifrado	Bloque	112/112/112
Three Key Triple DES	Cifrado	Bloque	168/168/168
Diffie-Hellman Key Exchange Algorithm	Intercambio de claves	Diffie-Hellman	1024/512/4096
Diffie-Hellman Ephemeral Algorithm	Intercambio de claves	Diffie-Hellman	1024/512/4096
Digital Signature Algorithm (DSA)	Firma	DSS	1024/512/1024
Message Digest 5 (MD5)	Hash	Cualquiera	128/128/128
RSA Data Security 2 (RC2)	Cifrado	Bloque	128/128/128
RSA Data Security 4 (RC4)	Cifrado	Stream	128/128/128
Secure Hash Algorithm (SHA1)	Hash	Cualquiera	160/160/160

6.1.1.8 MICROSOFT DH SCHANNEL CRYPTOGRAPHIC PROVIDER

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
CYLINK Message Encryption Algorithm	Cifrado	Bloque	40/40/40
Data Encryption Standard (DES)	Cifrado	Bloque	56/56/56
Two Key Triple DES	Cifrado	Bloque	112/112/112
Three Key Triple DES	Cifrado	Bloque	168/168/168
Diffie-Hellman Key Exchange Algorithm	Intercambio de claves	Diffie-Hellman	512/512/4096
Diffie-Hellman Ephemeral Algorithm	Intercambio de claves	Diffie-Hellman	512/512/4096
Digital Signature Algorithm (DSA)	Firma	DSS	1024/512/1024
Message Digest 5 (MD5)	Hash	Cualquiera	128/128/128
RSA Data Security 2 (RC2)	Cifrado	Bloque	40/40/128
RSA Data Security 4 (RC4)	Cifrado	Stream	40/40/128
Secure Hash Algorithm (SHA1)	Hash	Cualquiera	160/160/160
Schannel Encryption Key	Cifrado	Schannel	0/0/-1
Schannel MAC Key	Cifrado / Hash	Schannel	0/0/-1
Schannel Master Hash	Cifrado / Hash	Schannel	0/0/-1
Secure Sockets Layer (SSL3) Master	Cifrado	Schannel	384/384/384
Transport Layer Security (TLS1) Master	Cifrado	Schannel	384/384/384

6.1.1.9 MICROSOFT RSA SCHANNEL CRYPTOGRAPHIC PROVIDER

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
Advanced Encryption Standard 128 (AES128)	Cifrado	Bloque	128/128/128
Advanced Encryption Standard 256 (AES256)	Cifrado	Bloque	256/256/256
Data Encryption Standard (DES)	Cifrado	Bloque	56/56/56
Two Key Triple DES	Cifrado	Bloque	112/112/112
Three Key Triple DES	Cifrado	Bloque	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hash	Cualquiera	0/0/0
Message Authentication Checksum (MAC)	Hash	Cualquiera	0/0/0

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
Message Digest 5 (MD5)	Hash	Cualquiera	128/128/128
RSA Data Security 2 (RC2)	Cifrado	Bloque	128/128/128
RSA Data Security 4 (RC4)	Cifrado	Stream	128/128/128
RSA Key Exchange	Intercambio de claves	RSA	1024/384/16384
Schannel Encryption Key	Cifrado	Schannel	0/0/-1
Schannel Master Hash	Cifrado / Hash	Schannel	0/0/-1
Schannel MAC Key	Cifrado / Hash	Schannel	0/0/-1
Secure Hash Algorithm (SHA1)	Hash	Cualquiera	160/160/160
Secure Socket Layer 2 (SSL2) Master	Cifrado	Schannel	40/40/192
Secure Socket Layer 3 (SSL3) Master	Cifrado	Schannel	384/384/384
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hash	Cualquiera	288/288/288
Transport Layer Security (TLS1) Master	Cifrado	Schannel	384/384/384
Data Encryption Standard (DES)	Cifrado	Bloque	56/56/56

6.1.1.10 MICROSOFT BASE SMART CARD CRYPTO PROVIDER.

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
Advanced Encryption Standard 128 (AES128)	Cifrado	Block	128/128/128
Advanced Encryption Standard 192 (AES192)	Cifrado	Block	192/192/192
Advanced Encryption Standard 256 (AES256)	Cifrado	Block	256/256/256
Data Encryption Standard (DES)	Cifrado	Block	56/56/56
Two Key Triple DES	Cifrado	Block	112/112/112
Three Key Triple DES	Cifrado	Block	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hash	Any	0/0/0
Message Authentication Checksum (MAC)	Hash	Any	0/0/0
Message Digest 2 (MD2)	Hash	Any	128/128/128
Message Digest 4 (MD4)	Hash	Any	128/128/128
Message Digest 5 (MD5)	Hash	Any	128/128/128

Algoritmo	Utilización	Tipo	Longitud de clave (predeterminado / mínimo / máximo)
RSA Data Security 2 (RC2)	Cifrado	Block	128/40/128
RSA Data Security 4 (RC4)	Cifrado	Stream	128/40/128
RSA Key Exchange	Intercambio de claves	RSA	1024/1024/4096
RSA Signature	Firma	RSA	1024/1024/4096
Secure Hash Algorithm (SHA1)	Hash	Any	160/160/160
Secure Hash Algorithm 256 (SHA256)	Hash	Any	256/256/256
Secure Hash Algorithm 384 (SHA384)	Hash	Any	384/384/384
Secure Hash Algorithm 512 (SHA512)	Hash	Any	512/512/512
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hash	Any	288/288/288

A continuación, se muestran los algoritmos de cifrado soportados por los proveedores de servicios de cifrado (CSP) de tipo CNG (Cryptography API Next Generation).

6.1.1.11 ALGORITMOS SIMÉTRICOS

Algoritmo	Modos soportados	Longitud de clave (predeterminado / mínimo / máximo)
Advanced Encryption Standard (AES)	ECB, CBC, CFB8, CFB128, GCM, CCM, GMAC, CMAC, AES Key Wrap	128/192/256
Data Encryption Standard (DES)	ECB, CBC, CFB8, CFB64	56/56/56
Data Encryption Standard XORed(DESX)	ECB, CBC, CFB8, CFB64	192/192/192
Triple Data Encryption Standard (3DES)	ECB, CBC, CFB8, CFB64	112/168
RSA Data Security 2 (RC2)	ECB, CBC, CFB8, CFB64	16 to 128 in 8 bit increments
RSA Data Security 4 (RC4)		8 to 512, in 8-bit increments

6.1.1.12 ALGORITMOS ASIMÉTRICOS

Algoritmo	Modos soportados	Longitud de clave (predeterminado / mínimo / máximo)
Digital Signature Algorithm (DSA)	La implementación cumple con FIPS 186-3 para los tamaños de claves desde 1024 a 3072 bits. La implementación cumple con FIPS 186-2 para los tamaños de claves desde 512 a 1024 bits	De 512 a 3072 en incrementos de 64 bits
RSA	Incluye algoritmos RSA que utilizan PKCS1, codificación "Optimal Asymmetric Encryption Padding (OAEP)" o "Probabilistic Signature Scheme (PSS) plaintext padding"	De 512 a 16384 en incrementos de 64 bits

6.1.1.13 ALGORITMOS HASH

Algoritmo	Modos soportados	Longitud de clave (predeterminado / mínimo / máximo)
Secure Hash Algorithm 1 (SHA1)	Incluye HmacSha1	160/160/160
Secure Hash Algorithm 256 (SHA256)	Incluye HmacSha256	256/256/256
Secure Hash Algorithm 384 (SHA384)	Incluye HmacSha384	384/384/384
Secure Hash Algorithm 512 (SHA512)	Incluye HmacSha512	512/512/512
Message Digest 2 (MD2)	Incluye HmacMd2	128/128/128
Message Digest 4 (MD4)	Incluye HmacMd4	128/128/128
Message Digest 5 (MD5)	Incluye HmacMd5	128/128/128

6.1.1.14 ALGORITMOS DE INTERCAMBIO DE CLAVES

Algoritmo	Modos soportados	Longitud de clave (predeterminado / mínimo / máximo)
Secure Hash Algorithm 1 (SHA1)	Incluye HmacSha1	160/160/160
Secure Hash Algorithm 256 (SHA256)	Incluye HmacSha256	256/256/256
Secure Hash Algorithm 384 (SHA384)	Incluye HmacSha384	384/384/384

A continuación, y para finalizar la identificación de los diferentes proveedores de servicios de cifrado incluidos en los sistemas operativos Windows, se muestran los proveedores de almacenamiento de claves (CNG Key Storage Providers).

Al contrario de lo que sucede con Cryptography API (CryptoAPI), la nueva implementación que se incluye a partir de Windows Vista y Windows Server 2008, denominada Cryptography API Next Generation (CNG), separa los proveedores de cifrado de los proveedores de almacenamiento de claves (Key Storage Providers).

Los proveedores de almacenamiento de claves se utilizan para crear, eliminar, exportar, importar, abrir y almacenar claves de cifrado.

Dependiendo de la implementación, también se pueden utilizar para las funciones de cifrado asimétrico, acuerdo de secretos y firma digital.

De forma predeterminada, Microsoft instala los siguientes proveedores de almacenamiento de claves a partir de Vista y Windows Server 2008, sin embargo, otros fabricantes de software pueden instalar sus propias implementaciones.

6.1.1.15 MICROSOFT SOFTWARE KEY STORAGE PROVIDER

Algoritmo	Propósito	Longitud de clave (predeterminado / mínimo / máximo)
Diffie-Hellman (DH)	Acuerdo de secretos e intercambio de claves	De 512 a 4096 en incrementos de 64 bits
Digital Signature Algorithm (DSA)	Firma	De 512 a 1024 en incrementos de 64 bits
Elliptic Curve Diffie-Hellman (ECDH)	Acuerdo de secretos e intercambio de claves	P256, P384, P521
Elliptic Curve Digital Signature Algorithm (ECDSA)	Firma	P256, P384, P521
RSA	Cifrado asimétrico y firma	De 512 a 16384 en incrementos de 64 bits

6.1.1.16 MICROSOFT SMART CARD KEY STORAGE PROVIDER

Algoritmo	Propósito	Longitud de clave (predeterminado / mínimo / máximo)
Diffie-Hellman (DH)	Acuerdo de secretos e intercambio de claves	De 512 a 4096 en incrementos de 64 bits
Elliptic Curve Diffie-Hellman (ECDH)	Acuerdo de secretos e intercambio de claves	P256, P384, P521
Elliptic Curve Digital Signature Algorithm (ECDSA)	Firma	P256, P384, P521
RSA	Cifrado asimétrico y firma	De 512 a 16384 en incrementos de 64 bits

7. ARQUITECTURA Y SEGURIDAD DEL SERVICIO DE ENTIDAD DE CERTIFICACIÓN DE WINDOWS SERVER 2016

7.1 COMPONENTES DE LOS SERVICIOS DE CERTIFICADOS

Los servicios de certificados de Directorio Activo (AD CS) en Windows Server 2016 incluyen los siguientes componentes instalables:

a) Entidad de Certificación (CA). Las entidades de certificación de tipo raíz y subordinadas se utilizan para la emisión de certificados a usuarios, equipos y servicios, además de administrar sus características y tiempo de validez.

b) Inscripción Web de Entidad de Certificación. El servicio de inscripción Web de Entidad de Certificación permite a los usuarios conectarse a la Entidad de Certificación a través de un navegador para solicitar y renovar certificados, así como visualizar solicitudes pendientes, descargar la lista de revocación de certificados o realizar la inscripción para certificados de tarjetas inteligentes.

c) Servicio respondedor en línea. El servicio respondedor en línea implementa el protocolo en línea de estado de certificados (OCSP) y permite que los datos de comprobación de revocación de los certificados sean accesibles a clientes en entornos de red complejos. Se puede utilizar como una alternativa a las listas de revocación de certificados (CRLs). Este servicio cumple con la especificación RFC 2560 de OCSP.

d) Servicio de inscripción de dispositivos de red. El servicio de inscripción de dispositivos de red permite que enrutadores y otro tipo de dispositivos de red obtengan certificados basándose en el protocolo simple de inscripción de certificados (SCEP) de Cisco Systems. El servicio soporta el registro y la distribución de claves públicas de Entidades de Certificación, inscripción de certificados, revocación, consultas y renovación de certificados.

e) Servicio Web de inscripción de certificados. El servicio Web de inscripción de certificados permite a los usuarios y equipos inscribir certificados nuevos y renovar los existentes incluso cuando el equipo no es miembro de un dominio o se encuentra provisionalmente fuera del límite de seguridad de la red. Este servicio colabora con el servicio Web de directivas de inscripción de certificados a fin de proporcionar inscripciones automáticas de certificados basadas en directivas a los usuarios y equipos.

f) Servicio Web de directivas de inscripción de certificados. El servicio Web de directivas de inscripción de certificados permite a los usuarios y equipos obtener información sobre la directiva de inscripción de certificados incluso cuando el equipo no es miembro de un dominio o se encuentra provisionalmente fuera del límite de seguridad de la red corporativa.

7.2 ROLES DISPONIBLES EN LAS DIFERENTES EDICIONES DE WINDOWS SERVER

Una Entidad de Certificación se puede instalar en cualquier edición de Windows Server 2016, excepto la edición Web, sin embargo, no todas las ediciones incluyen todos los roles del servicio.

Los escenarios que presenta esta guía están basados en la edición Standard de Microsoft Windows Server 2016.

La siguiente tabla muestra los diferentes componentes del servicio de Entidad de Certificación de Directorio Activo que se pueden instalar en cada una de las ediciones disponibles de Windows Server 2016.

Componente	Web	Standard	Datacenter
Entidad de Certificación	No	Si	Si
Inscripción Web de Entidad de Certificación	No	Si	Si
Servicio respondedor en línea	No	Si	Si
Servicio de inscripción de dispositivos de red	No	Si	Si
Servicio Web de inscripción de certificados	No	Si	Si
Servicio Web de directivas de inscripción de certificados	No	Si	Si
Versión 2 y versión 3 de certificados	No	Si	Si
Plantillas	No	Si	Si
Archivado de claves	No	Si	Si
Separación de roles	No	Si	Si
Restricciones en la gestión de certificados	No	Si	No
Restricciones en la delegación del agente de inscripción	No	Si	Si
Compatibilidad del módulo de directivas con el Servicio de inscripción de dispositivos de red	No	Si	Si
Atestación de clave de TPM	No	Si	Si
Windows PowerShell para servicios de servidor de certificados	No	Si	Si

7.3 CONFIGURACIÓN DE LA SEGURIDAD DE LA ENTIDAD DE CERTIFICACIÓN

Es sumamente importante definir y planificar la seguridad de una infraestructura de clave pública como son los servicios de Entidad de Certificación de Windows Server 2016.

La Entidad de Certificación se convierte en un componente clave de la seguridad de la organización, por lo tanto, debe estar protegida y adecuadamente administrada, al mismo nivel, si cabe, en el que están los servidores controladores de dominio.

Si se vulnera la seguridad de una Entidad de Certificación, o de alguno de sus componentes o certificados, toda la seguridad de la organización queda expuesta a diferentes tipos de ataques, entre los que se encuentran los ataques “man in the middle”, suplantación de identidad, revelación de información confidencial, etc.

Es por ello que una de las recomendaciones de seguridad en la fase de diseño de una infraestructura de clave pública, es implementar la administración basada en roles, para organizar a los administradores de la Entidad de Certificación en roles separados y predefinidos.

Se pueden asignar roles a usuarios para que puedan desarrollar un tipo de tarea específica en la administración de la Entidad de Certificación, de tal forma que se tenga un control en todo momento, del usuario o grupo de usuarios que han podido realizar una tarea concreta.

La siguiente tabla muestra los roles, usuarios y grupos que se pueden utilizar para implementar una administración basada en roles.

Roles y grupos	Permisos de seguridad	Descripción
Administrador de la Entidad de Certificación	Administrar la Entidad de Certificación	Configura y mantiene la CA. Es un rol de CA que incluye la capacidad de asignar todos los demás roles de CA y renovar el certificado de CA. Estos permisos se asignan mediante el complemento Entidad de Certificación.
Administrador de certificados	Emitir y administrar certificados	Aprueba solicitudes de revocación e inscripción de certificados. Es un rol de CA. Este rol se llama, a veces, autoridad CA. Estos permisos se asignan mediante el complemento Entidad de Certificación.
Operador de copias de seguridad	Hacer copias de seguridad de archivos y directorios. Restaurar archivos y directorios	Lleva a cabo la copia de seguridad y la recuperación del sistema. Copia de seguridad es una característica del sistema operativo.
Auditor	Administrar registro de seguridad y auditoría	Configura, ve y mantiene los registros de auditoría. Auditoría es una característica del sistema operativo. Auditor es un rol del sistema operativo.
Inscritos	Leer e inscribir certificados	Los inscritos son clientes con autorización para solicitar certificados desde una CA. No es un rol de CA.

Los miembros del grupo “administradores locales”, “administradores de empresas” o “Admins. del dominio” pueden asignar y modificar todos los roles de la Entidad de Certificación.

Además, en las Entidades de Certificación de empresa, los administradores locales, administradores de empresas y administradores de dominio son administradores de la Entidad de Certificación de manera predeterminada.

Cada rol de la Entidad de Certificación tiene asociado una lista específica de tareas de administración de CA. En la siguiente tabla se enumeran todas las tareas de administración de la Entidad de Certificación junto con los roles en las que se llevan a cabo.

Actividad	Administrador de CA	Administrador de Certificados	Auditor	Operador de copias de seguridad	Administrador local
Emitir y aprobar certificados		X			
Denegar certificados		X			
Revocar certificados		X			
Reactivar certificados en suspensión		X			
Habilitar, publicar o configurar programaciones de lista de revocación de certificados (CRL)	X				
Recuperar claves archivadas		X			
Configurar parámetros de auditoría			X		
Registros de auditoría			X		
Copia de seguridad del sistema				X	
Restaurar el sistema				X	
Leer la base de datos de CA	X	X	X	X	
Leer información de configuración de CA	X	X	X	X	

Los inscritos pueden leer las propiedades de las entidades de certificación y listas CRL, y también pueden solicitar certificados. En una Entidad de Certificación de empresa, un usuario debe tener permisos de lectura y de inscripción en la plantilla de certificados para solicitar un certificado.

Además, los administradores de Entidad de Certificación, los administradores de certificados, los auditores y los operadores de copia de seguridad tienen permisos de lectura implícitos.

Un auditor tiene el derecho de usuario de auditoría del sistema.

Un operador de copia de seguridad tiene el derecho de usuario de copia de seguridad del sistema. Además, el operador de copia de seguridad puede iniciar y detener el servicio "Servicios de certificados de Active Directory (AD CS)".

7.4 RESTRICCIÓN DE LOS ADMINISTRADORES DE CERTIFICADOS

En entornos con un alto nivel de seguridad y control de las operaciones, es posible que se necesiten restringir los procesos de aprobación y emisión de certificados de forma individualizada y por plantilla de certificados a usuarios o grupos específicos.

El servicio de Entidad de Certificación de Windows Server 2016 permite precisar, aún más, su capacidad de administrar certificados por grupo y por plantilla de certificado. Por ejemplo, es posible que requiera implementar una restricción, para que solo puedan aprobar solicitudes o revocar certificados de inicio de sesión de tarjeta inteligente, para los usuarios de una determinada oficina o unidad organizativa que sea la base de un grupo de seguridad.

Esta restricción se basa en un subconjunto de plantillas de certificado habilitado para la Entidad de Certificación (CA) y los grupos de usuarios con permisos de inscripción para la plantilla de certificado de dicha CA.

7.5 AUDITORÍA DE EVENTOS DEL SERVICIO DE ENTIDAD DE CERTIFICACIÓN

Tal y como sucede con otros servicios de Windows Server, el servicio de Entidad de Certificación de Directorio Activo se puede configurar para que se registren los principales eventos relacionados con la administración y las actividades de la propia entidad.

Se puede habilitar la auditoría de los siguientes eventos:

a) Copia de seguridad y restauración de la base de datos de CA.

b) Cambio de la configuración de CA.

c) Cambio de la configuración de seguridad de CA.

d) Emisión y administración de solicitudes de certificados.

e) Revocación de certificados y publicación de listas de revocación de certificados (CRL).

f) Almacenamiento y recuperación de claves archivadas.

g) Inicio y detención individual de los Servicios de certificados de Active Directory (AD CS).

Para auditar eventos indicados, el servidor debe estar configurado para auditar también el acceso a objetos. De forma predeterminada, la auditoría no está habilitada.

Las opciones de directiva de auditoría se pueden ver y administrar mediante una directiva de grupo local o de dominio en **"Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales"**.

Si aplica esta configuración de directiva, aparecen los siguientes eventos en el sistema operativo:

Identificador del evento	Mensaje de evento
4868	El Administrador de certificados ha denegado una solicitud de certificado pendiente.
4869	Los servicios de certificación recibieron una solicitud de certificado reenviada.
4870	Los servicios de certificación han revocado un certificado.
4871	Los servicios de certificación recibieron una solicitud para publicar la lista de revocación de certificados (CRL).
4872	Los servicios de certificación han publicado la lista de revocación de certificados (CRL).
4873	Se ha cambiado una extensión de solicitud de certificado.
4874	Se ha cambiado uno o varios atributos de la solicitud de certificado.
4875	Los servicios de certificación recibieron una solicitud para apagar el servicio.
4876	Se inició la copia de seguridad de los servicios de certificación.
4877	Copia de seguridad completada.
4878	Se ha iniciado la restauración de los servicios de certificación.
4879	Se ha completado de restauración de los servicios de certificación.
4880	Se han iniciado los servicios de certificación.
4881	Se han detenido los servicios de certificación.
4882	Se han cambiado los permisos de seguridad para los servicios de certificación.
4883	Los servicios de certificación han recuperado una clave archivada.
4884	Los servicios de certificación han importado un certificado a su base de datos.
4885	El filtro de auditoría para los servicios de certificación ha cambiado.
4886	Los servicios de certificación recibieron una solicitud de certificado.
4887	Los servicios de certificación han aprobado una solicitud de certificado y se ha emitido un certificado.
4888	Los servicios de certificación han denegado una solicitud de certificado.
4889	Los servicios de certificación han establecido el estado de una solicitud de certificado como pendiente.
4890	Se ha cambiado la configuración del administrador de certificados para los servicios de certificación.
4891	Una entrada de configuración ha sido cambiada en los servicios de certificación.

Identificador del evento	Mensaje de evento
4892	Se ha cambiado una propiedad de los servicios de certificación.
4893	Los servicios de certificación han archivado una clave.
4894	Los servicios de certificación han importado y archivado una clave.
4895	Los servicios de certificación han publicado el certificado de entidad emisora de certificados en los servicios de dominio de Directorio Activo.
4896	Una o más filas se eliminaron de la base de datos de certificados.
4897	Habilitada la separación de funciones.

En esta guía, se mostrará como configurar paso a paso la auditoría de una Entidad de Certificación.

7.6 SOPORTE DE VALIDACIÓN EXTENDIDA (EV)

Los certificados de validación extendida son un tipo especial de certificados que requieren un proceso más exhaustivo de análisis del solicitante para poder emitir el certificado.

En el año 2006, el grupo "CA Browser Forum", el cual engloba a las principales autoridades de certificación y fabricantes de software de navegadores, aprobó un conjunto de estándares de visibilidad y validación de certificados denominadas directrices SSL con validación extendida (EV).

Los principales objetivos de un certificado de validación extendida son:

a) Identificar la entidad legal que controla un sitio Web y, por tanto, proporcionar una garantía razonable, a los usuarios de un navegador de internet, de que el sitio Web que están visitando está controlado por una entidad legal. Esta entidad legal vendrá identificada en el certificado de validación extendida por su nombre, dirección del negocio, jurisdicción, número de registro del negocio u otra información relativa a la organización.

b) Habilitar las comunicaciones cifradas con un sitio Web, facilitando el intercambio de claves de cifrado para permitir el envío cifrado de comunicación a través de internet entre el usuario del navegador y el sitio Web.

Así mismo, los certificados de validación extendida ayudan a establecer la legitimidad de una entidad y afrontar problemas relacionados con el phising, código dañino y otros tipos de fraudes o suplantaciones de identidad.

En el siguiente enlace se puede descargar la última versión de la guía de emisión de certificados de validación extendida que deben cumplir todas las Entidades de Certificación públicas adscritas al CA Browser Forum: https://cabforum.org/extended-validation/.

En entornos de ámbito privado, el servicio de Entidad de Certificación de Directorio Activo de Windows Server 2016 soporta la configuración de propiedades de aplicación y la emisión de certificados con un O.I.D. específico para la validación extendida.

8. NOVEDADES EN SERVIDOR DE CERTIFICADOS EN WINDOWS SERVER 2016

8.1 COMPATIBILIDAD PARA LA ATESTACIÓN DE CLAVES DE TPM

La atestación de clave de TPM permite a la entidad emisora de certificados (CA) comprobar que la clave privada está protegida por un TPM basado en hardware y que el TPM es de confianza para la autoridad de certificación.

La atestación de clave de TPM impide que el certificado se exponga a un dispositivo no autorizado y se puede enlazar la identidad del usuario con el dispositivo.

Los proveedores de almacenamiento de claves (KSP) es aquel que permite el almacenamiento y la recuperación de claves.

Como novedad, se admite la atestación de clave TPM de tarjeta inteligente como KSP, mejorando así la compatibilidad para la atestación de claves.

El Servicio de inscripción de dispositivos de red (NDES, Network Device Enrollment Service) es uno de los servicios de rol de Active Directory Certificate Services (AD CS). Implementa el protocolo Simple Certificate Enrollment Protocol (SCEP), que define la comunicación entre los dispositivos de red y una Autoridad de Registro (RA) para la inscripción de certificados.

Los dispositivos que no están unidos al dominio ahora pueden utilizar la inscripción NDES para obtener los certificados que pueden recibir atestación para las claves que están en TPM.