## 2.2.5 AUTENTICACIÓN DE CERTIFICADOS INDIVIDUALES

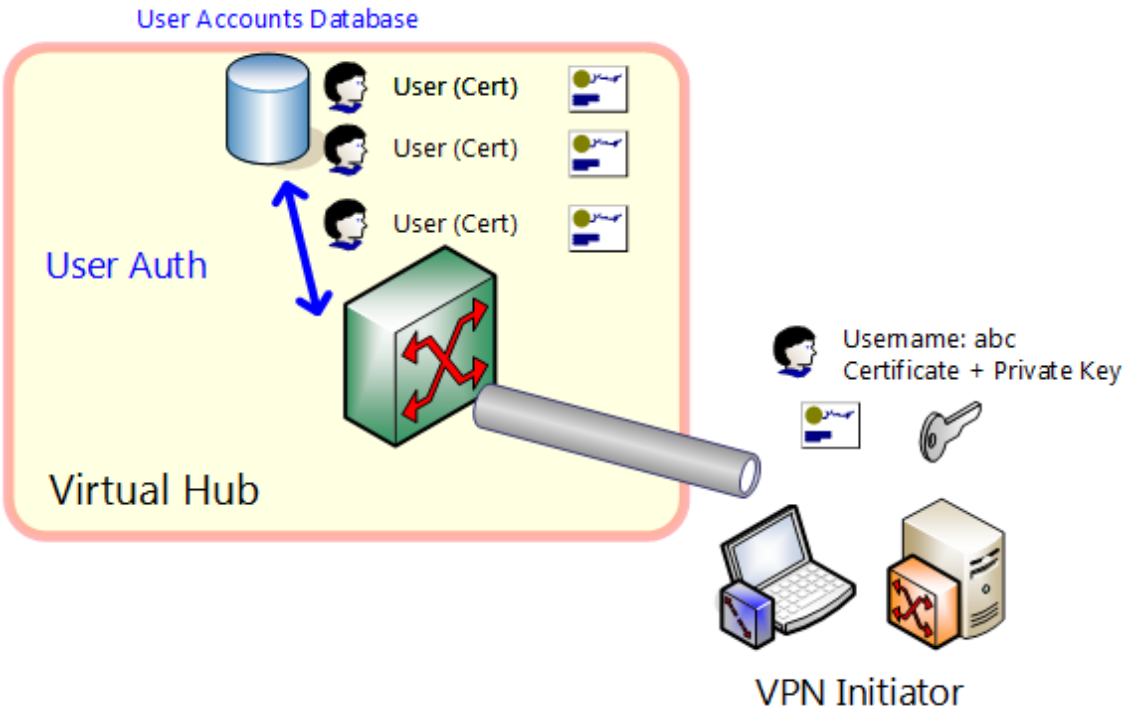
### CUESTIONES COMUNES A LA AUTENTICACIÓN DE CERTIFICADOS

Con la autenticación de certificado, cuando el ordenador de origen de la conexión intenta conectarse al concentrador virtual, presenta un nombre de usuario junto con un certificado electrónico X.509. El Servidor VPN SoftEther comprueba si es correcto y sólo se permite la conexión al ordenador de origen de la conexión si se aprueba. El Servidor VPN SoftEther comprueba si es correcto y el ordenador de origen de la conexión sólo puede conectarse si lo supera.

El ordenador de origen de la conexión debe poseer datos de certificado y una clave privada (clave privada RSA) que se corresponda con la clave pública del certificado a presentar. Los datos del certificado se envían desde el ordenador de origen de la conexión al Servidor VPN, pero los datos de la clave privada no se transmiten. A continuación, el Servidor VPN envía datos numéricos aleatorios (denominados valores de desafío) al cliente. Cuando el cliente recibe los datos, los firma mediante la clave privada que posee y devuelve los datos. El Servidor VPN verifica los datos de firma enviados por el cliente utilizando la clave pública del certificado electrónico recibido inicialmente y se asegura de que el ordenador cliente posee el certificado y la clave privada correspondiente (si no se puede confirmar, la autenticación del usuario falla en el acto). A continuación, comprueba si el certificado presentado posteriormente por el cliente coincide con el atribuido definido para cada usuario como datos de autenticación de usuario. En este momento puede seleccionar como método de comprobación la autenticación de certificado individual o la autenticación de certificado firmado.

Los certificados que se pueden utilizar con SoftEther VPN tienen formato X.509. Se utiliza RSA para el algoritmo PKI, y la longitud en bits de las claves pública y privada es de 1.024 o 2.048 bits. Se puede utilizar la versión 1 de los certificados X.509 y posteriores, pero algunos campos de extensión no son compatibles (se ignora su contenido). Los valores de asunto que pueden reconocer todos los módulos SoftEther VPN son "CN" y "O" y "OU", "C" y "ST", "L".

Los certificados que han caducado y los registrados en la lista de certificados inválidos que se puede configurar por Hub Virtual se reconocen como inválidos y la autenticación de usuario siempre falla.




Autenticación de certificados de cliente mediante autenticación de certificados individuales

Con la autenticación de certificado individual, los datos del certificado se registran para el usuario en la base de datos de usuarios del Hub Virtual, y se concede permiso para conectarse si el certificado presentado por el usuario coincide perfectamente con el certificado registrado previamente.

## VENTAJAS DE LA AUTENTICACIÓN INDIVIDUAL DE CERTIFICADOS

El uso de la autenticación de certificado individual facilita el uso de SoftEther VPN con la función de autenticación de certificado. Especialmente si el número de usuarios que utilizan la autenticación de certificados oscila entre varios y decenas de usuarios, el sistema VPN puede funcionar suficientemente mediante la autenticación de certificados individual. En cuanto al método de funcionamiento específico, el administrador del concentrador virtual crea varios certificados X.509, los registra secuencialmente en el concentrador virtual y, mediante la transferencia del certificado y la clave privada al usuario por un método seguro (correo electrónico en la LAN de la empresa, carpeta compartida o tarjeta inteligente), el usuario puede utilizarlos para conectarse al concentrador virtual del servidor VPN en cualquier momento. Por el contrario, el usuario puede crear el certificado y registrarlo transfiriéndolo al administrador del concentrador virtual (este método es más seguro porque la clave privada nunca deja de estar en posesión del usuario).

La clave privada y el certificado X.509 pueden crearse con una utilidad (freeware o software disponible comercialmente) compatible con varias PKI existentes. El archivo de certificado X.509 y el archivo de clave privada pueden crearse mediante el comando MakeCert de la herramienta de creación de certificados y la utilidad de gestión de línea de comandos de SoftEther VPN (vpncmd), que son funciones del Administrador del servidor VPN SoftEther. Estas sencillas utilidades admiten la creación tanto de certificados autofirmados como de certificados firmados.

### DESVENTAJAS DE LA AUTENTICACIÓN DE CERTIFICADOS INDIVIDUALES

La autenticación de certificado individual es difícil de utilizar si hay un gran número de usuarios que deben registrarse o la PKI ha sido adoptada por la empresa y cada empleado tiene una clave privada en una tarjeta inteligente (identificación de empleado, etc.). En tal caso, le recomendamos que seleccione la autenticación de certificado firmado.

## AUTENTICACIÓN DE CERTIFICADOS FIRMADOS

### AUTENTICACIÓN DE CERTIFICADOS DE CLIENTE MEDIANTE AUTENTICACIÓN DE CERTIFICADOS FIRMADOS

La autenticación de certificados firmados resulta útil cuando la CA (Autoridad de certificación) de la empresa distribuye un certificado X.509 y un archivo de clave privada a cada empleado. También si el sistema PKI aún no está adoptado, pero se quiere permitir el acceso a un gran número de usuarios al Hub Virtual, se puede utilizar si se quiere usar la autenticación por certificado. Los requisitos para utilizar este método son los siguientes.

Un certificado X.509 y su correspondiente clave privada deben ser distribuidos a cada usuario para acceder a Virtual Hub por archivo o tarjeta inteligente.

Los certificados para cada usuario respectivo están firmados por el certificado raíz (o certificado intermedio) y la clave privada que posee la CA de la empresa (asociación de certificados) y tienen relación de fiabilidad de estructura de árbol.

Si se utiliza la autenticación mediante certificado firmado, el certificado raíz (o intermedio) firmado para cada usuario se registra en la lista de certificados de la CA en la que confía el concentrador virtual.

A continuación, se crea un nuevo usuario y se establece la autenticación de certificado firmado como método de autenticación para ese usuario. De este modo, si se confirma que el certificado presentado por el ordenador cliente conectado por nombre de usuario está firmado por un certificado de la lista de certificados de una CA de confianza registrada en el concentrador virtual, ese ordenador cliente pasa la autenticación de usuario.

Con este método, sin embargo, debido a la igualdad de trato, cualquier empleado que tenga un certificado emitido por CA raíz de la empresa, por ejemplo, si se diferencian los usuarios que desean aumentar los tipos de protocolo que se pueden comunicar, se utiliza junto con el método de limitación de certificados conectables por número de serie o Nombre Común, que se describirá a continuación.

### LIMITACIÓN DE CERTIFICADOS CONECTABLES POR NOMBRE COMÚN O NÚMERO DE SERIE

El contenido de un certificado X.509 puede incluir un nombre común (CN) y un número de serie. En tal caso, limitando el Nombre Común y el número de serie, por ejemplo, incluso en el caso de que no se pudiera confirmar que el certificado está firmado por un certificado de un Núcleo Virtual de confianza CA o cuando uno o ambos elementos del número de serie no coinciden perfectamente, se puede denegar el acceso.

Si se utiliza esta función, mediante la creación de usuarios que pueden conectarse sólo si cierto número de serie o el valor CN del certificado firmado por el certificado que se puede confiar, la política de seguridad, etc se puede diferenciar de acuerdo con el tipo de certificado.

# AUTENTICACIÓN DEL SERVIDOR

Esta sección contiene una descripción del método de autenticación de los ordenadores cliente VPN que se conectan al Servidor VPN SoftEther en el punto anterior. La autenticación del servidor es, por el contrario, la función mediante la cual el Servidor VPN comprueba que el equipo cliente VPN (cliente VPN o Servidor VPN / Puente VPN que realiza la conexión en cascada) que intenta conectarse al Servidor VPN SoftEther es auténtico. Normalmente esta función está desactivada por defecto. Aunque la autenticación del servidor no es necesaria para el funcionamiento convencional, puede habilitarse para cada configuración de conexión de cliente o de conexión en cascada.

## NECESIDA DE AUTENTICACIÓN DEL SERVIDOR

### EN RELACIÓN CON EL ATAQUE DEL HOMBRE EN EL MEDIO EN INTERNET DE LA RED IP PÚBLICA

La autenticación del servidor es necesaria para verificar si el servidor VPN de destino de la conexión cuando se conecta a una VPN insegura utilizando una red pública es auténtico. Al plantar un software especial que reescribe el protocolo en la línea de una red IP, un tercero malintencionado puede técnicamente hacer que parezca que se está conectando a un servidor VPN auténtico cuando en realidad está intentando conectarse a uno falso. Al redirigir la conexión desde el servidor VPN falso al servidor VPN al que el usuario pretende conectarse, un tercero malintencionado puede leer temporalmente y volver a cifrar y enviar todos los paquetes que fluyen en la VPN a su puesto de destino, de modo que puede escuchar a escondidas o manipular la comunicación VPN sin que el usuario sea consciente de ello.

Esto se denomina "ataque directo", "ataque de hombre en el medio" o "ataque de persona en el medio". Debido a la enorme cantidad de tráfico en la red troncal de Internet, siendo realistas, es difícil instalar software especial en la red troncal para llevar a cabo estos ataques, pero tales ataques han tenido éxito en partes de las ramas de la red donde el rendimiento no es tan alto.

Por lo tanto, la función de autenticación del servidor se utiliza si se quiere evitar que los datos transmitidos en VPN sean escuchados o manipulados por este tipo de ataques.

## MECANISMO DE AUTENTICACIÓN DE SERVIDOR POR CERTIFICADO

La autenticación de servidor por certificado verifica que el servidor VPN de destino de la conexión es auténtico mediante la verificación del certificado, la función opuesta a la autenticación de certificado de cliente. El Servidor VPN de destino de la conexión posee un certificado X.509 y los datos de clave privada correspondientes, y el ordenador cliente VPN (cliente VPN o Servidor VPN / Puente VPN que realiza la conexión en cascada) que intenta conectarse al Servidor VPN determina si se puede confiar en el Servidor VPN de destino de la conexión por el contenido del certificado. Dado que para verificar el certificado se utiliza un algoritmo RSA, el Servidor VPN debe disponer de una clave privada que se corresponda con el certificado.

Si el servidor falla en la verificación o presenta un certificado caducado, se determina que el Servidor VPN de destino de la conexión no es suficientemente fiable y se interrumpe la conexión VPN.

Los dos métodos mediante los cuales el ordenador cliente VPN (cliente VPN o Servidor VPN / Puente VPN que realiza la conexión en cascada) puede determinar si el certificado presentado por el Servidor VPN de destino de la conexión es de confianza son los siguientes.

## AUTENTICACIÓN DE CERTIFICADO INDIVIDUAL DE SERVIDOR

La autenticación de certificado individual del servidor es un método de autenticación por el que el certificado X.509 del servidor VPN de destino de la conexión se registra para cada configuración de conexión al servidor VPN y la conexión al servidor VPN continúa sólo cuando el certificado presentado por el servidor VPN al conectarse coincide perfectamente con el certificado registrado de antemano, y si no la conexión se cortará.

Este método puede utilizarse si ya se posee el certificado del servidor VPN de destino de la conexión. El contenido del certificado se muestra en la ventana cuando se intenta conectar por primera vez al Servidor VPN de destino de la conexión con el modo para activar la confirmación del certificado del servidor por parte del Cliente VPN activado, y se muestra un mensaje preguntando si se desea registrar como servidor el certificado individual. Si el usuario selecciona "Sí", a partir de la próxima vez que se conecte al Servidor VPN, el certificado utilizado para conectarse la primera vez podrá utilizarse como certificado individual del servidor.

## AUTENTICACIÓN DE CERTIFICADOS FIRMADOS POR EL SERVIDOR

La autenticación de certificados firmados por el servidor es el método de autenticación por el cual el ordenador cliente VPN que realiza la conexión VPN dispone de una lista o certificados raíz (o certificados intermedios) fiables y se permite que la conexión continúe si el certificado presentado por el Servidor VPN de destino de la conexión está firmado por uno de los certificados fiables.

Si hay varios servidores VPN en la empresa o si se espera que el número aumente en el futuro, el certificado del servidor de cada servidor VPN estará firmado por el certificado raíz de la empresa y, al establecer que el certificado raíz es fiable, los clientes que intenten conectarse a la red VPN podrán seguir conectándose si el certificado presentado por el servidor VPN de destino de la conexión está firmado por uno de los certificados de confianza.