Contenido

Introducción

Este documento describe cómo:

- cree un pedido de firma de certificado (CSR) en el módulo de Secure Socket Layer (el SSLM)
- importe el certificado usando el cortar y pegar en el formato del Privacy Enhanced Mail (PEM)

prerrequisitos

Antes de que usted comience, usted necesita conocer el Domain Name que se asigna al certificado. Usted también necesita el certificado raíz de las autoridades de los Certificados (CA), y posiblemente el certificado del intermedio de CA.

Requisitos

Antes de utilizar esta configuración, asegúrese de que cumple con estos requisitos:

- Certificado raíz de CA; posiblemente el certificado raíz intermedio
- Domain Name para el certificado
- información

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- versión 2.1(2)
- Certificado de prueba de Verisign

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Tarea principal

Tarea

Esta sección detalla cada paso necesario para crear el CSR, de la creación del par clave a importar el certificado de servidor.

Instrucciones Paso a Paso

Complete las instrucciones en esta sección.

1. Cree el par clave.`nov10-key` es el nombre del par clave.**Nota:** Esté seguro de especificar **exportable**; si no, usted no puede exportar el par clave del SSLM.`ssl-proxy(config)#`**`crypto key generate rsa general-keys label nov10-key exportable`**`The name for the keys will be: nov10-keyChoose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.How many bits in the modulus [512]: `**`1024`**`% Generating 1024 bit RSA keys ...[OK]`
2. Cree el trustpoint.El nombre del trustpoint es yoursite. Usted necesita ingresar el asunto en el formato X.509 y su Domain Name. Esta información se utiliza para crear el CSR.`ssl-proxy(config)#`**`crypto ca trustpoint yoursite`**`ssl-proxy(ca-trustpoint)#`**`enrollment terminal pem`**`ssl-proxy(ca-trustpoint)#`**`crl optional`**`ssl-proxy(ca-trustpoint)#`**`subject-name C=US, ST=Massachusetts, L=Boxborough, O=Cisco, OU=Tac, CN=www.yourdomain.com`**`ssl-proxy(ca-trustpoint)#`**`fqdn www.yourdomain.com`**`ssl-proxy(ca-trustpoint)#`**`rsakeypair nov10-key`**`ssl-proxy(ca-trustpoint)#`**`exit`**
3. Genere el CSR.`ssl-proxy(config)#`**`crypto ca enroll yoursite`**`% Start certificate enrollment .. % The subject name in the certificate will be: C=US, ST=Massachusetts, L=Boxborough, O=Cisco, OU=Tac, CN=www.yourdomain.com% The fully-qualified domain name in the certificate will be: www.yourdomain.com% The subject name in the certificate will be: www.yourdomain.com% Include the router serial number in the subject name? [yes/no]: no% Include an IP address in the subject name? [no]: noDisplay Certificate Request to terminal? [yes/no]: `**`yes`**`Certificate Request follows:-----BEGIN CERTIFICATE REQUEST-----`
   `MIIB+jCCAWMCAQAwgZgxGzAZBgNVBAMTEnd3dy55b3VyZG9tYWluLmNvbTEMMAoGA1UECxMDVGFjMQ4wDAYDVQQKEwVDaXNjbzETMBEGA1UEBxMKQm94Ym9yb3VnaDEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czELMAkGA1UEBhMCVVMxITAfBgkqhkiG9w0BCQIWEnd3dy55b3VyZG9tYWluLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwwCQrKH+RYvhQpZuuVADHAh4BoFRefiV+b6UXXI8dOmnkKB/w1w+Hure4N6pQsBPMEg1mku5AT38JcrWKu8JfGVEEap54UX+ZGs4o37sskL4vr0qeNQ0PxkIVE44iZLb+KxS5XbGrNRN6Mx4A8npV8xe1Wew8TqNw2h+oNYEBcCAwEAAaAhMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBBAUAA4GBAKjWSeLVzYdRSIkEL+rrYeuJfpoQTPIgTyjLNeI1a/ipoA/cQYPR0RBQ3N1k8G2JhXhWDe4hNDsYPtnPZ65kUSjLLV6BenxKjXzIDhdc2x8MyhMu5t/tAbxelG3daJGhHUBdOf5meQ4JrbfwZHATmoiTEpAbWVNHC2h7oJO5Ldhw-----END CERTIFICATE REQUEST--------End - This line not part of the certificate request---Redisplay enrollment request? [yes/no]: no`
4. Envíe el CSR a su CA.Utilice la copia y pegúela para enviar el CSR a su CA. Si su CA pide un tipo de servidor, seleccione Apache.
5. Cargue el certificado raíz de CAAntes de que usted pueda cargar el certificado de servidor, usted debe cargar cualquier Certificados de CA. Al mínimo, esto es el certificado raíz de CA, y posiblemente un certificado del intermedio de CA. Su CA puede proveer de usted los Certificados necesarios.`ssl-proxy(config)#`**`crypto ca authenticate yoursite`**`Enter the base 64 encoded CA certificate.End with a blank line or the word "quit" on a line by itself`**`-----BEGIN CERTIFICATE-----`**
   `MIICTTCCAfcCEFKp9CTaZ0ydr09TeFKr724wDQYJKoZIhvcNAQEEBQAwgakxFjAUBgNVBAoTDVZlcmlTaWduLCBJbmMxRzBFBgNVBAsTPnd3dy52ZXJpc2lnbi5jb20vcmVwb3NpdG9yeS9UZXN0Q1BTIEluY29ycC4gQnkgUmVmLiBMaWFiLiBMVEQuMUYwRAYDVQQLEz1Gb3IgVmVyaVNpZ24gYXV0aG9yaXplZCB0ZXN0aW5nIG9ubHkuIE5vIGFzc3VyYW5jZXMgKEMpYlMxOTk3MB4XDTk4MDYwNzAwMDAwMFoXDTA2MDYwNjIzNTk1OVowgakxFjAUBgNVBAoTDVZlcmlTaWduLCBJbmMxRzBFBgNVBAsTPnd3dy52ZXJpc2lnbi5jb20vcmVwb3NpdG9yeS9UZXN0Q1BTIEluY29ycC4gQnkgUmVmLiBMaWFiLiBMVEQuMUYwRAYDVQQLEz1Gb3IgVmVyaVNpZ24gYXV`

```
0aG9yaXplZCB0ZXN0aW5nIG9ubHkuIE5vIGFzc3VyYW5jZXMgKEMpVlMxOTk3MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMak6x
ImJx44jMKcbkACy5/CyMA2fqXK4PlzTtCxRq5tFkDzne7scI8oFK/J+gFZNE3bjidDxf07O3JOYG9RGx8CAwEAATANBgkqhkiG9
w0BAQQFAANBAKWnR/KPNxCglpTP5nzbo+QCIkmsCPjTCMnvm7KcwDJguaEwkoi1gBSY9biJp9oK+cv1Yn3KuVM+YptcWXLfxxI=
-----END CERTIFICATE-----quitCertificate has the following attributes:Fingerprint: 40065311
FDB33E88 0A6F7DD1 4E229187 % Do you accept this certificate? [yes/no]: yesTrustpoint CA certificate
accepted.% Certificate successfully imported
```

6. Cargue el certificado de servidor.
```
ssl-proxy(config)#crypto ca import yoursite certificate % The
fully-qualified domain name in the certificate will be: www.yourdomain.comEnter the base 64 encoded
certificate.End with a blank line or the word "quit" on a line by itself-----BEGIN CERTIFICATE-----
MIIDNTCCAt+gAwIBAgIQAequL43ZqGWLN5H/5BzhGDANBgkqhkiG9w0BAQUFADCBqTEWMBQGA1UEChMNVmVyaVNpZ24sIEluYzF
HMEUGA1UECxM+d3d3LnZlcmlzaWduLmNvbS9yZXBvc2l0b3J5L1Rlc3RDUFMgSW5jb3JwLiBCeSBSZWYuIExpYWIuIExURC4xRj
BEBgNVBAsTPUZvciBWZXJpU2lnbiBhdXRob3JpemVkIHRlc3Rpbmcgb25seS4gTm8gYXNzdXJhbmNlcyAoQylWUzE5OTcwHhcNM
DQxMTEwMDAwMDAwWhcNMDQxMTI0MjM1OTU5WjB1MQswCQYDVQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czETMBEGA1UE
BxQKQm94Ym9yb3VnaDEOMAwGA1UEChQFQ2lzY28xDDAKBgNVBAsUA1RhYzEbMBkGA1UEAxQSd3d3LnlvdXJkb21haW4uY29tMIG
fMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDAJCsof5Fi+FClm65UAMcCHgGgVF5+JX5vpRdcjx06aeQoH/DXD4e6t7g3qlCwE
8wSDWaS7kBPfwlytYq7wl8ZUQRqnnhRf5kazijfuyyyQvi+vSp41DQ/GQhUTjiJktv4rFLldsas1E3ozHgDyelXzF7VZ7DxOo3D
aH6g1gQFwIDAQABo4HRMIHOMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEIGA1UdHwQ7MDkwN6A1oDOGMWh0dHA6Ly9jcmwudmVy
aXNpZ24uY29tL1NlY3VyZVNlcnZlclRlc3RpbmdDQS5jcmwwUQYDVR0gBEowSDBGBgpghkgBhvhFAQcVMDgwNgYIKwYBBQUHAgE
WKmh0dHA6Ly93d3cudmVyaXNpZ24uY29tL3JlcG9zaXRvcnkvVGVzdENQUzAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAw
IwDQYJKoZIhvcNAQEFBQADQQCbMUY/lyyp2jt6YxiZNEaFNFHPRU5kQZAY8X+IWnQ0tLfASd0nJ4wdaaeGpJSZQKbMdae3aunz5
5LCq8QsB0AH-----END CERTIFICATE-----quit% Router Certificate successfully imported
```

Certificados intermedios

Si usted tiene un certificado intermedio, usted necesita configurar dos trustpoints. Un trustpoint contiene el certificado raíz de CA solamente. Usted necesita solamente configurar la terminal PEM de la inscripción y el Listas de revocación de certificados (CRL) opcional. El segundo trustpoint contiene el certificado intermedio y el certificado de servidor. El segundo trustpoint es similar configurado al primer trustpoint, sin embargo, en vez del certificado raíz, utiliza el certificado intermedio.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Esta sección proporciona la información de Troubleshooting relevante a esta configuración.

Si usted se ejecuta en los problemas que cargan los Certificados, habilite el debugging con el **comando debug crypto pki transactions**.

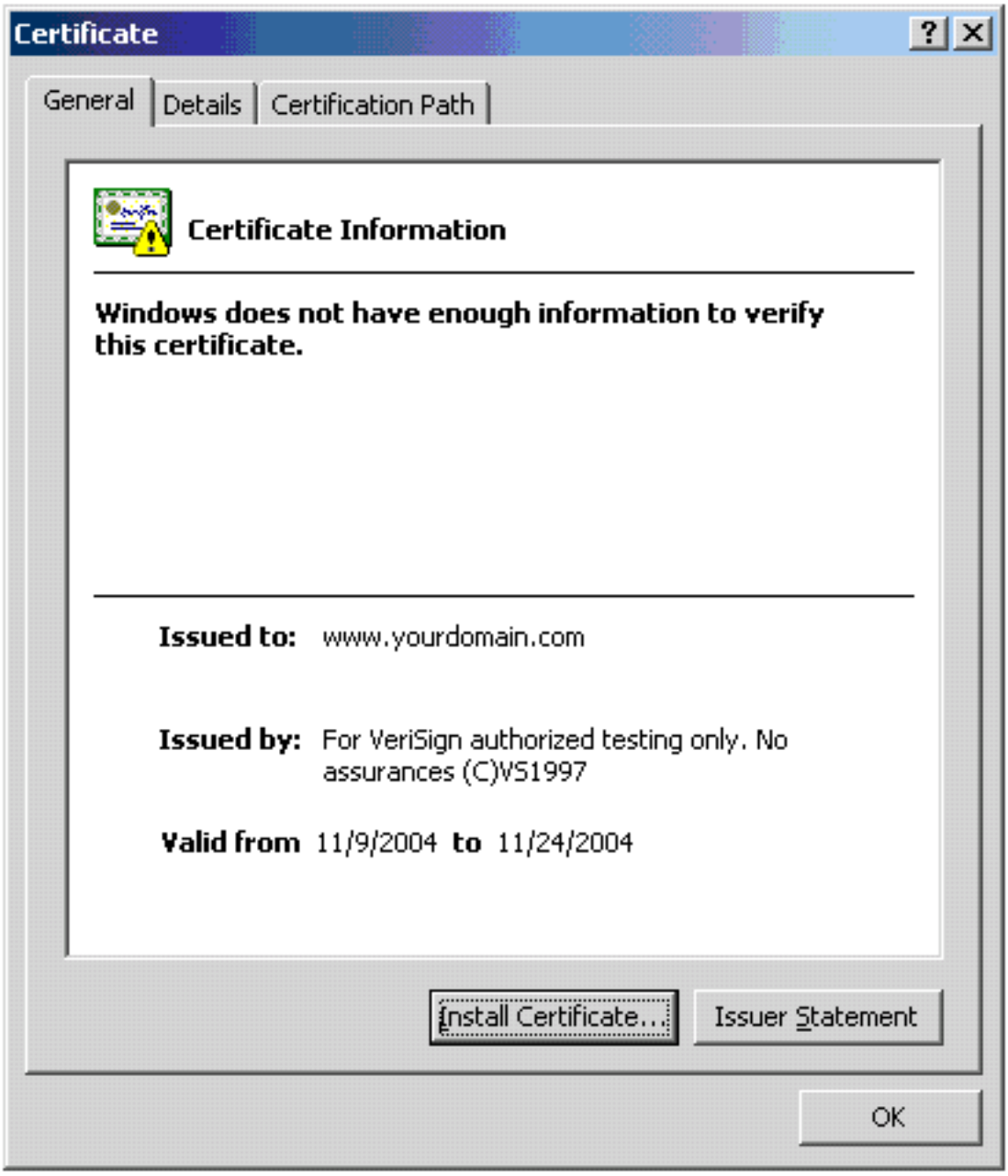
Aseegurese le tener la Cadena de certificados completa. Usted puede determinar esto viendo los Certificados en un PC. Salve los Certificados con una extensión de .cer, después doble el tecleo para abrirlos.

El certificado raíz se muestra en el cuadro 1. Usted puede determinar esto mirando **publicado a** y **publicado por las** secciones. Ambas secciones son lo mismo. También, observe que el certificado está apareciendo según lo no confiado en porque él un certificado de prueba.

Figura 1

El certificado de servidor se muestra en el cuadro 2. Usted llama determina que corresponde con el certificado raíz porque **publicado por la** sección corresponde con **publicado por la** sección en el certificado raíz.

Figura 2



Información Relacionada

- Instalación y nota de verificación del Catalyst 6500 Series SSL Services Module
- Nota de instalación y configuración del Catalyst 6500 Series SSL Services Module, 1.2
- Descargas - Software del módulo del Catalyst 6500/6000 (clientes registrados solamente)
- Release Note para el Software Release 2.x del módulo de servicios SSL del Catalyst 6500 Series Switch
- Guía de mensajes del sistema del Catalyst 6500 Series SSL Services Module, 2.1
- Referencia de comandos del Catalyst 6500 Series SSL Services Module, 2.1
- Soporte Técnico y Documentación - Cisco Systems