Sinal unificado da empresa do Contact Center único (UCCE) nos Certificados (SSO) e na configuração

Índice

Introdução

Este documento descreve as configurações do certificado que são exigidas para UCCE SSO. A configuração desta característica envolve diversos Certificados para o HTTPS, a assinatura digital e a criptografia.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Liberação 11.5 UCCE
- Microsoft ative directory (AD) - AD instalado em Windows Server
- Versão 2.0/3.0 do serviço da federação do diretório ativo (ADFS)

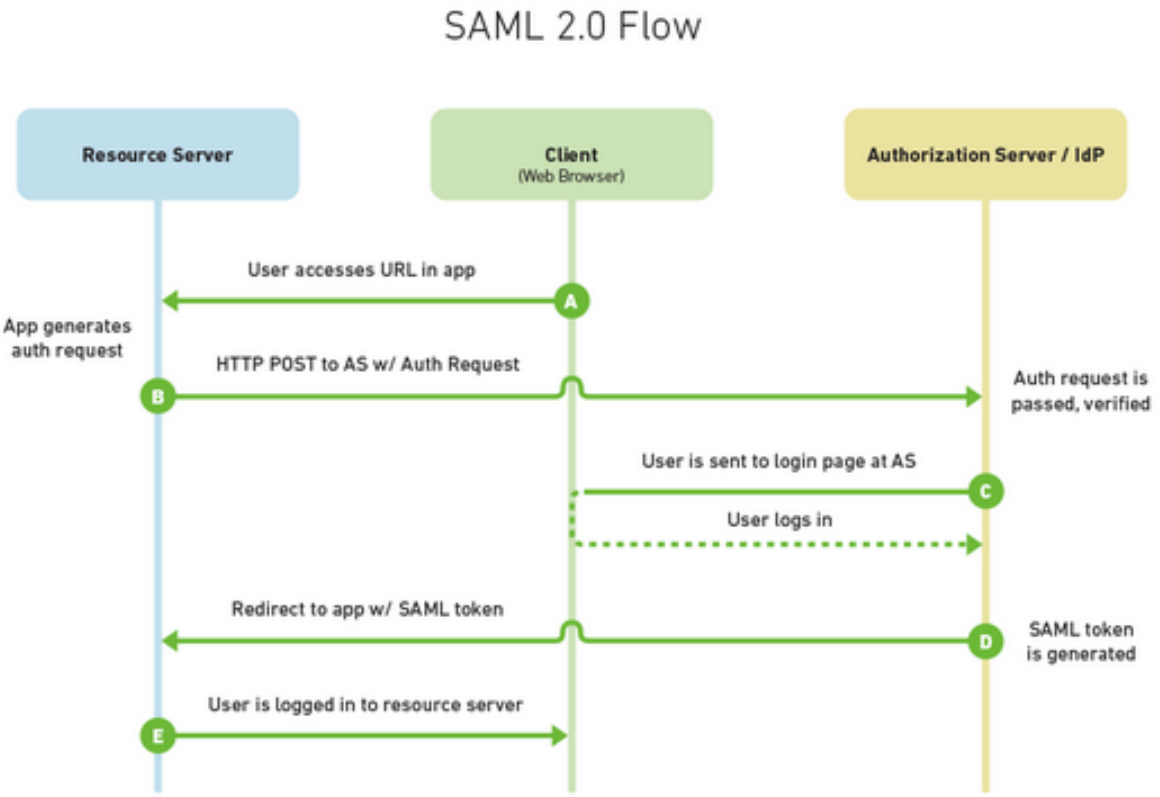
Componentes Utilizados

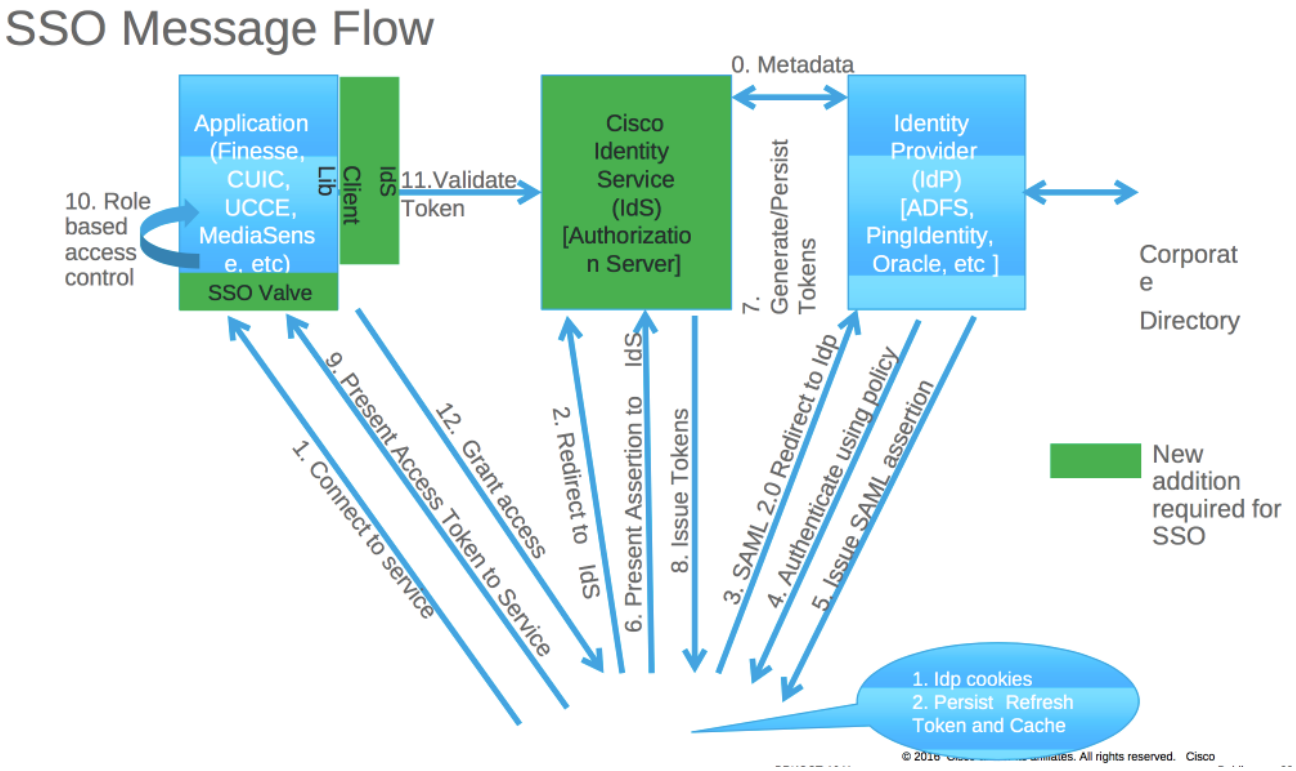
UCCE 11.5

Windows 2012 R2

Parte A. SSO Fluxo de mensagem

The most common SAML flow is shown below:



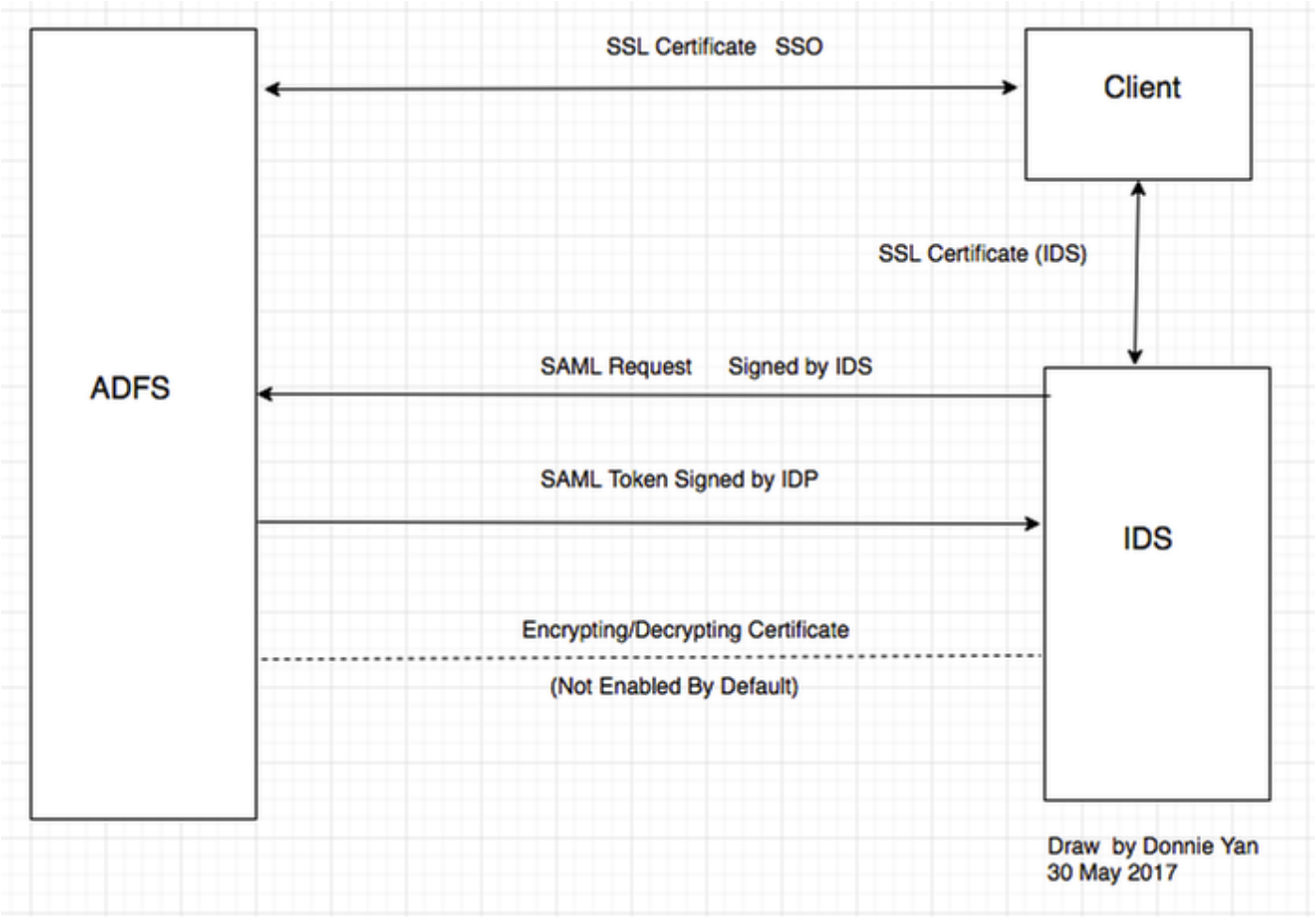


Quando o SSO estiver permitido, quando o agente entrar ao desktop da fineza:

- O server da fineza reorienta o navegador do agente para comunicar-se com o serviço da identidade (o IDS)
- O IDS reorienta o navegador do agente ao fornecedor da identidade (IDP) com pedido de SAML
- IDP gerencie o token de SAML e passa-o ao servidor IDS

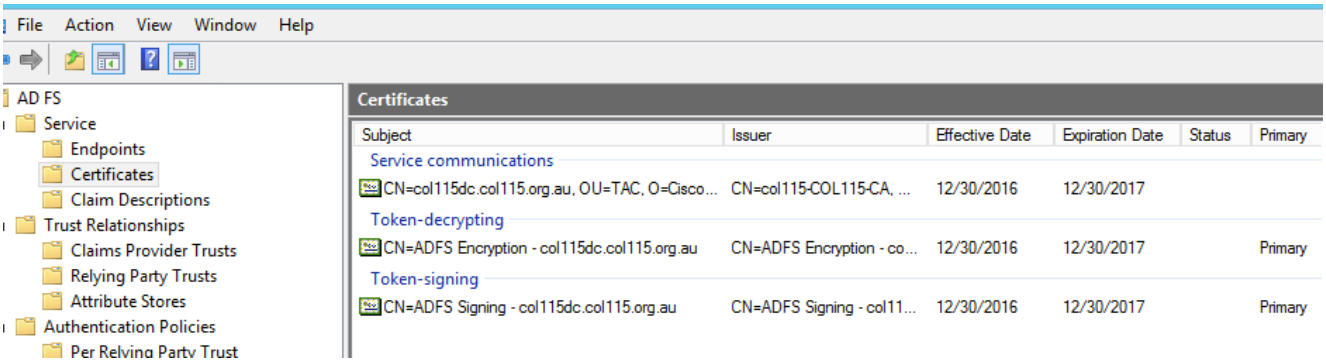
- Quando o token esteve gerado, cada vez que o agente consulta ao ppplication, usa este token válido para o início de uma sessão

Parte B. Certificados Used em IDP e em IDS



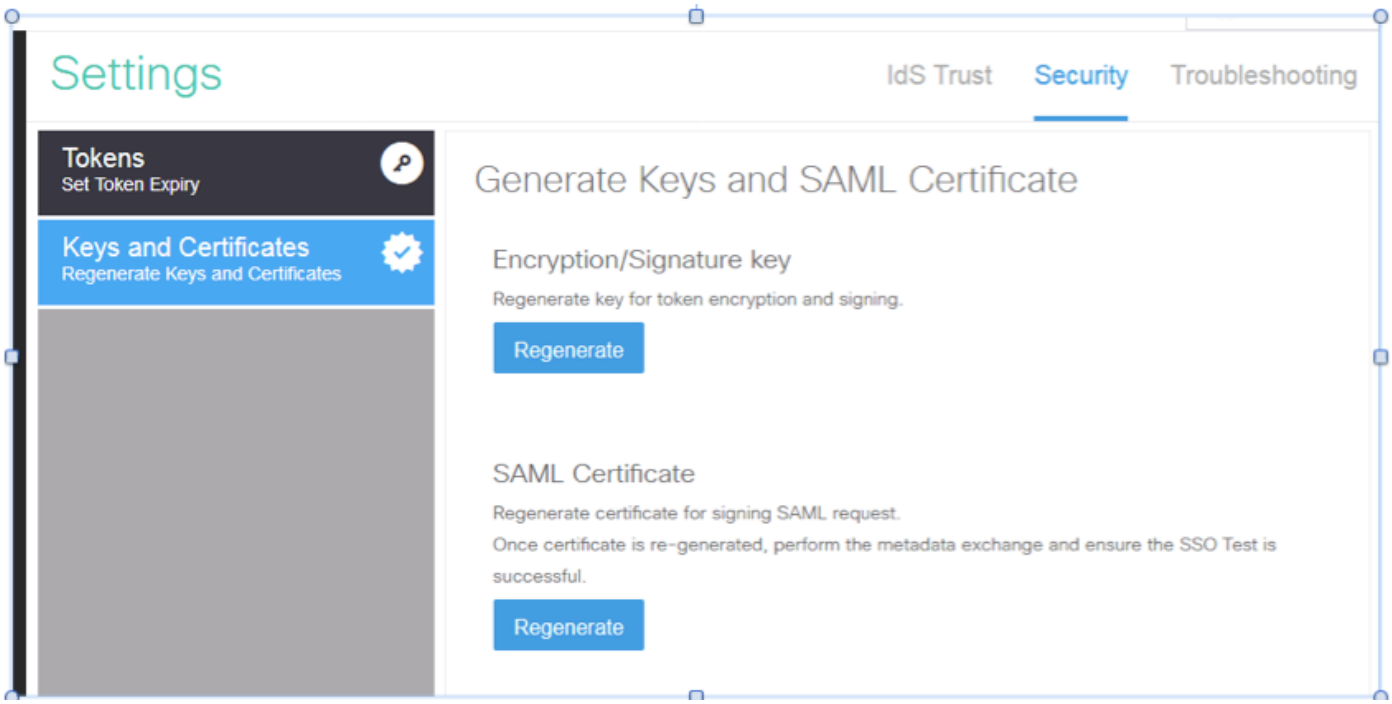
Certificados IDP

- Certificado SSL (SSO)
- Certificado de assinatura simbólico
- Token – decifrando

1. 

Certificados IDS

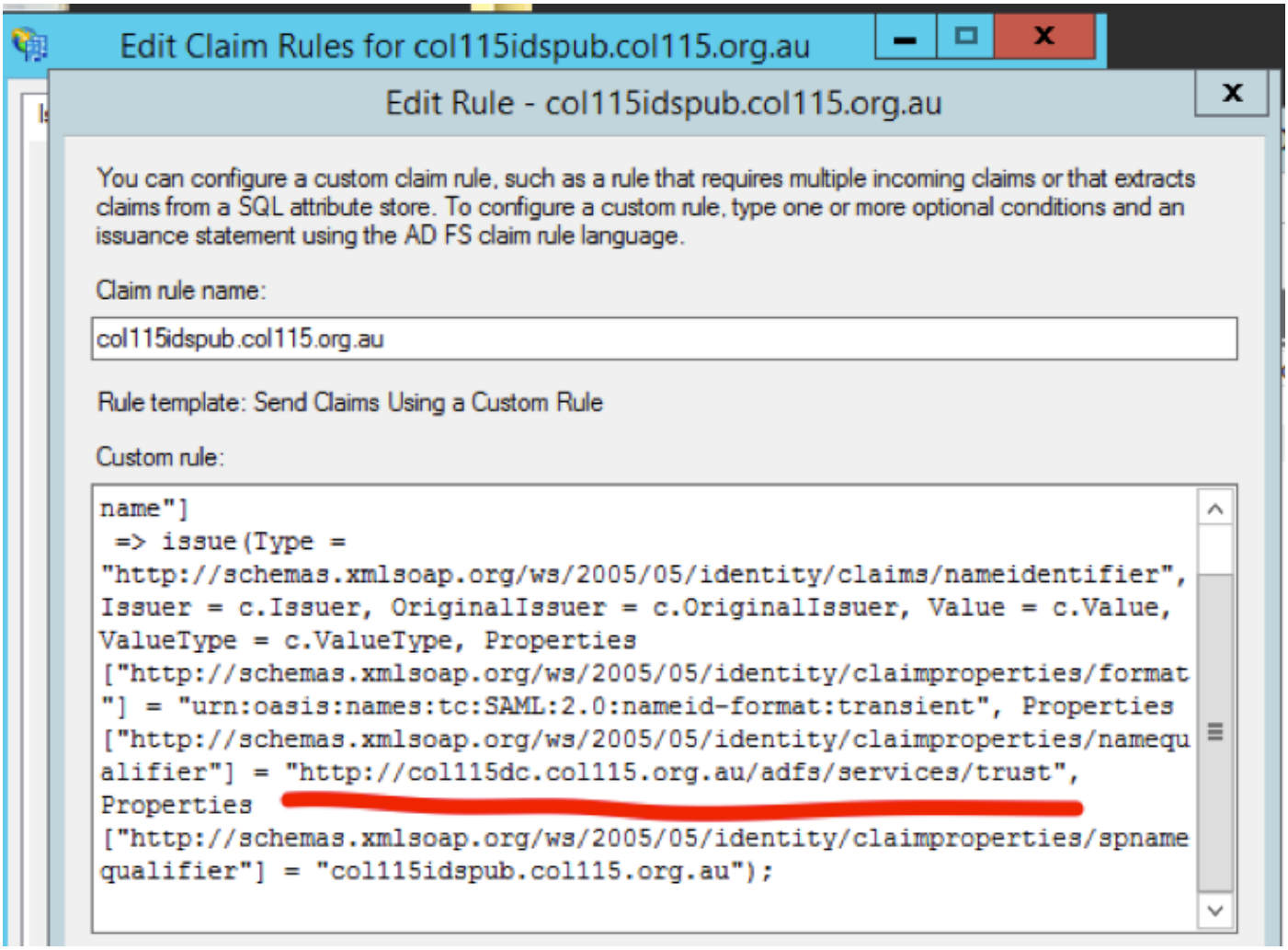
- Certificado de SAML
- Chave da assinatura
- Chave de criptografia



Parte C. IDP Certificação em detalhe e configuração

Certificado SSL (SSO)

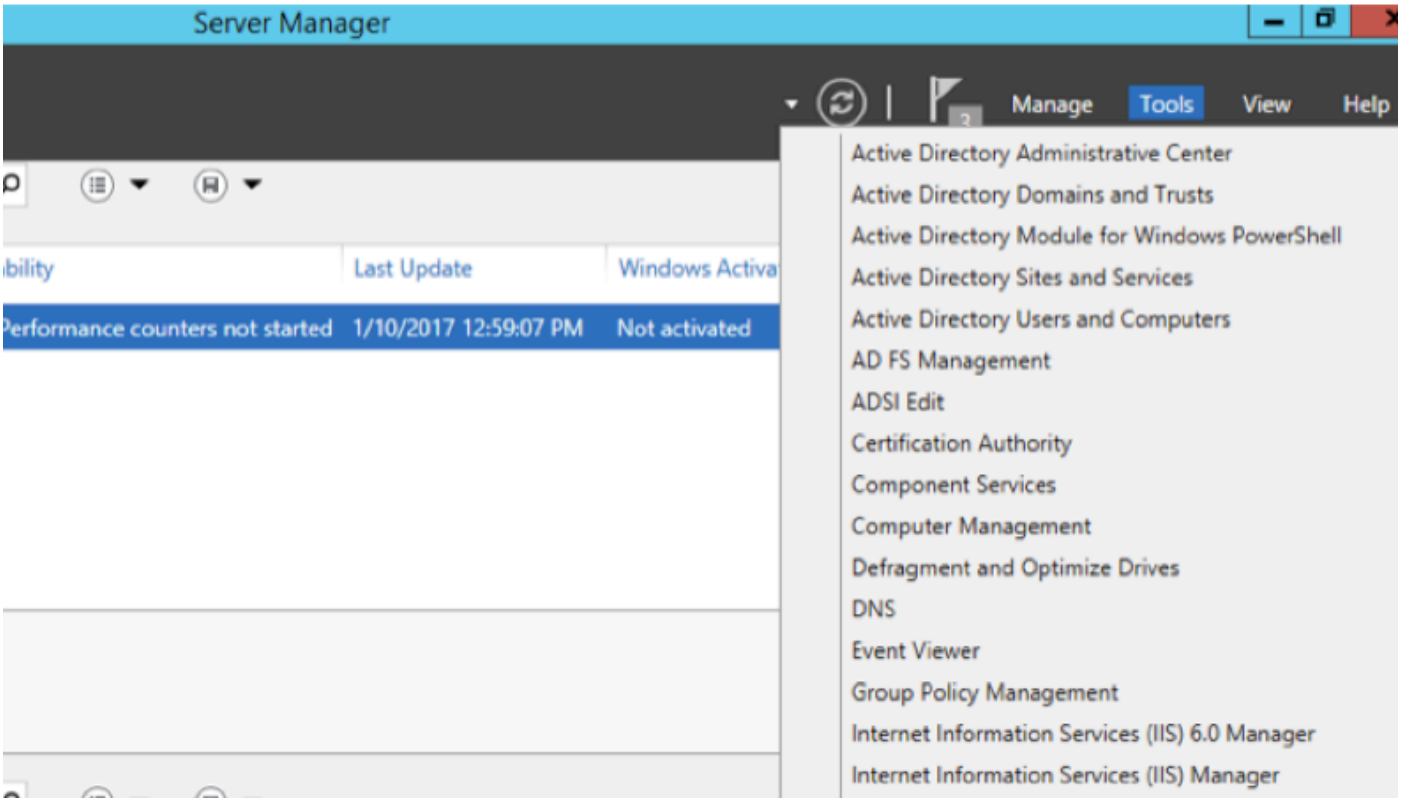
- Este certificado é usado entre IDP e cliente. O cliente deve confiar o certificado SSO
- O certificado SSL é colocado para cifrar a sessão entre o cliente e o server IDP. Este certificado não é específico a ADFS, mas a específico ao IIS
- O assunto do certificado SSL deve combinar com o nome usado na configuração ADFS

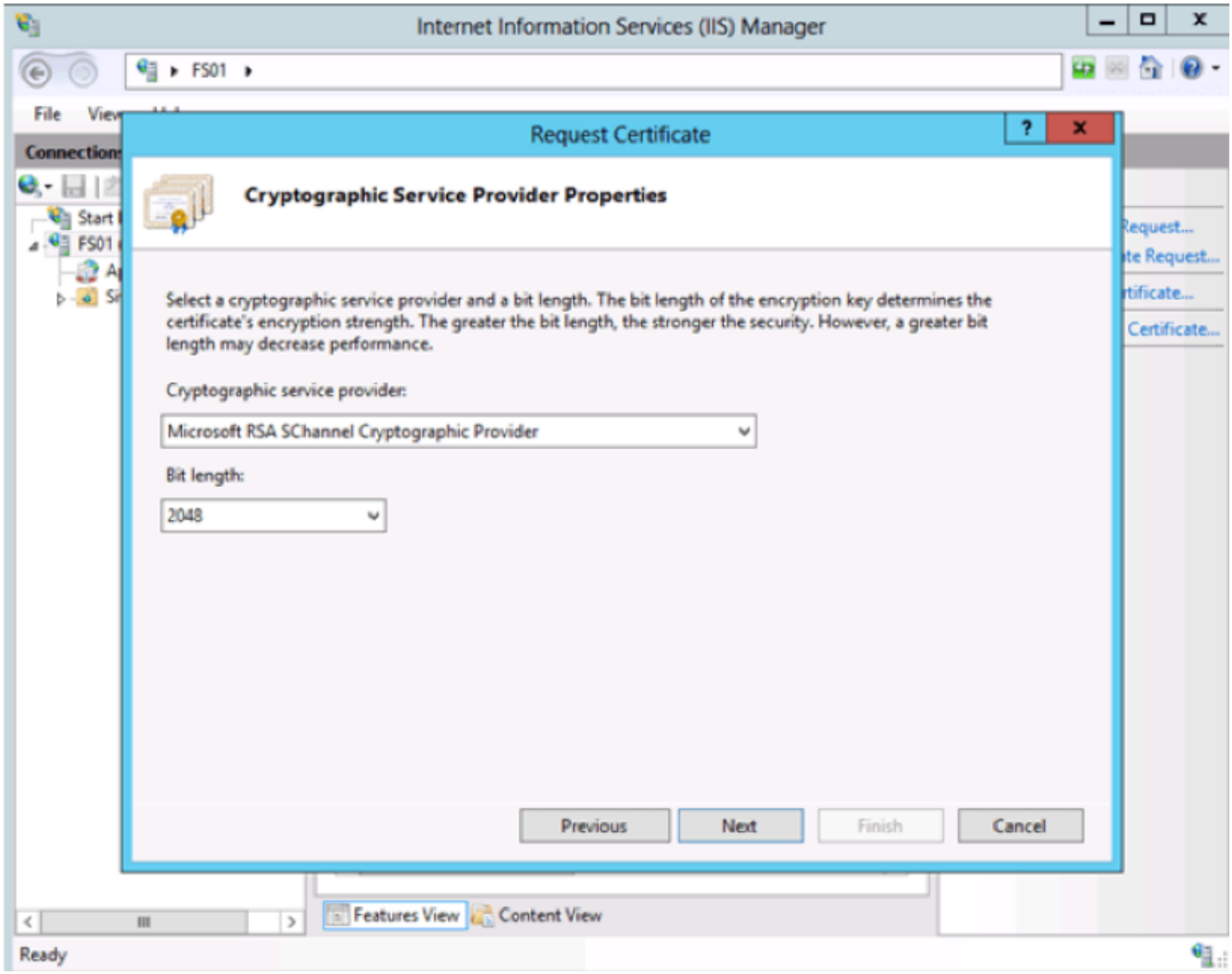


Etapas para configurar o certificado SSL para o SSO (o laboratório local com CA interno assinou)

Etapa 1. Crie o certificado SSL com a solicitação de assinatura de certificado (CSR) e o sinal por CA interno para ADFS.

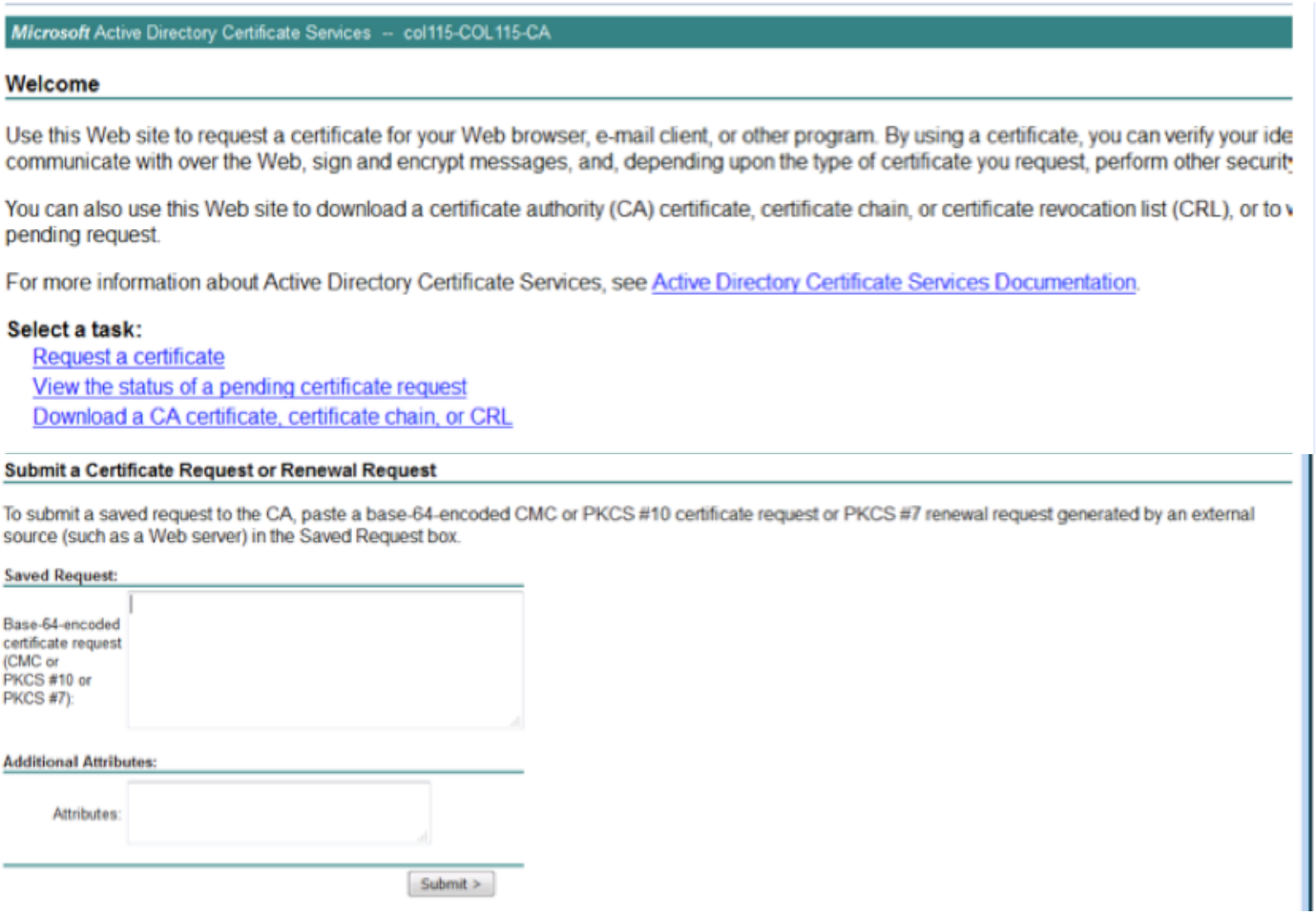
1. Abra o gerenciador do servidor.
2. Clique ferramentas.
3. Clique o gerente do Internet Information Services (IIS).
4. Selecione o servidor local.
5. Selecione certificados de servidor.
6. Clique a característica aberta (painel da ação).
7. O clique **cria o** pedido do certificado.
8. Deixe o provedor de serviços criptograficamente no padrão.
9. Mude o **comprimento de bit a 2048**.
10. Clique em Next.
11. Selecione um lugar para salvar os arquivos solicitados.
12. Clique em Finish.





Etapa 2. CA assina o CSR que foi gerado de etapa 1.

1. **Abra o** server de CA para cantar este **HTTP** CSR**: Endereço IP de Um ou Mais Servidores Cisco ICM NT >/certsrv/do server <CA**.
2. Pedido do clique um certificado.
3. Pedido do certificado avançado do clique.
4. **Copie o** CSR no pedido do certificado codificado Based-64.
5. **Submeta**.
6. Transfira o certificado assinado.



Etapa 3. Instale o certificado assinado de volta ao server ADFS e atribua-o à característica ADFS.

1. Instale o certificado assinado de volta ao server ADFS. A fim fazer isto, **abra a informação de Internet Services(IIS) Manager> do manager>Tools>Click do server**.

Característica local de Server>Server Certificate>Open (painel da ação).

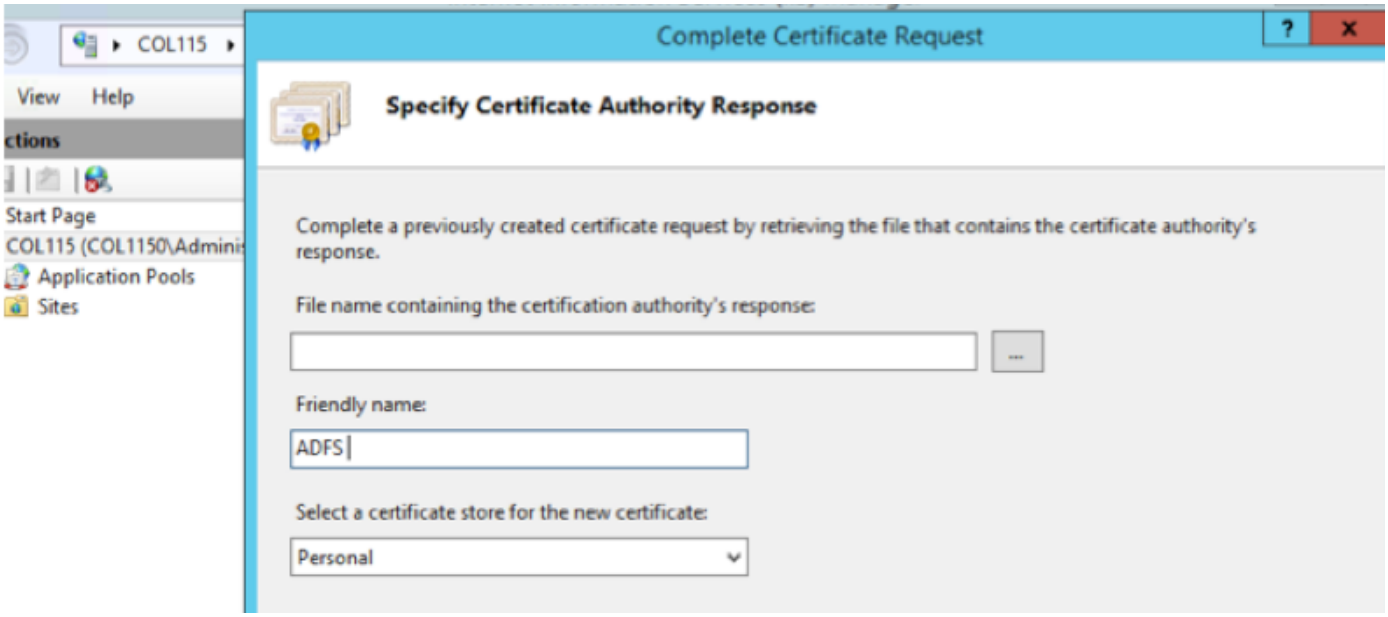
2. Pedido do certificado completo do clique.

3. Selecione o trajeto ao arquivo completo CSR que você terminou e transferiu do fornecedor do certificado da terceira parte.

4. **Dê entrada com o** nome amigável para o certificado.

5. Selecione pessoal como a loja do certificado.

6. Clique em **OK**.



7. Nesta fase, todo o certificado foi adicionado. Agora, a atribuição do certificado SSL é exigida.

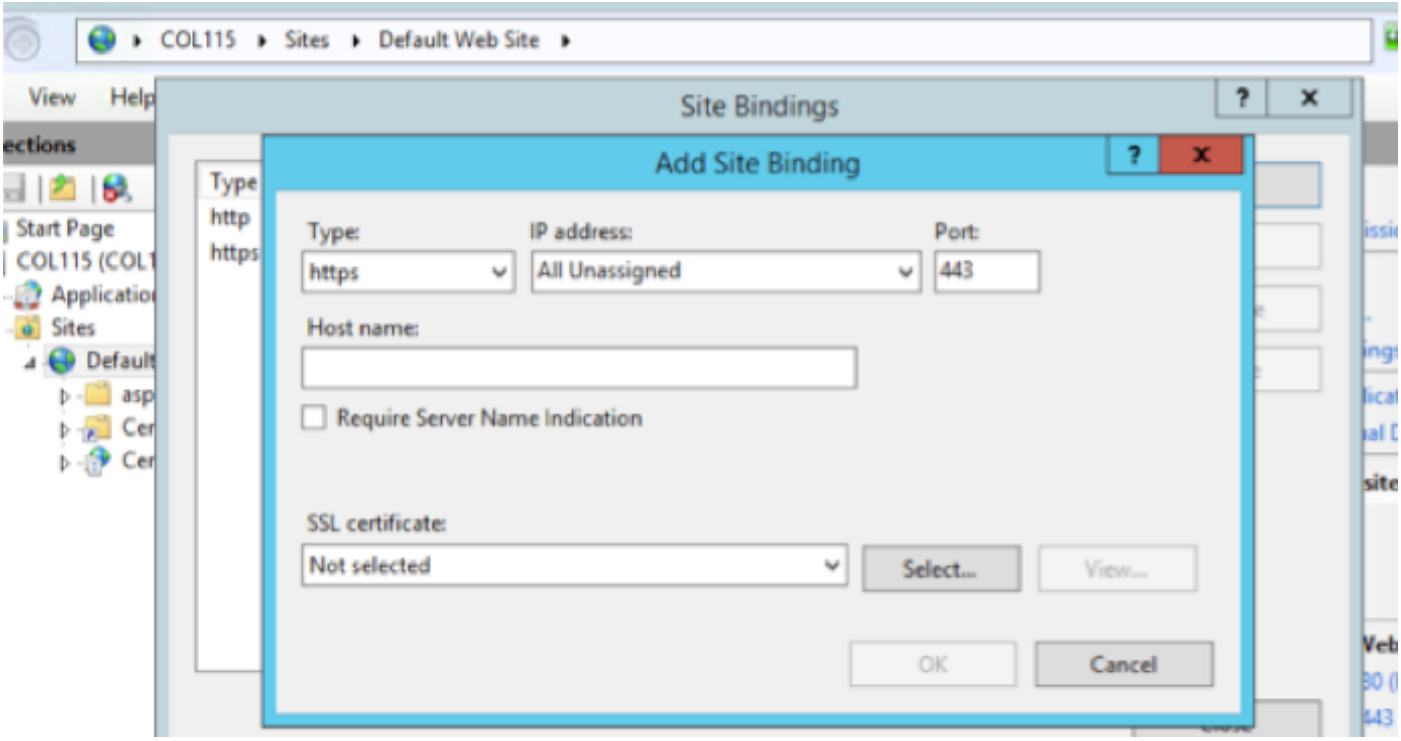
8. **Expanda os emperramentos locais do >Click da website padrão de Sites>Select do server>Expand** (placa das ações).

9.Click **adicionam**.

10. **Mude o** tipo ao HTTPS.

11. Selecione seu certificado do menu de gota para baixo.

12. Clique em **OK**.



Agora, o certificado SSL para o server ADFS foi atribuído.

Nota: Durante a instalação da característica ADFS, o certificado precedente SSL deve ser

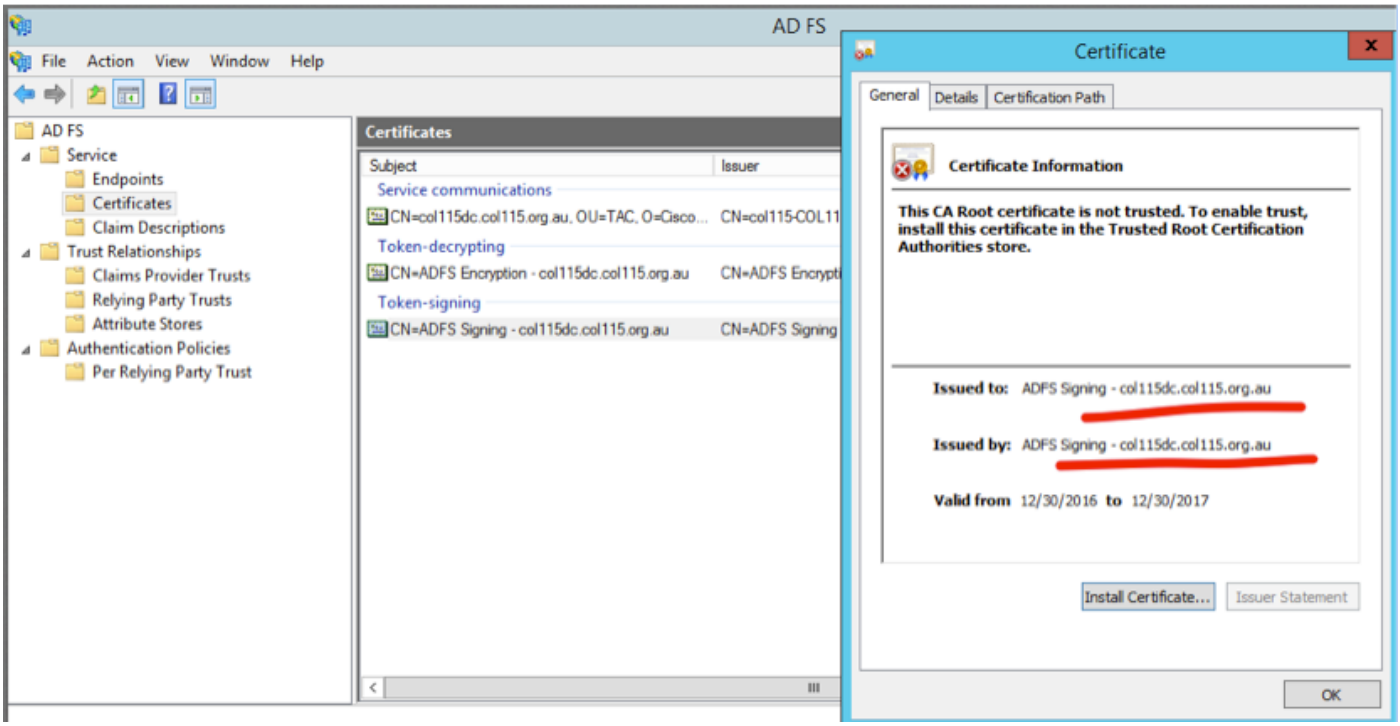
usado.

Certificado de assinatura simbólico

ADFS gerencie o certificado auto-assinado para o certificado de assinatura simbólico. À revelia é válido por um ano.

O token de SAML gerado por IDP é chamuscado pela chave privada ADFS (parte privada de assinatura simbólica do certificado). Então, o IDS usa a chave pública ADFS para verificar. Isto garante que o token assinado não é obter alterado.

O certificado de assinatura simbólico é usado todas as vezes que um usuário precisa de aceder a um aplicativo de confiança do partido (Cisco IDS).

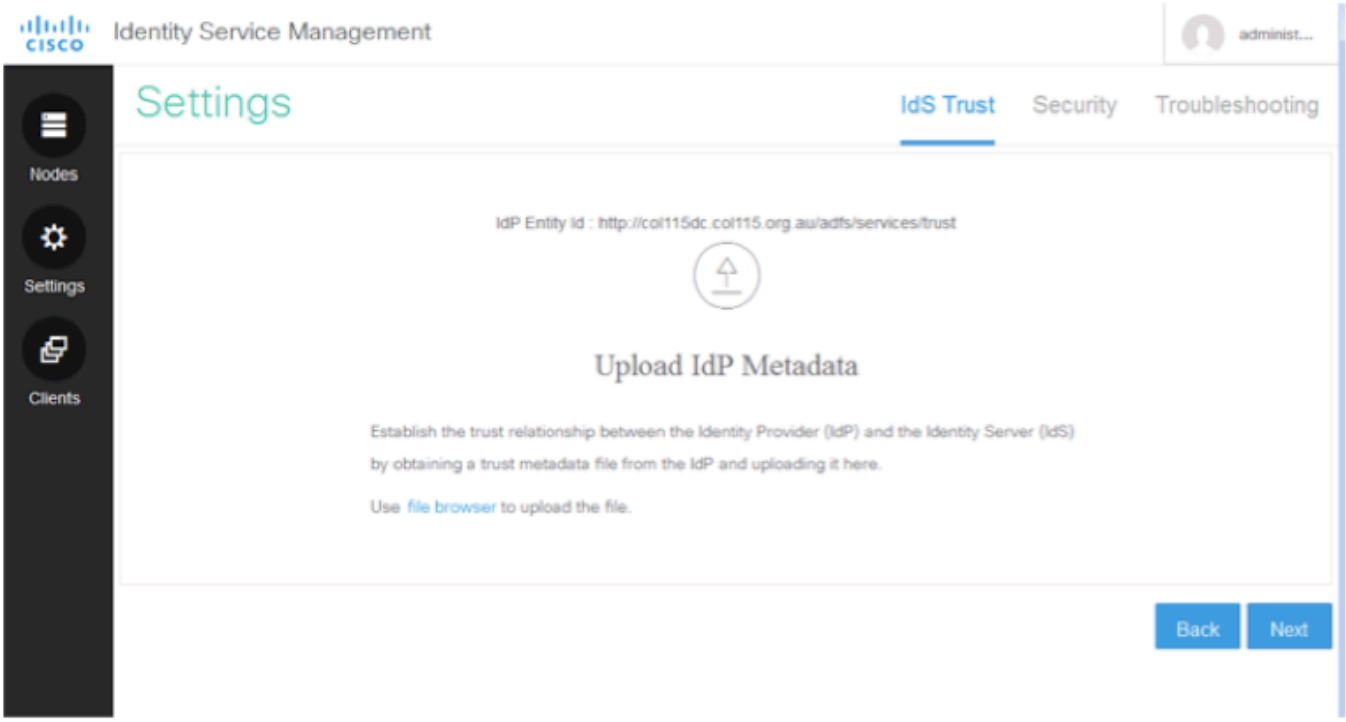


Como o server do Cisco IDS obtém a chave pública do certificado simbólico do canto?

Isto é feito transferindo arquivos pela rede metadata ADFS ao servidor IDS, e então passando a chave pública de ADFS ao servidor IDS. Desta maneira, o IDS ganha a chave pública do server ADFS.

Você precisa **de transferir** metadata IDP de ADFS. A fim transferir metadata IDP, refira o link **https:// <FQDN de ADFS>/federationmetadata/2007-06/federationmetadata.xml**.

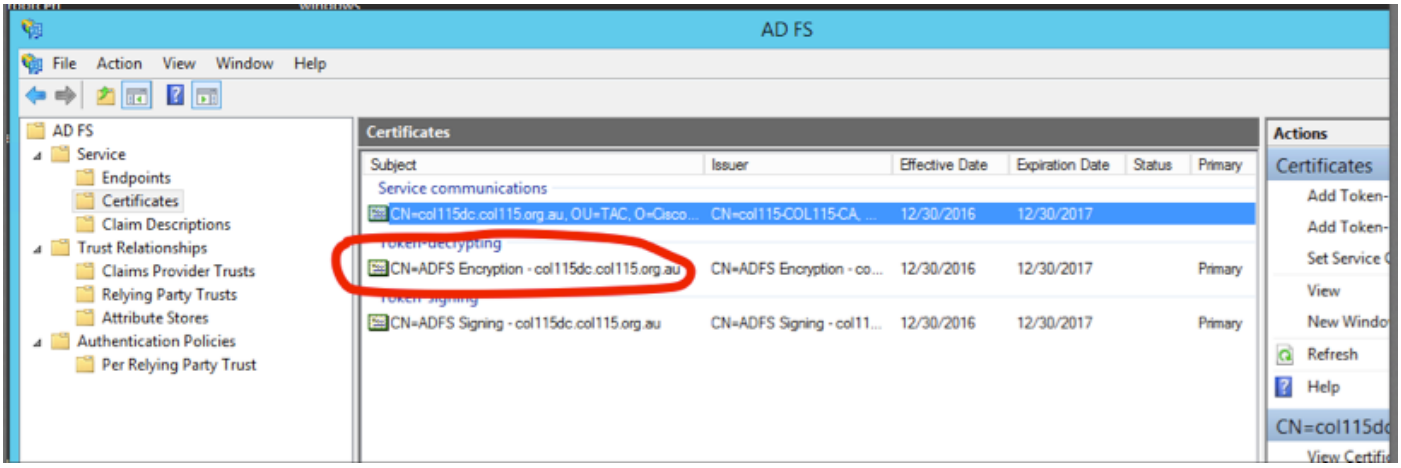
De ADFS os
Metadata



transferem arquivos pela rede Metadata ADFS ao IDS

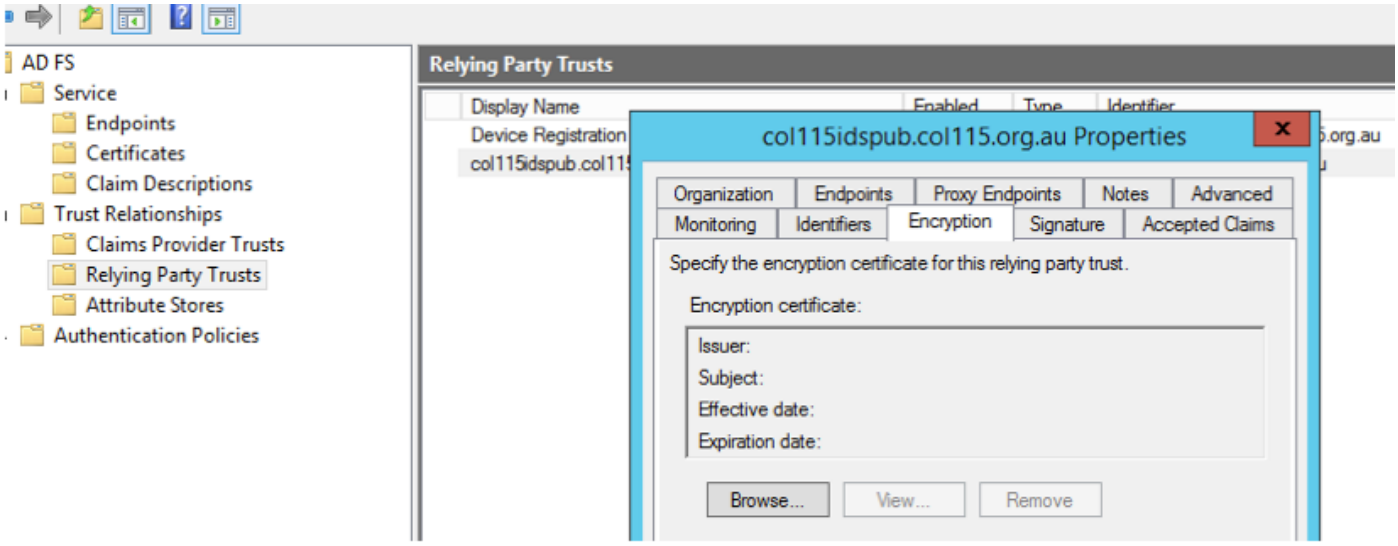
Descriptografia simbólica

Este certificado gerencie automaticamente pelo server ADFS (auto-assinado). Se o token precisa a criptografia, ADFS usa a chave pública IDS para decifrá-la. Mas, quando você vê o token-dcrypting ADFS, não significa que o token está cifrado.



Se você quer ver se a criptografia simbólica esteve permitida para um aplicativo de confiança específico do partido, você precisa de verificar a aba da criptografia em um aplicativo de confiança específico do partido.

Esta imagem mostra, a criptografia simbólica não foi permitida.



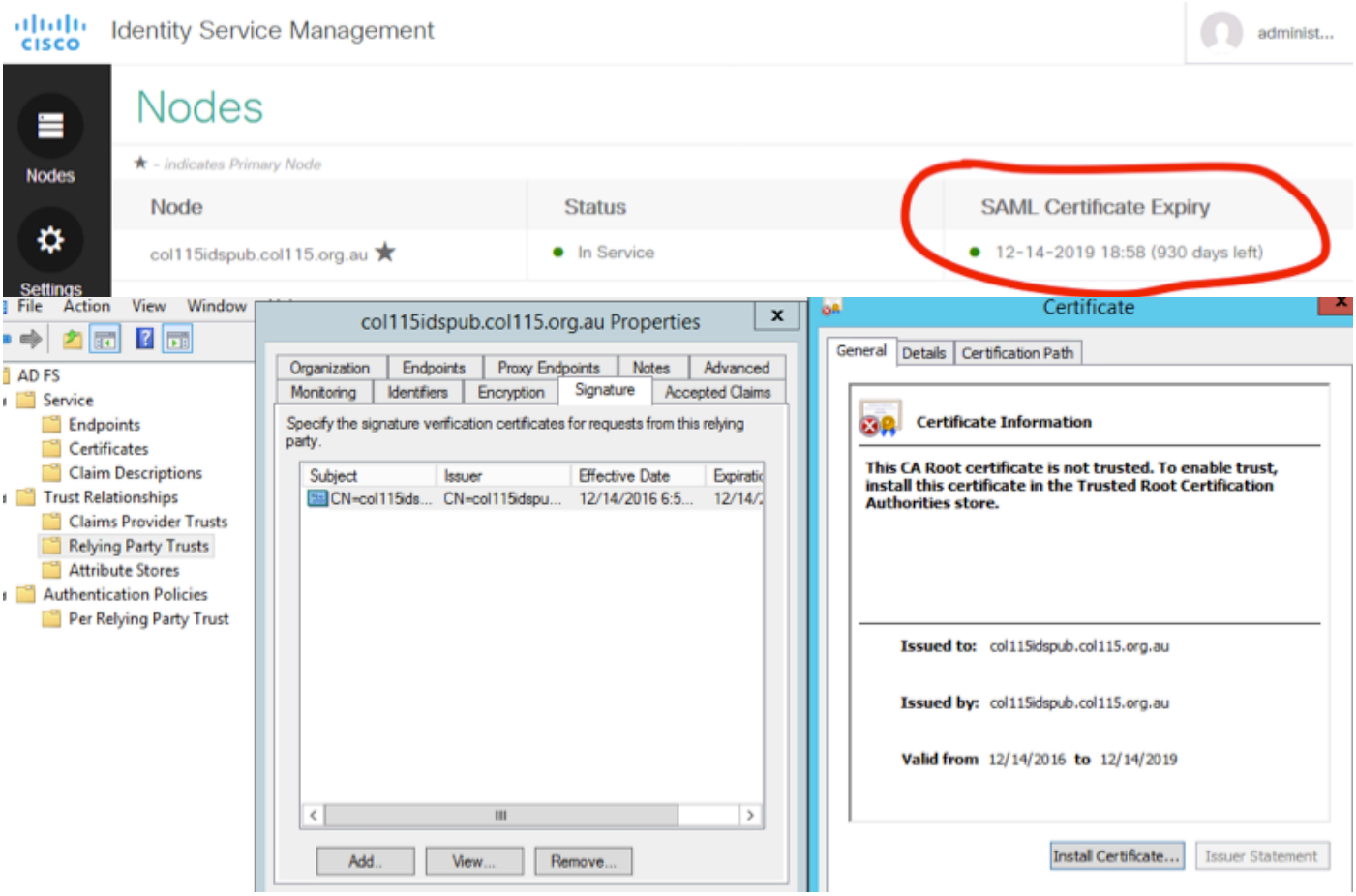
A criptografia não é permitida

Certificado do lado do Cisco IDS da parte D.

- Certificado de SAML
- Chave de criptografia
- Chave da assinatura

Certificado de SAML

Este certificado é gerado pelo servidor IDS (auto-assinado). À revelia é válido por 3 anos.

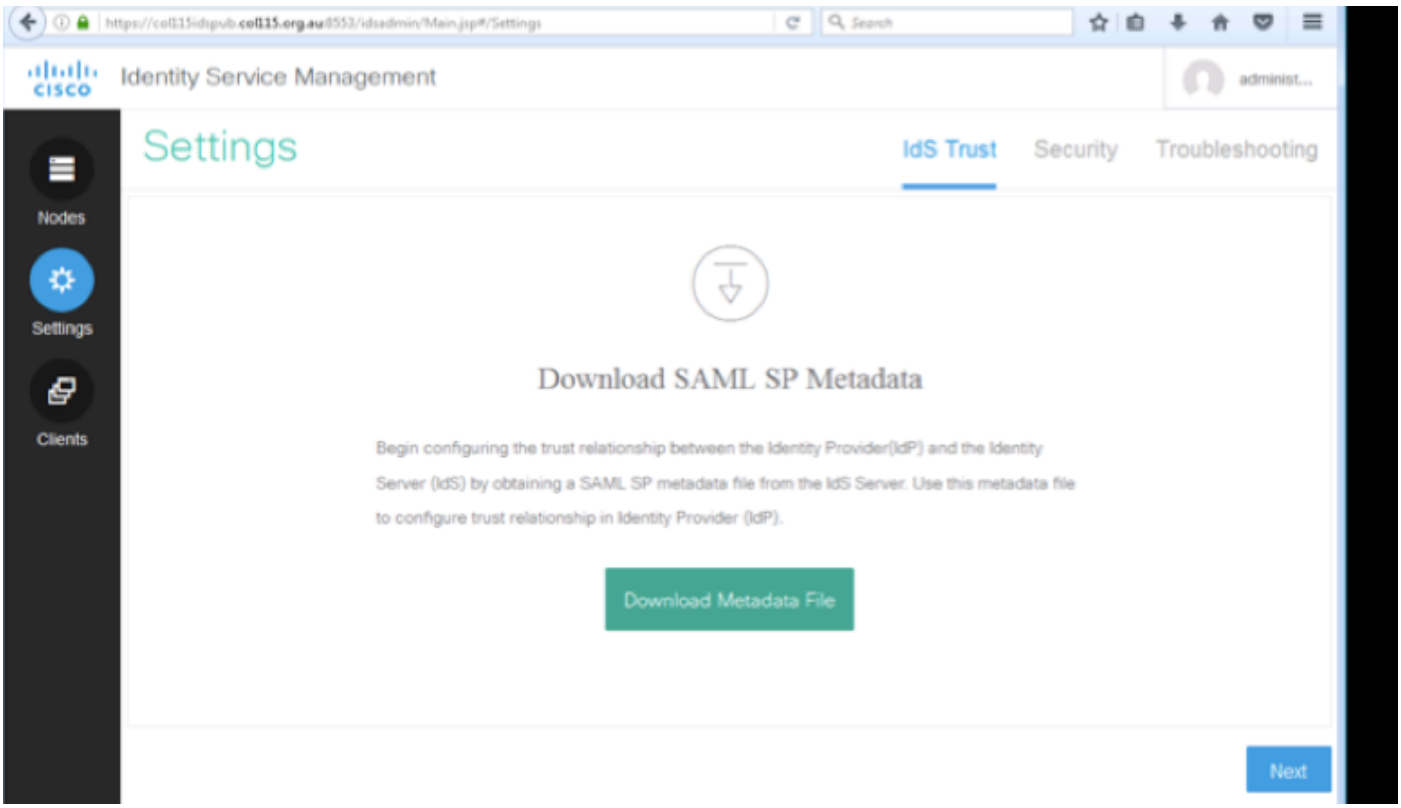


Este certificado é usado para assinar o pedido de SAML, e envia a IDP (ADFS). Esta chave pública está nos metadata IDS, e deve ser importada ao server ADFS.

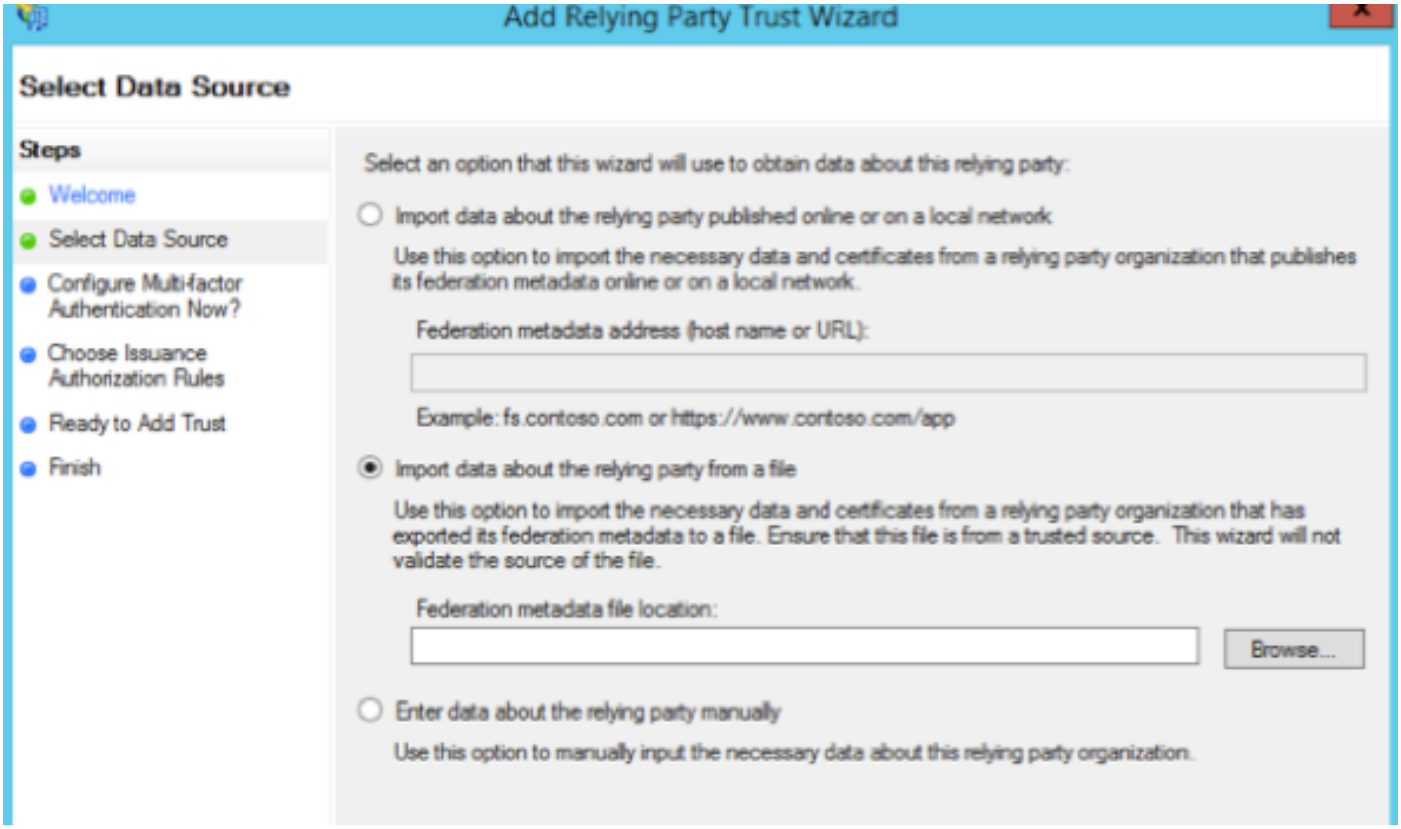
metadata 1.Download SAML SP do servidor IDS.

2. Broswer ao **server FQDN>:8553/idsadmin/ dos <ids de https://**.

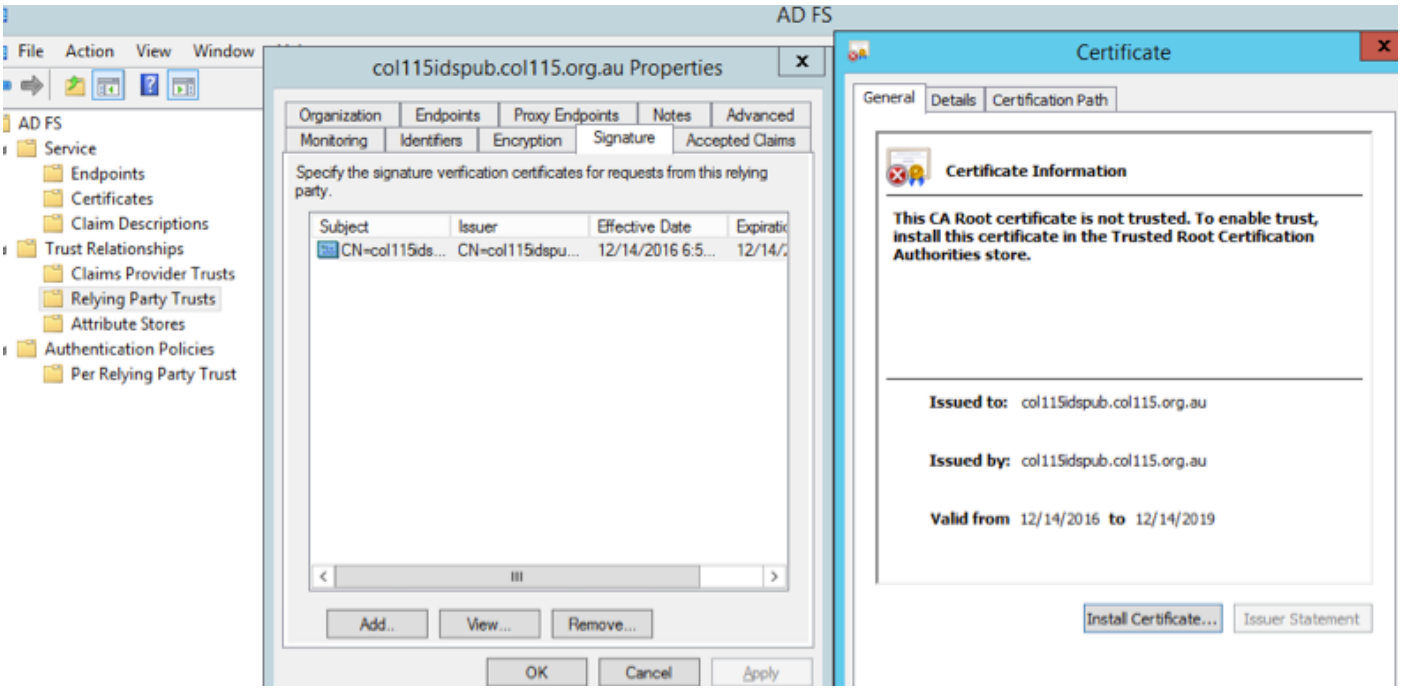
3. Selecione ajustes e metadata de SAML SP da transferência e **salvar** os.



Os Metadata da importação



do servidor IDS ao server ADFS

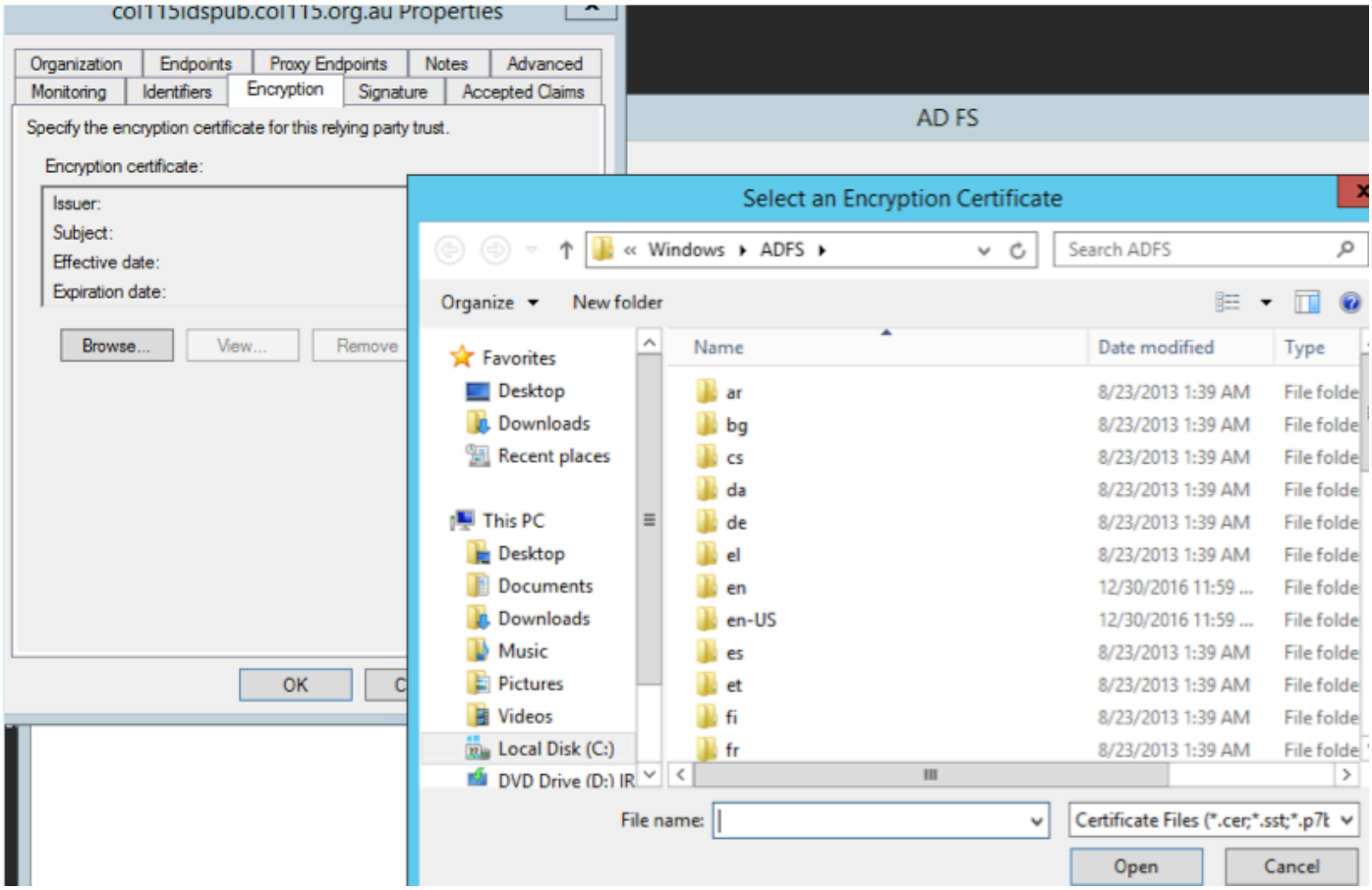


verificam do lado ADFS

Quando o IDS regenera o certificado- um de SAML está usado para assinar o pedido que de SAML executa a troca dos Metadata.

Criptografia/chave da assinatura

A criptografia não é permitida à revelia. Se a criptografia é permitida, precisa de ser transferida arquivos pela rede a ADFS.



Referecne:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-features-guide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf