

# Unified Contact Center Enterprise (UCCE) single aanmelding (SSO)-certificaten en -configuratie

## Inhoud

[Inleiding](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Deel A. SSO-berichtenstroom](#)

[Deel B. In IDP en IDS gebruikte certificaten](#)

[Deel C. IDP-certificering in detail en configuratie](#)

[SSL-certificaat \(SSO\)](#)

[Stappen om SSL-certificaat voor SSO te configureren \(lokaal lab met interne CA ondertekend\)](#)

[Token-signaalcertificaat](#)

[Hoe krijgt Cisco IDS-server de openbare sleutel van Token Signing Certificate?](#)

[Encryptie is NIET ingeschakeld](#)

[Deel D. Cisco IDS-zijcertificaat](#)

[SAML-certificaat](#)

## Inleiding

In dit document worden certificeringsconfiguraties beschreven die vereist zijn voor UCCE SSO. De configuratie van deze optie omvat verschillende certificaten voor HTTPS, digitale handtekeningen en encryptie.

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- UCS release 11.5
- Microsoft Active Directory (AD) - AD geïnstalleerd op Windows Server
- Active Directory Federation Service (ADFS) versie 2.0/3.0

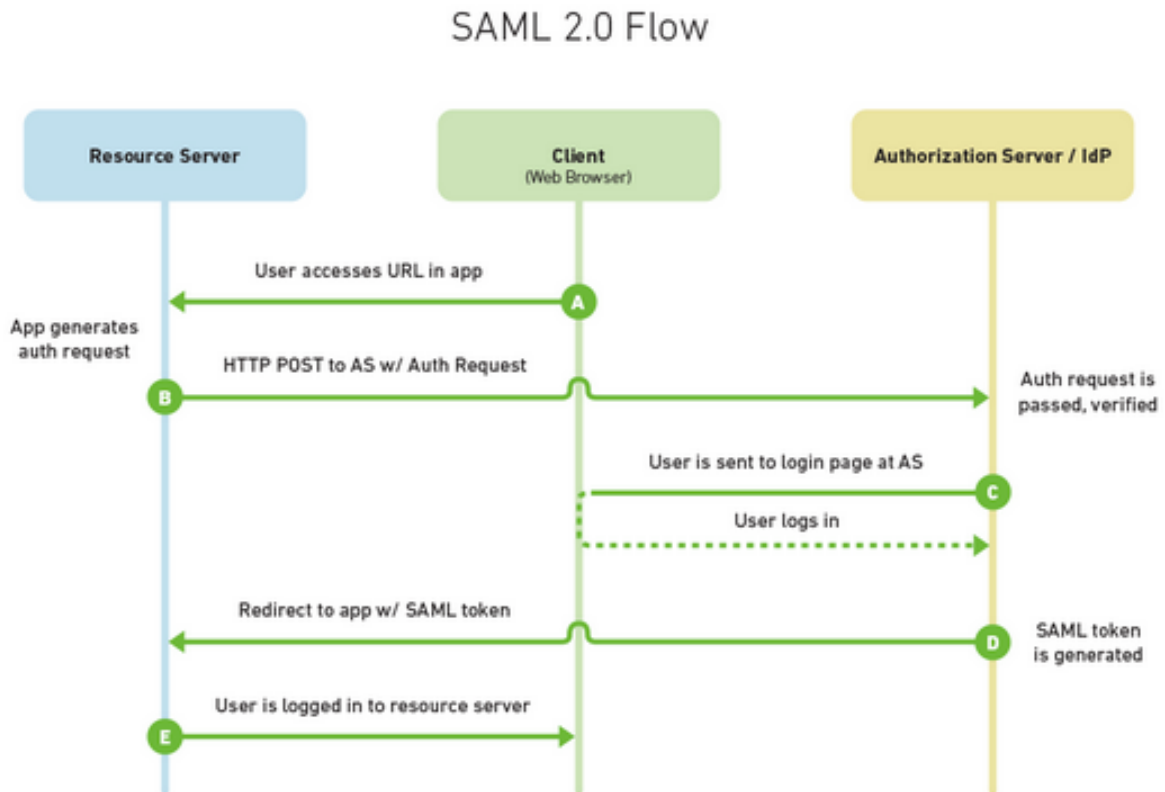
## Gebruikte componenten

UCS E11.5

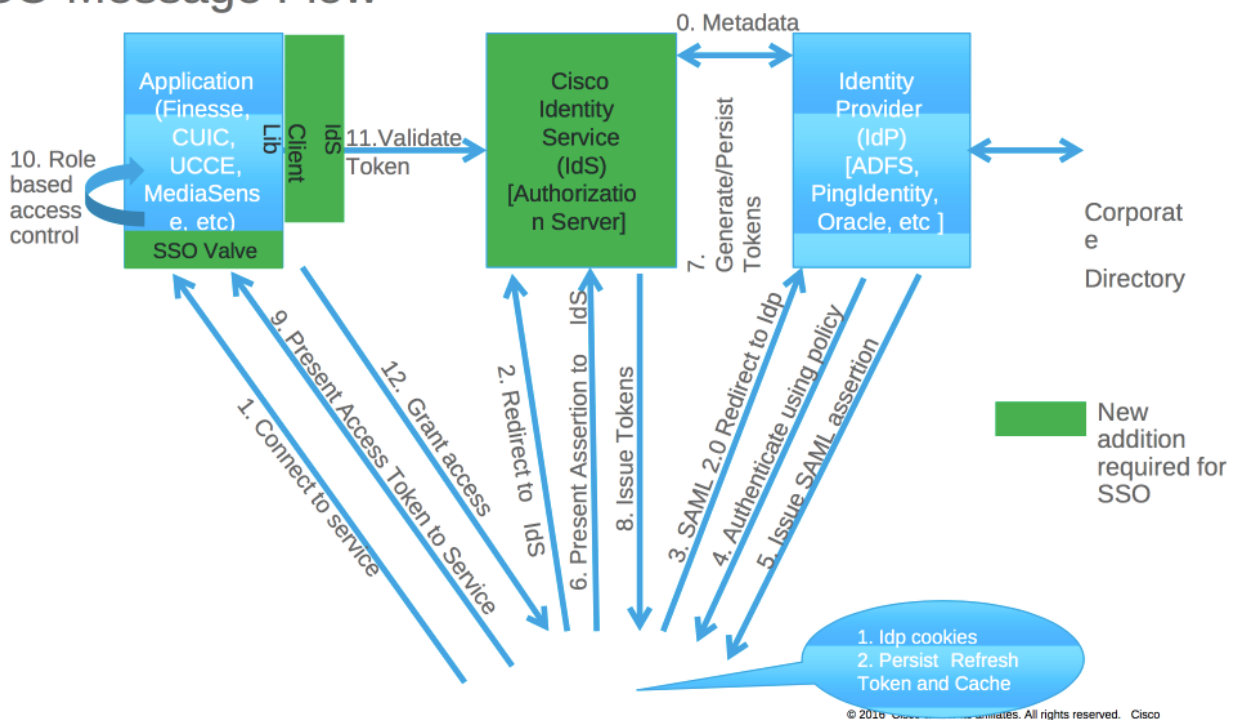
Windows 2012 R2

## Deel A. SSO-berichtenstroom

The most common SAML flow is shown below:



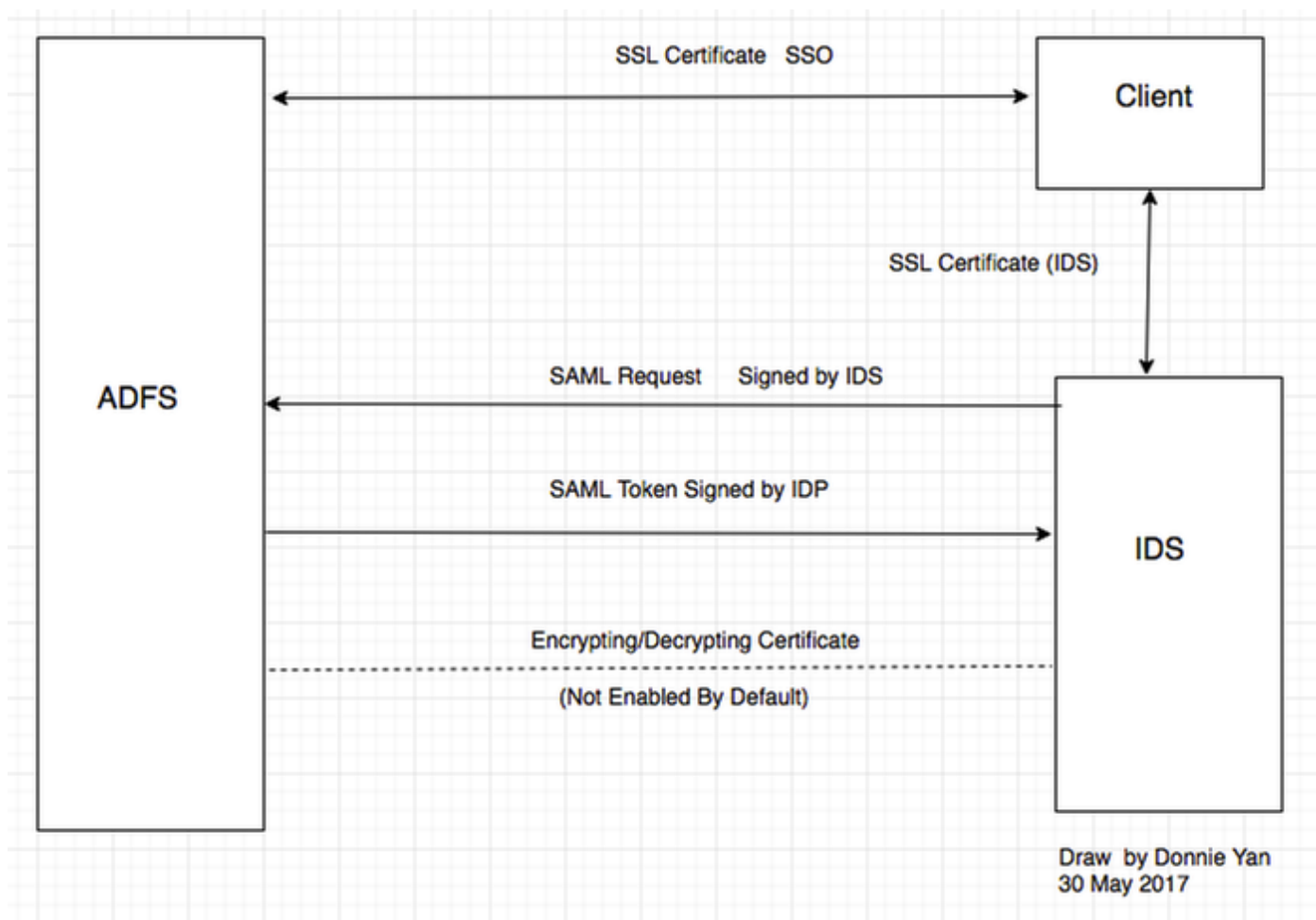
## SSO Message Flow



Als SSO is ingeschakeld, wanneer agent inlogt op Finesse desktop:

- Finesse server redirecteert agent browser om met Identity Service (IDS) te communiceren
- IDS-browser verwijst naar Identity Provider (IDP) met SAML-verzoek
- IDP genereert SAML-token en geeft deze door aan IDS-server
- Wanneer een token is gegenereerd, bladert elke keer dat de agent naar de toepassing bladert, er wordt deze geldige token gebruikt voor het loggen

## Deel B. In IDP en IDS gebruikte certificaten



### IDP-certificaten

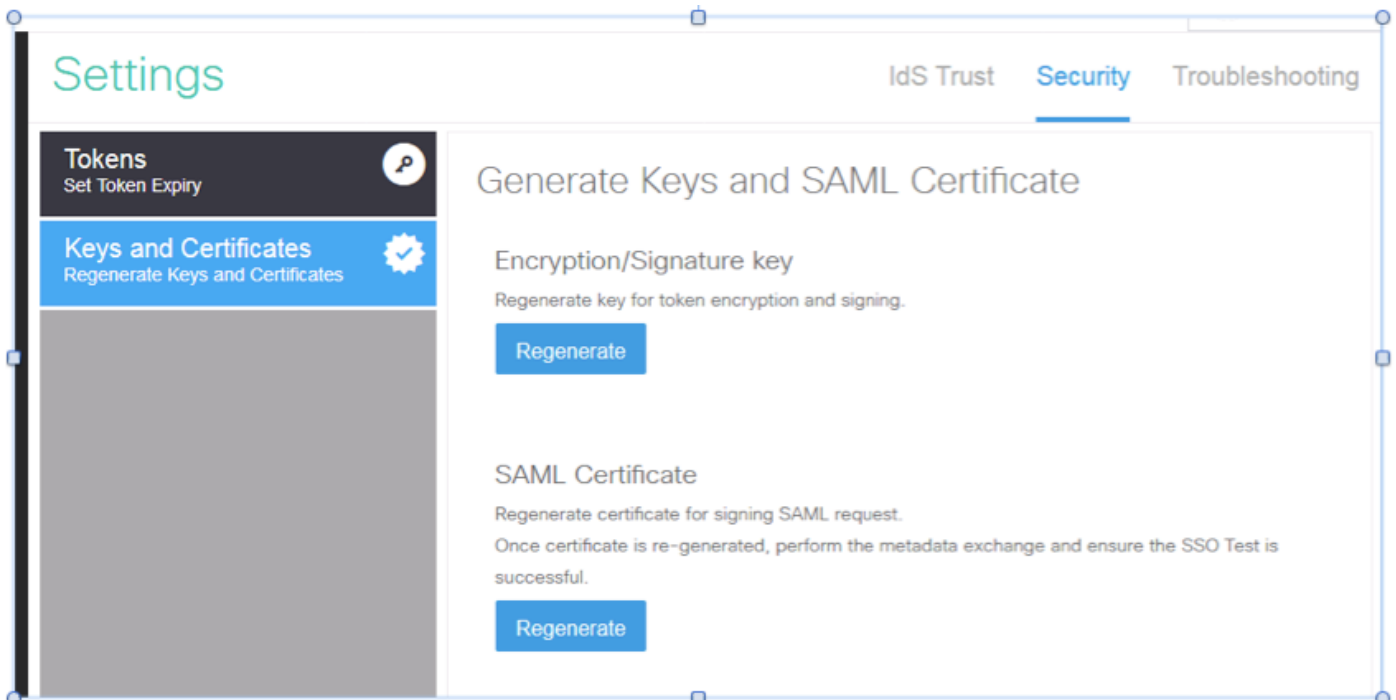
- SSL-certificaat (SSO)
- Token-signaalcertificaat
- Token - decryptie

1.

Subject	Issuer	Effective Date	Expiration Date	Status	Primary
<b>Service communications</b>					
CN=col115dc.col115.org.au, OU=TAC, O=Cisco...	CN=col115-COL115-CA, ...	12/30/2016	12/30/2017		
<b>Token-decrypting</b>					
CN=ADFS Encryption - col115dc.col115.org.au	CN=ADFS Encryption - co...	12/30/2016	12/30/2017		Primary
<b>Token-signing</b>					
CN=ADFS Signing - col115dc.col115.org.au	CN=ADFS Signing - col11...	12/30/2016	12/30/2017		Primary

### IDS-certificaten

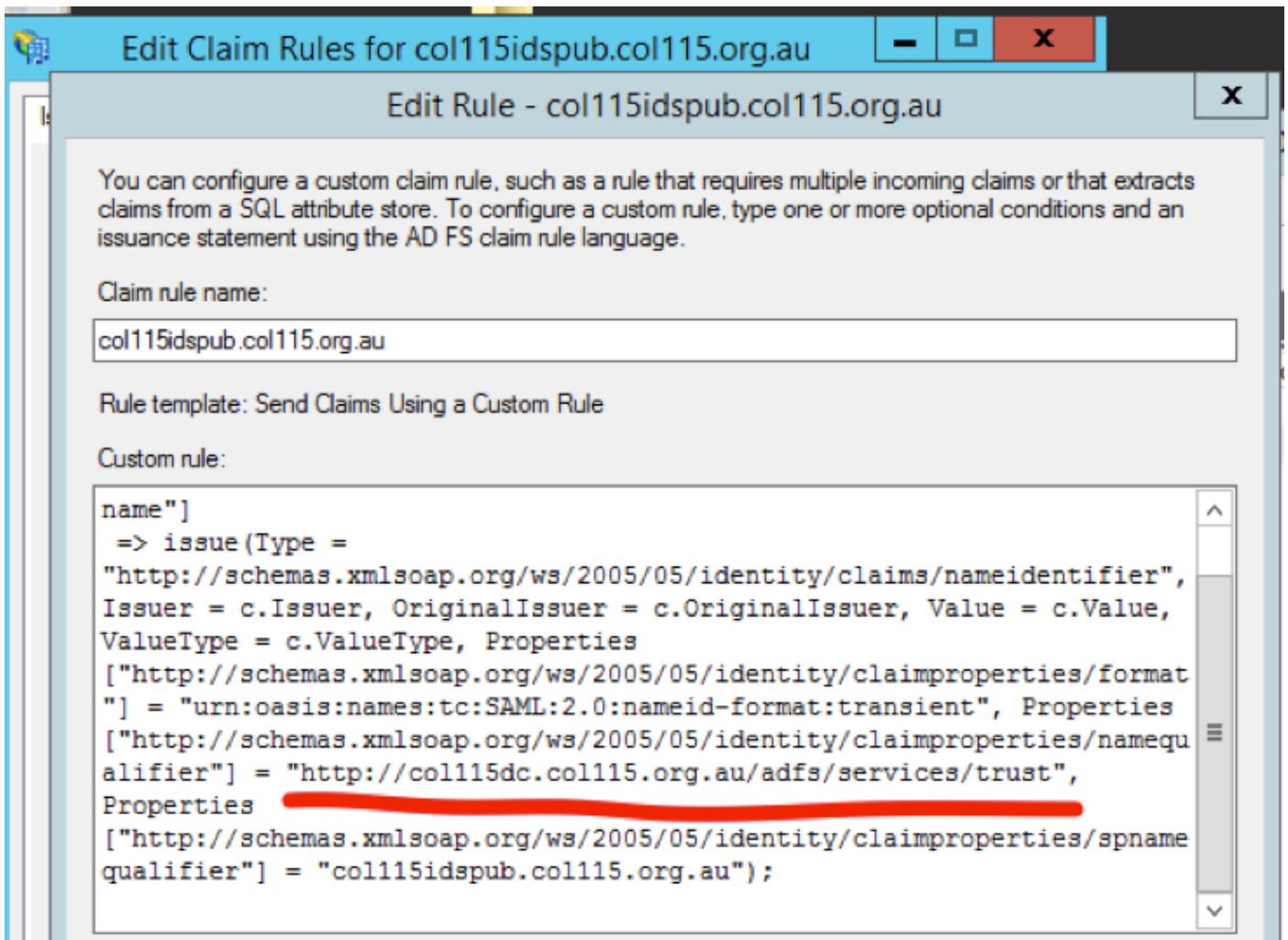
- SAML-certificaat
- Sleutel
- Encryptiesleutel



## Deel C. IDP-certificering in detail en configuratie

### SSL-certificaat (SSO)

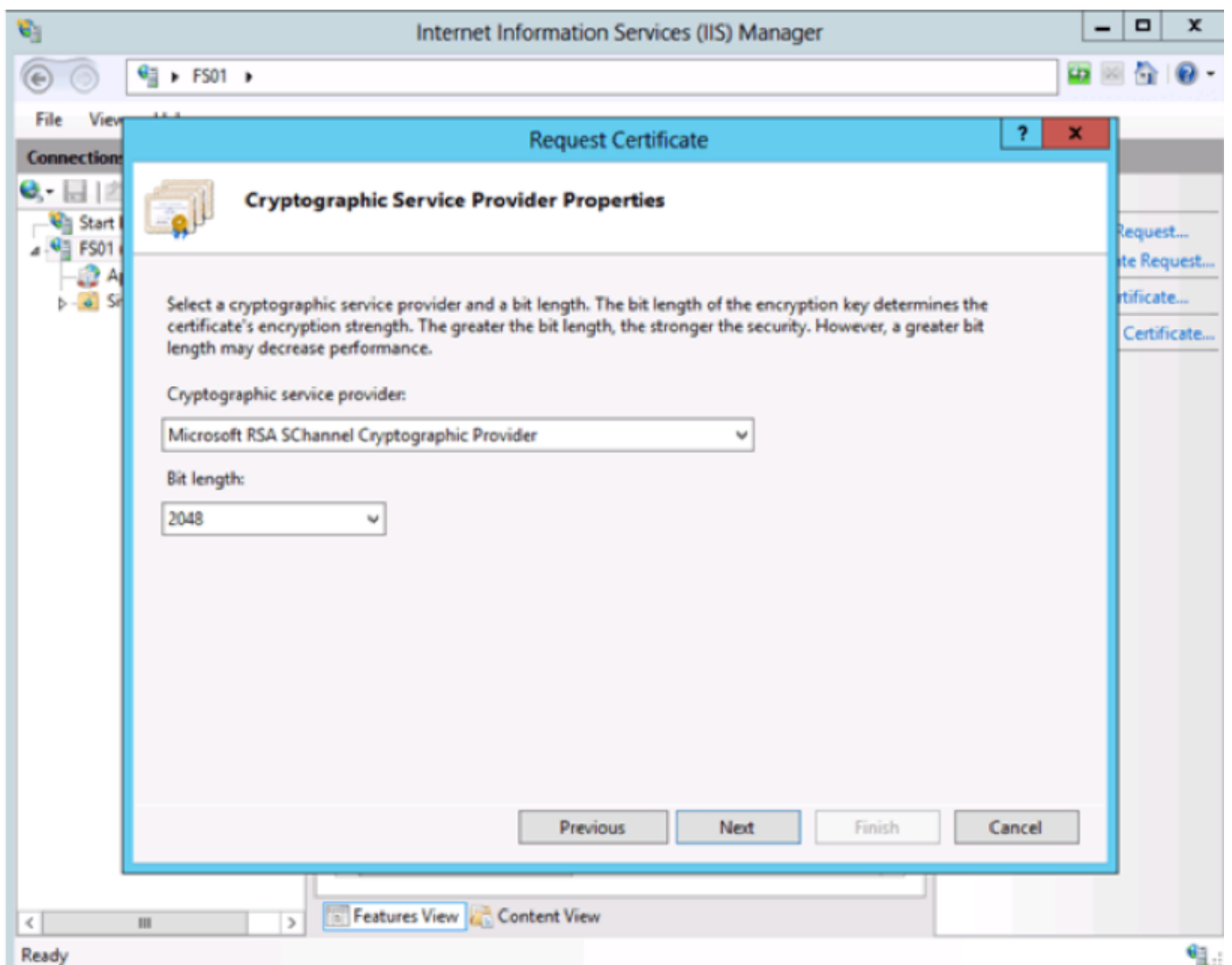
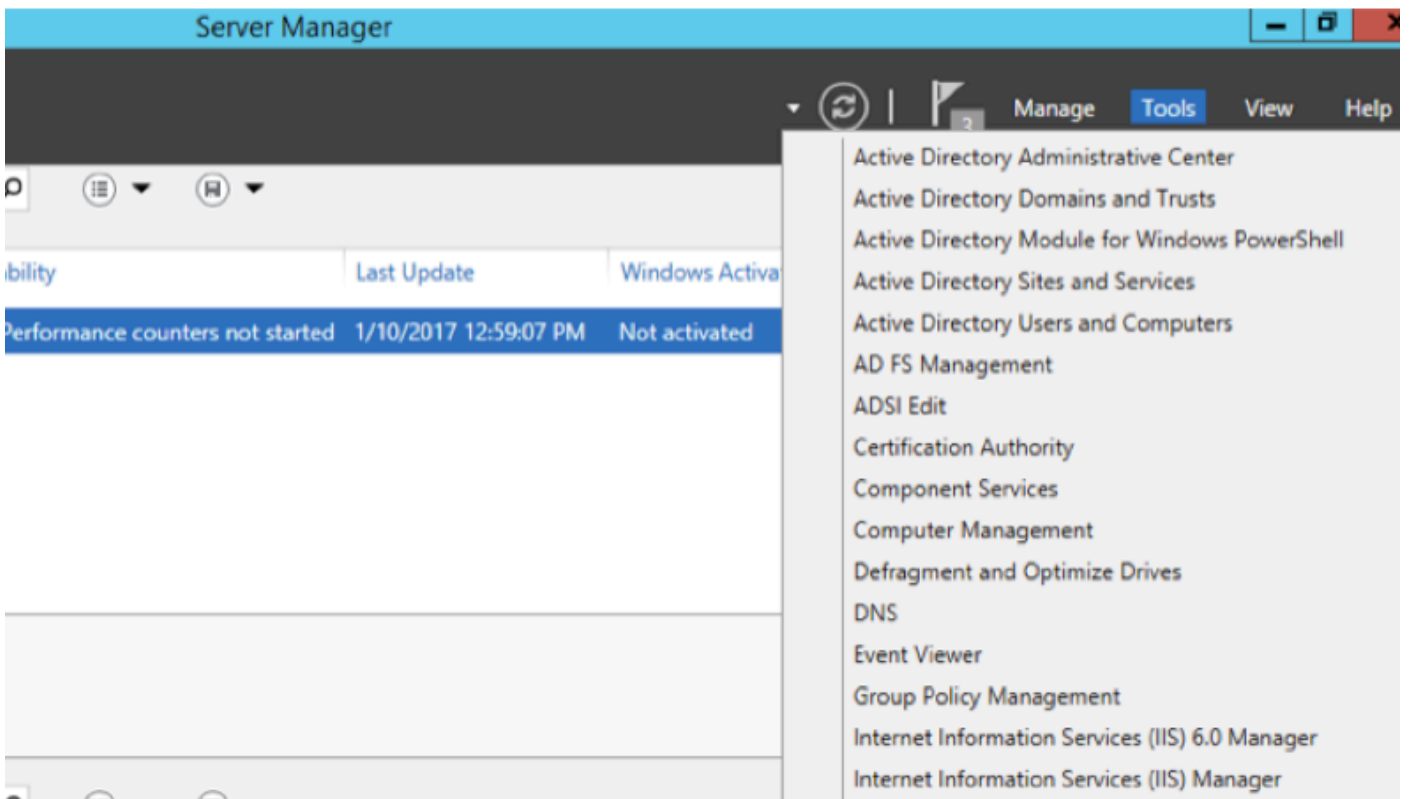
- Dit certificaat wordt gebruikt tussen IDP en client. De client moet een SSO-certificaat vertrouwen
- SSL-certificaat is geplaatst om de sessie tussen client en IDP server te versleutelen. Dit certificaat is niet specifiek voor ADFS, maar specifiek voor IS
- Het onderwerp van het SSL-certificaat moet overeenkomen met de naam die in de ADFS-configuratie wordt gebruikt



Stappen om SSL-certificaat voor SSO te configureren (lokaal lab met interne CA ondertekend)

Stap 1 . Maak SSL-certificaat met certificaataanvraag (CSR) en teken door interne CA voor ADFS.

1. Open Server Manager.
2. Klik op Gereedschappen.
3. Klik op Internet Information Services (IS) Manager.
4. Selecteer de lokale server.
5. Selecteer Server Certificaten.
6. Klik op Functie openen (actiepaneel).
7. Klik op certificaataanvraag **maken**.
8. Laat de cryptografische dienstverlener standaard staan.
9. Verander de **bit Length naar 2048**.
10. Klik op **Volgende**.
11. Selecteer een locatie voor het opslaan van het gevraagde bestand.
12. Klik op **Voltooien**.



Stap 2. CA tekent de CSR die uit stap 1 is gegenereerd.

1. **Open** CA-server om deze CSR [http:<CA Server ip-adres>/certsrv/](http://<CA Server ip-adres>/certsrv/)te gebruiken.
2. Klik op Een certificaat aanvragen.
3. Klik op Geavanceerde certificaataanvraag.
4. **Kopieer** de CSR naar de gecodeerde certificaataanvraag van Base-64.
5. **Indienen**.
6. Download het ondertekende certificaat.

Microsoft Active Directory Certificate Services -- col115-COL115-CA

## Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity, communicate with others over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

### Additional Attributes:

Attributes:

Submit >

**Stap 3.** Installeer het ondertekende certificaat terug naar ADFS-server en verdeel het naar ADFS-functie.

1. Installeer het ondertekende certificaat terug op de ADFS-server. Om dit te doen, **opent u Server Manager>Tools>Klik op Internet Information Services (IS) Manager>**.

**Lokale server>Server-certificaat>Open optie (actiepaneel).**

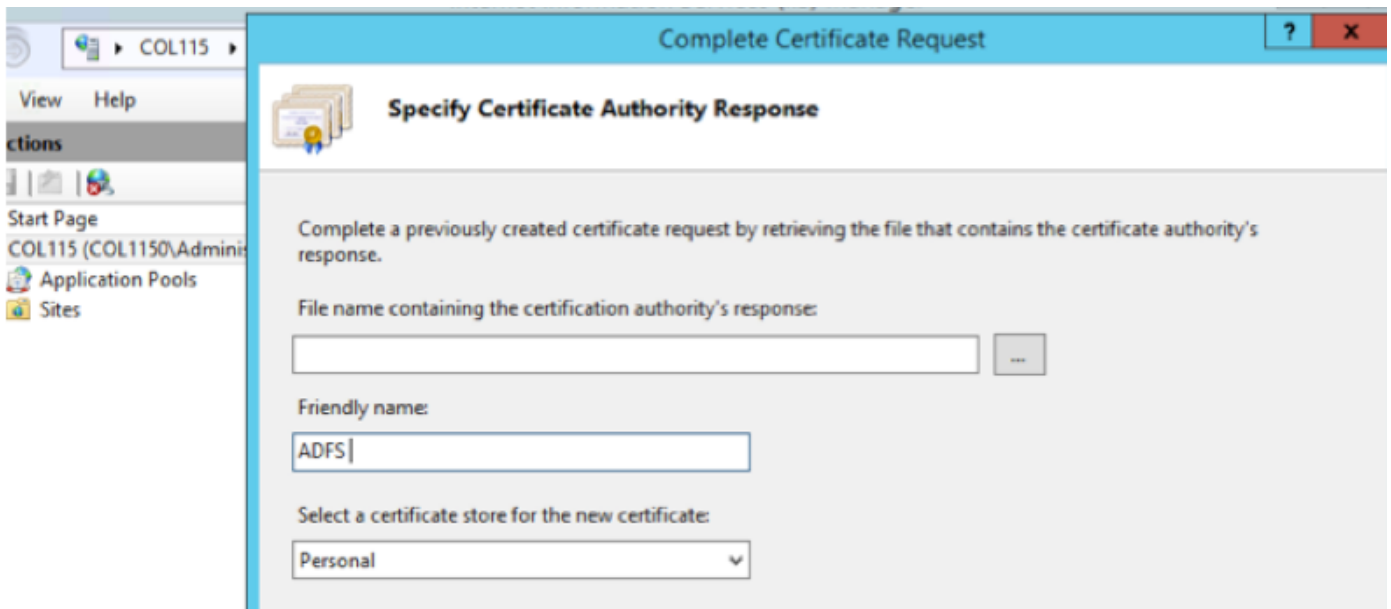
2. Klik op de volledige certificaataanvraag.

3. Selecteer het pad naar het volledige CSR-bestand dat u hebt ingevuld en gedownload van de derde certificatieprovider.

4. **Voer** de vriendelijke naam van het certificaat in.

5. Selecteer Persoonlijk als de certificaatwinkel.

6. Klik op **OK**.



7. In dit stadium werd alle certificaten toegevoegd. SSL-certificaat is nu vereist.

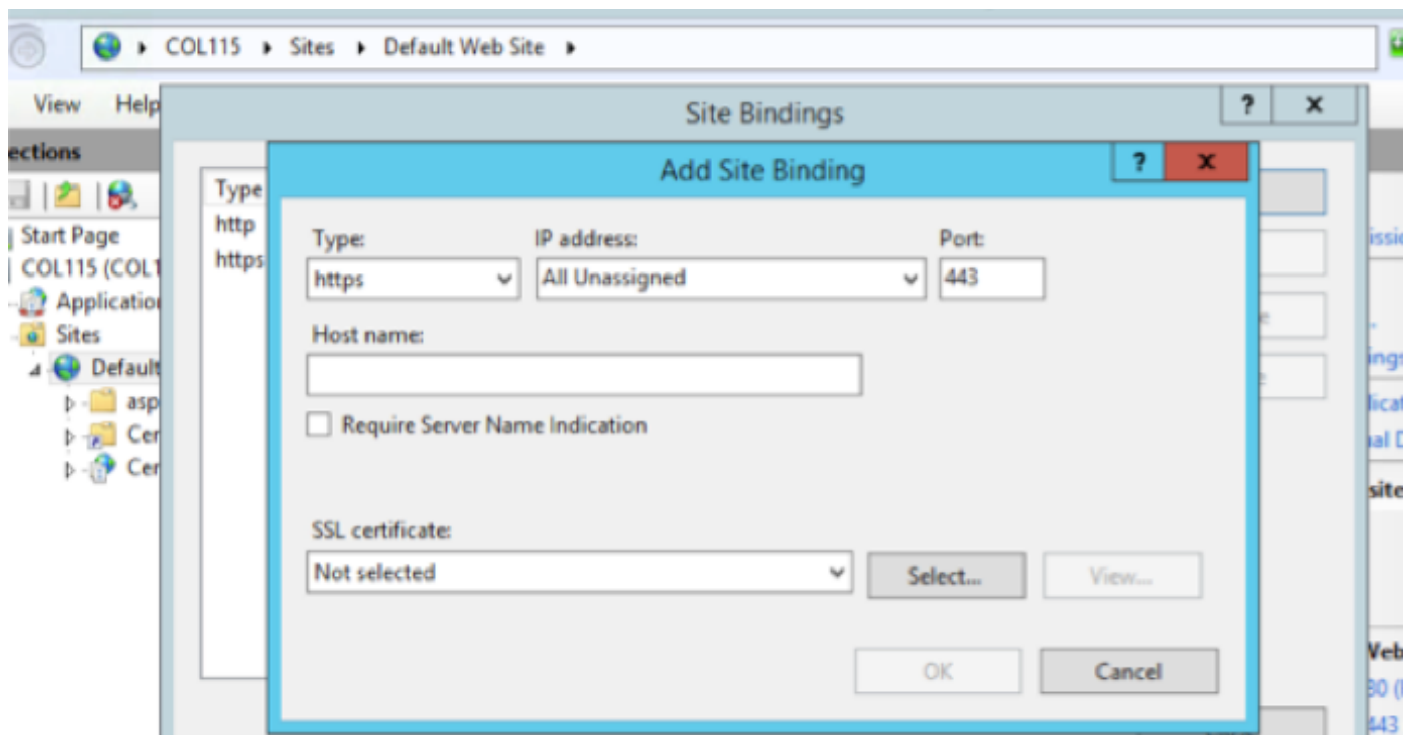
8. Vul de lokale server uit>Sites uitvouwen>Selecteer Standaardwebsite>Bindingen klikken (deelvenster met handelingen).

9. Klik op Toevoegen.

10. Wijzig het type naar HTTPS.

1. Selecteer uw certificaat in het uitrolmenu.

12. Klik op OK.



Nu is SSL-certificaat voor ADFS-server toegewezen.

Opmerking: Tijdens de installatie van de ADFS-functie moet er een eerder SSL-certificaat



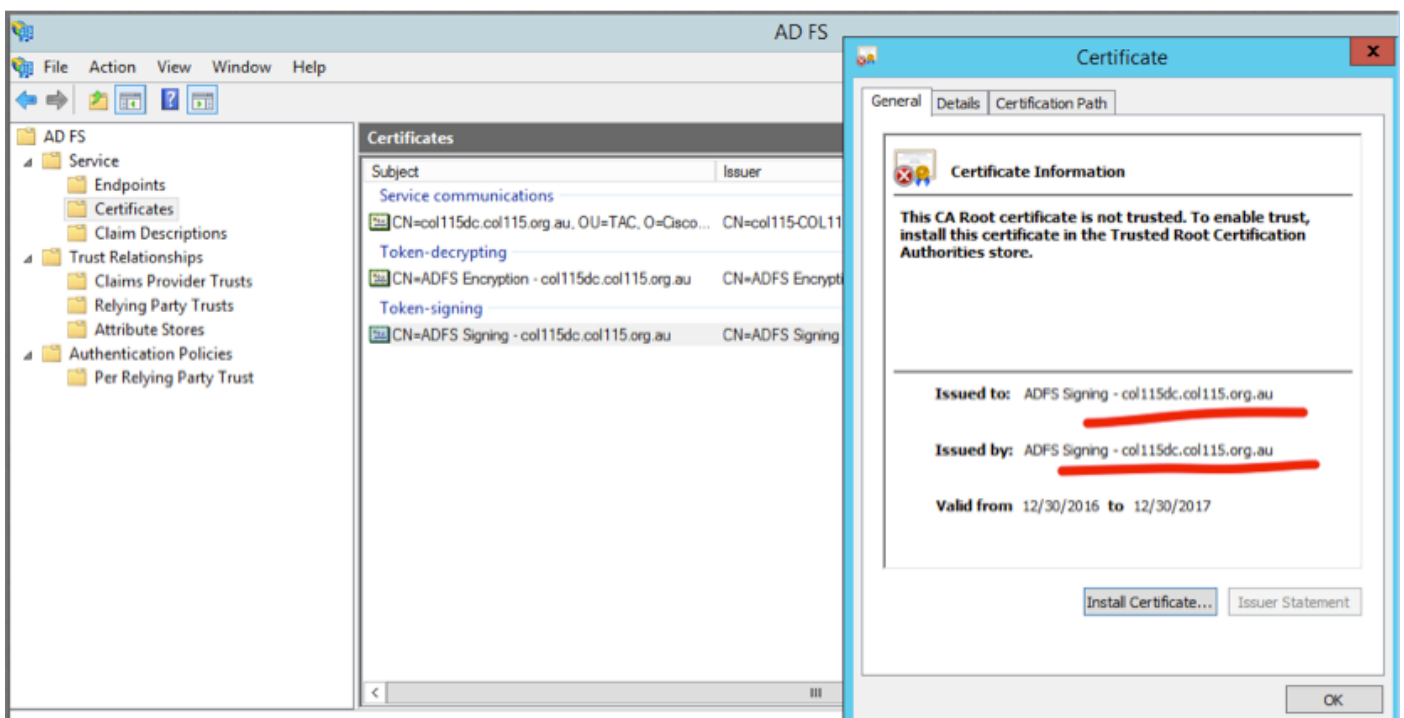
worden gebruikt.

## Token-signaalcertificaat

ADFS genereert zelfgetekend certificaat voor teken. Het is standaard een jaar geldig.

SAML-token gegenereerd door IDP is ingesloten door ADFS-toets (Token Signing Certificate Private Part). Vervolgens gebruikt IDS de ADFS-toets om dit te controleren. Deze garantie wordt niet aangepast.

Het Token Signing Certificate wordt elke keer gebruikt dat een gebruiker toegang moet krijgen tot een applicatie van een betrouwbare partij (Cisco IDS).



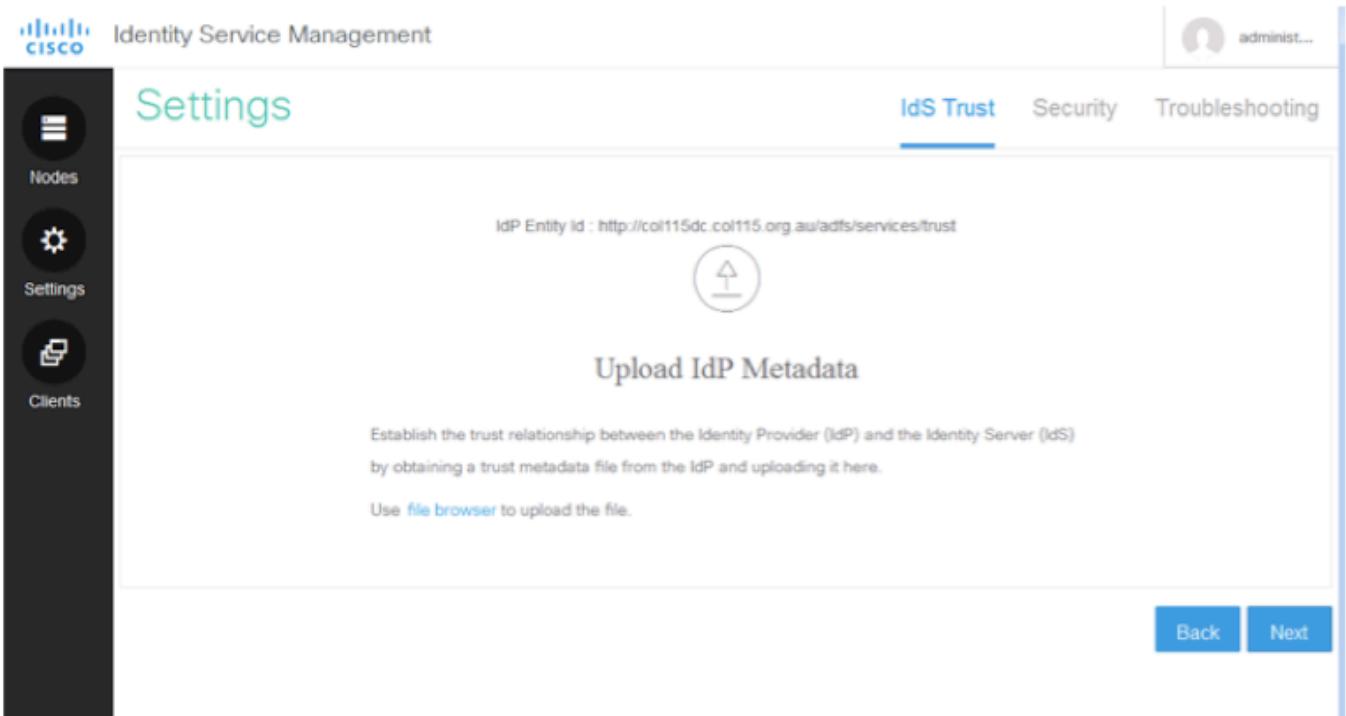
## Hoe krijgt Cisco IDS-server de openbare sleutel van Token Singing Certificate?

Dit gebeurt door ADFS-metagegevens te uploaden naar de IDS-server en vervolgens ADFS-publieke sleutel naar de IDS-server door te geven. Op deze manier verkrijgt IDS de openbare sleutel van ADFS-server.

U moet IDP-metagegevens downloaden van ADFS. Raadpleeg de link [https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml](https://<FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml) om IDP-metagegevens te downloaden.

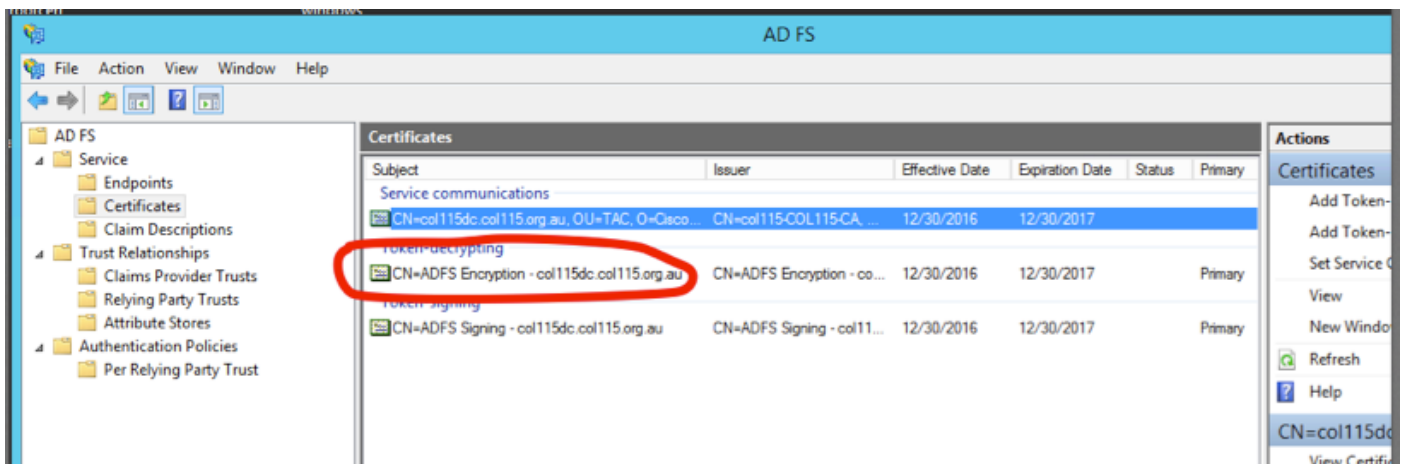
```
34
35
36 <!--KeyDescriptor use="signing"-->
37
38
39 <!--KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"-->
40
41 <!--X509Data-->
42
43
44 <X509Certificate>MIIC6DCCAdCgAwIBAgIQFpYJVv99CK9LN50rMdF5nDANBgkqhkiG9w0BAQsFADAwMS4wL2Y2OjE2L2GMyY29eMTE1Lm9yZy5hdTCCASIwDQYJKoZIhvcNAQEBBQADggE
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
```

Uit ADFS-  
metagegevens



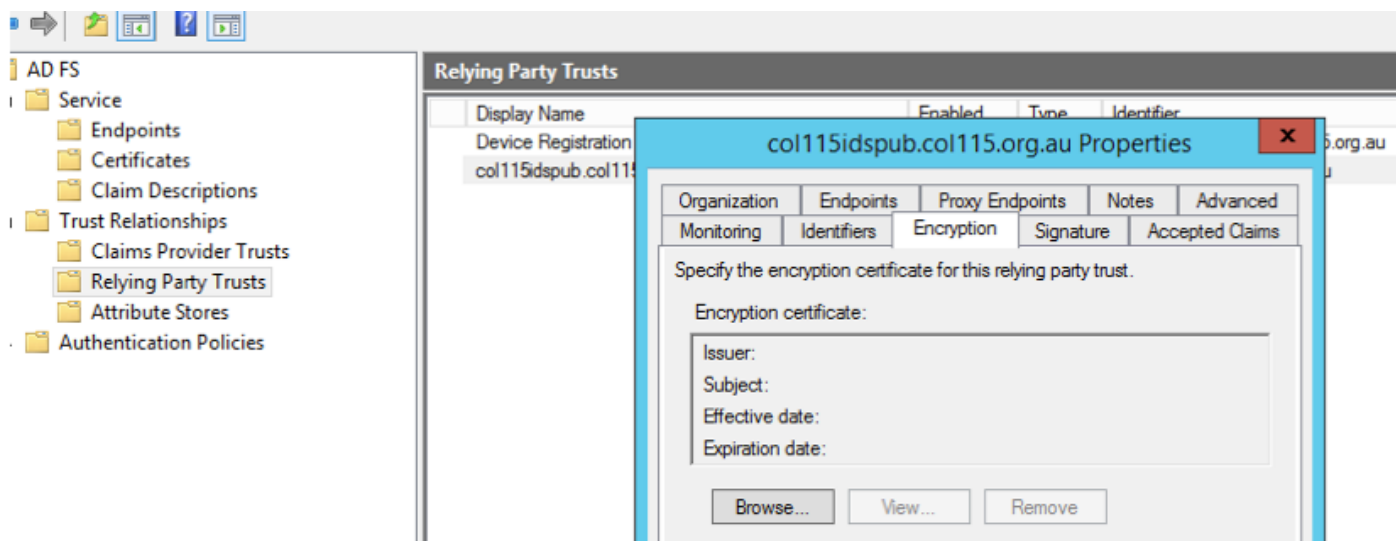
## ADFS-metagegevens uploaden naar IDS Token-decryptie

Dit certificaat genereert automatisch door ADFS-server (zelf-ondertekend). Als het token versleuteld moet worden, gebruikt ADFS de openbare sleutel van IDS om het te decrypteren. Maar wanneer je ADFS-token ziet, betekent dit NIET dat het token versleuteld is.



Als u wilt zien of de symbolische encryptie voor een specifieke aangesloten partijtoepassing werd toegelaten, moet u het coderingstabblad op een specifieke loyaliteits toepassing controleren.

Deze afbeelding toont dat een symbolische codering NIET is ingeschakeld.



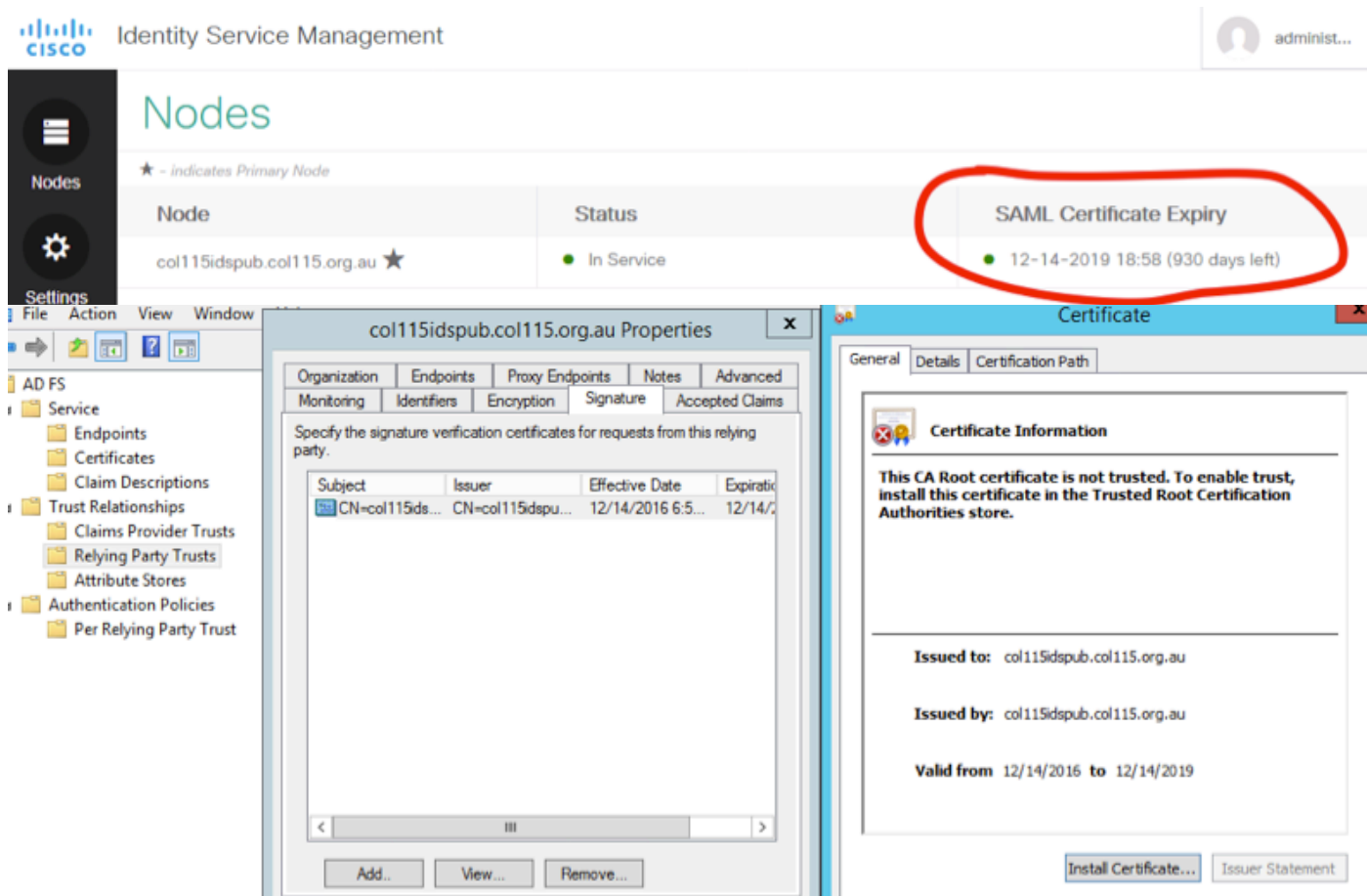
Encryptie is NIET ingeschakeld

### Deel D. Cisco IDS-zijcertificaat

- SAML-certificaat
- Encryptiesleutel
- Sleutel

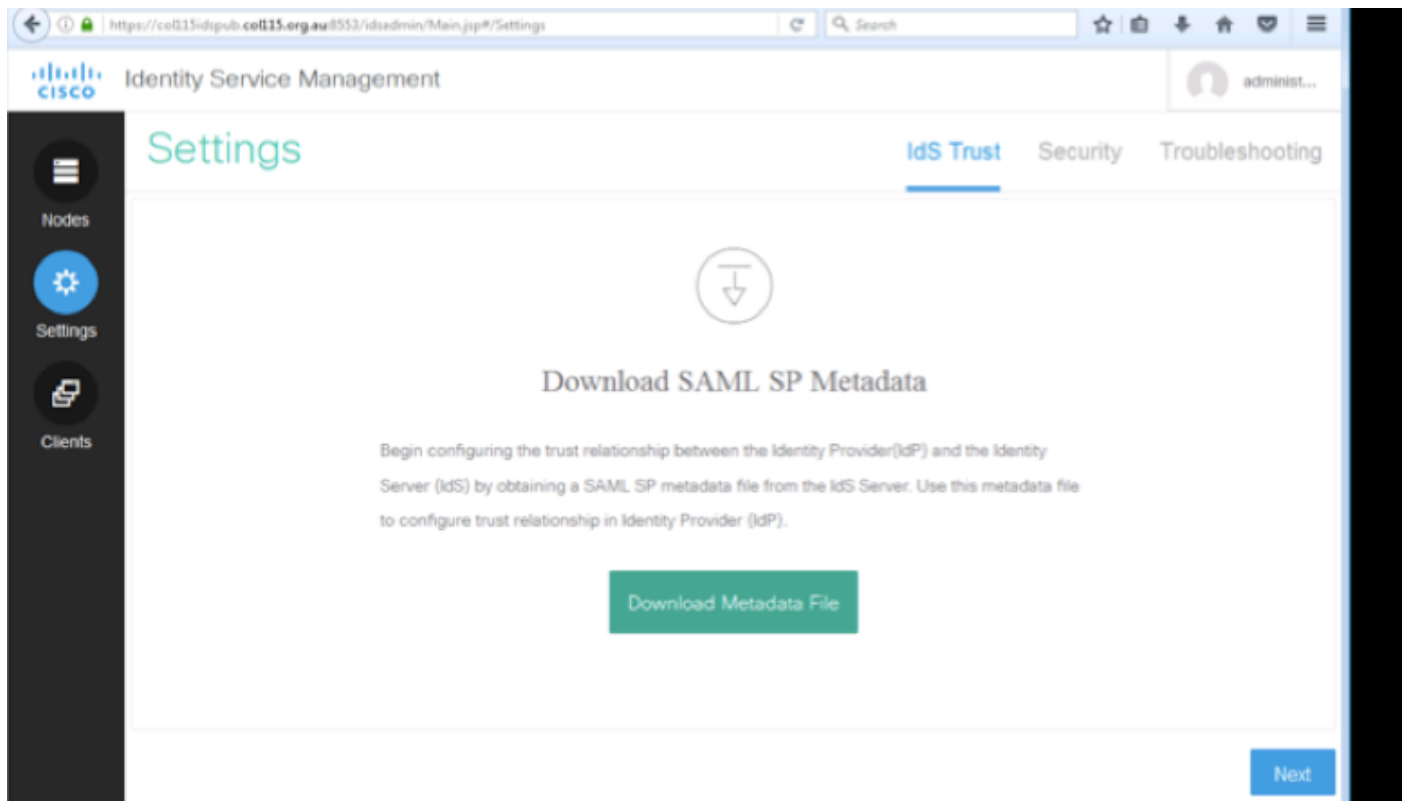
### SAML-certificaat

Dit certificaat wordt gegenereerd door een IDS-server (zelf-ondertekend). De standaard is 3 jaar geldig.



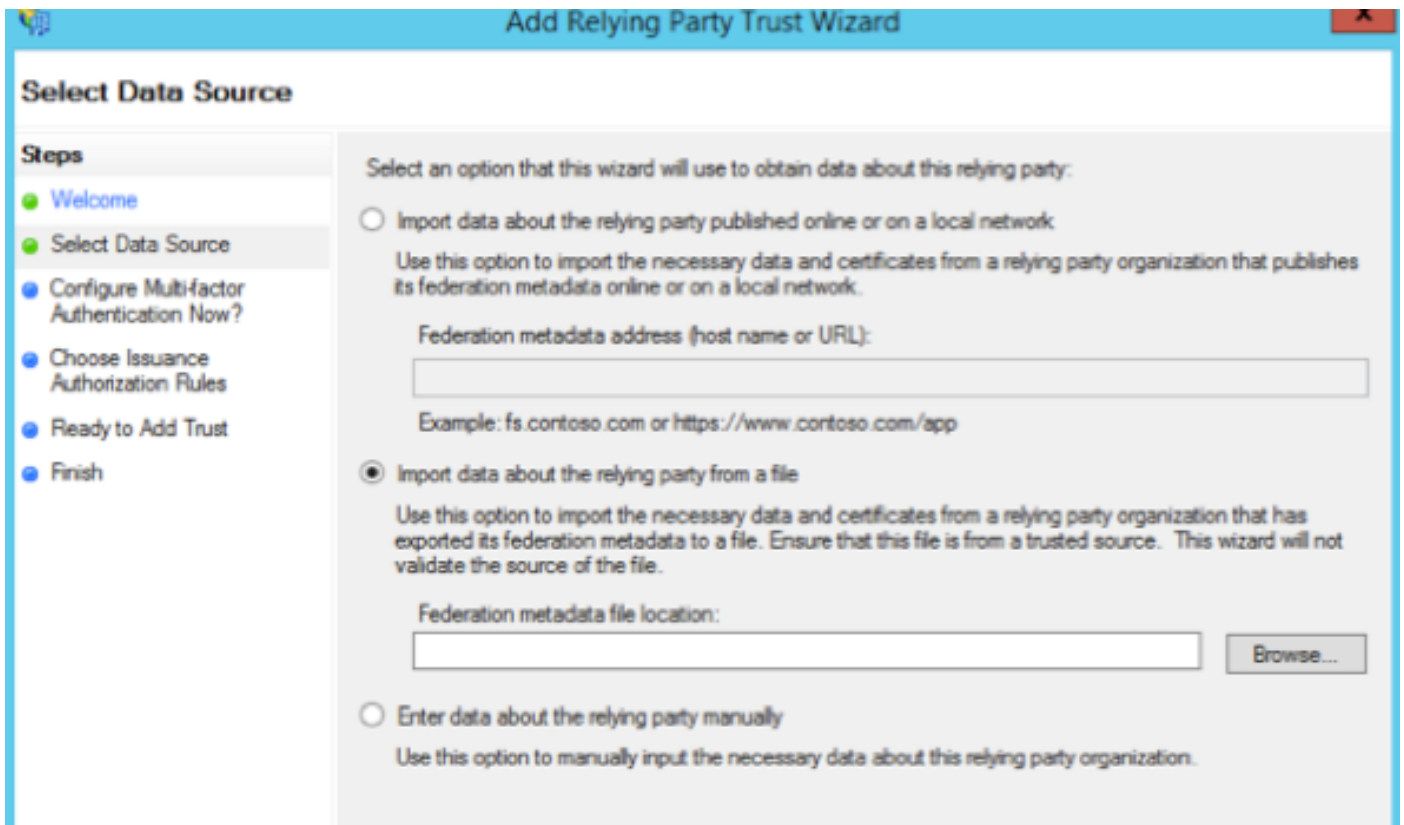
Dit certificaat wordt gebruikt voor het ondertekenen van SAML-aanvraag en voor het verzenden naar IDP (ADFS). Deze openbare sleutel bevindt zich in de IDS-metadata en moet worden geïmporteerd naar ADFS-server.

- 1.SAML SP-metadata van IDS server downloaden.
2. Browser naar <https://<ids server FQDN>:8553/disadmin/>.
3. Selecteer instellingen en download SAML SP-metagegevens en **bewaar** deze.

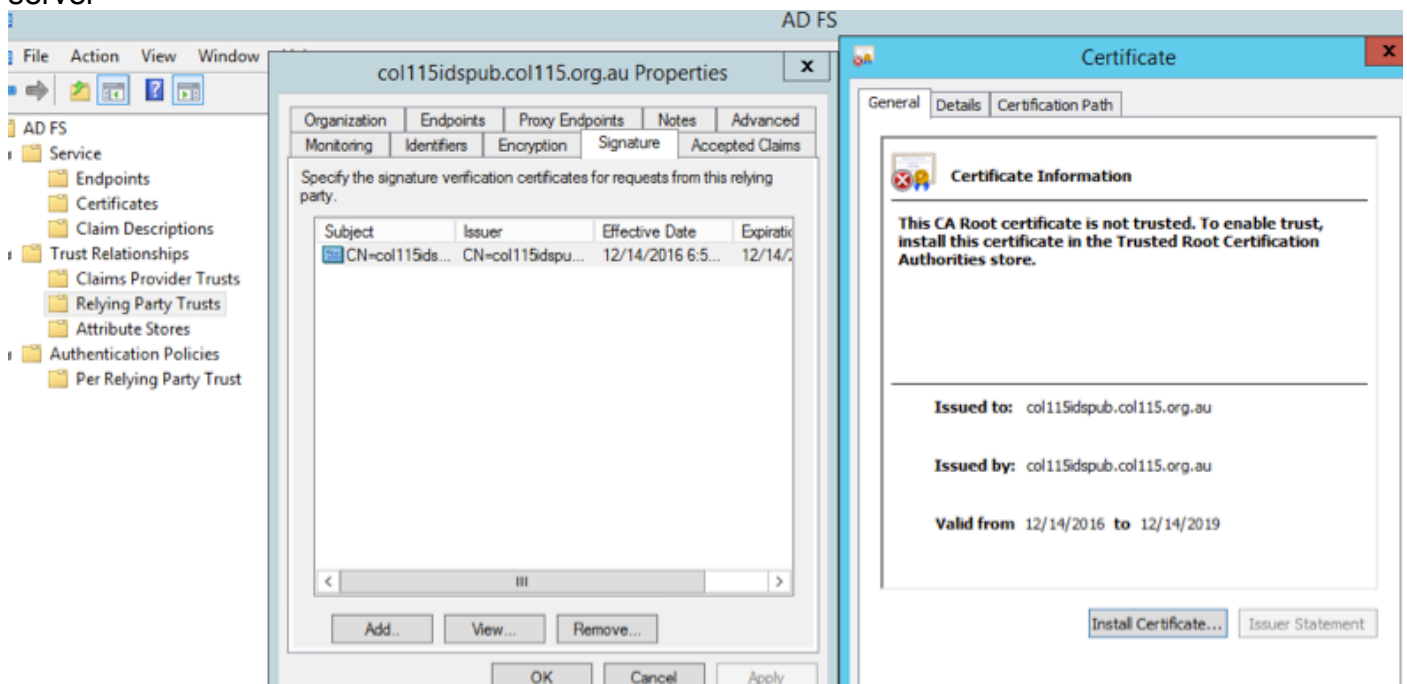


Metagegevens van IDS-server

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor entityID="col115idspub.col115.org.au" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  - <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
    - <KeyDescriptor use="signing">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
          <ds:X509Certificate>MIIC+TCCAeGgAwIBAgIEWD4KIDANBgkqhkiG9w0BAQUFADAISMwIQYDVQQDExpjb2wxMTVpZHNw
          dWl0Y29sMTE1Lm9yZy5hdTAeFw0xNjE5MTQwNzU4MjVhFw0xOTEyMTQwNzU4MjVhVAMCUxIzAhBgNV
          BAMTGmNvbDExNWlk3B1Y15jb2wxMTUub3JnLmF1F1MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
          CoKCAQEA4Qc09pm1wXcMM+WhS/Yht+3C2XY1eC0v09d0Q50hfmCsu176/C0I8uEUe713uA2ez8
```



importeren naar ADFS-server

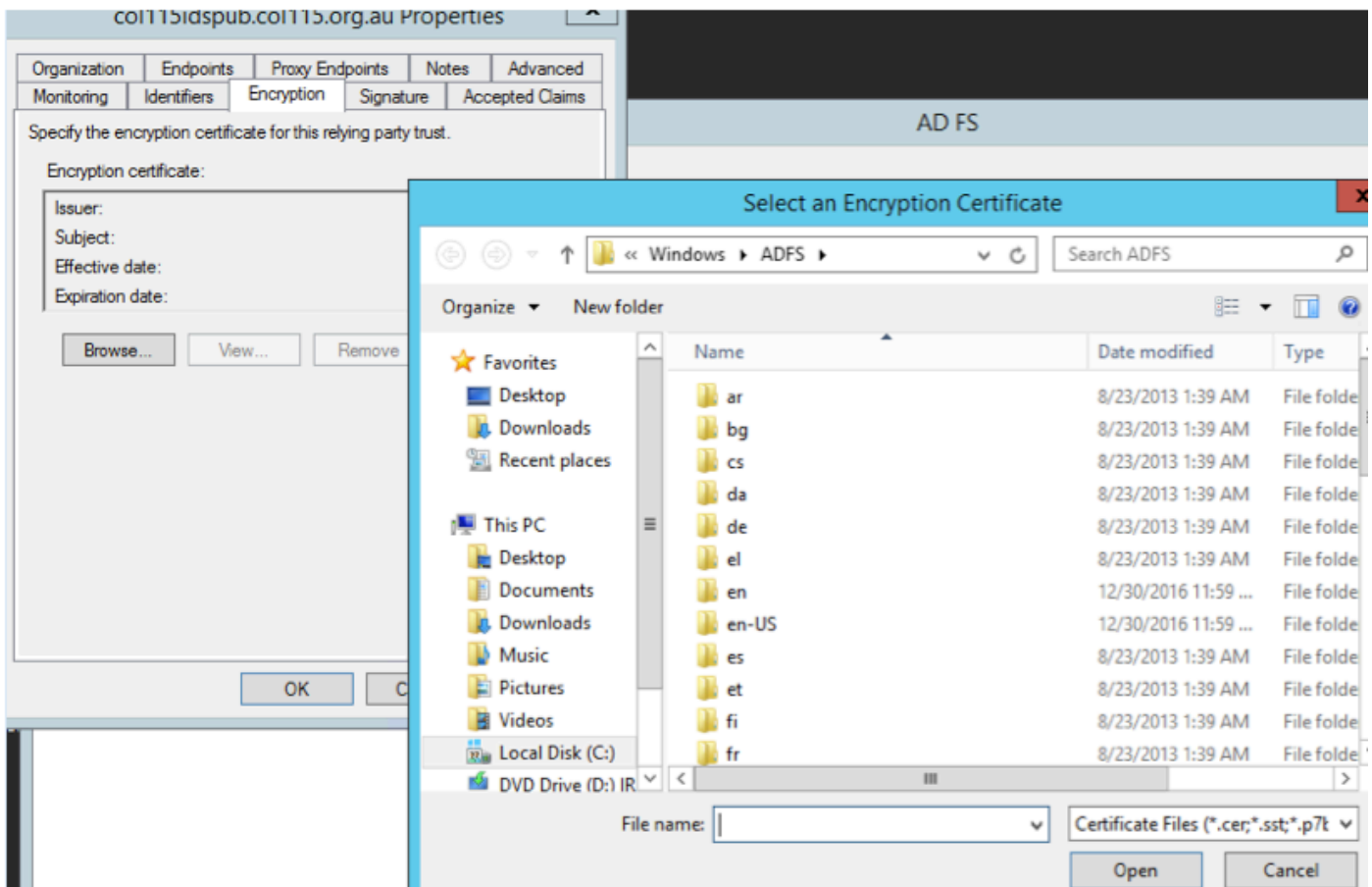


Verifiëren aan ADFS-zijde

Wanneer IDS het SAML-certificaat opnieuw genereert, wordt het gebruikt om het SAML-verzoek te ondertekenen, voert het metagegevens uit om te wisselen.

### Toetsen voor versleuteling/handtekening

Encryptie is standaard niet ingeschakeld. Als encryptie is ingeschakeld, moet deze naar ADFS worden geüpload.



Referentie:

[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cust\\_contact/contact\\_center/icm\\_enterprise/cm\\_enterprise\\_11\\_5\\_1/Configuration/Guide/UCCE\\_BK\\_U882D859\\_00\\_ucce-features-guide/UCCE\\_BK\\_U882D859\\_00\\_ucce-features-guide\\_chapter\\_0110.pdf](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/cm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-features-guide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf)