

Vorbereiding gegevensuitwisseling Ysis

Toelichting PKI/Certificaten

Inhoud

1	INLEIDING	1
1.1	DOEL	1
1.2	SAMENVATTING	1
2	HOE HET WERKT	2
2.1	CERTIFICAAT	2
2.2	ONDERTEKENING	2
2.3	CERTIFICATE AUTHORITY (CA)	3
2.4	BIDIRECTIONEEL	3
2.5	GELDIGHEID	3
3	ACTIES VOOR INREGELLEN KOPPELING	4
3.1	HET GEBRUIK MAKEN VAN DE YSIS WEBSERVICES	4
3.2	GERIMEDICA TOESTAAN DE WEBSERVICE VAN HET ANDERE ZORGPAKKET AAN TE ROEPEN	5

1 Inleiding

1.1 Doel

Voor het uitwisselen van informatie tussen informatiesystemen wordt vaak gebruik gemaakt van **public key infrastructure** (PKI). Hierbij worden digitale **certificaten** gebruikt als identificatiebewijs.

De doelgroep van dit document is primair voor integratiepartners en ICT afdeling van zorginstellingen.

De eerste paragrafen geven wel een korte functionele toelichting over het nut en de noodzaak van certificaten voor niet-technici.

1.2 Samenvatting

Certificaten worden binnen Ysis voor twee doelen toegepast:

- *Authenticatie.*
Bij het verbinden met een andere computer wordt het gebruikt voor het controleren van de identiteit van het andere systeem (de 'authenticatie'). Dit is krachtiger dan alleen een gebruikersnaam en wachtwoord omdat het ook garandeert dat de verbinding alleen vanaf 1 specifieke computer (server) kan worden gelegd, en niet vanuit andere computers.
- *Encryptie.*

Een certificaat wordt ook gebruikt voor het versleutelen van informatie zodat deze niet leesbaar is via het openbare internet. Alleen de computer die het certificaat bezit kan de informatie weer ontsleutelen.

Indien beide technieken worden toegepast is een beveiliging door middel van VPN overbodig; het gebruik van certificaten biedt een zelfde niveau van veiligheid.

Het uitgangspunt voor GeriMedica bij koppelingen is dat wij voor systemen die informatie *naar* ons systeem (Ysis) sturen, altijd een beveiliging met certificaten vereisen.

Elke partner heeft in hun systeem echter hun eigen methodes voor beveiliging geïmplementeerd. Voor het versturen van informatie *vanuit* Ysis naar het systeem van onze partners worden de veiligheidsmethoden van de betreffende partner toegepast.

2 Hoe het werkt

Voor het opzetten van een veilige verbinding zijn drie aspecten belangrijk:

- Identificatie van het doel en bron systeem
- Voorkomen dat informatie wordt gewijzigd tijdens transport
- Voorkomen dat anderen dan het doel systeem inzage heeft tot de informatie

Door gebruik te maken van **public key infrastructure** (PKI) en het TLS protocol gezamenlijk met onderliggende technieken worden de hiervoor genoemde aspecten ondervangen.

In dit document zullen wij ons verder richten op de zaken rondom PKI m.b.t. het uitgeven en aanvragen van certificaten. Andere onderdelen zijn reeds aan de orde gekomen tijdens de implementatie van de koppeling. Dit document richt zich op de acties bij uitrol van een koppeling.

2.1 Certificaat

Bij het gebruik van PKI worden (public key) certificaten gebruikt als identificatiebewijs. Voor het maken van een certificaat zijn drie onderdelen nodig: een public key, een private key en identificatie informatie(bv naam van de server).

De public key en private key vormen een paar en zullen dan ook samen worden gebruikt om eigendom van het resulterende certificaat te verifiëren. Iedereen die beschikt over de 'private key' kan het resulterende certificaat gebruiken om zich te identificeren. Derhalve is het dus **belangrijk dat de 'private key' niet gedeeld wordt**. Tijdens het vaststellen van eigenaarschap wordt de private key wel gebruikt, maar *niet* gecommuniceerd met de partij die de identiteit wilt vaststellen.

2.2 Ondertekening

Omdat iedereen zelf bovengenoemde onderdelen zelf kan creëren, respectievelijk kan specificeren zijn deze gegevens op zichzelf in beginsel geen waarde. Dit verandert echter wanneer een andere partij de opgegeven identiteitsinformatie onderschrijft. Dit geschiedt middels het ondertekenen van het certificaat. Dit wordt ook wel het **signen** van het certificaat genoemd. Dit is het digitale equivalent van het laten legaliseren van een document door een notaris.

Het aanmaken van een digitaal certificaat en deze te laten ondertekenen geschiet middels een zo genoemd Certificate Sign Request (CSR). **De partij waarvoor een digitale identiteit moet worden gemaakt maakt de CSR.** De CSR is een bestand met daarin alleen de public key tezamen met de identiteit informatie. Deze word gestuurd naar een partij die de geldigheid van de identiteit bevestigt. Deze partij is de zo genoemde Certificate authority (CA). Met het ondertekenen van het certificaat word de opgegeven identiteit bevestigt door de CA.

2.3 Certificate authority (CA)

Zoals hiervoor genoemd is de partij die de identiteit van andere partijen onderschrijft/erkent de certificate authority en bevestigt de indentiteitsinformatie in de certificaten die deze ondertekend. Iedereen kan zich opwerpen als een certificate authority. Wij zullen in een latere versie van dit document de stappen beschrijven om zelf een CA te worden. Gebruikers van certificaten, partijen/entiteiten die de identiteit willen vaststellen van mensen die een certificaat presenteren, moeten er voor kiezen om één of meerdere CA's te vertrouwen. 'Het vertrouwen van een CA' houdt in dat certificaten die ondertekend zijn door een CA ook vertrouwd worden. In het geval van Integratie koppelingen is de partij die optreedt als CA doorgaans ook de beheerder van het systeem dat de data ontsluit. Afhankelijk van de inrichting van de software waarmee gekoppeld word is dit de zorginstelling of de software leverancier. In het geval van Ysis is dit de software leverancier: Gerimedica.

2.4 Bidirectioneel

Bij koppelingen word bijna altijd de data bidirectioneel uitgewisseld. Gezien hier twee systemen bij betrokken zijn die beiden beheerd worden door een andere partij zal er ook sprake zijn van twee certificate authorities(CA's).

Bij het opzetten van een verbinding tussen systemen is er altijd sprake van één systeem die de verbinding initieert(de client) en de partij die zich voor verbindingen openstelt(de server). Bij het verbinden moeten beide systemen zich identificeren zodat de bron van de informatie als wel de ontvanger word vastgesteld. Hierbij is sprake van respectievelijk een cliënt certificaat en het server certificaat. Voor het verbinden vanuit een ander systeem met Ysis is dus een cliënt certificaat vereist. Een client certificaat, voor het verbinden met Ysis, word gemaakt door een CSR naar Gerimedica te sturen welke dan optreedt als CA. Gerimedica verwerkt de CSR (het certificaat word ondertekend) en stuurt deze dan retour naar de aanvrager. Daar Ysis ook moet verbinden met het te koppelen systeem verstuurd Gerimedica doorgaans ook een CSR naar de zorginstelling. Afhankelijk of de te koppelen software ook identificatie(authenticatie) uitvoert op basis van certificaten.

2.5 Geldigheid

Certificaten hebben een beperkte geldigheid duur. De CA geeft dit aan bij het ondertekenen van het certificaat. Gerimedica hanteert een periode van 3 jaar voor certificaten die zij uitgeeft als CA. Voor certificaten die Gerimedica niet uitgeeft maar aanvraagt houdt Gerimedica de geldigheidsduur bij en verwittigt de zorginstelling wanneer deze certificaten dreig te verlopen.

3 Acties voor inregelen koppeling

3.1 Het gebruik maken van de Ysis Webservices

Hiervoor moet u een Client Certificaat maken dat door GeriMedica word 'gesigned'.

1. Aanvragen (Zorginstelling of integratie partner)

Afhankelijk van het beheer van de server waarop de koppeling draait is het aan de Zorginstelling of aan de integratie partner(Saas oplossing) om de aanvraag van het certificaat te verzorgen.

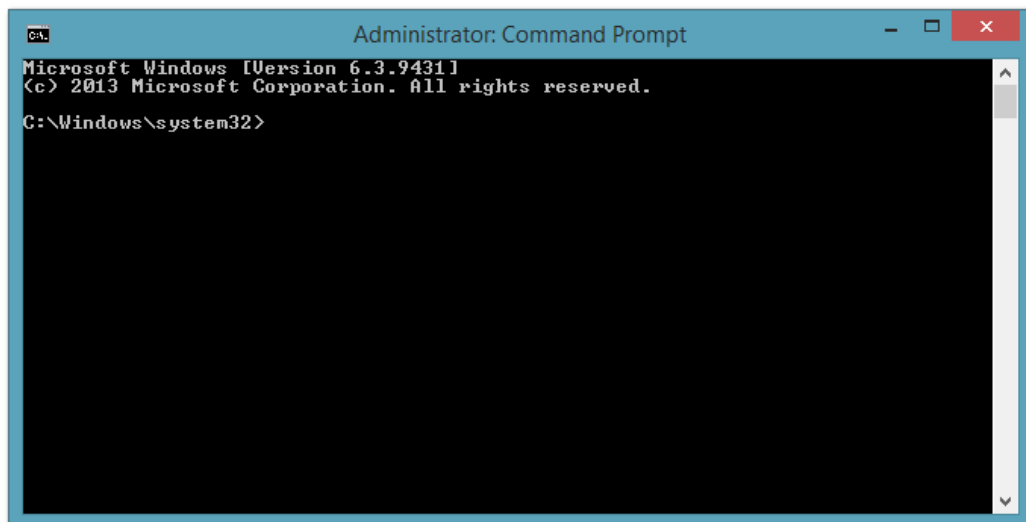
Aanmaken CSR onder windows:

a) Openssl bemachtigen

- Download openssl voor windows:
<https://www.openssl.org/related/binaries.html>
- Kies voor OpenSSL voor windows "Pre-compiled Win32/64 libraries without external dependencies..." dit leid tot de volgende lokatie:
<http://indy.fulgan.com/SSL/>
- Kies onderaan de pagina voor de meest recente versie van openssl-...-x64_86-win64.zip
- pak het bestand uit en onthou de locatie

b) Aanmaken private key

- ga naar start en type 'cmd'
- klik vervolgens met de rechtermuisknop op 'cmd.exe' en kies 'run as administrator'



- in de nieuw geopende window: cd naar de locatie waar u het eerder gedownloade bestand heeft uitgepakt.
- Voer het volgende command uit:
openssl.exe genrsa -out zorginstelling-koppelsoftwarenaam.key 4096
waarbij u zorginstelling met de naam van u zorg instelling vervangt en koppelsoftwarenaam met de naam van het te koppelen pakket.
- Het resultaat is het bestand **zorginstelling-koppelsoftwarenaam.key**, bewaar dit bestand goed dit stelt u instaat zich te identificeren met het uiteindelijke certificaat.

c) **Aanmaken van de CSR**

- maak een bestand met de naam openssl.txt aan met de volgende inhoud in zelfde directory als waar het zip bestand is uitgepakt:

```
[ req ]
distinguished_name      = req_distinguished_name
[ req_distinguished_name ]
countryName              = Land code (2 letter code)
countryName_default      = NL
countryName_min          = 2
countryName_max          = 2
localityName             = Locatie naam (bv, naam van de stad)
organizationalUnitName    = Organizational Unit Name (eg, section)
commonName               = Common Name (zorginstelling-koppelpartner)
commonName_max           = 64
emailAddress              = Email Adres
emailAddress_max         = 40
```

- Voer het volgende command uit:
openssl.exe req -new -sha512 -key zorginstelling-koppelsoftwarenaam.key -out zorginstelling-koppelsoftwarenaam.csr -config %CD%\openssl.txt
- Er word u gevraagd om de volgende gegevens:
Land code (2 letter code) [NL]:
Locatie naam (bv, naam van de stad) []:
Organizational Unit Name (eg, section) []:
Common Name (zorginstelling-koppelpartner) []:
Email Adres []:
- in de directory is nu een .csr bestand aangemaakt

2. **Verstuur de aanvraag**

Stuur het gecreëerde .csr bestand naar GeriMedica (support@gerimedica.nl)

Let op: houdt het .key bestand uit de eerste stap voor uzelf: dit is de private key die u nooit moet overhandigen.

3. **Signen, configureren en terugzenden(GeriMedica)**

GeriMedica zal uw certificaat signen, binnen het Ysis systeem configureren, en het geautoriseerde certificaat naar u terugsturen.

4. **Registreren bij onze partner of klant**

Dit is afhankelijk van de koppeling en de software, hoe dit certificaat geconfigureerd moet worden. Neem hiervoor contact op met de software leverancier van het te koppelen pakket.

3.2 **GeriMedica toestaan de webservice van het andere zorgpakket aan te roepen**

Indien het andere zorgpakket ook de beveiliging middels client certificaten regelt werkt het proces nu andersom:

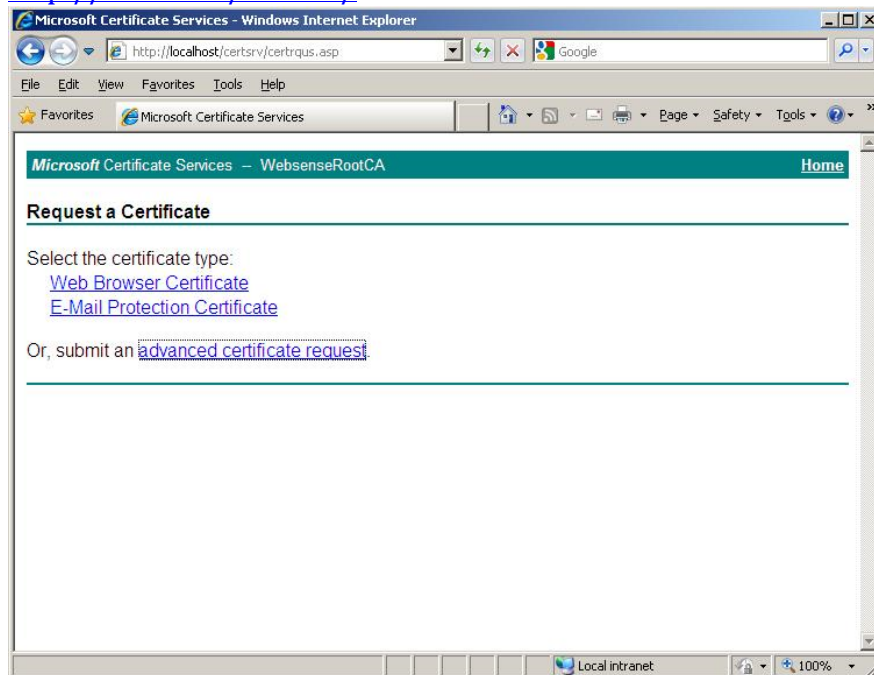
1. *U ontvangt een certificaat aanvraag van GeriMedica (.csr betand)*
2. *U moet deze vervolgens 'signen'*

Microsoft Windows:

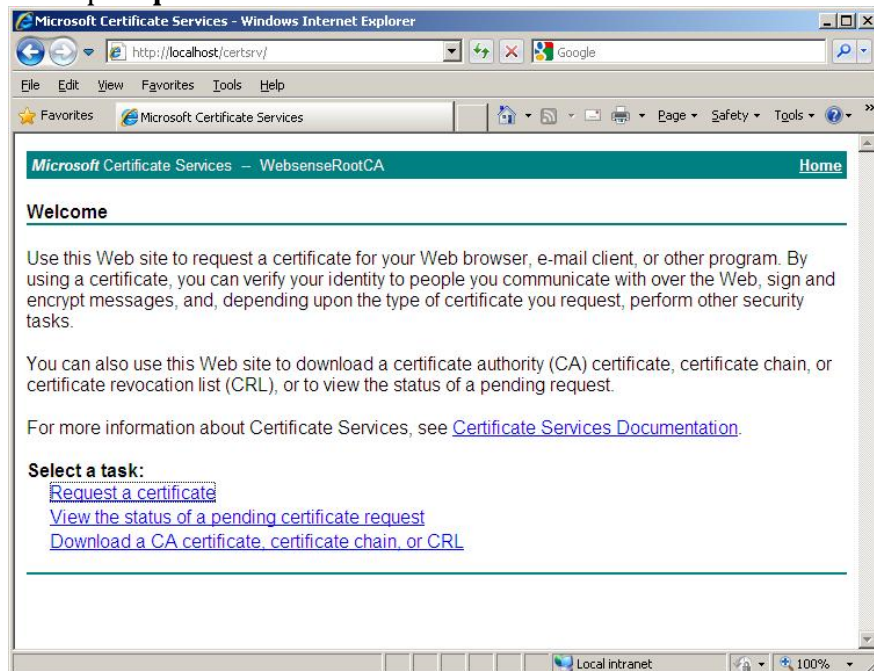
Wanneer u een Windows CA server heeft, kunt u met de volgende stappen volgen:

a) Op de windows CA server open een browser en ga naar:

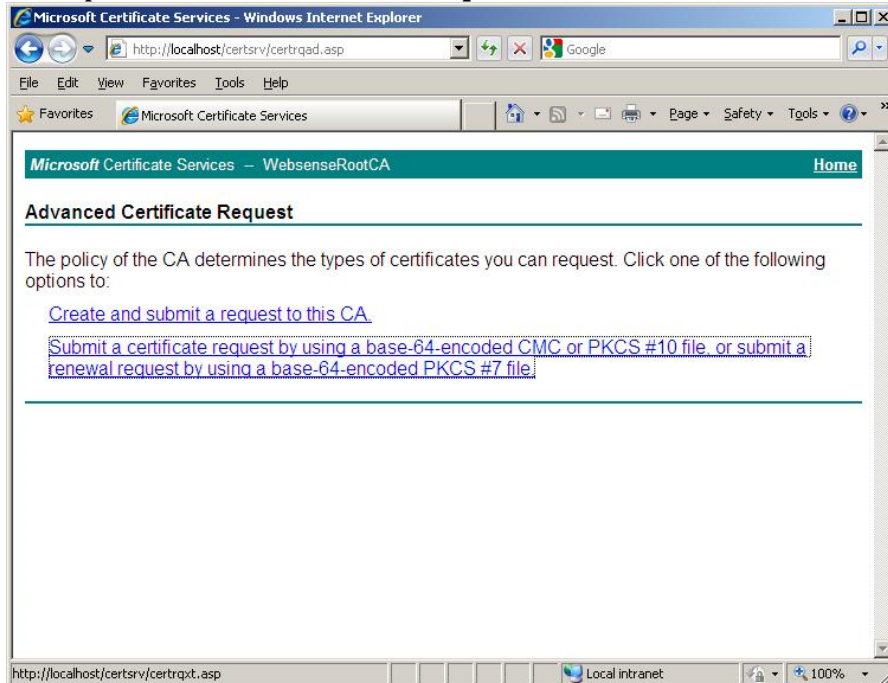
<http://localhost/certsrv/>



b) Klik op **request a certificate**



c) Klik op a **dvanced certificate request**



Microsoft Certificate Services - Windows Internet Explorer

http://localhost/certsrv/certrqad.asp

File Edit View Favorites Tools Help

Microsoft Certificate Services

Microsoft Certificate Services - WebsenseRootCA Home

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

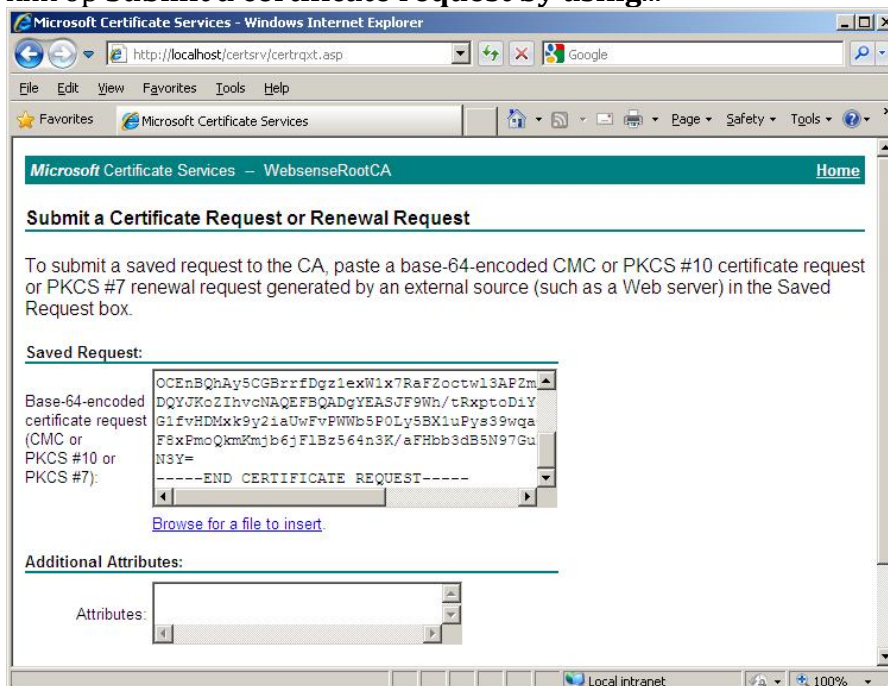
[Create and submit a request to this CA.](#)

[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file](#)

http://localhost/certsrv/certrqxt.asp

Local intranet 100%

d) klik op **Submit a certificate request by using...**



Microsoft Certificate Services - Windows Internet Explorer

http://localhost/certsrv/certrqxt.asp

File Edit View Favorites Tools Help

Microsoft Certificate Services

Microsoft Certificate Services - WebsenseRootCA Home

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):

OCEnBQhAySCGBrrfDgz1exW1x7RaFZoctw13AP2m
 DQYJKoZIhvcNAQEFBQADgYEAJF9Wh/tRxptoDiY
 G1fvHDMxk9y21aUwFvPWWb5P0Ly5BX1uFys39wqa
 F8xPmoQkmZmj6jF1Bz564n3K/aFHbb3dBSN97Gu
 NSY=
 -----END CERTIFICATE REQUEST-----

[Browse for a file to insert](#)

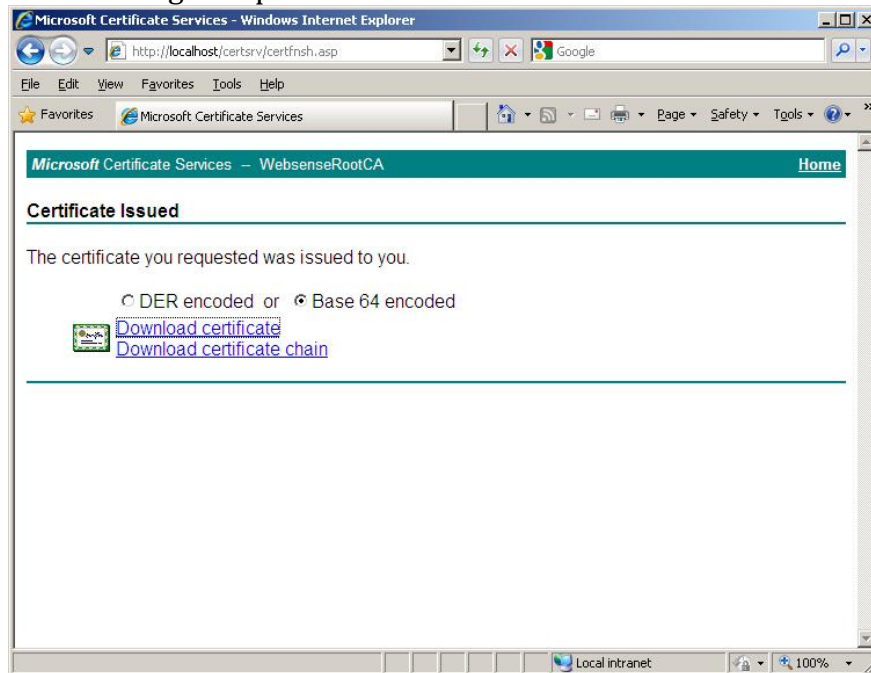
Additional Attributes:

Attributes:

Local intranet 100%

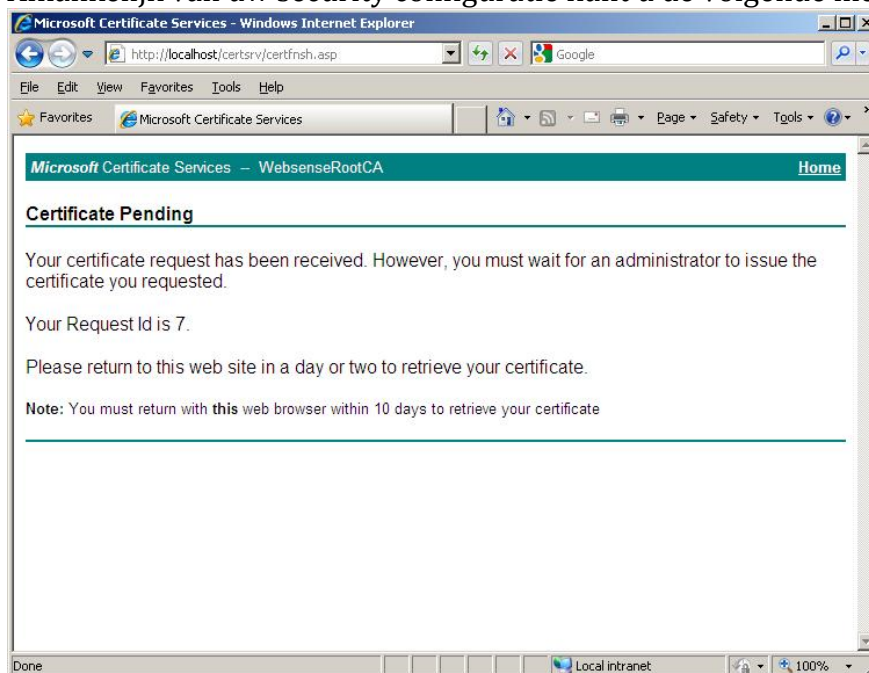
e) in het veld naast Base-64-encoded... moet of in het textveld de inhoud van het aan u toegestuurde CSR worden worden geplakt of kies **browse for a file to insert**

f) Click vervolgens op **submit**



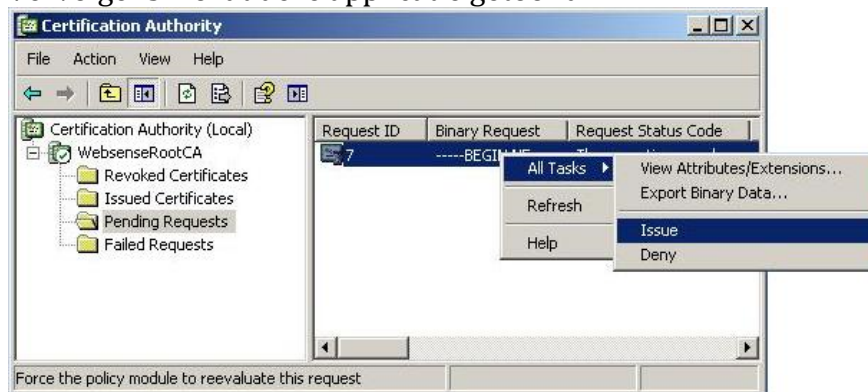
g) Download het certificaat en stuur deze op.

Afhankelijk van uw security configuratie kunt u de volgende melding krijgen:



In dit geval moet u de volgende aanvullende stappen uitvoeren:

- a) Ga naar Start -> uitvoeren. En typ '**certsrv.msc**' (gevolgd door een enter). Vervolgens wordt deze applicatie getoond:



- b) Ga naar **pending certificates**, en kies de juiste entry op basis van het Request ID Middels de rechter muisknop - > **all tasks** -> **issue**. De entry verdwijnt, deze staat nu in **issued certificates**.
- c) selecteer het certificaat en kies **open** Ga vervolgens naar het tabblad **details** en kies **copy to File..** Kies voor **DER** encoded en een naam voor het certificaat.
- d) Stuur het bestand naar Gerimedica.
3. *Registreer dit certificaat in uw eigen systeem.*
Dit kunt u doen door het bestand simpelweg te dubbelklikken.
4. *Verstuur dit geautoriseerde certificaat aan GeriMedica (support@gerimedica.nl)*
GeriMedica zal dit gebruiken voor het configureren van de koppeling in Ysis. U ontvangt bericht zodra dit is gedaan en de koppeling beschikbaar is voor testen.