



Vlaamse
overheid

Toegangsbeheer

Aanvragen VO-DCB
Certificaten voor ACM



Introductie

Certificaten?

- ▶ Binnen de Vlaamse overheid, en tussen de Vlaamse overheid en externe partijen (zoals lokale besturen), dienen vaak gegevens op een beveiligde manier uitgewisseld te worden.
- ▶ Digitale certificaten kunnen hierbij een belangrijke rol spelen, bv. voor het opzetten van een versleuteld communicatiekanaal (encryptie) of voor het handtekenen (signing) van berichten die uitgewisseld worden (controle van integriteit en onweerlegbaarheid).
- ▶ Voor SAML-integraties met het Toegangsbeheer zijn certificaten vereist (naast de https-ondersteuning):
 - Eén voor signing, één voor encryptie
 - Verschillend certificaat voor signing dan voor encryptie
 - Het Toegangsbeheer ondersteunt geen self-signed certificaten
 - De certificaten dienen van de VO zelf of van publieke (commerciële) CA afkomstig te zijn

Certificaten?

- ▶ Vlaamse entiteiten en lokale besturen kunnen gebruik maken van Vlaamse Certificatendienst.
 - Deze dienst garandeert een kwalitatieve registratie, een lage instapdrempel en een minimale kost.
- ▶ Voor algemene informatie over het Vlaams certificatenbeheer:
 - <https://overheid.vlaanderen.be/ict/ict-diensten/certificatendienst-vlaamse-overheid>
 - https://overheid.vlaanderen.be/sites/default/files/eIB_documents/Certificatendienst_DIENSTENFICHE.pdf (PDF)

Benodigde Certificaten

▶ Beveiliging van het transport (HTTPS)

- Dit certificaat wordt gebruikt om het verkeer tussen de client en de webserver te beveiligen.
- Indien de webserver benaderd zal worden door niet-Vo computers is het aan te raden hiervoor een commercieel certificaat aan te kopen dat door alle (ondersteunde) browsers vertrouwd wordt.

▶ Signing Certificaat

- Wanneer de Service Provider een Authentication Request naar de Identity Provider stuurt, dient deze de aanvraag te ondertekenen met een Signing Certificaat.
- Met deze handtekening kan de IDP de oorsprong van de aanvraag valideren.

▶ Encryptie Certificaat

- De SAML Assertion wordt geëncrypteerd met het Encryptie Certificaat van de Service Provider.

Terminologie

- ▶ Identity Provider (IDP)
De partij die de gebruiker authentiseert. In de context van deze presentatie nemen we aan dat dit het Toegangsbeheer (ACM) is.
- ▶ Service Provider (SP)
De integrerende toepassing.
- ▶ SAML Authentication Request
De aanvraag die door de Service Provider naar de Identity Provider gestuurd wordt om een gebruiker te laten authentifieren.
- ▶ SAML Assertion
Het onderdeel van de SAML Response waarin attributen met betrekking tot de geauthentiseerde gebruiker worden meegegeven, deze attributen bevatten bijv.: naam, voornaam,...

Terminologie

▶ VO-DCB

Vlaamse overheid Digitale Certificaten Beheer. VO-DCB is de web-toepassing die een 'Certificatenbeheerder' gebruikt om een CSR op te laden, en nadien het certificaat te downloaden. VO-DCB laat ook toe een certificaat in te trekken (revoken).

<https://certificatenbeheer.vlaanderen.be>

▶ CSR

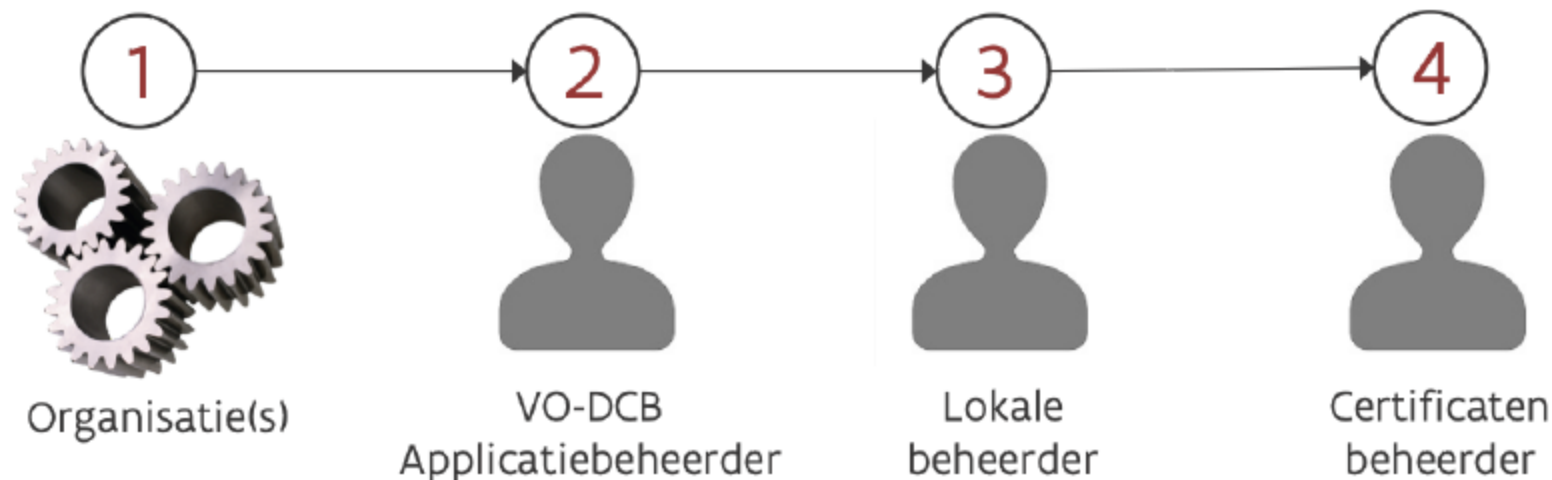
Certificate Signing Request, het bestand dat opgeladen wordt in VO-DCB. Deze bevat o.a. een public key en de CN (Common Name).

▶ Common Name (CN)

De naam die in het certificaat wordt opgenomen om de (instantie van de) toepassing die gebruik maakt van het certificaat te identificeren.

Aanvragen

Aanvraagprocedure



- Een organisatie heeft certificaten nodig en VO Certificaten zijn inzetbaar
- Afspraak rond naamgeving 'Common Name'
- CN wordt aangevraagd

CN wordt klaargezet in VO-DCB, voor de entiteit die het certificaat gaat gebruiken

Generiek contactadres :
vodcb@vlaanderen.be

De lokale beheerder (van de entiteit die het certificaat gaat gebruiken) past in Gebruikersbeheer het recht 'VO-DCB Certificatenbeheerder' aan

De Certificatenbeheerder laadt in VO-DCB een CSR op, en downloadt zelf het certificaat.

Stap 1: Organisatie

SSL Certificaat (HTTPS)

► **Formaat**

- **CN**=<FQDN>
- **E**=<generiek emailadres>
- **OU**=<Entiteit>
- **O**=Vlaamse overheid
- **L**=Brussel
- **ST**=Vlaams-Brabant
- **C**=BE

► **Voorbeeld**

- **CN**=testapplicatie.vlaanderen.be
- **E**=testapplicatie@kb.vlaanderen.be
- **OU**=Het Facilitair Bedrijf
- **O**=Vlaamse overheid
- **L**=Brussel
- **ST**=Vlaams-Brabant
- **C**=BE

Stap 1: Organisatie

Encryptie/Signing Certificaat

► **Formaat**

- **CN**=<Entiteit + "/" + Naam Applicatie + "-saml-" + Signing en/of Encryptie + "-" + T&I of PRD>
- **E**=<generiek emailadres>
- **OU**=<Entiteit>
- **O**=Vlaamse overheid
- **L**=Brussel
- **ST**=Vlaams-Brabant
- **C**=BE

► **Voorbeeld**

- **CN**=hetfacilitairbedrijf.be/hfbservicedesk-saml-sign-test
- **E**=testapplicatie@kb.vlaanderen.be
- **OU**=Het Facilitair Bedrijf
- **O**=Vlaamse overheid
- **L**=Brussel
- **ST**=Vlaams-Brabant
- **C**=BE

► "Purpose" van het certificaat: CLIENT + SIGNING

- Dient vermeld te worden wanneer de CSR wordt doorgestuurd ter ondertekening

Stap 2: VO-DCB Applicatiebeheerder

Toevoegen CN in VO-DCB

- ▶ De certificaatbeheerder van de organisatie vraagt via vodcb@vlaanderen.be aan om de nieuwe CN toe te voegen in VO-DCB.

Stap 3: Lokale beheerder

Aanpassen Certificatenbeheerder

- ▶ De Lokale Beheerder van de organisatie past in het Gebruikersbeheer het recht 'VO DCB - Certificaten Beheerder' aan.
- ▶ De Lokale beheerder selecteert de nieuw aangevraagde CN in het gebruikersrecht en bevestigt de keuze.

OrganisationName:

Organisatie code:

Categorie: Vlaamse Overheid Ambtenaar

Gebruikerstype: Geprivilegeerde accounts

Gebruikersrecht: VO DCB - Certificaten Beheerder

Omschrijving van het recht: Dit gebruikersrecht geeft een toegang tot het VO-DCB met de rol Certificaten Beheerder.

*Begindatum (dd/mm/jjjj):

*Einddatum (dd/mm/jjjj):

*Context: Type certificaat

Naam in certificaat

(FQDN / Common Name)

Keuze:

Stap 4: Certificatenbeheerder

Aanmaken Private Key + CSR

- ▶ Dit wordt rechtstreeks op de applicatie server uitgevoerd.
- ▶ De CSR kan ofwel via IIS Management Console op een Windows Server aangemaakt worden of via OpenSSL in Linux (zie commando's op de volgende slides)
- ▶ **Technische vereisten:**
 - **Keysize:** 4096bit
 - **Algoritme:** SHA 256
 - **Geldigheidsperiode:** 5jaar (3jaar indien 2048bit)

Stap 4: Certificatenbeheerder

OpenSSL Private Key + CSR

Lees grondig na in de openssl documentatie wat hier eigenlijk staat! Onderstaande kan je niet letterlijk overnemen.

► OpenSSL voorbeeld aanvraag SSL certificaat

```
C:\test>openssl req -new -newkey rsa:4096 -nodes -x509 -subj "/C=BE/ST=Vlaams-Brabant/L=Brussel/O=Vlaamse overheid/OU=Beheerders/ntiteit/>emailAddress=<generiek emailadres>/CN=<FQDN>" -keyout private.key -out certificate_request.csr
Generating a 4096 bit RSA private key
.....++
.....
.....++
writing new private key to 'private.key'
-----
```

► Voorbeeld:

→ openssl req -new -out test.csr -newkey rsa:4096 -nodes -keyout test.key -subj "/CN=hfb.be/app1-test/O=Vlaamse overheid/OU=Het Facilitair Bedrijf/emailAddress=functionelemailbox@vlaanderen.be/C=BE"

Stap 4: Certificatenbeheerder

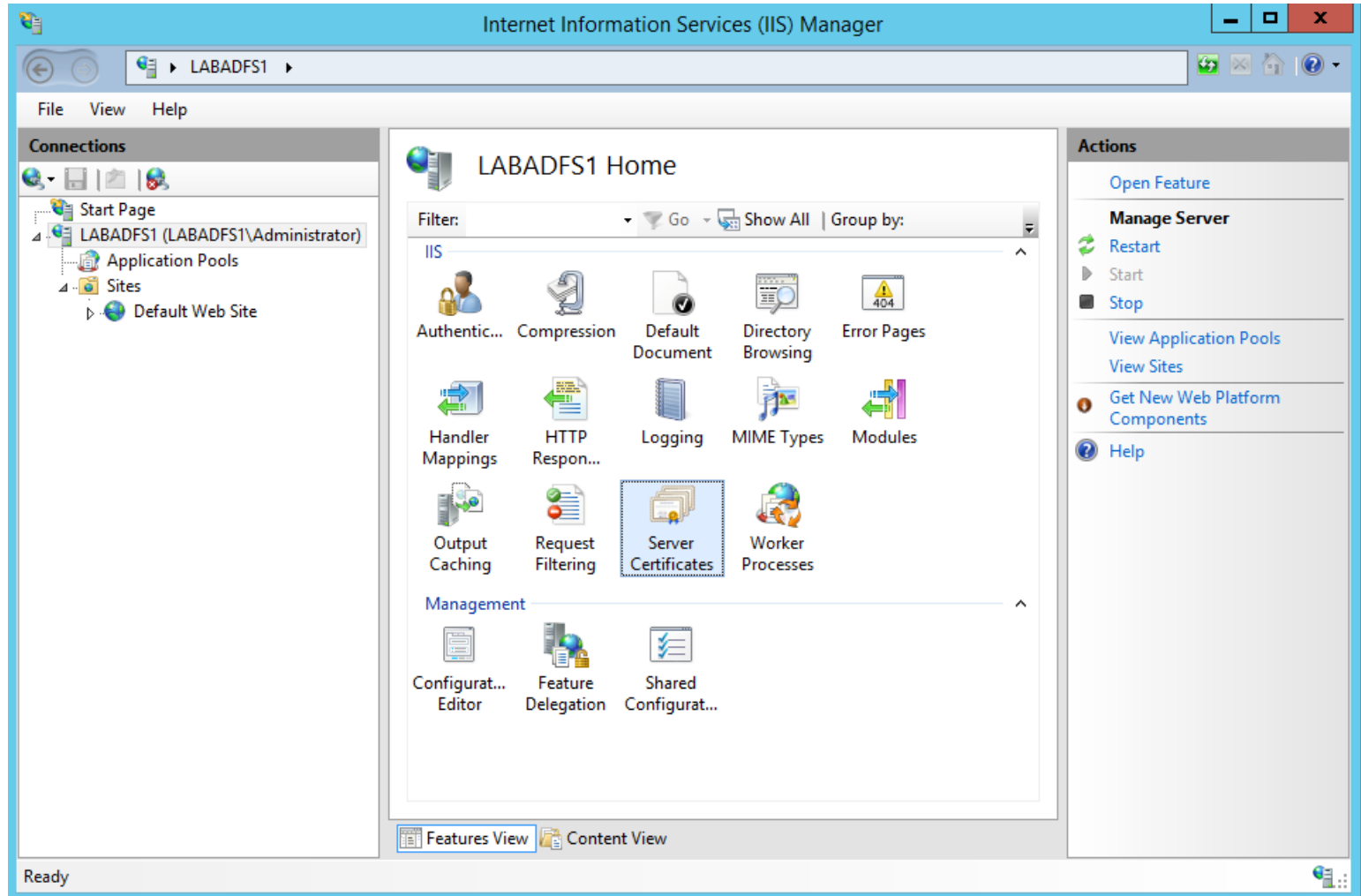
OpenSSL Private Key + CSR

- ▶ Na het uitvoeren van dit commando worden 2 bestanden gegenereerd:
 - Private.key
 - certificate_request.csr
- ▶ Het bestand certificate_request.csr dient opgeladen te worden in VO-DCB door de certificatenbeheerder. Nadien kan de certificatenbeheerder het bijhorende getekende certificaat downloaden

Stap 4: Certificatenbeheerder

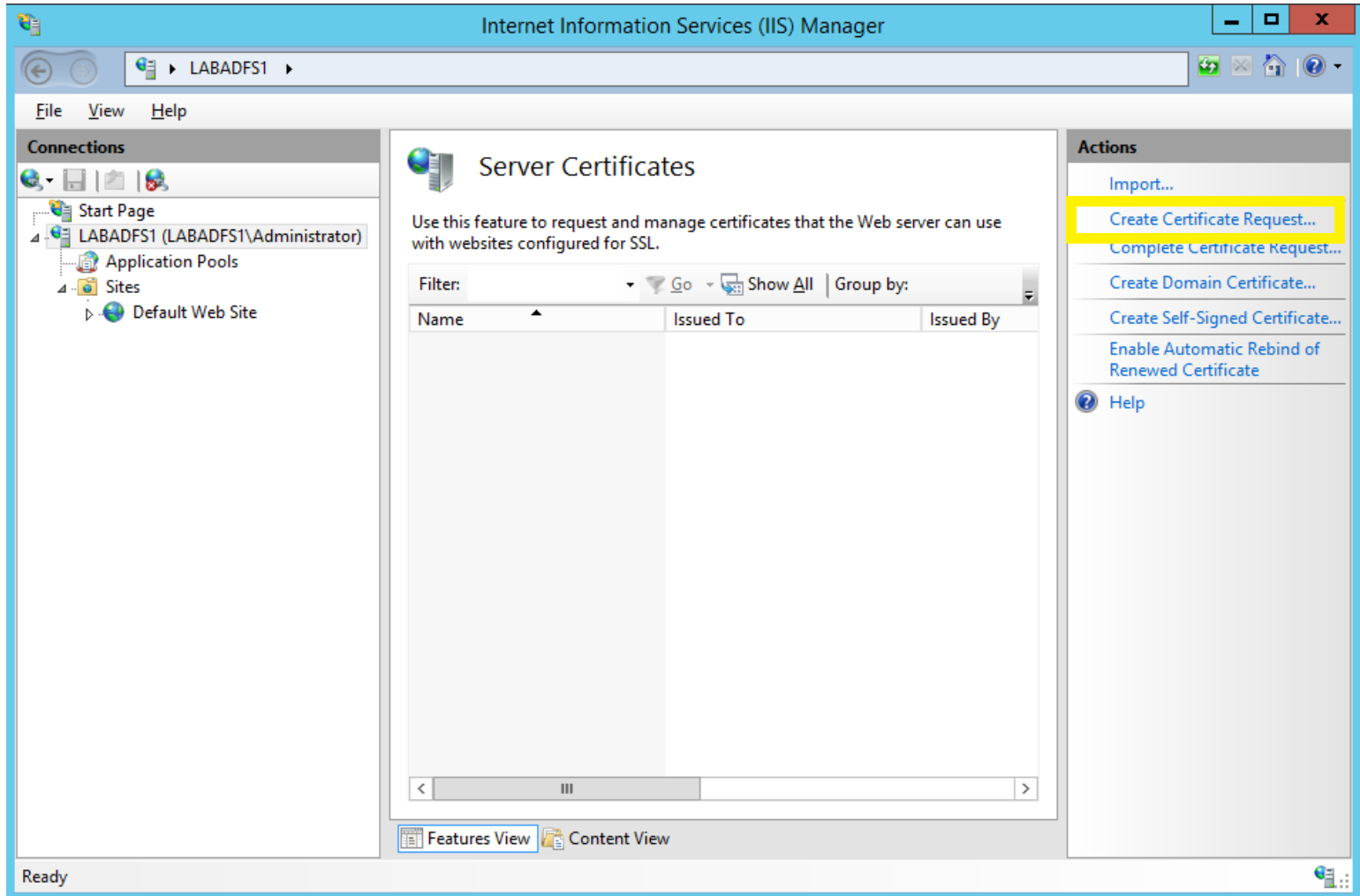
IIS Management Console

Lees na in de IIS documentatie wat hier eigenlijk staat! Dit kan je niet as is overnemen.



Stap 4: Certificatenbeheerder


IIS Management Console



Stap 4: Certificatenbeheerder

IIS Management Console

Request Certificate

 **Distinguished Name Properties**

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.


Common name:	<input type="text" value="testapplicatie.vlaanderen.be"/>
Organization:	<input type="text" value="Vlaamse overheid"/>
Organizational unit:	<input type="text" value="Het Facilitair Bedrijf"/>
City/locality	<input type="text" value="Brussel"/>
State/province:	<input type="text" value="Vlaams-Brabant"/>
Country/region:	<input type="text" value="BE"/>

Previous Next Finish Cancel

Stap 4: Certificatenbeheerder

IIS Management Console

Request Certificate

 **Cryptographic Service Provider Properties**

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Microsoft RSA SChannel Cryptographic Provider

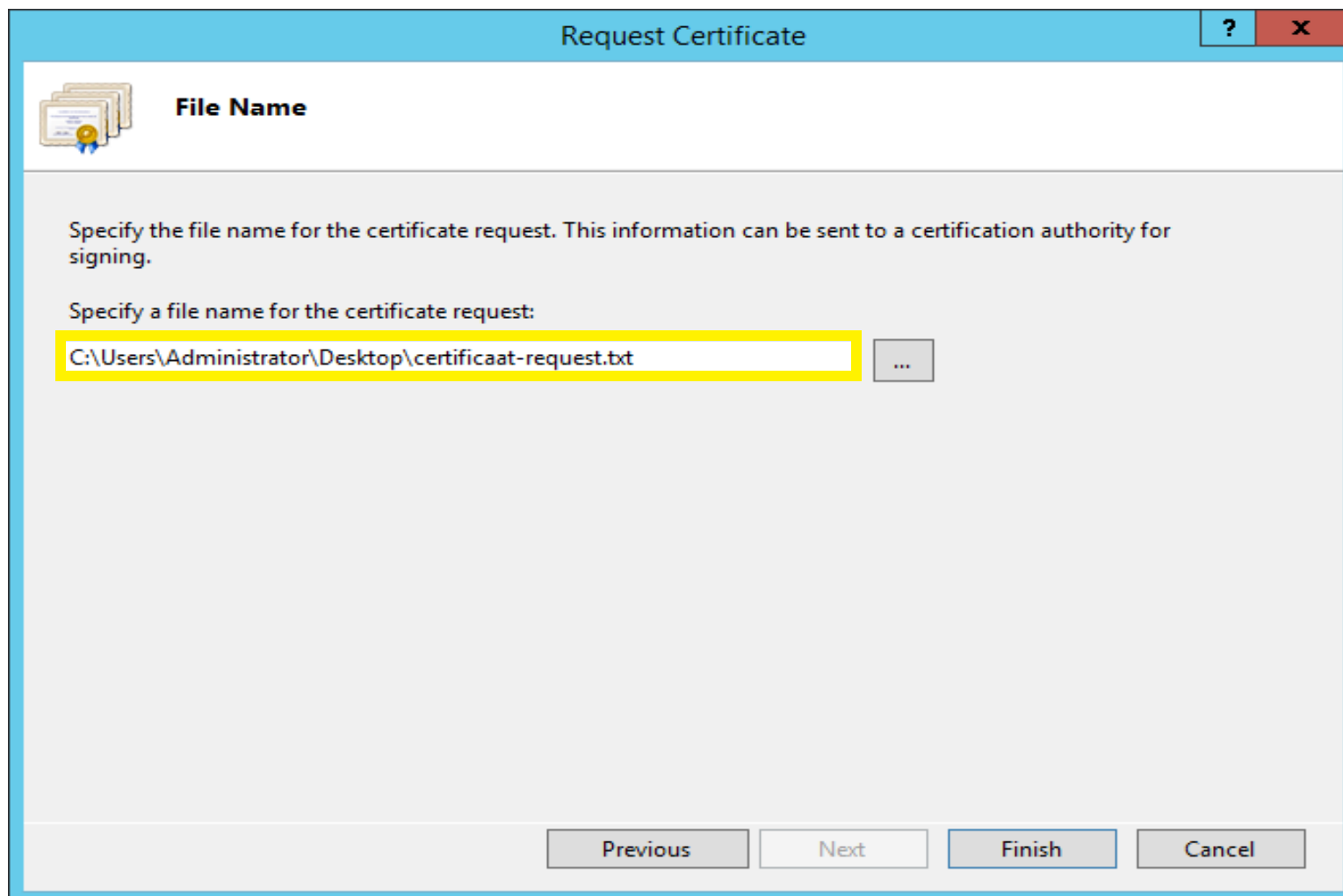
Bit length:

4096


Previous Next Finish Cancel

Stap 4: Certificatenbeheerder

IIS Management Console



Request Certificate

 **File Name**

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

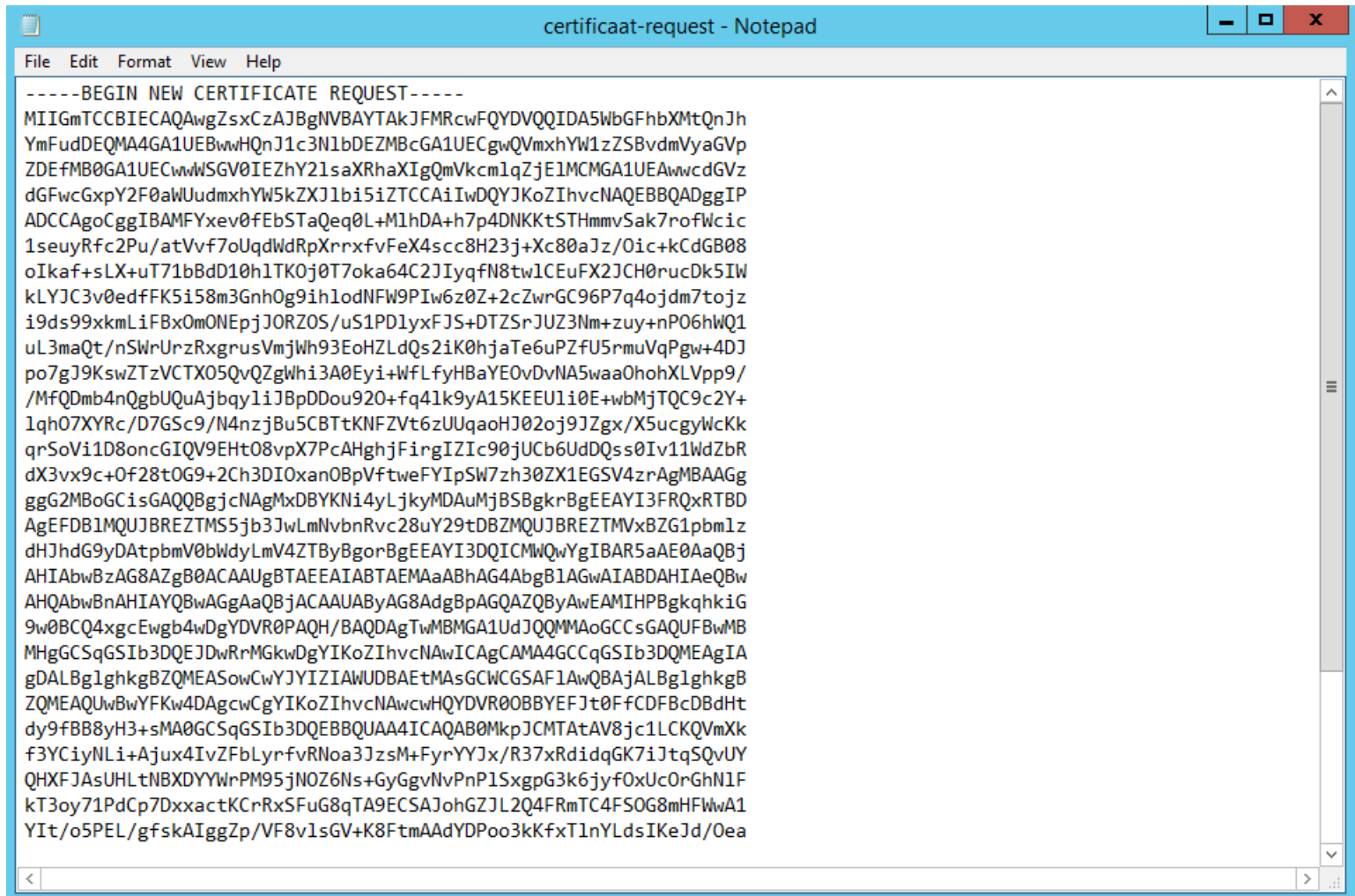
Specify a file name for the certificate request:

...

Previous Next Finish Cancel

Stap 4: Certificatenbeheerder

IIS Management Console

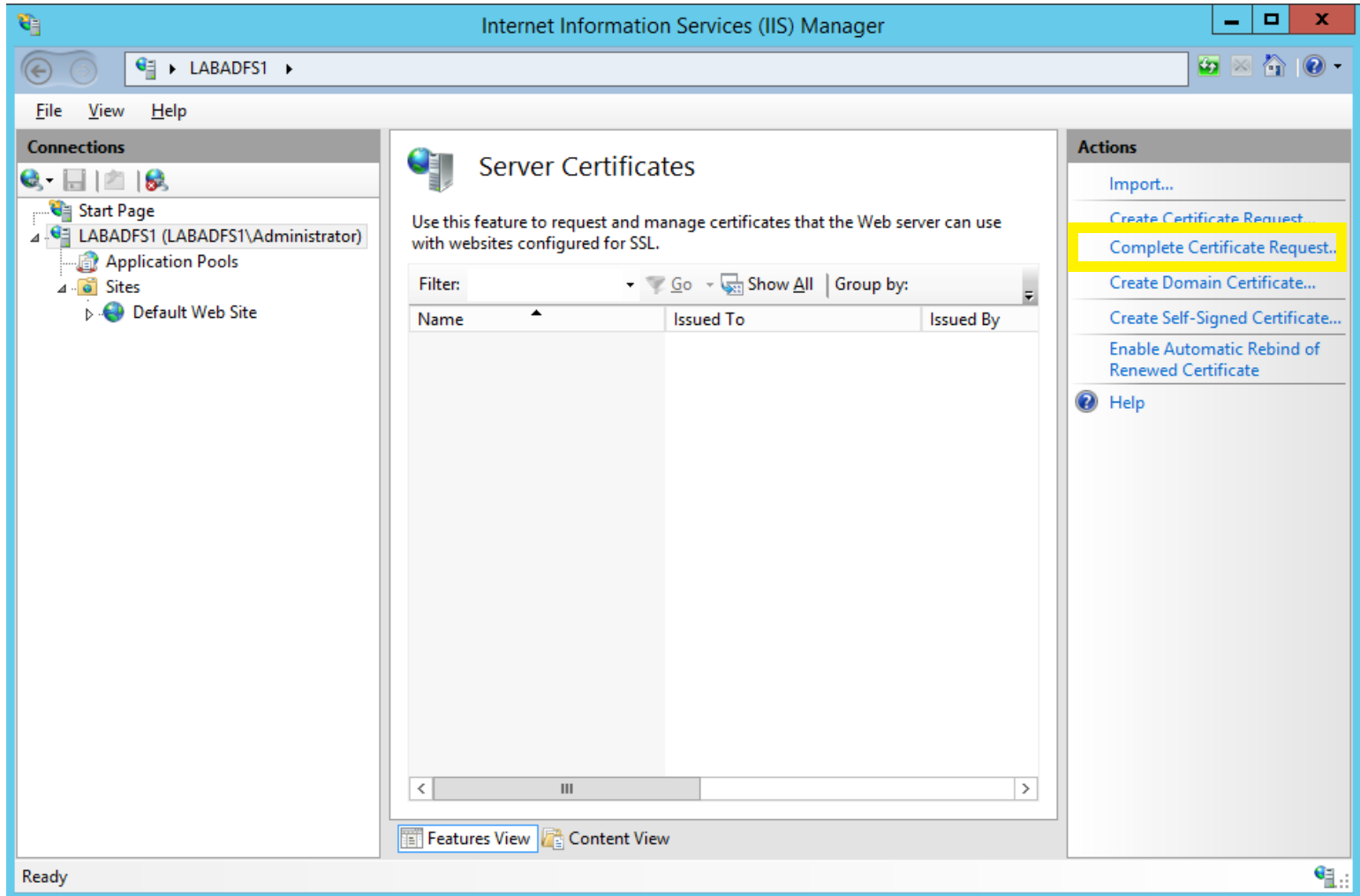


```
certificaat-request - Notepad
File Edit Format View Help
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIGmTCCBIECAQAwZSxCzAJBgNVBAYTAKJFMRcwFQYDVQQIDA5WbGFhbXMtQnJh
YmFudDEQMA4GA1UEBwwHQnJ1c3N1bDEZMBcGA1UECgwQVmxhYW1zZSBvdmVyaGVp
ZDEFM0GA1UECwwWSGV0IEZzY21saXRhaXIgQmVkcmlqZjE1MCMGA1UEAwwcdGVz
dGFwcGxpY2F0aWUudmVhYXkZDjE1b15iZTCCAIwDQYJKoZIhvcNAQEBBQADggIP
ADCCAgocGgIBAMFYxev0fEbSTaQeq0L+M1hDA+h7p4DNKKtSTHmvSak7rofWcic
1seuyRfc2Pu/atVvf7oUqdWdRpXrrxfvFeX4scc8H23j+Xc80aJz/Oic+kCdGB08
oIkaF+sLX+uT71bBdD10h1TK0j0T7oka64C2JIyqfN8tw1CEuFX2JCH0rucDk5IW
kLYJC3v0edfFK5i58m3Gnh0g9ih1odNFW9PIw6z0Z+2cZwrGC96P7q4ojdm7tojz
i9ds99xkmLiFBx0mONEpjJ0RZOS/uS1PD1yxFJS+DTZSrJUJ3Nm+zuy+nPO6hWQ1
uL3maQt/nSwrUnzRxgrusVmJWh93EoHZLdQs2iK0hjaTe6uPZfU5rmuVqPgW+4DJ
po7gJ9KswZTzVCTX05vQZgWhi3A0Eyi+WfLfyHBaYE0vDvNA5waa0hohXLVpp9/
/MfQDmb4nQgbUQuAjbjy1iJBpDDou920+f4q1k9yA15KEEU1i0E+wbMjtQC9c2Y+
lqh07XYRc/D7G5c9/N4nzjBu5CBTtKNFZvt6zUUqaoHJ02oj9JZgx/X5ucgyWcKk
qrSoVi1D8oncGIQV9EHt08vpX7PcAHghjFingIZiC90jUCb6UdDQs0Iv11WdZbR
dX3vx9c+0f28t0G9+2Ch3DI0xan0BpVftweFYIpSW7zh30ZX1EGSV4zrAgMBAAGg
ggG2MBoGcisGAQQBggjcnAgMxDBYKNI4yLjkyMDAuMjBSBgkrBgEEAYI3FRQxRTBD
AgEFDB1MQUBREZTMS5jb3JwLmNvbRvc28uY29tDBZMQUBREZTMVxBZG1pbm1z
dHJhdG9yDAtpbmV0bWdyLmV4ZTByBgorBgEEAYI3DQICMwQwYgIBAR5aAE0AaQBj
AHIAbwBzAG8AZgB0ACAUAUgBTAEEAIABTAEAAABhAG4AbgB1AGwAIABDAHIAeQBw
AHQAbwBnAHIAyQwBwAGgAaQBjACAUAUABYAG8AdgBpAgQAZQByAwEAMIHPBgkqhkiG
9w0BCQ4xgcEwgb4wDgYDVR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCsGAQUFBwMB
MHgGCSqGSIb3DQEJJDRWRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQMEAgIA
gDALBg1ghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCGSAF1AwQBAjALBg1ghkgB
ZQMEAUwBwYFk4DAGcwCgYIKoZIhvcNAwIwYDVR00BBYEFJt0FfCDFBcDBdHt
dy9fBB8yH3+sMA0GCSqGSIb3DQEBBQUAA4ICAQAB0MkpJCMTAtAV8jc1LCKQVmxK
f3YCIyNLi+Ajux4IvZfBLyrFvRNoa3Jzsm+FyrYYJx/R37xRdidqGK7iJtqSQvUY
QHXFJAsUHLtNBXDYYWpPM95jNOZ6Ns+GyGgvNvPnP1SxgpG3k6jyf0xUcOrGhN1F
kT3oy71PdCp7DxxactKCrRxFuG8qTA9ECSAJohGZJL2Q4FRmTC4F50G8mHFwA1
YIt/o5PEL/gfskAIggZp/VF8v1sGV+K8FtmAAdYDPoo3kKfxT1nYLDsIKeJd/Oea
```

- ▶ Het gegenereerde bestand dient opgeladen te worden in VO-DCB

Stap 4: Certificatenbeheerder

IIS Management Console




- ▶ Opladen van het gedownloadde certificaat uit VO-DCB

Stap 4: Certificatenbeheerder

IIS Management Console

Complete Certificate Request

 **Specify Certificate Authority Response**

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

...

Friendly name:

Select a certificate store for the new certificate:

OK Cancel



Stap 4: Certificatenbeheerder



Aanmelden in VO-DCB



certificatenbeheer: Aanmelden

Kies manier van aanmelden

Kies hieronder hoe u wil aanmelden. Klik op "meer info" voor uitleg over die manier van aanmelden. Klik op de knop "hulp nodig?" (rechts) voor veelgestelde vragen over aanmelden of om contact op te nemen met de helpdesk.

> eID en aangesloten kaartlezer 
UW LAATSTE KEUZE
[Meer info](#) 

> VO-token (Vlaamse overheid) 
[Meer info](#) 

> Federaal token 
[Meer info](#) 

▶ <https://certificatenbeheer.vlaanderen.be>

▶ Beschikken over 'VO DCB - Certificaten Beheerder' in IDM

Stap 4: Certificatenbeheerder

Aanmelden in VO-DCB

Vlaamse overheid Digitaal Certi x +

https://certificatenbeheer-ti.vlaanderen

VO-DCB
Vlaamse overheid Digitaal Certificaat Beheer

Pieter Lenaerts | [uitloggen](#)
[Bookmark deze pagina](#)

Keuze Vertrouwde Instantie

Welkom Pieter Lenaerts,

Gebruik deze toepassing voor:

- het aanvragen van digitale certificaten uitgegeven door de 'Certificate Authority'(CA) van de Vlaamse overheid
- het registreren van digitale certificaten uitgegeven door andere CA's (FedICT, Globalsign, ...)

In geval u hulp nodig heeft

- Lees de [toelichting voor deze toepassing](#). Deze kan eveneens opgeroepen worden vanuit de verschillende schermen in de toepassing
- In geval er zich een onverwachte fout voordoet, stuur dan een schermafdruck met toelichting van de uitgevoerde actie naar VODCB@vlaanderen.be

Vooraleer verder te gaan, kies de 'Vertrouwde Instantie' voor dewelke u wenst certificaten te beheren gedurende deze sessie.

Keuze Vertrouwde Instantie: ⓘ

► Kies vertrouwde instantie

→ De organisatie waarvoor je een certificaat wil krijgen

Stap 4: Certificatenbeheerder

Hoofdscherm om certificaat aan te vragen

Vlaamse overheid Digitaal Certi X +

https://certificatenbeheer-ti.vlaanderen

VO-DCB
Vlaamse overheid Digitaal Certificaat: Beheer

Aangemelde gebruiker: Pieter Lenaerts
Vertrouwde instantie momenteel in beheer: Agentschap Facilitair Bedrijf
RA-portaal versie: 1.1.3 dd. 2016-06-29 10:34 | [uitloggen](#)
[Bookmark deze pagina](#)

Hoofdmenu beheer certificaten

Certificaat Aanvragen

Certificaat gegevens

Domeinnaam*: **Kies er een** 1

Type certificaat*: **Kies er een** 2

Geldigheidsduur*: **Kies er een** 3

CSR bestand

selecteer een CSR bestand (formaat PKCS#10)*:

Browse... **No file selected.** 4

Extra info

Beschrijving: (max 500 karakters)

Contactpersoon*

Email	Acties
<input type="text"/>	Voeg toe 6

Ik ben akkoord met de [CPS/CP](#) voor het gevraagde certificaat. 7

Certificaat aanvragen 8

1. Kies domeinnaam
 - Deze moet overeenkomen met de CN in de subject
2. Kies het type
 - Voor ACM: SSL CLIENT SIGNING
3. Kies een geldigheidsduur
4. Laad de CSR op

5. Geef minstens één email adres.
6. Klik op voeg toe.
7. Aanvaard de voorwaarden.
8. Klik op certificaat aanvragen

Stap 4: Certificatenbeheerder

Certificaat aanvragen

Certificaat gegevens

Domeinnaam*: 01.eib.vlaanderen.be
Type certificaat*: SSL Signing Client
Geldigheidsduur*: 62 maand

CSR bestand

selecteer een CSR bestand (formaat PKCS#10)*:
Browse... test.csr
CN=testvoorpieter1.hfb.be
O=Vlaamse overheid
OU=Het Facilitair Bedrijf
L=null
S=null
C=BE

Extra info

Beschrijving: (max 500 karakters)

Contactpersoon*

Email	Acties
gebruikersbeheer@vlaanderen.be	Voeg toe
gebruikersbeheer@vlaanderen.be	X

Ik ben akkoord met de [CPS/CP](#) voor het gevraagde certificaat.

Certificaat aanvragen

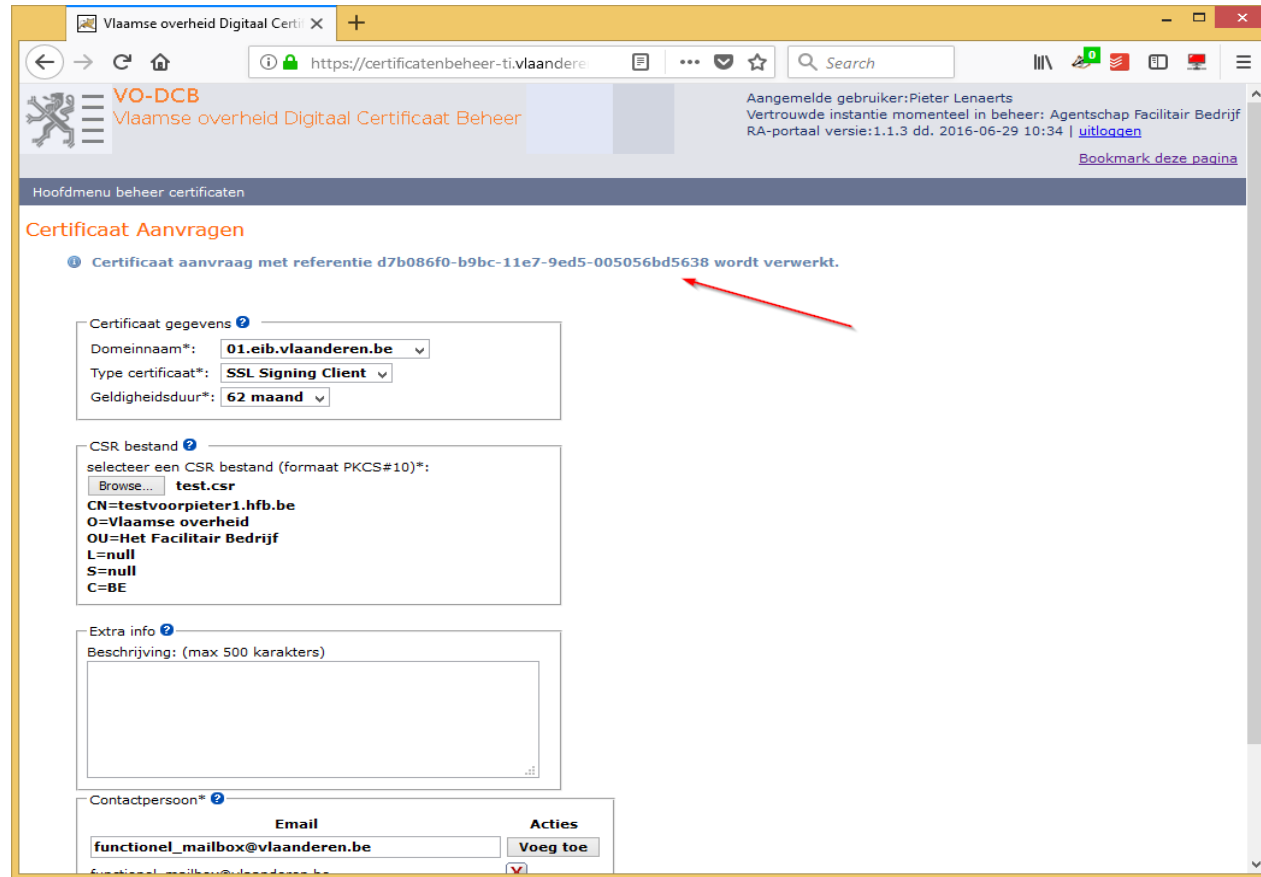
► Controleer alle velden

→ Domeinnaam moet kloppen

→ Certificaat moet van het type SSL signing client zijn

Stap 4: Certificatenbeheerder

Verwerking certificaataanvraag



The screenshot shows a web browser window with the URL <https://certificatenbeheer-ti.vlaanderen>. The page title is "VO-DCB Vlaamse overheid Digitaal Certificaat Beheer". The user is logged in as "Aangemelde gebruiker: Pieter Lenaerts" and the trusted institution is "Agentschap Facilitair Bedrijf". The page version is "RA-portaal versie: 1.1.3 dd. 2016-06-29 10:34".

The main content area is titled "Certificaat Aanvragen". A blue notification message at the top states: "Certificaat aanvraag met referentie d7b086f0-b9bc-11e7-9ed5-005056bd5638 wordt verwerkt." A red arrow points to this message.

Below the notification, there are three form sections:

- Certificaat gegevens:** Includes dropdowns for "Domeinnaam*" (01.eib.vlaanderen.be), "Type certificaat*" (SSL Signing Client), and "Geldigheidsduur*" (62 maand).
- CSR bestand:** Includes a "Browse..." button and a "test.csr" file. The CSR content is displayed as:
CN=testvoorpieter1.hfb.be
O=Vlaamse overheid
OU=Het Facilitair Bedrijf
L=null
S=null
C=BE
- Extra info:** Includes a text area for "Beschrijving: (max 500 karakters)".

At the bottom, there is a "Contactpersoon*" section with a table:

Email	Acties
functionel_mailbox@vlaanderen.be	Voeg toe
functionel_mailbox@vlaanderen.be	<input checked="" type="checkbox"/>

- ▶ Blauwe melding bovenaan vermeldt dat de aanvraag in verwerking is
- ▶ Klik niet nogmaals op 'aanvragen', want dan dien je een 2de aanvraag in
→ Indien toch gedaan, dan 1 certificaat revoked

Stap 4: Certificatenbeheerder

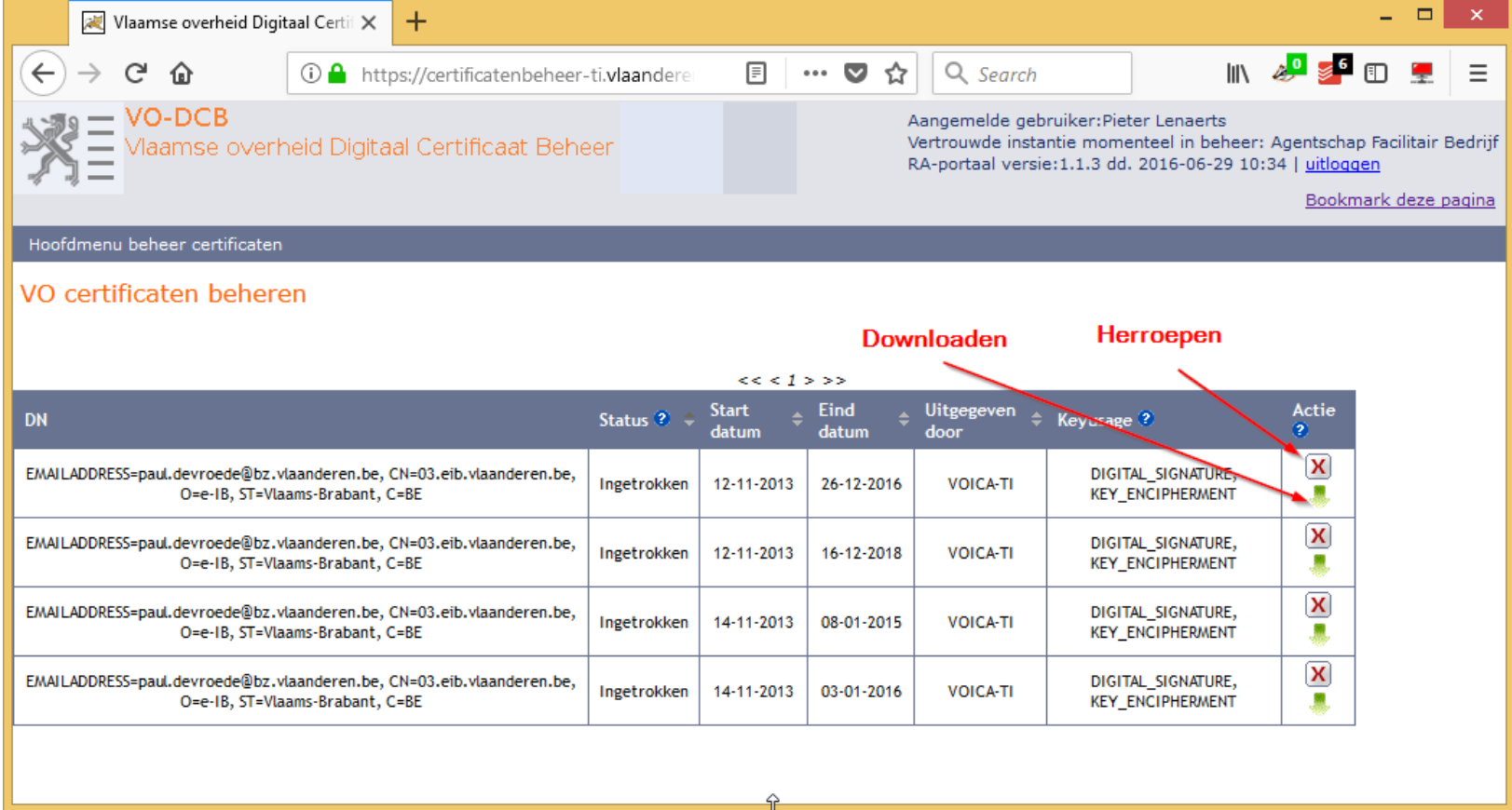
Certificaat downloaden/revoken

The screenshot displays the 'VO-DCB Vlaamse overheid Digitaal Certificaat Beheer' web application. The browser address bar shows the URL 'https://certificatenbeheer-ti.vlaanderen'. The page header includes the logo and name 'VO-DCB Vlaamse overheid Digitaal Certificaat Beheer' and user information for 'Aangemelde gebruiker: Pieter Lenaerts'. A navigation menu on the left has 'VO certificaten beheren' selected. The main content area shows a form for uploading a CSR file, with fields for 'testvoorpieter1.hfb.be', 'test.csr', and organizational details like 'Vlaamse overheid' and 'Het Facilitair Bedrijf'. There is also a 'Contactpersoon' section with an email field containing 'gebruikersbeheer@vlaanderen.be' and a 'Voeg toe' button.









- ▶ Ga naar 'VO certificaten beheren' om certificaten te downloaden/revoken

Stap 4: Certificatenbeheerder

Certificaat downloaden/revoken



The screenshot shows the 'VO-DCB Vlaamse overheid Digitaal Certificaat Beheer' web application. The user is logged in as 'Pieter Lenaerts'. The main menu includes 'VO certificaten beheren'. A table lists certificates with columns for DN, Status, Start datum, Eind datum, Uitgegeven door, Keyusage, and Actie. Red arrows point to the 'Downloaden' (green download icon) and 'Herroepen' (red X icon) actions in the 'Actie' column.

DN	Status	Start datum	Eind datum	Uitgegeven door	Keyusage	Actie
EMAILADDRESS=paul.devroede@bz.vlaanderen.be, CN=03.eib.vlaanderen.be, O=e-IB, ST=Vlaams-Brabant, C=BE	Ingetrokken	12-11-2013	26-12-2016	VOICA-TI	DIGITAL_SIGNATURE, KEY_ENCIPHERMENT	 
EMAILADDRESS=paul.devroede@bz.vlaanderen.be, CN=03.eib.vlaanderen.be, O=e-IB, ST=Vlaams-Brabant, C=BE	Ingetrokken	12-11-2013	16-12-2018	VOICA-TI	DIGITAL_SIGNATURE, KEY_ENCIPHERMENT	 
EMAILADDRESS=paul.devroede@bz.vlaanderen.be, CN=03.eib.vlaanderen.be, O=e-IB, ST=Vlaams-Brabant, C=BE	Ingetrokken	14-11-2013	08-01-2015	VOICA-TI	DIGITAL_SIGNATURE, KEY_ENCIPHERMENT	 
EMAILADDRESS=paul.devroede@bz.vlaanderen.be, CN=03.eib.vlaanderen.be, O=e-IB, ST=Vlaams-Brabant, C=BE	Ingetrokken	14-11-2013	03-01-2016	VOICA-TI	DIGITAL_SIGNATURE, KEY_ENCIPHERMENT	 

- ▶ Download het juiste certificaat.
- ▶ Herroep een certificaat als de sleutel gecompromitteerd werd, of als je meer dan één keer op aanvragen had geklikt.

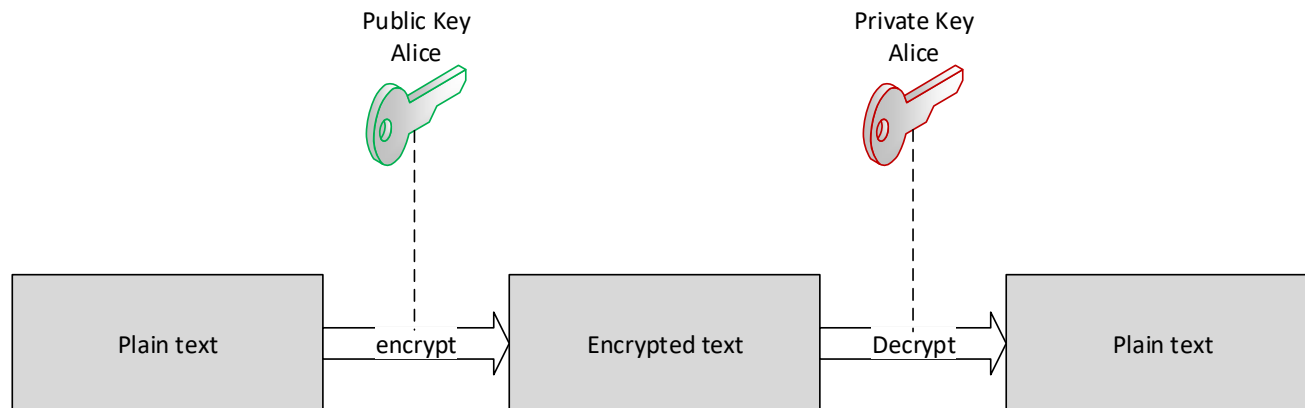
Annex: theoretische uitleg

Certificaten?

- ▶ Certificaten maken gebruik van Public key-Private key
- ▶ 2 sleutels met speciale verhouding
 - Private key: Nooit delen met andere mensen! Kan gebruikt worden om:
 - × Een ontvangend bericht te decrypteren
 - × Een te sturen bericht te tekenen (signing)
 - Public key: Mag gedeeld worden met iedereen. Kan gebruikt worden om:
 - × Een bericht voor de eigenaar van de public key te encrypteren
 - × Te valideren of een bericht afkomstig is van de eigenaar

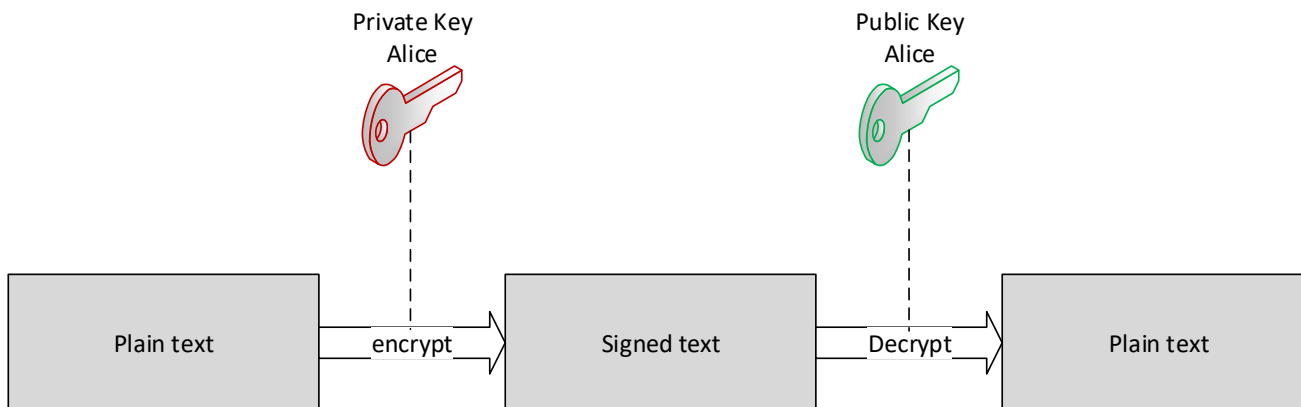
Voorbeeld Encryptie

- ▶ Alice deelt haar Public key uit aan haar vrienden, en houdt haar Private key voor zichzelf.
- ▶ Eén van haar vrienden encrypteert een bestand met de Public key van Alice.
- ▶ Nu kan enkel Alice het document decrypteren, aangezien zij als enige beschikt over de Private key.



Voorbeeld Signing

- ▶ Alice wil een document delen met andere personen, en wil bewijzen dat het document van haar afkomstig is.
- ▶ Alice encrypteert het document met haar Private key.
- ▶ Het document kan enkel gedecrypteerd worden met haar Public key (die met iedereen gedeeld is).
- ▶ Aangezien het gedecrypteerd kan worden met haar public key, is het document afkomstig van Alice.

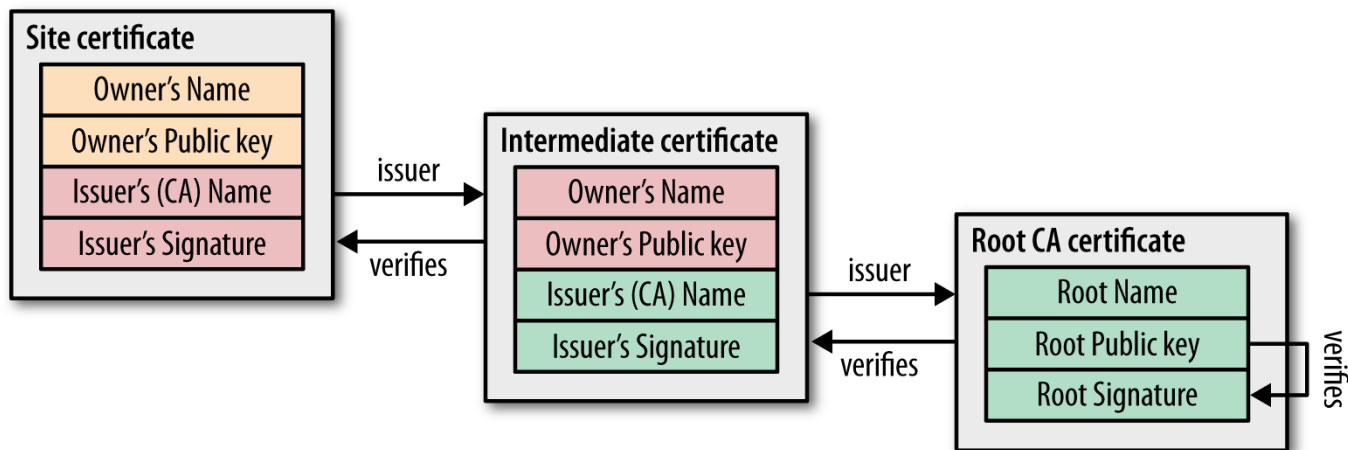


Trust

- ▶ Zolang alle Public keys op voorhand gekend zijn, is er geen probleem.
- ▶ MAAR: websites? Webservices? Daar hebben we toch geen Public key van?
- ▶ Als deze mee verstuurd worden met het bericht, hoe kunnen we die dan vertrouwen?
- ▶ Oplossing: Certificate Authorities
 - Vertrouwen wordt gegeven aan een aantal grote partijen, en zij tekenen/signen certificaten die zij vertrouwen.

Certificate Authorities

- ▶ Maken gebruik van signing om vertrouwen te garanderen:
 - Certificaat is gesigned door een intermediary CA, indien we de CA vertrouwen stopt de flow hier.
 - Indien niet vertrouwde intermediary CA, kijken we naar zijn signature. De intermediary CA is gesigned door een Root CA.
 - Indien we de root CA vertrouwen, vertrouwen we ook de intermediary CA, en het certificaat.



Inhoud Certificaat

- ▶ **Informatie over de eigenaar:**

- **CN**= Common Name

- **E**= Email – bij voorkeur een generiek adres ipv persoonlijk

- **OU**= Organizational Unit

- **O**= Organization

- **L**= Locality/City

- **ST**= State

- **C**= Country

- ▶ Public key

- ▶ CA signature

! Private key blijft op de server en zit niet in het certificaat, wordt niet meegedeeld

Contactinfo

- ▶ Online:

- <http://overheid.vlaanderen.be/gebruikersbeheer>

- <http://overheid.vlaanderen.be/toegangsbeheer>

- ▶ Miltje sturen?

- gebruikersbeheer@vlaanderen.be

- ▶ Ondersteuning via gratis nummer 1700