AGENTSCHAP
FACILITAIR BEDRIJF

HANDLEIDING VAN PRIVATE SLEUTEL TOT CERTIFICAAT

INHOUD

1 CERTIFICATEN AANMAKEN

1.1 Praktisch

Tool voor aanmaak private key en certificaat - XCA: https://hohnstaedt.de/xca/

Certificatenbeheer applicatie VO-DCBaaS: https://dcb.vlaanderen.be

Handleiding VO-DCBaaS: https://overheid.vlaanderen.be/publicaties-toegangs-en-gebruikersbeheer -> "Ik heb vragen over Vo-DCB of VoDCBaaS"

2 WAT HEB JE NODIG

Om een certificaat aan te vragen, maak je een Certificate Signing Request, of CSR, die je kan opladen in Vo-DCBaaS. Een CSR bevat je publieke sleutel en informatie over je organisatie, toepassing, contactgegevens,...

Om een CSR aan te maken, beschik je over:

- Een private sleutel: deze maken we aan in het stappenplan
- Minstens volgende informatie:
    - De Common Name of CN – doorgaans de domeinnaam of de naam van de toepassing of server waarvoor je een bepaald certificaat gebruikt
    - Je organisatienaam of organisatiecode
    - De landcode - deze is altijd 'BE'
- Optioneel:
    - Een e-mail adres dat Vo-DCBaaS kan gebruiken als contactgegeven
    - Subject Alternative Name of SAN

De gegevens die je invult, krijg je vaak vanuit de dienst die je aansluiting regelt. Raadpleeg deze informatie bij het aanmaken van een CSR, want ze zijn cruciaal voor de goede werking van het certificaat.

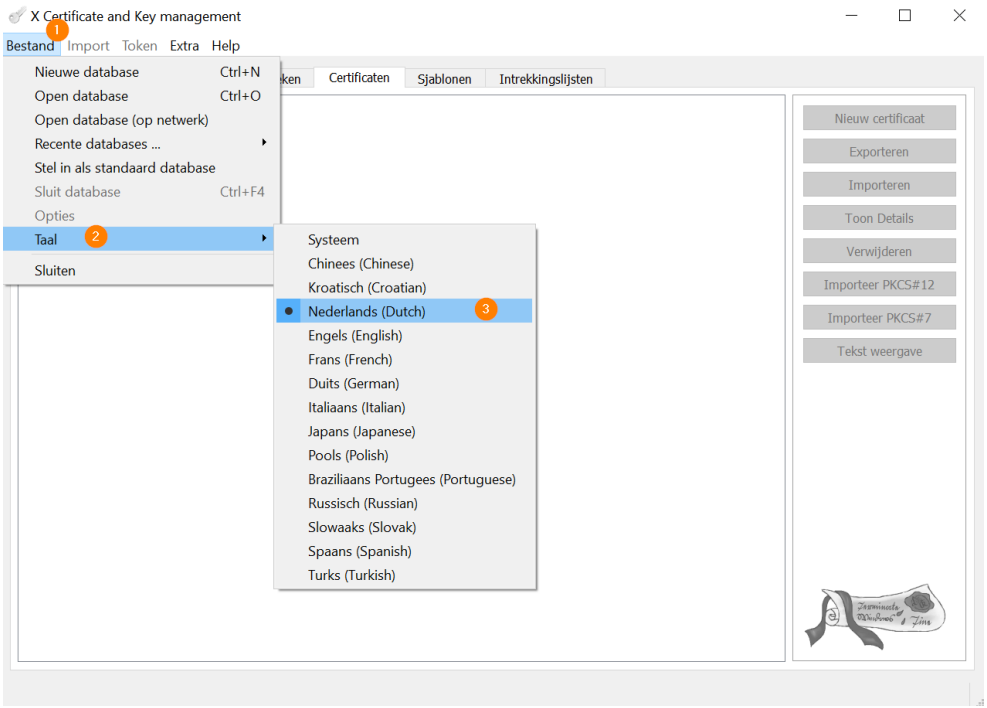
3 STAPPENPLAN

3.1 Installatie van de tool 'XCA'

Om een sleutelpaar, bestaande uit private en publieke sleutel, te genereren, maken we gebruik van XCA. Deze grafische tool maakt het aanmaken, beveiligen en beheren van een sleutelpaar eenvoudig.

Installeer deze tool op de computer waar later het certificaat zal gebruikt worden. Het is namelijk een goede praktijk dat **de private sleutel nooit de machine verlaat** waarop die aangemaakt werd.

1. Ga naar https://hohnstaedt.de/xca/ en kies 'Download'
2. Kies de meest recente versie voor jouw platform (linux, windows, mac).
   Tip: Vaak kan of mag je geen software installeren op de Windows computer waar je de sleutels aanmaakt, Kies in dat geval voor de XCA-portable versie die je kan downloaden en uitpakken zonder installeren
3. Download en installeer XCA
4. Open de toepassing
5. Optioneel: kies de gewenste taal. Deze handleiding bevat screenshots van de Nederlandstalige versie
   1. *Kies 'Bestand'*
   2. *Kies 'Taal'*
   3. *Kies 'Nederlands (Dutch)'*

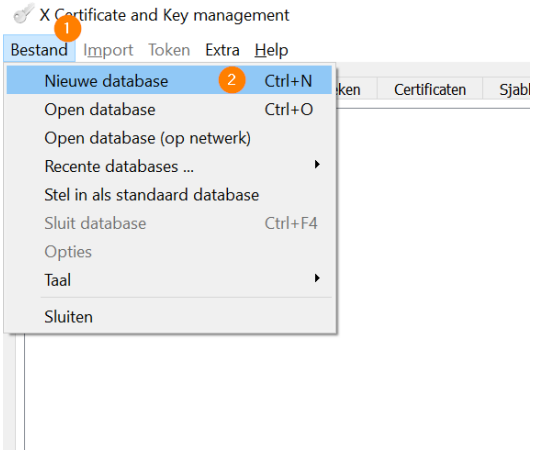


3.2 Een database aanmaken

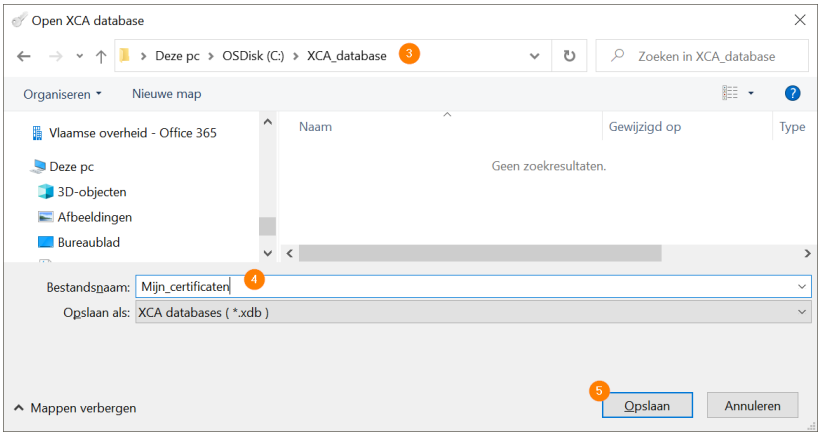
Voor we een sleutelpaar en een certificaat kunnen maken, moeten we een database aanmaken waar private sleutels, CSR's, certificaten, etc. kunnen bewaard worden.

1. Kies 'Bestand'

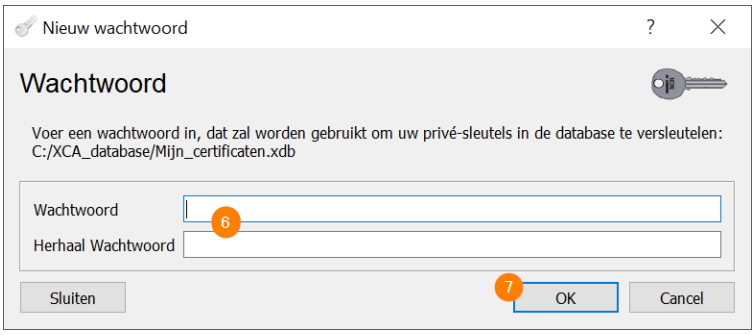
2. Kies ‘Nieuwe database’



3. Kies een locatie waar je de database wil opslaan
4. Geef je database een naam
5. Kies ‘Opslaan’



6. XCA zal je vragen een paswoord in te stellen om de private sleutel(s) te beschermen. Deze stap is optioneel maar ten zeerste aangeraden. Dit **paswoord moet je goed bewaren, anders kan je deze database met private sleutels niet meer gebruiken.**
7. Klik ‘OK’



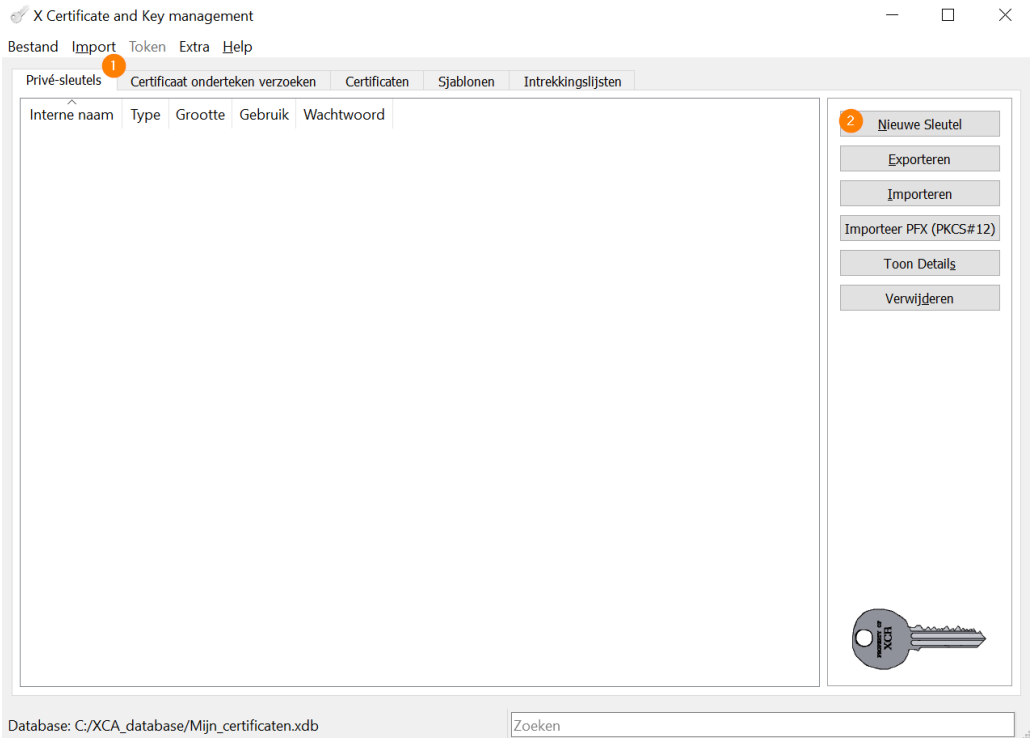
Je hebt nu een database aangemaakt waarbinnen we een private sleutel en later een CSR kunnen genereren en opslaan

3.3 Een private sleutel aanmaken

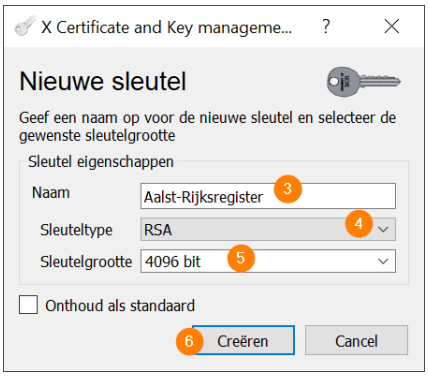
De private sleutel is een reeks tekens, berekend met behulp van een wiskundig algoritme. De sleutel heeft een bepaalde lengte en hoe langer die is, hoe sterker de sleutel, dus hoe moeilijker te kraken. Vo-DCBaaS raadt aan sleutel met een lengte van 4096bit te gebruiken.

Een private sleutel is het startpunt om een CSR aan te maken.

1. Kies de tab 'Privé-sleutels'
2. Kies 'Nieuwe sleutel'



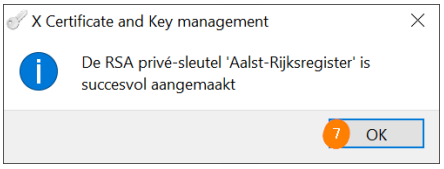
3. Geef je sleutel een (zinvolle) naam
4. Kies als 'Sleuteltype': **'RSA'**
5. Kies als 'Sleutelgrootte': '**4096 bit'**[1]
6. Klik op 'Creëren'



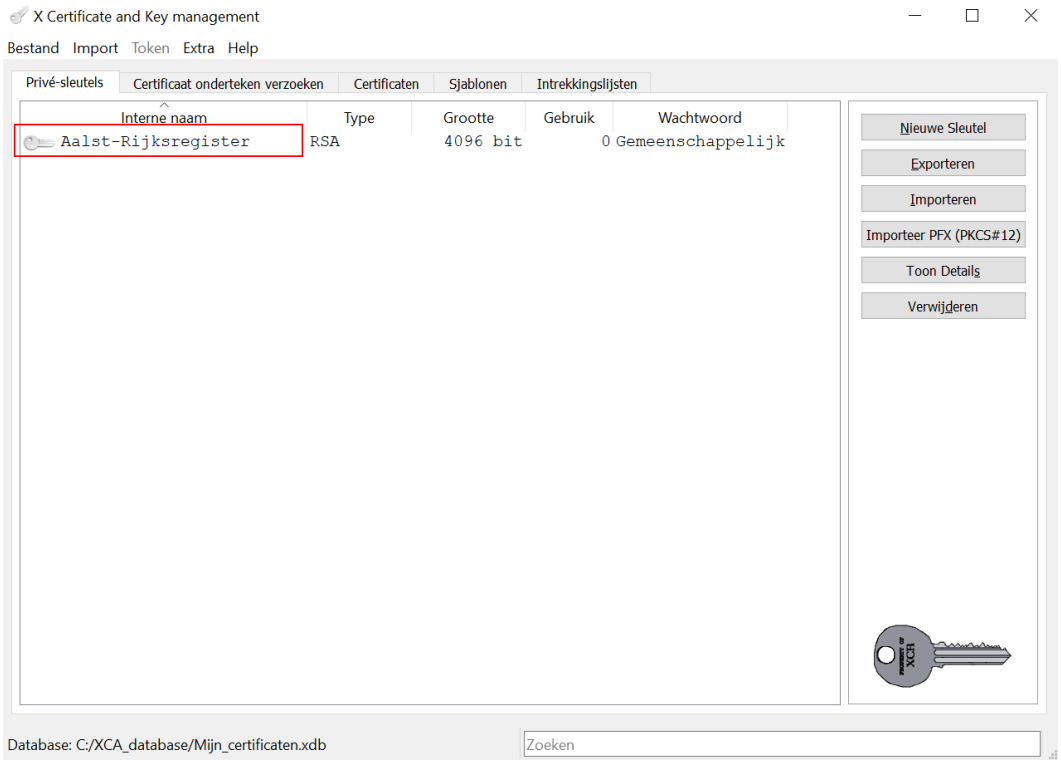
[1] 4096 bit is de standaard binnen Vo-DCBaaS. We ondersteunen ook 2048 bit. Dat is een zwakkere sleutel. Gebruik deze enkel als een 4096 bit sleutel niet ondersteund wordt door je toepassing

XCA maakt nu je sleutel aan en geeft een bericht als dat proces klaar is

7. Kies ‘OK’



Je private sleutel is nu zichtbaar in het overzicht van je sleutels

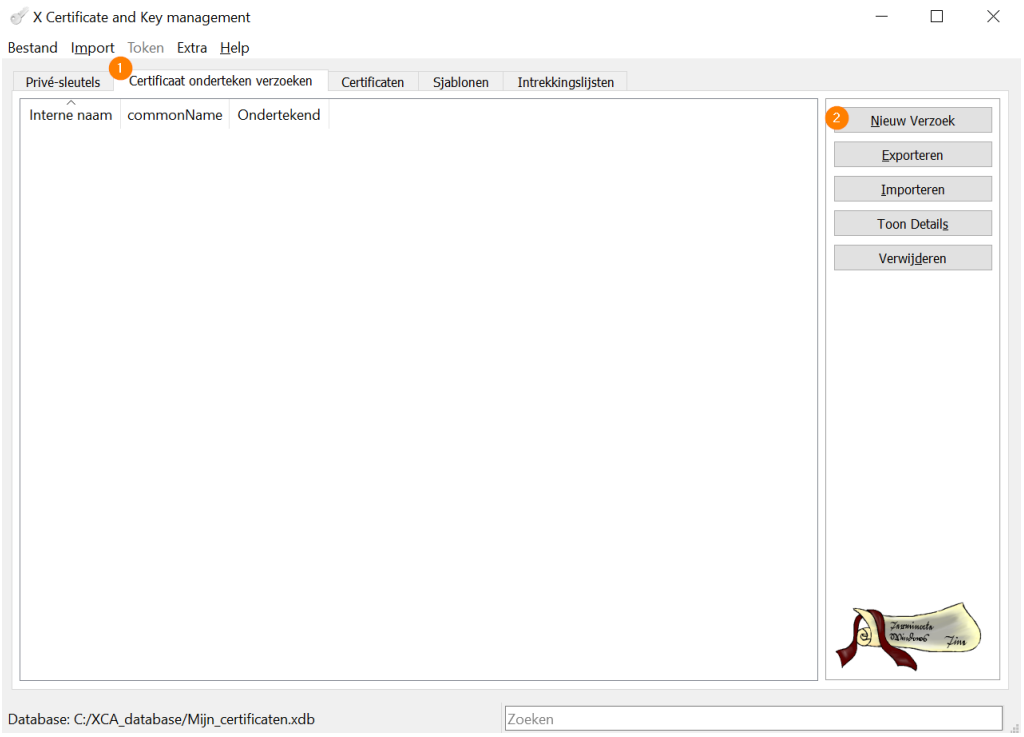


3.4 Een CSR aanmaken

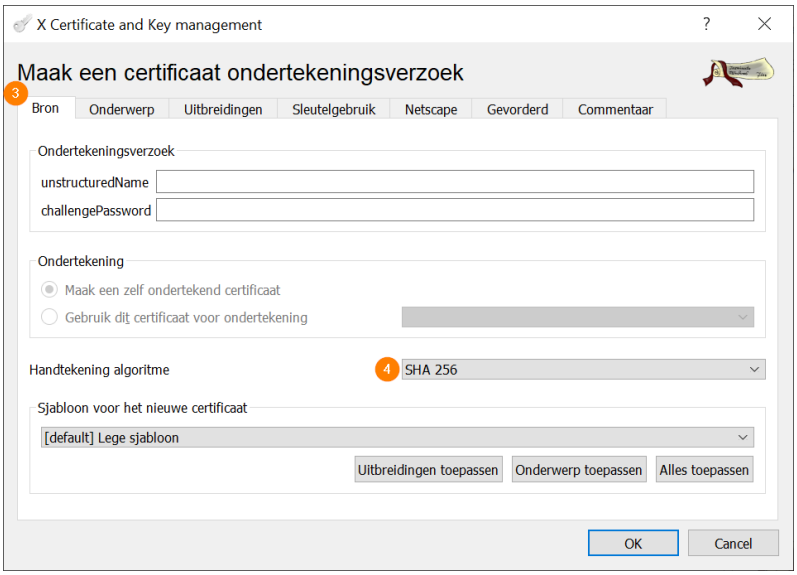
Een CSR bevat informatie over je toepassing, organisatie, contactgegevens, etc., en een publieke sleutel die door VO-PKI zal ondertekend worden. Hiermee bevestigen we die gegevens en heb je een certificaat dat je kan gebruiken in de dienstverlening tussen jouw organisatie en de Vlaamse overheid.

De **CSR heb je nodig om in Vo-DCBaaS** een certificaat aan te maken

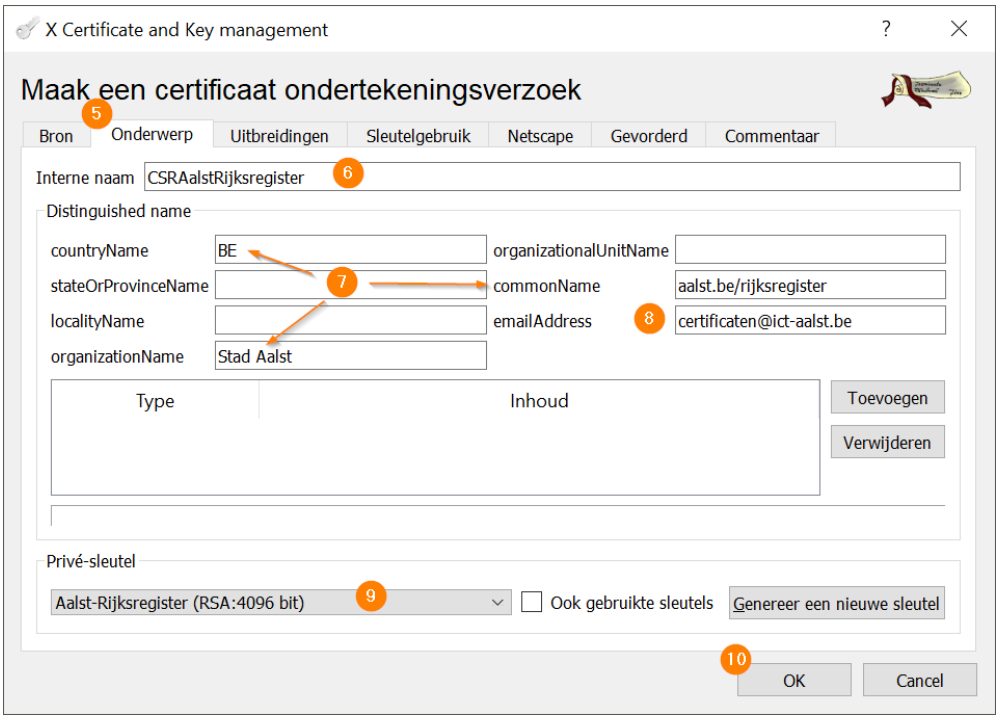
1. Kies de tab ‘Certificaat onderteken verzoeken’
2. Kies ‘Nieuw Verzoek’



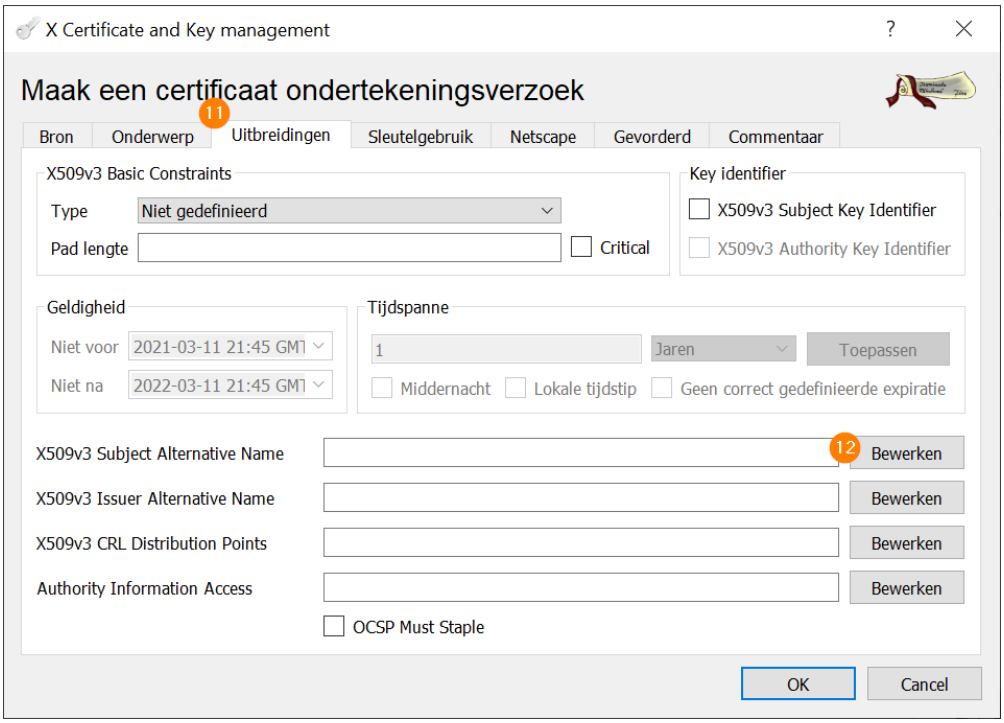
3. Kies de tab 'Bron'
4. Kies als handtekening algoritme: **SHA 256, SHA 384 of SHA 512**.
   Andere algoritmes worden niet ondersteund in Vo-DCBaaS



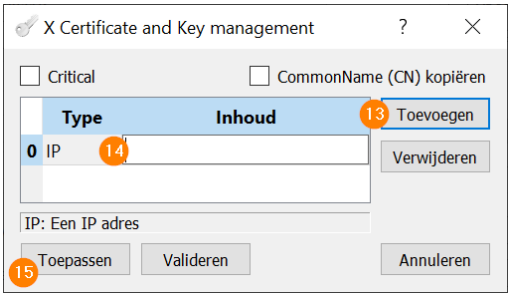
5. Kies de tab 'Onderwerp'
6. Geef de CSR een (zinvolle) interne naam
7. Vul minstens de verplichte attributen in:
    a. **countryName**: altijd '**BE**'
    b. **organizationName**: je organisatie of organisatiecodering
    c. **commonName**: de CN die je toepassing identificeert
    Deze wordt meestal meegedeeld door de dienst waar je aansluit, bijvb door Magda of door je ICT-dienstverlener
8. *[optioneel]* Als je een e-mail adres opgeeft, kan Vo-DCBaaS dat gebruiken als contactgegeven voor je certificaat
9. Kies de privé sleutel op basis waarvan de CSR gemaakt moet worden. Dat is de sleutel die we in de eerdere stappen hebben aangemaakt.
10. Als je geen SAN meer moet toevoegen, kan je nu op 'OK' klikken om je CSR aan te maken.
    *De volgende stappen zijn **optioneel***



11. *[optioneel]* Kies de tab 'Uitbreidingen'
12. *[optioneel]* Kies 'Bewerken' naast X509v3 Subject Alternative Name

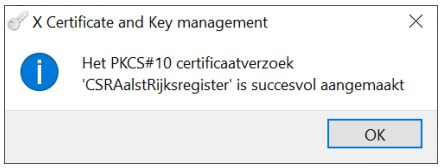


13. *[optioneel]* Kies 'Toevoegen' voor elke SAN die je wil toevoegen aan de CSR
14. *[optioneel]* Kies het gewenste type en vul de gewenste waardes in
15. *[optioneel]* Klik 'Toepassen' om te bewaren'

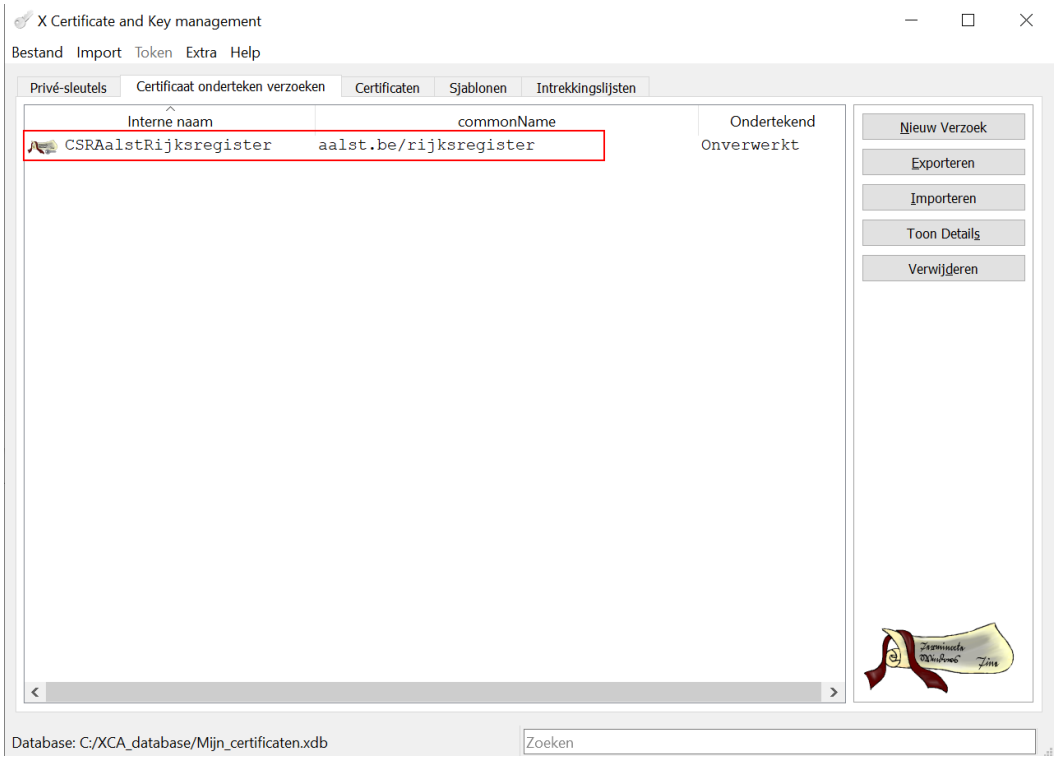


Je hoeft geen verdere gegevens in te vullen om een CSR aan te maken. Klik onderaan op 'OK' om de aanmaak van de CSR te bevestigen (zie stap 10).

Je krijgt een bevestiging als de CSR succesvol aangemaakt is. Sluit deze boodschap met 'OK'



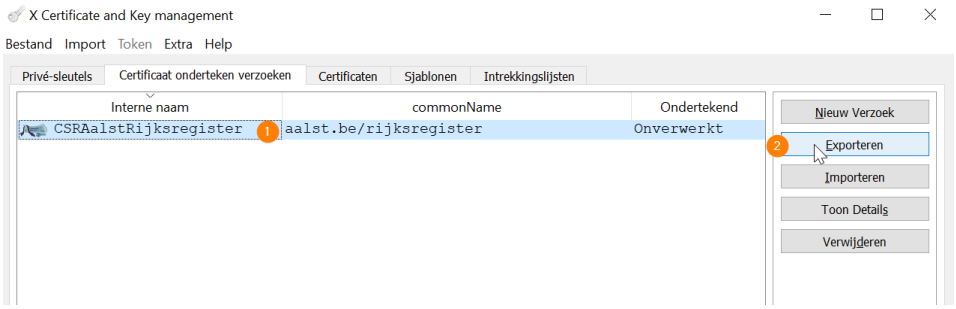
In XCA zie je de aangemaakte CSR in je overzicht van 'Certificaat onderteken verzoeken'



3.5 Een certificaat aanmaken

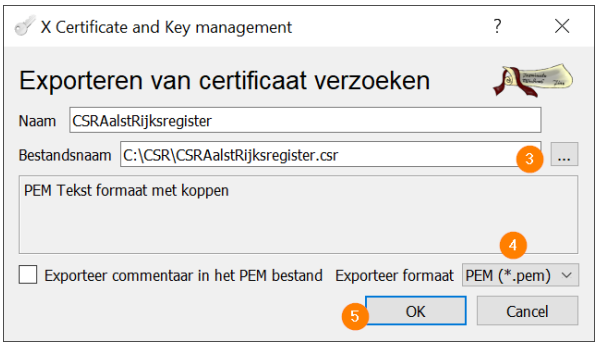
Met de CSR kan je in Vo-DCBaaS een certificaat aanvragen. Hiervoor exporteer je de aangemaakte CSR zodat je hem kan opladen in Vo-DCBaaS

1. Klik je CSR aan die je wil exporteren
2. Klik 'Exporteren'



3. Kies een locatie waar je de CSR wil opslaan.

   Via de knop [...] kan je gemakkelijk met de verkenner een locatie selecteren. Geef het bestand een zinvolle naam en zorg dat het **eindigt op de extensie .csr**
4. Selecteer '**PEM**' als formaat voor export
5. Klik 'OK'



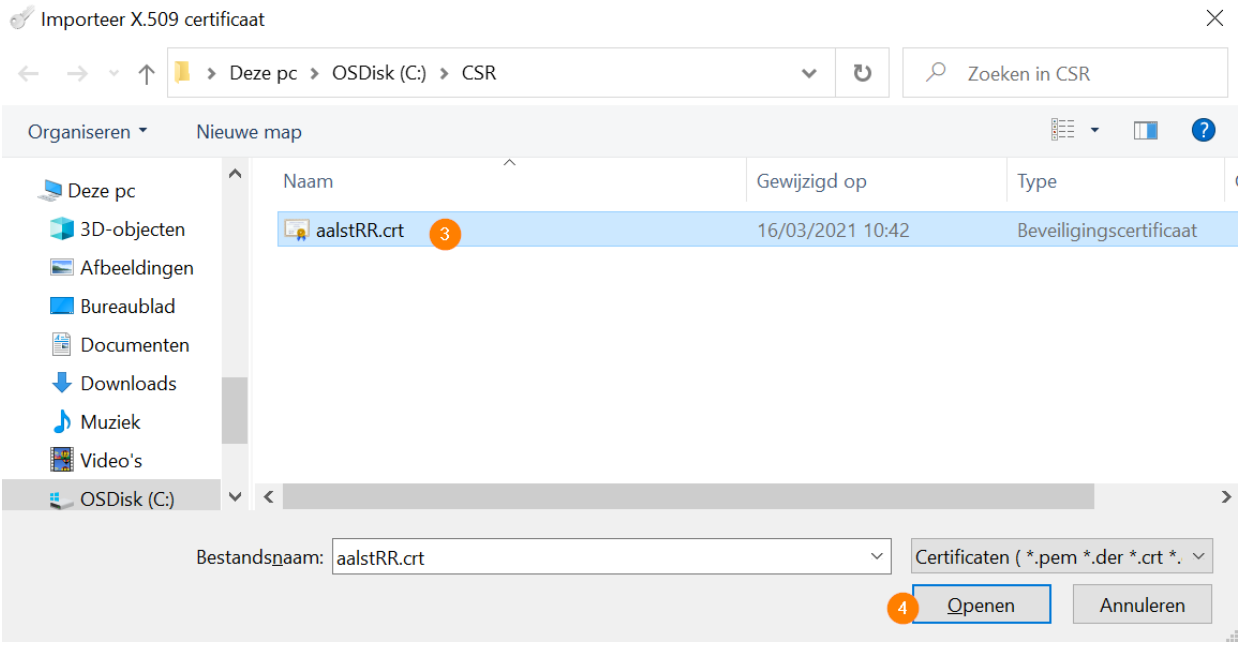
De CSR is nu opgeslagen op de gekozen locatie. Je kan deze nu opladen in het Certificatenbeheer om een certificaat aan te maken. Hoe je dat precies doet, staat beschreven in de Vo-DCBaaS handleiding

3.6 Een private sleutel en certificaat exporteren

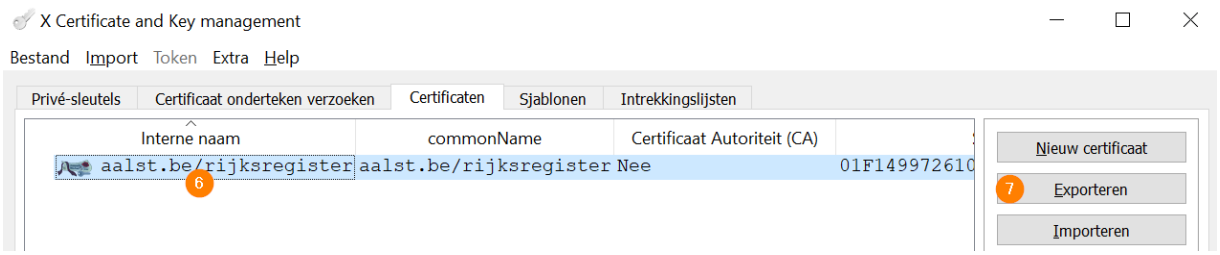
Om een private sleutel en bijhorend certificaat te gebruiken in een toepassing, worden ze vaak geëxporteerd als beveiligde 'sleutelkast'. Met de XCA tool kan je een PKCS #12 bestand maken (extensie .p12) en exporteren. Dit bestand wordt vervolgens geïmporteerd in je toepassing of bezorgt aan je IT-dienst of ICT-Dienstenleverancier.

1. Download en importeer het certificaat dat je in Vo-DCBaaS aangemaakt hebt via de tab ‘Certificaten’
2. Klik op ‘Importeren’

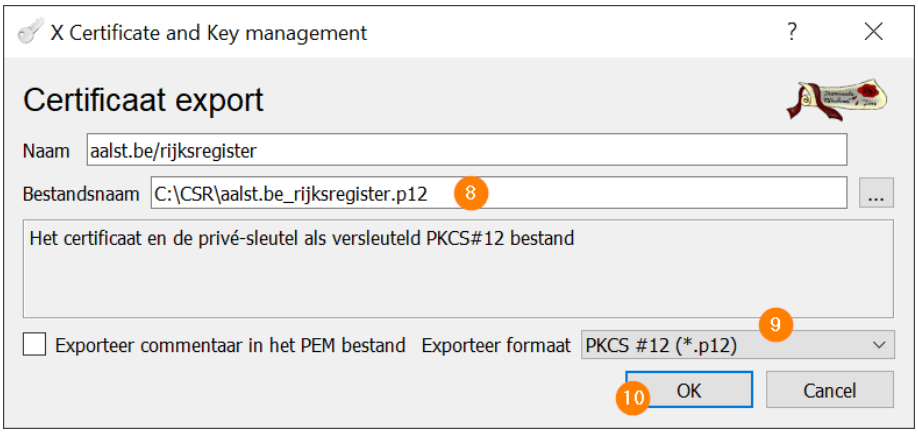
3. Kies het certificaat dat je gedownload hebt.
4. Klik op ‘Openen’



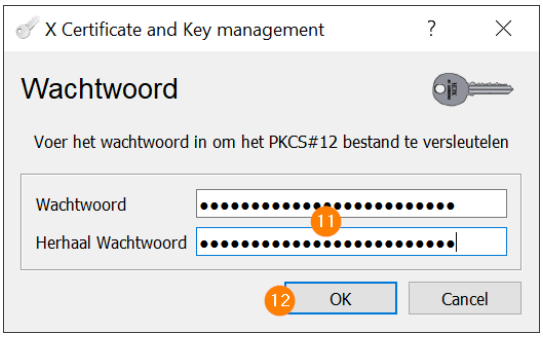
5. Je krijgt een melding dat het certificaat succesvol is ingeladen. Sluit deze boodschap met ‘OK’
6. Klik het certificaat aan.
7. Kies ‘Exporteren’



8. Kies een locatie waar je de sleutelkast wil opslaan.
   Via de knop ... kan je gemakkelijk met de verkenner een locatie selecteren.
   Geef het bestand een naam.
9. Kies PKCS #12 als export formaat
10. Klik op 'OK'



11. Geef een wachtwoord op waarmee de sleutelkast kan beveiligd worden. **Zonder dit wachtwoord kan je de sleutelkast niet gebruiken**
12. Klik op 'OK'



Je sleutelkast is nu beschikbaar op de gekozen locatie.

4 LIJST VAN GEBRUIKTE AFKORTINGEN

Afkorting	Betekenis
VO-DCBAAS	Vlaamse overheid Digitaal Certificatenbeheer as a Service, de toepassing die VO-DCB vervangt
CSR	Certificate Signing Request, een bestand waarmee je in Vo-DCBaaS een nieuw certificaat kan aanvragen
CN	Common Name, eigenschap van een certificaat die doorgaans de domeinnaam of gewoon de naam van de toepassing of server is waarvoor je een bepaald certificaat gebruikt.
VO-PKI	Vlaamse overheid - Private Key Infrastructure, de achterliggende infrastructuur waarmee toepassingen zoals Vo-DCBaaS certificaten aanmaken en ondertekenen. De Vlaamse overheid heeft een eigen (private) PKI-infrastructuur. Deze bestaat uit een root certificate authority en een issuing certificate authority.
VORCA2020	Vlaamse overheid – Root Certificate Authority, de root certificate authority van VOICA2.2020 (en dus Vo-DCBaaS)
VOICA2 2020	Vlaamse overheid – Issuing Certificate Authority, de nieuwe issuing certificate authority waarmee Vo-DCBaaS certificaten aanmaakt en ondertekent
SAN	Subject Alternative Name – attributen in een CSR die je applicatie verder identificeren of zorgen dat je certificaat meerdere identificaties bevat

5 VERSIEGESCHIEDENIS VAN HET DOCUMENT

Versie	*Datum*	*Wijzigingen*
V0.1	17/03/2021	Eerste publieke versie