HANDLEIDING Keystore Explorer

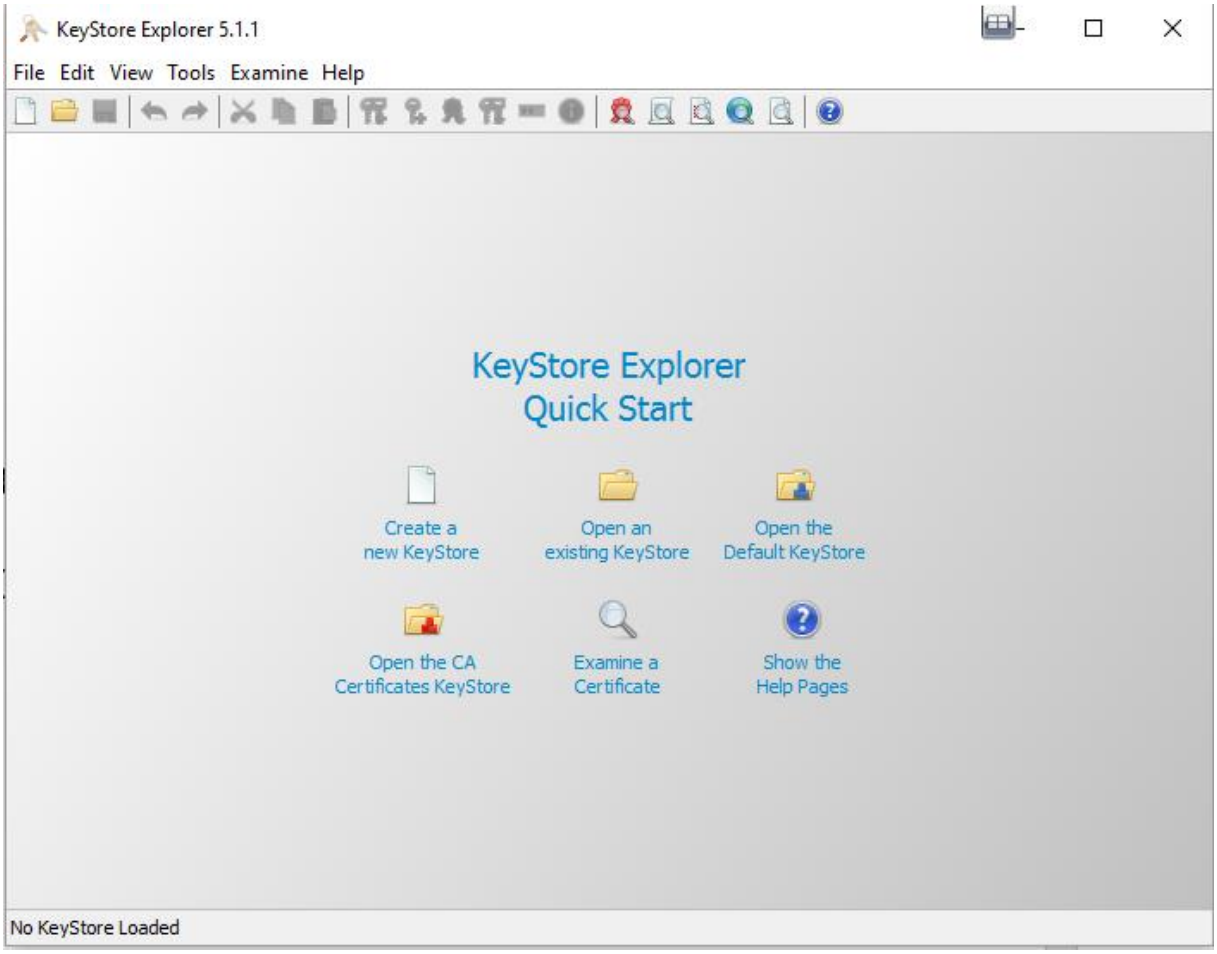
Inhoudstafel

Contents

Installatie Keystore Explorer 3
Aanmaken keystore 4
Genereer een sleutelpaar 4
Bewaren van de keystore 10
Genereer een Certificate Signing Request (CSR) 12
Importeer ondertekend certificaat van K&G in de keystore 15
Download de trusted chain certificaten 15
Importeer de trusted chain certificaten in de keystore 15
Importeer ondertekend certificaat in de keystore 19

Installatie Keystore Explorer

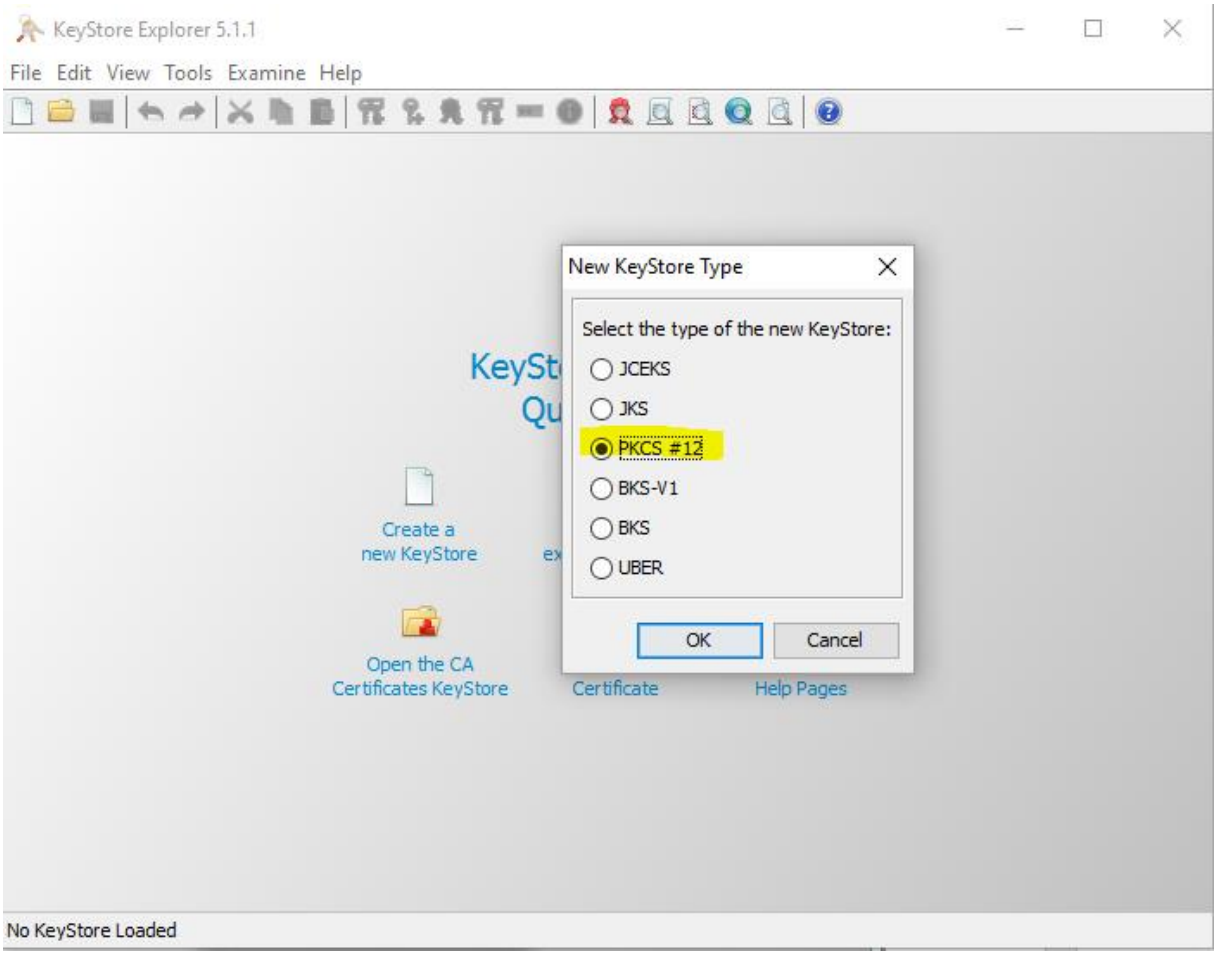
- Download keystore explorer via http://www.keystore-explorer.org/
- Installeer programma
- Open Keystore Explorer



Aanmaken keystore

Maak een keystore aan waarin je private en publieke sleutel zal bewaren.

- Selecteer in het beginscherm de optie “**Create a new keystore**”
- Kies vervolgens voor **PCKS#12**

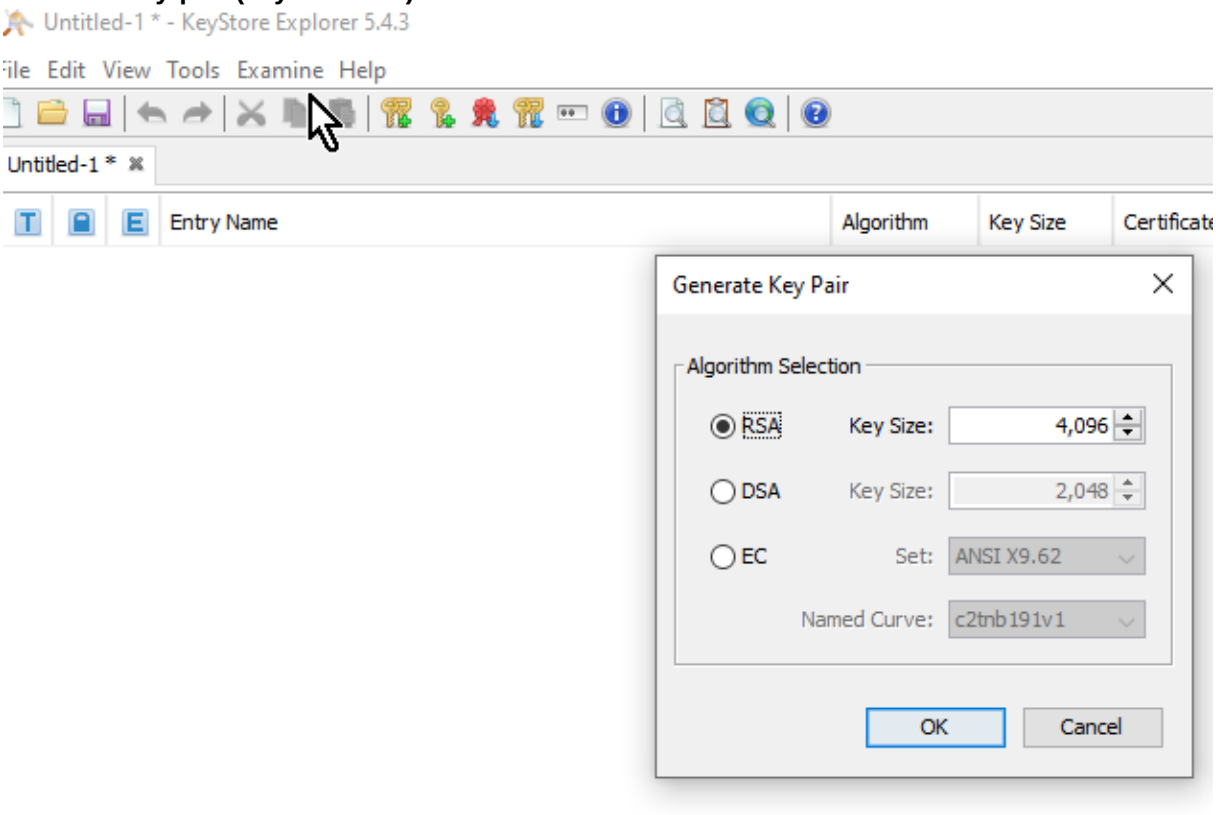


Genereer een sleutelpaar

Een sleutelpaar zal bestaan uit een public key en een private key, de private key is geheim en wordt dus nooit doorgegeven aan derde partijen.

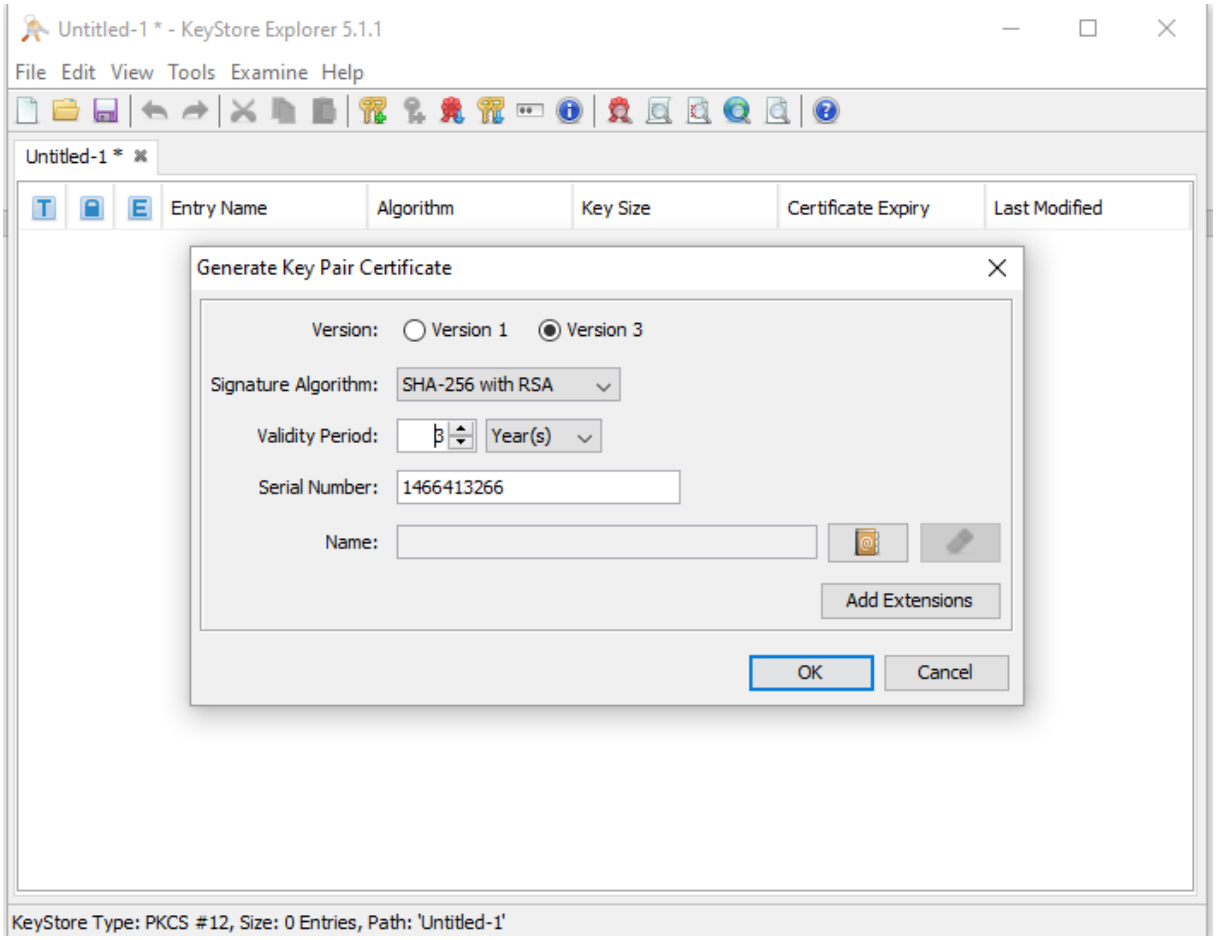
Via het menu kiest men:

- **Tools**
- **Generate key-pair (keysize 4096)**

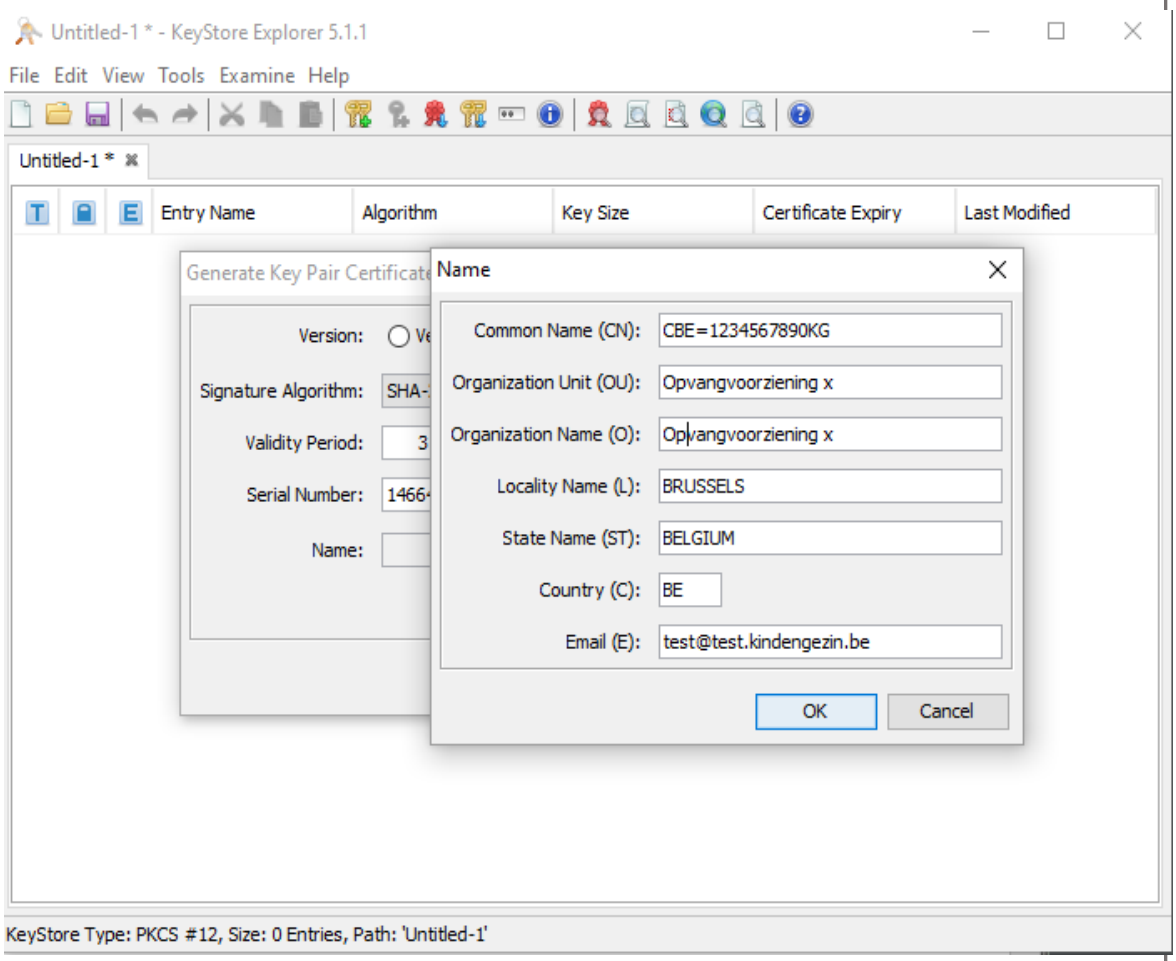


- Er verschijnt kort een boodschap "**Generating keypair**"
- Selecteer vervolgens algorithme **SHA-256 with RSA**

- Geef een geldigheidsperiode in (bijvoorbeeld 3 jaar)

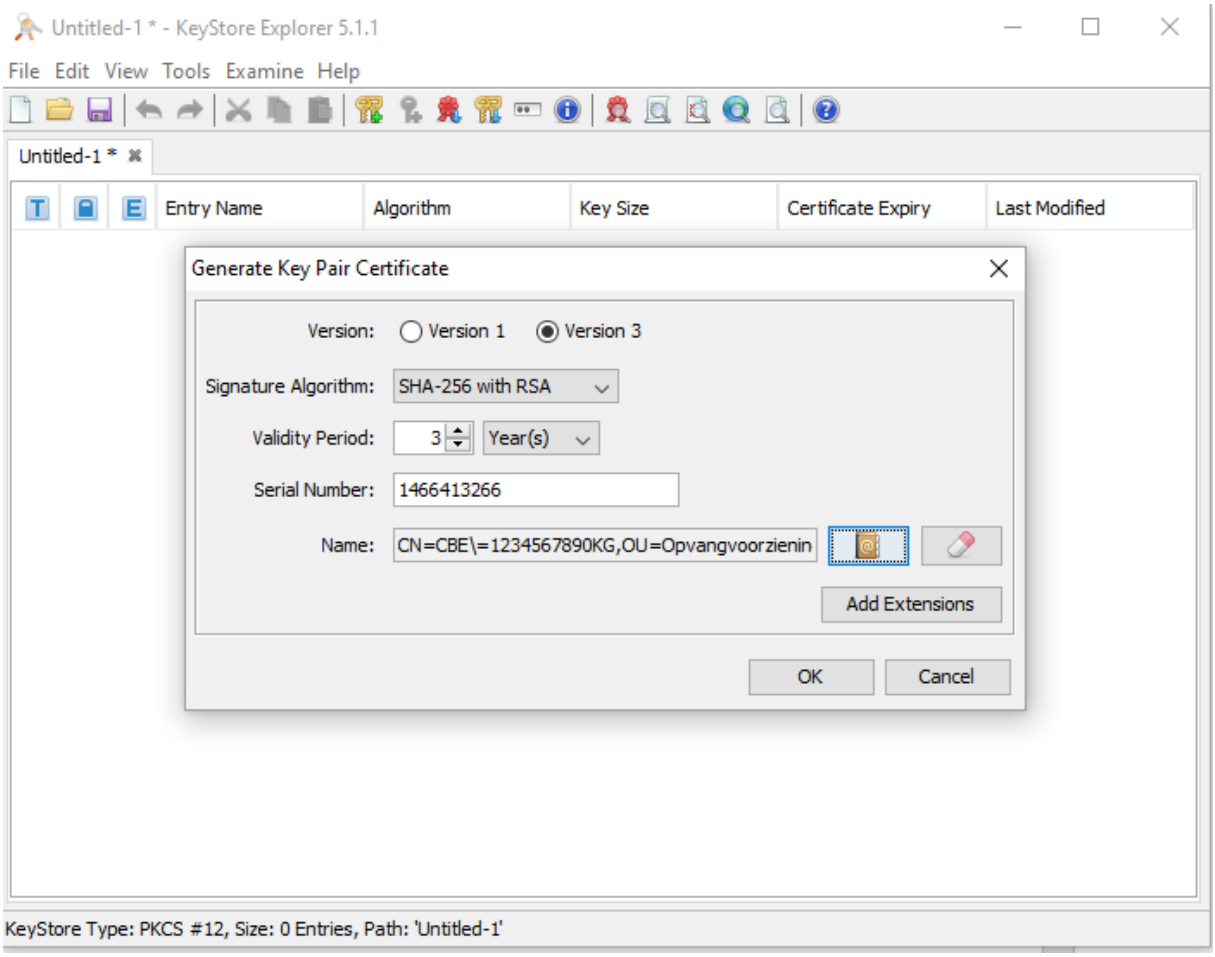


- Geef vervolgens de nodige gegevens in bij **Name**, hiervoor klikt men op de button die naast het veld **Name** staat
  - **CN**
    Hierin wordt het onderneminsgnummer geplaatst.
    Opgelet ! Prefix **CBE=** en suffix **KG** is verplicht om in te geven anders wordt het certificaat niet aanvaard om te signen door K&G.
  - **OU** en **O**
    Hierin mag men dezelfde waarde ingeven, is meestal de naam van de organisator.
  - **L**
    Hierin geeft men de gemeente in
  - **ST**
    Hierin geeft men als waarde **BELGIUM** in
  - **C**
    Hierin geeft men de landcode **BE** in
  - **E**
    Hierin geeft men het emailadres op (deze zal ook gebruikt worden om aan te geven dat certificaat bijna vervallen is etc...)

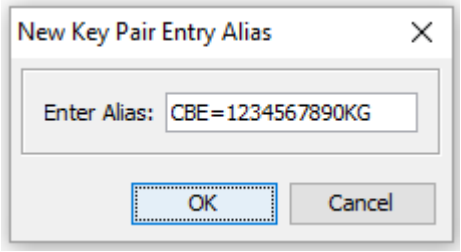


- Klik vervolgens op **OK**

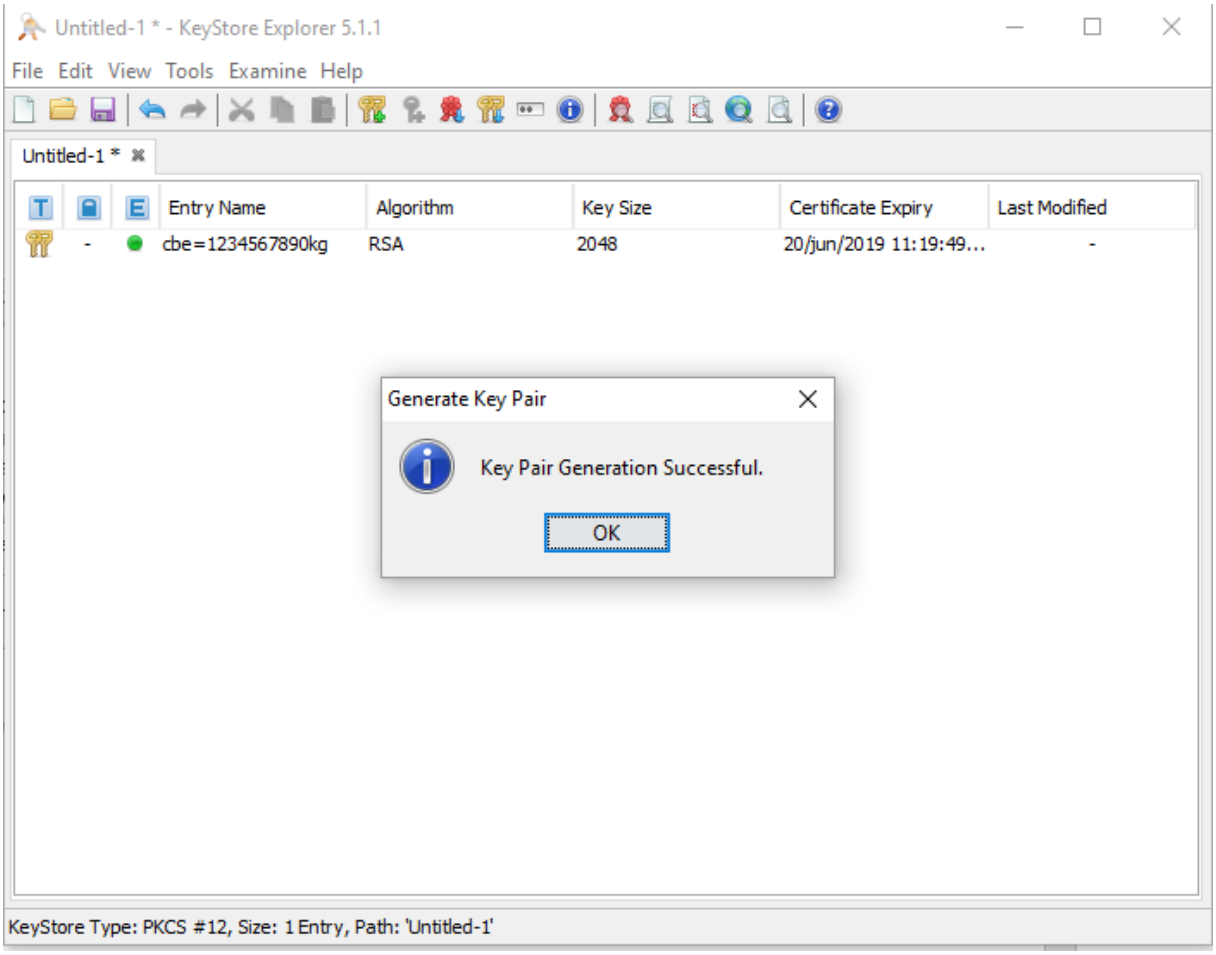
- Men ziet vervolgens onderstaand scherm



- Klik op de **OK**-knop
- Geef nu een alias in (dit is de naam die zal verschijnen in je keystore)
  Standaard wordt hier de waarde van het veld **CN** voorgesteld, men kan hier gerust een andere waarde ingeven indien gewenst.



- Het sleutelpaar is succesvol aangemaakt en onderstaand scherm wordt dan getoond.
  De kolom **Entry Name** toont de **alias** die we in het voorgaande scherm hebben opgegeven.

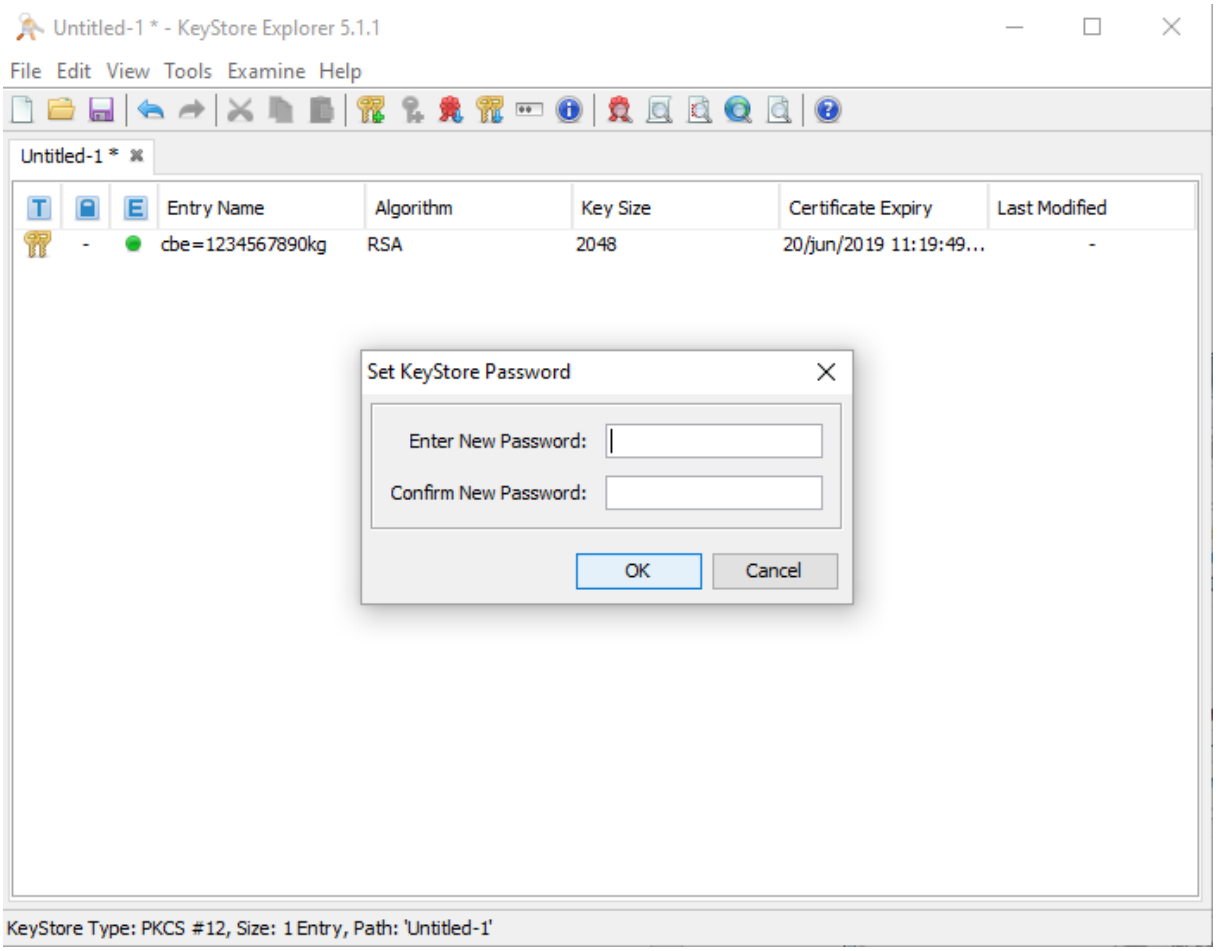


Bewaren van de keystore

Men kan de keystore ook in een latere fase voor de eerste maal bewaren maar in geval de PC zou crashen of iets dergelijks moeten bovenstaande stappen opnieuw worden uitgevoerd.

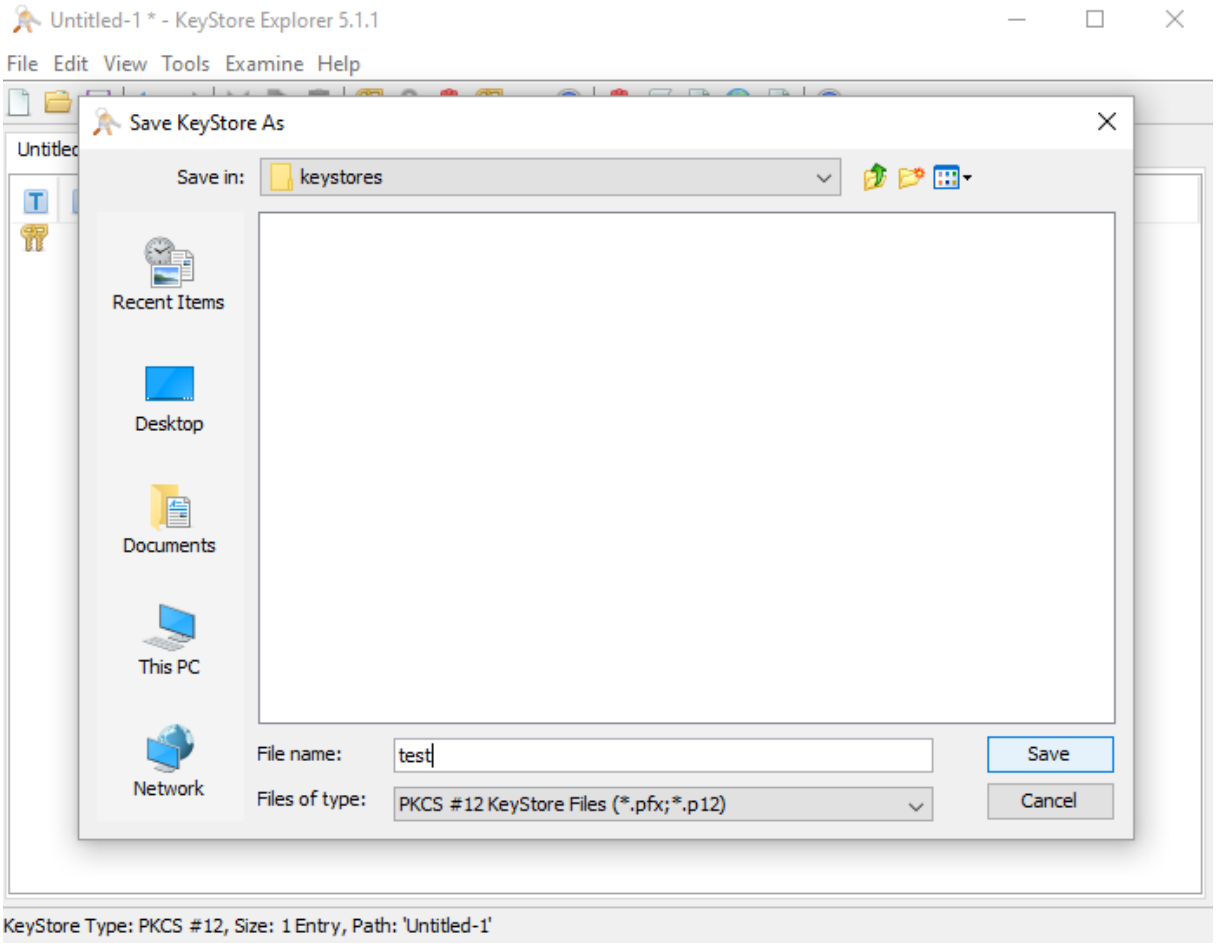
Daarom best na een succesvolle Key Pair certificate generation de keystore opslaan.

- Kies via menu de optie **File**
- Kies vervolgens **Save**



- Geef nu een paswoord in om de keystore te beveiligen
- Selecteer een folder om de keystore in te bewaren
- Geef een naam aan de keystore
- Selecteer als type **PCKS #12 Keystore Files**

- Klik op de knop **Save**

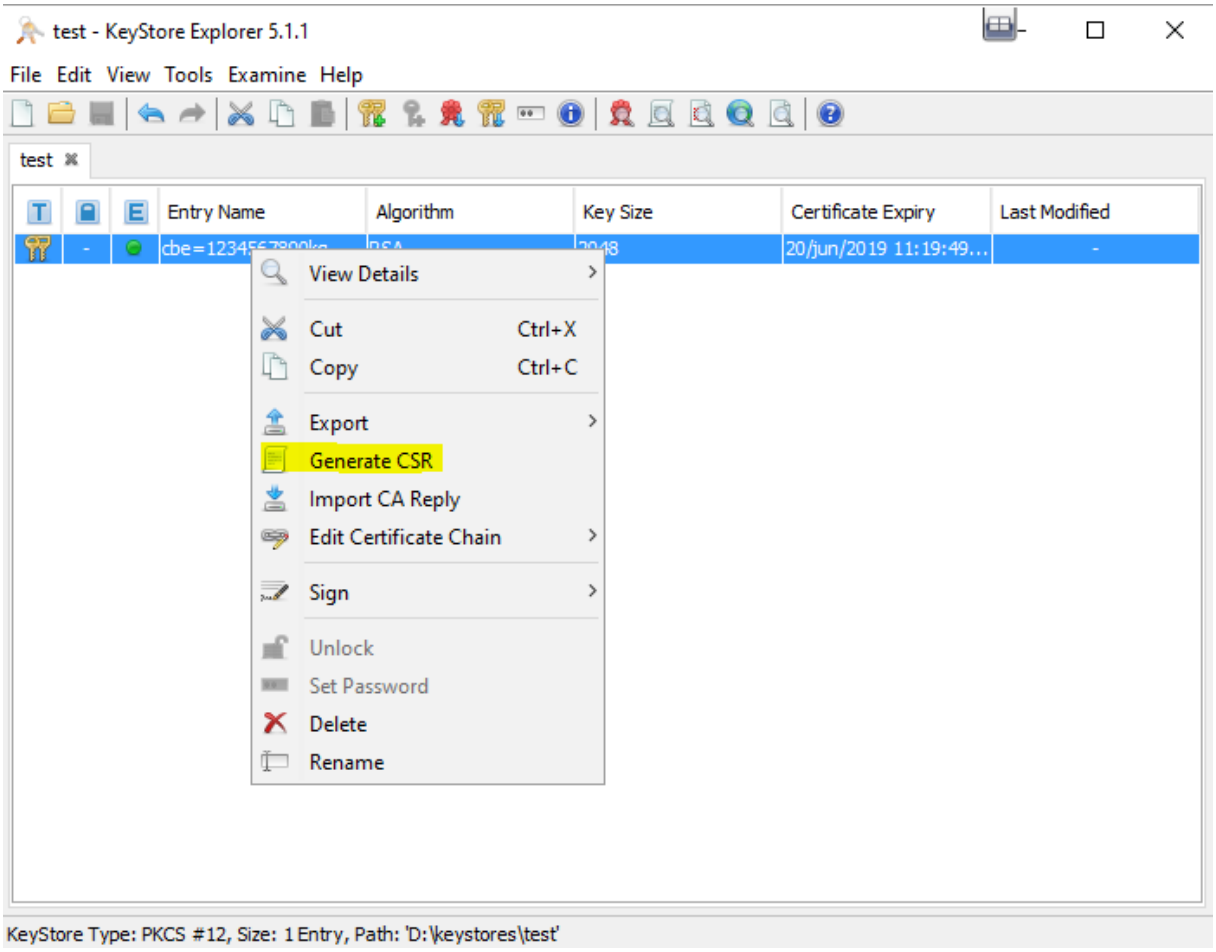


Genereer een Certificate Signing Request (CSR)

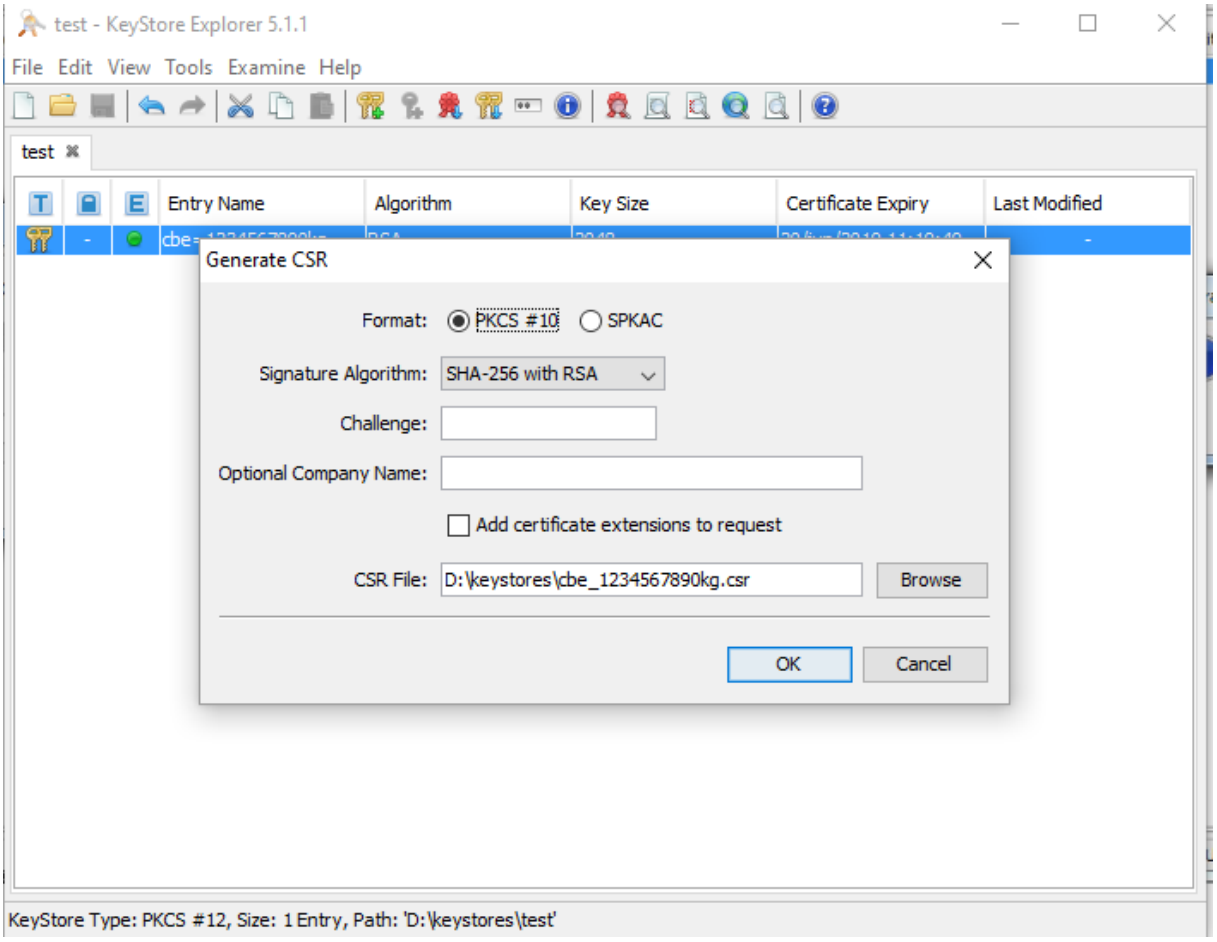
In de keystore heeft men een sleutelpaar aangemaakt, vervolgens maakt men een CSR aan zodat er op basis hiervan een getekend certifcaat kan afgeleverd worden.

Deze CSR mag de private key niet bevatten.

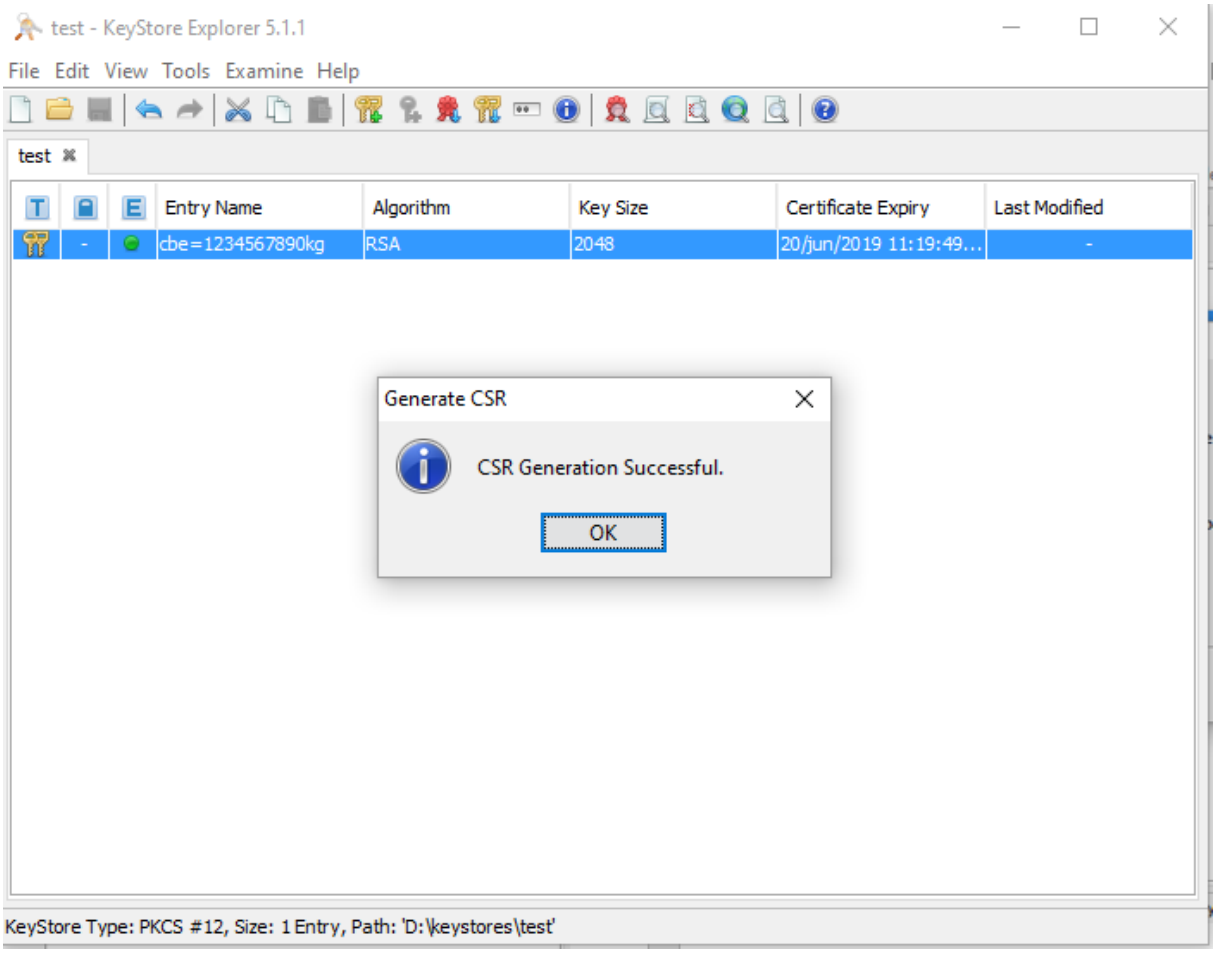
- Selecteer het sleutelpaar
- Via rechtermuisklik kiest men de optie **Generate CSR**



- Indien gewenst kan men de bestandsnaam aanpassen
  Formaat is **PCKS#10**



- Vervolgens wordt de boodschap getoond dat CSR request succesvol werd aangemaakt



Dit **.CSR** bestand moet worden doorgestuurd naar **software-ontwikkeling@kindengezin.be** waarbij het onderwerp van de mail moet bevatten:

  - **[CSR-<ondernemingsnummer>]**
    Een geldig onderwerp zou dus zijn [CSR-1234567890] (gebaseerd op het fictieve ondernemingsnummer dat we in deze handleiding hebben gebruikt)

Importeer ondertekend certificaat van K&G in de keystore

Het toegestuurde .CSR-bestand is verwerkt bij K&G en het ondertekende certificaat werd via mail toegestuurd.

Download de trusted chain certificaten

Via de link http://documenten.pki.vlaanderen.be/ kan u volgende .cer-bestanden downloaden:

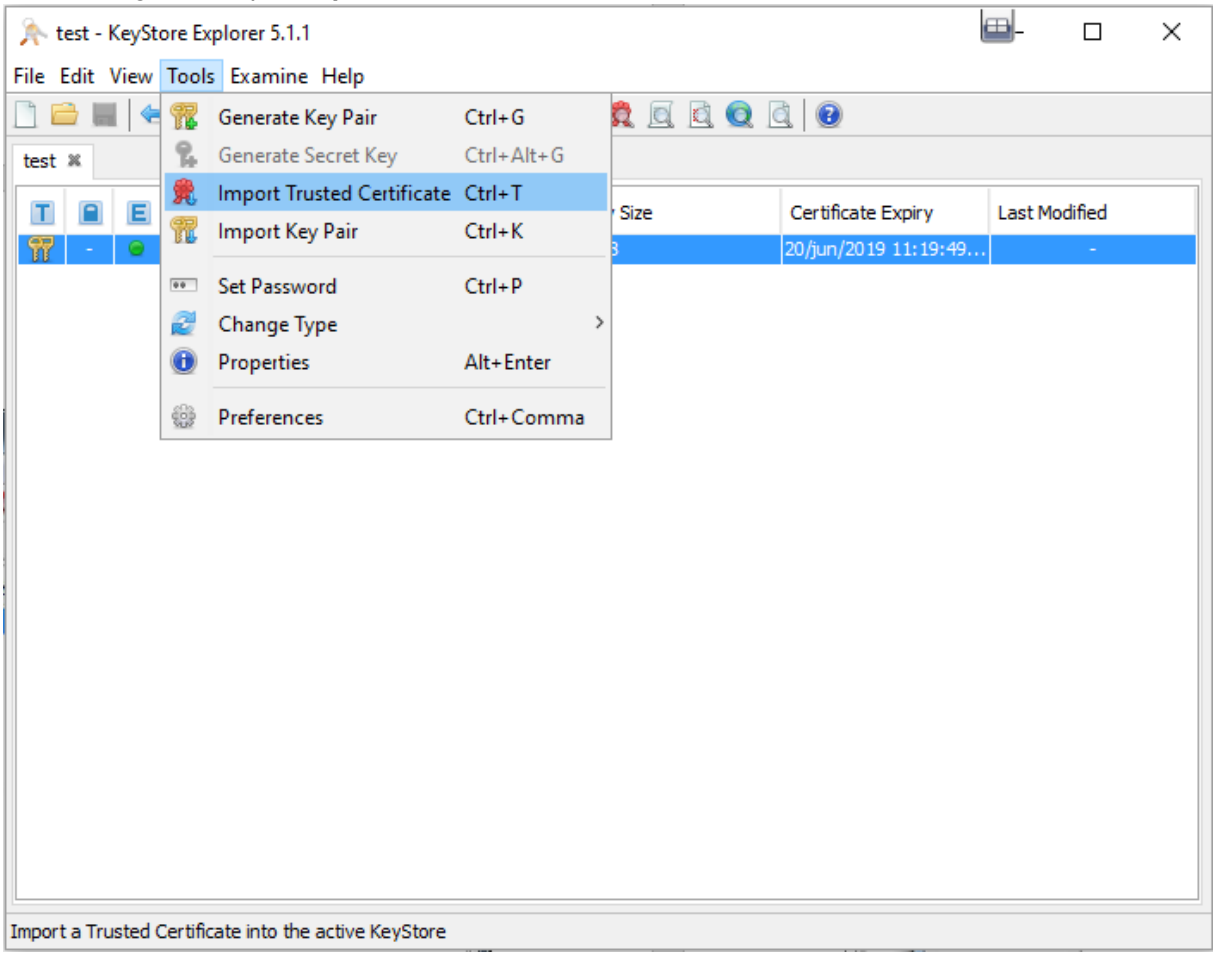
- Certificaat Vlaamse overheid Root CA
- Certificaat Vlaamse overheid Issuing CA 2

Als deze .cer-bestanden zijn gedownload kan u deze importeren in de keystore

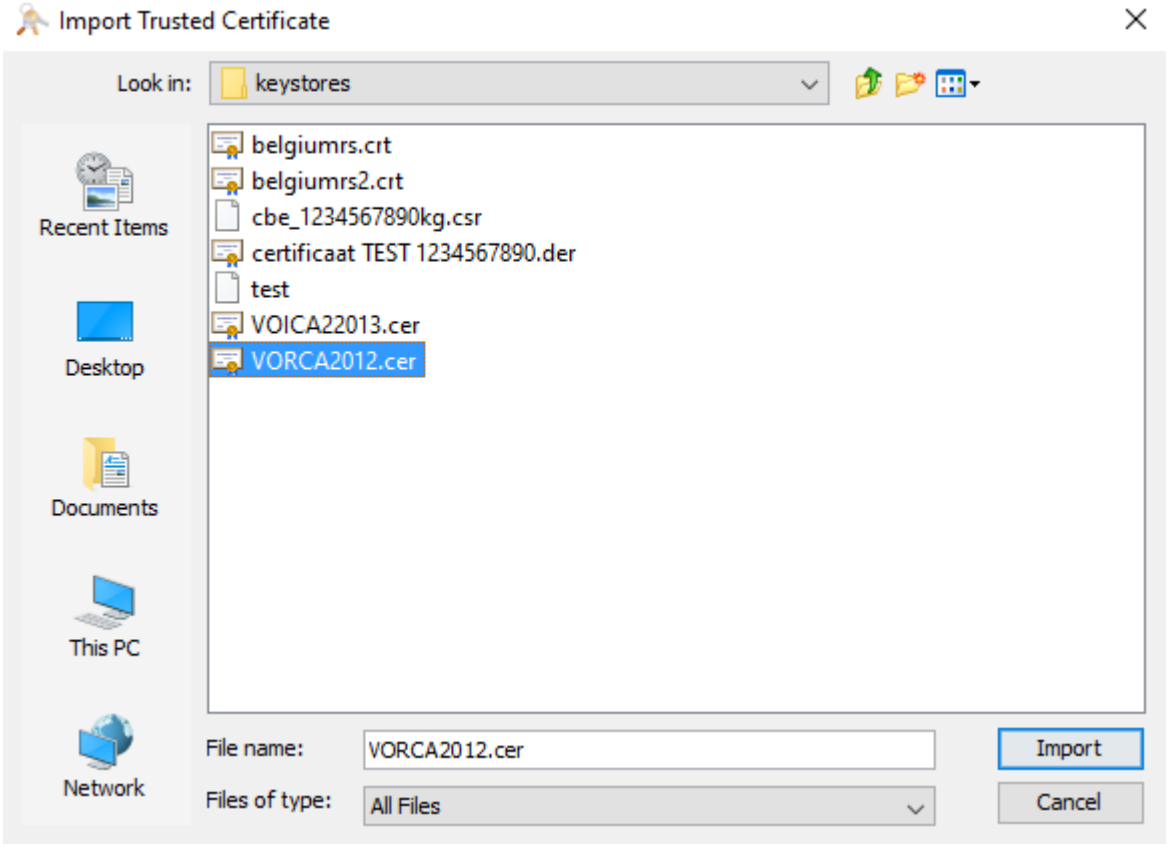
Importeer de trusted chain certificaten in de keystore

Nu men de trusted chain certificaten heeft gedownload kan men deze importeren in de keystore:

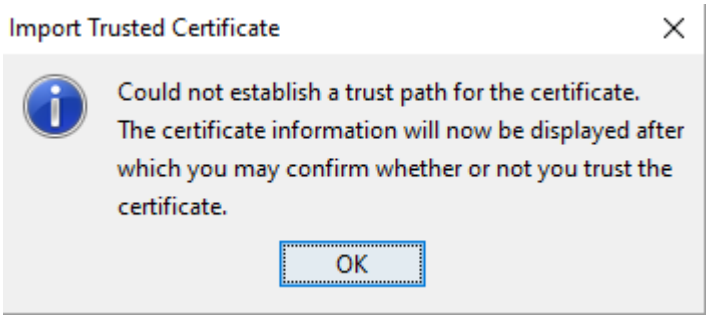
- Selecteer de menu-optie **Tools**
- Kies vervolgens de optie **Import trusted certificate**



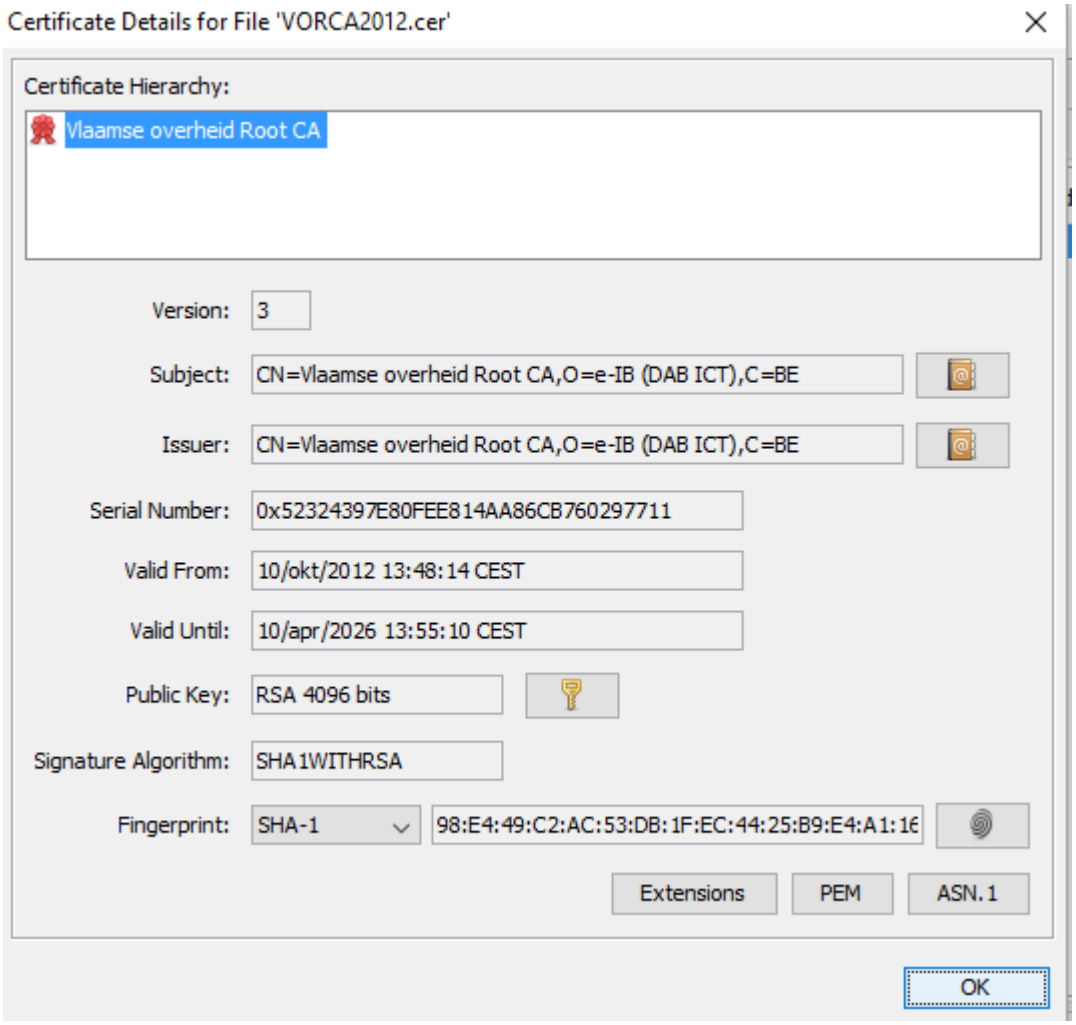
- Kies vervolgens het cer-bestand van Certificaat Vlaamse Overheid Root CA



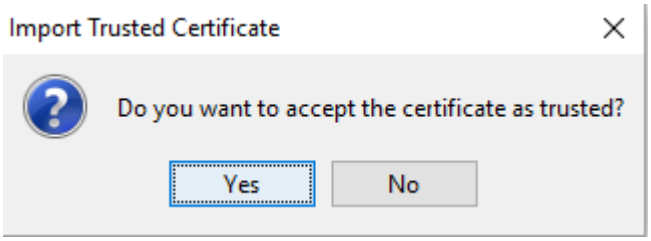
- Klik op de knop **Import**
- Er verschijnt volgende boodschap, klik op de **OK-knop**



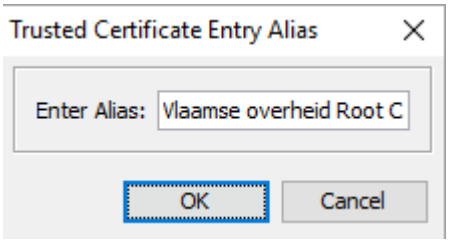
- Vervolgens worden de gegevens van het certificaat getoond



- Klik op de knop **OK**
- Klik vervolgens op de knop **OK** om het certificaat als trusted te aanvaarden

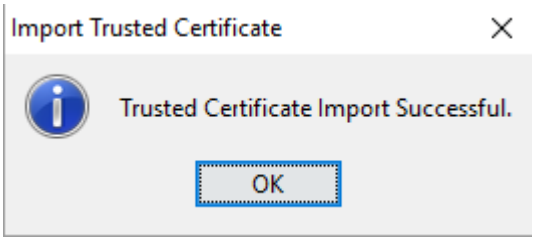


- Geef een alias op voor dit certificaat (standaard staat dit op **Vlaamse overheid Root CA**

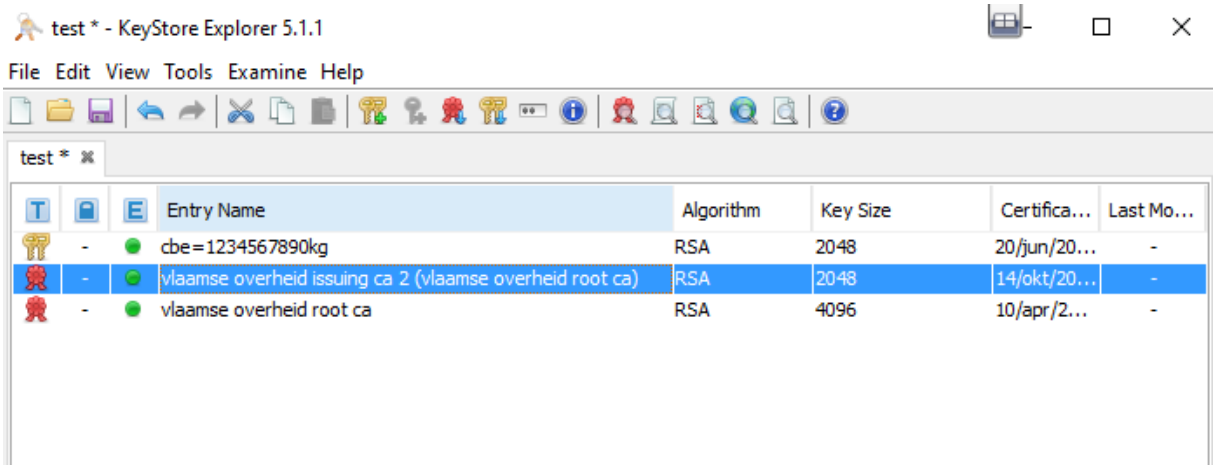


- Klik op de knop **OK**

- Vervolgens verschijnt de boodschap dat het succesvol geïmporteerd is



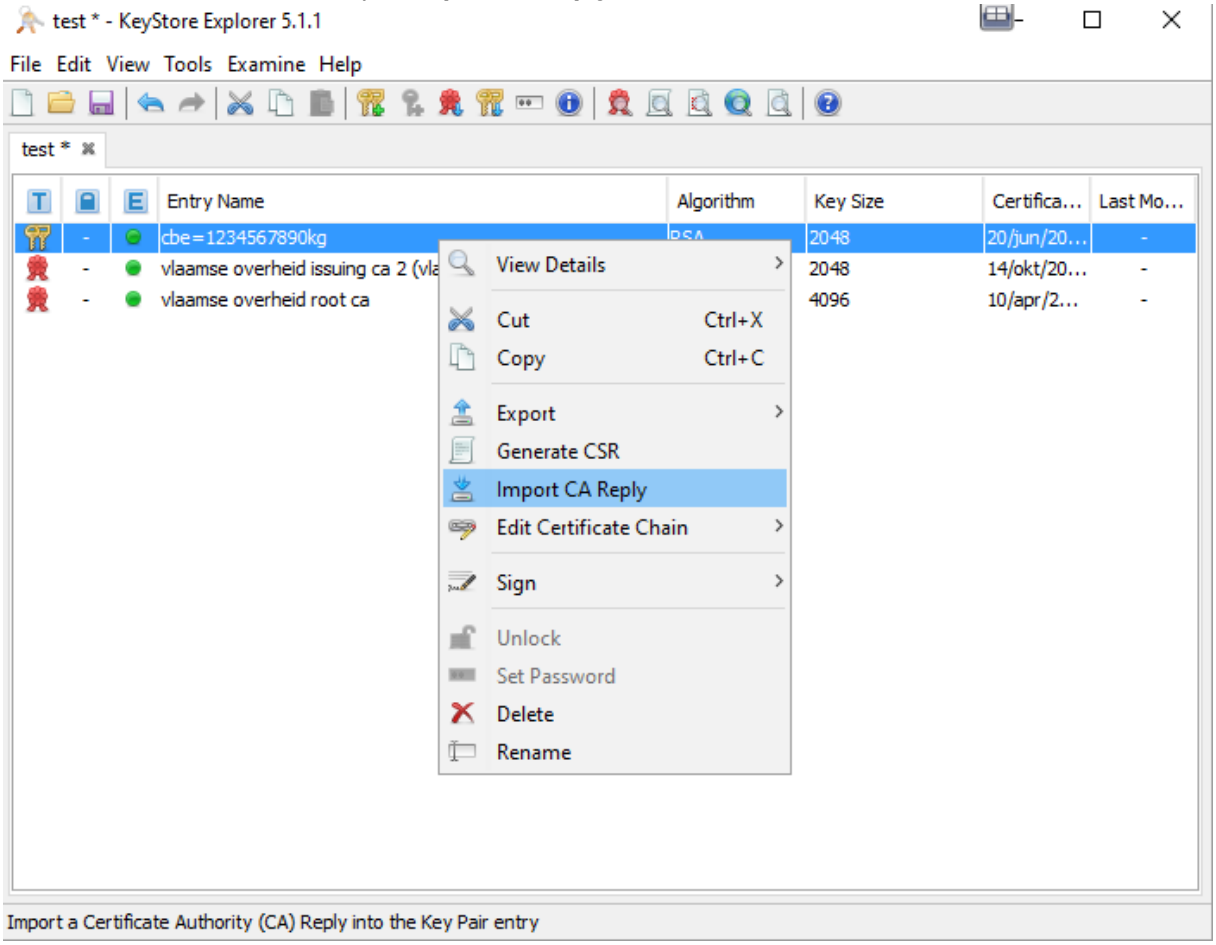
- **Herhaal bovenstaande stappen nu ook voor Certificaat Vlaamse Overheid Root CA2**
- In de keystore staan nu ook de trusted chain certificaten



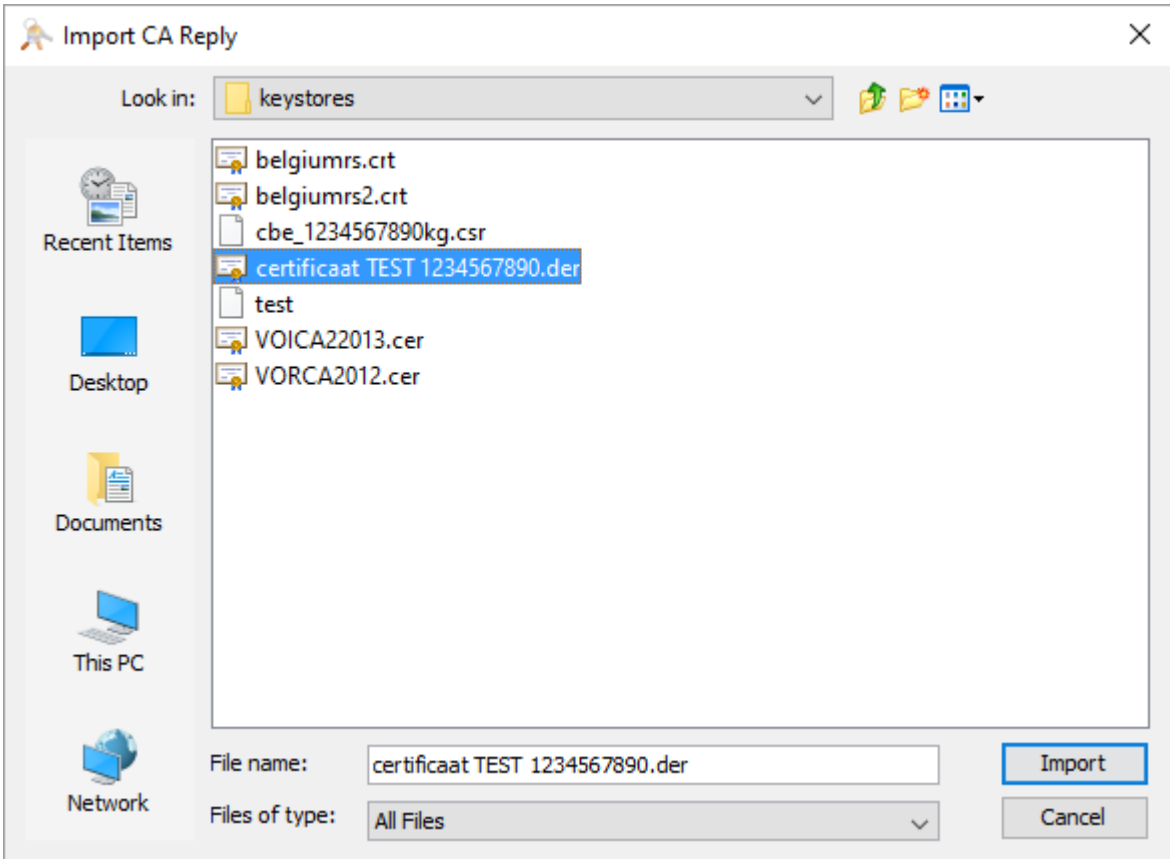
Importeer ondertekend certificaat in de keystore

Men heeft de trusted chain certificaten in de keystore geïmporteerd, nu kan men het ondertekend certificaat dat door K&G werd teruggestuurd importeren.

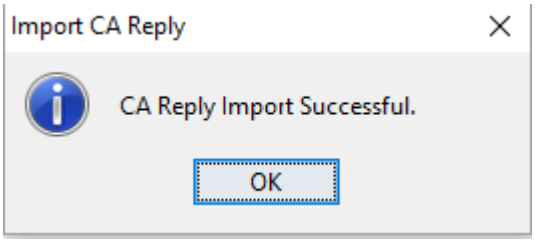
- Selecteer het sleutelpaar
- Via rechtermuisklik de menu-optie **Import CA reply** selecteren



- Selecteer vervolgens het certificaat dat door K&G werd opgestuurd



- Vervolgens verschijnt de boodschap dat het succesvol werd geïmporteerd



- **BEWAAR de keystore** door op het icoon van bewaren te klikken (of gebruik de combinatie van toetsen CTRL en S)