Technische instructie dienstenportaal

Inhoud

Inleiding

Het Dienstenportaal biedt de eindgebruiker op het Internet de mogelijkheid om gebruik te maken van diensten op het JustitieNet. De werkplek van de gebruiker moet echter wel aan een aantal technische eisen voldoen. Lees hiervoor deze instructie goed door.

Gewijzigd op 17-10-2022 door FB IFZO

- **UZI linken zijn aangepast**

1. Vereisten voor gebruik Dienstenportaal

Om gebruik te kunnen maken van het dienstenportaal zijn de volgende zaken vereist:

1. Browser Google Chrome of Microsoft Edge. voorzien van de nieuwste updates.

2. Een geldig UZI pas en een cardreader waar de drivers voor zijn geïnstalleerd op uw systeem.

Zie voor de vereisten: Activeer en installeer uw UZI-pas | UZI-pas | UZI-register (uziregister.nl) (wij bieden alleen ondersteuning voor Windows 10 en kunnen geen werking garanderen op systemen met een alternatief besturingssysteem als Linux of MacOSX).

3. Het dienstenportaal is extra beveiligd met beveiligingscertificaten. Deze moeten op uw

systeem geïnstalleerd staan zodat het dienstenportaal u als aanmelder vertrouwt. U dient

hiervoor de Safe-Sign Software gedonwload te hebben. Zie hiervoor:

Activeer en installeer uw UZI-pas | UZI-pas | UZI-register (uziregister.nl)

Vraag een UZI-servercertificaat aan | UZI-servercertificaat | UZI-register (uziregister.nl)

4. Werkt u met Citrix of een ander extern bureaublad, laat dan uw interne ICT-organisatie de installatie van de certificaten uitvoeren voor u. Een technische instructie voor ICT-beheerders is te vinden in hoofdstuk 2 en 3.

U kunt na het doorlopen van bovenstaande stappen inloggen op www.dienstenportaal.nl

Met hulp van de Gebruikershandleiding Dienstenportaal kunt u IFZO benaderen.

Mocht u middels bovenstaande stappen nog geen toegang tot het Dienstenportaal hebben, neem dan contact met uw ICT-beheerder. Een technische instructie voor ICT-beheerders is te vinden in hoofdstuk 3 en 4.

2. Faq's / Veelgestelde vragen

- ***Is mijn UZI pas nog geldig?***

Ga naar onderstaande link:

Uitgegeven UZI-passen | Zorg CSP

Vul een van de volgende gegevens in:

UZI-nummer: <UZI Nummer>

UZI-pasnummer: <UZI Pasnummer>

Check of de naam Pashouder overeenkomt met de aanmelder.

Controleer vervolgens de geldigheid van de uzi-pas bij "Geldigheidsperiode".

Als de geldigheid verstreken is, dan dient de gebruiker een nieuwe pas aan te vragen. Zodra de pas binnen is dient de gebruiker een wijzigingsverzoek in bij ifzo@dji.minjus.nl om toegang te verschaffen tot het dienstenportaal middels een nieuwe pas.

- ***Ondanks dat ik jullie technische handleiding gevolgd heb, heb ik nog steeds problemen met mijn pas, cardreader en/of certificaten.***

Neem in dat geval contact op met UZI register. U krijgt de helpdesk van Atos aan de lijn. Zij zullen u verder helpen. Tel 088 - 265 5902 of UZI-pas.support@atos.net.

- ***Als ik naar de door jullie verstrekte link https://www.dienstenportaal.nl ga krijg ik een melding in mijn browser (Google Chrome of Microsoft Edge) te zien dat de pagina niet kan worden weergegeven.***

Dan heeft u de handelingen nog niet correct uitgevoerd om de certificaten te installeren of maakt u niet gebruik van een recente versie van eerdergenoemde browsers. Loop deze handleiding goed door en/of vraag hulp aan uw ICT-beheerder.

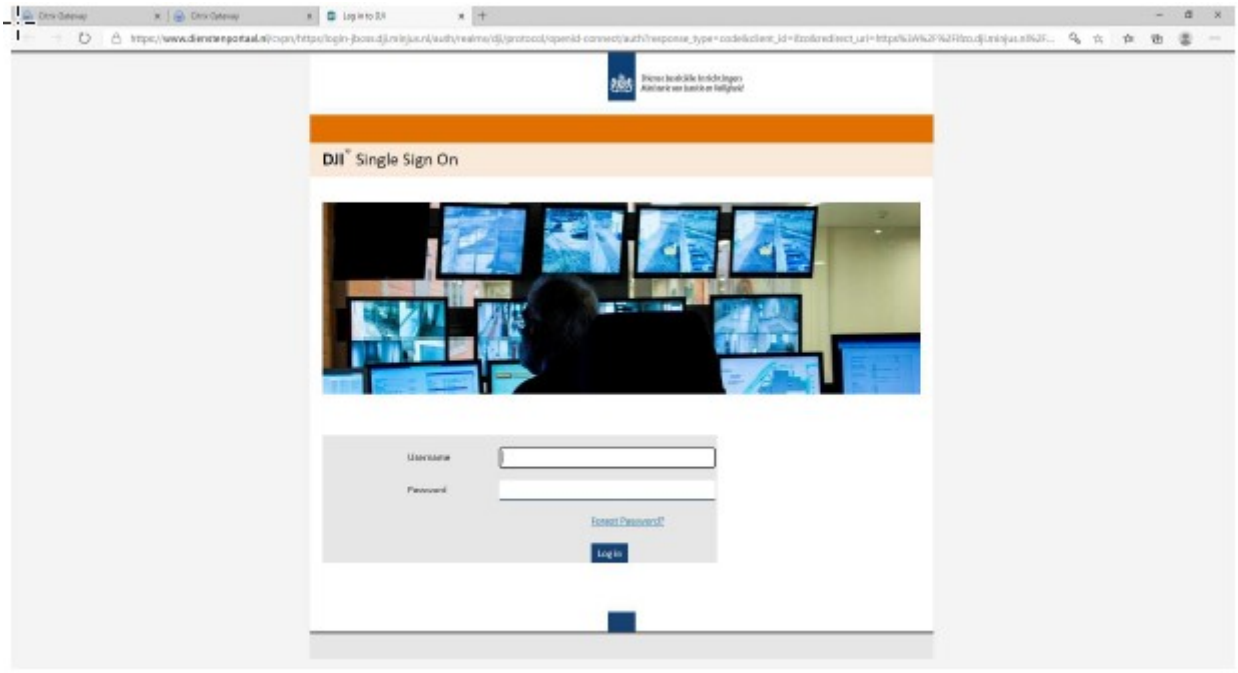
- ***Om toegang tot het dienstenportaal te krijgen wordt mij gevraagd om een wachtwoord.***

- ***Ik heb dit wachtwoord echter niet, ben het kwijt of kom niet verder.***

Neem hiervoor contact op met onze servicedesk – 088-0712345 of mail naar

Ict-servicedesk@dji.minjus.nl

- ***Ik kan niet inloggen in de applicatie IFZO. Ik weet mijn wachtwoord niet meer of weet niet wat ik hier moet invoeren. Ik heb wel eerder in IFZO gewerkt.***



Voor het herstellen van uw wachtwoord klikt u op “Wachtwoord vergeten?” en vult u IFZO gebruikersnaam + emailadres in. U krijgt op mail een tijdelijk wachtwoord dat u, samen met uw gebruikersnaam, moet invoeren in IFZO. Daarna dient u direct een nieuw, zelfgekozen, wachtwoord in te stellen.

Blijft u problemen ondervinden met het inloggen in de applicatie IFZO. Neem dan contact op met het functioneel beheer van IFZO. ifzo@dji.minjus.nl

- ***Ik maak gebruik van de browser Firefox. Kan ik daarmee ook inloggen in het***

Dienstenportaal?

Firefox kan werken door via de safe sign software voor keuzemenu 'integration' te kiezen ->install safe sign in Firefox. Firefox moet hierbij afgesloten worden. Let op dat de certificaten 'Staat der Nederlanden Root CA - G3' en 'QuoVadis PKIoverheid Server CA 2020' nog steeds op uw systeem in de certificate store van Microsoft dienen te staan.

Als alternatief kunt u de stap voor het installeren van certificaten in Firefox overslaan en de volgende instructie volgen:
https://www.windowscrush.com/how-to-configure-firefox-touse-

windows-certificate-store.html deze instructie stelt Firefox zo in dat deze kijkt naar de certificate store van Microsoft. Als u voor deze optie kiest, loop dan deze handleiding alsnog geheel door en volg de bovengenoemde instructie hierna. U hoeft dan niet de optie uit te voeren de certificaten te installeren in Firefox via de safe sign software.

!Wij bieden op dit moment support voor Edge en Chrome en nog niet voor Firefox. Met volgen van bovenstaande instructies heeft u grote kans dat het werkt, maar dit is wel op eigen risico en zonder verdere support. Dit zal in de toekomst wellicht veranderen!

3. Voor ICT-beheerders: welke certificaten zijn vereist?

In deze instructie staat beschreven hoe u certificaten installeert op uw systeem zodat uw gebruiker op de omgeving van het dienstenportaal kan komen. Als eerste wordt vermeld welke certificaten u moet downloaden en waar u dit kunt doen. Vervolgens krijgt u instructie waar u deze certificaten kunt installeren. Als u alle certificaten op uw systeem geïnstalleerd hebt, kunt u gebruik maken van de nieuwe omgeving van het dienstenportaal. Het is belangrijk dat u beheerders-rechten op uw werkstation heeft. Indien u deze niet heeft, raden wij u aan contact op te nemen met uw ICT afdeling of technisch beheerder zodat zij uw certificaten kunnen installeren.

1. Staat der Nederlanden Root CA - G3
2. QuoVadis PKIoverheid Server CA 2020
3. De volgende 3 certificaten kunnen verschillen en hieronder wordt beschreven welke u nodig heeft.

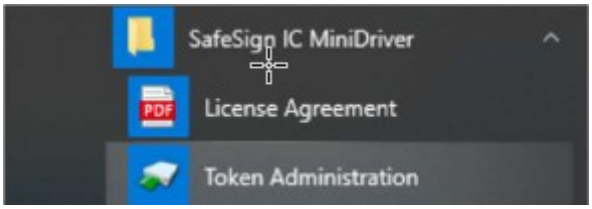
Ga voor de eerste 2 certificaten naar https://www.pkioverheid.nl/ en zoek de certificaten op. U kunt in uw browser zoeken en de namen van de certificaten uit

dit document kopiëren en plakken. Het is aan te raden een map aan te maken (nb certificaten) en hier alle benodigde certificaten in te zetten zodat u ze hierna gemakkelijk kan importeren.

NB: Als u bij bent met de nieuwste Windows updates zal ‘Staat der Nederlanden Root CA - G3’ automatisch geïnstalleerd zijn. Het andere certificaat (QuoVadis PKIoverheid Server CA 2020) dient sowieso handmatig te worden toegevoegd.

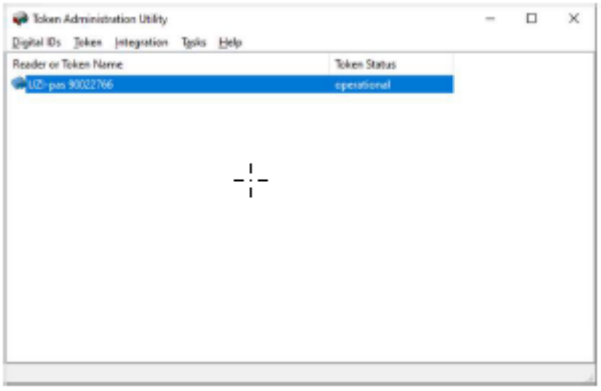
Ga vervolgens naar https://www.uziregister.nl/uzi-pas/installatie-van-kaartlezer-en-software en downloadt hier de safe sign minidriver Windows.

Pak het bestand uit en voer deze vervolgens uit als administrator (beheerder). Nadat u de Safe Sign software geïnstalleerd hebt kunt u deze vinden in het startmenu van Windows.



Klik op Token Administration

Het volgende programma wordt geopend. Zorg dat u de UZI pas in de cardreader gestoken hebt.



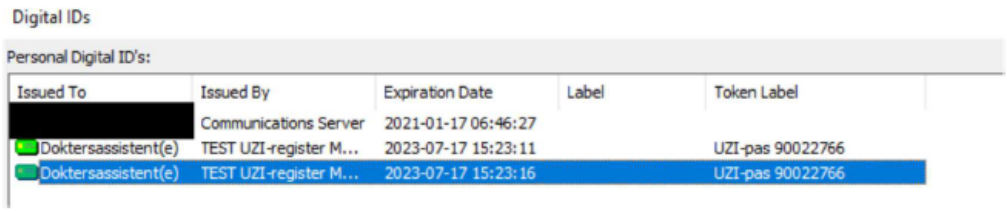
In principe is recentelijk een nieuwe versie uitgekomen van de SafeSign software waardoor de certificaten weer correct worden ingelezen. Chrome en Edge zouden hierdoor direct moeten werken.

Voor Firefox kiest u onder de SafeSign software Integratie -> installeer SafeSign onder Firefox. Als bovenstaande handelingen niet werken, ga dan door met de verdere stappen van deze handleiding.

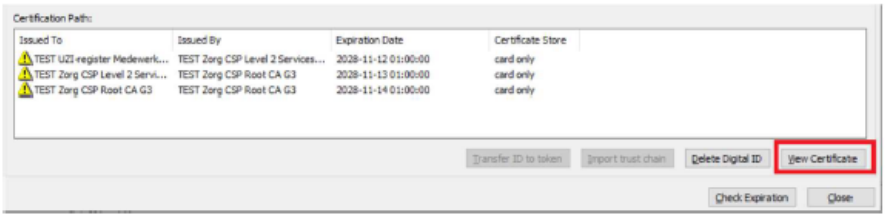
Als u nu al gebruik kunt maken van het dienstenportaal, stop dan hier.

Klik op ‘Digital IDs’ -> ‘Show registered digital IDs’

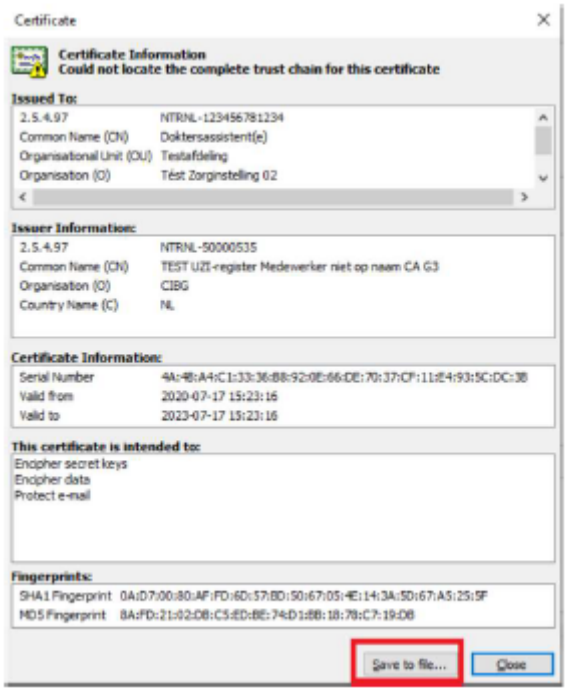
U ziet vervolgens in het bovenste venster een groen icoontje met uw functie of uw naam. U kunt hierop klikken met uw muis.



Onderin het scherm ziet u ‘Certification Path’. Hier worden de laatste 3 certificaten genoemd die nodig zijn om verbinding te krijgen met het dienstenportaal. U installeert deze als volgt:



Klik 1x op 1 van de certificaten met uw linkermuistoets. Het certificaat waar het woord ‘root’ in genoemd wordt opent u door op ‘View Certificate’ te klikken.



Klik vervolgens op ‘Save to file’. Zet deze vervolgens in de door u eerder aangemaakte certificaat map.

Herhaal deze stappen voor de andere 2 certificaten die u ziet. Noem deze 2 certificaten echter ‘intermediate1’ en ‘intermediate2’.

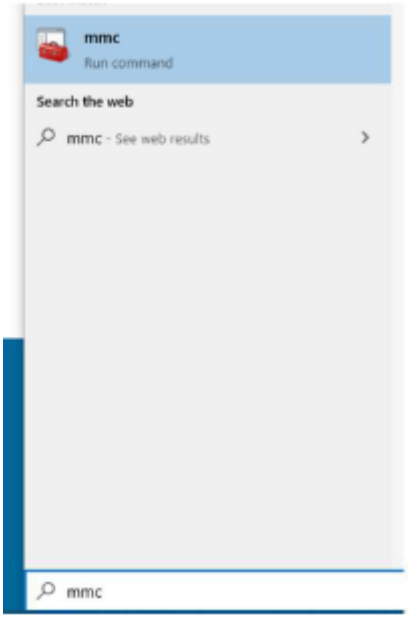
Het eindresultaat is dat u in de door u aangemaakte map 5 certificaten ziet.

- Staat der Nederlanden Root CA - G3
- QuoVadis PKIoverheid Server CA 2020
- De 3 certificaten die u zojuist heeft opgeslagen door te openen en op te slaan.

Deze verschillen dus per pas en zijn voor u, uw bedrijf of uw rol persoonlijk.

4. Voor ICT-beheerders: De certificaten installeren in de 'Microsoft certificate store'

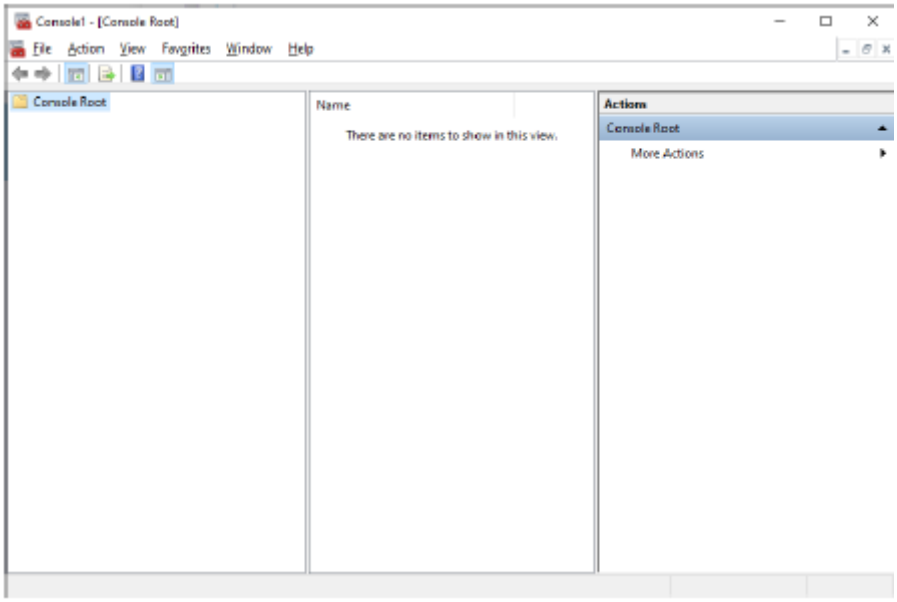
Klik links onder het vergrootglas (Zoekfunctie) van Windows aan en typ 'mmc' in op uw toetsenbord.



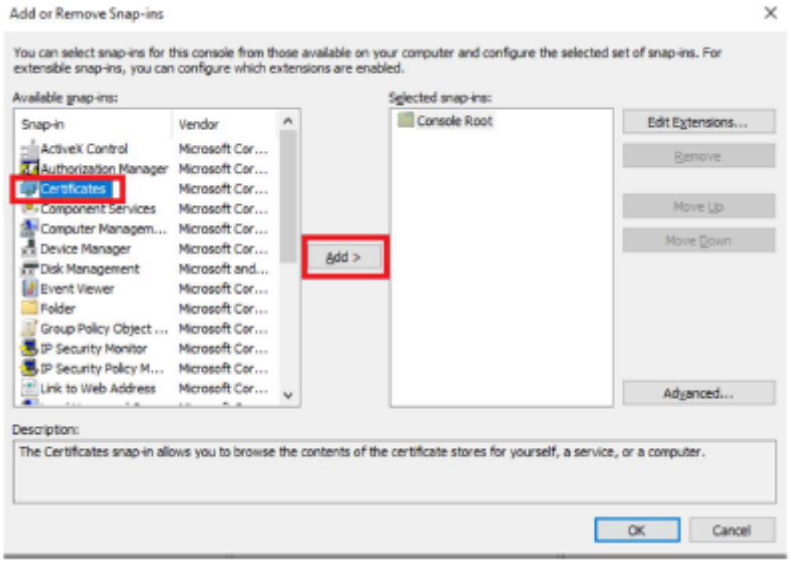
Klik met rechts op mmc en kies 'run as administrator' of 'uitvoeren als beheerder'

Geef een bevestiging op de tussenliggende vraag.

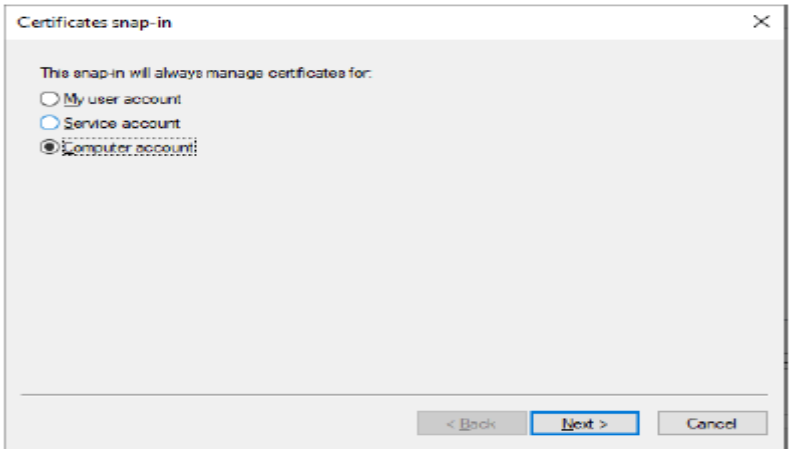
Het volgende scherm wordt geopend Klik hier op 'file' -> Add/Remove snap-in



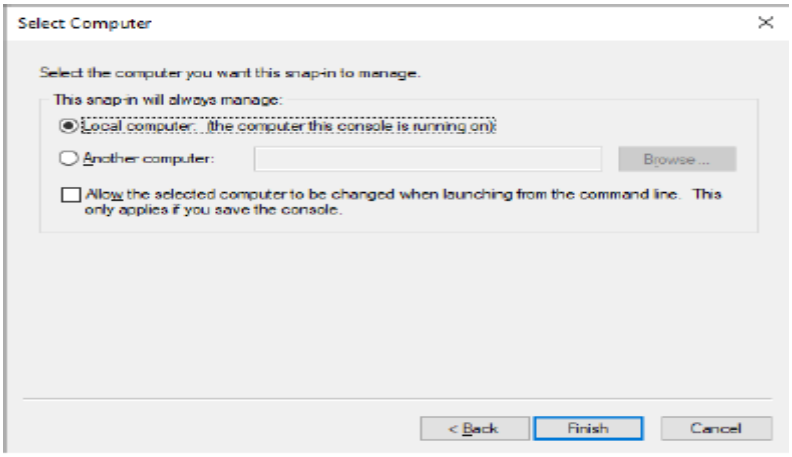
Klik ‘certificates’ aan en kies voor ‘Add’



Kies in het tussenliggende scherm voor ‘Computer account’ en kies voor ‘Next’

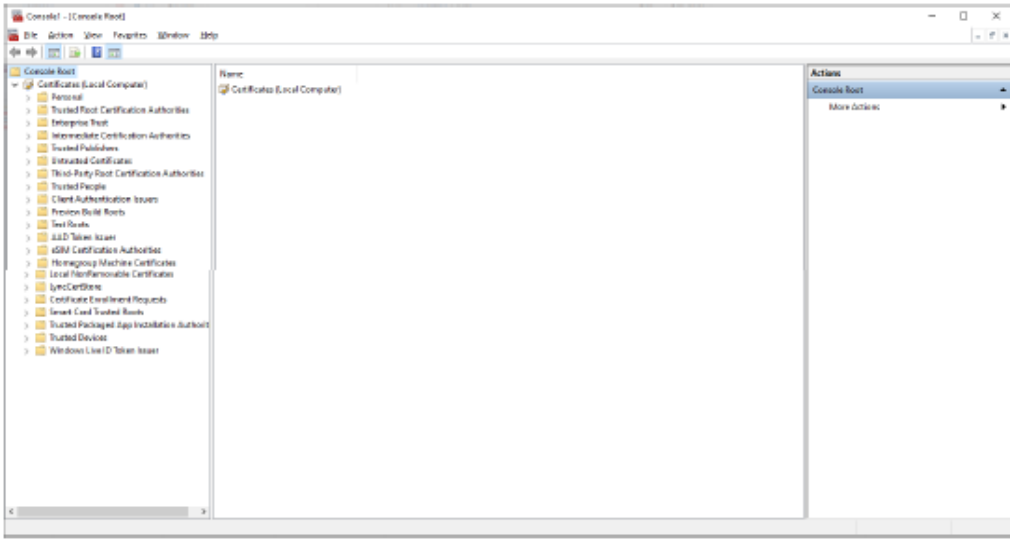


De keuze moet in het hierna volgende scherm op ‘Local computer’ staan. Klik op ‘Finish’ en ‘Ok’

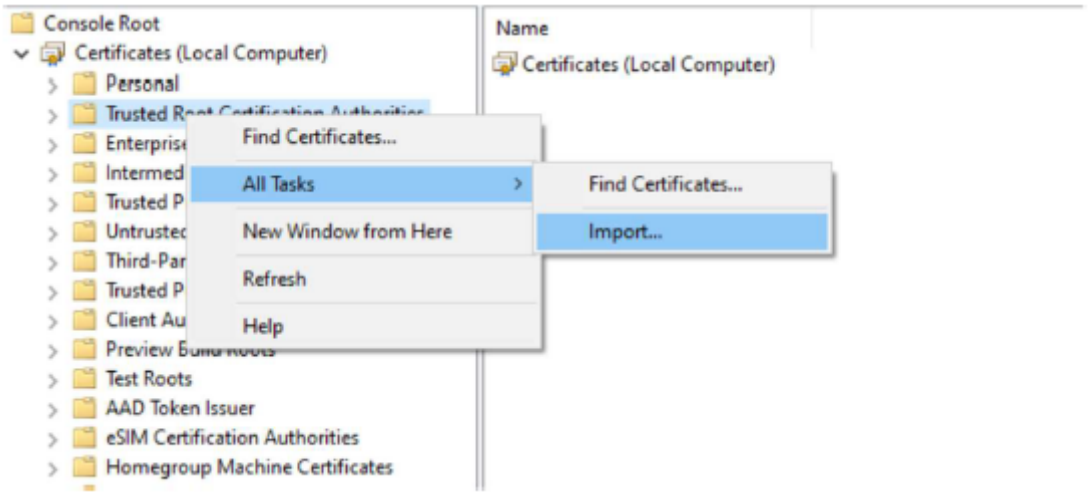


Het volgende scherm verschijnt in beeld

Klik hier het pull down menu ‘certificates (Local Computer)’ uit



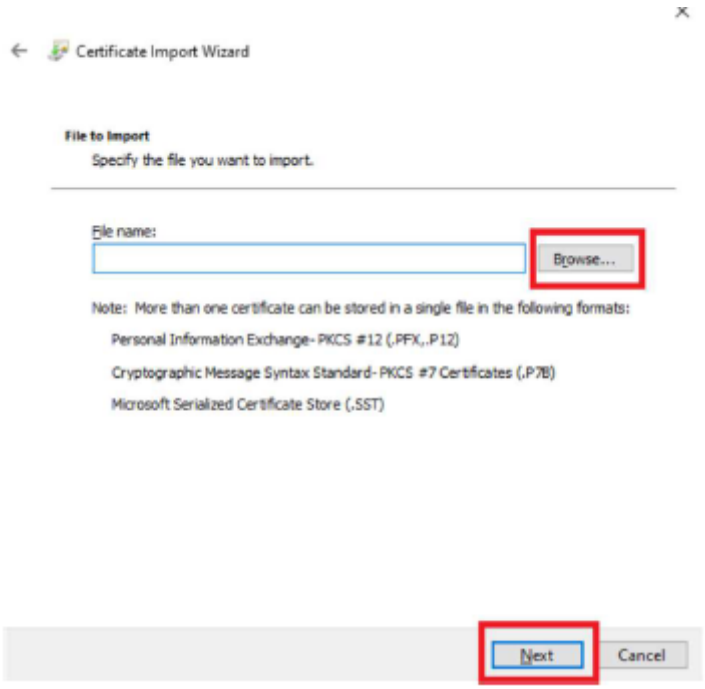
Klik met rechts op ‘Trusted Root Certification Authorities’ -> ‘All Tasks’ -> ‘import’



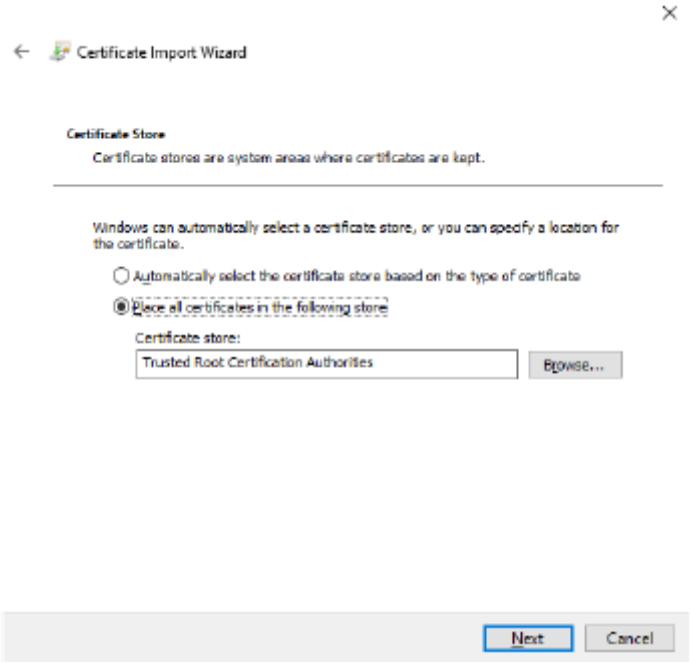
Klik in het eerste scherm op ‘next’

Klik vervolgens op de knop ‘Browse’ en ga naar de certificaat folder die u heeft aangemaakt.

Kies hier vervolgens het door u opgeslagen certificaat met de naam ‘root’



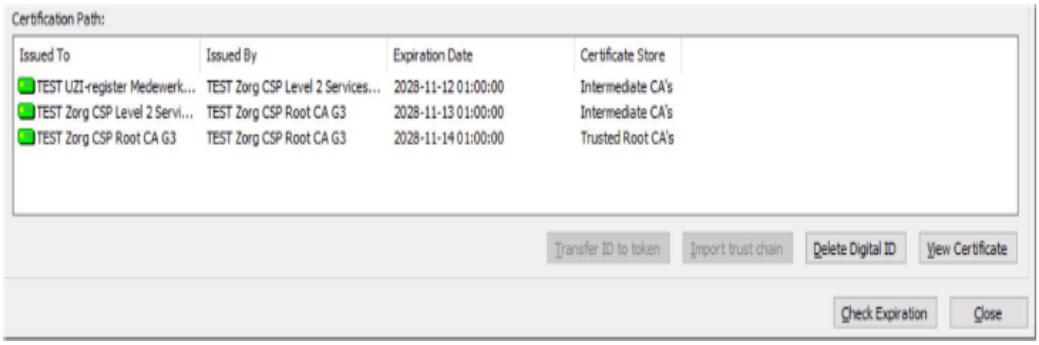
Klik op ‘Next’ -> ‘Place all certificates in the following store’ -> ‘Trusted Root Certification Authorities’ en in het volgende scherm op ‘Finish’. Klik op ‘Ok’ bij de melding dat het importeren van het certificaat succesvol was.



NB: Het certificaat ‘Staat der Nederlanden Root CA - G3’ zou reeds geïnstalleerd moeten zijn met de nieuwste Windows updates. Mocht dit niet zo zijn, herhaal dan bovenstaande stappen om het certificaat in de root store te importeren.

Vervolgens gaat u naar het pull down menu voor ‘Intermediate Certification Authorities’ of ‘Tussenliggende certificeringsinstanties’. Herhaal eerdere stappen (nb ‘All Tasks’ -> ‘Import’) en specificeer via de ‘browse’ knop de overige certificaten. In totaal voert u de procedure voor het importeren van de intermedia certificaten 3x uit. 2x voor de door u opgeslagen ‘intermediate1’ en ‘intermediate2’ certificaten en 1x voor het ‘QuoVadis PKIoverheid Server CA 2020’ certificaat.

Het eindresultaat is dat u in de door u geïnstalleerde ‘Safe Sign’ software de gehele certificate chain op groen ziet staan zoals hieronder.



Nu heeft u alle certificaten die benodigd zijn voor verbinding maken met het dienstenportaal geïnstalleerd. U kunt nu klikken op de link https://www.dienstenportaal.nl en inloggen met de door u bekende gegevens. Mocht u nog niet bekend zijn met de nieuwe omgeving, neem dan de instructie ‘handleiding dienstenportaal Ifzo’ door.