Aanschaf van een PKI Overheid Private Services Server certificaat

1.1 Schaf het certificaat aan in de webshop

1. Ga naar https://www.digicert.com/.
2. Kies bovenin voor “Buy” (of ‘Kopen’ als uw browser standaard alles vertaalt).
3. Kies onder “Trust Services” voor eIDAS/PKIo.
4. Als u iets naar beneden scrollt, vindt u onder het kopje “PKIOverheid Qualified Certificates” (PKIoverheid Gekwalificeerde Certificaten) de optie “Buy a TLS Certificate” (Koop een TLS-certificaat). Deze dient u te selecteren.
5. Voeg het product toe aan de winkelwagen via “Add to cart” (Voeg toe aan winkelwagen). Overigens kunt u bovenin de munteenheid op euro zetten als gewenst.
6. De winkelwagen vindt u rechtsbovenin. U kunt hier op klikken en kiezen voor “Go to cart” (Ga naar winkelwagen). Hier zou u het product “PKIo Private Services Server” moeten zien.
7. U kunt hier kiezen voor “Checkout”.

   Let op! Alleen creditcards en PayPal kunnen worden verwerkt. Is het van belang dat u op basis van een factuur dient te betalen, dan dient u een account aan te maken en vervolgens contact te zoeken met onze salesafdeling. Zie hiervoor “Betalen dmv factuur” (Addendum 1) en volg deze instructies. Houd er rekening mee dat de doorlooptijd hierdoor toe zal nemen met 1 à 2 werkdagen.
8. U vult uw gegevens in (naam, mailadres, telefoonnummer en organisatienaam en vervolgt met de betaling naar keuze (Creditcard of PayPal).
9. U vult uw betaalgegevens in en geeft op of u zelf wil optreden als contact inzake facturatie of dat dit iemand anders dient te zijn. Jaarlijks zult u een factuur ontvangen voor de dienst. Uiteraard kunt u het abonnement stopzetten als u er vanaf dat moment geen gebruik meer van wenst te maken.
10. U geeft uw BTW-nummer op en het adres waarop de factuur van toepassing is.

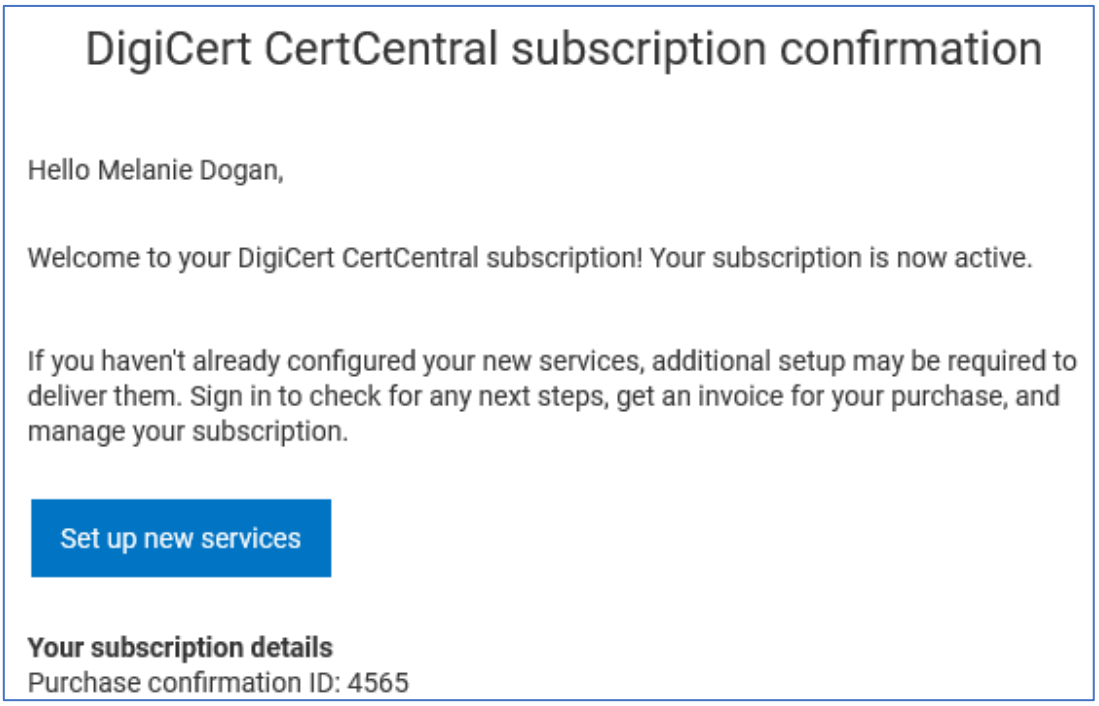
11. Geef uw Username (Gebruikersnaam) op (bij voorkeur uw mailadres – u kunt dan het vinkje plaatsen bij “Use my account email”) en maak een wachtwoord aan. Onthoud deze goed.
12. “Pay Now” (Betaal Nu)

1.2 Maak uw CertCentral account aan

Nu dient u uw accountaanmaak af te ronden. Dat kan op 2 manieren.

a. *U kunt direct na de bestelling in de browser kiezen voor.*

b. *Of u kunt dit doen via de mail, die u heeft ontvangen (van admin@digicert.com).*

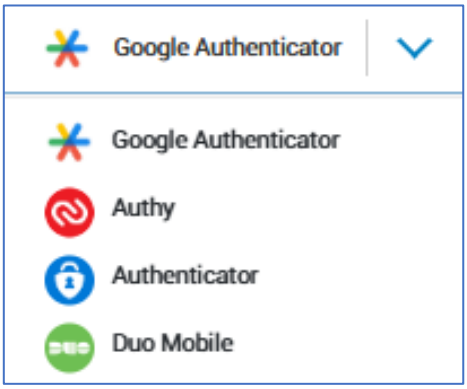


1. U gaat middels 1 van beide mogelijkheden naar “Set up (your) new services” (Nieuwe diensten instellen”).
2. Kies een beveligingsvraag en vul uw persoonlijke antwoord op deze vraag in. Dit is belangrijk, zodat we u deze vraag kunnen stellen (en u het antwoord kunt geven) als u ooit hulp nodig heeft met het account zelf.

3. Het is verplicht om gebruik te maken van OTP om in te loggen. Heeft u reeds een van de volgende authenticator apps op uw telefoon? Selecteer dan de juiste en scan de QR code door die specifieke app te gebruiken.

   Heeft u nog geen authenticator app? Download dan 1 van deze op uw telefoon en scan vervolgens de QR code die in beeld is middels de specifieke app.

   De betreffende apps waaruit gekozen kan worden:



4. De app geeft u vervolgens een code, die u kunt invullen bij One-time passcode (OTP).
5. Eenmaal ingevuld opent er een nieuw scherm. Dit is uw account en deze kunt u vanaf nu ook altijd benaderen door in te loggen via https://certcentral.digicert.eu/account/login.php met de gebruikersnaam en wachtwoord (1.1.11) en OTP code (1.2.4).
6. U gaat nu de gegevens invullen zodat de aanvraag van uw certificaat wordt doorgevoerd.

1.3 Certificaat aanvragen

U bent nu aangekomen op het punt om de certificaatdetails in te geven.

1. Ga naar “My Digital Trust Products” (Mijn Producten voor Digitaal vertrouwen) aan de linkerzijde (onder Dashboard) en kies voor “My subsription” (Mijn abonnement).
2. Klik op “Actions” (Acties) en “Request a certificate” (Vraag een certificaat aan).

   Krijgt u een foutmelding? Neem dan graag even contact op met gv.sales.nl@digicert.com met de vraag het product te activeren. Dit gebeurt soms. Zij horen graag welk accountnummer u heeft. Als u dit kunt vermelden in de mail, zullen zij het product activeren in het account. Uw accountnummer vindt u rechtsbovenin uw account als u op het pijltje naast uw organisatienaam klikt (#0000000). Eenmaal geactiveerd door sales, kunt u dit hoofdstuk doorlopen.

a. U dient te kiezen voor “Generate CSR in the browser” (Genereer een CSR in de browser) of “I have my CSR” (Ik heb mijn CSR). Indien u het certificaat gebruikt voor DigiPoort is het hier het eenvoudigst om te kiezen voor “Generate CSR in the browser” (Genereer een CSR in de browser). U krijgt dan uiteindelijk een link om het certificaat als .p12 te downloaden, dat u vervolgens kunt koppelen aan uw softwarepakket. Kiest u er toch voor een eigen CSR te genereren, dan zult u het certificaat (.p7b of .crt) op een later moment zelf moeten converteren naar een .p12 bestand.

b. U dient een domeinnaam op te geven. Daar mag u uw eigen domein opgeven. Houd er dan rekening mee dat dit gevalideerd dient te worden en dat u hiervoor stappen moet doorlopen. U mag ook kosteloos een domeinnaam van ons gebruiken, zodat wij die stappen voor u doorlopen. Vink in dat geval “Use a DigiCert qvt.nl domain” (Gebruik een DigiCert qvtl.nl-domein) aan.

c. U kiest de doorlooptijd. Het abonnement wordt jaarlijks in rekening gebracht, maar u kunt kiezen voor een langere looptijd. Dit betekent dat u de betaling wel jaarlijks doet, maar het certificaat niet ieder jaar opnieuw hoeft te worden aangevraagd en geïnstalleerd. Let op dat u hier de juiste optie aanklikt. Het standaardvinkje heeft doorgaans niet te voorkeur.

d. Kies als DCV method (methode) “DNS TXT Record” en als DCV scope (bereik) “submit exact domain voor validation” (dien de exacte domeinnaam in ter validatie) wanneer u gekozen hebt voor een **qvtl.nl domein** (1.3.2.b). Gebruikt u een eigen domein? Dan geeft de “i” meer informatie over de mogelijkheden.

e. Additional certificate options (Aanvullende certificaatopties) mag u overslaan.

f. U kunt vervolgens kiezen voor “Add Organization” (Organisatie toevoegen) door op de knop te klikken. Als het goed is heeft u eerder de juiste gegevens opgegeven. Dan kunt u kiezen voor “Existing Information” (Bestaande Organisatie) en kunt u kiezen voor “Add” (Toevoegen). U mag ook een nieuwe organisatie aanmaken als de gegevens daar niet juist zijn.

g. Organisation Identification Number (OIN) or Dutch KVK-number (HRN). Het vinkje staat standaard juist. Voor DigiPoort wil u een OIN/HRN in uw certificaat opnemen, omdat het anders niet zal werken. U dient dit nummer zelf in te vullen. Het nummer dient 20 karakters te zijn. Heeft u een OIN, dan is dit nummer bij u bekend. Heeft u geen OIN?

   Zorg dat dat u zo een 20-cijferig nummer invult:00000003 + KVKnummer + 0000
   Voorbeeld (als uw KVKnummer 12345678 is): 00000003123456780000

h. U dient een bevoegd vertegenwoordiger op te geven. Deze persoon dient **zelfstandig** bevoegd te zijn volgens de Kamer van Koophandel. Is de persoon dat niet? Geen probleem, maar dan hebben we een volmacht nodig. Meer informatie is hier te vinden: volmacht.

   Als u hier namen ziet, kunt u de betreffende persoon selecteren. Zo niet, klik dan het vakje “New contact” (Nieuw contact) aan en vul de naam en contactgegevens van deze persoon in. U kunt dit uiteraard zelf zijn. Klik op “Add” (Toevoegen).

i. U hoeft geen technisch contact toe te voegen, dus u kunt verder door aan te vinken dat u gebruikersvoorwaarden en de Master service agreement accepteert.

j. Dit resulteert in een order. Het ordernummer kunt u terugvinden door links bij “My Digital Trust Products” (Mijn Producten voor Digitaal Vertrouwen) aan de linkerzijde (onder Dashboard) te kiezen voor “Certificates” (Certificaten). U kunt hier ook de status zien van een aantal controles die wij dienen te doen.

1.4 Controles

U kunt in uw account volgen welke controles wij reeds hebben afgerond en wat er nog van u wordt verwacht.

Voor Digipoort kan de status wat verwarrend zijn, dus beschrijven we hieronder welke controles er plaatsvinden en waar we uw hulp bij nodig hebben.

1. CSR - Indien u heeft gekozen voor het genereren van een CSR in de browser wordt er in een later stadium (1.5 installeren certificaat) een email verzonden met een link om de CSR in de browser te genereren. Tot die tijd zal de status CSR op pending (oranje) blijven staan.

2. “Prove control over domains” (Bewijs controle over domeinen) is misleidend als u gekozen heeft voor qvtl.nl. Dan zullen wij dit verzorgen. U hoeft geen actie te nemen. Gebruikt u een eigen domein, dan dient u de validatie zelf af te ronden.

3. “Order approval” (Goedkeuring van de bestelling) volgt als wij alle controles aan onze kant hebben doorlopen. Degene die is opgegeven als bevoegd vertegenwoordiger (1.3.3.h) krijgt dan een e-mail met een link om de aanvraag goed te keuren. Wanneer deze persoon (mogelijk uzelf) deze link volgt en goedkeuring geeft, kunnen we het certificaat ter download aanbieden mits de domeinvalidatie is uitgevoerd (zie punt 2 hierboven).

4. **Identiteitsvaststelling van de bevoegd vertegenwoordiger**. Dit is niet duidelijk te volgen in uw account. Maar na plaatsing van de bestelling, ontvangt de bevoegd vertegenwoordiger (1.3.3.h) direct een e-mail om een identiteitsvaststelling per app te doorlopen. De mail heet “Verify your identity” en wordt verzonden vanaf noreply@digicert.com. De instructies spreken voor zich, maar u kunt meer vinden in Addendum 2 Identiteitsvaststelling.

5. Controles die wij aan onze kant zullen doen bestaan met name uit het opvragen van een KVK-uittreksel en het controleren van alle data die u heeft ingevuld. Bij vragen of problemen, zullen we direct contact met u opnemen. Heeft u vragen over openstaande controles betreffende een aangevraagd certificaat? Neem dan contact op via nl.validation@digicert.com.

6. Als **alle controles** gedaan zijn, zal de bevoegd vertegenwoordiger een mail krijgen om de order goed te keuren. De mail wordt verstuurd vanaf no-reply@digitalcertvalidation.com en heeft als onderwerp “Please approve digital certificate order #XXXXXXXXXX for account XXXXXXX”. De link in de e-mail dient gevolgd te worden om de aanvraag goed te keuren. De certificaataanaanvrager krijgt na deze goedkeuring de mail om het certificaat in gebruik te nemen. Zie hiervoor hoofdstuk 1.5.

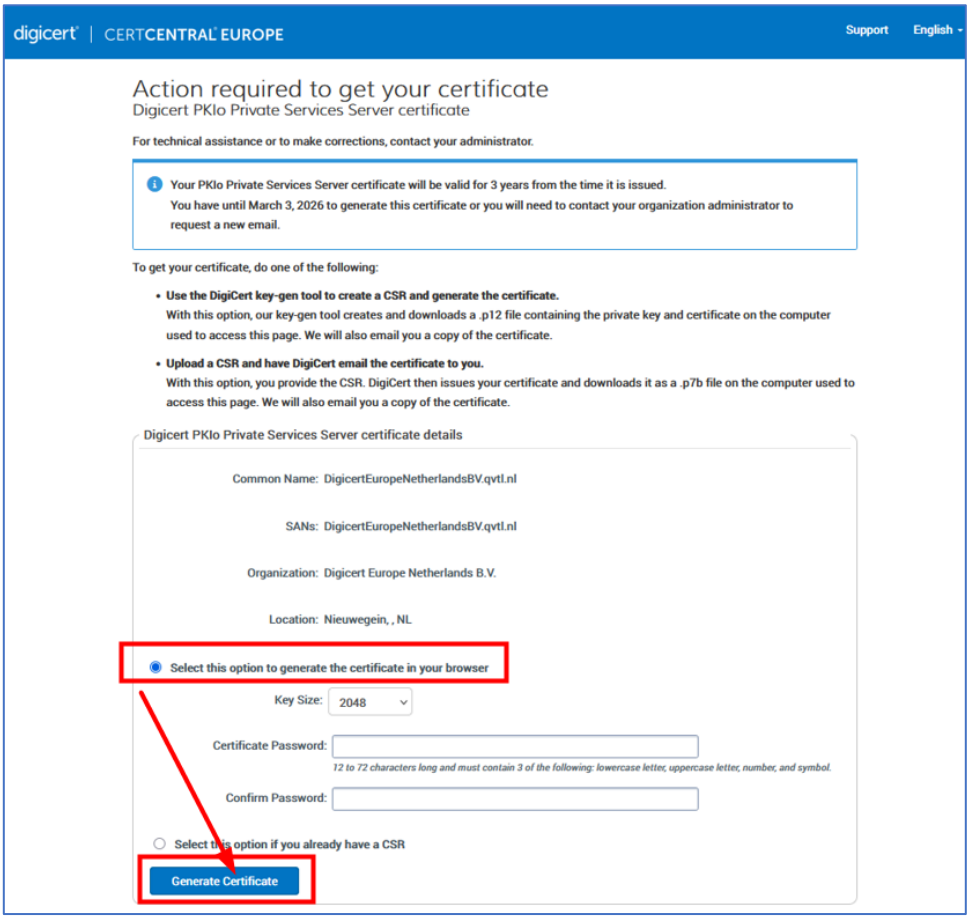
1.5 Installeren certificaat

U bent nu aangekomen bij de laatste stap. Indien u bij hoofstuk 1.3, punt 2a, heeft gekozen voor “Generate CSR in the browser” (Genereer een CSR in de browser), dan heeft u als aanvrager een mail ontvangen van admin@digicert.com, met als onderwerp “Create Your DigiCert PKIo Private Services Server Certificate”. U gaat het certificaat aanmaken in P12 formaat. Houd er rekening mee dat u het certificaat en het wachtwoord zorgvuldig bewaart, zodat er geen misbruik van kan worden gemaakt.

1. In deze mail zit een link, die u dient te volgen (vb: https://certcentral.digicert.eu/link/generate-cert/upload-csr.php?token=reeks-cijfers-en-letters).

   Gebruik hiervoor geen Microsoft Edge als standaard browser type, deze ondersteunt het maken van het sleutelpaar voor het certificaat niet zomaar.

2. U komt dan in het volgende scherm:

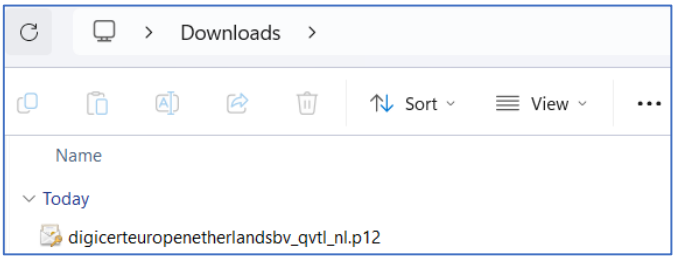


Het juiste vakje is aangevinkt en u wordt gevraagd een wachtwoord aan te maken. Onthoud dit wachtwoord goed of sla deze op in een wachtwoordmanager. Het is niet mogelijk deze te resetten als u het wachtwoord niet meer weet.

3. U kunt klikken op “Generate certificate”.

   U krijgt in uw scherm de text te zien: “Your DigiCert PKIo Private Services Server certificate has been generated and should now be downloaded”.

4. Het certificaat zelf kunt u nu terugvinden in uw downloadmap (met uw organisatienaam op de plek van digicerteuropenetherlandsbv of met uw gekozen domeinnaam):



   Het is aan te raden dit bestandje ergens anders te bewaren, zodat u deze kunt terugvinden wanneer nodig. Dat kan eenvoudig, door met de rechtermuisklik te kopiëren en elders te plakken. Als u het bestand op de juiste plek (in een specifieke map) hebt opgeslagen, kunt u de versie in uw download folder verwijderen.

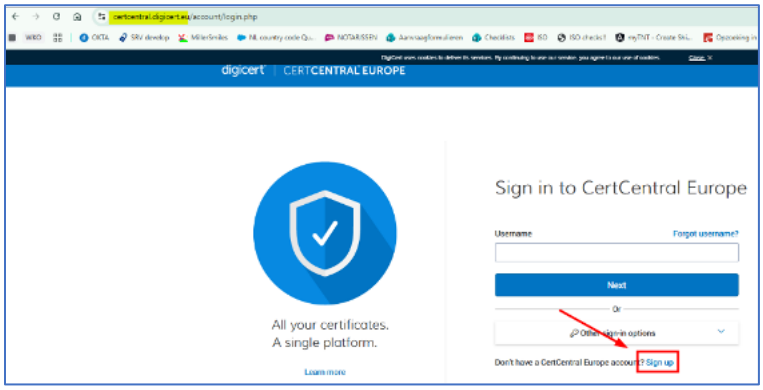
Dit is het bestand dat u dient te uploaden in uw softwarepakket. Het pakket zal vragen om een wachtwoord of pincode. Dat is het wachtwoord dat u zojuist heeft aangemaakt bij punt 1.5.2.

Er volgt nog een laatste e-mail met als onderwerp “Your certificate for *gekozen domeinnaam*” van admin@digicert.com met een ZIP-file als bijlage. U heeft deze in principe niet nodig. Mocht er op enig moment iemand vragen om het *publieke deel* van uw certificaat. Dan kunt u deze hierin vinden als “*domeinaam.crt*”. In de bijlage zit **niet** het certificaat dat u koppelt aan het softwarepakket, dat u zojuist heeft gedownload.

Addendum 1 Betalen dmv factuur

Indien u niet kunt betalen via Credit card of Paypal, dan kunt u de volgende stappen volgen.

1. Ga naar https://certcentral.digicert.eu/account/login.php.
2. Heeft u reeds een account, dan kunt u hier inloggen. Heeft u deze nog niet, kies dan voor “Sign up” (Meld je aan!). Mocht u twijfelen of u een account heeft, kunt u kiezen voor “sign up”. Indien het mailadres bekend is, wordt u gewaarschuwd dat er al een account bestaat.



3. Vul de gevraagde gegevens in
    - Your information (Uw gegevens) – naam, zakelijk, persoonlijk, mailadres, telefoonnummer en functietitel.
    - Organization information (Organisatie-informatie) – naam, telefooonnummer (mag uw directe nummer zijn) postcode, adres, plaatsnaam en provincie.
    - Account information (Accountgegevens) verzin een username (gebruikersnaam), zoals bijvoorbeeld uw mailadres, en maak een wachtwoord aan. U dient hier ook 2 beveiligingsvragen te selecteren en het antwoord daarop in te vullen. Vul uw BTW-nummer in (Een Nederlands btw-nummer begint met NL, dan komen 9 cijfers, de letter B en dan nog eens 2 cijfers) en plaats een vinkje in het hokje omtrent de algemene voorwaarden.
    - Kies voor “Sign up”.
    - U dient een OTP aan te maken. Zie 1.2.3 voor meer informatie.
4. Eenmaal doorlopen, zult u aangemeld worden in uw account (dit kan overigens ook via de mails die u inmiddels heeft ontvangen. Rechtsbovenin, onder uw organisatienaam, vind u uw accountnummer #0000000. Sales zal u moeten helpen de betaling per factuur aan te zetten en te zorgen dat het product actief wordt gemaakt in uw account.

Vriendelijk verzoek om, wanneer u bovenstaande heeft doorlopen, een mail te sturen naar gv.sales.nl@digicert.com, waarin uw accountnummer vermeldt en de wens om een PKI Overheid Private Services Server certificaat – voor Digipoort aan te schaffen middels betaling per factuur. Zij zullen contact met u opnemen en u verder helpen.

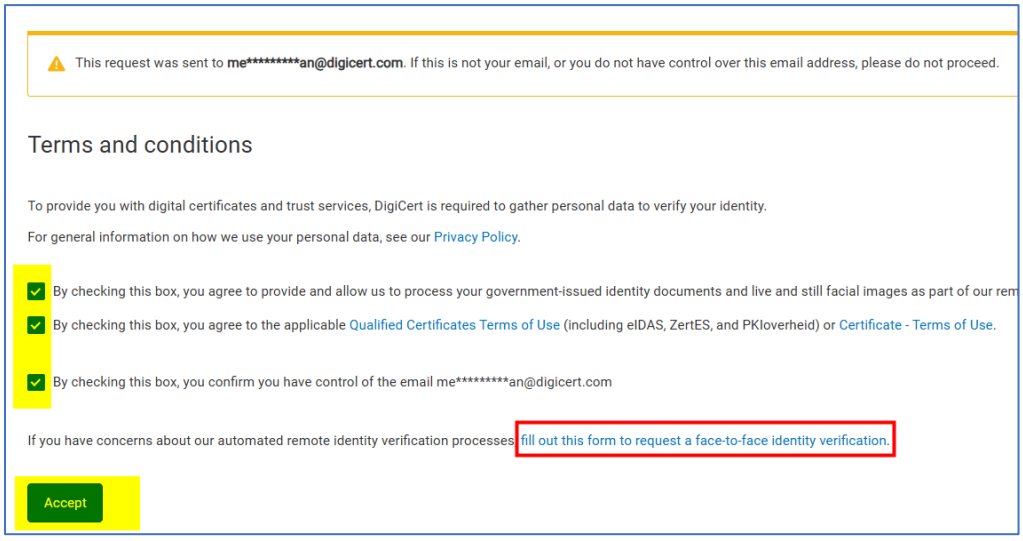
Addendum 2 Identiteitsvaststelling

Na plaatsing van de bestelling, ontvangt de bevoegd vertegenwoordiger (1.3.3.h) direct een e-mail om een identiteitsvaststelling per app te doorlopen. De mail heet “Verify your identity” en wordt verzonden vanaf noreply@digicert.com.

In deze mail zit een link https://certcentral.digicert.eu/biometric-consent/nummer die gevolgd dient te worden

De vertegenwoordiger vinkt alle hokjes aan (zie geel gearceerd) en klikt “Accept”.

> Let op: indien deze persoon geen gebruik wenst te maken van de app, kan het identificeren ook via een notaris (en, in sommige gevallen, een koerier). De doorlooptijd zal dan een aantal dagen toenemen. Maar indien dit gewenst is klikt de gebruiker op de tekst in het rode kader.



Het volgende scherm laat zien welke app de gebruiker kan downloaden op de telefoon (scan met de camera-app op de telefoon de QR code van toepassin).

Eenmaal gedownload kan de gedownloade app worden geopend en vraagt deze om de code die in het scherm te zien is. Het is geen probleem om op een later moment verder te gaan. U kunt dan de link in de eerdere mail nogmaals volgen.

Als de code is ingevuld in de app, zal de app vragen het paspoort/de identiteitskaart (geen rijbewijs) te scannen en een aantal selfies te maken. Dit werkt vaak het best als:

- u zorgt dat NFC herkenning is ingeschakeld op een androïd telefoon (iPhones zouden het automatisch moeten accepteren)
- -het originele identiteitsbewijs op een vlakke ondergrond wordt gelegd tijdens het uitlezen van de NFC (chip)
- -deze niet wordt afgeschermd door vingers/duimen
- -weerkaatsing van direct (zon)licht wordt vermeden

Als de app geheel is doorlopen, zal deze terugkeren naar het scherm waar een code wordt gevraagd. Dit betekent helaas niet altijd (wel bijna altijd) dat de vaststelling succesvol was. Deze zal nu beoordeeld worden door IDNow, waarna wij een succes doorkrijgen per rapport (doorgaans binnen 30 minuten).