Handleiding aanmaak CSR

Digipoort SBR

Voordat u begint:

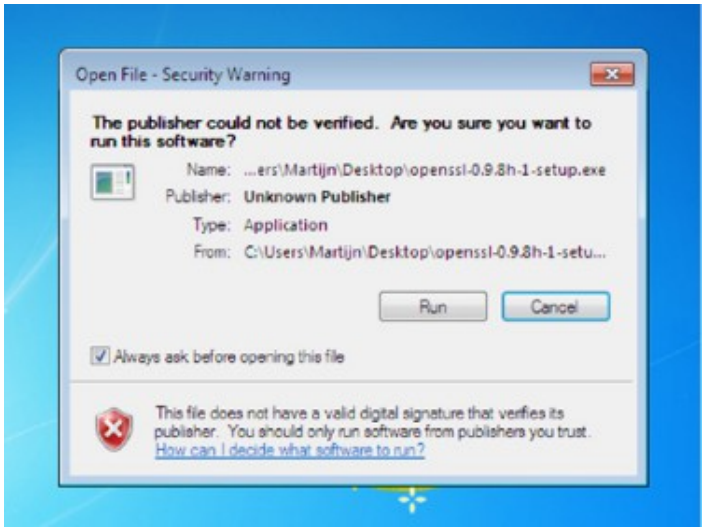
Om een Certificate Signing Request (CSR) te maken moet het programma [OpenSSL] geïnstalleerd worden. Dit programma kan geheel gratis gedownload worden vanaf de OpenSSL website middels de volgende link: http://gnuwin32.sourceforge.net/packages/openssl.htm
Let op!: Er zijn verschillende bestanden beschikbaar, kies voor:
"Complete package, except sources"

Hoewel de installatie voor zich spreekt zou het voor kunnen komen dat u hier meer informatie over wil raadplegen. U kunt de OpenSSL installatie handleiding door nemen via de volgende link: http://gnuwin32.sourceforge.net/install.html

Wanneer u geen (administrator) rechten of kennis heeft om software te installeren dient u uw systeem beheerder om advies te vragen. Het aanmaken van een CSR hoeft niet perse op een server. Het kan ook op uw desktop, zeker in het geval van een certificaat voor SBR communicatie, voer dan de stappen uit op het apparaat waar het certificaat gebruikt gaat worden. Tevens adviseren wij u sterk om OpenSSL niet te deinstalleren na het proces maar gewoon te laten staan

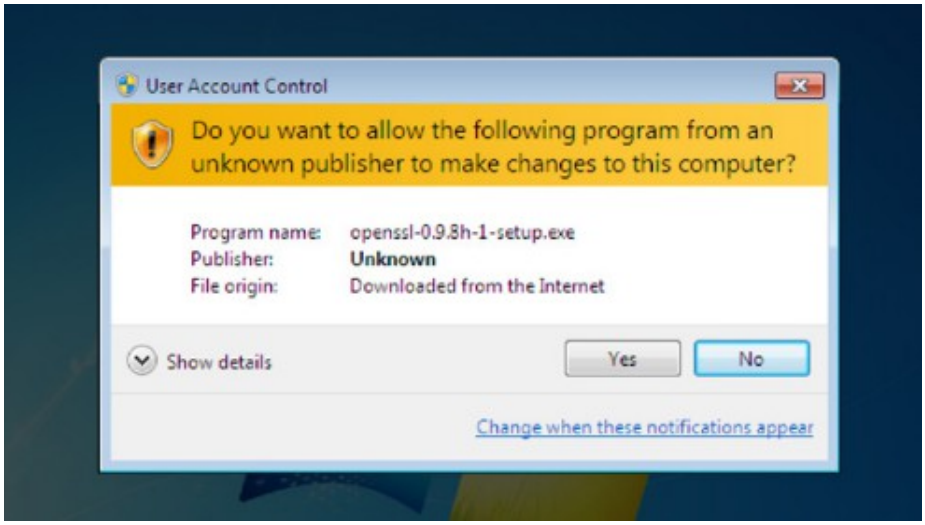
Stap 1: Installatie OpenSSL

1.1) Na het downloaden van OpenSSL dient het programma allereerst geïnstalleerd te worden. Dubbelklik op het bestand dat u van de OpenSSL website heeft gedownload. Windows zal u nu eerst een waarschuwing geven over het uitvoeren van bestanden afkomstig van het Internet. U kunt deze waarschuwing negeren en op "run/uitvoeren" klikken.



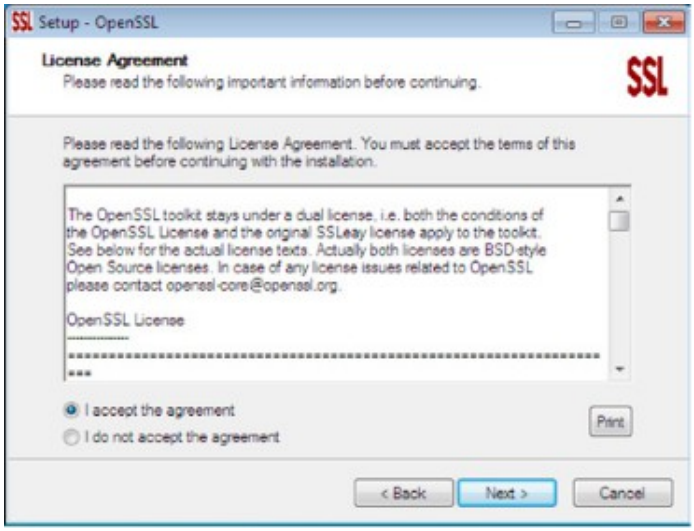
Figuur 1: De waarschuwing. Dit scherm kan variëren afhankelijk van de versie van Windows die u gebruikt.

1.2) Windows UAC zal op Windows Vista en hoger ook om toestemming vragen om het bestand uit te kunnen voeren met administrator rechten, ook hier kunt u instemmen door op "Ja/Yes" te klikken.



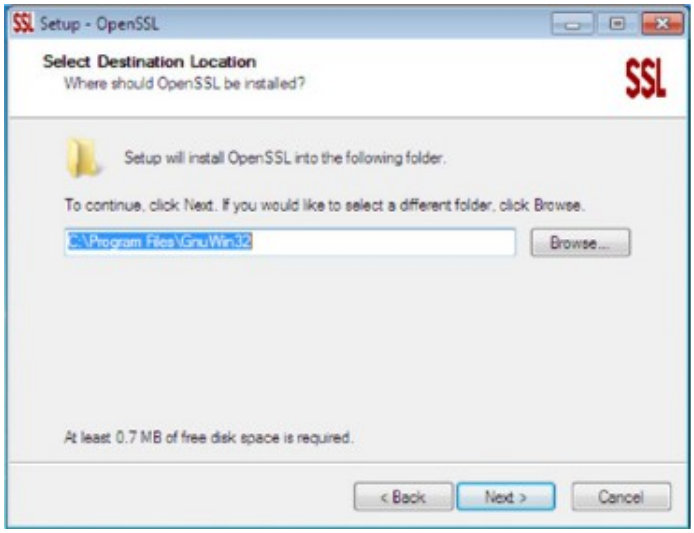
Figuur 2: het Windows UAC venster (alleen in Windows Vista en hoger)

1.3) Nu ziet u het eerste scherm van de installatie, met een korte samenvatting over wat er op uw systeem geïnstalleerd gaat worden. U kunt verder gaan met de installatie door op “Next” te klikken. U dient akkoord te geven voor de licentie en kunt pas verder met de installatie wanneer u kiest voor “I accept the agreement” en vervolgens op “Next” klikt.



Figuur 3: Kies voor “ I accept the agreement” om verder te gaan met de installatie

1.4) Kies in alle volgende schermen voor de optie “Next”. Wij raden u sterk aan de installatie opties niet te veranderen, deze handleiding gaat er dan ook van uit dat u het standaard installatie pad gebruikt.



Figuur 4: Het standaard installatie pad, wij adviseren u dit niet aan te passen

1.5) De installatie van Open SSL is nu voltoid, klik op “Finish” om de installatie af te ronden.

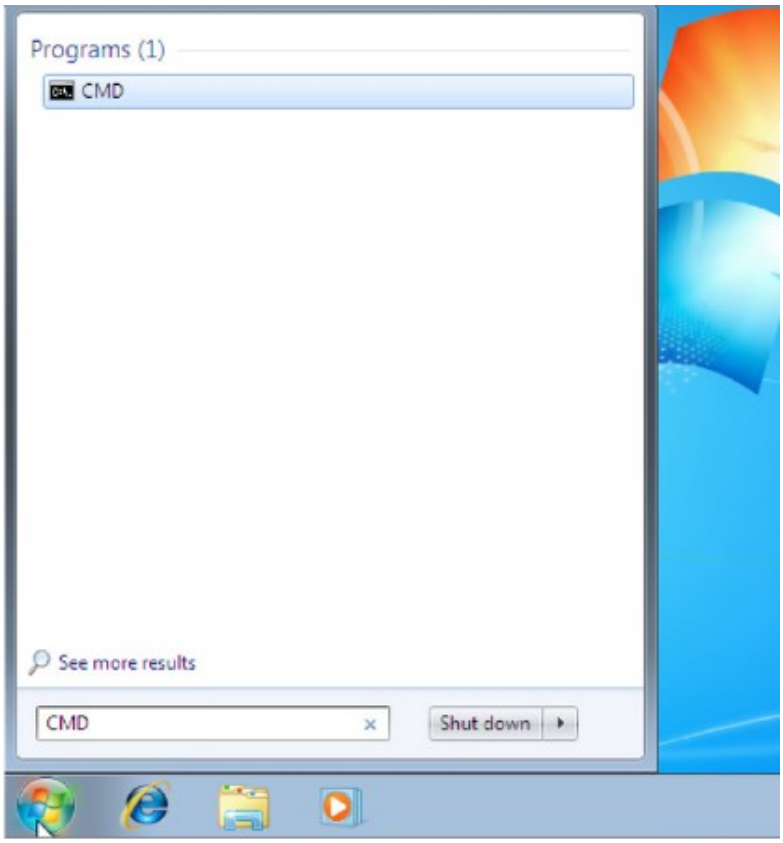
Figuur 5: De installatie is afgerond

Hiermee is de eerste stap van het proces compleet. U kunt nu verder met de tweede stap waarin u het CSR daadwerkelijk aan gaat maken.

Stap 2: Aanmaken CSR

Het aanmaken van uw CSR wordt voornamelijk uitgevoerd in het Windows command prompt, afhankelijk van uw Windows versie kan de manier waarop u het command prompt opstart verschillen.

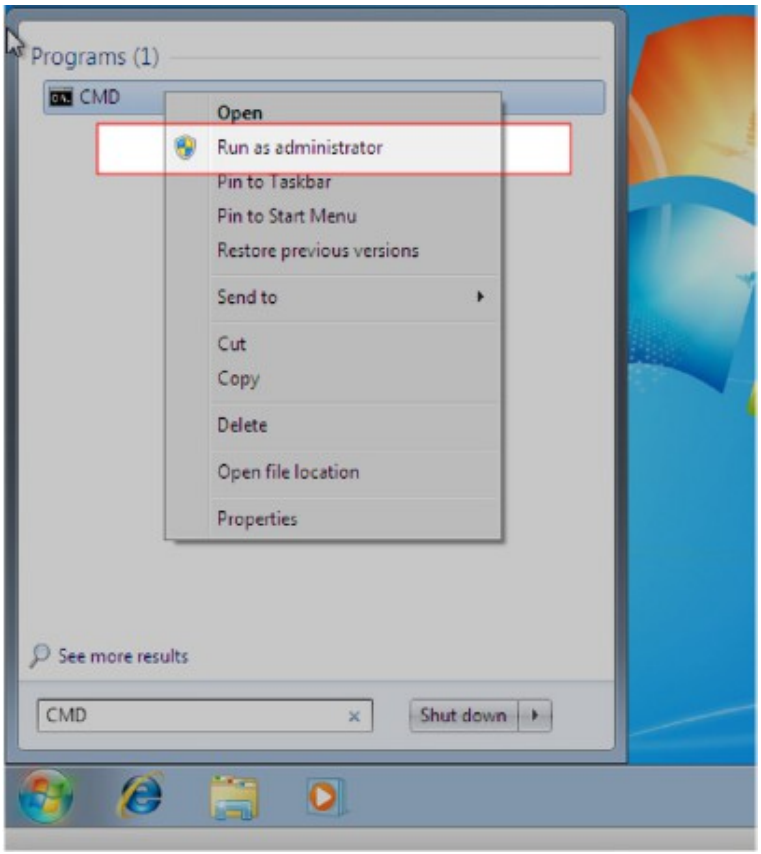
2 .1) Start uw command prompt op. Klik op de Windows start knop (of druk de Windows key op uw toetsenbord in) en type in het zoek/uitvoeren veld aan de onderkant van het start menu de letters “CMD” in.



Figuur 6: Het Windows start menu met onderaan het zoek veld

Op Windows XP/Server 2003 gebaseerde systemen kunt u vervolgens gewoon op Enter drukken. Maakt u echter gebruik van Windows Vista of hoger (te herkennen aan het feit dat u in Stap 1 het Windows UAC venster te zien heeft gekregen) dan is het noodzakelijk om een aanvullende stap uit te voeren. Zie hiervoor stap 2.2

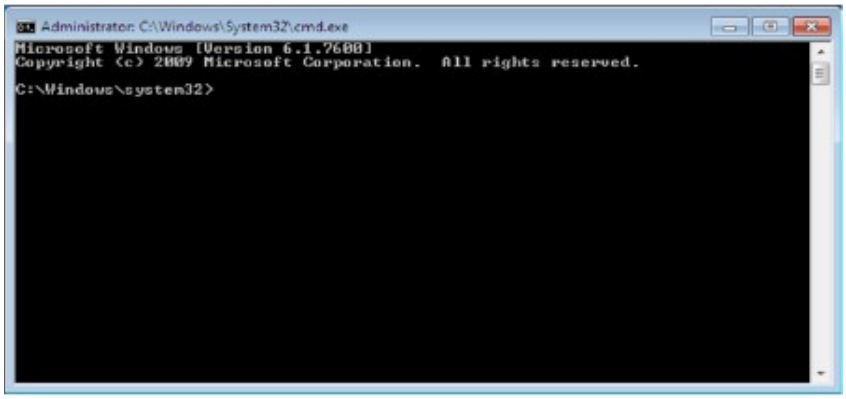
2.2) Command Prompt als administrator uitvoeren op Windows Vista en Hoger. Op Windows Vista en Windows 7 is het nodig om expliciet aan te geven dat uw command prompt extra rechten nodig heeft.



Figuur 7: voer het command prompt als administrator uit

Klik met de rechtermuisknop op het CMD icoon en klik op “Als Administrator Uitvoeren” en vervolgens, wanneer Windows u vraagt of u zeker weet dat u dit wilt doen, op “Ja”.

2.3) Als u de voorgaande stappen heeft uitgevoerd heeft u nu uw command prompt venster open staan. In dit venster dient u een aantal commando's in te voeren.



Figuur 8: het Windows Command Prompt

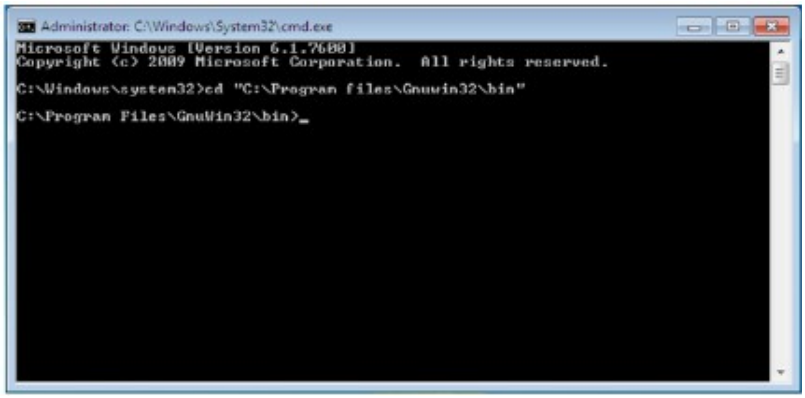
2.4) Type de volgende opdracht:

cd "C:\Program Files\Gnuwin32\bin"

OF: Gebruikt u een 64-bit versie van windows 7?

voer dan de volgende opdracht uit:

cd "C:\Program Files (x86)\Gnuwin32\bin"



Figuur 9: de directory is gewijzigd

2.5) Voer vervolgens het onderstaande commando uit.

set OPENSSL_CONF=c:\program files\gnuwin32\share\openssl.cnf

OF: Gebruikt u een 64-bit versie van windows 7, voer dan het volgende commando uit:

set OPENSSL_CONF=c:\program files (x86)\gnuwin32\share\openssl.cnf

2.6) Nu gaat u een CSR commando maken waarmee u uw CSR kan genereren. U kunt het onderstaande template gebruiken om uw commando te maken (Let op! Op dit moment kunnen wij alleen certificaten met een RSA-2048 sleutel accepteren):

openssl req -nodes -newkey rsa:2048 -keyout private.key -out CSR.csr -subj "/serialNumber=<OIN>/C=<Landcode>/ST=<Provincie>/L=<Plaats>/O=<Organisatie>/OU=<Afdeling>/CN=<Domeinnaam>"

Vervang het gegevens tussen de < en> met uw eigen gegevens. U kunt een uitleg van de gegevens hieronder vinden.
Zorg ook dat u het < en > verwijdert, anders zal deze commando niet correct werken.
Een werkende commando ziet er zo uit:

openssl req -nodes -newkey rsa:2048 -keyout private.key -out CSR.csr -subj "/serialNumber=00000003123456780000/C=NL/ST=Zuid-Holland/L=Den Haag/O=example/OU=algemeen/CN=sbr.example.nl"

Domeinnaam:

U vult hier uw domeinnaam in, in de volgende vorm: sbr.uwdomein.nl
Het is niet noodzakelijk dat er een website op dit subdomein (sbr.) aanwezig is, de reden dat uw certificaat met dit subdomein geassocieerd zal worden is om conflicten met eventuele bestaande certificaten op uw domein te voorkomen.
Vraagt u een PKIOverheid SSL certificaat aan (niet voor SBR communicatie, maar bijvoorbeeld voor een website)?
Dan moet u hier de domeinnaam invullen waar uw certificaat uw gebruikt gaat worden, is deze domeinnaam niet correct, dan zal het certificaat niet juist werken.

Landcode:

In dit veld vult u de ISO landcode van uw land in, normaliter is dit: NL
(het is momenteel nog niet mogelijk SBR certificaten voor landen buiten Nederland te maken)

Provincie:

U vult hier de volledige naam van de provincie waar uw bedrijf gevestigd is in, zonder afkortingen.

Plaats:

De plaatsnaam waar uw bedrijf gevestigd is, wederom zonder afkortingen.

Organisatie:

De naam van uw bedrijf, zoals deze bekend staat bij de Kamer van Koophandel.

Afdeling:

Indien van toepassing kunt u hier de afdeling waar het certificaat voor is noteren, gebruik hiervoor geen speciale tekens (< > ~ ! @ # $ % ^ * / \ ( ) ?).
Als het certificaat niet voor een speciale afdeling is vult u in dit veld “Algemeen” in.

OIN:

OIN staat voor
Overheids Identificatie Nummer. In de meeste gevallen is dit nummer gebaseerd op uw KvK nummer. De opbouw is als volgt:

[00000003] + [uw 8 cijferig KvK nummer] + [vestigingsnummer, 4 tekens]

Als u geen specifiek vestigingsnummer heeft, dan vult u simpelweg 0000 in. Het resultaat is dus een enkel 20- cijferig nummer. Vul dit nummer zonder spaties in.
Voorbeeld:
00000003123456780000

Mocht u al in het bezit zijn van een OIN verstrekt door Digikoppeling of een FI-nummer uitgegeven door de Belastingdienst, raadpleeg dan de tabel aan de onderkant van deze handleiding.

2.7) Wanneer u weer terug bent in het Windows command prompt venster kunt u het commando dat u in de voorgaande stap heeft aangemaakt plakken (rechtermuisknop in het venster => plakken) en druk dan op ENTER. Hiermee zal het CSR aangemaakt worden.

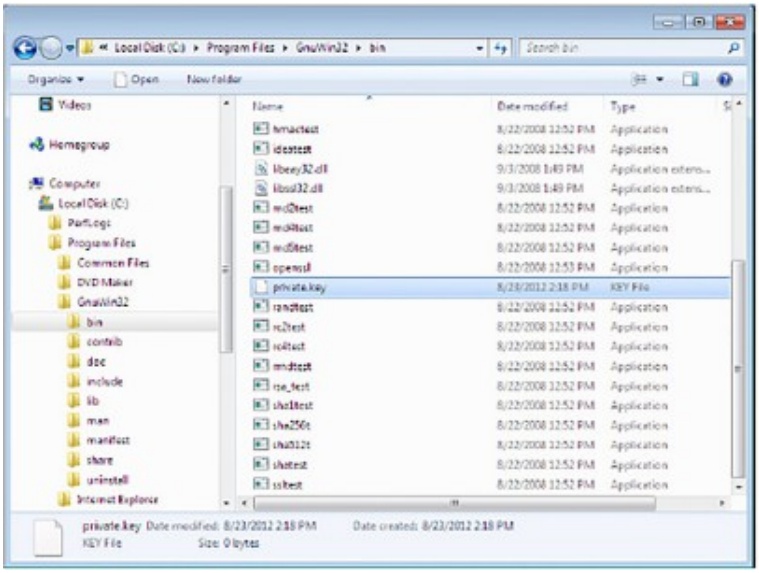
2.8) Type nu het commando: **notepad CSR.csr**
Het programma Kladblok/Notepad opent zich nu met uw CSR bestand. Kopieer het volledige blok (van ----BEGIN tot en met END REQUEST---) en plak dit vervolgens in het kader op de sslstore van Digidentity: http://sslstore.digidentity.eu/

2.9) U heeft hiermee uw certificaat aangevraagd. Het is belangrijk om te begrijpen dat u nu ook in het bezit bent van een zogenaamde " private key ". Dit bestand is de sleutel tot uw certificaten en uw identiteit.

- Deel daarom nooit uw private key met derden.

Wanneer u (na de levering van uw certificaten) helemaal klaar bent met het installeren van uw certificaten, en u heeft de werking van uw applicatie getest, raden wij u aan uw private key van de computer te verwijderen.

U kunt uw private key vinden in de map:
c:\program files\gnuwin32\bin of **c:\program files(86)\gnuwin32\bin**, het bestand heet "private.key"



Mocht u toch een backup van het bestand willen bewaren, dan adviseren wij u om middels het Open Source programma TrueCrypt uw private key op een versleuteld volume op een USB stick op te slaan. Deze stick kunt u vervolgens veilig opslaan in bijvoorbeeld een kluis. Kijk voor meer informatie op: http://www.truecrypt.org/

Overheids Identificatie Nummer (OIN):

Het OverheidsIdentificatieNummer (OIN) is het nummer dat aan uw organisatie is uitgegeven door de beheerorganisatie van Digikoppeling. Het basisformaat van het OIN is:

00000003 KVK Nummer 0000 (of uw vestigingsnummer)

00000003 12345678 0000
<prefix><nummer><suffix>

Heeft u geen FI nummer toegewezen gekregen dan is onderstaande tekst niet op u van toepassing.

Hierbij kunnen de volgende waardes voor deze drie velden gebruikt worden:

Prefix	Nummer	Suffix
00000001	Fi nummer van de Belastingdienst (9 Posities)	000
00000002	Fi nummer van de Belastingdienst (9 Posities)	Volgnummer (3 posities)
00000003	KvK nummer (8 positites)	Vestigingsnummer (4 posities) of 0000
00000004	Nummer van Digikoppeling beheerder (9 posities)	Volgnummer (3 posities) of 000
00000005 en volgende	Nog niet toegewezen	000