Aanmaken Certificate Sign Request (CSR) - 1 november 2025

Voor het aanmaken van een PKIoverheid Private Server Certificate, ondersteunt Digidentity de mogelijkheid om een eigen Certificate Sign Request (CSR) in te dienen. In dit geval kan de beheerder zelf een private key aanmaken en een CSR genereren.

De andere methode die Digidentity ondersteunt is het genereren van de CSR in de browser.

Eisen CSR

Een CSR voor PKIoverheid Private Server certificaten moet aan de volgende velden bevatten:

- commonName = [naam van de eerste server]
- organizationName = [naam van de organisatie zoals in Handelsregister]
- organizationIdentifier = [OIN (Organisatie Identificatie Nummer)]
- serialNumber = [OIN (Organisatie Identificatie Nummer)]
- country = [twee letterige landcode vb. NL]
- subjectAltName = [servernamen - maximaal tien]*

* Eerste servernaam in subjectAltName moet gelijk zijn aan servernaam in commonName.

Voor het genereren van een CSR is kennis van OpenSSL noodzakelijk. U dient met een aantal commando's de private key te genereren, een configuratiebestand aan te maken en een CSR te genereren.

Hieronder volgt een instructie op basis van een casus:

Instructie aanmaken CSR

Creëer een server certificaat voor organisatie Voorbeeld B.V. met registratienummer '12345679' in het Handelsregister (KvK) voor de servernaam 'server1.voorbeeld.nl'.

In een servercertificaat is een OIN (Organisatie Identificatie Nummer) verplicht. Heeft uw organisatie een OIN, vul dan dit OIN in. Heeft u geen OIN, dan kunt u het registratienummer in het KvK omzetten naar een OIN. Een OIN op basis van KvK start met 00000003 dan het registratienummer en afgesloten met 0000

00000003 12345678 0000 = OIN = 00000003123456780000

For Internal Use Only

[1] Maak een plat tekstbestand (notepad, textedit of Sublime Text) met de naam "voorbeeldbv.cnf". Neem de volgende inhoud op in het bestand:

```
oid_section = OIDs

[ req ]
default_bits            = 2048
encrypt_key             = no
default_md              = sha256
utf8                    = yes
string_mask             = utf8only
prompt                          = no
distinguished_name              = req_distinguished_name
req_extensions                  = req_ext
[ OIDs ]
organizationOID=2.5.4.97
[ req_distinguished_name ]
countryName             = NL
organizationName                = Voorbeeld B.V.
organizationOID                 = 00000003123456780000
serialNumber            = 00000003123456780000
commonName                      = server1.voorbeeld.nl
[ req_ext ]
subjectAltName                  = @alt_names
[alt_names]
DNS.1                           = server1.voorbeeld.nl
```

Bewaar het voorbeeldbv.cnf bestand.

LET OP: de gegevens in het bestand als organisatienaam, OIN, land en de domeinnaam van de servers moeten overeenkomen met de gegevens die Digidentity heeft geverifieerd. Als de gegevens niet overeenkomen, zullen wij de CSR afkeuren.

[2] Genereer een private key (sleutellengte 2.048) met het volgende commando:

```
openssl genrsa -out voorbeeldbv.key 2048
```

Dit commando zal een bestand genaamd "voorbeeldbv.key" aanmaken.

Om een CSR aan te maken moeten alle bestanden in dezelfde folder staan.

For In

[3] Maak vervolgens de CSR aan door het volgende commando uit te voeren:

```
openssl req -new -sha256 -out voorbeeldbv.csr -key voorbeeldbv.key -config voorbeeldbv.cnf
```

Dit commando maakt het bestand "voorbeeldbv.csr" aan op basis van het configuratiebestand "voorbeeldbv.cnf" en het sleutelbestand "voorbeeldbv.key".

Het bestand "voorbeeldbv.csr" kunt u uploaden naar Digidentity.

Extra servernamen in een certificaat

U kunt maximaal tien (10) servernamen opnemen voor het domein in het certificaat. De eerste servernaam staat zowel in de CommonName als DNS.1 veld. Voor iedere servernaam neemt u een DNS.# op in het bestand tot DNS.10.

[4] Wilt een CSR aanmaken met drie servernamen (server.voorbeeld.nl, applicatie.voorbeeld.nl en eherkenning.voorbeed.nl), neem de volgende inhoud op in de alt_names sectie van het bestand:

```
[alt_names]
DNS.1        = server.voorbeeld.nl
DNS.2        = applicatie.voorbeeld.nl
DNS.3        = eherkenning.voorbeeld.nl
```

Digidentity controleert de inhoud van de CSR. Komen de organisatienaam, land, OIN en domeinnaam overeen met de geverifieerde gegevens? Indien de CSR correct is, kunt u CSR laten tekenen en het certificaat (getekende CSR) downloaden als een .PEM bestand.

For Internal Use Only