Logius - Vastgestelde versie

Digikoppeling Gebruik en Achtergrond Certificaten 1.6.1

Logius Best Practice
Vastgestelde versie 20 september 2020

Deze versie:
https://publicatie.centrumvoorstandaarden.nl/dk/def-bp-gbachtcert-20200920/

Laatst gepubliceerde versie:
https://publicatie.centrumvoorstandaarden.nl/dk/gbachtcert/

Laatste werkversie:
https://logius-standaarden.github.io/Digikoppeling-Gebruik-en-achtergrond-certificaten/

Redacteurs:
Peter Haasnoot (Logius)
Pieter Hering (Logius)

Auteur:
Logius

Doe mee:
GitHub Logius-standaarden/Digikoppeling-Gebruik-en-achtergrond-certificaten
Dien een melding in:
Revisiehistorie:
Pull requests

Samenvatting

Dit document beschrijft de wijze waarop, binnen de context van Digikoppeling, met certificaten wordt omgegaan.

Status van dit document

Dit is de definitieve versie van de best practice. Wijzigingen naar aanleiding van consultaties zijn doorgevoerd.

Inhoudsopgave

Documentbeheer

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
04/04/2016	1.4	Logius	Referenties naar Beveiligingsvoorschriften aangepast naar nieuw document Digikoppeling beveiligingsstandaarden en voorschriften Nieuw hoofdstuk 2 over PKIoverheid toegevoegd TLS offloading toegevoegd Bijlage 4 OIN & HRN verplaatst naar Digikoppeling Identificatie en Authenticatie
12/10/2017	1.5	Logius	Tekstuele redactie, Figuur overzicht documentatie aangepast
01/09/2020	1.6	Logius	Informatie over Private Root CA en Pkioverheid generaties toegevoegd; CSP vervangen door TSP

Colofon

Logius Servicecentrum:	Postbus 96810 2509 JE Den Haag t. 0900 555 4555 (10 ct p/m) e.servicecentrum@logius.nl

1. Inleiding §

1.1 Doel en doelgroep §

Dit document beschrijft de wijze waarop, binnen de context van

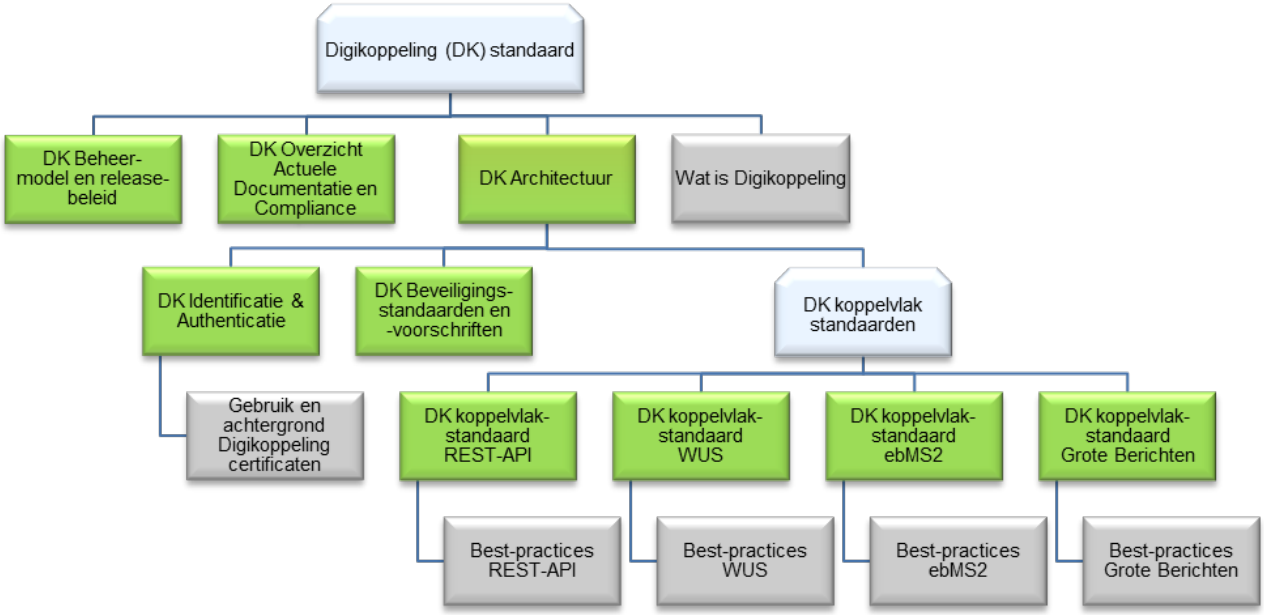
Digikoppeling, met certificaten wordt omgegaan. Inhoudelijk voorziet het in de detaillering van de architectuur voor identificatie, authenticatie en autorisatie. Bovendien geeft het uitleg over de gebruikelijke werkwijze bij het toepassen van certificaten. Meer informatie over certificaten is te vinden op de website: www.pkioverheid.nl en cert.pkioverheid.nl.

Onderstaande tabel geeft de doelgroep van dit document weer.

Afkorting	Rol	Taak	Doelgroep?
[MT]	Management	Bevoegdheid om namens organisatie (strategische) besluiten te nemen.	**Nee**
[PL]	Projectleiding	Verzorgen van de aansturing van projecten.	**Nee**
[A&D]	Analyseren & ontwerpen (design)	Analyseren en ontwerpen van oplossings-richtingen. Het verbinden van Business aan de IT.	**Ja**
[OT&B]	Ontwikkelen, testen en beheer	Ontwikkelt, bouwt en configureert de techniek conform specificaties. Zorgen voor beheer na ingebruikname.	**Ja**

1.2 Digikoppeling standaarden §

Dit document is een onderdeel van de Digikoppeling standaard.



Figuur 1 Opbouw documentatie Digikoppeling

1.3 Achtergrond §

Een belangrijk aspect voor beveiliging van Digikoppeling is de juiste identificatie, authenticatie en autorisatie van organisaties. Voor Digikoppeling is daarbij gekozen om certificaten toe te passen die voldoen aan de eisen van PKIoverheid[1]. Het juist toepassen van deze certificaten is essentieel voor een goede beveiliging. Helaas is dit toepassen ook complex. Digikoppeling heeft daarom aanvullend aan de door PKIoverheid gestelde eisen een aantal afspraken gemaakt die enerzijds de beveiliging conform PKIoverheid garanderen en anderzijds de complexiteit beheersbaar maken[2]. De praktische toepassing van deze afspraken is uitgewerkt in dit document. Het bevat daarvoor:

[1]: Zie http://www.logius.nl/pkioverheid

[2]: Zie het document “Digikoppeling Identificatie en Authenticatie”

- een uitwerking van de consequenties van deze authenticatie-afspraken;
- voorstellen / best practices voor het gebruik van certificaten.

In document wordt duidelijk aangegeven of het een uitwerking betreft (die verplicht is vanuit deze afspraken) of een voorstel (waar men van af kan wijken).

1.4 Omgang met certificaat §

Certificaten zijn gebaseerd op sleutelparen waarvan het publieke deel in het certificaat is opgenomen en het privédeel door de certificaateigenaar geheim wordt gehouden. Beide delen passen op elkaar in de zin dat:

- ondertekening met de privésleutel via de publieke sleutel gecontroleerd kan worden;
- encryptie met de publieke sleutel alleen met de privésleutel ontcijferd kan worden.

De privésleutel vertegenwoordigt in de elektronische communicatie de eigenaar. Binnen de huidige Digikoppeling afspraken is dit een overheidsorganisatie. Overheidsorganisaties hebben veelal toegang tot (meerdere) basisregistraties en hebben vergaande rechten binnen de e-overheid. Het is daarom van het grootste belang om

zeer vertrouwelijk om te gaan met een privésleutel behorend bij een certificaat en te voorkomen dat deze zoek raakt of in verkeerde handen belandt. Een dergelijke situatie leidt namelijk tot:

- toegang tot de e-overheidssystemen voor onbevoegden;
- het intrekken van een sleutel met het gevolg dat een organisatie niet kan deelnemen aan de e-overheid;
- de noodzaak tot het opnieuw genereren van het sleutelpaar en het aanvragen van een certificaat.

1.5 Leeswijzer §

Dit document is opgebouwd volgens een karakteristiek proces dat organisaties bij invoering van Digikoppeling doorlopen:

- Uitleg over PKIoverheid (hoofdstuk 2)
- Ontwerpen van de aansluiting op Digikoppeling met een Digikoppeling adapter (hoofdstuk 3).
- Bestellen van een certificaat (hoofdstuk 4).
- Ontvangst en installatie van het certificaat (hoofdstuk 5).
- Distributie van het certificaat (hoofdstuk 6).
- Gebruik van het certificaat (hoofdstuk 7).

De volgende hoofdstukken gaan hier per processtap op in. Elk hoofdstuk begint met de opsomming van een aantal vragen die duidelijk maken op welke informatiebehoefte het hoofdstuk antwoord geeft. Daarna volgt belangrijke achtergrondinformatie. Het hoofdstuk sluit af met een beschrijving van de benodigde activiteiten voor deze proces stap.

In bijlagen is de volgende aanvullende informatie opgenomen:

- Informatie over bestandsformaten waarin sleutels en/of certificaten uitgewisseld kunnen worden (Bijlage 1).
- Richtlijnen voor een veilig wachtwoord (Bijlage 2)
- Gegevens die in een certificaat opgenomen kunnen worden opgenomen (Bijlage 3)

1.6 Referenties §

Overige standaarden	Referentie
PKIoverheid “Programma van Eisen”	[PKI Policy], www.logius.nl/pkioverheid/

2. Achtergrond PKIoverheid certificaten §

2.1 PKIoverheid §

De Nederlandse overheid heeft een eigen Public Key Infrastructure ingericht waarmee de veiligheid van digitale diensten in Nederland kan worden geborgd door middel van het uitgeven (en intrekken) van digitale certificaten.

De certificaat autoriteit (CA) borgt de integriteit en authenticiteit van het certificaat en staat in voor de identiteit van de certificaateigenaar.

De certificatie dienstverleners (TSPs[3]) verstrekken PKIoverheid certificaten (onder de root of stamcertificaat van de Staat der Nederlanden) conform de eisen van PKIoverheid en vallen onder toezicht van Logius als Policy

Authority (PA). De PA beheert het Programma van Eisen (het normenkader) en Certification Practice Statements. De PA bepaalt de toetreding van TSPs tot het stelsel en houdt toezicht op de TSPs.[4]

[3]: Trust Service Providers (TSPs) is de engelse term voor certificatie dienstverleners. De afkorting TSPs wordt in dit document gebruikt voor beide begrippen. TSP's werden eerder CSP genoemd, Certificate Service Provider.

[4]: https://www.logius.nl/standaarden/pkioverheid/

Kenmerken PKIoverheid[5]:

[5]: www.PKIoverheid.nl

- Exclusief keurmerk van de Staat der Nederlanden.
- Gebaseerd op Nederlandse wet- en regelgeving en Europese standaarden.
- Beheer van de standaard door de Rijksoverheid.
- Regie van incidenten of calamiteiten door de Rijksoverheid.
- Actief toezicht op de certificatiedienstverleners door de Rijksoverheid.
- Mogelijkheid om een rechtsgeldige elektronische handtekening te zetten.
- Eén digitaal certificaat voor meerdere voorzieningen.

2.1.1 Stamcertificaat §

De Staat der Nederlanden heeft een eigen stamcertificaat die de basis vormt voor het vertrouwen van de onderliggende certificaten.

Binnen de PKI voor de overheid zijn op vier niveaus verschillende typen certificaten gedefinieerd, te weten:

- Stamcertificaat;
- Domeincertificaat;
- TSP certificaat;
- Eindgebruikercertificaat.

Het Staat der Nederlanden G3 stamcertificaat, wordt vanaf 1-1-2021 niet langer gebruikt, in plaats daarvan wordt voor machine to machine verkeer (en dus ook voor Digikoppeling) gebruik gemaakt van het Staat der Nederlanden Private Root CA G1 stamcertificaat. (Voor webauthenticatie wordt vanaf 1-1-2021 gebruik gemaakt van het stamcertificaat Staat der Nederlanden EV Root CA, Dit stamcertificaat wordt niet gebruikt voor Digikoppeling[6])

Het Public Root G3 en de Private Root G1 Stamcertificaten maken gebruik van SHA-256.

[6]:Zie de Digikoppeling Beveiligingsvoorschriften en richtlijnen voor de specifieke eisen en evt. uitzonderingen.

2.1.2 Certificaat hiërarchieën §

Op dit moment zijn er meerdere certificaathiërarchieën PKIoverheid. Na verloop van tijd zijn steeds sterkere algoritmes of andere functionaliteiten nodig om de betrouwbaarheid van certificaten te kunnen garanderen. Alle certificaten binnen eenzelfde hiërarchie zijn gebaseerd op hetzelfde algoritme. De oudste hiërarchie is gebaseerd op het SHA1-algoritme; de nieuwere hiërarchieën op SHA256. De EV-hiërarchie is speciaal ingericht om alleen certificaten voor Extended Validation uit te geven.[7]

Om foutmeldingen te voorkomen bij machine-to-machine communicatie, moet de gehele certificaatketen van

eindgebruikerscertificaat tot aan het stamcertificaat gevalideerd kunnen worden. Deze hiërarchieën zijn te raadplegen op de website van PKIoverheid[8].

[7]: https://www.logius.nl/standaarden/pkioverheid/certificaten/ [8]: Idem

2.1.3 TSPs §

Een Certificatie dienstverlener (Trust Service Provider oftewel TSP) verstrekt een PKIoverheid certificaat aan de aanvrager op basis van een aanvraag die voldoet aan de voorwaarden, een identiteitscontrole en controle van het Handelsregister.

2.1.4 Persoonsgebonden certificaten §

Een certificaat kan worden verstrekt ter identificatie en authenticatie van een persoon, een organisatie of een apparaat. Persoonsgebonden certificaten kunnen b.v. worden gebruikt om documenten te ondertekenen of om iemand te kunnen authenticeren.

2.1.5 Server (service) certificaten §

Digikoppeling vereist het gebruik van server (of service) certificaten voor de beveiliging van endpoints van webservices. Voor het signen en versleutelen van berichten wordt aanbevolen om een apart certificaat te gebruiken.

2.1.6 Public en Private services servercertificaten §

Een PKIoverheid services servercertificaat komt in twee soorten, een Public Root en een Private Root certificaat. Servercertificaten zijn geschikt voor de beveiliging van verkeer tussen systemen en verkeer naar/van websites.

Voor beide typen certificaten geldt dat ze aan de eisen van PKIoverheid voldoen, veilig beheerd worden en een audit ondergaan door een derde, onafhankelijke partij.

De certificaten verschillen echter op twee punten, de geldigheidsduur en de toepasbaarheid van het certificaat.

Een Public Root certificaat is ongeveer 1 jaar en 1 maand (397 dagen)[9] geldig. Dit geldt voor nieuw uit te geven certificaten. Reeds uitgegeven certificaten behouden hun geldigheidsduur. Dit type certificaat is aangemeld bij softwareleveranciers en wordt door webbrowsers automatisch vertrouwd.

[9]: Laatste raadpleging februari 2020

Een Private Root certificaat is 3 jaar geldig. Dit type certificaat is niet aangemeld bij softwareleveranciers en wordt door browsers niet automatisch vertrouwd. Dit is echter geen belemmering als het certificaat gebruikt wordt voor berichtenverkeer tussen systemen.

Raadpleeg [Digikoppeling Beveiligingsstandaarden en voorschriften] voor de eisen m.b.t certificaten.

2.1.7 Generaties en naamgeving §

Er zit een maximumlengte aan de geldigheidsduur van een Root CA-certificaat. In het geval van PKIoverheid is dat 12 à 15 jaar. De periode waarin een Root CA-certificaat geldig is wordt een generatie genoemd. De generaties worden opvolgend genummerd, vandaar dat we spreken over Public Root CA G1, Public Root CA G2 en Public Root CA G3. Aangezien het aanmeldingsproces bij de browsers enkele jaren kan duren is het zaak om tijdig een nieuwe generatie aan te maken. Zo'n nieuwe generatie is vaak ook een moment om de te gebruiken crypto-algoritmen nog eens kritisch te bekijken en –indien nodig- te vernieuwen. Bij de overgang van de Public

Root G1 naar Public Root G2 is bijvoorbeeld destijds overgeschakeld naar een langere sleutellengte en sterker hashing alghoritme. Voor de generatienaamgeving voor de Private Root CA wordt dezelfde nummersystematiek gebruikt. Bij de Private Root, die later is ingevoerd dan de Public Root, 'leven' we nog in de 1e generatie, vandaar de naam Private Root G1. Deze generatie loopt tot 14 november 2028.

2.2 Toepassingen §

Een PKIoverheid-certificaat wordt gebruikt bij:

- beveiliging van websites
- authenticatie (van servers en/of personen)
- rechtsgeldige elektronische handtekeningen
- versleuteling van elektronische berichten

Zie www.pkioverheid.nl voor meer informatie.

2.2.1 Hoe werkt PKI in Digikoppeling? §

PKI beveiliging werkt met PKI sleutelparen: elke partij beschikt altijd over een publieke sleutel en een private sleutel. De private sleutel is geheim en mag nooit worden gedeeld met een ander. De publieke sleutel wordt gedeeld met andere uitwisselingspartners. Zowel de verzender als de ontvanger beschikken over een eigen PKI sleutelpaar; zij wisselen hun publieke sleutels met elkaar uit.

Digikoppeling schrijft voor dat het transport kanaal (internet of diginetwerk) wordt beveiligd via tweezijdig TLS. Beide partijen wisselen hun publieke sleutels uit en zetten hiermee een tweezijdig versleutelde TLS verbinding op. Dit document geeft uitleg over hoe dit werkt en wat hiervoor nodig is.

Daarnaast geeft de Digikoppeling standaard de mogelijkheid de inhoud van het bericht te versleutelen of te ondertekenen (of allebei):

- De verzender gebruikt zijn private (of geheime) sleutel om een bericht of bericht inhoud te ondertekenen.
- De verzender gebruikt de publieke of openbare sleutel van de ontvanger om het bericht of bericht inhoud te versleutelen (encryptie). De ontvanger gebruikt zijn eigen private sleutel om het bericht te ontcijferen. Dit heet asymmetrische encryptie.

Digikoppeling onderkent de profielen *signed*, en *signed en encrypted* die zowel voor WUS als ebMS2 zijn uitgewerkt.

3. Ontwerp aspecten Digikoppeling adapter §

3.1 Vragen §

Dit hoofdstuk geeft antwoord op de volgende vragen met betrekking tot certificaten voor Digikoppeling:

1. Wat zijn de consequenties van het authenticeren en autoriseren met certificaten op organisatorisch niveau?
2. Welke organisaties kunnen een OIN krijgen?
3. Moet ik dezelfde of verschillende certificaten gebruiken voor servicerequester en serviceprovider?
4. Moet ik dezelfde of verschillende certificaten gebruiken voor WUS en ebMS2?
5. Wat moet ik doen als ik al een certificaat heb?

3.2 Achtergrond §

Het document “Digikoppeling Identificatie en Authenticatie” beschrijft de afspraken over gestandaardiseerde authenticatie volgens Digikoppeling standaarden. Een onderdeel van deze afspraken is dat authenticatie plaatsvindt op het niveau van organisaties. Dit heeft consequenties voor het certificaat dat organisaties gebruiken:

- Certificaten voor het gebruik van Digikoppeling worden beschikbaar gesteld aan organisaties en niet aan personen.
- Digikoppeling identificeert organisaties aan de hand van het OIN. Zie Digikoppeling Identificatie en Authenticatie.
- Voor de unieke identificatie en authenticatie van deze organisaties wordt het OIN opgenomen in een PKIoverheid certificaat in het zogenaamde Subject.serialNumber-veld door de TSP.[10]

[10]: Indien er sprake is van een twintig-cijferig nummer is dit altijd het OIN.

Een belangrijke overweging is of voor verschillende doelen ook verschillende certificaten gebruikt worden of dat deze doelen in hetzelfde certificaat worden gecombineerd. Keuzes hierbij zijn de combinatie van:

- Verschillende servicerequesters (dus clients in TLS-omgeving).
- Verschillende serviceproviders (dus servers in TLS-omgeving) zoals basisregistraties en andere gegevensbronnen.
- Servicerequesterrol en serviceproviderrol van een organisatie.
- Certificaten voor authenticatie, signing en/of encryptie.
- Gebruik voor WUS-omgeving en/of ebMS2-omgeving.

Combinatie van verschillende doelen in hetzelfde certificaat is efficiënt aangezien minder certificaten hoeven te worden aangeschaft en periodiek vernieuwd. Dat scheelt in kosten en inspanning. Combinatie van certificaten heeft ook een nadeel. Soms moeten hetzelfde certificaat en de bijbehorende privésleutel op meerdere servers (in zogenaamde keystores) opgeslagen worden. Het is dan lastiger om vast te stellen of er misbruik van een certificaat heeft plaatsgevonden. Daarom wordt sterk afgeraden om hetzelfde certificaat op verschillende servers toe te passen. Als deze servers een gemeenschappelijke keystore gebruiken geldt het bezwaar niet.

Voor gebruik van certificaten voor Digikoppeling is het toegestaan om certificaten te combineren voor alle genoemde doelen. Verder scheiden van certificaten per server wordt sterk aanbevolen, maar is niet vereist.

Vaak spelen ook technische inrichtingsaspecten een rol. Voor gebruik ten behoeve van server-authenticatie dient een Common Name (CN)[11] te zijn opgenomen in het certificaat. Combinatie is technisch daarom alleen mogelijk voor zover de TLS-afhandeling in dit verband plaatsvindt op dezelfde (proxy)server met dezelfde CN.

[11]: Hostname of Fully Qualified Name (FQN).

3.3 Stappen §

Allereerst dient een organisatie te kiezen voor welke doelen certificaten gecombineerd dan wel gescheiden worden (zie voorgaande paragraaf). Het advies hierbij is om elke server een eigen certificaat te geven zodat er normaliter geen hergebruik van het Digikoppeling certificaat plaatsvindt.

Het volgende hoofdstuk beschrijft stapsgewijs hoe men een OIN en een PKIoverheid certificaat kan verkrijgen.

4. Bestellen certificaat §

4.1 Vragen §

Dit hoofdstuk geeft antwoord op de volgende vragen met betrekking tot certificaten voor Digikoppeling:

1. Wat heb ik nodig voordat ik een certificaat kan bestellen?
2. Bij wie kan ik een certificaat bestellen?
3. Wie genereert het sleutelpaar en waarom geeft PKIoverheid de voorkeur aan generatie door de aanvrager?
4. Wat zijn de formaten voor het opslaan van certificaten?

4.2 Achtergrond §

Er zijn twee manieren om een sleutelpaar van een certificaat aan te maken: zelf genereren of dit door de Trust Service Provider (TSP) laten doen. Als het sleutelpaar zelf aangemaakt wordt, blijft de primaire sleutel achter op de server en zal alleen de publieke sleutel aan de TSP verzonden worden. De TSP stuurt dan een door hem ondertekend certificaat terug waarin de publieke sleutel is opgenomen. Dit is de meest veilige oplossing aangezien de vertrouwelijke privésleutel nooit de gebruikersorganisatie (of zelfs de server waarop deze gebruikt gaat worden) verlaat.

Als de TSP het sleutelpaar aanmaakt, zal de TSP samen met het certificaat (en de daarin opgenomen publieke sleutel) een vertrouwelijke privésleutel opsturen. Deze sleutel wordt via een wachtwoord beveiligd. Dit is een minder veilige oplossing aangezien de privésleutel uitgewisseld wordt. PKIoverheid adviseert daarom om zelf een sleutelpaar te genereren, wat in het kader van Digikoppeling met klem wordt benadrukt. In het verdere document gaan we ervan uit dat een organisatie zelf het sleutelpaar genereert.

4.3 Stappen §

De procesgang voor het aansluiten op Digikoppeling is beschreven in het document “Leeswijzer aansluitprocedure gebruik Digikoppeling”. Deze maakt onderdeel uit van de aanvraagprocedure Digikoppeling die u vindt https://www.logius.nl/diensten/digikoppeling/aanvragen. Het bestellen van certificaten vormt hiervan een onderdeel. Om certificaten te kunnen bestellen, moet de organisatie een identificerend nummer hebben: het OIN. Dit nummer wordt verkregen bij de beheerorganisatie van Digikoppeling volgens de procedure die is beschreven op de website van Logius.

Bestellen van een certificaat vindt plaats bij een door PKIoverheid aangewezen TSP die certificaten op commerciële basis verstrekt. Logius houdt op haar website een lijst met goedgekeurde TSP's bij die een PKIoverheid certificaat kunnen leveren[12]. Op deze website staat ook achtergrondinformatie over certificaten en hun werking. Belangrijk aandachtspunt hierbij is dat de eerste keer een aantal extra handelingen (bijvoorbeeld een bezoek aan de notaris of GWK) voorafgaat aan het daadwerkelijk bestellen van het certificaat. De website van Logius en het stelselhandboek bieden een heldere beschrijving van het bestellen en de daarbij betrokken TSP's.

[12]: https://www.logius.nl/pkioverheid/ bevat specifieke informatie over het aanschaffen van een certificaat.

De websites van de TSP's bevatten formulieren voor de aanvraag van certificaten. In het bestelproces en leveringsproces voor certificaten is het nodig om informatie zoals sleutels en certificaten uit te wisselen. Hiervoor bestaan verschillende bestandsformaten. Deze zijn beschreven in “Bestandsformaten voor certificaten“ in bijlage 1.

Om op deze wijze een certificaat te bestellen moet u eerst een Certificate Signing Request (CSR) maken op de server waarop u het certificaat wilt installeren. Dit CSR bevat naast de door u gegenereerde publieke sleutel ook gegevens die u in het certificaat wilt opnemen (zie hieronder). Vervolgens stuurt u dit CSR in p10 formaat op (afhankelijk van de TSP-procedure) per mail of op een fysieke drager per aangetekende post. Het aanmaken van een CSR verschilt per type server, maar er zijn veel leveranciers die hier handleidingen voor publiceren[13]. De privésleutel kunt u uit de keystore van uw server exporteren voor veilige back-up in een kluis; het p12 formaat is

hiervoor geschikt (zie ook “Bestandsformaten voor certificaten“ in bijlage 1. Het volgende hoofdstuk beschrijft hoe u deze privésleutel zou moeten beveiligen.

[13]: Zie bijvoorbeeld https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR235

Bij bestelling van het certificaat dient u de volgende onderdelen te specificeren:

- Country Name (C): twee letterige landcode C=NL.
- State or Province (S): PKIoverheid raadt het gebruik van dit veld af.
- Locality or City (L): PKIoverheid raadt het gebruik van dit veld af; indien gebruikt hier de vestigingsplaats van de organisatie opnemen. Bijvoorbeeld: L=Den Haag.
- Organisation (O): Volledige naam van de organisatie overeenkomstig gegevens in basisregistratie of formeel document. Bijvoorbeeld: O=Stichting ICTU.
- Organisational Unit (OU): Optionele naam van een organisatieonderdeel. Bijvoorbeeld: OU=Digikoppeling
- Common Name (CN): Dit is de FQN van de server (Host + Domain Name). Bijvoorbeeld: www.logius.nl/digikoppeling/
- OrganisatieIdentificatieNummer (OIN): Nummer dat is uitgegeven door de beheerorganisatie van Digikoppeling. Hoewel PKIoverheid in haar Programma van Eisen dit nummer als optioneel vermeldt is het verplicht in de context van Digikoppeling. Bijvoorbeeld: OIN=00000001123456789000. Dit nummer wordt vermeld op het aanvraagformulier.
- Key usage: In certificaten voor Digikoppeling moeten het digital Signature en keyEncipherment bit uit de key usage zijn opgenomen en zijn aangemerkt als essentieel. Geen ander key usage mag hiermee worden gecombineerd. Deze gegevens zijn standaard voor een Digikoppeling certificaat en kan men niet opnemen in het CSR of de aanvraag.
- Extended key usage: In certificaten voor Digikoppeling wordt afgeraden om dit veld toe te passen[14]. Deze gegevens zijn daarom standaard voor een Digikoppeling certificaat en kan men niet opnemen in het CSR of de aanvraag.

[14]: Interoperabiliteit met sterk verouderde Java-tooling kan vereisen dat de “extended key usage”-bits TLSwwwServerAuthentication en/of TLSwwwClientAuthentication opgenomen worden.

Het programma van Eisen deel 3b van PKIoverheid bevat een uitgebreider overzicht van velden die (deels optioneel) in een certificaat voor kunnen komen. Zie www.logius.nl/pkioverheid, zoekterm “deel 3b”.

Het door de TSP ondertekende certificaat ontvangt u meestal in een .p7b formaat of een .cer formaat (zie ook “Bestandsformaten voor certificaten“). Veranderen van informatie in het certificaat is niet mogelijk behalve door een nieuw certificaat aan te vragen. Het volgende hoofdstuk beschrijft hoe u dit certificaat kunt installeren.

5. Installatie certificaat §

5.1 Vragen §

Dit hoofdstuk geeft antwoord op de volgende vragen met betrekking tot certificaten voor Digikoppeling:

1. Waarom is het belangrijk om de privésleutel van mijn certificaat te beveiligen?
2. Hoe moet ik de privésleutel van een certificaat opslaan?
3. Hoe beveilig ik de toegang tot deze sleutel?

5.2 Achtergrond §

Het programma van eisen[15] dat PKIoverheid aan TSP's oplegt bevat de verplichting aan TSP's om over de juiste beveiliging van sleutels door gebruikers te waken inclusief de mogelijkheid tot audit (zie kader).

[15]: Zie [PKI Policy], zoekterm “deel 3b”.

5.3 Stappen §

Zodra u een door de TSP ondertekend certificaat ontvangt kunt u dit installeren bij de privésleutel op uw server. Dit certificaat (met de daarin opgenomen publieke sleutel) is niet vertrouwelijk. De bijbehorende privésleutel daarentegen des te meer. Het is belangrijk om deze privésleutel goed te beveiligen. Immers: de privésleutel vertegenwoordigt in de elektronische communicatie de eigenaar en kan toegang tot (meerdere) basisregistraties en andere services geven (zie verder “Omgang met certificaat“).

Om de privésleutel behorend bij certificaten veilig op te slaan in een keystore is het noodzakelijk om veilige wachtwoorden te kiezen. Gebruik daarom een wachtwoord dat moeilijk te herleiden is (zie “Bijlage 2: Richtlijnen voor een veilig password“ voor een voorbeeld). Basisregistraties en andere gegevenshouders kunnen aanvullende maatregelen eisen vanuit de vertrouwelijkheid van de door hen beheerde gegevens en het gebruik van daarbij behorende certificaten[16].

[16]: Een voorbeeld hiervoor vormt de zorg, waar men eisen stelt aan opslag van servercertificaten.

Het opslaan van een privésleutel van een certificaat in een keystore verschilt per systeem. Raadpleeg de documentatie van uw systeem voor de manier waarop dit moet plaatsvinden. Er zijn ook veel leveranciers die hier handleidingen voor publiceren. Probeer te allen tijde het kopiëren van privé-sleutels zo veel mogelijk tegen te gaan met fysieke, technische en procedurele maatregelen.

6. Distributie en CPA-creatie §

6.1 Vragen §

Dit hoofdstuk geeft antwoord op de volgende vragen met betrekking tot certificaten voor Digikoppeling:

1. Op welke wijze kan ik anderen mijn certificaat ter beschikking stellen t.b.v. authenticatie en hoe verkrijg ik certificaten van anderen?
2. Wat is de rol van het serviceregister bij distributie van certificaten?
3. Wat is de rol van een CPA bij distributie van certificaten?

6.2 Achtergrond §

Identificatie van organisaties vindt voor Digikoppeling plaats aan de hand van het OIN dat is opgenomen in het certificaat. Het certificaat zelf (dat ook een uniek identificatienummer heeft) wordt niet rechtstreeks voor identificatie gebruikt; dit verloopt altijd via het OIN uit het certificaat. Nieuwe (of extra) certificaten voor dezelfde organisatie hebben altijd hetzelfde OIN nummer (maar een ander certificaatnummer). Zolang het certificaat geldig is (ondertekend door de TSP, geldigheidsdatum nog niet verstreken en niet ingetrokken) kunnen organisaties ervan uitgaan dat dit OIN correct is.

Basisregistraties en gegevensbronnen met vertrouwelijke gegevens autoriseren toegang tot hun gegevens aan de hand van het OIN in het certificaat.

Het is daarom nodig om uw OIN vooraf aan organisaties ter beschikking te stellen. Distributie van certificaten is afhankelijk van het profiel vaak niet nodig voor Digikoppeling op basis van WUS. Bij Digikoppeling op basis van ebMS2 worden certificaten echter ook opgenomen in de CPA's die organisaties uitwisselen.

6.3 Stappen §

Uitwisseling van certificaten is vaak nodig voor gebruik binnen Digikoppeling verband.

Voor het maken van CPA's kunnen organisaties gebruikmaken van het Digikoppeling CPA register.

7. Gebruiksaspecten §

7.1 Vragen §

Dit hoofdstuk geeft antwoord op de volgende vragen met betrekking tot certificaten voor Digikoppeling:

1. Hoe worden organisaties geautoriseerd?
2. Welke alternatieven heb ik om autorisatie in mijn applicatie te regelen?
3. Hoe vaak moet een certificaat vernieuwd worden?
4. Hoe controleer ik of een certificaat nog geldig is?
5. Hoe zorg ik dat ik met mijn certificaat kan testen?

7.2 Achtergrond §

Identificatie van organisaties vindt plaats aan de hand van het OIN. Authenticatie van dit OIN vindt plaats door te controleren of het certificaat waarin dit OIN is opgenomen ook geldig is. Autorisatie beperkt zich in beginsel tot organisatorisch niveau en maakt daarom gebruik van dit OIN[17].

[17]: Een leidend principe van Digikoppeling is dat de overheidsorganisatie waar een persoon werkzaam is, verantwoordelijk is om deze persoon (medewerker) te authenticeren en juist te autoriseren voor deeltaken binnen de organisatie. Overheidsorganisaties onderling autoriseren (en authenticeren) elkaar vervolgens voor toegang tot bepaalde services op basis van de aan een organisatie toegewezen taak.

In specifieke gevallen kan autorisatie op een gedetailleerder niveau noodzakelijk zijn. Voor overheidsorganisaties is het bijvoorbeeld mogelijk om een subOIN aan te vragen.

Organisaties hebben daarom in hoofdlijnen de keuze uit de volgende opties voor autorisatie:

- *Iedereen autoriseren (na succesvolle authenticatie)*: Een dergelijke autorisatie kan in bijzondere situaties soms zinvol zijn. Het gaat hierbij om situaties waarbij elke overheidsorganisatie[18] dezelfde handelingen mag verrichten op een gegevensbron (of basisregistratie) of wanneer onjuiste handelingen beperkte consequenties hebben.
- *Autoriseren op OIN (na succesvolle autorisatie)*: Een dergelijke situatie is zinvol als organisaties niet dezelfde handelingen mogen verrichten omdat dit vergaande consequenties heeft voor de integriteit en vertrouwelijkheid. In deze situatie is het noodzakelijk dat de basisregistratie (of een andere service) een autorisatietabel met daarin OIN-nummers bijhoudt[19] [20].
- Autoriseren op organisatieonderdeel:
  Een dergelijke situatie kan nodig zijn vanuit een wettelijke verplichting aan de gegevenshouder om dit te doen. De gegevenshouder zal in dit geval van de communicatiepartners kunnen eisen dat zij een subOIN aanvragen om het specifieke organisatieonderdeel te onderscheiden.

[18]: Deze autorisatie is vaak te ruim. Het is namelijk mogelijk dat hackers een certificaat bedoeld voor medewerkers misbruiken om zich als Digikoppeling applicaties voor te doen. Dit komt doordat (afhankelijk van de TSP) ook persoonsgebonden PKIoverheid certificaten worden uitgegeven (zoals smartcards) die lijken op Digikoppeling certificaten. De technische achtergrond hiervan is dat een persoonsgebonden certificaat namelijk ook de key usage 'digitalSignature' heeft. Dit volstaat voor een TLS-client in Digikoppeling omgevingen.

Sommige TSP's gebruiken bovendien dezelfde TSP-key voor signing van persoonsgebonden certificaten en server-certificaten zodat het verschil tussen de beide type certificaten nog moeilijker is vast te stellen.

[19]: Digikoppeling communicatiepartners wisselen het OIN uit ten behoeve van deze autorisatietabel.

[20]: zie het document : Digikoppeling Identificatie en Authenticatie.

In sommige gevallen kan het audit-proces vereenvoudigd worden met aanvullende identificatiegegevens. Bij dergelijke behoeften kunnen bijvoorbeeld afdelings- of persoonsgegevens als inhoud in een bericht opgenomen worden. Ook gegevens over authenticatie van afdelingen en personen kunnen, bijvoorbeeld in de vorm van certificaten, toegevoegd worden, maar spelen geen rol bij het Digikoppeling autorisatieproces.

Een geldig certificaat vormt binnen de overheid de basis voor vertrouwen op elektronisch gebied. Om risico van het gebruik van privésleutels door onbevoegden te beperken hebben certificaten een beperkte geldigheid (enkele jaren). Als dit vertrouwen tussentijds verloren gaat wordt het certificaat ingetrokken. Het is van groot belang dat de eigenaar van het certificaat een dergelijke situatie zo snel mogelijk meldt aan zijn TSP. Via een zogenaamde Certificate Revocation List (CRL) maken TSP's publiek kenbaar welke certificaten niet meer vertrouwd mogen worden. Het intrekken van een certificaat kan om verschillende redenen plaatsvinden:

- De privésleutel van het certificaat is niet meer beschikbaar:
  - Er is geen pending request aanwezig in de server bij installatie van het certificaat.
  - Er is sprake van een 'private key mismatch' bij installatie van het certificaat op de server.
  - De privésleutel is corrupt.
  - De privésleutel is verloren geraakt (bijvoorbeeld bij een server crash of upgrade).
  - Het wachtwoord van de privésleutel is vergeten.
- De privésleutel is gecompromitteerd.
- Bij installatie van het certificaat blijkt dat er een certificaat voor een onjuiste common name is aangevraagd.
- Informatie in het certificaat is niet meer juist (bijvoorbeeld wijziging van organisatienaam).

Ingetrokken certificaten waarvan de geldigheidsduur is verlopen worden niet meer in de CRL gepubliceerd.

TSP's kunnen informatie over ingetrokken certificaten in plaats van via een CRL ook via een onlinevoorziening opvraagbaar maken. Deze ondersteuning via het Online Certificate Status Protocol (OCSP) is voor TSP's niet verplicht (behalve voor EV certificaten)[21]. Indien beschikbaar biedt dit wel de mogelijkheid om elk certificaat direct online te verifiëren.

[21]: Zie voor detaileisen de Pkioverheid PVE deel 3: aanvullende eisen

7.3 Stappen §

Om de betrouwbaarheid van het certificaat te waarborgen is het nodig om dit regelmatig te vernieuwen. PKIoverheid eist van TSP's dat een certificaat maximaal vijf jaar geldig is maar in de praktijk geven TSP's certificaten uit die niet langer dan drie jaar geldig zijn. Vernieuwen van het certificaat zal moeten plaatsvinden ruim voordat dit verlopen is. Dit is vooral van belang als met meerdere organisaties samengewerkt wordt en met deze organisaties certificaten en CPA's (ebMS2) uitgewisseld worden.

PKIoverheid eist dat bij vernieuwing van het certificaat ook een nieuw sleutelpaar gegenereerd wordt.

Een certificaat is geldig als het aan de volgende drie eisen voldoet:

- De ondertekening van het certificaat berust op een geldige hiërarchie van certificaten afgeleid van het overheid stamcertificaat[22].
- De geldigheidsduur van het certificaat is niet verstreken.
- Het certificaat is niet ingetrokken door de TSP.

[22]: Het stamcertificaat Staat der Nederlanden Root CA vindt u ophttps://www.pkioverheid.nl/ onder “Stamcertificaat installeren”. Hier vindt u ook per TSP een link naar de CRL met ingetrokken certificaten.

Om na te gaan of het certificaat is ingetrokken (Engels: revoked) publiceren de TSP's een Certificate Revocation List (CRL). In deze lijst worden de serienummers van ingetrokken certificaten opgenomen. Het is daarom nodig dat de CRL op regelmatige basis geraadpleegd wordt (of indien beschikbaar het OCSP-alternatief). Aangezien er meerdere TSP's zijn aangewezen binnen het overheidsdomein zullen deze allemaal moeten worden geraadpleegd. PKIoverheid certificaten zijn onderdeel van een hiërarchie. Daarom moeten ook 'bovengelegen' CRL's worden geraadpleegd[23].

[23]: Servers bieden standaard configuratieparameters voor een CRL. Niet altijd kan er naar meerdere CRL's verwezen worden. In dat geval kunnen automatische scripts helpen om meerdere CRL's samen te voegen.

Bij het gebruik van een CRL dient men erop te letten dat ook een CRL een bepaalde geldigheidsduur heeft. Voor het verlopen van de CRL dient er een nieuwe opgehaald te zijn. Bij het verzuim hiervan en het laten verlopen van de geldigheidsduur van de CRL worden alle certificaten van de betreffende TSP als ongeldig beschouwd[24]. Hoewel een CRL bruikbaar blijft tot de next update, is het verstandig om deze minimaal elke vier uur te verversen[25]. Basisregistraties (en andere gegevenshouders) kunnen voor hun domein specifieke eisen stellen.

[24]: Tevens kan het zijn dat de tooling die de CRL uitleest niet dynamisch de update van het CRLbestand registreert. Zo kan het zijn dat een webserver herstart moet worden voordat deze het nieuwe bestand inleest. Dit gedrag is afhankelijk van het gebruikte product. Het is daarom belangrijk dat dat goed getest wordt.

[25]: TSP's zijn verplicht om het intrekken van een certificaat uiterlijk vier uur na melding via de CRL te publiceren.

Bij het testen van applicaties is het van belang om certificaten te gebruiken waarvan de structuur overeenkomt met die van een PKIoverheid certificaat[26]. Pkioverheid kent een TEST hiërarchie voor dit doeleinde. Logius biedt daarnaast self signed testcertificaten om haar voorzieningen te kunnen testen.

[26]: Een belangrijk kenmerk van PKIoverheid certificaten is behalve het OIN voor Digikoppeling dat deze een vierlaagsstructuur hebben (stamcertificaat, domein, TSP en certificaathouder). Niet alle software kan standaard goed omgaan met een vierlaagsstructuur. Het is daarom belangrijk dat dit goed getest wordt.

Het is niet toegestaan om (keten)testsystemen uit te rusten met certificaten die zijn gegenereerd op basis van het overheid stamcertificaat; voor testen moet een testcertificaat gebruikt worden.

7.3.1 TLS Offloading - CPA §

Door het gebruik van TLS Offloading zijn er minder afhankelijkheden van certificaten in CPA’s. Daardoor kan de geldigheid van een CPA langer zijn dan de geldigheid van het certificaat.

7.3.2 TLS offloading - WUS §

Bij het gebruik van TLS Offloading, specifiek voor WUS (bevragingen), zijn er mogelijkheden om het OIN of andere kenmerken van het certificaat door te geven aan achterliggende applicaties. Dit kan nodig zijn voor het controleren van autorisaties.

Bij TLS-offloading is het mogelijk om het OIN (en andere certificaatgegevens) door te geven aan de achterliggende message-handler en de daarop aangesloten applicaties voor autorisatiedoeleinden.

Voorbeeld voor Apache

Er zijn voor een http-proxy o.b.v. Apache speciale mods om certificaat-gegevens door te geven aan de achterliggende messagehandler. Tussen Apache en Tomcat kun je werken met modSSL. Men krijgt dan overigens niet alleen het OIN maar alle certificaatgegevens. Met een kleine Java-app is het mogelijk de

gegevens eruit te filteren en bijvoorbeeld toe te voegen aan het bericht dat de messagehandler via JMS doorgeeft aan de achterliggende applicatie.

8. Bijlage 1: Bestandsformaten voor certificaten §

De volgende bestandsformaten worden gebruikt voor uitwisseling van sleutels en/of certificaten:

p7b	De Cryptographic Message Syntax standaard (PKCS #7) wordt gebruikt voor uitwisseling van certificaten en hogere orde certificaten uit de hiërarchie waarmee dit certificaat is ondertekend (en op hun beurt de bovengelegen certificaten zijn ondertekend). Bestanden in dit formaat hebben vaak de extensie .p7b en soms .p7c. Hetzelfde formaat wordt gebruikt voor CRL's.
p10	De Certification Request Standard (PKCS #10) wordt gebruikt voor aanvraag van een door een TSP ondertekend certificaat en aangeduid als Certificate Signing Request (CSR). Het CSR bevat daartoe informatie die in het certificaat opgenomen moet worden waaronder de publieke sleutel. Bestanden in dit formaat hebben vaak de extensie .p10.
p12	Het Personal Information Exchange formaat (PKCS #12) wordt gebruikt voor uitwisseling van certificaten en de bijbehorende privésleutel. Als de privésleutel ook in het bestand is opgenomen, is het gebruikelijk (en hoogstnoodzakelijk) om dit bestand met een wachtwoord te beveiligen. Bestanden in dit formaat hebben vaak de extentie .p12 of .pfx.
cer (BER of DER)	De Basic Encoding Rules (BER) en de Distinguished Encoding Rules (DER) zijn beide een platform-onafhankelijke manier om certificaten weer te geven (encoding) ten behoeve van uitwisseling. DER-encoding heeft de voorkeur. Bestanden in dit formaat hebben vaak de extensie .cer. .der-encoded bestanden hebben soms ook de extensie .der. Bestanden bevatten soms meer dan één certificaat.
cer (base64)	Base64 is een een platform-onafhankelijke manier om certificaten weer te geven (encoding); base64 is ontwikkeld ten behoeve van uitwisseling over internet middels Secure/Multipurpose Internet Mail Extensions (S/MIME). Bestanden in dit formaat hebben vaak de extentie .cer of .pem. Een .pem bestand kan soms ook een privésleutel bevatten (dit wordt afgeraden).

Bij gebruik in het kader van Digikoppeling zullen deze formaten vaak (maar niet uitsluitend) als volgt toegepast worden:

- aanvraag van een certificaat: .p10;
- ontvangst van het ondertekende certificaat: .p7b of .cer of .ber;
- export van de privésleutel en certificaat voor backup; .p12.

9. Bijlage 2: Richtlijnen voor een veilig password §

Overgenomen uit “LRD-beleid ten aanzien van wachtwoorden”

Instelling en wijziging van het wachtwoord

1. Het wachtwoord bestaat uit minimaal zes tekens en maximaal acht tekens;
2. Indien het wachtwoord bestaan uit zes tekens dan worden de resterende posities automatisch aangevuld met twee spaties, bij een wachtwoord met zeven tekens wordt de laatste positie automatisch aangevuld met één spatie;
3. Een teken mag maximaal twee keer in het wachtwoord voorkomen;
4. Het wachtwoord mag niet gelijk zijn aan een van de tien voorafgaande wachtwoorden;
5. Er kan worden gebruik gemaakt van alle tekens (NB: alle tekens in een computer hebben een waarde tussen 000 en de 255);
6. Er worden vier soorten tekens onderscheiden:
    - letters A... Z (de tekens met de waarden 065 t/m 090) en a..z (de tekens met de waarden 097 t/m 122)
    - cijfers 0... 9 (de tekens met de waarden 048 t/m 057)

- de spatie (het teken met waarde 032)
- overige tekens

7. Indien in het wachtwoord letters worden gebruikt dan geldt dat deze of losstaand (dus in de vorm van één enkele letter) of in een reeks van drie letters mogen voorkomen. Reeksen van twee, vier of meer letters mogen dus niet worden gebruikt;
8. Indien in het wachtwoord cijfers worden gebruikt dan geldt dat deze of losstaand (dus in de vorm van één enkel cijfer) of in een reeks van drie cijfers mogen voorkomen. Reeksen van twee, vier of meer cijfers mogen dus niet worden gebruikt;
9. Indien in het wachtwoord reeksen van drie tekens voorkomen dan geldt dat de waarden van deze tekens niet met één mogen oplopen, bv. de waarden 065,066,067 (=ABC) of met 1 mogen aflopen, bv. de nummers 057,056,055 (=987);
10. Spaties mogen alleen voorkomen in de 7e of 8e positie; De volgende wachtwoorden zijn dus niet goed:
    - 2ABC154Z (oplopende reeks van drie letters)
    - AD1BOB33 (reeks van twee letters en reeks van tweecijfers)
    - A A571A2 (spatie op de tweede positie en driemaal dezelfde letter)
    - Rien127 (reeks van vier letters)
11. Indien u in uw wachtwoord gebruik maakt van drie of meer overige tekens, dan komen de regels onder punt 7, 8 en 10 te vervallen. U kunt dan uw wachtwoord samenstellen uit elke combinatie van waarden die u wenst (zolang de tekens maar niet vaker dan twee keer in het wachtwoord voorkomen).
12. Een wachtwoord heeft slechts een beperkte geldigheidsduur van negentig dagen. U dient dus voor het verstrijken van deze termijn uw wachtwoord te wijzigen. Indien u deze termijn overschrijdt, dan kunt u na de fatale datum geen contact meer leggen met het netwerk. Er volgt dan een foutmelding.

10. Bijlage 3: Basisattributen in certificaat §

Voor de meest actuele versie zie het Programma van Eisen van PKIoverheid deel 3b[27]

[27]: http:// https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen/

Veld / attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Version	V	*MOET* ingesteld worden op 2 [rfc6187], [rfc7633].	[rfc5280]	Integer	Beschrijft de versie van het certificaat, de waarde 2 staat voor X.509 versie 3.
SerialNumber	V	Een serienummer dat op unieke wijze het certificaat binnen het uitgevende CA domein *MOET* identificeren.	[rfc5280]	Integer	Alle eindgebruiker certificaten moeten tenminste 8 bytes aan niet te voorspellen willekeurige data bevatten in het serienummer (SerialNumber) van het certificaat.

Veld / attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Signature	V	*MOET* worden ingesteld op het algoritme, zoals deze door de PA is bepaald.	[rfc5280], [etsi-ts-102-176-1] [etsi-ts-102-176-2]	OID	*MOET* gelijk zijn aan het veld signatureAlgorithm. Voor certificaten onder het G2 en G3 stamcertificaat wordt alleen sha-256WithRSAEncryption toegestaan.
Issuer	V	*MOET* een Distinguished Name (DN) bevatten. Veld heeft de onderstaande attributen:	[PKI Policy], [rfc3739], [etsi-ts-102-280]		Andere attributen dan hieronder genoemd *MOGEN* NIET worden gebruikt.
Issuer.countryName	V	zie eis 7.1-pkio174 [PKI Policy]	[etsi-ts-101-862], [X520], [ISO3166]	Printable String	
Issuer.OrganizationName	V	zie [PKI Policy] eis 7.1-pkio174	[etsi-ts-102-280]	UTF8String	
Issuer. organizationalUnitName	O	zie [PKI Policy] eis 7.1-pkio174	[etsi-ts-102-280]	UTF8String	
Issuer.serialNumber	O	zie [PKI Policy] eis7.1-pkio174	[rfc3739]	Printable String	
Issuer.commonName	V	zie [PKI Policy] eis 7.1-pkio174	[PKI Policy], [rfc3739]	UTF8String	Het commonName attribuut *MAG* NIET nodig zijn om de uitgevende instantie te identificeren (geen onderdeel van de Distinguished Name, eis uit [rfc3739]).
Issuer.organizationIdentifier	V/N	In het organizationIdentifier veld wordt een identificatie van de uitgevende CA opgenomen. Dit veld *MOET* worden opgenomen wanneer het veld subject.organizationIdentifier voorkomt in het TSP certificaat en *MAG* NIET worden opgenomen wanneer dit veld in het betreffende TSP certificaat niet voorkomt.	[etsi-en-319-412-1]	String	De opmaak van de identificatiestring wordt gespecificeerd in paragraaf 5.1.4 van ETSI [etsi-en-319-412-1] en bevat: 3 character legal person identity type reference; 2 character [ISO3166] [2] country code; hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and identifier (according to country and identity type reference).
Validity	V	*MOET* de geldigheidsperiode (validity) van het certificaat definiëren volgens [rfc5280].	[rfc5280]	UTCTime	*MOET* begin- en einddatum bevatten voor geldigheid van het certificaat conform het van toepassing zijnde beleid vastgelegd in het CPS.

Veld / attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Subject	V	De attributen die worden gebruikt om het subject (service) te beschrijven *MOETEN* het subject op unieke wijze benoemen en gegevens bevatten over de abonneeorganisatie. Dit veld heeft de volgende attributen:	[PKI Policy], [rfc3739], [etsi-ts-102-280]		*MOET* een Distinguished Name (DN) bevatten. Andere attributen dan hieronder genoemd *MOGEN* NIET worden gebruikt.
Subject.countryName	V	C vullen met tweeletterige landcode conform [ISO3166-1]. Indien een officiële alpha-2 code ontbreekt, *MAG* de TSP de user-assigned code XX gebruiken.	[rfc3739], [X520], [ISO3166], [PKI Policy]	PrintableString	De landcode die wordt gehanteerd in Subject.countryName *MOET* in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.commonName	V	Naam die de service identificeert. Bij services certificaten is dit veld verplicht	[rfc3739], [etsi-ts-102-280], [PKI Policy]	UTF8String	In de subject.commonname wordt de functie van een organisatorische entiteit of de naam waarmee het apparaat of systeem wordt aangeduid opgenomen.
Subject.organizationName	V	Volledige naam van de organisatie van de abonnee conform geaccepteerd document of Basisregistratie.	[PKI Policy]	UTF8String	De abonnee-organisatie is de organisatie waarmee de TSP een overeenkomst heeft gesloten en namens welke de certificaathouder (service) communiceert of handelt.
Subject.organizationIdentifier	V	In het organizationIdentifier veld wordt een identificatie van het subject.	[etsi-en-319-412-1]	String	De opmaak van de identificatiestring wordt gespecificeerd in paragraaf 5.1.4 van ETSI [etsi-en-319-412-1] en bevat: 3 character legal person identity type reference; 2 character [ISO3166] [2] country code; hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and identifier (according to country and identity type reference).

Veld / attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Subject.stateOrProvinceName	A	Het gebruik wordt afgeraden. Indien aanwezig *MOET* dit veld de provincie van vestiging van de abonnee conform geaccepteerd document of Basisregistratie bevatten.	[PKI Policy], [rfc3739]	UTF8String	Naam van de provincie *MOET* in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.localityName	A	Het gebruik wordt afgeraden. Indien aanwezig *MOET* dit veld de vestigingsplaats van de abonnee conform geaccepteerd document of Basisregistratie bevatten.	[PKI Policy], [rfc3739]	UTF8String	Naam van de vestigingsplaats *MOET* in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.postalAddress	A	Het gebruik wordt afgeraden. Indien aanwezig *MOET* dit veld het postadres van de abonnee conform geaccepteerd document of Basisregistratie te bevatten.	[PKI Policy], [rfc3739]	UTF8String	Adres *MOET* in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.serialNumber	O	Het is de verantwoordelijkheid van een TSP om de uniciteit van het subject (service) te waarborgen. Het Subject.serialNumber *MOET* gebruikt worden om het subject uniek te identificeren. Het gebruik van 20 posities is uitsluitend toegestaan voor OIN en HRN na aanvullende afspraken met Logius.	[rfc3739], [X520], [PKI Policy]	Printable String	Het nummer wordt door de TSP en/of de overheid bepaald. Het nummer kan per domein verschillen en voor meerdere toepassingen gebruikt worden.

11. Conformiteit §

Naast onderdelen die als niet normatief gemarkeerd zijn, zijn ook alle diagrammen, voorbeelden, en noten in dit document niet normatief. Verder is alles in dit document normatief.

12. Lijst met figuren §

A. Referenties §

A.1 Normatieve referenties §

[etsi-en-319-412-1]
ETSI EN 319 412-1 V1.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. ETSI. February 2016. Published. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf

[etsi-ts-101-862]
ETSI TS 101 862 V1.3.3 (2006-01): Qualified Certificate profile. ETSI. January 2006. Historical. URL: http://www.etsi.org/deliver/etsi_ts/101800_101899/101862/01.03.03_60/ts_101862v010303p.pdf

[etsi-ts-102-176-1]
ETSI TS 102 176-1 V2.1.1 (2011-07): Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms. ETSI. July 2011. Historical. URL: http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.01.01_60/ts_10217601v020101p.pdf

[etsi-ts-102-176-2]
ETSI TS 102 176-2 V1.2.1 (2005-07): Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices. ETSI. July 2005. Historical. URL: http://www.etsi.org/deliver/etsi_ts/102100_102199/10217602/01.02.01_60/ts_10217602v010201p.pdf

[etsi-ts-102-280]
ETSI TS 102 280 V1.1.1 (2004-03): X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons ETSI. March 2004. Historical. URL: http://www.etsi.org/deliver/etsi_ts/102200_102299/102280/01.01.01_60/ts_102280v010101p.pdf

[ISO3166]
ISO 3166: Codes for the representation of names of countries and their subdivisions – Part 1: Country codes. International Organization for Standardization (ISO). November 2013. Published. URL: https://www.iso.org/standard/63545.html

[PKI Policy]
Programma van Eisen (PKIoverheid). Logius. URL: https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen

[rfc3739]
Internet X.509 Public Key Infrastructure: Qualified Certificates Profile. S. Santesson; M. Nystrom; T. Polk. IETF. March 2004. Proposed Standard. URL: https://tools.ietf.org/html/rfc3739

[rfc5280]
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. D. Cooper; S. Santesson; S. Farrell; S. Boeyen; R. Housley; W. Polk. IETF. May 2008. Proposed Standard. URL: https://tools.ietf.org/html/rfc5280

[rfc6187]
X.509v3 Certificates for Secure Shell Authentication. K. Igoe; D. Stebila. IETF. March 2011. Proposed Standard. URL: https://tools.ietf.org/html/rfc6187

[rfc7633]
X.509v3 Transport Layer Security (TLS) Feature Extension. P. Hallam-Baker. IETF. October 2015. Proposed Standard. URL: https://tools.ietf.org/html/rfc7633

[X520]
ITU-T Recommendation X.520 (2001) ISO/IEC 9594-6. ISO. URL: https://www.iso.org/standard/43796.html

↥