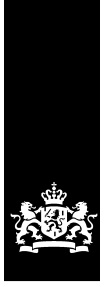

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Gebruik en Achtergrond Digikoppeling Certificaten

Versie 1.3.1

Datum 1 oktober 2014
Status Definitief

Colofon

Logius Servicecentrum:
Postbus 96810
2509 JE Den Haag

t. 0900 555 4555 (10 ct p/m)
e. servicecentrum@logius.nl

Inhoud

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.

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 Achtergrond

Een belangrijk aspect voor beveiliging van Digikoppeling is de juiste identificatie, authenticatie en autorisatie van organisaties. Digikoppeling maakt hiervoor gebruik van een PKI-infrastructuur met certificaten. 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:

- een uitwerking van de consequenties van deze authenticatie-afspraken;
- voorstellen / bestpractices 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).

1.3 Omgang met certificaat

Certificaten zijn gebaseerd op sleutelparen waarvan het publiekedeel 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

[1] *Zie http://www.logius.nl/pkioverheid*
[2] *Zie het document "Digikoppeling Identificatie en Authenticatie"*

(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.

1.4 Leeswijzer

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

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

De volgende hoofdstukken gaan hier per proces stap 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 2: Richtlijnen voor een veilig password.
- Gegevens die in een certificaat opgenomen kunnen worden.
- De opbouw van het OverheidsIdentificatieNummer-formaat.

1.5 Samenhang met andere documenten

De uitwerking van het gebruik van certificaten is gebaseerd op en wordt aangevuld door de volgende documenten:

Meer informatie	Referentie
Digikoppeling 2.0 Architectuur	www.logius.nl/digikoppeling
Digikoppeling 3.0 Architectuur	www.logius.nl/digikoppeling
PKIoverheid "Programma van Eisen"	www.logius.nl/pkioverheid/
Digikoppeling Identificatie en Authenticatie	www.logius.nl/digikoppeling
Digikoppeling 2.0 Koppelvlakstandaard ebMS	www.logius.nl/digikoppeling
Digikoppeling 2.0 Best practices ebMS	www.logius.nl/digikoppeling
Digikoppeling 2.0 Koppelvlakstandaard WUS	www.logius.nl/digikoppeling
Digikoppeling 3.0 Koppelvlakstandaard WUS	www.logius.nl/digikoppeling
Digikoppeling 2.0 Best practices WUS	www.logius.nl/digikoppeling
Digikoppeling 2.0 Koppelvlakstandaard Grote Berichten	www.logius.nl/digikoppeling
Digikoppeling Best practices Grote Berichten	www.logius.nl/digikoppeling

2 Ontwerp aspecten Digikoppeling adapter

2.1 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 ebMS?
5. Wat moet ik doen als ik al een certificaat heb?

2.2 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 zoveel mogelijk in lijn met de Staatsalmanak. Voor Digikoppeling is van belang of organisatie(onderdelen) taken hebben in een wettelijk kader en hun bestuurders tekenbevoegd zijn. Soms identificeert Digikoppeling daarom onderdelen van organisaties.
- Voor de unieke identificatie en authenticatie van deze organisaties is er door PKIoverheid gekozen (zie PKIoverheid Programma van Eisen 3b) om het OIN toe te voegen aan een PKIoverheid certificaat in het zogenaamde Subject.serialNumber-veld.

Een belangrijke overweging is of voor verschillende doelen ook verschillende certificaten gebruikt worden of dat deze doelen in het zelfde 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[3].
- Gebruik voor WUS-omgeving en/of ebMS-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

[3] *Signing is geen functie van Digikoppeling 1.0. Encryptie van data vindt in Digikoppeling 1.0 op TLS-niveau plaats en niet rechtstreeks met de sleutel van het PKIoverheid-certificaat.*

servers een gemeenschappelijke key-store 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)[4] te zijn opgenomen in het certificaat. Combinatie is technisch daarom alleen mogelijk voorzover de TLS-afhandeling in dit verband plaatsvindt op dezelfde (proxy)server met dezelfde CN.

2.3 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] *Hostname of Fully Qualified Name (FQN).*

3 Bestellen certificaat

3.1 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?

3.2 Achtergrond

Er zijn twee manieren om een sleutelpaar van een certificaat aan te maken: zelf genereren of dit door de Certification Service Provicer (CSP) laten doen. Als het sleutelpaar zelf aangemaakt wordt, blijft de primaire sleutel achter op de server en zal alleen de publieke sleutel aan de CSP verzonden worden. De CSP 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 CSP het sleutelpaar aanmaakt, zal de CSP 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.

3.3 Stappen

De procesgang voor het aansluiten op Digikoppeling is beschreven in het document "Leeswijzer aansluitprocedure gebruik Digikoppeling". Deze maakt onderdeel uit van de aansluitkit stelselhandboek die te downloaden is van www.logius.nl/digikoppeling. 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[5].

Bestellen van een certificaat vindt plaats bij een door PKIoverheid aangewezen CSP die certificaten op commerciële basis verstrekt. Logius houdt op haar website een lijst met goedgekeurde CSP's bij die een PKIoverheid certificaat kunnen leveren[6]. 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 CSP's.

[5] *Bijlage "Bijlage 4: Nummersystematiek OIN en HRN" beschrijft de opbouw van het OIN.*
[6] *http://www.logius.nl/pkioverheid/ bevat specifieke informatie over het aanschaffen van een certificaat.*

De websites van de CSP'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".

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 CSP-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[7]. 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"). Het volgende hoofdstuk beschrijft hoe u deze privésleutel zou moeten beveiligen.

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 organisatie onderdeel. Bijvoorbeeld: OU=Digikoppeling
- Common Name (CN): Dit is de FQN van de server (Host + Domain Name). Bijvoorbeeld: www.logius.nl/digikoppeling/
- OverheidsIdentificatieNummer (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[8]. Deze gegevens zijn daarom standaard voor een Digikoppeling certificaat en kan men niet opnemen in het CSR of de aanvraag.

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

[8] *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 CSP 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 nieuwe certificaat aan te vragen. Het volgende hoofdstuk beschrijft hoe u dit certificaat kunt installeren.

4 Installatie certificaat

4.1 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?

4.2 Achtergrond

Beveiliging van de privésleutel kan plaatsvinden door deze op een smartcard (in PKI-termen een Secure User Device of afgekort SUD) te plaatsen. Een dergelijke fysieke beveiliging wordt vaak gecombineerd met een userid/password. Als alternatief kan de privésleutel ook in een password-beveiligde keystore opgeslagen worden. De eerste optie (SUD) heeft de voorkeur van PKIoverheid. Er zijn extra maatregelen nodig als er geen SUD gebruikt wordt. Het programma van eisen[9] dat PKIoverheid aan CSP's oplegt bevat de verplichting aan CSP's om over de juiste beveiliging van sleutels door gebruikers te waken inclusief de mogelijkheid tot audit (zie kader).

PKIoverheid Programma van Eisen deel 3b

In plaats van gebruik te maken van een hardwarematige SUD mogen de sleutels van een services certificaat softwarematig worden beschermd indien compenserende maatregelen worden getroffen in de omgeving van het systeem dat de sleutels bevat. De compenserende maatregelen moeten van een dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren.

De beheerder van de services certificaten die gebruik maakt van deze mogelijkheid voor softwarematige opslag dient bij registratie ten minste een schriftelijke verklaring te overleggen dat compenserende maatregelen zijn getroffen die voldoen aan de hiervoor gestelde voorwaarde. In de overeenkomst tussen abonnee en CSP dient te worden opgenomen dat de CSP het recht heeft om een controle uit te voeren naar de getroffen maatregelen.

4.3 Stappen

Zodra u een door de CSP 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

[9] *Zie http://www.logius.nl/pkioverheid, zoekterm "deel 3b".*

maatregelen eisen vanuit de vertrouwelijkheid van de door hen beheerde gegevens en het gebruik van daarbij behorende certificaten [10].

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.[11] Probeer te allen tijde het kopiëren van privé-sleutels zo veel mogelijk tegen te gaan met fysieke, technische en procedurele maatregelen.

[10] *Een voorbeeld hiervoor vormt de zorg, waar men eisen stelt aan opslag van servercertificaten.*
[11] *Zie bijvoorbeeld https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR212*

5 Distributie en CPA-creatie

5.1 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?

5.2 Achtergrond

Identificatie (en autorisatie) 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 identificatie nummer 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 CSP, 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 ebMS worden certificaten echter ook opgenomen in de CPA's die organisaties uitwisselen. Het is daarom het eenvoudigst om één lijn te trekken en certificaten standaard via het Digikoppeling serviceregister beschikbaar te stellen.

5.3 Stappen

Uitwisseling van certificaten is vaak nodig voor gebruik binnen Digikoppeling verband. Aanbevolen wordt om het certificaat daarom standaard op te nemen in het Digikoppeling serviceregister.

Voor het maken van CPA's kunnen organisaties de daarbij benodigde certificaten uit het Digikoppeling serviceregister ophalen.

6 Gebruiksaspecten

6.1 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?

6.2 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[12].

In specifieke gevallen kan autorisatie op een gedetailleerder niveau noodzakelijk zijn. Voor grote organisaties is het bijvoorbeeld mogelijk om een volgnummer toe te voegen.

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[13] 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[14] [15].

---

[12] *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.*

[13] *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 CSP) 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 CSP's gebruiken bovendien dezelfde CSP-key voor signing van persoonsgebonden certificaten en server-certificaten zodat het verschil tussen de beide type certificaten nog moeilijker is vast te stellen.*

[14] *Digikoppeling communicatiepartners wisselen het OIN uit ten behoeve van deze autorisatietabel.*

[15] *Bijlage 4: "Bijlage 4: Nummersystematiek OIN en HRN" beschrijft de opbouw van het OIN.*

- Autoriseren op organisatie onderdeel:
  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 eisen dat zij een OIN met daaraan toegevoegd een volgnummer toepassen om het specifieke organisatie onderdeel te onderscheiden.

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 CSP. Via een zogenaamde Certificate Revocation List (CRL) maken CSP'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.

CSP'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 CSP's niet verplicht (maar voor CRL's wel). Indien beschikbaar biedt dit wel de mogelijkheid om elk certificaat direct online te verifiëren.

6.3 Stappen

Om de betrouwbaarheid van het certificaat te waarborgen is het nodig om dit regelmatig te vernieuwen. PKIoverheid eist van CSP's dat een certificaat maximaal vijf jaar geldig is maar in de praktijk geven CSP'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 (ebMS) 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[16].
- De geldigheidsduur van het certificaat is niet verstreken.
- Het certificaat is niet ingetrokken door de CSP.

Om na te gaan of het certificaat is ingetrokken (Engels: revoked) publiceren de CSP'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 CSP'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[17].

Bij het gebruik van een CRL dient men er op 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 CSP als ongeldig beschouwd[18]. Hoewel een CRL bruikbaar blijft tot de next update, is het verstandig om deze minimaal elke vier uur te verversen[19]. Basisregistraties (en andere gegevenshouders) kunnen voor hun domein specifieke eisen stellen.

Bij het testen van applicaties is het van belang om certificaten te gebruiken waarvan de structuur overeenkomt met die van een PKIoverheid certificaat[20]. Binnenkort kunnen certificaten met een vergelijkbare structuur maar gegenereerd met een afwijkend stamcertificaat aangevraagd worden. In de tussentijd voorziet het project Digikoppeling in levering van testcertificaten.

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.

---

[16] *Het stamcertificaat Staat der Nederlanden Root CA vindt u op http://www.pkioverheid.nl/ onder "Stamcertificaat installeren". Hier vindt u ook per CSP een link naar de CRL met ingetrokken certificaten.*

[17] *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. Digikoppeling biedt best practices waarin wordt beschreven hoe CRL's worden geconfigureerd voor bijvoorbeeld de Apache Tomcat en Apache HTTP server.*

[18] *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.*

[19] *CSP's zijn verplicht om het intrekken van een certificaat uiterlijk vier uur na melding via de CRL te publiceren.*

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

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 extentie .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 CSP 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 extentie .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 hoogst noodzakelijk) 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 extentie .cer. .der-encoded bestanden hebben soms ook de extentie .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.

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 eenmogen 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 drie maal 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.

Bijlage 3: Subject attributen in certificaat

Voor de meest actuele versie zie het Programma van Eisen van PKIoverheid deel 3b![21]

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 abonnee-organisatie. Het veld heeft de volgende attributen:		PKIo, RFC3739, ETSI TS 102 280	Moet een Distinguished Name (DN) bevatten. Andere attributen dan hieronder genoemd MOETEN NIET worden gebruikt.
Subject.countryName	V	Vaste waarde: C=NL, conform ISO 3166	RFC 3739, X520, ISO 3166, PKIo	PrintableString	Met countryname wordt aangegeven dat het certificaat is uitgege-ven binnen de context van de PKI voor de (Nederlandse) overheid.
Subject.commonName	V	Naam die de service of server identificeert.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	De abonnee dient aan te tonen dat de organisatie deze naam mag voeren. Als de service een DNS-naam heeft, moet deze in de commonName vermeld worden als "fully-qualified domain name" (zie de definitie in deel 4). Een certificaat dat bijvoorbeeld voor pkioverheid.nl wordt aangevraagd, is niet geldig voor secure.pkioverheid.nl.
Het is niet toegestaan in dit attribuut wildcards te gebruiken.					
Subject.Surname	N	Wordt voor servicescertificaten niet gebruikt.			Servicescertificaten zijn niet persoonsgebonden. Gebruik van dit attribuut wordt daarom niet toegestaan om verwarring te voorkomen.
Subject.givenName	N	Wordt voor services certificaten niet gebruikt.			Services certificaten zijn niet persoonsgebonden. Gebruik van dit attribuut wordt daarom niet toegestaan om verwarring te voorkomen.
Subject.pseudonym	N	Het gebruik van pseudoniemen is niet toegestaan.	ETSI TS 102 280, RFC 3739, PKIo		
Subject.organizationName	V	Volledige naam van de organisatie van de abonnee conform geaccepteerd document of basisregistratie	PKIo	UTF8String	De abonnee-organisatie is de organisatie waarmee de CSP een overeenkomst heeft gesloten en namens welke de certificaathouder (service / server) communiceert of handelt
Subject.organizationalU	O	Optionele aanduiding van een organi-satieonderdeel. Dit	PKIo		Dit attribuut mag meerdere malen voorkomen. Het veld moet een

[21] *http://www.logius.nl/pkioverheid/*

nitName		attribuut mag geen functieaanduiding of dergelijke bevatten.			geldige naam van een organisatieonderdeel van de abonnee bevatten conform geaccepteerd document of registratie.
Subject.stateOrProvinceName	A	Het gebruik wordt afgeraden. Indien aanwezig dient dit veld de provincie van vestiging van de abonnee conform geaccepteerd document of basisregistratie te bevatten.	PKIo, RFC 3739	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 dient dit veld de vestigingsplaats van de abonnee conform geaccepteerd document of basisregistratie te bevatten.	PKIo, RFC 3739	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 dient dit veld het postadres van de abonnee conform geaccepteerd document of basisregistratie te bevatten.	PKIo, RFC 3739	UTF8String	Adres moet in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.emailAddress	N	Gebruik is niet toegestaan.	RFC 3280	IA5String	Dit veld mag niet worden gebruikt in nieuwe certificaten.
Subject.serialNumber	O	Het is de verantwoordelijkheid van een CSP om de uniciteit van het subject (service) te waarborgen. Het Subject.serialNumber moet gebruikt worden om het subject uniek te identificeren.	RFC 3739, X 520, PKIo	Printable String	Het nummer wordt door de CSP en/of de overheid bepaald. Het nummer kan per domein verschillen en voor meerdere toepassingen gebruikt worden.
Subject.title	A	Voor services certifcaten is gebruik van het title-attribuut niet toegestaan		ETSI TS 102 280, RFC 3739, RFC 3280	Dit attribuut wordt alleen gebruikt in persoonsgebonden certificaten en dus niet in services certificaten.
subjectPublicKeyInfo	V	Bevat o.a. de publieke sleutel.	ETSI TS 102 280, RFC 3279		Bevat de publieke sleutel en identificeert het algoritme waarmee de sleutel kan worden gebruikt.
IssuerUniqueIdentifier	N	Wordt niet gebruikt.	RFC 3280		Gebruik hiervan is niet toegestaan (RFC 3280)
subjectUnqueIdentifier	N	Wordt niet gebruikt.	RFC 3280		Gebruik hiervan is niet toegestaan (RFC 3280)

Bijlage 4: Nummersystematiek OIN en HRN

OIN formaat, als thans in gebruik voor Overheidsorganisaties
Het basisformaat van het OIN (Overheidsorganisatie Identificatie Nummer) is:

<prefix><nummer><suffix>

Logius maakt voor overheidsorganisaties primair gebruik van het fiscale nummer van de Belastingdienst dat ook is/wordt opgenomen in het NHR. In die gevallen waar een overheidsorganisatie nog geen fiscaal nummer heeft, kan worden uitgeweken naar alternatieven.

Om rekening te houden met een andere systematiek in de toekomst is de lengte van het prefixveld bepaald op 8 posities.

De prefix definieert welk soort nummer volgt.
De waarde van het OIN in het Digikoppeling Service Register en in het veld subject.serialNumber is inclusief de prefix en suffix en daarbij behorende voorloopnullen. Door het gehele nummer te gebruiken wordt zeker gesteld dat het nummer uniek is.

Prefix	Nummer	Suffix
00000001	Fi-nummer van Belastingdienst (9 posities). Dit wordt het RSIN uit het NHR.	"000"
00000002	RSIN of FI-nummer (9 posities)	Volgnummer (3 posities)
00000003	KvK nummer (8 posities)	Volgnummer "0000" (4 posities)
00000004	Nummer van Logius-beheerder (9 posities)	Volgnummer of "000" (3 posities)
00000005	Niet toegewezen	
00000006	Reservering (vestigingsnummer KvK)	
00000007	Niet toegewezen (BRIN)	
00000008 t/m 00000098 en vanaf 00000100	Nog niet toegewezen	
00000099	Reservering (9 posities)	Volgnummer (3 posities)

- Het Fi-nummer (RSIN) wordt opgegeven door de aanvrager en bij Belastingdienst (dan wel in het NHR) gecontroleerd door Logius.
- De suffix met volgnummer voor het RSIN / Fi-nummer wordt door Logius sequentieel (beginnen bij 1) uitgedeeld op volgorde van aanmelding.
- Het KvK-nummer kan uit het Handelsregister van de KvK na opgave door de aanvrager gecontroleerd worden door Logius.
- Het door Logius toegekende nummer van Logius beheerder wordt sequentieel toegekend (te beginnen bij 1) op volgorde van aanmelding.

- De suffix met volgnummer voor het Logius toegekende nummer wordt sequentieel (beginnen bij 1) uitgedeeld op volgorde van aanmelding. De suffix "000" geeft aan dat dit de totale organisatie betreft en niet een onderdeel.

Voorbeelden:
OIN o.b.v. FI-nr: 00000001123456789000
OIN o.b.v. Logius-beheerder: 00000004123456789012

Het gehele nummer wordt opgenomen in het certificaat (subject.serialNumber). Dat gehele nummer geldt dus als OIN.

HRN formaat, als te gebruiken voor Bedrijven
De opbouw van het HRN (Handels Register Nummer) is identiek aan het OIN:

<prefix><nummer><suffix>

Voor het HRN worden tot nog toe alleen onderstaande mogelijkheden onderkend.

Prefix	Nummer	Suffix
00000001	RSIN uit NHR (9 posities)	"000"
00000003	KvK nummer uit NHR (8 posities)	Volgnummer "0000" (4 posities)
00000002 en 00000004	Niet gebruikt.	
vanaf 00000005	Niet gebruikt.	

In de HRN-variant worden de nummers vastgesteld door de CSP, op basis van het door de aanvrager opgegeven KvK-nummer, dat door de CSP wordt gecontroleerd.