



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Digikoppeling Identificatie en Authenticatie

Versie 1.1

Datum 6 januari 2010

Colofon

Projectnaam	Digikoppeling
Versienummer	Definitief
Organisatie	Servicecentrum Logius Postbus 96810 2509 JE Den Haag T 0900 555 4555 servicecentrum@logius.nl
Bijlage(n)	0

Inhoud

Colofon	2
Inhoud	3
1 Inleiding	4
2 Probleemstelling	5
3 Kernbegrippen	6
3.1 <i>Identificatie</i>	6
3.2 <i>Authenticatie</i>	6
3.3 <i>Autorisatie</i>	6
3.4 <i>Niveau van identiteit</i>	6
3.5 <i>Vastlegging, audittrail</i>	7
4 Gewenst niveau van identiteit	8
4.1 <i>Autorisatie</i>	8
4.2 <i>Voorstel voor principe</i>	9
4.2.1 <i>Gevolg voor verantwoordelijkheden</i>	9
4.2.2 <i>Beoogd resultaat</i>	9
4.2.3 <i>Voorbeelden</i>	9
4.3 <i>Vastlegging</i>	10
4.3.1 <i>Beoogd resultaat</i>	10
4.4 <i>Intermediair en koppelpunt</i>	11
4.4.1 <i>Identiteit, authenticatie en vastlegging bij koppelpunten</i> 11	
5 Identiteit en nummer	13
5.1 <i>Voorstel</i>	14
Bijlage WPB (Wet Bescherming Persoonsgegevens)	15

1 Inleiding

Dit document beschrijft de uitgangspunten en principes voor identificatie- en authenticatieafspraken die gehanteerd worden tussen overheidsorganisaties bij gebruik van Digikoppeling (voorheen Overheidsservicebus).

Digikoppeling maakt het mogelijk voor overheidsorganisaties om op een gestandaardiseerde wijze gebruik te maken van elkaars services, conform de NORA (Nederlandse Overheids Referentie Architectuur).

In de e-overheid gaat het over geautomatiseerde systemen van die organisaties die services aanbieden en afnemen dus over zogeheten system-to-system verkeer.

Conform de NORA moet eerst duidelijkheid bestaan over de bedrijfs- en informatiearchitectuur voor dit onderwerp. Daarvan afgeleid komt pas de technische architectuur. Die architectuuraspecten van identificatie en authenticatie richten zich op drie verschillende onderwerpen, die in separate documenten worden beschreven:

- Welke identiteit is gewenst en waarom (bedrijfs- en informatiearchitectuur) - dat wordt in dit document beschreven.
- Wat betekent die benadering van identiteit voor het authenticatiemiddel in combinatie met PKIoverheid certificaten (informatie- en technische architectuur).
- Hoe wordt authenticatie ondersteund op Digikoppeling, dat wil zeggen: hoe wordt met dat middel omgegaan (technische architectuur).

Dit document gaat over de bedrijfsarchitectuur. Eerst beschrijven we de probleemstelling in hoofdstuk 2. De kernbegrippen staan gedefinieerd in hoofdstuk 3. In hoofdstuk 4 analyseren we het gewenste niveau van de identiteit voor overheidsorganisaties, uitmondend in een architectuurprincipe. Hoofdstuk 5 gaat in op de vraag hoe de (nummer)identiteit vorm krijgt.

2 Probleemstelling

Als een overheidsorganisatie gebruik wil maken van een service van een andere organisatie, zal vastgesteld moet worden of dat is toegestaan. In e-overheidstermen vertaald: er moet vastgesteld worden of een systeem van een organisatie gebruik mag maken van een webservice van een andere organisatie. Deze vaststelling (autorisatie) gebeurt door de serviceaanbiedende organisatie, die dus moet weten wie de service wil afnemen, om te kunnen bepalen of dat mag. Daartoe moet de serviceafnemer geïdentificeerd worden, dat wil zeggen: zijn identiteit moet geverifieerd worden (authenticatie) bij de aanbieder.

NORA principe P5 stelt:

Burgers, bedrijven en maatschappelijke instellingen beschikken over één identiteit die bruikbaar is voor alle contacten met organisaties in het publieke domein en die afhankelijk van de soort dienstverlening ook nodig is en gevraagd moet worden. Dit ongeacht de keuze voor een kanaal. Een en ander komt neer op één administratieve identiteit (één identificatienummer). Deze administratieve identiteit dient afgebeeld te worden op een (ook digitaal toepasbaar) identiteitsbewijs.

Dit principe moet ook van toepassing zijn op de overheidsorganisaties. Daarbij bestaan nog een aantal vragen. Wanneer vanuit een systeem van overheidsorganisatie A een verzoek komt om een service bij een andere organisatie B af te nemen, zijn er nog veel vragen bij het vaststellen van wie een verzoek afkomstig is. Is het van belang welke medewerker van organisatie A het verzoek geïnitieerd heeft? Is het van belang of het verzoek uit een bepaald organisatieonderdeel (dienst, directoraat, agentschap of ZBO) komt? Is het van belang op basis van welke wettelijke taak het verzoek gedaan wordt. Als een organisatieonderdeel geïdentificeerd moet worden, wat is daarvan dan de identiteit (het 'id-nummer')? Antwoorden op dit soort vragen hebben meestal gevolgen voor verantwoordelijkheden en daarmee voor de onderlinge relatie tussen de betrokken partijen.

Dit document beoogt antwoorden te geven op deze vragen. Het gewenste doel is het aantal discussies dat nu over deze onderwerpen plaatsvinden te verminderen en te komen tot standaardoplossingen die optimaal hergebruikt kunnen worden.

3 Kernbegrippen

Voor Kernbegrippen- zie ook voetnoten ⁻¹

3.1 Identificatie

Identificatie is het kenbaar maken van de identiteit van een subject² (een persoon/gebruiker of een proces/systeem). De identiteit wordt gebruikt om de autorisatie (zie verder) - de toegang tot een service - te beheersen.

3.2 Authenticatie

Authenticatie is als volgt gedefinieerd:

Authenticatie is het proces waarbij nagegaan wordt of een subject daadwerkelijk is wie hij beweert te zijn, dat wil zeggen: daadwerkelijk de identiteit bezit die hij opgeeft.

Bij de authenticatie wordt bijv. gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken^{3 4}. Het proces van authenticatie is dus onlosmakelijk verbonden met identiteit.

Authenticatie levert als het ware de kwaliteit van de identificatie. Tevens speelt hier een 'chain of trust'. Als een paspoort beschikt over de echtheidskenmerken (en het is niet gestolen of verlopen) dan mag men op de inhoud vertrouwen. Hetzelfde geldt voor een PKI-overheid certificaat. Als het 'root' certificaat te vertrouwen is (en het certificaat is niet ingetrokken of verlopen) dan mag men op de inhoud vertrouwen.

3.3 Autorisatie

Autorisatie is het proces waarin een subject rechten krijgt op het benaderen van een service. De autorisatie wordt toegekend door de service-eigenaar. Het leidende principe (met name bij persoonsgegevens) is doelbinding: je mag alleen zien wat je voor je taak nodig hebt.

De primaire reden voor het vaststellen van de identiteit van een subject is om op basis daarvan vervolgens vast te stellen of dat subject ook gerechtigd is om de gewenste service af te nemen. Die autorisatie (al of niet mede op basis van rollen, machtigingen, vertegenwoordigingen enzovoort) is nadrukkelijk een op de authenticatie volgende, aparte stap. De geauthenticeerde identiteit is dus nodig om autorisatie te kunnen doen. Autorisatie stelt eisen aan authenticatie.

3.4 Niveau van identiteit

Vooral het niveau van de identiteit is van belang. Het gaat dan om de vraag of het niveau 'organisatie' voldoende is of dat het meer gedetailleerde niveau 'medewerker binnen een organisatie' noodzakelijk is.

¹ Er circuleren vele tekstvarianten voor de definities; de kern is in het algemeen gelijk

² Voor terminologie wordt aangesloten bij de OASIS standaarden, o.a. SAML: 'Subject: A principal in the context of a security domain. SAML assertions make declarations about subjects'. De term subject wordt ook gehanteerd in de PKI-wereld, X509

³ Voor authenticatie wordt daarom ook wel de term verificatie gehanteerd.

⁴ De definitie van authenticatie in de NORA gaat meer in op het aspect hoe authenticatie wordt uitgevoerd dan op wat het is. Daarom wordt die definitie hier niet overgenomen.

3.5 Vastlegging, audittrail

Met vastlegging wordt hier bedoeld het vastleggen (loggen, bijvoorbeeld in een audittrail) van het resultaat van authenticatie en autorisatie. De eisen die daaraan gesteld worden, zijn belangrijk. Moet jaren later nog voor de rechter bewezen kunnen worden dat dit subject op dit tijdstip een specifieke service vraag gesteld heeft, of wordt alleen vastgelegd ten behoeve van latere statistische bewerkingen.

De eisen die gesteld worden aan vastlegging, zijn weliswaar belangrijk, maar ze hebben met name betrekking op zaken als traceerbaarheid van authenticatie; heeft authenticatie wel plaatsgevonden en hoe dan wel enzovoort. Ze hoeven geen rol te spelen bij de bepaling van de gewenste (niveau van) identiteit.

Dat kan anders zijn als de eisen aan niveau van zowel autorisatie als vastlegging verschillen. Dat zou het geval kunnen zijn als er regels gelden zoals: 'iedere medewerker van een geautoriseerde partij heeft toegang, maar er moet wel onweerlegbaar worden vastgelegd welke medewerker het betrof' (autorisatie op niveau van partij, vastlegging op niveau van medewerker). De eisen vanuit de behoefte aan autorisatie en de noodzakelijke vastlegging voor bewijs achteraf kunnen dus verschillen.

4 Gewenst niveau van identiteit

Het gewenste niveau van de identiteit wordt in dit hoofdstuk eerst bepaald aan de hand van de eisen vanuit autorisatie, en daarna vanuit vastlegging.

4.1 **Autorisatie**

In de Service Gerichte benadering van de NORA maken applicaties van de ene organisatie gebruik van services van een andere organisatie. Een service mag alleen afgenomen worden door geautoriseerde afnemers, namelijk die afnemers die een juridische basis⁵ of een overeenkomst hebben met de aanbieder van de betreffende service.

Afnemers in de overheid kennen vele organisatorische 'niveaus' met diverse juridische statussen: gemeentelijke diensten, departementale directoraten, agentschappen, ZBO's etc., al dan niet zijnde rechtspersonen. De vraag is dus welk niveau, en dus welke identiteit, gebruikt zou moeten worden.

Het ligt voor de hand om hier uit te gaan van de organisatie(onderdeel), dat kennelijk zelfstandig bevoegd is (bijv. op basis van een besluit of mandaat) dan wel een juridische basis heeft. Een dergelijke vastlegging tussen aanbieder en afnemer noemen we hierna een overeenkomst.

Uitgangspunt is:

- de identiteit van de afnemer die gebruikt wordt voor autorisatie tot het afnemen van een service, moet overeenkomen met de identiteit van de organisatie(onderdeel) waarmee een overeenkomst bestaat tot het gebruik van de service. Authenticatie en vervolgens autorisatie vinden daarom in eerste instantie plaats op het niveau van de identiteit die is gebruikt bij de overeenkomst.

De vraag is of dat niveau het juiste niveau is voor autorisatie of dat er nog verfijning nodig is. Een serviceaanbieder kan theoretisch op verschillende manieren de autorisatie en de daarvoor benodigde identificatie inrichten. De aanbieder zou bijvoorbeeld kunnen stellen, dat medewerker X van afnemersorganisatie A een service wel mag afnemen en medewerker Y van diezelfde organisatie niet.

Er bestaat brede consensus (ook in andere landen), dat dit ongewenst is. Enerzijds is namelijk de afnemende organisatie verantwoordelijk voor eigen informatiebeveiliging, dus voor het op de juiste wijze autoriseren van de eigen medewerkers. Anderzijds wordt de organisatie die de service aanbiedt dan niet met medewerkers van een ander geconfronteerd en om dezelfde reden ook niet met 'afdelingen' of informatiesystemen van die organisatie. Het is gewenst is om alleen maar te autoriseren op het niveau van een organisatie.

Als dat het autorisatieprincipe is, dan stelt dat als eis aan de identificatie, dat alleen de identiteit van de afnemerorganisatie vastgesteld (geauthenticeerd) hoeft te worden.

⁵ De terminologie moet nog juridisch correct gemaakt worden; in deze notitie wordt (juridisch) wat losjes gesproken over 'zelfstandig bevoegd', 'juridische basis' enzovoort.

4.2 Voorstel voor principe

Autorisatie tot afnemen van een service vindt plaats op basis van de identiteit van de zelfstandig bevoegde afnemerorganisatie, dat wil zeggen: op het niveau van de overheidsorganisatie waarop de juridische afspraak gemaakt is.

Autorisatie en authenticatie gebeurt bij de serviceaanbieder niet op een verder gedetailleerd niveau, zoals medewerker, afdeling, applicatie of wettelijke taak.

4.2.1 *Gevolg voor verantwoordelijkheden*

Consequentie is, dat afnemende organisaties verantwoordelijk zijn voor de eigen interne autorisaties (met betrekking tot medewerkers, afdelingen, taken enzovoort), bijbehorende maatregelen moeten treffen en daar controleerbaar verantwoording over moeten afleggen.

Alle overheidsorganisaties hebben al een dergelijke verplichting in het kader van persoonsgegevens, in relatie tot de Wet Bescherming Persoonsgegevens (WBP).

Een belangrijk deel van de verantwoordelijkheid voor informatiebeveiliging komt te liggen bij de afnemerorganisatie. Die dient ervoor zorg te dragen, dat servicerequests alleen kunnen worden gedaan door daartoe bevoegde medewerkers en daartoe bevoegde applicaties/systemen. Ook dit is feitelijk gezien vanuit WBP en andere privacy/beveiligingskaders geen nieuwe eis.

4.2.2 *Beoogd resultaat*

Met dit voorstel bereiken we, dat er uniformiteit ontstaat bij het afnemen van services. Afgezien van de spreekwoordelijke uitzonderingen zal er duidelijkheid en eenduidigheid ontstaan over welke overheidsorganisaties 'bestaan' in de e-overheid.

De onderlinge verantwoordelijkheden worden hiermee scherper. Organisaties die services aanbieden, hebben allemaal te maken met dezelfde afspraken met organisaties die services afnemen. Een afnemende organisatie hoeft niet de ene keer wel (een bewijs van) de identiteit van een medewerker mee te leveren om geautoriseerd te kunnen worden voor een bepaalde service en de andere keer niet.

4.2.3 *Voorbeelden*

Voorbeelden van zelfstandig bevoegde organisaties volgens bovenstaande uitgangspunten zijn:

- Individuele gemeenten, provincies, waterschappen enzovoort.
- Uitvoeringsorganisaties, ZBO's.
- Agentschappen als BPR.
- Projecten als PIP (met een bijzonder status volgens AmvB⁶).
- Afdelingen als BKWI (onderdeel van CWI/UWV), Logius.

Nog vastgesteld moet worden wat het gewenste niveau is bij grote onderdelen van zeer grote organisaties, bijvoorbeeld van de Douane binnen de Belastingdienst.

⁶ Algemene Maatregel van Bestuur

4.3 Vastlegging

Ongeacht het voorgaande is het mogelijk, dat aan de afnemende organisatie strengere eisen gesteld worden aan het vastleggen van het gebruik van gegevens.

Ook de WBP formuleert, in het kader van verstrekking aan derden en informeren van betrokkene, de eisen op het niveau van verantwoordelijke dat wil zeggen de rechtspersoon. Aangezien het hier een juridische omgeving betreft en de WBP expliciet open geformuleerd is, dient dit in voorkomende gevallen verder juridisch uitgezocht te worden.

Uitgangspunt in dit document is dat – in termen van de WBP - bij verstrekking alleen de ontvangende verantwoordelijke relevant is en niet de kring van «personen die onder rechtstreeks gezag van de verantwoordelijke gemachtigd zijn om gegevens te verwerken». Personen lijken dus niet relevant, wel verantwoordelijken in de zin van de WBP.

Een praktisch argument om niet de gegevens van medewerkers van de afnemer vast te leggen bij de aanbieder is, dat overheidsorganisaties vaak een dossier of zaak behandelen, waarbij diverse medewerkers van de betreffende organisatie betrokken zijn. De aanbieder kan hooguit zicht houden op de toevallige eerste medewerker die informatie opvraagt, maar niet op alle volgende medewerkers. Dat geldt zeker wanneer dat dossier actueel gehouden wordt door (een mechanisme van) abonnementen.

De bovenstaande redenering voor medewerkers is ook geldig voor andere onderverdelingen, zoals medewerker afdeling, systeem, enzovoort bij de (zelfstandig bevoegde) afnemer.

Conclusie:

De vastlegging van de gebeurtenis van afnemen gebeurt door de aanbieder op het niveau van afnemerorganisatie. Het is niet nodig en niet gewenst om dat te doen op een niveau binnen die afnemer zoals medewerker afdeling, systeem of wettelijke taak.

Gevolg van dit uitgangspunt is, dat een verantwoordelijke alleen maar inzage kan geven in de organisaties aan wie gegevens zijn verstrekt. Die andere organisatie moet dan vervolgens inzicht kunnen geven welke medewerkers (en welke andere organisaties, indien van toepassing) de informatie hebben opgevraagd.

Iets heel anders is, dat er onderling kan worden afgesproken dat een naam van een medewerker wordt meegegeven als onderdeel van de via de service uitgewisselde informatie, zodat men daarmee contact kan opnemen bij verdere vragen (vergelijk 'behandeld door').

4.3.1 Beoogd resultaat

Met dit voorstel bereiken we dat de uniformiteit, die ontstaat door vanuit de autorisatie, blijft bestaan als ook de vastlegging wordt meegenomen. Als niet gekozen zou worden voor de vastlegging op niveau van organisatie, dan kan een diversiteit ontstaan bij gebruik van services. Bepaalde serviceaanbieder zouden dan kunnen gaan eisen, dat identiteitsbewijzen worden meegeleverd bij een serviceaanvraag. Door een dergelijke eis van een bepaalde serviceaanbieder zou een

serviceafnemer gedwongen kunnen worden om extern verifieerbare identiteitsbewijzen te kunnen leveren.

4.4 Intermediair en koppelpunt

Een bijzondere situatie ontstaat wanneer er sprake is van een intermediaire organisatie. Deze situatie komt tussen overheidsorganisaties het meest voor aan de rand van een sector. Partijen in de sector communiceren via een sector koppelpunt met de wereld buiten de sector. Zie hierover NORA paragraaf 6.5:

Koppelpunten versus aanspreekpunten

Voor de koppeling tussen servicebussen kan gekozen worden tussen twee niveaus:

- een puur logistieke koppeling, dat wil zeggen: een overslagpunt waarin verkeer over de ene bus naar de andere wordt overgebracht door middel van koppelpunten, zonder interpretatie van de gegevensinhoud;
- een inhoudelijke koppeling, dat wil zeggen: een keten, sector- of domeinloket of –aanspreekpunt, dat de interne complexiteit van de keten, de sector of het domein voor de buitenwereld afschermt.

De belangrijkste factor in dit onderscheid zit niet op de eerste plaats in het technische of functionele. Veel belangrijker is dat er in geval van een inhoudelijke koppeling een echte overheidsorganisatie (of wellicht privaat publieke organisatie) moet worden aangewezen of gecreëerd die de bedoelde inhoudelijke diensten ook feitelijk namens de keten, de sector of het domein kan aanbieden of afnemen en daarvoor inhoudelijk verantwoordelijk gehouden kan worden, op basis van en/of passend in toepasselijke wetgeving. Anders gezegd, hier is sprake van inhoudelijke intermediaire. Denk hierbij bijvoorbeeld aan:

- een virtueel ketendossier dat via één loket voor afnemers buiten de keten wordt ontsloten
- het sectorloket voor het onderwijsveld, ondergebracht bij de IB-Groep
- het BKWI dat namens het werk- en inkomensveld bevestigingen doet bij de RDW e.a.

Aanspreekpunten kunnen beide kanten op werken: zij kunnen services namens de hele sector, keten of domein aanbieden aan 'externe partijen', maar zij kunnen ook, namens de gehele sector, keten of domein diensten afnemen van buiten.

Een inhoudelijke koppeling is niet mogelijk zonder een logistieke koppeling. Andersom kan wel: een logistieke koppeling zonder een inhoudelijk aanspreekpunt. In dat geval is er alleen sprake van een logistieke 'brug' naar de sector, zonder dat de keten, de sector of het domein als geheel is aan te spreken of handelt. Mengvormen zijn ook mogelijk, waarin de sector, het domein of de keten voor bepaalde services als geheel optreedt en voor andere niet.

4.4.1 *Identiteit, authenticatie en vastlegging bij koppelpunten*

In het onderlijnde gedeelte van bovenstaande NORA tekst is al aangegeven, dat in de variant van de inhoudelijke koppeling een echte overheidsorganisatie moet bestaan die verantwoordelijk kan worden gehouden. Voorgesteld wordt om die variant van de inhoudelijke koppeling in deze notitie als intermediair te benoemen. In dat geval wordt de intermediaire organisatie op basis van de toepasselijke wetgeving (dus weer 'zelfstandig bevoegd') als serviceafnemer beschouwd, die

geauthenticeerd en geautoriseerd moet worden. Voor de serviceaanbieder is dat gelijk aan het aanbieden van een service aan een 'gewone' organisatie. Er dient dan ook alleen vastgelegd te worden, dat de intermediair de service heeft afgenomen. Het formeel vastleggen, dat een achterliggende partij eigenlijk de service wil afnemen, gebeurt dan niet bij de uiteindelijke service verlenner, maar natuurlijk wel bij de intermediair. Ook de vastlegging gebeurt bij de serviceaanbieder (net als bij een normale afnemer).

In het geval van een logistiek koppelpunt heeft de aanbieder feitelijk te maken met de identiteit van de achterliggende afnemer. Het logistieke koppelpunt wordt niet gezien. Bij de vastlegging is het de vraag of het noodzakelijk is te weten of de serviceaanvraag via het logistieke koppelpunt tot stand kwam.

Als we consequent de redenering volgen zoals in § 4.3 - is beschreven, dan is het niet nodig om het logistieke koppelpunt in de vastlegging mee te nemen. Uiteraard kan dat alleen als er voldoende waarborgen en afspraken (bijvoorbeeld bewerkovereenkomst⁷) zijn.

De criteria die bepalen wanneer een intermediair als inhoudelijk koppelpunt beschouwd wordt en wanneer als een puur logistiek koppelpunt, moeten nog worden aangescherpt.

⁷ Andere vormen van bewerkers, die ten behoeve van een verantwoordelijke (in de zin van de WBP) gegevens verwerken, laten we hier vooralsnog buiten beschouwing. De hoofdlijn is ook daar dat er voor de identiteit uitgaan wordt van de 'zelfstandig bevoegde', dus de verantwoordelijke.

5 Identiteit en nummer

In hoofdstuk 4 beschreven we, dat zowel de autorisatie tot afnemen van een service als de vastlegging ervan plaats vindt op basis van de identiteit van de zelfstandig bevoegde afnemerorganisatie.

Dat betekent dat er behoefte is aan eenduidige identificatie van overheidsorganisaties op het niveau van zelfstandig bevoegde organisaties. Een identificatienummer is gewenst voor deze overheidsorganisaties, bij voorkeur onderdeel van een authentieke registratie, logischerwijs het NHR.

Dat nummer van de hier bedoelde zelfstandig bevoegde overheidsorganisaties wordt hierna aangeduid onder de werknaam 'Organisatie Identificatie Nummer' OIN.⁸

Idealiter zou dat OIN overeenkomen met een nummer uit het NHR. Daarbij rijst de vraag: 'Komen alle organisaties die we willen identificeren met een OIN wel voor in het NHR?'.

De inhoud van het NHR is (ten aanzien van overheidsorganisaties) nog onzeker. Het wetsvoorstel is nog niet afgerond en de behandeling zal mogelijk nog wijzigingen brengen. NHR onderkent in de structuur drie niveaus:

- Het niveau rechtspersoon met als identificatienummer het Fi-nummer. NHR heeft aangegeven, dat dat niveau, en dus dat nummer, in principe het meest geschikt is om voor identificatie op Digikoppeling te gebruiken.
- Het niveau onderneming/maatschappelijke activiteit met als identificatienummer het KvKnummer. Aangegeven is, dat dat nummer naar alle waarschijnlijkheid voor de overheid als OIN (dus op Digikoppeling) niet geschikt is.
- Het niveau vestiging, een relatief zelfstandig onderdeel binnen rechtspersoon en/of onderneming. Mogelijk is/wordt dat niveau wel bruikbaar voor OIN.

Volgens NHR is 'rechtspersoon' met een Fi-nummer een criterium voor een op te nemen organisatie. Maar: niet alle ZBO's bijvoorbeeld zijn een rechtspersoon. Ander voorbeeld is PIP. PIP is door middel van het besluit PIP gerechtigd (heeft de bevoegdheid gekregen) om GBA services af te nemen en wordt daarmee dus onderkend als een zelfstandige 'organisatie', die door de GBA geautoriseerd moet kunnen worden. Komt PIP dan in het NHR? En gebeurt dat dan als rechtspersoon of bijvoorbeeld als vestiging (bijvoorbeeld van BZK)?

Naar verwachting zullen er 'organisaties' zijn die services aanbieden of afnemen, maar niet als zodanig in het beoogde NHR voorkomen. Duidelijkheid over de inhoud van NHR zal er pas zijn na behandeling in de Kamer, thans gepland medio 2008.

Gebruik van het Fi-nummer ten behoeve van identificatie op Digikoppeling benadert de gewenste situatie het meest, maar dekt de behoefte van OIN niet volledig. Vrijwel alle ZBO's, alle gemeenten, provincies enzovoort zullen op dat niveau met Fi-nummer opgenomen worden in het NHR. Voor overige organisaties is er nu in het NHR geen identificatie.

⁸ De term BIN wordt hier bewust niet gebruikt, omdat die een veel bredere lading heeft.

De voortgang van de e-overheid en de ontwikkeling van Digikoppeling daarbinnen vereist echter een keuze op korte termijn. Die keuze moet optimaal aansluiten bij de verwachte ontwikkelingen van het NHR.

5.1

Voorstel

Op basis van het voorgaande wordt voorgesteld om voor gebruik op Digikoppeling als OIN te hanteren:

- ofwel het Fi-nummer voor de grote groep organisaties waarvoor dat Fi-nummer bestaat en gebruikt kan worden.
- ofwel een nieuw nummer voor de overige organisaties. Dat nieuwe nummer wordt uitgereikt door Logius als beheerder van Digikoppeling.

Verder:

- Het OIN wordt opgenomen in het Digikoppeling serviceregister. Daarin worden tenminste opgenomen alle services die m.b.v. Digikoppeling worden gepubliceerd en afgenomen, met daarbij o.a. informatie over de betreffende organisaties. Het OIN wordt op deze manier gehanteerd als het identificatienummer van die organisaties op Digikoppeling. Door zowel Fi-nummer als Digikoppelingnummer op te nemen in het serviceregister, ontstaat één register dat alle identificatienummers voor gebruik op Digikoppeling bevat.
- Wanneer later organisaties uit de tweede categorie (dus zonder bruikbaar Finummer) alsnog opgenomen worden in het NHR, kan het OIN daarmee in overeenstemming worden gebracht. De inhoud van het NHR blijft leidend.

Dat OIN wordt opgenomen in het PKIoverheid certificaat. Omdat PKIoverheid certificaten niet alleen door overheidsorganisaties gebruikt worden voor identificatie naar andere overheidsorganisaties, maar ook bijvoorbeeld voor bedrijfsleven naar overheid, is het nodig onderscheid te kunnen maken naar het soort nummer.

Er wordt daarom een prefix gehanteerd voorafgaand aan dat nummer, dat aangeeft of het een NHRFi-nummer, of bijvoorbeeld een NHR-KvK-nummer betreft, ofwel een door Logius uitgereikt nummer.

De systematiek in deze notitie is bedoeld om zo duidelijk mogelijk te zijn over de inrichting van identificatie en authenticatie bij gebruik van Digikoppeling. Het is uitgesloten, dat hiermee de gehele werkelijkheid wordt afgedekt. Daarom beslist de beheerder van Digikoppeling over alle verzoeken die afwijken van de in deze notitie aangegeven lijn.

Bijlage WPB (Wet Bescherming Persoonsgegevens)

Delen uit WBP

WBP Artikel 34

1. Indien persoonsgegevens worden verkregen op een andere wijze dan bedoeld in artikel 33, deelt de verantwoordelijke de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij deze reeds daarvan op de hoogte is:
 - a. op het moment van vastlegging van hem betreffende gegevens, of
 - b. wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.
2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking mede.
3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
4. Het eerste lid is niet van toepassing indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige service providerinspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast. .
5. Het eerste lid is evenmin van toepassing indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid.

Memorie van Toelichting WBP

Onderdeel g

De derde is degene, die niet de betrokkene, noch de verantwoordelijke, noch de bewerker en noch de persoon is die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om de gegevens te verwerken.

De begripsomschrijving van «derde» sluit inhoudelijk aan bij hetgeen reeds onder de WPR gold. De kring van «personen die onder rechtstreeks gezag van de verantwoordelijke gemachtigd zijn om gegevens te verwerken» sluit aan bij de personen die «binnen de organisatie van de houder» gegevens mogen ontvangen(zie de omschrijving van «verstrekken van gegevens aan een derde» in artikel 1, in samenhang gelezen met artikel 6, tweede lid, WPR). Uit de omschrijving van «derde» in het onderhavige artikel blijkt nu expliciet dat personen binnen de organisatie van de verantwoordelijke die niet onder zijn rechtstreeks gezag staan, als derden moeten worden aangemerkt. Verschillende rechtspersonen binnen een concern kunnen om die reden ten opzichte van elkaar in beginsel als derden worden beschouwd. Het onderscheid tussen verantwoordelijke, bewerker en derde uit zich in de relatie die ze onderling hebben. Kent de persoon een hiërarchische relatie tot verantwoordelijke dan zal gesproken moeten worden van (intern) beheer.

Gegevensverwerking vindt dan plaats binnen de organisatie van de verantwoordelijke en onder diens rechtstreeks gezag. Valt de persoon niet

onder rechtstreeks gezag van de verantwoordelijke (geen hiërarchische relatie) echter is wel sprake van een relatie met de verantwoordelijke met betrekking tot de te verwerken gegevens (contractuele relatie), dan kan die persoon worden aangemerkt als bewerker. Valt de persoon niet onder rechtstreeks gezag van de verantwoordelijke en kent hij evenmin een contractuele relatie met betrekking tot de te verwerken gegevens met de verantwoordelijke, dan zal de persoon als derde zijn aan te merken. In tegenstelling tot de bewerker zal de derde de gegevens veelal voor eigen behoefte verwerken. Het begrip «derde» speelt in dit wetsvoorstel een minder centrale rol dan in de WPR. In paragraaf 3 van de WPR is het begrip cruciaal in het verstrekkingenregime dat van toepassing is. In paragraaf 9.2 van het algemeen deel van de toelichting is hier reeds op ingegaan. In de WBP speelt het begrip alleen nog een rol bij het verstrekken van bepaalde gevoelige gegevens (artikelen 17, derde lid, 19, tweede lid, en 20, tweede lid), het moment waarop een informatieplicht ontstaat (artikel 34, eerste lid, onder b) en in bepaalde gevallen als rechtvaardigingsgrond voor het verwerken van gegevens (bijvoorbeeld artikelen 8, onder f, en 22, vierde lid).

Onderdeel h

Ontvanger is degene aan wie de gegevens worden medegedeeld. De ontvanger kan zowel een persoon binnen de organisatie van de verantwoordelijke zijn als een persoon buiten de organisatie van de verantwoordelijke (bewerker of derde). Het begrip «ontvanger» heeft in dit wetsvoorstel met name betekenis ten aanzien van de informatieverplichtingen van de verantwoordelijke. De verantwoordelijke moet de betrokkene onder bepaalde omstandigheden op de hoogte stellen van de bij de verwerking betrokken ontvangers of categorieën van ontvangers indien de betrokkene daarvan niet reeds op de hoogte is. Daarnaast speelt het begrip een rol bij de aanmeldingsverplichting: op grond van artikel 28 moeten ontvangers of categorieën ontvangers aan wie de gegevens kunnen worden verstrekt worden aangemeld bij de Registratiekamer.