Logius - Vastgestelde versie

Digikoppeling Handreiking Adressering en Routering 1.1.0

Logius Handreiking
Vastgestelde versie 13 februari 2023

Deze versie:
https://publicatie.centrumvoorstandaarden.nl/dk/bpadres/1.1.0

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

Laatste werkversie:
https://logius-standaarden.github.io/Digikoppeling-Handreiking-Adressering-en-Routering/

Vorige versie
https://publicatie.centrumvoorstandaarden.nl/dk/bpadres/1.0.1/

Redacteur:
Logius (Logius)

Auteur:
Logius (Logius)

Doe mee:
GitHub Logius-standaarden/Digikoppeling-Handreiking-Adressering-en-Routering
Dien een melding in
Revisiehistorie
Pull requests

This document is also available in this non-normative format: pdf

---

Samenvatting

Dit document beschrijft op welke manieren het OIN kan worden gebruikt voor Adressering en Routering.

Status van dit document

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

Inhoudsopgave

§ 1. Handreiking Adressering en Routering

§ 1.1 Doel van de Handreiking

De handreiking heeft tot doel organisaties een hulpmiddel te bieden hoe om te gaan met adresseren en routeren en het gebruik van het OIN hierbij.

§ 1.2 Welke vragen worden beantwoord

Deze handreiking beschrijft wat we verstaan onder adresseren en routeren en op welke manier het OIN hierbij een rol speelt. Verder beschrijven we in detail hoe OIN's en subOIN's gebruikt kunnen worden in een berichtenketen.

Naast de identificatie van organisaties die niet in aangesloten registers staan, bieden subOIN's ook de mogelijkheid van routeren van berichten door gebruik te maken van fijnmazige identificatie.

De volgende vragen komen aan de orde:

1. Het OIN wordt zowel gebruikt voor authenticatie als voor adressering.

- Hoe werkt dit precies?
- Op welke plek wordt het OIN gebruikt?
- Kunnen er verschillende OIN's gebruikt worden?

2. Wanneer is het aan te raden om subOIN's te gebruiken voor adresseren en routeren?

3. Hoe werkt routeren en adresseren?

- Wat zijn de regels die partijen met elkaar moeten afspreken over het routeren en adresseren van berichten?
- Wat is de rol van certificaten bij routeren en adresseren

§ 1.3 Welke onderdelen worden besproken

- Berichtenverkeer (bevragingen en meldingen)
- Cloud / SAAS partijen

§ 1.4 Omgeving waar de handreiking voor geldt

Routeren van berichten is nodig als een ontvanger van een bericht meerdere endpoints of knooppunten kent. De ontvanger bezit één of meerdere knooppunten waarop berichten voor de organisatie -en zijn onderdelen- binnenkomen. Op basis van attributen op de envelop – en eventueel de inhoud – van het bericht routeert het knooppunt het bericht naar het juiste endpoint. Een knooppunt kan ook op basis van de kenmerken van de *zender* een bericht routeren naar het juiste endpoint. In beide gevallen maakt de ontvanger gebruik van een routeringstabel.

Organisaties die meerdere berichten-endpoints hebben, kunnen ervoor kiezen om een subOIN aan te maken, om deze endpoints uniek te kunnen identificeren. De zender moet dit subOIN dan gebruiken in het bericht dat wordt verstuurd naar de ontvanger. Een zender kan zelf ook gebruik maken van subOIN's, bijvoorbeeld om een organisatieonderdeel of een door haar beheerde voorziening te identificeren.

Als ontvanger of zender geen gebruik willen maken van subOIN's moet de *afzender* en/of het *adres* van het endpoint uit andere kenmerken van het bericht worden afgeleid.

§ 1.5 Beschrijving van de werking

§ 1.5.1 Het OIN wordt zowel gebruikt voor authenticatie als voor adressering.

- *Hoe werkt dit precies?*

Voor de authenticatie van de zender en de ontvanger in het berichtenverkeer tussen overheidspartijen worden PKIo-certificaten gebruikt. Het PKIo-certificaat wordt zowel gebruikt om het transport van de berichten veilig te laten verlopen (gebruikmakend van het TLS-protocol) als voor authenticatie. Bij het gebruik van Digikoppeling wordt tweezijdige authenticatie vereist. Zender en ontvanger moeten elkaars certificaat vertrouwen en elkaars publieke TLS-sleutel kennen.

Naast het OIN is ook het endpoint van belang. Het endpoint is de URL van de service die benaderd wordt. In Digikoppeling ebMS wordt het endpoint in het CPA vastgelegd. In WUS is dit onderdeel van het WS-addressing deel in de SOAP-header. Voor asynchroon verkeer (ebMS) moet ook de endpoint van de zender bekend zijn. Voor REST API-aanroepen wordt het endpoint in de URL van de HTTP-actie aangegeven.

Adresseren en Routeren vindt plaats op het niveau van de berichtheader. Voor het routeren kan gebruik gemaakt worden van het OIN, het opgegeven endpointadres of beide.

- *Op welke plek wordt het OIN gebruikt?*

Een PKIo-certificaat dat gebruikt wordt voor berichtenuitwisseling met Digikoppeling bevat het OIN van de organisatie of organisatieonderdeel. Dit OIN wordt opgeslagen in het `Subject.SerialNumber` veld van het certificaat.

De Digikoppelingstandaard beschrijft per Profiel – ebMS, WUS of REST API – op welke manier het OIN gebruikt moet worden.

1. ebMS: OIN van zender en ontvanger worden vastgelegd als PartyId in het CPA (berichtencontract). De ebMS-berichtenheader wordt gegenereerd op basis van de CPA.
2. WUS: in de querystring van de endpointuri in de SOAP ws-addressing header.
3. REST API: in de querystring van de HTTP-operatie.

> Zender en ontvanger kunnen hier worden vastgelegd met een "to" en een "from" parameter, dit maakt het mogelijk om ook bij gebruik van intermediairs aan te geven wat de oorspronkelijke afzender - of eindbestemming is . In Bijlage 1 vindt u een uitgebreid voorbeeld.

- *Kunnen er in certificaat en header verschillende OIN's gebruikt worden?*

In het meest eenvoudige geval wisselen organisaties onderling berichten uit zonder tussenkomst van intermediairs of knooppunten. In dat geval is het OIN in het certificaat identiek aan het OIN gebruikt in de berichtenheader.

Indien gebruik wordt gemaakt van knooppunten (of SAAS) zijn er meerdere varianten mogelijk. Het berichtenverkeer van een organisatie die een SAAS-oplossing gebruikt kan gebruikmaken van het certificaat van die SAAS-provider of bij de SAAS-provider een eigen certificaat deponeren, zodat de SAAS-provider het juiste certificaat selecteert als een bericht namens de zender wordt gestuurd.

> De optie om een generiek eigen certificaat bij de SAAS leverancier te deponeren is onwenselijk, immers de SAAS leverancier verkrijgt op deze manier een sleutelbos van certificaten Zie ook : Bijlage 3 : Analyse Knelpunten Routering. Een optie is om te werken met een certificaat met een beperkte specifieke scope op basis van Sub-OIN om risico's te beperken.

Een vergelijkbare situatie treedt op als een bericht naar een knooppunt wordt verstuurd, die het ontvangen bericht doorrouteert naar de uiteindelijke bestemming.

Het OIN dat wordt gebruikt in de berichtenheader kan afwijken van het OIN in het certificaat. In het geval dat een bericht wordt gestuurd naar een knooppunt dat het bericht verder doorstuurt binnen de eigen of een andere organisatie kan dit OIN uit de berichtenheader wordt gebruikt door het knooppunt als middel om het bericht te routeren. Naast routeren op basis van het OIN wordt ook gebruik gemaakt van endpointadressen.

> Bij gebruik van Knooppunten (of SAAS leveranciers) is het van belang de bevoegdheid (en de gegevensverantwoordelijke) te kunnen vaststellen, in Bijlage 3 : Analyse Knelpunten Routering worden de mogelijkheden hiervoor beschreven.

1.5.1.1 Routeringstabel

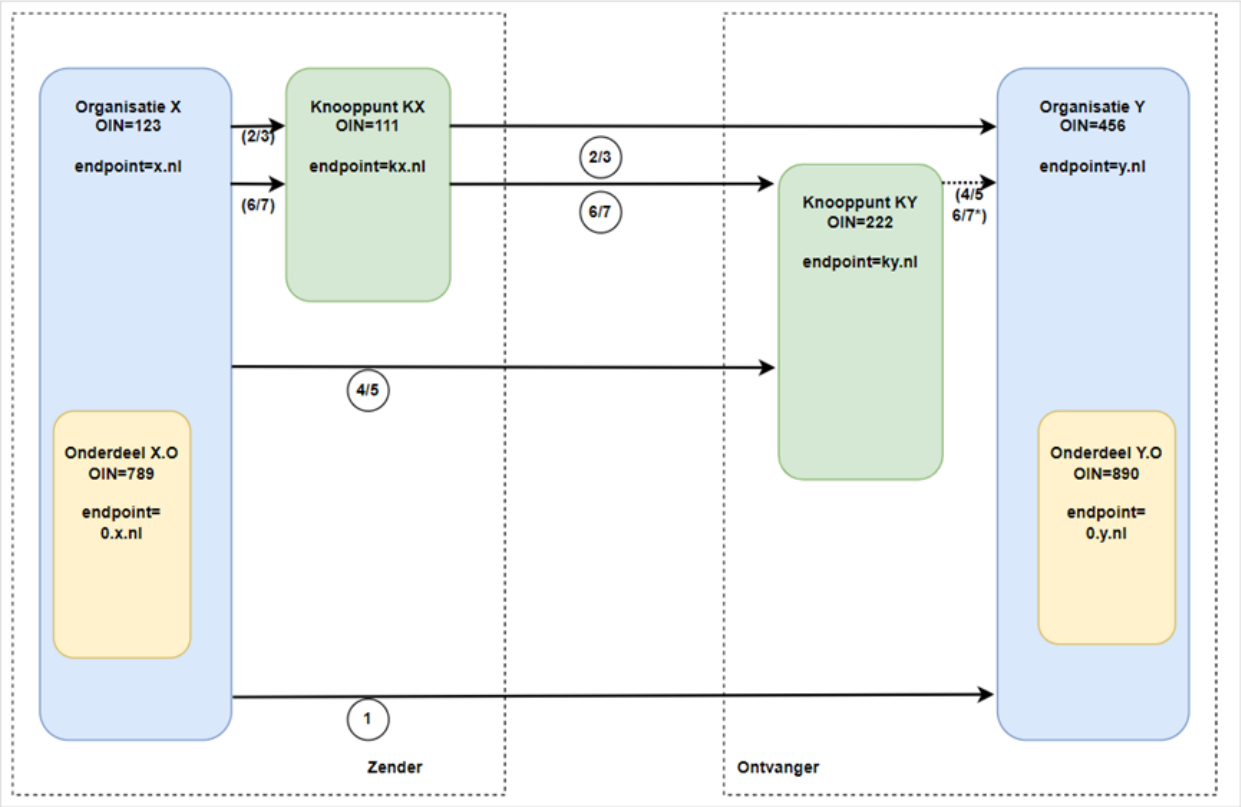
In veel gevallen wordt door het knooppunt een routeringstabel (of mappingtabel) gebruikt. In de tabel wordt beschreven naar welk endpointadres een bericht wordt verstuurd op basis van het TO-adres dat in het bericht is vermeld.

1.5.2 Wanneer is het aan te raden om subOIN's te gebruiken voor adresseren en routeren?

Over het gebruik van subOIN's voor adresseren en routeren bestaan verschillende opvattingen. Sommige organisaties kennen verschillende digitale postbussen van organisatieonderdelen of voorzieningen en gebruiken subOIN's om deze digitale postbussen te identificeren. Andere organisaties willen het gebruik van OIN reserveren om Organisaties te identificeren en gebruiken voor het routeren van berichten binnen de organisatie ander kenmerken van het bericht. Het OIN-stelsel maakt het eenvoudiger om subOIN's aan te maken, maar legt de partijen geen verplicht patroon op hoe subOIN's gebruikt kunnen worden ten behoeve van adresseren en routeren. Partijen die met elkaar berichten uitwisselen zullen over het gebruik van subOIN's onderling afspraken moeten maken.

1.5.3 Wat zijn de regels die partijen met elkaar moeten afspreken over het routeren en adresseren van berichten?

In deze handreiking zijn hieronder een aantal scenario's uitgewerkt: (zie ook bijlage 1).



Figuur 1 Scenario's

		(Sub)OIN	(Sub)OIN	(Sub)OIN	(Sub)OIN
Nr	Type	Verzender	Knooppunt A	Knooppunt B	Ontvanger
			*1	*2	
1	Direct	123			456
2	Via alleen A (eigen OIN A)	123	111	nvt	456
3	Via alleen A (A gebruikt OIN verzender)	123	123	nvt	456
4	Via alleen B (eigen OIN B)	123	nvt	222	456
5	Via alleen B (B gebruikt OIN ontvanger)	123	nvt	456	456
6	Via A-B (eigen OIN A,B)	123	111	222	456
7	Via A-B (gebruikt OIN verzender, ontvanger)	123	123	456	456

*1 Knooppunt A verzendt 'namens' verzender

*2 Knooppunt B ontvangt 'namens' ontvanger

§ *1.5.3.1 (Nr 1) Direct*

In deze situatie gebruikt de verzender het eigen (Sub)OIN als afzender en het (Sub)OIN van de ontvanger als bestemming. Identificatie en Authenticatie geschiedt op basis van de beide TLS-certificaten. Signing en encryptie kan gebruikt worden voor end-to-end beveiliging.

§ *1.5.3.2 (Nr 2) Via Knooppunt A (waarbij eigen OIN van A gebruikt wordt voor TLS-verbindingen met verzender en ontvanger)*

In deze situatie verloopt de communicatie via een knooppunt A.

Wanneer A een SAAS-partij is, is een aandachtspunt bij de communicatie van verzender naar de SAAS-partij de beveiliging van dit traject (wanneer dit niet via Digikoppeling loopt).

Bij de communicatie van SAAS-partij naar ontvanger zijn de afspraken rond machtiging relevant. In deze situatie gebruikt de SAAS-partij het eigen OIN in het TLS-certificaat. De ontvanger zal dit moeten accepteren en de oorspronkelijke verzender afleiden uit de afspraken, de bericht header of inhoud of op basis van end-to-end signing met een signingcertificaat van de verzender.

§ *1.5.3.3 (Nr 3) Via Knooppunt A (waarbij A (Sub)OIN van verzender gebruikt voor TLS-verbindingen met ontvanger)*

In deze situatie wordt een knooppunt (bijv. SAAS-partij) gemachtigd om namens verzender te communiceren door het verstrekken van een certificaat van de verzender aan deze partij. De verzender kan dit certificaat intrekken wanneer het knooppunt niet langer is toegestaan om dit te gebruiken. Aandachtspunt is het certificaat d.m.v. subOIN fijnmazig te definiëren om misbruik uit te sluiten.

§ *1.5.3.4 (Nr 4) Via Knooppunt B (waarbij B eigen OIN van B gebruikt voor TLS-verbindingen met verzender)*

In deze situatie is B gemachtigd om berichten te ontvangen en door te geven aan ontvanger;

Hierbij gelden vergelijkbare aandachtspunten als bij punt 2.

§ *1.5.3.5 (Nr 5) Via Knooppunt B (waarbij B (Sub)OIN van ontvanger gebruikt voor TLS-verbindingen met verzender)*

In deze situatie wordt een knooppunt (bijv. SAAS-partij) gemachtigd om namens ontvanger te communiceren door het verstrekken van een certificaat van de ontvanger aan deze partij.

Hierbij gelden vergelijkbare aandachtspunten als bij punt 3.

§ *1.5.3.6 (Nr 6) Via Knooppunt A en B (met gebruik van eigen OIN A,B voor TLS verbindingen)*

A en B maken verbinding via het eigen TLS-certificaat. Aandachtspunt is daarom het machtigen van deze partijen om te acteren in de keten. Routering kan op basis van afspraken, de berichtheader of berichtinhoud of op basis van end-to-end signing met een signing certificaat van de verzender/ontvanger. Specifiek is dat ook Knooppunt A en B elkaar moeten 'vertrouwen' in de communicatie.

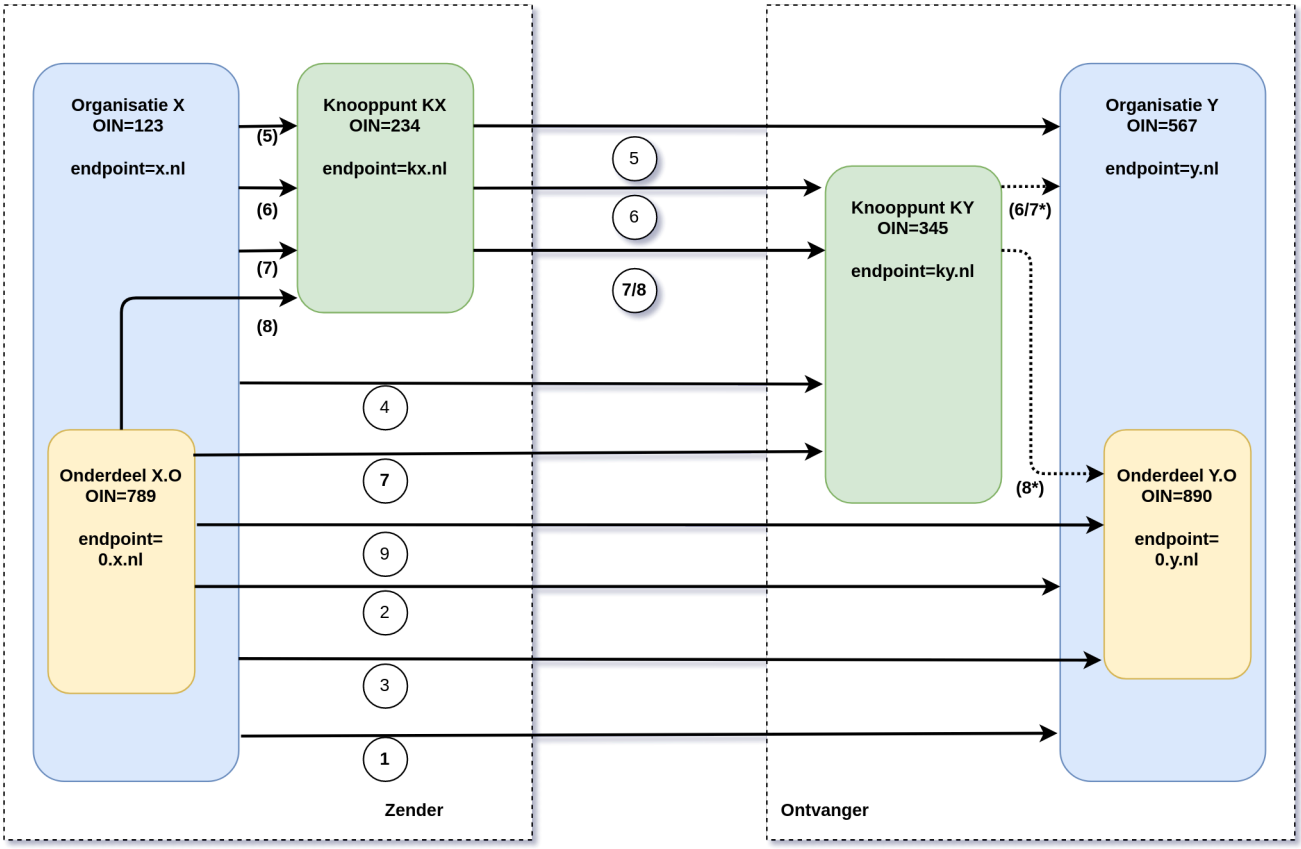
1.5.3.7 (Nr 7) Via Knooppunt A en B (met gebruik van OIN verzender, ontvanger voor TLS verbindingen)

In deze situatie worden knooppunten (bijv. SAAS-partijen) gemachtigd om namens ontvanger te communiceren door het verstrekken van een certificaat van de ontvanger aan deze partij. Hierbij gelden vergelijkbare aandachtspunten als bij punt 3.

1.6 Bijlage 1. Voorbeeld van routering

In deze handreiking hebben we een aantal scenario's uitgewerkt. De scenario's zijn hier in detail uitgewerkt.

1.6.1 Voorbeeldsituatie: zowel zender als ontvanger maken gebruik van subOIN's



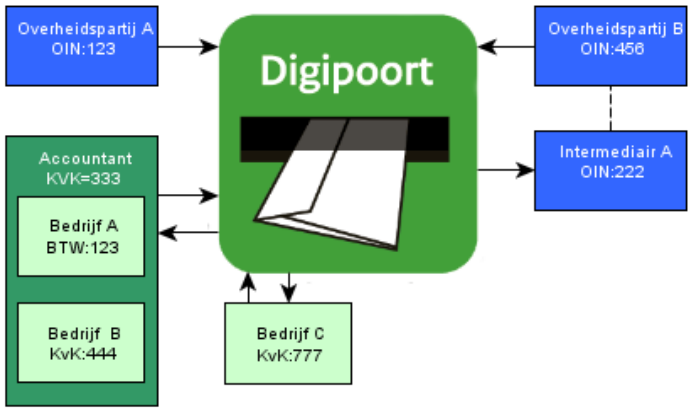
Figuur 2 Adressering

1	Zendende Partij	Ontvangende Partij	Via	OIN in Certificaat Zender (tbv TLS)	OIN in Certificaat Ontvanger (tbv TLS)	OIN in HEADER FROM	OIN in HEADER TO	Endpoint Zender	Endpoint Ontvanger
1	Organisatie X	Organisatie Y		123	567	123	567	x.nl	y.nl
2	Organisatie Onderdeel	Organisatie Y		123 of 789	567	789	567	o.x.nl	y.nl

1	Zendende Partij	Ontvangende Partij	Via	OIN in Certificaat Zender (tbv TLS)	OIN in Certificaat Ontvanger (tbv TLS)	OIN in HEADER FROM	OIN in HEADER TO	Endpoint Zender	Endpoint Ontvanger
	X.O								
3	Organisatie X	Organisatie Onderdeel Y.O		123	567 of 890	123	890	x.nl	o.y.nl
4	Organisatie X	Organisatie Y	Knooppunt Y	123	567 of 345	123	567 of 345	x.nl	y.nl of ky.nl
5	Organisatie X	Organisatie Y	Knooppunt X	123 of 234	567	123	567	kx.nl	y.nl
6	Organisatie X	Organisatie Y	Knooppunt X en Knooppunt Y	12of 2343	567 of 345	123	567	kx.nl	ky.nl
7	Organisatie Onderdeel X.O	Organisatie Y	Knooppunt X en Knooppunt Y	123 of 789 of 234	567 of 345	789	567	o.kx.nl	ky.nl
8	Organisatie Onderdeel X.O	Organisatie Onderdeel Y.O	Knooppunt X en Knooppunt Y	123 of 789, of 234	567, of 345, of 890	789	890	o.kx.nl	o.y.nl
9	Organisatie Onderdeel X.O	Organisatie Onderdeel Y.O		123 of 789	567, of 890	789	890	o.x.nl	o.y.nl

§ 1.7 BIJLAGE 2. Digipoort

Digipoort -- Routeermechanisme (vereenvoudigd)



Figuur 3 Digipoort

Routeertabel

naam	identiteit	berichtsoort	intermediair	endpoint ontvanger
Overheidspartij A	OIN:123	factuur		oA.nl
Overheidspartij B	OIN:456	factuur	OIN: 222	
Intermediair A	OIN:222	factuur		ia.nl
Accountant	KvK:333	order		x@ac.nl
Bedrijf A	BTW:123	order	KvK:333	
Bedrijf B	KvK:444	order	KvK:333	
Bedrijf C	KvK:777	order		bC.nl

OIN matrix (al het verkeer loopt over Digipoort)

#	Zendende	Ontvan-gende	Bericht	ID in PKIo Zender è Digipoort	ID in PKIo Ontvanger ç Digipoort	ID Belang-hebbende (bericht)	ID Ont-vanger (bericht)	Endpoint	Endpoint
Partij	Partij	type	Zender	Ontvanger					
1	OIN:123	BTW:123	order	OIN:123	KvK:333	OIN:123	BTW:123	oA.nl	x@ac.nl
2	BTW:123	OIN:123	factuur	KvK:333	OIN:123	BTW:123	OIN:123	x@ac.nl	oA.nl
3	OIN:456	KvK:444	order	OIN:456	KVK:333	OIN:123	KvK:444	oB.nl	x@ac.nl
4	KvK:444	OIN:456	factuur	KvK:333	OIN:222	KvK:444	OIN:456	x@ac.nl	ia.nl
5	OIN:123	KvK:777	order	OIN:123	KvK:777	OIN:123	KvK:777	oA.nl	bC.nl
6	KvK:777	OIN:123	factuur	KvK:777	OIN:123	KvK:777	OIN:123	bC.nl	oA.nl

Aandachtspunten:

- Het OIN in een certificaat is niet relevant voor TLS. Alleen de trustconfiguratie speelt een rol.
- Een Organisatie Onderdeel is een uniek te identificeren systeem binnen de organisatie.

§ 1.8 BIJLAGE 3. Analyse knelpunten Routering en Intermediairs

§ 1.8.1 Introductie

Het is binnen overheidsketens steeds gebruikelijker om gebruik te maken van dienstverlening vanuit de Cloud, en diensten af te nemen van SAAS leveranciers. Dit heeft impact op vragen als wat is het endpoint in een keten, wie is de oorspronkelijker aanbieder of uiteindelijke ontvanger, hoe herken ik die en hoe weet ik dit zeker. Digikoppeling biedt met signing en encryptie tools aan, sommige sectoren hebben voorzieningen ontwikkeld, die bovenstaande vragen deels beantwoorden, andere partijen zijn zoekende hoe om te gaan met de nieuwe situatie.

Dit document gaat in op de knelpunten en oplossingsrichtingen m.b.t. routering.

1.8.2 Intermediairs & SAAS

1.8.2.1 Definitie Intermediair

*Een intermediair is een organisatie **die tussen twee (of meer) partijen berichten via Digikoppeling ontvangt en routeert**. Een intermediair kan dienen als sectoraal knooppunt, waarbij de intermediair meerdere partijen in een samenwerkingsverband ontzorgt en ondersteunt.*

Een intermediair vormt een schakel in de Digikoppeling-keten tussen serviceaanbieder en serviceafnemer:

- *Een transparante intermediair stuurt berichten door naar het eindpunt (ontvanger) zonder de berichten te bewerken. Een transparante intermediair is zelf dus geen eindpunt in Digikoppeling (1). Het versleutelen van berichtinhoud (berichtenniveau versleuteling) kan worden toegepast indien de intermediair niet vertrouwd wordt.*
- *Een niet-transparante intermediair (b.v. een sectoraal knooppunt) bewerkt berichten en is dus een eindpunt binnen Digikoppeling.*

(1): We beschouwen transparantie hier op de logistieke laag. Op technisch niveau is de intermediair een eindpunt omdat de TLS verbinding tussen twee servers moet worden opgezet.

Bron: Digikoppeling Architectuur 2.0

1.8.2.2 Definitie van SAAS

***Software as a service**, vaak afgekort als **SaaS**, ook weleens **software on demand** genoemd, is software die als een online dienst wordt aangeboden. De klant hoeft de software niet aan te schaffen, maar sluit bijvoorbeeld een contract per maand per gebruiker af, eventueel in combinatie met andere parameters. De SaaS-aanbieder zorgt voor installatie, onderhoud en beheer, de gebruiker benadert de software over het internet bij de SaaS-aanbieder.*

Kenmerken:

- *De klant hoeft de software en de daarvoor benodigde hardware niet aan te schaffen, maar betaalt slechts voor het gebruik ervan.*
- *De software en hardware wordt niet bij de klant geïnstalleerd, maar bij de ASP / SaaS-aanbieder. De klant heeft toegang tot de software via internet of een privénetwerk.*

1.8.3 Identificatie van organisaties met OIN

Het OIN (Organisatie Identificatie Nummer) wordt gebruikt om organisaties te identificeren (zie ook OIN Stelsel Het SubOIN is een afgeleide van het OIN en is opgesteld volgens de OIN-nummersystematiek en wordt gebruikt voor een organisatieonderdeel, samenwerkingsverband of voorziening. SubOIN's kunnen worden gebruikt om fijnmazig te identificeren. (Aan een OIN kunnen meerdere SubOIN's gekoppeld worden).

1.8.4 Knelpunten

Knelpunten bij gebruik van intermediairs / SAAS oplossingen zijn:

- Hoe herken je de oorspronkelijke afzender
- Hoe adresseer je de uiteindelijk bestemming
- Hoe regel je identificatie en authenticatie van partijen in een keten

1.8.5 Oplossingen

1.8.5.1 (1) Bevoegdheid intermediair via afspraken

Figuur 4 Intermediair

Een intermediair in de rol van 'knooppunt' krijgt de bevoegdheid om dienst van B af te nemen (op basis van of passend in toepasselijke regelgeving). Voor B blijft achterliggende partij A buiten beeld. Of A bevoegd is om de dienst via de Intermediair af te nemen bepaalt de Intermediair op basis van de regelgeving en verantwoordelijkheid;
(een voorbeeld is een sector loket)

(Bron: Digikoppeling Identificatie en Authenticatie 1.4.2)

1.8.5.2 (2) Bevoegdheid intermediair/SAAS partij door verlenen certificaat

Organisatie A geeft een certificaat aan de SAAS partij waarmee de SAAS partij zich naar buiten toe identificeert als A. Voor partij B is het dan alsof deze direct met A communiceert

Aandachtspunt:

In de gevallen waarbij certificaten (van A) aan een SAAS leverancier worden afgegeven is dit de manier waarop de SAAS leverancier gemachtigd wordt om namens A te acteren;

Nadeel van deze manier van werken is dat de SAAS leverancier over een 'sleutelbos' van certificaten gaat beschikken wanneer de diensten aan meerdere partijen worden aangeboden.

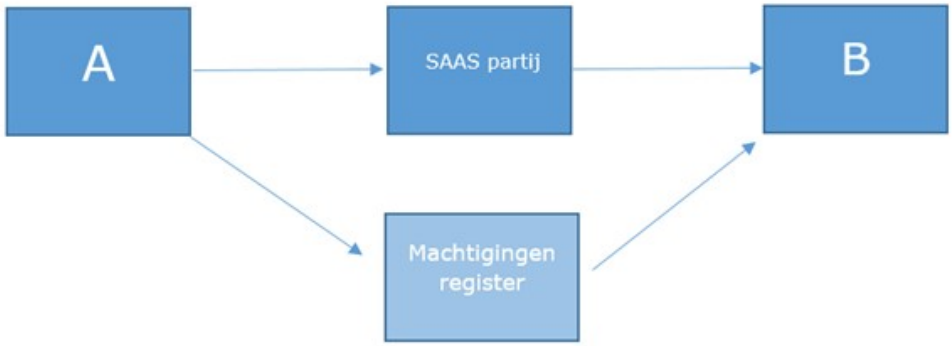
(Dit vraagt om specifieke aandacht voor certificaatbeheer en beveiligingsaspecten / mogelijk misbruik, denk hierbij bv aan het intrekken van een machtiging)

§ *1.8.5.3 (3) Bevoegdheid intermediair/SAAS partij door 'machtigen'*

3a. In dit geval acteert de SAAS partij onder het eigen OIN / SubOIN, Voor partij B is het duidelijk dat zij communiceren met de SAAS partij. Onderlinge afspraken bepalen of de SAAS partij gemachtigd is om namens A bepaalde diensten te gebruiken;

3b. Gebruik van een machtigingen register

De SAAS partij identificeert zich met het eigen OIN / SubOIN. In het machtigingen register kan worden nagegaan of de SAAS partij geautoriseerd is om bepaalde diensten namens een organisatie te verrichten.



Figuur 5 Machtigen

§ 2. Lijst met figuren

↥