



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Digikoppeling Architectuur

Versie 1.2

Datum 2 april 2010
Status Definitief

Colofon

Projectnaam	Digikoppeling
Versienummer	Definitief
Organisatie	Servicecentrum Logius Postbus 96810 2509 JE Den Haag T 0900 555 4555 (10 ct p/m) servicecentrum@logius.nl
Bijlage(n)	0

Inhoud

Colofon	2
Inhoud	3
Inleiding	5
1.1 Doel en doelgroep	5
1.2 Opbouw van dit document	5
2 Positionering Digikoppeling	6
2.1 Wat is Digikoppeling volgens de NORA?	6
2.1.1 Positionering Digikoppeling in de NORA	7
2.1.2 Resulterende scope m.b.t. aan te sluiten soorten services/diensten	8
2.2 Stelsel van bussen	8
2.2.1 Welke organisaties sluiten aan: resulterende scope	8
2.3 Uitwisselingslagen	9
2.3.1 Basisfuncties en rijkere functies	10
2.3.2 Scope dunne bus	11
3 Eisen aan Digikoppeling	12
3.1 Gewenste functionaliteiten van de dunne bus	12
3.2 Gewenste interactievormen	12
3.2.1 Scope: Interactievormen Digikoppeling versie 1	14
3.3 Security (vertrouwelijkheid en integriteit)	15
4 Standaarden	16
4.1 Waarom standaardisatie	16
4.2 Families van standaarden: WUS en ebMS	16
5 Inrichting van de servicebus	18
5.1 Mapping functionaliteit op componenten	18
5.2 Dunne bus	19
5.3 Dikke bus	21
6 Basisinrichting van Digikoppeling	23
6.1 Inleiding	23
6.2 Digikoppeling Koppelvlakstandaarden	23
6.2.1 Koppelvlakstandaarden WUS en ebMS	23
6.2.2 Compliancevoorzieningen	24

6.3	<i>Digikoppeling Service Register</i>	24
6.3.1	Digikoppeling Service Register: inhoud.....	24
6.4	<i>Adapters, Gateway en bedrijfseigen broker</i>	25
6.4.1	Organisaties met een eigen broker.....	26
6.4.2	Organisaties met een gateway.....	26
6.5	<i>Overzicht Digikoppeling compleet</i>	27
6.6	<i>Productie en test</i>	27
6.7	<i>Relatie met transport (Diginetwerk)</i>	28
7	Dwarsverbanden	29
7.1	<i>Inleiding</i>	29
7.2	<i>Authenticatie, identiteit en autorisatie</i>	29
7.3	<i>Versleuteling</i>	30
7.4	<i>Adressering en routing</i>	30
7.5	<i>Service Register</i>	31
7.6	<i>Berichtidentificatie</i>	31
7.7	<i>Karakterset en Codering</i>	31
	Bijlage: Gateway	32

Inleiding

1.1 Doel en doelgroep

Dit document beschrijft de achtergronden, de scope en de resulterende inrichting van de Digikoppeling (voorheen Overheidsservicebus). Ofwel: het waarom, wat en hoe van Digikoppeling.

Deze beschrijving van de architectuur betreft de eerste operationele versie van Digikoppeling, genaamd 'Digikoppeling versie 1.0'. Een doorgroei naar versies met meer functionaliteit, dus Digikoppeling versie 2, 3 et cetera, is voorzien.

Dit document is bedoeld voor architecten en ontwerpers die zijn betrokken bij de e-overheid of onderdelen daarvan.

1.2 Opbouw van dit document

- Hoofdstuk 2 gaat in op de basis, het 'waarom' van Digikoppeling zoals beschreven in de Nederlandse Overheid Referentie Architectuur (NORA), het stelsel van servicebussen en de te onderkennen lagen in de architectuur van berichtenuitwisseling. Dit bepaalt de scope van Digikoppeling.
- Hoofdstuk 3 beschrijft de belangrijkste eisen die, gegeven de scope, aan Digikoppeling worden gesteld. Hierin staan ook de noodzakelijke interactievormen beschreven.
- Hoofdstuk 4 gaat in op de internationale standaarden die relevant zijn voor Digikoppeling en de keuzes die daarin zijn gemaakt.
- Hoofdstuk 5 beschrijft de hoofdlijnen van de inrichting van Digikoppeling.
- Hoofdstuk 6 gaat dieper in op de daarbij onderkende componenten.
- Hoofdstuk 7 beschrijft de 'dwarsverbanden', dat wil zeggen de belangrijkste functionele afspraken ten aanzien van identiteit & authenticatie, adressering et cetera, die gelden voor Digikoppeling.

2 Positionering Digikoppeling

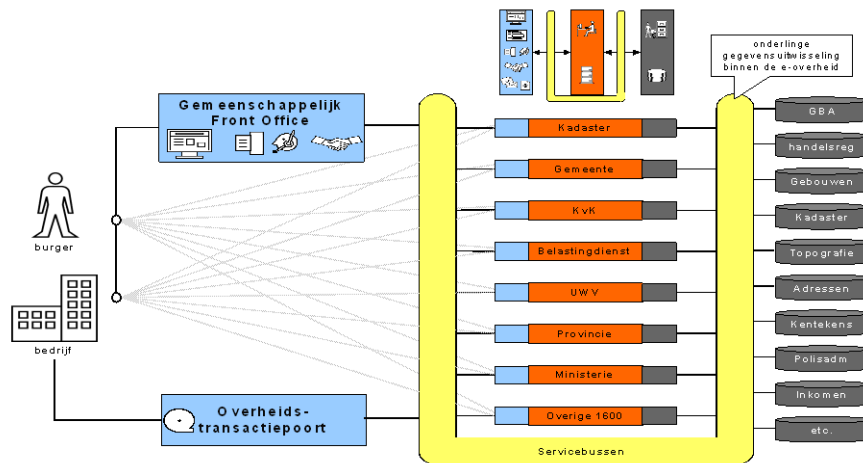
Digikoppeling is een essentieel onderdeel van de e-overheid zoals beschreven in de NORA. Dit hoofdstuk beschrijft de algemene kenmerken van Digikoppeling, ook zoals beschreven in en voortvloeiend uit de NORA. Hier vindt u ook de nadere uitwerking daarvan in het stelsel van bussen en in de te onderscheiden communicatielagen. Dit hoofdstuk beschrijft de positionering, de scope en afbakening van Digikoppeling: ' wat is Digikoppeling wel en wat niet'.

2.1 **Wat is Digikoppeling volgens de NORA?**

In de NORA is op verschillende plaatsen (NORA 2.0 § 4.3.2, § 6.3, Bijlage B) een aantal kernpunten opgenomen, dat bepalend is voor Digikoppeling. Hieronder volgt een samenvatting van die kernpunten:

- Een Servicegerichte Architectuur is gebaseerd op samenwerken door gebruik te maken van services. Dat wil zeggen: de ene organisatie biedt services aan die een andere organisatie afneemt om samen de uiteindelijk gewenste dienstverlening te bieden.
- Gebruik van een service is gebaseerd op het uitwisselen van berichten.
- De minimale hoofdtaak van een servicebus is het bieden van een uitwisselingsmedium tussen serviceaanbieders en serviceafnemers.
- Die bus kan zelf ook rijkere functies bieden, maar dat hoeft niet. Ook als er geen functies (soms ook wel ook services genoemd) 'in de bus' zitten, is er sprake van een servicebus.
- Berichten worden uitgewisseld tussen applicaties. Er is sprake van Application-to-Application verkeer (A2A), en niet van Person-to-Application (P2A).
- Digikoppeling moet verschillende organisaties en technisch verschillende omgevingen koppelen, en dus volledig onafhankelijk zijn van implementaties van bepaalde leveranciers. Dit principe wordt vaak aangeduid met Business-to-Business (B2B); het geeft een belangrijk verschil aan met een Enterprise ServiceBus, die in het algemeen weliswaar Open Standaarden ondersteunt, maar ook veel leveranciersgebonden functies kent.

2.1.1 Positionering Digikoppeling in de NORA



Figuur 1 - E-overheid in NORA

Bovenstaande figuur uit de NORA schetst de hoofdcomponenten van de e-overheid. In dit figuur is op hoofdlijnen de inrichting van de e-overheid weergegeven:

- Burgers en bedrijven communiceren met de overheid via een aantal "poortcomponenten":
 - Digipoort, bedoeld voor massale, structurele stromen tussen bedrijven en overheidsorganisaties.
 - Portals, bedoeld voor de meer adhoc e-dienstverlening (via internet) van de overheid aan burgers en bedrijven.
 - Contactcentrum (callcenter) bedoeld voor de dienstverlening via het telefoonkanaal.
- De overheidsorganisaties (tussen de 1600 en 2500 in aantal) zijn ieder opgebouwd uit een:
 - Multichannel frontoffice (vestiging, post, telefoon en internet).
 - Verwerkingsdeel (backoffice).
 - Gegevensregistraties.
- Basisregistraties: registraties waarvoor één of meer overheidsorganisaties verantwoordelijk zijn, die aan bijzondere (wettelijke) eisen voldoen en daardoor een bijzondere status hebben.
- Servicebus(sen), bedoeld voor de onderlinge gegevensuitwisseling tussen overheidsorganisaties onderling, met basisregistraties en de koppeling aan de gemeenschappelijke frontoffice, ofwel de poortvoorzieningen.

NORA zegt over service: Een service is het resultaat van een afgeronde inspanning die een ambtenaar of applicatie op basis van wettelijke taken of onderling gemaakte afspraken levert en waarmee in een behoefte van een of meer andere ambtenaren of applicaties wordt voorzien.

Op Digikoppeling beperken we ons tot het geautomatiseerde, dus (ICT-) deel, dat wil zeggen een afgeronde inspanning die een applicatie levert voor een of meer andere applicaties. Een dergelijke 'afgeronde ICT-

inspanning', beschikbaar gesteld door een applicatie op basis van SOAP, wordt een webservice genoemd. De servicebus regelt het verkeer tussen webservices.

Omdat het gaat om (technische) webservices, wordt in dit document verder niet meer gesproken van serviceaanbieders of serviceafnemers, maar van 'serviceproviders' en 'servicerequesters'.

2.1.2 Resulterende scope m.b.t. aan te sluiten soorten services/diensten
Digikoppeling richt zich op de afspraken/standaards betreffende het verkeer tussen servicerequester en serviceprovider en maakt geen onderscheid naar het soort dienst.

2.2 Stelsel van bussen

In NORA 2.0 paragraaf 6.5 zijn de principes en uitgangspunten t.a.v. een stelsel van servicebussen neergelegd. Hieruit twee citaten:

NORA 2.0, paragraaf 6.5:

In plaats van één servicebus voor al het organisatieoverstijgende verkeer binnen de overheid zal er sprake zijn van een gelaagd en geschakeld stelsel van servicebussen. Specifieke servicebussen ondersteunen het verkeer binnen ketens, domeinen of sectoren van overheidsorganisaties. Centraal daartussen staat een Digikoppeling. Op deze Digikoppeling zijn zowel rechtstreeks bepaalde organisaties en services aangesloten, maar zij verbindt ook deze specifiekere gemeenschappen. Deze gemeenschappen zijn immers geen eilanden; zij bieden sommige van hun services ook buiten hun gemeenschap aan en omgekeerd.

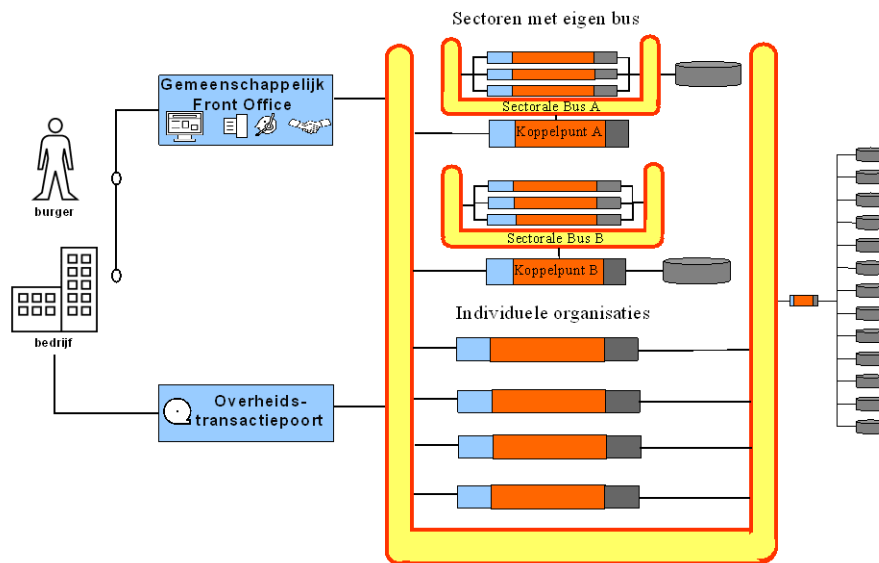
Het betreffende principe in die paragraaf luidt:

6.5.2	e-overheids principe	P19	Koppelingen tussen verschillende sectorale servicebussen lopen altijd via Digikoppeling.
Koppeling tussen twee servicebussen wordt gerealiseerd door ze beide te koppelen aan Digikoppeling, tenzij er duidelijke redenen zijn om hiervan af te wijken.			

2.2.1 Welke organisaties sluiten aan: resulterende scope

Versie 1 van Digikoppeling richt zich alleen op uitwisseling tussen overheidsorganisaties. Dit zal later worden uitgebreid naar inrichting voor alle organisaties met een publieke taak.

Omdat er zoets als een stelsel van bussen bestaat, kunnen overheidsorganisaties niet altijd direct op Digikoppeling koppelen. Dat kan ook via een sectorale bus en een zogenaamd koppelpunt of aanspreekpunt gebeuren.



Figuur 2 - Stelsel van servicebussen

2.3 Uitwisselingslagen

Berichten over Digikoppeling worden, zoals we al eerder vermeldden, uitgewisseld tussen twee applicaties. De ene communicatiepartner stelt zich op als servicerequester en de andere als serviceprovider.

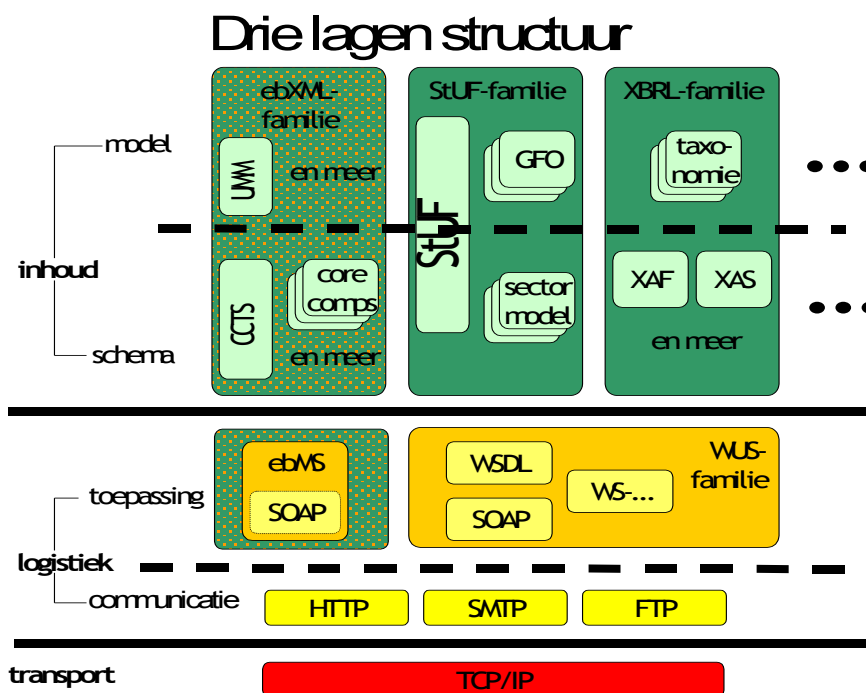
Bij het uitwisselen van berichten tussen applicaties zijn drie hoofdlagen te onderscheiden¹:

- **Inhoud** (payload): de laag waarin de berichtinhoud wordt gespecificeerd en uitgewisseld. Deze laag delen we op in:
 - Model: de laag waar de berichtinhoud wordt gespecificeerd (onafhankelijk van het uitwisselformaat, zoals XML).
 - Schema: de laag waar de gegevensinhoud vorm heeft gekregen in een specifiek formaat, zoals een XML-schema.
- **Logistiek** (envelop): de laag van de interface waarin, zonder gebruik te maken van de berichtinhoud, de afhandeling van berichtenstromen wordt geregeld, zoals routing, adressering, vraag/antwoord koppeling et cetera. Deze logistieke laag delen we op in:
 - **Communicatie**: in deze laag bevinden zich de standaarden als HTTP, SMTP etc. Deze zijn gepositioneerd in de applicationlaag (laag 5) van de TCP/IP stack. Vanwege dit 'applicatiekarakter' is deze communicatiesublaag in de logistieke laag getrokken.
 - Toepassing: in deze laag bevinden zich de afspraken die daadwerkelijk de (logistieke) afhandeling regelen, onder te verdelen in:
 - basisfuncties: adressering/routing, beveiliging en betrouwbaarheid.

¹ Zie eindrapport COMBI

- rijkere logistieke functies, zoals abonnementenadministratie, content-based routing of choreografie.
- **Transport:** de laag van het interface die ervoor zorgt dat een bericht technisch wordt overgebracht van de ene naar de andere locatie. In termen van de 'TCP/IP stack' de lagen 4 (Transport, TCP), 3 (Network, IP etc) en lager.

Onderstaande figuur geeft deze lagen weer. Ter illustratie is een aantal namen van bekende standaarden, onderverdeeld naar relevante families, in deze figuur geplaatst.



Figuur 3 - Ingevulde lagenstructuur communicatie

Belangrijk is, dat de lagen onderling in hoge mate zijn ontkoppeld. Een bepaalde 'inhoud', de payload, moet (afhankelijk van de afspraken die daarover gemaakt zijn) op een bepaalde wijze gemodelleerd en in een schema gegoten kunnen worden. De keuzes die daarbij gemaakt zijn, mogen geen invloed hebben op de keuzes die in de logistieke laag gemaakt worden en omgekeerd. De keuzes in de logistieke laag hebben geen invloed op de wijze waarop de transportlaag is ingericht, bijvoorbeeld transport over internet of eigen verbindingen.

Digikoppeling is een set van afspraken en gemeenschappelijke voorzieningen die de implementatie van de logistieke laag vormt.

2.3.1

Basisfuncties en rijkere functies

Zie ook NORA Bijlage B.

In de logistieke laag is een veelheid van functies te onderkennen. Er kan onderscheid gemaakt worden naar bovengenoemde basisfuncties (adressering/routing, beveiliging, betrouwbaarheid en vindbaarheid) en

rijkere functies (abonnementenadministratie, content-based routing of choreografie).

De basisfuncties zijn die functies, die noodzakelijk zijn om berichtenuitwisseling veilig en betrouwbaar uit te voeren.

2.3.2

Scope dunne bus

Versie 1 van Digikoppeling is beperkt tot deze basisfuncties. Een bus die (vrijwel) alleen die basisset omvat wordt een dunne bus genoemd. Dit in tegenstelling tot een dikke bus, die ook bovengenoemde rijkere functies bevat.

Versie 1 van Digikoppeling is dus een dunne bus, die de basisfuncties adressering/routing, beveiliging en betrouwbaarheid en vindbaarheid ondersteunt.

3 Eisen aan Digikoppeling

3.1 Gewenste functionaliteiten van de dunne bus

In de vorige paragrafen is de scope bepaald van Digikoppeling Versie 1. Binnen dat kader zijn eisen geformuleerd en vastgesteld. Deze eisen betreffen de volgende gebieden:

- Communicatie (de invulling van de in 2.3 genoemde sublaag communicatie) - aspecten zijn Messaging en Protocol.
- Adressering en routing.
- Interactiepatronen (message exchange patterns).
- Betrouwbaarheid en beschikbaarheid (reliable messaging): garandeert dat een bericht met zekerheid slechts één keer wordt afgeleverd en dat berichten in de juiste volgorde worden afgeleverd, ook als de partner tijdelijk niet beschikbaar is.
- Beveiliging (security): zorgt voor vertrouwelijkheid, authenticatie, integriteit en onweerlegbaarheid van berichten.
- Vindbaarheid (description en directory).
- Non-functional: leveranciersafhankelijk - Digikoppeling maakt zo veel mogelijk gebruik van leveranciersafhankelijke interoperabele open standaarden. Dit is nodig om een 'vendor lock-in' te voorkomen.
- Geen maatwerk: de functionaliteit wordt zoveel mogelijk geïmplementeerd met gebruikmaking van op de markt beschikbare software.
- Enkelvoudig koppelpunt. De aanwezigheid van slechts één (logistiek) koppelpunt tussen de organisatie en externe services (bijv. gegevensbronnen) van andere organisaties is wenselijk.

Een belangrijk punt, waar veel aandacht aan moet worden besteed, betreft de mogelijkheden voor aansluiting op Digikoppeling. Hoewel dat een aspect 'achter de voordeur' van aansluitende organisaties is, blijkt dat aspect een zeer belangrijke rol te spelen bij de implementatie van Digikoppeling en dus bij de acceptatie van Digikoppeling. Daarom is dat aspect hier bij de eisen opgenomen. De uitwerking en de gekozen oplossing is niet opgenomen in het hoofddocument, maar beschreven in bijlage A. Die oplossing is optioneel, dat wil zeggen dat een organisatie er wel of niet voor kan kiezen.

Een aantal van de geformuleerde eisen is eerst nader uitgewerkt. Vervolgens zijn in hoofdstuk 5 en 6 de resulterende inrichtingskeuzes beschreven.

Uitwerkingseisen:

- De gewenste interactievormen, met per interactievorm de eisen aan beschikbaarheid en betrouwbaarheid, is beschreven in paragraaf 3.2
- Security is nader beschreven in paragraaf 3.3.
- De leveranciers-onafhankelijke open standaarden die op de markt beschikbaar zijn, staan beschreven in hoofdstuk 4.

3.2 Gewenste interactievormen

Applicaties werken op verschillende manieren interactief met elkaar. Bij een bepaalde wijze van interactief werken horen bepaalde kenmerken. Die kenmerken vereisen weer een bepaalde ondersteuning door de logistieke laag, en daarom bepaalde invullingen van en afspraken over de

functionaliteit van de bus. Het is dus noodzakelijk om goed inzicht te hebben in de interactievormen² op de businesslaag om zo de eisen aan de logistieke laag scherp te krijgen.

Op de businesslaag (paragraaf 2.3) kunnen we de volgende vormen en afspraken tussen 'business-services' van verschillende organisaties onderkennen³. De serviceaanbieder levert als dienst:

- alleen informatie, die bevroegd kan worden. Dit heeft geen impact op de aanbiedende organisatie;
- het verwerken van een gevraagde transactie. Dit heeft wel impact op de aanbiedende organisatie.

Naast deze impact op de serviceverlenende organisatie kunnen we ook onderscheid maken naar de procesinrichting:

- (het proces en) de applicatie van de afnemer wacht op een 'onmiddellijk' antwoord (synchrone proceskoppeling; de afnemer houdt de context vast en weet dus direct waar het antwoord op slaat).
- het resultaat is uitgesteld / komt enige tijd later (asynchroon; de applicatie moet dan het antwoord bij de vraag zoeken) of wellicht helemaal niet. De applicatie of het businessproces wacht niet.

Op basis van deze twee verschillen komen we tot vier primitieve businessinteracties, weergegeven in onderstaande tabel.

	Onmiddellijk	Uitgesteld
Bevraging	Onmiddellijke businessbevraging	Businessbevraging met uitstel
Transactie	Onmiddellijke businesstransactie	Businesstransactie met uitstel

Deze businessafspraken worden geïmplementeerd in (bedrijfs)applicaties.

- Logistiek: de eis die aan de logistieke laag gesteld wordt, is het ondersteunen van de mogelijkheden die gevraagd worden vanuit de (business)applicatie. Die ondersteuning wordt geleverd door twee logistieke basispatronen:
 - Een vraag/antwoord bericht bedoeld voor de situatie waarbij het antwoord altijd 'direct verwacht wordt (de businesslaag wacht op antwoord, dit is een synchrone proceskoppeling).' De (business)applicatie bepaalt of er sprake is van een vraag/antwoord en zal dus 'wachten op het antwoord' (ook wel synchrone of blokkerende vraag genoemd). Als dat zo is, verwacht de applicatie het antwoord in dezelfde sessie retour; de applicatie hoeft dus niet het antwoord aan de vraag te koppelen (correlatie).
 - Een enkelvoudig bericht, waarbij eventueel een resultaat enige tijd later komt; een dergelijke bericht van A naar B wordt 'melding' genoemd. De (business)applicatie zal niet wachten op het antwoord: deze applicatie zal het eventuele 'antwoordbericht' op een ander moment

² In NORA Communicatiepatronen genoemd.

³ Zie ook rapport van de werkgroep COMBI, blz xxxxxNOEMEN!

ontvangen en moet correleren aan het oorspronkelijke vraag bericht.

Voor de logistieke laag maakt het wel wat uit of er sprake is van een synchrone (business)bevraging of van een synchrone (business)transactie. Het verschil komt tot uiting als er iets misgaat en er wordt geen antwoord ontvangen.

Bij een synchrone (business)bevraging is het niet belangrijk of de vraag verloren ging of dat het antwoord niet aankwam. De vraagsteller wacht een bepaalde tijd (time-out) en bepaalt als er binnen die tijd geen antwoord is ontvangen of de vraag opnieuw gesteld wordt of nu even niet. De logistieke laag biedt hiervoor de synchrone vraag/antwoord berichten.

Bij een synchrone (business)transactie is het wel van belang om te weten of de transactieaanvraag is aangekomen en verwerkt gaat worden of niet. De aanvrager moet dat weten, omdat er anders een ongedefinieerde toestand ontstaat. Daarom wordt ervan uitgegaan, dat een synchrone (business)transactie in de logistieke laag met asynchrone berichten wordt afgehandeld met een betrouwbare overdracht van de aanvraag (en van het antwoord).

3.2.1

Scope: Interactievormen Digikoppeling versie 1

We hebben nu bovengenoemde twee hoofdvormen van interactie op de logistieke laag onderkend. Per interactievorm is aangegeven welk businesspatroon dat ondersteunt en wat de kenmerken van die interactievorm zijn op de logistieke laag en op de communicatielaag.

- Bevragingen
 - Ondersteunen businesspatroon: synchroon vraag/antwoord, dus blokkerende vraag door applicatie, geen expliciete correlatie door applicatie;
 - Logistiek: synchroon vraag/antwoord; logistieke laag correleert niet expliciet. Dat gebeurt impliciet door de synchrone context;
 - Communicatie: één synchrone sessie, mogelijk op termijn twee asynchrone sessies: De logistieke laag (sublaag toepassing uit paragraaf 2.3) kunnen we zo inrichten, dat vraag en antwoord gesplitst worden in bijvoorbeeld twee verschillende technische HTTP-sessies (sublaag communicatie). De logistieke laag moet dan wel expliciet correleren.
- Meldingen
 - Ondersteunen businesspatroon synchrone én asynchrone (business)transactie;
 - Logistiek: asynchrone melding met acknowledgement, dus betrouwbaar;
 - Communicatie: melding (business)transactieaanvraag en logistieke bevestiging; in principe in twee verschillende (synchrone) sessies.

3.3 Security (vertrouwelijkheid en integriteit)

De afspraken van Digikoppeling richten zich met name op de aspecten vertrouwelijkheid (encryptie) en integriteit (onwizigbaarheid, zekerheid afzender).

Dit onderwerp is nader uitgewerkt in het document "Digikoppeling Authenticatie". De belangrijkste eisen zijn:

- Een serviceprovider moet de identiteit van de servicerequester éénduidig en betrouwbaar kunnen vaststellen (authenticeren). Betrouwbaar betekent voor Digikoppeling dat daarvoor een (PKIoverheid) certificaat gebruikt wordt.
- De autorisatie tot het gebruik van een service is een verantwoordelijkheid van de serviceprovider. De autorisatie wordt verleend (of niet) op het niveau van de (requester)organisatie en niet op het niveau van medewerker of afdeling, respectievelijke applicatie binnen die organisatie.
- Het bericht mag onderweg niet gelezen of veranderd kunnen worden door onbevoegden (encryptie).
- De beheerlast (bijvoorbeeld van het aantal certificaten) moet zo laag mogelijk zijn, waardoor een bron van storingen wordt verminderd.

Verder moet het onderwerp informatiebeveiliging nog geconsolideerd worden. Dat gebeurt op basis van en in samenhang met het katern Informatiebeveiliging NORA 3.0.

4 Standaarden

4.1 **Waarom standaardisatie**

Eén van de belangrijkste eisen die door de overheid gesteld wordt bij de inrichting van generieke voorzieningen is, dat er door gebruikers daarvan (de overheidsorganisaties) geen maatwerk ontwikkeld hoeft te worden, maar dat gebruik gemaakt kan worden van "common off the shelf" (COTS) software (hetzij commercieel of OPEN geleverd). Voor Digikoppeling (de logistieke laag) hoeft dan geen software te worden ontwikkeld. Dit doel wordt bereikt (benaderd) door te kiezen voor internationale vastgelegde standaarden, die door "alle" leveranciers interoperabel zijn geïmplementeerd.

Internationale standaarden voor berichtenuitwisseling vormen een "raamwerk" voor het vastleggen van logistieke informatie. Dat betekent o.a. dat naast een keuze voor een internationale standaard ook nog altijd in detail (voor Digikoppeling) vastgelegd moet worden hoe de gekozen standaard precies ingevuld wordt. Bijvoorbeeld: als afgesproken wordt dat authenticatie gebeurt op basis van één van de mogelijkheden die in het internationale raamwerk zijn gedefinieerd, zoals TLS, dan zal vervolgens nog moeten worden afgesproken hoe het certificaat er precies uit ziet, wat als identificatie voor een afnemer wordt gebruikt etc.

4.2 **Families van standaarden: WUS en ebMS**

Het European Interoperability Framework (IDABC) benoemt twee families van op het concept van webservices gebaseerde standaarden. Voor de toepassing binnen Digikoppeling is in eerste instantie de beperking van die twee families overgenomen; andere families hebben onvoldoende relevantie voor de Europese en Nederlandse overheid.

De relevante families zijn:

- ebXML en op de logistieke laag met name ebMS;
- WS-* (WS-Security, WS-Addressing, etc). Het is wat verwarrend om deze familie aan te duiden met 'webservices', want webservices is een algemeen concept dat gerelateerd is aan SOA. Ook ebMS werkt volgens dat concept. Omdat de WS-* familie voortbouwt op de basisstandaarden WSDL, UDDI en SOAP, wordt deze familie wel aangeduid met WUS⁴. Deze terminologie is hier overgenomen.

⁴ Bijv: IBM Redbook: Patterns: Service-Oriented Architecture and Web Services April 2004, pag 145:

It includes Web Service Definition Language (WSDL) and Universal Description, Discovery, and Integration (UDDI), also called the WUS (WSDL, UDDI, SOAP) stack as a whole

6.3.1	e-overheids-principe	P17	Het berichtenverkeer binnen de e-overheid wordt vooralsnog gebaseerd op standaarden conform ofwel de ebXML-familie ofwel de webservice familie.
<p>Standaardisatie van het berichtenverkeer</p> <p>In een werkgroep, bestaande uit architecten van diverse e-overheidsprogramma's, is gekeken naar mogelijke standaardisatie van het berichtenverkeer. Geconcludeerd werd, dat vooralsnog het naast elkaar bestaan van twee families van standaarden onontkoombaar is. Het advies luidt om gebruik te maken van ebMS als betrouwbaar (secure) berichtenverkeer nodig is .</p> <p>Verder constateerde de werkgroep, dat er voor webservices een standaard moet worden ontwikkeld, waarmee ook betrouwbaar berichtenverkeer met webservices mogelijk wordt. Verder moeten we voor zowel ebMS als webservices nog standaarden afspreken over:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Identificatie, authenticatie en autorisatie <input type="checkbox"/> Versleuteling <input type="checkbox"/> Adressering en routing <input type="checkbox"/> Vindbaarheid en beschrijving services <input type="checkbox"/> Berichten identificatie <input type="checkbox"/> Karakterset en codering 			

Dit document geeft invulling aan bovenstaande punten.

Bovenstaande tekst geeft nog geen volledige duidelijkheid over de vraag wanneer een service wordt aangeboden op basis van ebMS en wanneer op basis van WUS. Als reliability belangrijk is, is in Digikoppeling versie 1 alleen ebMS mogelijk. Als reliability geen rol speelt, dus bij bevestigingen, laat bovenstaande omschrijving die keuze nog open.

Een van de hoofddoelstellingen van Digikoppeling is het vereenvoudigen van de logistieke onderdelen van gegevensuitwisseling voor iedere overheidspartij. Een belangrijke bijdrage daarin is, het vermijden van keuzes die per uitwisseling gemaakt moeten worden. Dat geldt ook voor overbodige dubbele inspanningen.

Daarom werden in overleg en samenwerking met vertegenwoordigers van gebruikers⁵ van Digikoppeling de volgende conclusies getrokken:

- Gebruik WUS voor bevestigingen, omdat daar WS-I (Web Services Interoperability Organization) standaarden beschikbaar zijn. Die WS-I standaarden bieden een goede basis voor deze interactievorm.
- Gebruik ebMS voor meldingen, waarbij reliability belangrijk is.
- Partijen kunnen als extra optie onderling afspreken, dat voor bevestigingen ook ebMS wordt toegepast.

Hiermee bereiken we, dat bij een nieuwe bevestigingsservice aan Digikoppeling geen discussie hoeft te ontstaan of additionele keuzes gemaakt hoeven te worden over hoe die service logistiek wordt aangeboden. Sectoren worden altijd via een koppelpunt (zie § 2.2) aan Digikoppeling gekoppeld. Verschillen tussen een sectorbus of sectorale afspraken en Digikoppeling worden opgelost (getransformeerd) in het sectorkoppelpunt. Transformaties vinden alleen plaats in dat koppelpunt. Individuele serviceproviders of -requesters werken via Digikoppeling altijd op dezelfde wijze en ze investeren daar slechts éénmaal in.

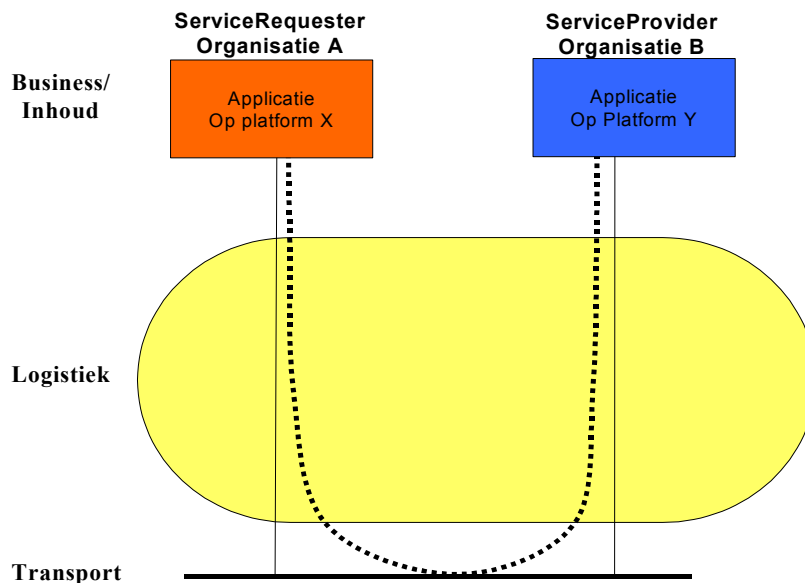
⁵ Werkgroep servicebus o.l.v. W. Keller

5 Inrichting van de servicebus

5.1 Mapping functionaliteit op componenten

In de vorige hoofdstukken hebben de we scope en de daarvoor gewenste functionaliteit met de te ondersteunen open standaarden geïdentificeerd. Dit hoofdstuk beschrijft de mapping van die functionaliteit naar de te realiseren componenten. Een belangrijk deel van de architectuur van de servicebus, van de logistiek, betreft het onderkennen van die componenten, het maken van keuzes daarover en het bepalen van hun onderlinge relaties.

De kerntaak van de dunne bus is het mogelijk maken van de uitwisseling van berichten tussen applicaties. Applicaties houden zich bezig met de inhoud en niet met de logistiek. De vereiste logistieke functies worden uitgevoerd door componenten die zich bevinden in het pad tussen de betreffende applicaties (zie figuur 4). Die componenten regelen de logistiek. Ze bevinden zich daardoor binnen het logistieke domein. Dat logistieke domein is een functioneel aandachtsgebied en is niet bedoeld als een begrenzing van verantwoordelijkheden. Dat gehele logistieke domein vormt het aandachtsgebied van Digikoppeling.

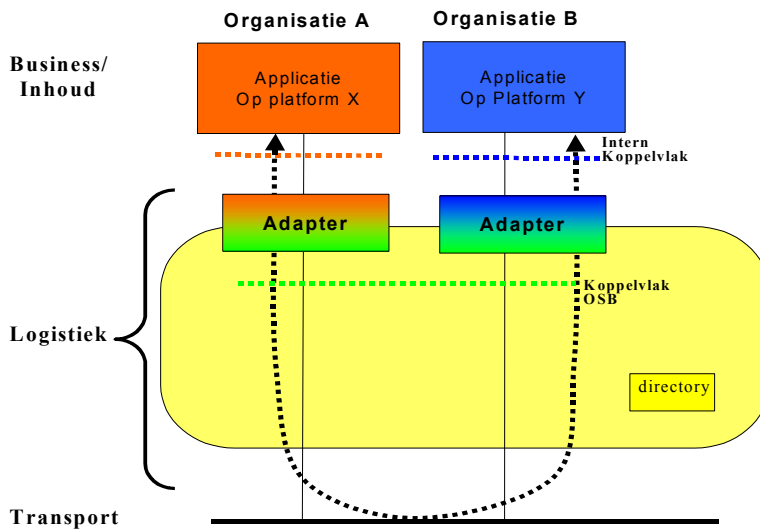


Figuur 4 - Generieke schets van een servicebus op de logistieke laag

De afspraken en voorzieningen in de logistieke laag moeten het mogelijk maken, dat verschillende applicaties, in verschillende (leveranciers)omgevingen, eenduidig berichten kunnen uitwisselen conform gemaakte afspraken over quality of service.

De huidige marktontwikkelingen (zowel gesloten als Open Source) richten zich meestal op het leveren van de vereiste dunne bus functionaliteit. De markt levert een 'off the shelf' functionaliteit die meer of minder binnen de bedrijfseigen omgeving geïntegreerd is (middleware). Die

functionaliteit kan ook naar buiten toe conform internationaal vastgestelde koppelvlakken interoperabel communiceren met vergelijkbare andere producten. Die standaard functionaliteit wordt in Digikoppeling architectuur aangeduid met de term "adapter".



Figuur 5 - Logistieke functionaliteit ondergebracht in adapters

Iedere organisatie moet dus een adapter hebben die de vertaling verzorgt van en naar het externe (Digikoppeling) koppelvlak en het (bedrijfs-)interne koppelvlak en omgekeerd, en die met name de logistieke functionaliteit uitvoert. Bijvoorbeeld: de ene adapter encrypt en de andere decrypt, alles conform de gemeenschappelijke standaard.

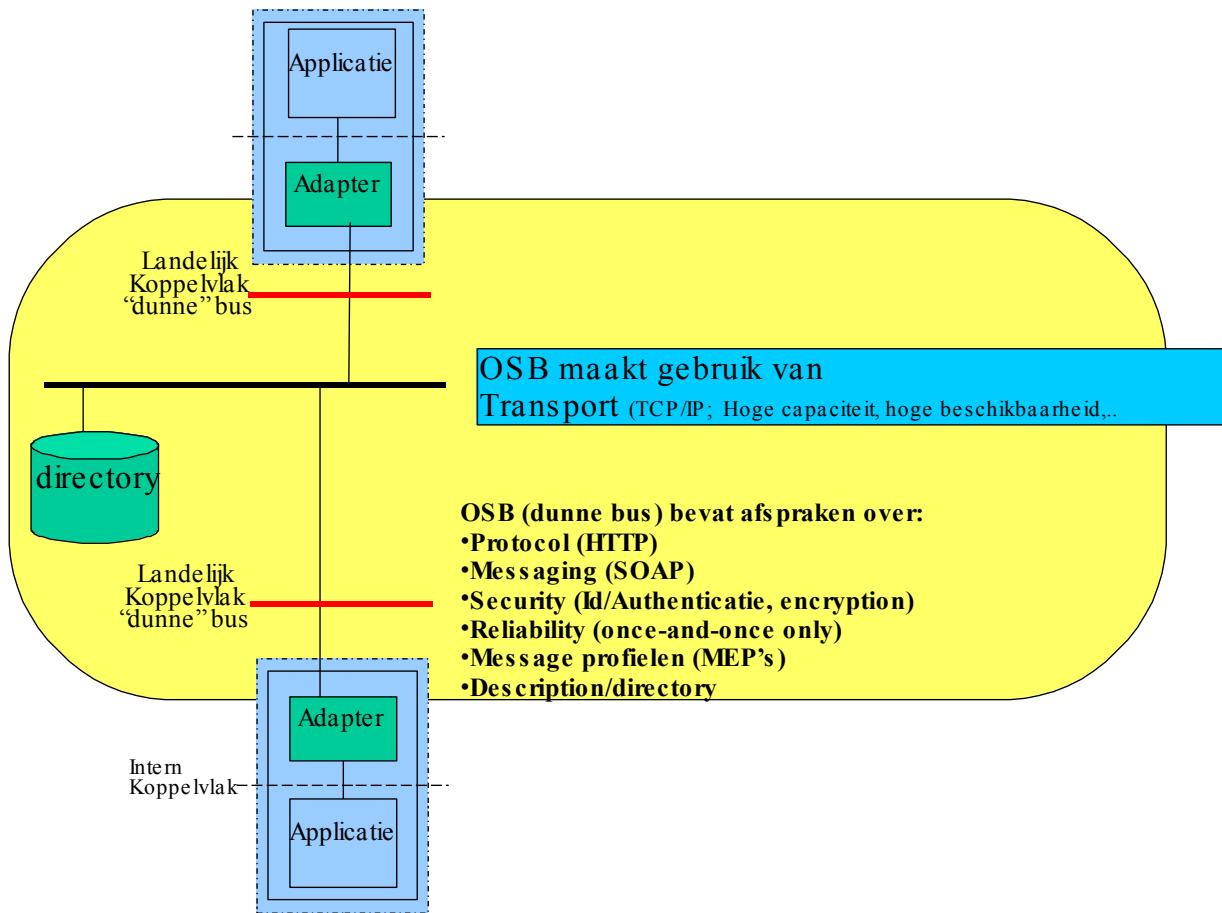
5.2

Dunne bus

De dunne bus maakt het mogelijk om op een standaard manier berichten uit te wisselen. Daarvoor is het nodig, dat er een koppelvlakdefinitie is opgesteld, dus dat er afspraken gemaakt zijn betreffende:

- te hanteren communicatieprotocol: HTTP.
- te hanteren messaging protocol: SOAP.
- inrichting van security, identificatie, authenticatie, encryptie.
- inrichting van reliability.
- ondersteunde Message Exchange patterns, ofwel interactiepatronen (met hun kenmerken).
- het vastleggen van beschrijvingen van services (bijv. WSDL) en waar die te vinden zijn.

Een van de kenmerken van de dunne bus van Digikoppeling versie 1 is, dat er geen actieve logistieke componenten zitten in het pad tussen adapters van servicerequester en serviceprovider. Alleen het netwerk zit er tussen. Performance, snelheid en beschikbaarheid worden daarom niet door de bus bepaald, maar alleen door het netwerk en door de serviceprovider. Een en ander is weergegeven in het volgende figuur:



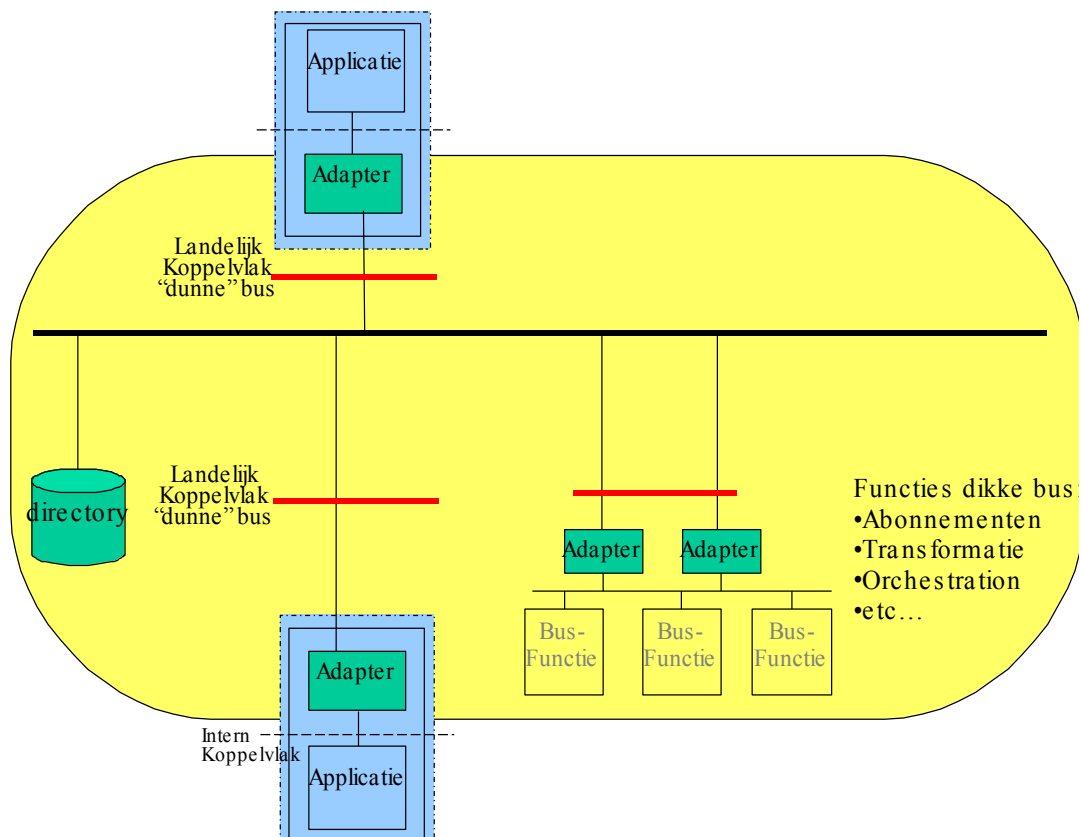
Figuur 6 - Afspraken en functies in dunne bus

5.3

Dikke bus

De dikke bus bevat meer functionaliteit met betrekking tot de logistiek van berichten. Het is daarom belangrijk om vast te stellen, dat de dunne bus een goede basis biedt voor de latere dikke bus.

In de dikke bus is een veelheid van (generieke) services⁶ mogelijk. Te denken valt aan services als een abonnementenadministratie, choreografie over (business)services heen, berichtentransformatie et cetera. De concrete behoefte hieraan als onderdeel van Digikoppeling moet nog worden vastgesteld. Dergelijke uitbreidingen komen zo nodig in latere versies van Digikoppeling.



Figuur 7 - De dikke bus als uitbreiding van de dunne bus

Services in de dikke bus verschillen functioneel van businessservices, omdat ze inhoudelijk neutraal en generiek zijn. Dat wil zeggen, dat zij op geen enkele manier zelf de service-, proces- of informatie-inhoud van de bouwstenen bepalen. Een abonnementenadministratie bijvoorbeeld kan aangeboden worden als een generieke 'busservice'. Een abonnementenadministratie is immers in wezen niet meer dan de mogelijkheid om een abonnement te nemen, zodat je bij het optreden van bepaalde events (gebeurtenis) (bijv. huwelijk) van een bepaald object (bijv. persoon met een BSN) een bepaalde set gegevens (bijv. persoonsgegevens) ontvangt. De business bepaalt de invulling, dat wil zeggen: welke events, objecten en gegevenssets er zijn.

⁶ NORA duidt de services die in de bus worden aangeboden niet met de term service aan, maar meer algemeen als "functies", om het onderscheid met business-services te benadrukken. In deze paragraaf wordt toch gewerkt met de term services, omdat hier de (technische) overeenkomst tussen generieke infrastructurele service en business services wordt benadrukt.

Qua architectuur zijn die generieke services niet anders dan de (business)services die aangeboden worden door de aanbieders. Ze zijn beschikbaar via hetzelfde koppelvlak (van de dunne bus) en ze leveren een bepaalde service. Of een dergelijke service 'in de bus' zit of 'aan de bus', is niet relevant voor de architectuur.

Dergelijke generieke services kunnen ook door een willekeurige organisatie aangeboden worden via de bus. Gezien de missie van Logius ligt het voor de hand, dat generieke infrastructurele voorzieningen beheerd worden door Logius. Eigenlijk is de discussie 'in' of 'aan' een non-discussie, omdat het feitelijk gaat om services die 'aan' de dunne bus zitten. Het is dus een kwestie van scope of het 'in' of 'aan' de bus genoemd wordt.

6 Basisinrichting van Digikoppeling

6.1 Inleiding

De functionaliteit van Digikoppeling wordt in versies gerealiseerd. De eerste stap is Digikoppeling versie 1.0. Deze versie 1.0 levert de dunne bus, dat wil zeggen de functionaliteiten als vermeld in hoofdstuk 3. In de volgende versies worden uitbreidingen toegevoegd als daar afspraken worden over gemaakt.

In paragraaf 2.3 constateerden we: Digikoppeling is een set van afspraken en gemeenschappelijke voorzieningen die de implementatie van de logistieke laag vormt.

In dit hoofdstuk beschrijven we hoe die verschillende afspraken en voorzieningen samenhangend ingericht worden.

In hoofdstuk 5 staat, dat de kernfunctionaliteit van de dunne bus wordt ondergebracht in adapters (voorzieningen). De 'buitenkant' van die adapters is vastgelegd in Digikoppeling Koppelvlakstandaarden (afspraken). Rond Digikoppeling Koppelvlakstandaarden zijn voorzieningen onderkend om te kunnen testen of services wel aan de standaarden voldoen, de zogenaamde 'Compliancevoorzieningen'. Koppelvlakstandaarden en compliancevoorzieningen worden verder beschreven in § 6.2.

De beschikbare services moeten gevonden en gebruikt kunnen worden. Daartoe is een voorziening onderkend, het Digikoppeling Service Register (uitgewerkt in § 6.3).

De adapters bevinden zich bij iedere overheidsorganisatie; ze zijn de verantwoordelijkheid van die organisatie. Het is als het ware de postkamer van die organisatie, die verantwoordelijk is voor de afhandeling van al het in- en uitgaande berichtenverkeer. Er zijn verschillende inrichtingen mogelijk. Dat is beschreven in § 6.4.

6.2 Digikoppeling Koppelvlakstandaarden

De koppelvlakstandaarden zijn de basis van Digikoppeling. Door het vergaand standaardiseren van de koppelvlakken wordt bereikt, dat organisaties – op het gebied van de logistieke laag – interoperabel met elkaar berichten kunnen uitwisselen in het kader van webservices. Ze hoeven daarin maar één keer te investeren. Er zijn twee koppelvlakstandaarden: één voor ebMS en één voor WUS.

6.2.1 *Koppelvlakstandaarden WUS en ebMS*

De kernfunctionaliteit is gelegen in het met elkaar kunnen communiceren conform strikte standaarden. Digikoppeling **Koppelvlakstandaarden** zijn zodanig opgesteld, dat die functionaliteit geïmplementeerd kan worden met behulp van standaard beschikbare COTS (Common of the Shelf) software. Hiermee vermijden we ongewenst maatwerk om aan Digikoppeling Koppelvlakstandaarden te voldoen. Afhankelijk van de interactievorm gebeurt de uitwisseling met behulp van een profiel gebaseerd op ofwel **WUS** (bevragingen) ofwel **ebMS** (meldingen). Zie hiervoor ook hoofdstuk 4. Aangezien de interactievorm bepalend is, vindt geen transformatie plaats in Digikoppeling. Buiten Digikoppeling, dus net

binnen de overheidsorganisatie, kan uiteraard wel een transformatie plaatsvinden naar interne standaarden. Datzelfde kan gelden net binnen andere sectoren (zie stelsel van bussen).

6.2.2 *Compliancevoorzieningen*

Direct gerelateerd aan de koppelvlakstandaarden zijn voorzieningen (gedefinieerd en beschikbaar gesteld door Logius), die het mogelijk maken om te controleren of een ontwikkelde service (provider of requester) voldoet aan die standaarden. Deze worden Compliancevoorzieningen genoemd.

6.3 **Digikoppeling Service Register**

Serviceproviders die een bevragingenservice aanbieden, doen dat conform Digikoppeling standaard. Ze publiceren onder andere⁷ hun webservicedefinitie, dat wil zeggen het contract (WSDL-WebService Definition Language) in een directory. Die directory heet het **Digikoppeling Service Register**.

Servicerequesters die een dergelijke service willen afnemen, gebruiken de met de serviceprovider overeengekomen servicedefinitie uit de directory. Partijen baseren identiteit en de authenticatieprocessen op de afspraken in Digikoppeling standaard.

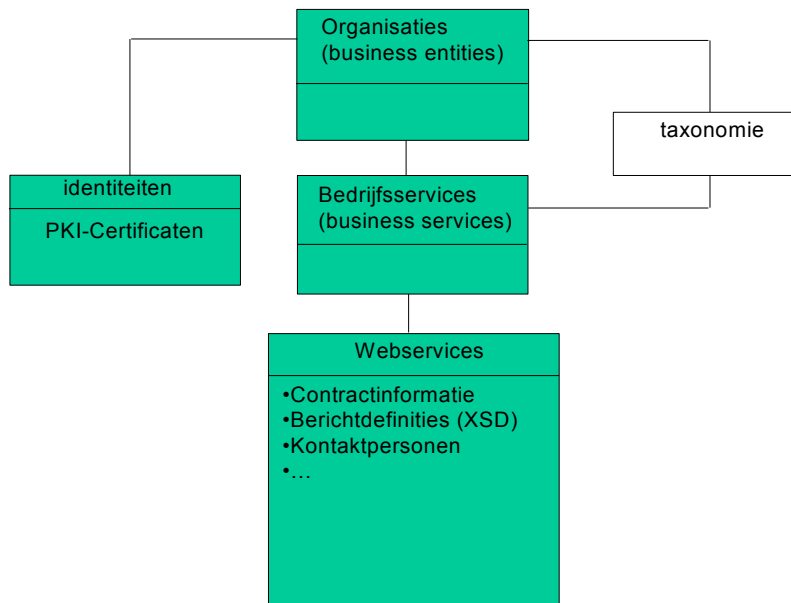
Een vergelijkbare situatie treedt op bij een melding. Dan wordt gebruik gemaakt van een ebMS profiel uit Digikoppeling ebMS standaard. Op dat profiel wordt het contract (CPA, Collaboration Protocol Agreement) voor de betreffende uitwisseling gebaseerd. Ook dat contract wordt gepubliceerd in het Digikoppeling Service Register. Identiteit en authenticatie zijn op dezelfde afspraken gebaseerd als bij WUS.

Iedere organisatie heeft zoals in hoofdstuk 5 beschreven een **adapter** die het WUS-verkeer conform Digikoppeling-WUS standaard afhandelt en/of een **adapter** die het ebMS verkeer conform Digikoppeling-ebMS standaard afhandelt.

6.3.1 *Digikoppeling Service Register: inhoud*

De dunne Digikoppeling versie 1.0 bevat beheervoorzieningen in de vorm van een 'Service Register'. Deze neutrale term is gekozen om de verzameling functionaliteiten aan te duiden die het beheer van services ondersteunt. Het Digikoppeling Service Register bevat een repository, waarin de gewenste informatie is opgeslagen over organisatie, afdelingen, contactpersonen, helpdesks en services inclusief de wijze waarop ze gebruikt moeten worden, zoals WSDL's en CPA's en dergelijke. Tevens omvat deze voorziening functies voor beheer van die informatie, zoals publiceren van nieuwe of gewijzigde contracten, notificaties bij voorgenomen wijziging van een service en het genereren van CPA's. Uiteraard is de toegang (lezen en schrijven) tot de informatie voorbehouden aan geautoriseerde medewerkers en gelden Open Standaarden zoals UDDI als uitgangspunt.

⁷ Zie Dossier SGA, hoofdstuk "Publiceren en Afspraken".



Figuur 8 - Globaal objectenmodel Service Register

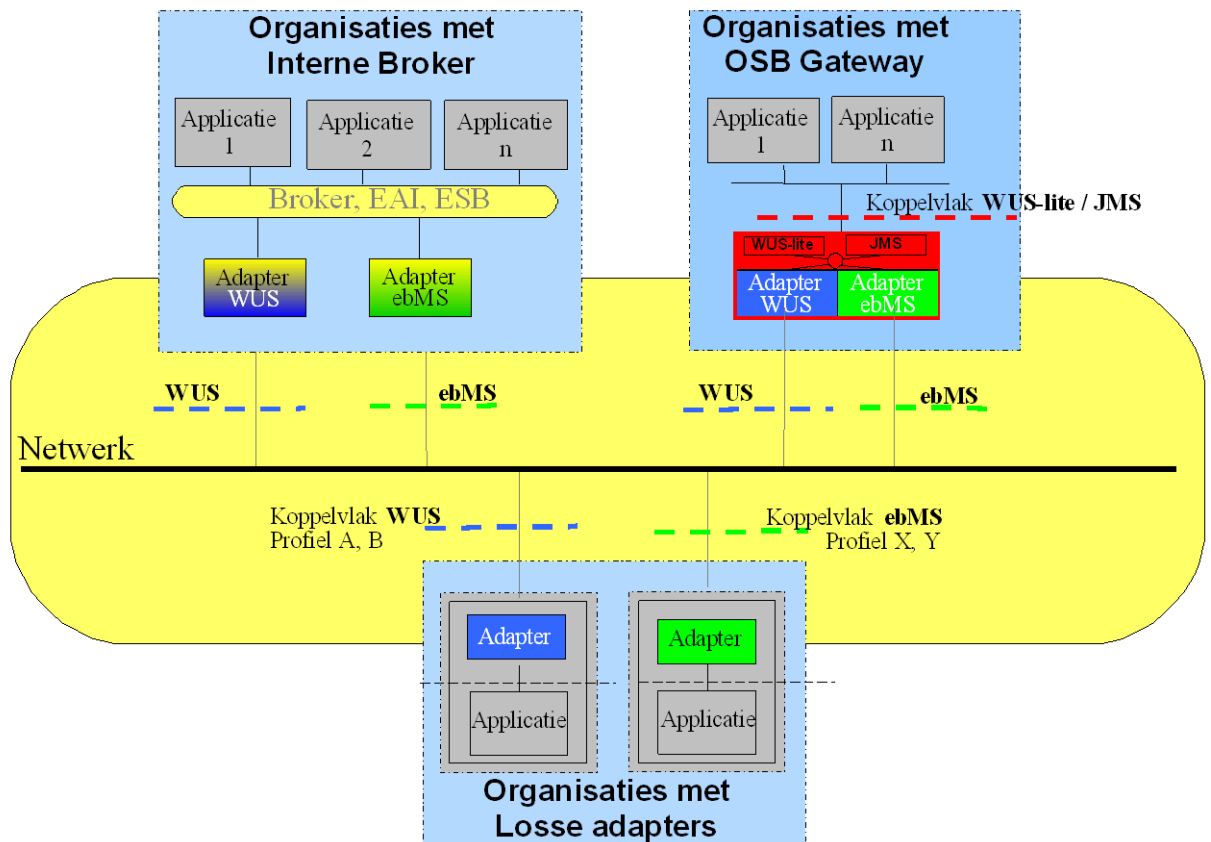
6.4 Adapters, Gateway en bedrijfseigen broker

Omdat Digikoppeling Koppelvlakstandaarden gebaseerd zijn op internationale standaarden, waarvoor in voldoende mate interoperabele COTS-software beschikbaar is, is iedere organisatie vrij in de keuze van (software voor) de adapter, geleverd door bijvoorbeeld de leverancier van de eigen middleware/ESB.

Voor organisaties die niet beschikken over middleware/ESB of bijbehorende ICT-kennis, is in het Digikoppeling-concept een standaardvoorziening opgenomen waar de benodigde adapters in gebundeld zijn. Die standaardvoorziening heet gateway. Om aan te sluiten op Digikoppeling kan iedere organisatie dus kiezen om of zelf de adapters te verzorgen óf de gateway in te zetten óf te kiezen voor mengvormen.

Een analogie voor een adapter is te vinden bij de vaste telefonie. Er bestaat een internationaal gestandaardiseerde 'stekkerdefinitie', die wordt afgemonteerd bij binnenkomst in een huis, om van het vaste telefoonnet gebruik te maken. Aan die stekker worden één of meer toestellen aangesloten, waardoor het mogelijk wordt om de businessboodschap (een telefoongesprek) te vertalen naar de koppelvlakstandaarden van de stekker. De toestellen moeten voldoen aan de koppelvlakstandaarden. Een instantie in Nederland stelt die standaarden vast. Vroeger werden de toestellen alleen door de PTT geleverd, maar tegenwoordig is het de regel dat iedereen zijn eigen telefoon gebruikt, met eigen toeters en bellen en bijvoorbeeld een huiscentrale. Dit valt echter onder 'eigen verantwoordelijkheid'. De telefoniewereld heeft het businessprobleem 'op afstand met elkaar kunnen praten' opgelost door gebruikers een abonnee te laten kiezen, waarna ze een gesprek kunnen voeren. De 'adapters' (telefoon toestellen) tussen mensen (applicaties) zijn essentieel onderdeel van het aandachtsgebied, maar aanschaf en installatie is de verantwoordelijkheid van iedere abonnee.

De twee belangrijkste inrichtingsvormen zijn geschetst in figuur 9. Het betreft inrichting bij 'Organisaties met een Interne Broker' en bij 'Organisaties met een gateway'. In deze figuur is in het midden gelaten of het gaat om requesters of providers. Beide rollen kunnen op dezelfde wijze worden gerealiseerd.



Figuur 9 - Aansluiting op Digikoppeling

6.4.1 Organisaties met een eigen broker

Organisaties met een eigen broker⁸ omgeving (meestal de grotere ICT-gebruikers) maken gebruik van de door hun brokerleverancier geleverde WUS- en ebMS adapters ofwel: ze dragen zelf zorg voor de koppeling van een adapter aan hun interne broker.

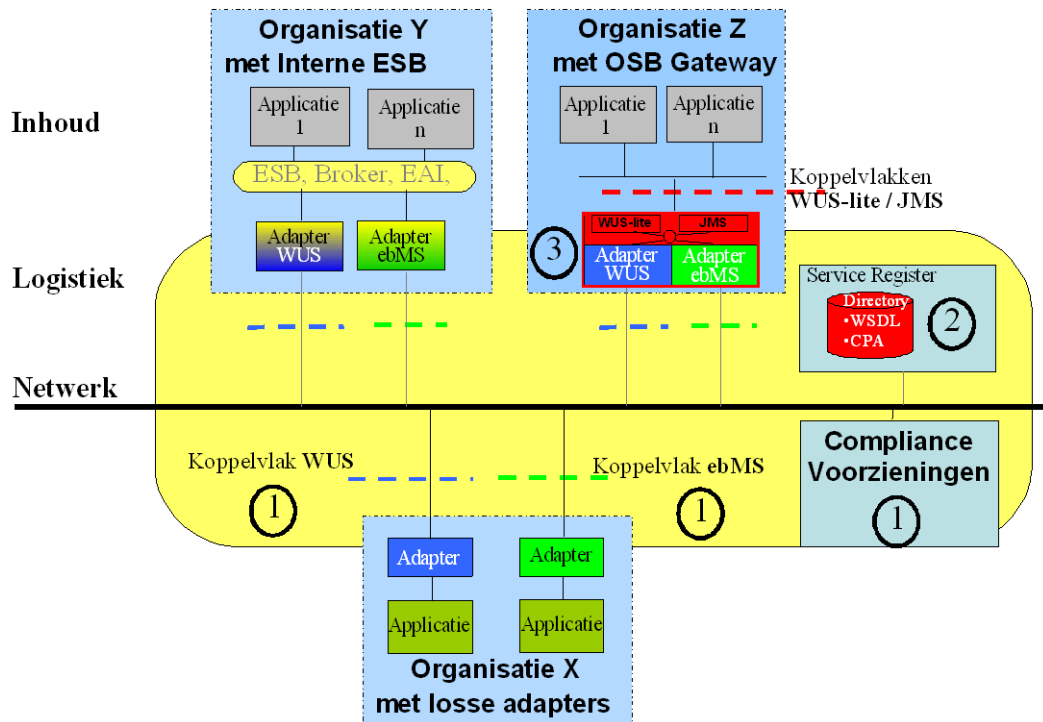
6.4.2 Organisaties met een gateway

Voor organisaties die niet beschikken over een dergelijke broker, is een voorziening ontworpen: Gateway. Die gateway communiceert aan Digikoppeling-kant op basis van Digikoppeling-WUS en Digikoppeling-ebMS. Aan de kant van de interne organisatie wordt een vereenvoudigd (ook gestandaardiseerd) koppelvlak ondersteund. Daarmee ontstaat uniformiteit aan de kant van de Organisatie. Dit vereenvoudigde koppelvlak wordt ingevuld op basis van twee profielen: WUS-lite en JMS. De gateway is op hoofdlijnen beschreven in Bijlage A.

⁸ Dergelijke software wordt ook wel met andere benaming aangeduid, o.a. middleware, ESB, etc.

6.5 Overzicht Digikoppeling compleet

Onderstaande figuur schetst alle componenten van Digikoppeling in één figuur. Dit is een functionele plaat - de figuur identificeert de functies in de logistieke laag. Hoe verantwoordelijkheden zijn belegd, is niet



weergegeven.

Figuur 10 Digikoppeling compleet

De componenten van Digikoppeling zijn:
Onder centrale verantwoordelijkheid:

1. Digikoppeling Koppelvlakstandaarden WUS en ebMS, inclusief compliancevoorzieningen.
2. Digikoppeling Service Register.

Onder verantwoordelijkheid van aangesloten organisaties

1. Adapters - een organisatie kan kiezen om 'eigen' software in te zetten of gebruik te maken van de gateway.

Voor monitoring van het berichtenverkeer, diagnose et cetera is in Digikoppeling versie 1.0 geen specifieke voorziening aanwezig. De eisen daarvoor moeten nog worden vastgesteld. Dat gebeurt in afstemming met gewenste netwerkvoorzieningen.

6.6 Productie en test

Digikoppeling is te beschouwen als een set van infrastructurele afspraken en voorzieningen. Die positionering is bepalend voor de manier waarop in Digikoppeling wordt omgegaan met het verschil tussen productie en test. Een uitgangspunt bij de ontwikkeling en onderhoud van IT-systemen is, dat productie- en testomgevingen volledig gescheiden zijn. Voor een aantal generieke infrastructurele zaken geldt dat meestal niet. Zo is er bijvoorbeeld in het algemeen slechts één LAN, één WAN en één firewall.

Ook Digikoppeling componenten maken geen onderscheid tussen productie en test:

- Digikoppeling Koppelvlakstandaarden gelden (uiteraard) voor zowel productie als test.
- Het Digikoppeling Service Register bevat de informatie van/over productie- en testservices (voor zover extern zichtbaar).

In de ontwikkel- en onderhoudsomgeving van Digikoppeling zelf is natuurlijk wel een testversie van bijvoorbeeld het Service Register aanwezig.

6.7 Relatie met transport (Diginetwerk)

In deze paragraaf wordt zeer beknopt een relatie gelegd met de beoogde oplossing voor de landelijke voorzieningen op de transportlaag. Die transportlaag regelt TCP/IP connectivity zoals in hoofdstuk 3 is beschreven. Dat maakt geen deel uit van Digikoppeling.

Digikoppeling is in principe onafhankelijk van het onderliggende transportnetwerk. Er zijn maar een paar eisen:

- Digikoppeling is gebaseerd op de TCP/IP stack, dus een TCP/IP laag 3 netwerk is noodzakelijk.
- Standaarden zijn gebaseerd op bindings naar URI's (url's). Het netwerk moet de DNS resolving van de domeinnaam uit de URI regelen en de routing naar het resulterende IP-adres.
- Digikoppeling stelt geen eisen aan de beveiliging (encryptie en authenticatie); dat wordt in de logistieke laag (dus in Digikoppeling afspraken) geregeld.

Digikoppeling heeft dus alleen basale connectivity nodig. Zonder connectivity 'werkt' Digikoppeling niet. Waarop alle bedrijfsnetwerken van de overheidsorganisaties zijn aangesloten. Binnen Diginetwerk bestaan dan verscheidene VPN's⁹. Een bedrijfsnetwerk is aangesloten op een of meer VPN's van Diginetwerk. Via een dergelijk VPN van Diginetwerk kunnen uitsluitend (delen van bedrijfsnetwerken van) andere partijen bereikt worden, die op hetzelfde VPN zijn aangesloten. Zo zal naar alle waarschijnlijkheid de OOV-sector gebruik maken van een ander VPN dan Digikoppeling. Ze 'zien' elkaar dus niet. Digikoppeling zal gebaseerd zijn op één VPN binnen Diginetwerk, het zogenaamd VPN van Digikoppeling.

In de aanloop naar dat Diginetwerk zal men voor de TCP/IP connectivity van diverse soorten verbindingen gebruikmaken, voor het grootste deel gebaseerd op de bestaande koppelnetwerken als Haagse Ring, Gemnet, Suwinet et cetera.

⁹VPN: Virtual Private Network

7 Dwarsverbanden

7.1 Inleiding

Een aantal belangrijke afspraken over de functionaliteit van Digikoppeling is onafhankelijk van de te gebruiken protocolfamilie, dat wil zeggen dat ze bij ebMS en WUS (functioneel) gelijk zijn. Deze afspraken landen soms direct in de koppelvakstandaarden en soms indirect. Bijvoorbeeld: bepaalde functionaliteit is als gevolg van die afspraken niet nodig, en er hoeven dus geen afspraken in de koppelvakstandaarden gemaakt te worden. Als er slechts indirect een relatie is met Digikoppeling Koppelvakstandaarden, is er impact op andere afspraken. Dit geldt bij Digikoppeling versie 1.0 met name voor de identiteit van organisaties, de wijze van authenticatie (bijvoorbeeld ten behoeve van autorisatie), de certificaten en daarmee samenhangende zaken.

Deze zaken worden 'dwarsverbanden' genoemd, omdat ze dwars over de families lopen. In de NORA zijn ze onderkend (zie principe P17):

- Identificatie, authenticatie en autorisatie
- Versleuteling
- Adressering en routing
- Vindbaarheid en beschrijving services
- Berichten identificatie
- Karakterset en codering

7.2 Authenticatie, identiteit en autorisatie

Alle overheidsorganisaties hebben een unieke identiteit, weergegeven door een nummer uit het Nieuw HandelsRegister (NHR). Men heeft ervoor gekozen om hiervoor het FI-nr plus het vestigingsnummer te gebruiken. Beide liggen vast in het NHR. Dit wordt in meer detail beschreven in 'Digikoppeling Identificatie en Authenticatie'.

Van elke servicerequest moet bekend zijn van welke afzender die request afkomstig is, omdat dat de basis vormt voor autorisatie. Mag die afzender die bepaalde request wel uitvoeren? Autorisatie is in NORA een verantwoordelijkheid die is belegd bij iedere serviceaanbieder (provider). Authenticatiemechanismes aanbieden is een onderdeel van de logistieke laag, dus van Digikoppeling.

Uitgangspunt is, dat de autorisatie van services in Digikoppeling alleen gebaseerd is op de organisatie waar de servicerequest van afkomstig is. Een requesterorganisatie heeft immers op basis van juridische kaders, wettelijke taken en bevoegdheden, mandaten et cetera een 'overeenkomst' met de serviceaanbieder om de service te mogen gebruiken.

De autorisatie bij een serviceaanbieder voor een bepaalde service wordt dus formeel alleen bepaald door de (overheids)organisatie waar de request vandaan komt en niet door de medewerker die bij die overheidsorganisatie de request veroorzaakt. Het is niet gewenst, dat de serviceaanbieder op de een of andere manier op de hoogte moet zijn van het bestaan en/of rechten van een medewerker van een andere organisatie.

Het gevolg is, dat de organisatie waar de request van afkomstig is, verantwoordelijk is voor het inrichten van een adequaat

autorisatiesysteem voor de eigen medewerkers. Zo mogen alleen requests geïnitieerd worden vanuit een bepaald bedrijfssysteem door daartoe gerechtigde medewerkers.

Het is ook niet gewenst, dat de aanbiederorganisatie op de hoogte moet zijn van het bestaan van afdelingen of systemen binnen de requesterorganisatie. Dat niveau is dus evenmin wenselijk als criterium voor de autorisatie bij de serviceaanbieder.

Het gevolg hiervan is, dat requesterorganisaties ervoor verantwoordelijk zijn, dat alleen (externe) requests geïnitieerd mogen worden door daartoe gerechtigde systemen van hun organisatie.

Zoals we al eerder zeiden, moet de autorisatie van een request plaatsvinden op basis van de identiteit van de requesterorganisatie. Er is dan een eenduidige systematiek voor die identiteit nodig. In het ideale geval is er een basisregistratie die identiteiten bevat. Dat moet vanzelfsprekend het NHR zijn. Maar voorlopig zal het NHR nog geen overheidsorganisaties bevatten op het niveau van de hier gewenste bevoegdheden, mandaten etc.

Zolang dat nog niet het geval is, zal voor gebruik op Digikoppeling de gewenste identiteit vastgelegd worden binnen Digikoppeling in het Digikoppeling Service Register.

De authenticatie zelf vindt altijd plaats met een PKIoverheid certificaat. Het hierboven beschreven identiteitsnummer wordt opgenomen in ieder PKIoverheid certificaat.

In Digikoppeling versie 1.0 is ervoor gekozen om dat certificaat te gebruiken op het niveau van het communicatie KANAAL (TLS) en (nog) niet op het niveau van het BERICHT (XMLDsigof bijv. x509 token). Dit is in detail uitgewerkt in ' Digikoppeling Identificatie en Authenticatie'.

7.3 Versleuteling

Zowel de koppelvlakstandaard van ebMS als van WUS maken gebruik van TLS/SSL v3 (tweezijdig) voor encryptie van berichten. Als in de toekomst versleuteling van de payload opgenomen wordt in de standaarden, zal dat in beide gevallen gebeuren op basis van XML Encryption of mogelijke andere toekomstige standaarden.

7.4 Adressering en routing

Uitwisseling over Digikoppeling is gebaseerd op services. Iedere service heeft een definitie (WSDL of CPA). De servicerequester stuurt de request naar het adres in die definitie. Dat adres is een 'logisch' adres gekoppeld aan een transportadres, een URI (url). De feitelijke routing van (de pakketjes van) het bericht gebeurt door TCP/IP op basis van het IP-adres, dat bij de domeinnaam van de betreffende URI hoort. De vertaling van domeinnaam naar IP-adres gebeurt op de netwerklaag, in principe via DNS resolving op internet.

Adresinformatie is zowel in de WUS-standaard, door het gebruik van WS-addressing, als in ebMS aanwezig op de verbindingslaag (HTTP-binding). Die informatie is ook op een meer logisch niveau aanwezig in de logistieke header. Die laatste informatie kan zo nodig gebruikt worden voor verdere routing in/achter de service in de servicebeschrijving.

In Digikoppeling versie 1.0 wordt dus door een servicerequester het bericht rechtstreeks gestuurd naar de serviceprovider op basis van de informatie in het 'contract' (WSDL of CPA). In de servicebus zit geen centrale hub die de routing verzorgt. Die heeft voor routing ook geen toegevoegde waarde zolang er geen sprake is van content-based routing. Er is in de koppelvlakstandaard WUS en ebMS wel rekening gehouden met de behoefte aan (toekomstige) transparante intermediairs. Dergelijke intermediairs kunnen zich ook bevinden op de aansluitpunten aan Digikoppeling (bijvoorbeeld een proxy bij een organisatie).

7.5 Service Register

Er is één Service Register (directory), waarin (tenminste) de benodigde informatie voor alle Digikoppeling services is opgenomen. Op detailniveau van syntactische informatie over een webservice zijn er verschillen tussen ebMS (CPA) en WUS (WSDL). Verder wordt Digikoppeling Service Register uniform ingericht.

7.6 Berichtidentificatie

Alle berichten, zowel WUS als ebMS, hebben een unieke identificatie. We hebben gekozen voor een structuur die geldig is in zowel de ebMS omgeving als in de WUS omgeving. Zo kan dezelfde berichtidentificatie gebruikt worden op zowel een ebMS traject als op een voorafgaand of volgend WUS traject. Een bepaald bericht kan daardoor direct 'gevolgd' worden.

Gekozen is voor de structuur UUID@URI.

7.7 Karakterset en Codering

Op Digikoppeling versie 1.0 is voor alle uitwisselingen het gebruik van UTF-8 voorgeschreven.

De karakterset is in feite een zaak van de 'inhoud' en niet van de logistieke laag. Het is aanbevolen om een brede internationale standaard te hanteren, zoals ISO/IEC 10646 ofwel Unicode 2.0.

Bedenk wel dat niet alle applicaties de volledige set zullen (of kunnen) ondersteunen (denk aan legacy applicaties met bijvoorbeeld alleen een ISO karakterset). Er zullen dus onderling afspraken gemaakt moeten worden over het gebruik van de karakterset.

Bijlage: Gateway

Doel van de gateway is om aan de kant van de organisatie (intern) één koppelvlak ('één stekker') aan applicaties aan te bieden. Daarmee kunnen alle interacties, dat wil zeggen betrouwbare meldingen én synchrone bevragingen, aan de buitenkant via Digikoppeling (extern) worden afgehandeld. We hebben afgesproken dat ene koppelvlak in twee smaken te leveren: WUS-lite en JMS.

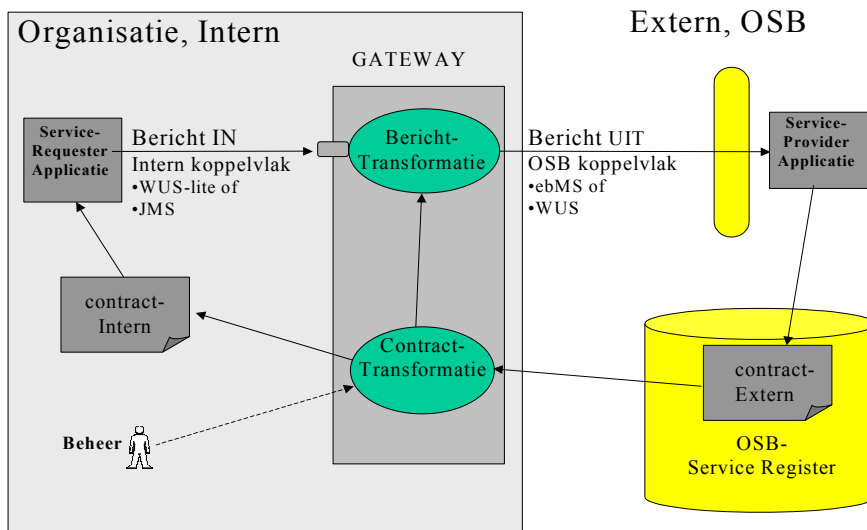
Om dat doel te bereiken, ondersteunt de gateway diverse transformaties tussen intern (WUS-lite respectievelijk JMS) en extern (Digikoppeling-WUS respectievelijk Digikoppeling-ebMS profielen). De transformaties gelden voor zowel serviceproviderverkeer (SP) als servicerequesterverkeer (SR) dus vanuit de organisatie gezien zowel ingaand als uitgaand.

We verwachten, dat de gateway bij heel veel organisaties ingezet zal worden. Daarom is een van de belangrijkste eisen, dat de gateway niet of nauwelijks onderhoud nodig heeft als er nieuwe services, die via de gateway bereikbaar moeten zijn, aangesloten worden op Digikoppeling. Als bijvoorbeeld een nieuwe basisregistratie beschikbaar komt met een aantal services dan moeten natuurlijk de applicaties die er gebruik van willen maken, aangepast worden aan de nieuwe functionaliteit en berichten. Maar op de gateway die tussen die applicaties en de services zit, zijn aanpassingen - anders dan configuratieaanpassingen niet gewenst.

Organisaties kunnen gebruikmaken van dat ene interne koppelvlak, maar zouden ook kunnen kiezen voor mengvormen. Bijvoorbeeld: alle meldingenverkeer via de gateway (JMS en ebMS) en alle bevragingen rechtstreeks via Digikoppeling-WUS. Dit is een keuze van de betreffende (groep van) organisaties, gezien de mogelijkheden van de gateway is het in ieder geval mogelijk.

Inrichting gateway op hoofdlijnen

Schetst gateway met de twee hoofdfuncties:



Figuur 11 Schets gateway

- Berichttransformatie: het bericht dat door de gateway ontvangen wordt (of aan de kant van Digikoppeling, of - zoals hier getekend - vanuit de interne kant) moet worden getransformeerd naar het juiste protocol aan de andere kant van de gateway.
- Contracttransformatie: het contract, dat wil zeggen de definitie van de service en de berichten, is aan de ene kant iets anders dan aan de ander kant. Dat geldt alleen voor de logistiek en niet voor de inhoud. De gatewayfunctie Contracttransformatie zorgt ervoor, dat (zoals bijv. geschetst in de figuur) het externe contract wordt getransformeerd naar een intern contract, dat gebruikt wordt door de ontwikkelaar van de interne applicatie.

Door het uitvoeren van de ContractTransformatie wordt ook de informatie gegenereerd, die voor de latere berichttransformatie nodig is.

Gateway heeft één adres - een zogenaamd 'endpoint' - aan iedere kant per protocol. Alle ebMS en WUS berichten vanuit Digikoppeling worden via één adres afgehandeld. Datzelfde geldt voor de binnenkant voor JMS en WUS-lite.