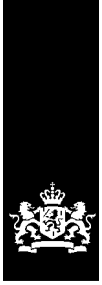


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Architectuur

Digikoppeling 3.0

Versie 1.2

Datum 13/01/2015
Status Definitief

Colofon

Logius Servicecentrum:
Postbus 96810
2509 JE Den Haag

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

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
26/11/2013	1.0	Logius	-
04/06/2014	1.1	Logius	Redactionele wijzigingen
11/11/2014	1.2	Logius	Actualisering en verduidelijking.
13/01/2015	1.2	Logius	Status definitief

Inhoud

Managementsamenvatting

Digikoppeling (DK) is sinds 2007 in gebruik en steeds meer overheidsorganisaties zien het nut van het gebruik van deze standaard. Digikoppeling wordt daardoor steeds breder ingezet als logistieke standaard voor veilige berichtuitwisseling tussen organisaties in de (semi-)publieke sector in Nederland. Digikoppeling is een essentiële bouwsteen van de elektronische overheid en geeft invulling aan de servicegerichte architectuur zoals NORA die voorschrijft.

Digikoppeling standaardiseert de uitwisseling van berichten (services) tussen overheidsorganisaties. Door Digikoppeling kunnen zij eenvoudiger, veiliger, sneller en goedkoper elkaars gegevens gebruiken dan wanneer alle organisaties bilateraal afspraken zouden maken. Het belang en de omvang van gegevensuitwisselingen in de e-overheid neemt alleen maar toe. Digikoppeling is een onmisbare voorwaarde om die uitwisseling efficiënt uit te voeren.

Het College Standaardisatie heeft Digikoppeling daarom op de ‘Pas toe of leg uit’-lijst geplaatst. Deze lijst betreft onder meer de uitwisseling met wettelijke landelijke basisadministraties en gegevensuitwisseling tussen sectoren (intersectoraal). Daarnaast wisselen organisaties onderling of in samenwerkingsverbanden gegevens uit in de dienstverlening aan burgers en bedrijven op basis van Digikoppeling.

De *Architectuur Digikoppeling* beschrijft de kaders, de principes en voorschriften, de koppelvlakstandaarden, voorzieningen en de keten waarin via Digikoppeling gegevens worden uitgewisseld (de Digikoppeling keten).

Digikoppeling 3.0 is 'backwards compatible'. Partijen die Digikoppeling 1.0, 1.1 of 2.0 gebruiken, voldoen daardoor automatisch aan de nieuwste 3.0 versie van Digikoppeling. De nieuwe functionaliteiten zijn dan echter niet beschikbaar.

1 Inleiding

Digikoppeling is een standaard voor berichtuitwisseling waarmee overheden op een veilige manier gegevens met elkaar kunnen uitwisselen.

1.1 Doel

De *Architectuur Digikoppeling* definieert de kaders – de gehanteerde principes en voorschriften - waarbinnen de berichtenuitwisseling op basis van Digikoppeling plaatsvindt en beschrijft de rol van vertaaldiensten en intermediairs in de keten van berichtuitwisseling.

Dit document beschrijft de stand van zaken voor Digikoppeling 3.0. De richting waarin Digikoppeling zich verder zal gaan ontwikkelen wordt beschreven in een apart document: de Toekomstvisie.

1.2 Doelgroep

De *Architectuur Digikoppeling* is bedoeld voor ICT-professionals in de publieke sector en voor ICT-leveranciers die Digikoppeling (willen gaan) gebruiken. Zie ook onderstaande tabel.

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

1.3 Verantwoording

De *Architectuur Digikoppeling 3.0* is tot stand gekomen in samenwerking met leden van het Technisch Overleg Digikoppeling en andere belanghebbenden. Wij danken hen voor hun input en reviewopmerkingen. Dit document vervangt de *Digikoppeling Architectuur versie 1.2.*

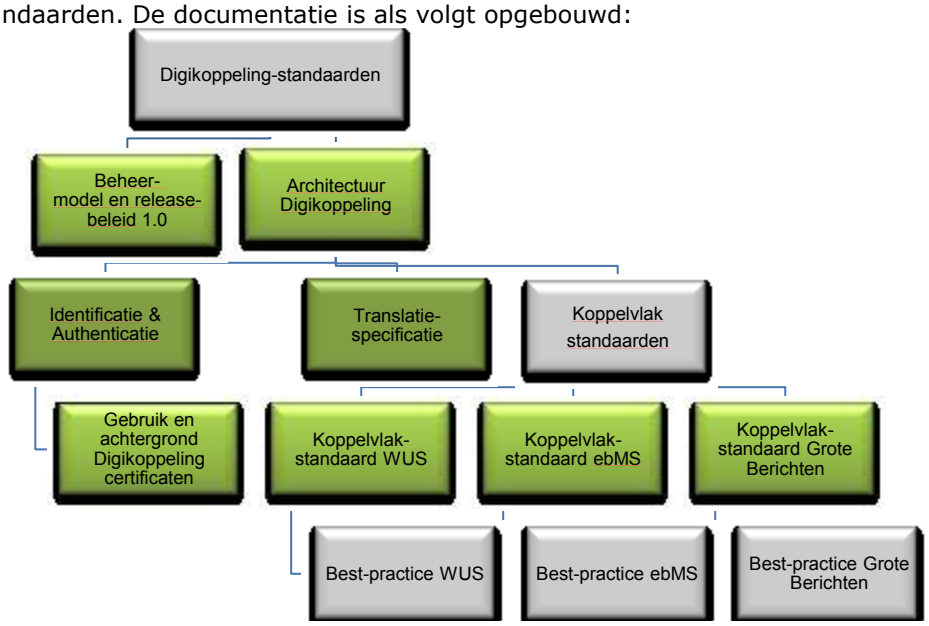
De *Architectuur Digikoppeling 3.0* is mede gebaseerd op:

- Digikoppeling Architectuur versie 1.2.
- De *Digikoppeling-koppelvlakstandaarden.* Onderdelen uit deze documenten zijn hier samengevat om voor de lezer duidelijk te maken.
- Het *hoofdstuk over de Digikoppeling* keten bevat elementen *uit De Architectuurschets*, de context voor gegevensuitwisseling binnen de overheid in algemene zin en voor Digikoppeling in het bijzonder. *De Architectuurschets* is een tijdelijk product; de essentiële elementen van *De Architectuurschets* worden opgenomen in het *NORA Katern Verbinden*.

De architectuur van Digikoppeling wordt regelmatig geactualiseerd om goed te blijven aansluiten op de behoeften van overheden en de wensen van de maatschappij.

1.4 Digikoppeling-standaarden

De *Architectuur Digikoppeling* is onderdeel van de Digikoppeling-standaarden. De documentatie is als volgt opgebouwd:



Figuur 1: Digikoppeling-standaarden

- Alle groene documenten vallen onder het beheer zoals geformaliseerd in het *Beheermodel en releasebeleid 1.0*.
- Een overzicht van alle Digikoppeling documentatie is opgenomen in *Bijlage A: Bronnen.*
- Alle goedgekeurde documenten zijn te vinden op de website van Logius, www.logius.nl.

1.5 Begrippen

Belangrijke begrippen en afkortingen zijn opgenomen in Bijlage B*: Begrippen*. Waar in dit document WUS wordt genoemd, is dat inclusief WSRM.

1.6 Leeswijzer

De Architectuur Digikoppeling is als volgt opgebouwd:

Hoofdstuk	Titel
Hoofdstuk 2	Wat is Digikoppeling?
Hoofdstuk 3	Digikoppeling architectuurprincipes
Hoofdstuk 4	De Digikoppeling-keten
Hoofdstuk 5	Digikoppeling-standaarden en Digikoppeling-voorschriften
Hoofdstuk 6	Digikoppeling-voorzieningen
Hoofdstuk 7	Vertaaldienst
Hoofdstuk 8	Implementatieaspecten
Bijlage A	Bronnen
Bijlage B	Begrippenlijst
Bijlage C	NORA-principes
Bijlage D	Eisen aan de standaard

Tabel 1: Leeswijzer

2 Wat is Digikoppeling?

Dit hoofdstuk geeft een overzicht van wat Digikoppeling inhoudt en hoe deze standaard wordt gebruikt binnen de Nederlandse overheid en publieke sector.

De belangrijkste verschillen tussen Digikoppeling 1.0, 2.0 en 3.0 worden in dit hoofdstuk toegelicht. De Architectuur heeft verder steeds betrekking op versie 3.0 tenzij anders vermeld.

2.1 Doel van Digikoppeling

(Overheids)organisaties willen diensten klantgericht, efficiënt, flexibel en rechtmatig aanbieden aan burgers en bedrijven. Daarvoor moeten zij gegevens en documenten op een generieke manier met elkaar kunnen uitwisselen.

Digikoppeling voorziet hierin door de standaarden voor deze uitwisseling te definiëren. Met deze logistieke standaardisatie bevordert Digikoppeling de interoperabiliteit tussen (overheids)organisaties. Digikoppeling richt zich op de 'envelop' van het bericht, niet op de inhoud. Daardoor kan iedere organisatie die Digikoppeling gebruikt, de postverzending onafhankelijk van de inhoud inrichten.

Digikoppeling is primair bedoeld voor gegevensuitwisseling tussen systemen van overheidsorganisaties, in het bijzonder de basisregistraties en landelijke of intersectorale gegevensdiensten, maar wordt breder ingezet in de (semi)publieke sector. Digikoppeling is beschikbaar voor elke organisatie die veilig en betrouwbaar gegevens wil uitwisselen met andere organisaties in de publieke sector. Gebruik van Digikoppeling buiten de publieke sector is ook mogelijk.

2.2 Servicegerichte architectuur conform NORA

Digikoppeling sluit aan bij de servicegerichte architectuur die NORA (Nederlandse Overheids Referentie Architectuur)[1] voorstaat. Deze vorm van informatie-uitwisseling verloopt via geautomatiseerde systemen van organisaties. Digikoppeling richt zich dus op de communicatie tussen ICT-systemen van verschillende organisaties, specifiek in de vorm van berichtenverkeer.
NORA 3.0 bestaat uit basisprincipes, afgeleide principes en katernen. Bijlage C geeft aan hoe Digikoppeling aansluit op de NORA-principes en welke NORA-principes met Digikoppeling worden ingevuld. Digikoppeling sluit ook aan op het NORA Katern Verbinden[2] en het NORA Katern Informatiebeveiliging.

[1] *Voor meer informatie over NORA zie http://www.noraonline.nl*
[2] *In ontwikkeling.*

2.3 Scope van Digikoppeling

Om digitale berichten uit te wisselen moeten organisaties op drie niveaus afspraken maken:

- Over de inhoud en betekenis van berichten (payload en eventuele bijlagen): de structuur, semantiek, waardebereiken enzovoort.
- Over de logistiek (envelop): transportprotocollen (HTTP), messaging (SOAP), adressering, beveiliging (authenticatie en encryptie) en betrouwbaarheid.
- Over het transport (netwerk): de protocollen van de TCP/IP stack (TCP voor Transport, IP voor Netwerk) en de infrastructuur, bijvoorbeeld Diginetwerk of Internet.

Digikoppeling richt zich op de logistieke laag van de berichtuitwisseling in de publieke sector. Daarbij conformeert Digikoppeling zich aan de Nederlandse Overheid Referentie Architectuur (NORA) en het European Interoperability Framework.
De kaders van die logistieke laag zijn uitgewerkt in deze Digikoppeling Architectuur. De wijze waarop deze kaders worden toegepast en ingevuld zijn uitgewerkt in de Digikoppeling-koppelvlakstandaarden. De Digikoppeling-voorzieningen ondersteunen de implementatie van Digikoppeling: ze zijn bedoeld om koppelvlakken te testen, om services te registreren en om (CPA-)contracten te genereren.

2.4 De Digikoppeling-standaarden

Digikoppeling is gebaseerd op internationale open standaarden van OASIS en W3C, twee wereldwijde standaardisatie-organen voor open standaarden.

De Digikoppeling-standaarden bestaan uit koppelvlakstandaarden en de Translatiespecificatie. De koppelvlakstandaarden beschrijven de afspraken die nodig zijn om het berichtenverkeer tussen informatiesystemen mogelijk te maken.

Digikoppeling beschrijft drie verschillende, maar aanvullende koppelvlakstandaarden: ebMS, WUS en Grote Berichten. In de Digikoppeling-documentatie zijn de koppelvlakstandaarden onafhankelijk van specifieke implementaties beschreven. Dat geeft organisaties de vrijheid om ICT-producten met een aansluiting op Digikoppeling te selecteren uit het aanbod van de markt of zelf iets te ontwikkelen.

De keuze voor het gebruik van de ebMS of WUS standaarden hangt onder meer af van het gewenste berichtenverkeer (bevragingen en/of meldingen), of er al gebruik wordt gemaakt van deze standaarden en welke standaarden door ketenpartners worden gebruikt.

Basisregistraties en landelijke voorzieningen moeten ten behoeve van bevragingen WUS ondersteunen en ten behoeve van meldingen beide protocollen of, als dat niet mogelijk is, voorzien in een protocolvertaling met een vertaaldienst. Wanneer alle serviceafnemers hetzelfde protocol gebruiken, kan de serviceaanbieder zich beperken tot dat protocol. Een vertaaldienst is dan ook niet nodig. De vraag van de serviceafnemers is dus leidend.

2.5 Besparingen door Digikoppeling

In 2010 heeft PriceWaterhouseCoopers de meerwaarde onderzocht van de gemeenschappelijke stelselvoorzieningen die de verplichte uitwisseling

van gegevens tussen bronhouder en afnemer uit 13 landelijke registraties ondersteunen.[3]

De business case stelt dat:

> *'Met de ontwikkeling van gemeenschappelijke voorzieningen wordt redundantie in investeringen en kosten in het stelsel voorkomen doordat faciliteiten gemeenschappelijk worden ontwikkeld en toegepast. De baten van de businesscase zijn vermeden kosten en investeringen."*[3]*.*[4]

Voor Digikoppeling is het geraamde netto voordeel[5] 560 miljoen euro over 10 jaar voor gebruik binnen het stelsel van basisregistraties. Het gebruik daarbuiten is nog groter.
Een aandachtspunt is de adoptie van de standaarden en voorzieningen. Wanneer meer organisaties Digikoppeling gaan gebruiken, is de winst in termen van tijd, geld en snelheid voor alle partijen groter.

2.6 Toepassing van Digikoppeling

De toepassing van Digikoppeling heeft enkele grote voordelen:

- Organisaties die Digikoppeling implementeren, kunnen veilig digitaal berichten uitwisselen met andere organisaties die ook Digikoppeling gebruiken[6].
- Met Digikoppeling kan een serviceaanbieder met één interface al zijn serviceafnemers bedienen. En een serviceafnemer kan met één interface alle serviceaanbieders bevragen.
- De implementatie van Digikoppeling (en de bijbehorende investering) is eenmalig. Na implementatie zijn nieuwe gegevensuitwisselingen met andere organisaties snel en tegen lagere kosten te realiseren.
- Digikoppeling is niet sectorgebonden: het kan door alle partijen gebruikt worden voor berichtuitwisseling tussen systemen.

2.6.1 De 'Pas toe of leg uit'-lijst

Digikoppeling staat op de 'Pas toe of leg uit'-lijst van open standaarden van het Forum en College Standaardisatie[7]. Welke koppelvlakken nodig zijn en welke standaarden uit de lijst ingezet moeten worden, is afhankelijk van de aan te schaffen functionaliteit[8].
De opname op de 'Pas toe of leg uit'-lijst houdt in dat Digikoppeling de standaard is voor gegevensuitwisseling voor organisaties binnen het organisatorisch werkingsgebied (zie 2.6.3). Bij openbare aanbestedingen voor nieuwe systemen waarbij sprake is van berichtuitwisseling, moeten deze overheidsorganisaties Digikoppeling opnemen in het Programma van Eisen – of verantwoorden waarom zij dat niet doen. Opname op de 'Pas toe of leg uit lijst' is een middel om adoptie van open standaarden te bevorderen. Deze standaarden moeten voldoen aan de eisen zoals beschreven in bijlage D.

---

[3] *Verfijning en herijking kosten- batenanalyse voor investeringen in gemeenschappelijke voorzieningen in het stelsel van basisregistraties: Grip op centrale en decentrale investeringen en kosten maximaliseert de businesscase, 23 februari 2010. Hierna "Business Case", 2010*
[4] *Verfijning en herijking kosten- batenanalyse voor investeringen in gemeenschappelijke voorzieningen in het stelsel van basisregistraties: Grip op centrale en decentrale investeringen en kosten maximaliseert de businesscase, 23 februari 2010. Hierna "Business Case", 2010.*
[5] *Het netto voordeel bestaat uit de vermeden kosten en investeringen minus kosten en investeringen in Digikoppeling voor ontwikkeling, beheer en gebruik door aanbieders en afnemers.*
[6] *Expertadvies Digikoppeling v2.0, final, 13 februari 2013.*
[7] *Voor meer informatie over open standaarden en de 'pas toe of leg uit' lijst zie: www.forumstandaardisatie.nl/open-standaarden.*
[8] *Expertadvies Digikoppeling v2.0, final, 13 februari 2013*

2.6.2 *Het functioneel toepassingsgebied*

Het functioneel toepassingsgebied van Digikoppeling is door het Forum Standaardisatie als volgt gedefinieerd:

> 'Geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgend berichtenverkeer, op basis van:
> - Digikoppeling ebMS-standaard voor meldingen tussen informatiesystemen.
> - Digikoppeling WUS-standaard voor de bevraging van informatiesystemen.
> - Digikoppeling GB-standaard voor de uitwisseling van grote berichten.'[9]

Voor Digikoppeling versie 3.0 wordt de volgende aanvullende toepassing voorgesteld[10]:

- Digikoppeling WUS-standaard voor meldingen tussen informatiesystemen.
- Translatiespecificatie voor protocolvertaling van ebMS naar WUS en andersom.

2.6.3 *Het organisatorisch werkingsgebied*

Het organisatorisch werkingsgebied van Digikoppeling is door het College Standaardisatie gedefinieerd als:

> '*Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de publieke sector.*
>
> *Het werkingsgebied van de standaard is bedoeld voor intersectoraal verkeer en verkeer met basisregistraties en kent geen verplichting binnen sectoren. Het Forum is wel van mening dat gebruik binnen sectoren ook aanbevelenswaardig is en roept de beheerder van de standaard dan ook op dit gebruik te promoten.'*[11]

Het organisatorisch werkingsgebied beschrijft de overheden die verplicht zijn om Digikoppeling te gebruiken voor een bepaald doel, in dit geval berichtenverkeer met basisregistraties en sectoroverstijgend berichtenverkeer. In de praktijk wordt Digikoppeling ook door vele organisaties buiten dit domein gebruikt en in sommige sectoren ook voor het sectorale verkeer. De landelijke eOverheids voorzieningen maken tevens gebruik van Digikoppeling voor het berichtenverkeer met hun afnemers.

2.6.4 *Toepassing binnen sectoren of buiten de overheid*

Digikoppeling kan door alle (publieke en private) organisaties worden toegepast die onderling gegevens willen uitwisselen. Een verplichting geldt alleen voor het hierboven genoemde organisatorisch werkingsgebied, dus voor de uitwisseling met basisregistraties en intersectoraal verkeer. Het gebruik van Digikoppeling buiten het organisatorisch werkingsgebied gebeurt dus altijd in overleg en in samenwerking met de betrokken uitwisselingspartners.

---

[9] *HTTPS://lijsten.forumstandaardisatie.nl/open-standaarden/digikoppeling*
[10] *Deze tekst wordt aangepast n.a.v. het advies van het Forum Standaardisatie.*
[11] *HTTPS://lijsten.forumstandaardisatie.nl/open-standaarden/digikoppeling*

2.7 Ontwikkeling van Digikoppeling

2.7.1 Digikoppeling 1.0 en 1.1

Digikoppeling is ontstaan uit de behoefte van overheidsorganisaties om eenduidig en veilig onderling gegevens uit te kunnen wisselen. Het standaardiseren van de logistieke laag voor services was een randvoorwaarde om een servicegerichte architectuur conform NORA te realiseren. Versie 1.0 van Digikoppeling richtte zich alleen op uitwisseling tussen overheidsorganisaties.
In 2007 voegde het Forum en College Standaardisatie Digikoppeling 1.0 toe aan de 'Pas toe of leg uit'-lijst van standaarden. Versie 1.1 is in 2009 opgenomen op die lijst.

2.7.2 Digikoppeling 2.0

Digikoppeling 2.0 maakte het mogelijk om een bericht te beveiligen (te ondertekenen en versleutelen) en om bijlagen toe te voegen. Daarnaast introduceerde Digikoppeling 2.0 een koppelvlakstandaard voor het uitwisselen van grote berichten.
Versie 2.0 is 'backwards compatible': organisaties die versie 1.0 gebruiken kunnen blijven communiceren met partijen die werken met nieuwere versies van de standaard. De nieuwe functionaliteiten zijn uiteraard niet beschikbaar in versie 1.0.
Digikoppeling 2.0 is in 2013 door het College Standaardisatie opgenomen op de 'Pas toe of leg uit'-lijst van standaarden. Omdat versie 2.0 backwards compatible is, voldoen implementaties van Digikoppeling 1.0 nog steeds aan die lijst.

2.7.3 Digikoppeling 3.0

De volgende punten zijn nieuw in Digikoppeling 3.0:

- meldingen via WUS
  Toevoeging van Web Service Reliable Messaging (WSRM) inclusief non-repudiation aan de WUS-Koppelvlakstandaard zodat men ook via WUS betrouwbare berichten kan versturen en ontvangstbevestigingen kan ontvangen.
- Translatiespecificatie
  De specificatie van de protocolvertaling van ebMS- naar WUS-meldingen en andersom.
- Vertaaldiensten in de Digikoppeling-keten
  Vertaaldiensten hebben invloed op de Digikoppeling-keten waarin Digikoppeling functioneert. De Architectuur Digikoppeling beschrijft die Digikoppeling-keten en de rol van vertaaldiensten daarin.

Er zijn geen wijzigingen in de koppelvlakstandaarden van ebMS en van grote berichten.
Ook versie 3.0 is 'backwards compatible'. Organisaties die Digikoppeling 1.0, 1.1 of 2.0 gebruiken, kunnen daardoor blijven communiceren met partijen die nieuwere versies gebruiken. De nieuwe functionaliteiten zijn dan echter niet beschikbaar.

2.8 Digikoppeling-beheeromgeving

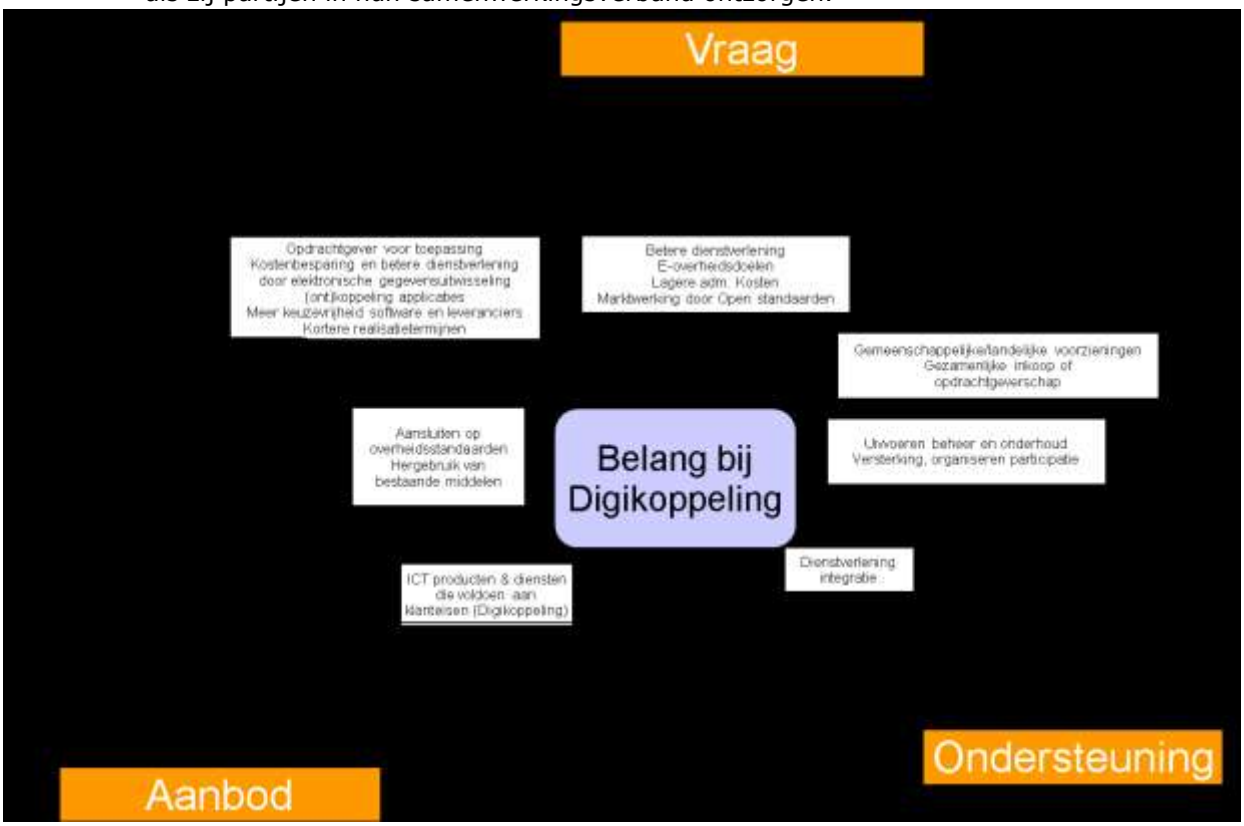
Het Digikoppeling-beheermodel waarborgt dat de Digikoppeling-standaarden niet alleen onderhouden worden, maar ook meegroeien met de behoeften van haar gebruikers. Het *Digikoppeling Beheermodel en Releasebeleid* geeft hier invulling aan.

Veel verschillende partijen hebben direct of indirect belang bij de ontwikkeling, de implementatie en het gebruik van de Digikoppeling-standaarden.

De Digikoppeling-standaarden worden in stand gehouden en doorontwikkeld door de participatie van de belanghebbenden. We onderscheiden daarbij drie posities: de vraagkant, de aanbodkant en de ondersteuningskant.

- Aan de vraagkant staan de gebruikers: organisaties die Digikoppeling gebruiken voor de eigen informatievoorziening, sectoren die Digikoppeling gebruiken als standaard voor (keten)integratiedoeleinden en e-overheidsvoorzieningen die Digikoppeling toepassen.
- Aan de aanbodkant staan ICT-leveranciers die de producten maken waarmee Digikoppeling kan worden gerealiseerd (leveranciers van Digikoppeling adapters of Digikoppeling diensten, SAAS-leveranciers). Ook standaardisatie-organisaties (OASIS, W3C e.d.) rekenen we tot de aanbodkant.
- Aan de ondersteuningskant staan de beheerders van de Digikoppeling-standaarden en de Digikoppeling-voorzieningen en Digikoppeling expertise (zowel uit de markt als binnen de overheid).

Een bijzondere groep vormen sectorale knooppunten (zie Hoofdstuk 3). Zij staan vaak niet alleen aan de vraagkant (als gebruiker en/of vertegenwoordiger van hun achterban), maar bieden ook ondersteuning als zij partijen in hun samenwerkingsverband ontzorgen.



Figuur 2: De Digikoppeling-beheeromgeving van vraag, aanbod en ondersteuning

Hieronder staan de belangrijkste onderdelen van de beheeromgeving.

- De gebruikers van Digikoppeling, die samenkomen in:

    - Een openbare community op Pleio voor het uitwisselen van kennis en het voeren van een bredere discussie over de wijze van samenwerken en het uitwisselen van gegevens via Digikoppeling.
    - Het Technisch Overleg Digikoppeling, waarin voorgestelde wijzigingen worden afgestemd.
    - Het Afnemersoverleg, het formele orgaan dat besluiten neemt over stelselvoorzieningen.
    - Bijeenkomsten met leveranciers en gebruikers.
- De beheerorganisatie, ondergebracht bij Logius, die de standaarden en voorzieningen beheert, ontwikkelingen in de omgeving volgt en periodiek voorstellen ter doorontwikkeling uitwerkt.
- Standaardisatieprocessen en -organen (onder andere het Forum en College Standaardisatie).

Het hele beheerproces staat beschreven in het *Digikoppeling Beheermodel en Releasebeleid.*

De Digikoppeling-beheerder is verantwoordelijk voor het opstellen en beheren van overheidsbrede standaarden en afspraken over het gebruik van Digikoppeling en voor het beheren van de Digikoppeling-voorzieningen.

3 Digikoppeling-architectuurprincipes

3.1 Uitgangspunten

De volgende uitgangspunten vormen de basis voor de uitwerking van deze architectuur:

1. De Digikoppeling standaarden zijn openbaar, vindbaar, transparant, leveranciersonafhankelijk en inter-operabel. Zie bijlage D voor uitleg.
2. De Digikoppeling-standaarden ondersteunen veilige gegevensuitwisseling op basis van meldingen (WUS en ebMS), bevragingen (WUS) of in combinatie met grote berichten (GB).
3. Partijen kunnen kiezen voor meldingen en/of bevragingen, afhankelijk van hun behoefte. Partijen bepalen in onderling overleg welke WUS- of ebMS-profielen ze gebruiken.
4. Basisregistraties en landelijke voorzieningen moeten beide koppelvlakstandaarden ondersteunen, eventueel door middel van protocolvertaling[12]. Mochten de serviceafnemers voldoende hebben aan één van de protocollen, dan kan de aanbieder zich tot dat protocol beperken.
5. Wanneer er wel behoefte is aan een protocolvertaling, dan geldt het volgende:
   - Partijen kunnen gebruik maken van een vertaaldienst die voldoet aan de Translatiespecificatie.
   - Vertaaldiensten kunnen sectoraal worden ingericht. Ook ICT-leveranciers kunnen vertaaldiensten leveren. De protocolvertalingen moeten altijd voldoen aan de Translatiespecificatie, die is opgesteld conform de uitgangspunten en principes uit deze architectuur.
   - Een protocolvertaling van een gestandaardiseerd protocol naar een afwijkend protocol van de serviceafnemer valt onder verantwoordelijkheid van degene in wiens opdracht de vertaling plaatsvindt.

3.2 Architectuurprincipes

De architectuurprincipes geven richting aan de Digikoppeling-standaarden en Digikoppeling-voorzieningen en zijn afgeleid van de NORA Principes (zie bijlage C):

1. **Interoperabiliteit:** De interoperabiliteit van diensten is mogelijk door het gebruik van bewezen interoperabele internationale standaarden.
2. **Standaardoplossingen:** Het gebruik van standaardoplossingen is mogelijk, met een minimum aan ontwikkelinspanning of maatwerk.
3. **Veiligheid en vertrouwelijkheid:** Gegevens worden veilig uitgewisseld conform de eisen van de toepasselijke wet en regelgeving. Wanneer berichten met persoonsgegevens verstuurd worden, moet de serviceafnemer nagaan of de uitwisseling voldoet aan de wet- en regelgeving (in het bijzonder de WBP).
4. **Betrouwbaarheid:** Berichtuitwisseling is betrouwbaar indien nodig.
5. **Ontkoppeling:** De ontkoppeling van diensten wordt mogelijk door de verantwoordelijkheid van de logistieke laag, de transportlaag en de bedrijfsproceslaag strikt te scheiden.

[12] *Serviceafnemers kunnen hierdoor ebMS gebruiken voor zowel bevragingen (binnen de sector), meldingen als grote berichten.*

3.3 Interoperabiliteit

Principe: De interoperabiliteit van diensten is mogelijk door het gebruik van bewezen interoperabele internationale standaarden.
Rationale: Door het gebruik van internationale open standaarden is het eenvoudiger en goedkoper om gegevens onderling uit te wisselen. Dit volgt uit de NORA en het European Interoperability Framework (IDABC).
Invulling: Het European Interoperability Framework 2.0 maakt gebruik van een conceptueel model voor de levering van publieke diensten . In dit model is de *Secure Data Exchange/Management* laag verantwoordelijk voor de veilige uitwisseling van diensten en informatie. Deze laag regelt de veilige uitwisseling van gecontroleerde en betrouwbare berichten, documenten, formulieren en ander informatiedragers tussen verschillende systemen. Naast het transport van gegevens moet deze laag ook specifieke beveiligingsaspecten regelen zoals elektronische handtekeningen, certificaten, encryptie en tijdregistratie. [13]
Deze laag wordt in de Nederlandse publieke sector ingevuld door Digikoppeling. Digikoppeling maakt hiervoor gebruik van twee internationale families van open standaarden voor webservices:[14]

- ebXML en op de logistieke laag met name ebMS;
- WS-*familie: WUS (WSDL, UDDI en SOAP), inclusief WS-Security, WS-Addressing enzovoort.

Deze internationale open standaarden worden door OASIS (www.oasis.org) en W3C-Consortium (http://www.w3.org) beheerd.[15]
Gevolg: Digikoppeling schrijft de ebMS- en WUS-standaarden voor in de vorm van de Digikoppeling-koppelvlakstandaarden en profielen. Organisaties kunnen hiermee effectief, snel en veilig berichten uitwisselen.

3.4 Gebruik standaardoplossingen (minimum aan maatwerk)

Principe: Het gebruik van standaardoplossingen is mogelijk, met een minimum aan benodigde ontwikkelinspanning of maatwerk.
Rationale: Door gebruik te maken van standaard software die de internationale standaarden ondersteunen wordt gegevensuitwisseling eenvoudiger, duurzamer en goedkoper. Ook wordt het beheer eenvoudiger.
Invulling: Eén van de belangrijkste eisen die de NORA stelt aan de inrichting van generieke voorzieningen is dat de gebruikers (de overheidsorganisaties) geen maatwerk nodig hebben omdat ze standaard software kunnen gebruiken, bij voorkeur open source.
Gevolg: Omdat organisaties geen maatwerk nodig hebben beperkt de investering tot de initiële inrichting, de implementatie en het beheer.

[13] Annex II - EIF (European Interoperability Framework) of the Communication "Towards interoperability for European public services" on the 16th of December 2010.
[14] EIF 1.0. Het begrip webservices is een algemeen concept dat gerelateerd is aan Service georiënteerde architectuur. Zowel WUS als ebMS werken volgens dit concept. Omdat de WS-* familie voortbouwt op de basisstandaarden WSDL, UDDI en SOAP, wordt deze familie wel aangeduid met WUS.
[15] Voor de toepassing binnen Digikoppeling is in eerste instantie de beperking van die twee families overgenomen; de andere families hebben onvoldoende relevantie voor de Europese en Nederlandse overheid om afwijking van dit kader te rechtvaardigen.

3.5 Veiligheid en vertrouwelijkheid

Principe: Gegevens worden veilig uitgewisseld conform de eisen van de toepasselijke wet en regelgeving.
Rationale: Er zijn diverse redenen om gegevens veilig en vertrouwelijk uit te wisselen. De Wet Bescherming Persoonsgegevens (WBP) verplicht adequate maatregelen om de veiligheid en vertrouwelijkheid van (persoons)gegevens te bewaken. Partijen die onderling gegevens uitwisselen moeten hier afspraken over maken. De Wet Elektronische Handtekeningen bepaalt de rechtsgeldigheid van berichten die ondertekend zijn met een geldige digitale handtekening. Naast deze wetgeving zijn er ook andere wetten en beleidskaders die eisen stellen aan beveiliging en uitwisseling van gegevens.
Wanneer het gaat over veiligheid en vertrouwelijkheid zijn ook de Wet politiegegevens (informatiedeling met derden) en de Archiefwet van belang.
Invulling: Digikoppeling borgt de vertrouwelijkheid en integriteit van berichten gedurende de berichtuitwisseling. De afspraken van Digikoppeling richten zich met name op de aspecten vertrouwelijkheid, integriteit en onweerlegbaarheid. Hiermee vult Digikoppeling de verantwoordelijkheid rond veiligheid en vertrouwelijkheid in.
Gevolg: Berichten worden veilig uitgewisseld wanneer de berichtuitwisseling aan de Digikoppeling-standaarden voldoet. Bij de uitwisseling van gegevens via Digikoppeling is de afnemer verantwoordelijk voor het juist gebruik van de ontvangen gegevens. De aanbieder dient de wettelijk basis (doelbinding) van de afnemer om gegevens te mogen ontvangen te toetsen.

Details:
De belangrijkste beveiligingseisen zijn:

- Identiteit en authenticatie: Een serviceaanbieder moet de identiteit van de serviceafnemer eenduidig en betrouwbaar kunnen vaststellen. Andersom wil de serviceafnemer ook zeker weten dat hij bij de goede serviceaanbieder is.
- Autorisatie: De autorisatie wordt (al dan niet) verleend op het niveau van de organisatie. De autorisatie voor het gebruik van een service is een verantwoordelijkheid van de serviceaanbieder. Autorisatie kan door de wet verplicht zijn gesteld. De afnemer is verantwoordelijk voor het borgen dat ontvangen gegevens alleen door geautoriseerde gebruikers kunnen worden gebruikt.
- De vertrouwelijkheid, integriteit en onweerlegbaarheid van het bericht worden op protocolniveau geborgd (dus tussen systemen). Daarbuiten moeten partijen maatregelen treffen om deze aspecten te waarborgen.
- Beveiliging van de transportlaag (point-to-point security) is randvoorwaardelijk: Beveiliging van het verkeer tussen twee (eind-)punten vindt plaats door middel van tweezijdig Transport Layer Security[16].

Digikoppeling stelt het gebruik van het PKIoverheid certificaten verplicht voor de authenticatie van partijen en voor de versleuteling en ondertekening van berichten. Deze eisen gelden voor de Digikoppeling-keten en de Digikoppeling-standaarden. Dit onderwerp is nader uitgewerkt in het document 'Digikoppeling Identificatie en Authenticatie'. Zie ook het *NORA Katern Informatiebeveiliging* (NORA 3.0) voor een nadere uitleg.

[16] *Dit is een randvoorwaarde die Digikoppeling stelt aan de transportlaag. Zie de Koppelvlak-standaarden voor de versienummers van de gebruikte protocollen.*

3.6 Betrouwbaarheid

Principe: De berichtuitwisseling is betrouwbaar indien nodig.
Rationale: Betrouwbaarheid betekent een goede aflevering van berichten. Zie ook NORA BP09.
Invulling: Dit principe wordt ingevuld met meldingen. De verzender is verantwoordelijk voor de goede aflevering van gegevens (d.m.v. berichten) en kan hiervoor betrouwbare Digikoppeling-profielen gebruiken.
Gevolg: Een betrouwbaar profiel garandeert dat een bericht met zekerheid (slechts één keer) wordt afgeleverd en dat berichten zo mogelijk in de juiste volgorde worden afgeleverd, ook als de partner tijdelijk niet beschikbaar is. Berichtuitwisseling is traceerbaar.
Details:

- Een bericht is pas betrouwbaar afgeleverd als de verzender een ontvangstbevestiging heeft gehad van de ontvanger.
- Als het bericht via een vertaaldienst gaat, moet de vertaaldienst het bericht doorleveren. De aanbieder is en blijft eindverantwoordelijk en bepaalt wat er moet gebeuren als er fouten optreden.
- Een ontvangstbevestiging wordt pas gegeven als gegarandeerd kan worden dat het bericht niet meer verloren gaat. Dit stelt eisen aan de inrichting bij de ontvanger, bijvoorbeeld in de vorm van persistent storage en betrouwbare doorlevering 'achter de voordeur'.
  NB: zodra berichten buiten de Digikoppeling-keten komen, vervalt de betrouwbaarheid die de protocollen garanderen.
- Betrouwbare WUS- en ebMS-profielen gebruiken een 'reliability contract' (sequence voor WUS en CPA voor ebMS) tussen verzender en ontvanger.
- De berichtuitwisseling wordt bewaakt door middel van monitoring, foutafhandeling en vastgelegd via een audittrail.
- Een vertaaldienst stelt de audittrail van het knooppunt beschikbaar aan de betrokken partijen in de keten.
- In de audittrail worden berichten individueel geregistreerd op datum en tijdstip[17]/(sequence of message)id/ontvangstbevestiging en eventueel foutcodes. Tevens worden de verzendende en ontvangende services vastgelegd.
- Het is mogelijk om berichtvolgorde op protocolniveau te regelen, maar dit is beperkt tot en met ontvangst door de adapter; daarna is de berichtvolgorde niet meer zichtbaar. Om die reden is het aan te raden om de berichtvolgorde aan te geven door middel van volgnummers in het bericht zelf of iets vergelijkbaars. Partijen kunnen dit onderling afspreken.

[17] Om de tijd correct te registreren is de algemeen geaccepteerde best practice dat servers gebruikmaken van Netwerk Time Protocol (NTP). NTP is een protocol voor de synchronisatie van klokken van computers via een netwerk op basis van een gemeenschappelijke tijd (meestal UTC – gecoördineerde wereldtijd).

3.7 Ontkoppeling

Principe: Digikoppeling maakt ontkoppeling mogelijk door de verantwoordelijkheid van de logistieke laag, de transportlaag en de bedrijfsproceslaag strikt te scheiden.
Rationale: De semantische afspraken (inhoud van het bericht) kennen grote diversiteit. Daarnaast zijn er procesmatige aspecten zoals kwaliteit, interne routering en afhandeling die niet door Digikoppeling worden ingevuld omdat ze niet generiek van aard zijn. Hierover kunnen partijen onafhankelijk van de logistieke aspecten afspraken maken. Door vergaande ontkoppeling ontstaat een grotere mate van flexibiliteit, waardoor de standaard breder ingezet kan worden en daarmee de efficiency van de overheid bevordert.
Invulling: Digikoppeling maakt ontkoppeling van services mogelijk door de logistieke aspecten zoals adressering, routering en beveiliging op generieke wijze in te vullen.
Gevolg: Dit maakt Digikoppeling als standaard generiek van aard en dus breder toepasbaar.

4 De Digikoppeling-keten

Dit hoofdstuk beschrijft de Digikoppeling als bouwsteen van de eOverheid. de keten van alle Digikoppeling-gerelateerde componenten die gegevensuitwisseling voor de eOverheid invullen duiden we in dit document aan als de de Digikoppeling-keten. In dit hoofdstuk worden de vormen van gegevensuitwisseling – vraag/antwoord en meldingen - op procesniveau beschreven.

4.1 Digikoppeling als bouwsteen van de eOverheid

De Nederlandse overheid werkt aan betere dienstverlening aan burgers en bedrijven met een basisinfrastructuur voor de eOverheid die is gebaseerd op services zoals beschreven in de Nederlandse Overheids Referentie Architectuur (NORA). Een reden voor het gebruik van services is dat ze herbruikbaar en daardoor efficiënt zijn.
De basisinfrastructuur bestaat uit bouwstenen voor de dienstverlening aan burgers, aan bedrijven en de inrichting van de informatiehuishouding van de overheid zelf. De bouwstenen beslaan drie pijlers:

- Loketten en voorzieningen voor burgers.
- Loketten en voorzieningen voor bedrijven.
- Registraties in algemene zin, waaronder het stelsel van basisregistraties, inclusief voorzieningen zoals met onder meer Digilevering (abonnementen services) en Digimelding (terugmelding van wijzigingen of fouten aan basisregistraties).

In dit document vatten we de loketten en voorzieningen voor burgers en bedrijven samen met het begrip ‘landelijke voorzieningen”. Om deze pijlers als samenhangend geheel te laten functioneren is het nodig dat zij informatie kunnen uitwisselen’.
Digikoppeling maakt het mogelijk om berichten uit te wisselen en services aan te roepen en is daarmee een essentiële bouwsteen van de basisinfrastructuur van de eOverheid. Organisaties kunnen via Digikoppeling rechtstreeks (bilateraal) gegevens met elkaar uitwisselen. Vaak zijn er extra schakels betrokken, zoals een sectoraal knooppunt of een intermediair.
Digikoppeling biedt een standaard voor het uitwisselen van berichten tussen systemen. Het is dus niet bedoeld om gegevens aan een eindgebruiker te tonen; dat gebeurt via een applicatie bij de eindgebruiker zelf. Digikoppeling standaardiseert de inrichting van het berichtenverkeer zodat verschillende partijen berichten kunnen uitwisselen, ongeacht om welke gegevens het gaat.

4.2 De Digikoppeling-keten

De Digikoppeling-keten bestaat uit:

- Deelnemende publieke organisaties die gegevens met elkaar uitwisselen (partijen). Een partij kan een service aanbieden – in de rol van serviceaanbieder – of een service afnemen – in de rol van serviceafnemer.
- Intermediairs: organisaties die voor deze deelnemende organisaties bemiddelen in de uitwisseling van gegevens. Partijen maken onderling (of via een intermediair) afspraken over de inhoud en vorm van de gegevensuitwisseling.
- Componenten die de Digikoppeling-keten vormgeven.

4.2.1 *Partijen*

Een partij is een (publieke) organisatie die gegevensdiensten via Digikoppeling aanbiedt aan andere organisaties en/of afneemt van andere organisaties. Een partij (in de rol van serviceafnemer of serviceaanbieder) is tevens het eindpunt van de Digikoppeling-keten. Partijen maken onderling of via een intermediair afspraken over de samenwerking en over de gegevensuitwisseling.

De uitwisseling tussen een serviceaanbieder en een serviceafnemer moet altijd betrouwbaar/vertrouwd zijn, ondanks of dankzij de betrokkenheid van intermediairs.

4.2.2 *Intermediairs*

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[18]. Het versleutelen van berichtinhoud (berichtenniveau versleuteling) kan worden toegepast indien de intermediair niet vertrouwd wordt.[19]
- Een *niet-transparante* intermediair (b.v. een vertaaldienst of een sectoraal knooppunt) bewerkt berichten en is dus een eindpunt binnen Digikoppeling.

Een intermediair zoals een sectoraal knooppunt of SAAS leverancier kan in opdracht van partijen inhoudelijke bewerkingen op berichten uitvoeren zoals de integratie, conversie en distributie van gegevens. Een dergelijke ondersteunende rol kan partijen ontzorgen bij de implementatie van standaarden, het beheer van gedeelde/gezamenlijke voorzieningen en de afstemming tussen partijen op het gebied van gegevensuitwisseling.

Figuur 3: Positionering intermediair/sectoraal knooppunt

[18] 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.

[19] Bericht-niveau versleuteling wordt op applicatieniveau toegepast tussen de verzender en ontvanger; de berichtinhoud wordt versleuteld zodat de intermediair alleen de headers kan lezen.

4.2.3 Componenten in de logistieke Digikoppeling-keten

De volgende componenten maken onderdeel uit van de Digikoppeling-keten van berichtuitwisseling.

Componenten	Toelichting
Applicatie	Een systeem waarmee gegevens worden geproduceerd, vastgelegd en gebruikt.
Broker of Enterprise Servicebusenterprise servicebus (ESB)	Een component waarmee berichten worden gegenereerd, aangeboden, afgenomen, gemonitord en verwerkt. Dit type systeem wordt gebruikt in de integratielaag. Een enterprise servicebus, broker of message handler zijn voorbeelden van een dergelijke component.
Digikoppeling-adapter	Een software-adapter voor middleware systemen die door een ICT-leverancier wordt geleverd en die de Digikoppeling-koppelvlakstandaarden implementeert. De Digikoppeling-adapter handelt alle aspecten van de berichtverwerking af, inclusief de versleuteling/ontsleuteling, ondertekening etc. Een broker of ESB bevat vaak een (configureerbare) Digikoppeling adapter.
Gegevens	Informatie die wordt beheerd en opgeslagen. Gegevens worden voor een specifieke uitwisseling in een bericht geplaatst.
PKIoverheid certificaten	Identificatie en authenticatie vindt plaats op basis van het PKIoverheidscertificaat. Zie voor nadere uitleg Digikoppeling Identificatie en Authenticatie en Gebruik van Digikoppeling Certificaten.
Servicecontract	Een technisch formaat voor het vastleggen van afspraken over de inhoud van de gegevensuitwisseling tussen partijen. Een servicecontract wordt vormgegeven d.m.v. een CPA (voor ebMS services) en een WSDL (voor WUS services) en wordt ingelezen in de Digikoppeling-adapter. Partijen stellen samen een servicecontract op.
Vertaaldienst	Een voorziening die zorgt voor de protocolvertaling van ebMS naar WUS en andersom, in opdracht van een serviceaanbieder of serviceafnemer en conform de eisen in de Architectuur Digikoppeling en de Translatiespecificatie.

Tabel 2: Componenten van de Digikoppeling-keten

N.B.: De Digikoppeling-voorzieningen (de compliancevoorzieningen, het Serviceregister en de CPA-creatievoorziening) vormen geen onderdeel van de Digikoppeling-keten maar ondersteunen alleen tijdens de ontwikkel- en test-fasen.

4.3 Uitwisselingsvormen

Uitwisselingsvormen onderscheiden we op alle niveaus van inhoud, logistiek en transport.

1. De business heeft op inhoudelijk niveau behoefte aan specifieke uitwisselingsvormen. Dat zijn veel verschillende vormen die we in de volgende subparagraaf aan de hand van een tweetal kenmerken terugbrengen tot een viertal primitieve business-interacties.
2. op logistiek niveau biedt Digikoppeling een beperkt aantal patronen voor uitwisseling. De tweede subparagraaf licht deze patronen toe en geeft aan voor welke business-interactie deze toegepast moeten worden.
3. Op transport niveau is in Digikoppeling voorgeschreven welke vormen van uitwisseling (protocollen) toegepast worden. Deze worden hier niet behandeld.

4.3.1 Business-behoefte

Op business-niveau is er een veelheid aan uitwisselingsvormen waaraan behoefte bestaat. Deze zijn vaak contextspecifiek. Soms zijn deze vormen ook specifiek voor een sector waardoor het loont om deze in een sectorale berichtstandaard voor de inhoud van een bericht af te spreken (b.v. StUF, SuwiML en NEN3610). Een aantal proceskenmerken op business-niveau bepaalt welke door Digikoppeling geboden logistieke vormen geschikt zijn. Zonder alle mogelijke behoeften uit te werken, behandelt deze sub-paragraaf wel de voor de keuze van Digikoppeling belangrijke kenmerken:

1. De impact op de serviceaanbieder is afhankelijk van de dienst die deze levert:
    - alleen informatie, die bevraagd kan worden; dat heeft geen impact op de aanbiedende organisatie;
    - het verwerken van een gevraagde transactie; dat heeft wel impact op de aanbiedende organsiatie.
2. 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 (de vraagsteller, applicatie/gebruiker houdt de context vast en weet dus direct waar het antwoord op slaat).
    - het resultaat is 'uitgesteld, komt enige tijd later (de applicatie moet dan het antwoord bij de vraag zoeken) of wellicht helemaal niet. De applicatie of het business proces wachten niet.

Op basis van deze twee verschillen komen we tot vier primitieve business-interacties, 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. Combineren van deze primitieve interacties tot meerdere (eventueel over

de tijd verspreide interacties) maken complexe business-patronen mogelijk.

4.3.2 Digikoppeling-aanbod

Digikoppeling onderscheidt twee hoofdvormen van uitwisseling:

- bevraging (synchrone request-response)
- melding (asynchrone reliable messaging)

Bij een bevraging (vraag-antwoord) stuurt de service-requester een voorgedefinieerde vraag (request) aan de service-provider, die een antwoord (response) verstrekt. Het initiatief ligt bij de service-requester. Gaat er in de uitwisseling iets mis dan zal de service-requester na een bepaalde tijd de uitwisseling afbreken (time-out).
Bij een melding (betrouwbaar bericht) verstuurt de service-requester een betrouwbaar bericht (melding) naar de ontvangende partij (ontvanger) en wacht op een (technische) ontvangstbevestiging. De verzendende (business) applicatie vertrouwt er op dat het bericht (betrouwbaar) afgeleverd wordt. De (business)applicatie zal niet wachten op het antwoord: deze applicatie zal het eventuele 'antwoordbericht' op een ander moment ontvangen en moeten correleren aan het oorspronkelijke vraag bericht.

4.3.3 Invulling van de behoefte met het aanbod

Beide door Digikoppeling geboden uitwisselingsvormen moeten op de volgende wijze voor de eerder aangegeven vier primitieve business-interacties, toegepast worden.

	Onmiddellijk	**Uitgesteld**
Bevraging	Digikoppeling bevraging	Digikoppeling melding
Transactie	Digikoppeling melding[20]	Digikoppeling melding

Uit bovenstaande tabel blijkt dat de Digikoppeling bevraging niet identiek is aan de bevraging op business-niveau en dat de Digikoppeling melding niet identiek is aan de transactie op business-niveau.

Onmiddelijke bevraging

In deze situatie wordt altijd een Digikoppeling bevraging toegepast. Het onmiddelijke karakter, direct een response die automatisch gerelateerd wordt aan het request, is hier doorslaggevend voor. De betrouwbaarheid van een Digikoppeling melding is niet nodig.
Een typische toepassing voor deze vorm is een gebruiker die via een on-line web-applicatie informatie opvraagt aan een achterliggend systeem; de koppeling tussen de web-applicatie en het achterliggende systeem vindt dan met een Digikoppeling bevraging plaats.

Uitgestelde bevraging

In deze situatie wordt altijd een Digikoppeling melding toegepast. Het uitgestelde karakter , een antwoord komt later en hoeft niet automatisch gerelateerd te worden aan de vraag, is hier doorslaggevend voor. De betrouwbaarheid van een Digikoppeling melding is weliswaar niet nodig maar kan hier ook geen 'kwaad'.
Een typische toepassing voor deze vorm is een business-applicatie die

[20] *Soms kan ook een Digikoppeling bevraging toegepast worden. Zie toelichting.*

voor een interne (bijvoorbeeld batch) verwerking een actuele status uit een andere applicatie nodig heeft. De applicatie zal met andere verwerking verder gaan terwijl zolang geen antwoord ontvangen is. Een dergelijke situatie komt minder vaak voor.

Onmiddelijke transactie

In deze situatie wordt normaliter een Digikoppeling-melding toegepast. De betrouwbaarheid van de Digikoppeling melding is hier bepalend. In bijzondere situaties kan betrouwbaarheid ook anders geregeld worden (zie hieronder) maar algemeen wordt dat afgeraden.

Een typische toepassing voor deze vorm is een gebruiker die via een online web-applicatie informatie aanpast en deze aanpassing moet met zekerheid in een achterliggende registratie afgehandeld worden (bijvoorbeeld uitvoeren van een bank-overschrijving[21]). De koppeling tussen de web-applicatie en de achterliggende registratie verloopt via een Digikoppeling-melding.

Een uitzondering bestaat wanneer de service-requester dringend een response nodig heeft om verder te gaan. In dit geval geeft het onmiddelijke karakter de doorslag en zal betrouwbaarheid anders opgelost moeten worden. Aangeraden wordt echter om een andere proces-implementatie te kiezen[22].

Een typische toepassing voor deze vorm is een gebruiker die via een online web-applicatie informatie aanpast/toevoegt aan een achterliggende registratie en zekerheid moet hebben dat zijn input geaccepteerd wordt voordat hij verder kan[23]. De koppeling tussen de web-applicatie en de achterliggende registratie verloopt via een Digikoppeling-bevraging; de gebruiker zorgt voor de betrouwbaarheid door te bewaken dat er geen foutmelding optreedt en zonodig actie te nemen.

Uitgestelde transactie
In deze situatie wordt Digikoppeling melding toegepast. Zowel de betrouwbaarheid als het uitgestelde karakter zijn hier bepalend.
Een typische toepassing hiervoor is een batch-verwerkende applicatie die in een (andere) registratie veranderingen doorvoert.

Samenvatting
Een Digikoppeling bevraging is vooral geschikt als de (business) applicatie een onmiddelijke reactie nodig heeft. Een Digikoppeling melding is vooral geschikt voor uitgestelde verwerking en transacties.

4.3.4 Bevraging

Digikoppeling-bevragingen zijn synchroon : het vragende informatiesysteem wacht op een antwoord. Dit wachten heeft een beperkte duur (time-out). Als een (tijdig) antwoord uitblijft moet de vrager besluiten of hij de vraag opnieuw stelt of niet. De snelheid van afleveren is hier vaak belangrijker dan een betrouwbare aflevering.

---

[21] *N.B. ; Merk op dat in dit voorbeeld afhandelen geen garantie geeft op verwerking als er een saldo-tekort is op het moment van uitvoeren.*

[22] *Vaak kan ontkoppeld worden door onmiddellijk lokaal te registreren en de service-requester uitgesteld in de achterliggende registratie te laten verwerken.*

[23] *Vaak is deze afhankelijkheid van een achterliggende registratie ongewenst. Een andere vormgeving van het proces is mogelijk door invoer van gebruikers lokaal af te handelen en vervolgens off-line door te zetten naar een achterliggende registratie.*

Bevragingen worden ingericht op basis van de Digikoppeling-koppelvlakstandaard WUS.

4.3.5 Melding

Een melding is een enkelvoudig bericht waarop eventueel enige tijd later een retour-melding volgt. Het gebruikte protocol regelt de betrouwbare ontvangst en de onweerlegbaarheid (non-repudiation) van een bericht. Bij meldingen is de betrouwbare aflevering van het bericht essentieel. Als een partij het bericht niet direct kan aannemen, voorzien de protocollen erin dat het bericht nogmaals wordt aangeboden.
Meldingen kunnen worden ingericht op basis van de Digikoppeling-koppelvlakstandaard WUS of de Digikoppeling-koppelvlakstandaard ebMS.

4.3.6 Grote Berichten

De situatie kan zich voordoen dat een bericht een omvang krijgt die niet meer efficiënt door de Digikoppeling-adapters verwerkt kan worden bijvoorbeeld vanwege de overhead bij eventuele hertransmissies. Ook kan het voorkomen dat er behoefte bestaat aan het sturen van aanvullende informatie naar systemen buiten de normale procesgang ('out-of-band'). In die gevallen zal dit grote bestand op een andere wijze uitgewisseld moeten worden: middels de Digikoppeling Koppelvlakstandaard Grote Berichten.

Bij 'grote berichten' worden grotere bestanden uitgewisseld via een melding of een bevraging in combinatie met een (HTTPS-)download vanaf een beveiligde website. Grote berichten vormen een functionele uitbreiding op bevragingen en meldingen voor de veilige bestandsoverdracht van berichten groter dan 20 Mb.
Digikoppeling Grote Berichten maakt verschillende vormen van uitwisseling op business-niveau mogelijk. De best-practice beschrijft de volgende vormen:

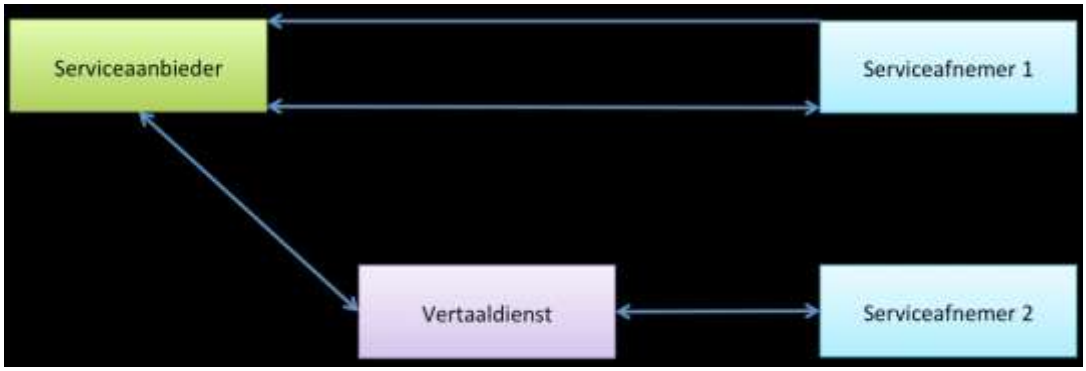
- Upload – grote hoeveelheid gegevens uploaden.
- Download – grote hoeveelheid gegevens downloaden.
- Selectie – een selectie van grote hoeveelheden gegevens verkrijgen.
- Verzending - grote hoeveelheid gegevens versturen.
- Multi-distributie - grote hoeveelheid gegevens aan meerdere ontvangers versturen.

4.4 Scenario's voor bevragingen en meldingen

4.4.1 Overzicht bevragingen en meldingen

Bij bevragingen hanteren partijen dezelfde koppelvlakstandaard (WUS[24]) en bevragen elkaar rechtstreeks. Voor een bevraging moet de service op het moment van bevraging beschikbaar zijn. Bij meldingen bestaat de mogelijkheid dat partijen verschillende koppelvlakstandaarden hanteren: de verzender wil een WUS-melding versturen terwijl de ontvanger ebMS gebruikt of andersom. Een vertaaldienst voorziet dan zo nodig in een protocolvertaling.

[24] *ebMS best effort mag binnen een sector worden gebruikt voor bevragingen (met een uitgesteld antwoord) indien partijen dit onderling overeenkomen.*



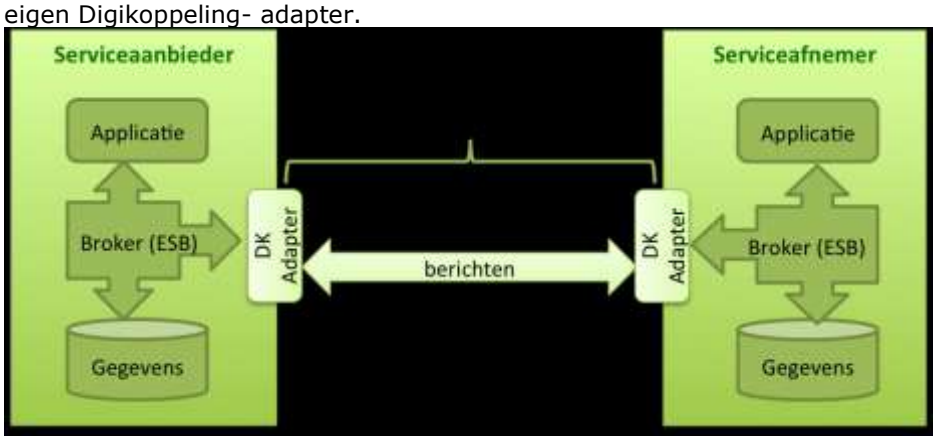
Figuur 4: Digikoppeling-bevragingen en -meldingen

Een melding (ebMS en WUS) wordt door de verzender verstuurd naar de ontvanger maar kan ook lopen via een transparante intermediair of via een vertaaldienst.
Er zijn dus de volgende mogelijkheden:

- Bilaterale uitwisseling tussen partijen
- Bilaterale uitwisseling via een transparante intermediair (zonder vertaaldienst)
- Meldingen via een vertaaldienst

4.4.2 Bilaterale uitwisseling tussen partijen

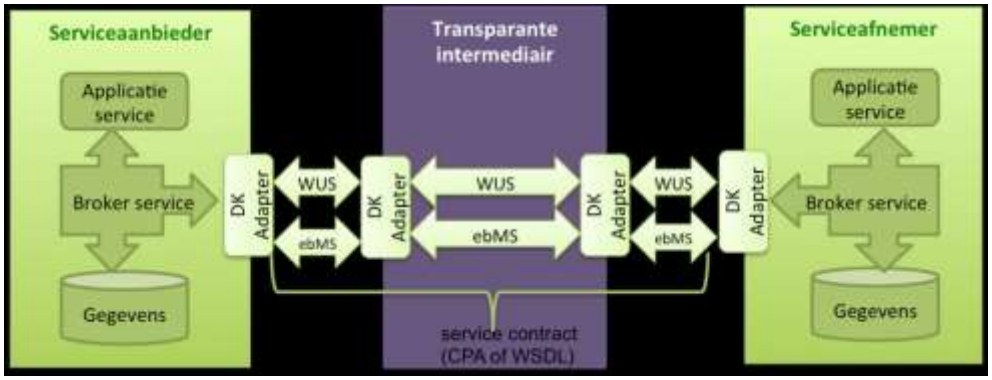
In het eenvoudigste patroon gebruiken de serviceaanbieder en serviceafnemer Digikoppeling rechtstreeks voor bevragingen of meldingen, eventueel in combinatie met grote berichten. Partijen stellen samen een (technisch) servicecontract op dat ingelezen kan worden in de eigen Digikoppeling- adapter.



Figuur 5: bilaterale uitwisseling

4.4.3 Bilaterale uitwisseling via een transparante intermediair (zonder vertaaldienst)

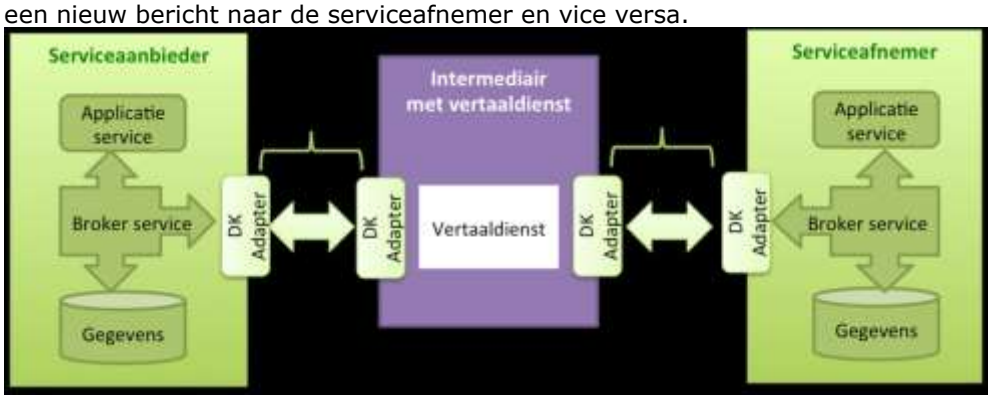
Een transparante keten is alleen mogelijk als zowel de service-aanbieder als de serviceafnemer hetzelfde protocol hanteren. De intermediair routeert berichten tussen de serviceaanbieder en de serviceafnemer waarbij het bericht intact blijft (alleen de header wordt gelezen). De uitwisseling verloopt op dezelfde manier als bij een bilaterale uitwisseling.



Figuur 6: Transparante intermediair

4.4.4 Meldingen via een vertaaldienst

Een partij kan gebruik maken van een intermediaire vertaaldienstvertaaldienst. Vertaaldiensten zullen in de praktijk vooral bij knooppunten worden belegd, al kunnen ze ook door serviceaanbieders of serviceafnemers worden uitgevoerd. De vertaaldienst opereert als verlengstuk van de serviceaanbieder en onder diens verantwoordelijkheid. De vertaaldienst vertaalt het bericht van de serviceaanbieder en verstuurt een nieuw bericht naar de serviceafnemer en vice versa.



Figuur 7: Digikoppeling-keten via een intermediair met vertaaldienst

5 Digikoppeling-koppelvlakstandaarden en voorschriften

5.1 Overzicht

Bevragingen en meldingen - eventueel in combinatie met grote berichten - bieden door hun verscheidenheid aan profielen en opties de logistieke bouwstenen om diverse interactiepatronen te realiseren. Digikoppeling heeft drie koppelvlakstandaarden onderkend die deze interactiepatronen ondersteunen:

- WUS voor bevragingen en meldingen[25].
- ebMS voor meldingen.
- Grote berichten voor het uitwisselen van grote bestanden.

Afnemers kunnen dus kiezen tussen WUS of ebMS als standaard koppelvlak voor meldingen. Aanbieders zoals basisregistraties en landelijke voorzieningen moeten beide protocollen ondersteunen of, als dat niet mogelijk is, voorzien in een protocolvertaling via een vertaaldienst[26]. Digikoppeling specificeert in de Translatiespecificatie de eisen die aan een protocolvertaling worden gesteld. Organisaties die een vertaaldienst aanbieden, moeten deze op basis van de Translatiespecificatie inrichten.
De Digikoppeling-koppelvlakstandaarden beschrijven verschillende profielen. Elk profiel biedt een combinatie van kenmerken die in een bepaalde functionele behoefte voorziet.

De volgende profielen zijn onderkend voor WUS en ebMS:

- Best effort – geschikt voor bevragingen
- Betrouwbaar (reliable) – geschikt voor meldingen

Deze komen in de volgende varianten voor:

- Standaard (niets) – best effort of reliable
- Signed – geschikt voor de ondertekening van berichten
- Encrypted – geschikt voor de versleuteling van de payload en attachments (bericht-niveau security)

Door het gebruik van deze profielen worden deze aspecten correct afgehandeld en kunnen partijen sneller een koppelvlakstandaard implementeren.

Onderdeel	Toelichting
Koppelvlakstandaard WUS	het gebruik van WUS voor bevragingen en meldingen en de WUS profielen.
Koppelvlakstandaard ebMS	Het gebruik van ebMS voor meldingen en de ebMS profielen
Koppelvlakstandaard Grote Berichten	Voor de uitwisseling van grote berichten maakt gebruik van WUS met HTTPS bestandsoverdracht of ebMS met HTTPS bestandsoverdracht
Translatiespecificatie	Beschrijft de beoogde werking van een vertaaldienst en de mapping van elementen tussen de protocollen ebMS en WUS.
Identificatie en	Beschrijft de identificatie van partijen, het opzetten

[25] *Digikoppeling ondersteunt WS-RM (Web Services Reliable Messaging Protocol) in de Digikoppeling-WUS Koppelvlakstandaard.*
[26] *Wanneer alle serviceafnemers hetzelfde protocol gebruiken, kan de serviceaanbieder zich beperken tot dat protocol. Een vertaaldienst is dan ook niet nodig.*

Authenticatie en Gebruik en Achtergrond Digikoppeling Certificaten	van een tweezijdige beveiligde TLS-verbinding en over het ondertekenen en versleutelen van berichten en bijlagen.

Tabel 3: Digikoppeling-standaarden

5.2 Digikoppeling-voorschriften

Enkele afspraken over de functionaliteit van Digikoppeling hebben betrekking op de Digikoppeling-keten als geheel waar behalve de koppelvlakstandaarden ook partijen, intermediairs, vertaaldiensten e.d. een onderdeel van vormen. . En voor elke keten geldt dat deze 'zo sterk is als de zwakste schakel'.
Onderstaande voorschriften gelden voor de hele Digikoppeling-keten. Partijen moeten er in hun eigen organisatie voor zorgen dat hun systemen, applicaties en toegang voor gebruikers aan de eisen voldoen.

Aspect	Voorschrift	Toepassing en uitleg
Identiteit, authenticatie en autorisatie	Identificatie en authenticatie van partijen maar ook intermediairs en vertaaldiensten vindt plaats in overeenstemming met het beleid hiervoor. Zowel service aanbieder als service afnemer moeten overeenkomstig afspraken autoriseren. De autorisatie gebeurt op organisatieniveau, niet op medewerkersniveau.	Beleid staat uitgewerkt in het document "Digikoppeling Identificatie en Authenticatie". Een praktische werkwijze is uitgewerkt in het document "Gebruik en achtergrond Digikoppeling certificaten". Autoriseren kan afhankelijk van noodzaak tweezijdig afgesproken worden. Immers bijvoorbeeld ook het stellen van een vraag kan al vertrouwelijk zijn.
Betrouwbaarheid en beschikbaarheid (reliability)	Alle componenten in de Digikoppeling-keten dienen de betrouwbaarheid en beschikbaarheid van het berichtenverkeer in de keten te handhaven, met name door het gebruik van een betrouwbaar profiel. Het gaat hier specifiek om de betrouwbare aflevering van berichten via reliable messaging (het gaat dus niet om de beschikbaarheid of betrouwbaarheid van de applicaties in de keten).	Een betrouwbaar profiel garandeert dat een bericht met zekerheid (precies één keer) wordt afgeleverd en dat berichten zo mogelijk in de juiste volgorde worden afgeleverd, ook als de ontvanger tijdelijk niet beschikbaar is. Tussenliggende intermediairs en vertaaldiensten maar ook de Digikoppeling-adapters bij de partijen zullen deze garanties moeten handhaven om zinvol toegepast te kunnen worden. Dit stelt eisen aan de inrichting en eventueel intern transport. Dit geldt met name voor de betrouwbare profielen.
Traceerbaarheid	De berichtenstroom is traceerbaar via elke schakel in de logisitieke keten.	Elke schakel in de Digikoppeling-keten moet inkomende en uitgaande berichten monitoren, loggen en moet voorzien in een audittrail. Dit geldt met name voor de betrouwbare profielen.

Foutafhandeling	Fouten worden correct en tijdig afgehandeld. Uitval van meldingen wordt zoveel mogelijk voorkomen, mede door het gebruik van een betrouwbaar profiel.	Elke schakel in de Digikoppeling-keten moet foutafhandeling inrichten. Dit geldt met name voor de betrouwbare profielen.

Tabel 4: Digikoppeling-voorschriften

5.3 WUS

5.3.1 WUS familie van standaarden

Digikoppeling maakt gebruik van een familie van standaarden die we binnen Digikoppeling de naam "WUS" geven. Deze familie van standaarden is gebaseerd op web-service standaarden uit de profielen van de OASIS "Web Services – Basic Reliable and Secure Profiles" Technical Committie (WS-BRSP)[27]. De naam WUS staat voor WSDL, UDDI en SOAP, drie belangrijke deelstandaarden. Hoewel Digikoppeling geen gebruik van UDDI maakt is deze term inmiddels gebruikelijk.
Kenmerkend voor de WUS-standaarden die voortkomen uit de Internet-wereld is de 1-op-n relatie tussen service aanbieder en meerdere service afnemers. Dit betekent b.v. dat een WUS service één WSDL heeft die door alle afnemers kan worden gebruikt.

5.3.2 WUS voor bevragingen

De Digikoppeling-koppelvlakstandaard WUS (KVS WUS) ondersteunt het uitvoeren van bevragingen tussen geautomatiseerde informatiesystemen.
De KVS WUS biedt de volgende functionaliteiten voor bevragingen:

- Identificatie en authenticatie van partijen
- Versleutelen van transport
- Adresseringsinformatie voor routering 'achter de voordeur'
- Routeren via message-handlers
- Berichtuitwisseling vast leggen in standaard technisch contract formaat
- Beveiligen van berichten d.m.v. technische handtekening
- Beveiligen van berichten door de content te versleutelen
- Foutmeldingen

5.3.3 WUS voor meldingen

De Digikoppeling-koppelvlakstandaard WUS (KVS WUS) ondersteunt het uitvoeren van meldingen tussen geautomatiseerde informatiesystemen.
De KVS WUS biedt de volgende functionaliteiten voor meldingen:

- Identificatie en authenticatie van partijen
- Versleutelen van transport
- Adresseringsinformatie voor routering 'achter de voordeur'
- Routeren via message-handlers
- Asynchroon berichten correleren d.m.v. message ID
- Meerdere berichten logisch samenvoegen
- Berichten voorzien van een beveiligde datum en tijd stempel (time-stamping)
- Berichtuitwisseling vast leggen in standaard technisch contract formaat (servicecontract)
- Beveiligen van berichten d.m.v. technische handtekening
- Beveiligen van berichten door de content te versleutelen
- Onweerlegbaarheid op protocolniveau (non-repudiation)

[27] *Voorheen Web Services Interoperability (WS-I) organization*

- Betrouwbaar asynchroon berichten versturen met ontvangstbevestigingen
- Ondersteuning voor foutafhandeling op asynchrone berichten
- Volgorde van berichten zo mogelijk handhaven
- Hertransmissies op protocolniveau totdat ontvangst is bevestigd

5.3.4 WSDL

Een WSDL is een formeel xml-document om de gebruikte functionele en technische eigenschappen van de berichtuitwisseling via WUS vast te leggen. Elke service heeft één WSDL, die door de serviceaanbieder wordt opgesteld. Deze is door alle afnemers te gebruiken. Door importeren van de WSDL in de Digikoppeling-adapter van een afnemer wordt de berichtuitwisseling geconfigureerd.
De wijze waarop een WSDL wordt toegepast staat beschreven in Digikoppeling Best Practices WUS.

5.4 ebMS

5.4.1 ebMS familie van standaarden

Digikoppeling maakt ook gebruik van een familie van standaarden die we "ebMS" noemen. Deze familie van standaarden is gebaseerd op web-service standaarden uit de profielen van de OASIS "ebXML Messaging Services" Technical Committie (ebMS).
Kenmerkend voor de ebMS-standaarden die voortkomen uit de EDIFACT-wereld is de 1-op-1 relatie tussen een beperkt aantal (vaak twee) partijen. Dit betekent dat twee partijen samen een CPA moeten afspreken, creëren en implementeren; de CPA is dus van zowel de serviceaanbieder als de serviceafnemer.

5.4.2 ebMS voor meldingen

De Digikoppeling-koppelvlakstandaard ebMS (KVS ebMS) ondersteunt het uitvoeren van meldingen tussen geautomatiseerde informatiesystemen. Het protocol regelt de betrouwbare ontvangst van een bericht en eventueel de onweerlegbaarheid (non-repudiation) in de vorm van een ondertekende ontvangstbevestiging. Hoewel Digikoppeling-meldingen (op de logistieke laag) asynchroon zijn kan de business-laag wel synchroon werken als de verzender wacht op een retour-melding.
De KVS ebMS regelt de volgende functionaliteiten voor meldingen:

- Identificatie en authenticatie van partijen
- Versleutelen van transport
- Adresseringsinformatie voor routering 'achter de voordeur'
- Routeren via message-handlers
- Asynchroon berichten correleren d.m.v. message ID
- Meerdere berichten logisch samenvoegen
- Berichten voorzien van een beveiligde datum en tijd-stempel (time-stamping)
- Berichtuitwisseling vast leggen in standaard technisch contract formaat (servicecontract)
- Beveiligen van berichten d.m.v. technische handtekening
- Beveiligen van berichten door de content te versleutelen
- Onweerlegbaarheid op protocolniveau (non-repudiation)
- Betrouwbaar asynchroon berichten versturen met ontvangstbevestigingen
- Ondersteuning voor foutafhandeling op asynchrone berichten
- Volgorde van berichten zo mogelijk handhaven
- Hertransmissies op protocolniveau totdat ontvangst is bevestigd

5.4.3 CPA

Een CPA is een formeel xml-document om de gebruikte functionele en technische eigenschappen van de ebMS protocol-karakteristieken vast te leggen. Het is dus een formele beschrijving voor het vastleggen van de gegevensuitwisseling. Een CPA moet worden gecreëerd als twee partijen afspreken om van elkaars ebMS services gebruik te maken. Beide partijen moeten de CPA importeren in hun Digikoppeling-adapter om deze te configureren voor de berichtuitwisseling.

De wijze waarop een CPA wordt toegepast staat beschreven in Digikoppeling Best Practices ebMS. De CPA Creatievoorziening ondersteunt partijen in het creëren van een CPA.

5.4.4 ebMS voor vragen met een uitgesteld antwoord

In sommige sectoren wordt een vraag verstuurd met ebMS en komt het (uitgestelde) antwoord ook via ebMS retour. Deze vorm van uitwisseling is asynchroon en voldoet dus niet aan de definitie voor bevragingen, omdat een bevraging synchroon is. Digikoppeling biedt hiervoor meldingen (ook ingeval van WUS). Bij dit type gebruik is de betrouwbaarheid eigenlijk overbodig. Het ebMS best effort profiel van de koppelvlakstandaard ebMS kan ook voor dit type vragen met uitgestelde antwoorden worden gebruikt, als partijen dit onderling afspreken. Dit gebruik wordt niet op landelijk of intersectoraal niveau toegestaan en is dus uitsluitend optioneel binnen sectoren.

5.5 Grote berichten

5.5.1 Werking grote berichten

Zoals eerder aangegeven kan de situatie zich voordoen dat een WUS en/of ebMS bericht een grootte krijgt die niet meer efficiënt door de WUS / ebMS adapters verwerkt kan worden. Ook kan het zich voordoen dat er behoefte bestaat aan het buiten de normale procesgang ('out-of-band') sturen van aanvullende informatie naar systemen. In die gevallen zal dit "grote bericht" op een andere wijze verstuurd moeten worden: middels de Digikoppeling-koppelvlakstandaard Grote Berichten.

De volgende standaard aanpak wordt hierbij gehanteerd:

- Met WUS of ebMS wordt referentie (link) verstuurd;
- de referentie wordt gebruikt om een groot bestand te downloaden.

Het grote bericht zelf zal vaak volledig in het grote bestand zijn opgenomen; het WUS of ebMS bericht bevat dan alleen metadata (waaronder de link naar het bestand). Maar het kan ook gebeuren dat een klein deel van het oorspronkelijk grote bericht al in het WUS-bericht is opgenomen en de rest (bijvoorbeeld bijlagen bij het bericht) in een of meerdere bestanden is opgenomen.

Het principe dat Digikoppeling grote berichten toepast is het 'claim-check' principe. Dit betekent dat het bericht zelf (WUS of ebMS) alleen een referentie (claim-check) naar het grote bestand bevat. Deze referentie wordt vervolgens gebruikt om het bestand zelf op te halen.

Een belangrijk voordeel hiervan is dat het grootste deel (het grote bestand zelf) de berichtenuitwisseling niet verstoort doordat het niet door de message-handler afgehandeld hoeft te worden (en deze bijvoorbeeld vertraagt). Maar ook is een voordeel dat de afhandeling van het grote deel op een ander moment in de tijd kan plaatsvinden en daardoor de procesgang van achterliggende informatiesystemen niet verstoord.

De standaard doet geen uitspraak over gegevensstromen waarin kleine en grote berichten voorkomen. Bij implementatie van dergelijke

gegevensstromen zal een organisatie moeten afwegen of kleine berichten anders of gelijk aan de 'echte' grote berichten verwerkt worden. In z'n algemeenheid zal een uniforme afhandeling eenduidiger en vooral ook eenvoudiger zijn; slechts in bijzondere gevallen zal dit niet volstaan.

5.5.2 Standaarden voor grote berichten

De *Digikoppeling Koppelvlakstaard Grote Berichten* (KVS GB) maakt gebruik van WUS en ebMS voor het verzenden van metadata. Voor ophalen van het grote bestand maakt de standaard gebruik van HTTPS-downloads. Daardoor zijn reliability en security gelijkwaardig aan WUS en eBMS. Ook is het gebruik van transparante intermediairs mogelijk.
De KVS GB regelt de volgende functionaliteiten voor meldingen of bevragingen, in aanvulling op WUS of ebMS:

- Identificatie en authenticatie van partijen (OIN)
- Versleutelen van transport
- Routeren via (http) proxies
- Bestand correleren aan bericht
- Ondersteuning voor foutafhandeling
- Na onderbreking hervatten waar de overdracht is afgebroken ('resume')
- Optioneel beperkte tijdsperiode om bestand beschikbaar te stellen.

5.6 Digikoppeling Translatiespecificatie

De Translatiespecificatie bevat voorschriften voor de protocolvertaling van ebMS-meldingen naar WUS-meldingen en andersom. De Translatiespecificatie wordt toegepast in een vertaaldienst. Partijen en ICT-leveranciers kunnen een vertaaldienst aanbieden mits deze voldoet aan de eisen en voorschriften van deze Architectuur en gebruik maakt van de Translatiespecificatie.

De Translatiespecificatie is opgesteld om te garanderen dat vertaaldiensten eenduidig omgaan met protocolvertalingen, zodat serviceaanbieders en serviceafnemers zeker weten dat relevante logistieke informatie behouden blijft.

WUS en ebMS meldingen hebben afwijkende headers. Om niet verloren te gaan moet logistieke informatie daarom worden overgezet tussen ebMS-headers en WUS-headers.

6 Digikoppeling-voorzieningen

6.1 Inleiding

Partijen zijn zelf verantwoordelijk voor de bereikbaarheid, inrichting van hun systemen en voor een correcte afhandeling van berichten. De consequentie is organisaties zelf hun deel van Digikoppeling moeten inrichten. Zij kunnen zich daarbij laten ondersteunen door ICT-leveranciers of een intermediair. Alle partijen kunnen gebruik maken van de Digikoppeling-voorzieningen.
De volgende Digikoppeling-voorzieningen ondersteunen het ontwikkel- en implementatieproces:

- Compliancevoorziening WUS en ebMS voor het testen van services
- CPA Creatievoorziening voor het creëren van een CPA contract (ebMS)
- Serviceregister voor het registreren van services en zoeken naar services

Digikoppeling adapters of applicaties kunnen worden getest op compliance met de koppelvlakstandaarden via de Compliancevoorziening. Nieuwe services kunnen op verzoek door Logius worden geregistreerd in het Serviceregister. Al deze voorzieningen zijn bereikbaar via www.digikoppeling.nl.

Functionaliteit	Uitleg	Invulling
Compliance WUS services	WUS services kunnen worden getest op compliance met de Digikoppeling-koppelvlakstandaard WUS.	Compliancevoorziening WUS
Compliance ebMS services	ebMS services kunnen worden getest op compliance met de Digikoppeling-koppelvlakstandaard ebMS.	Compliancevoorziening ebMS
Compliance Grote Berichten	Grote berichten kunnen in combinatie met WUS of ebMS services worden getest op compliance met de koppelvlakstandaarden	Compliancevoorziening WUS en Compliancevoorziening ebMS
Services publiceren en zoeken	Services kunnen worden geregistreerd en gezocht. Aanbieders kunnen services registreren t.b.v. vindbaarheid.	Serviceregister
CPA creatie	Een CPA-contract voor ebMS services kan via de CPA Creatievoorziening worden opgesteld tussen twee partijen.	CPA Creatievoorziening

Tabel 5: Ondersteunende functionaliteiten van de Digikoppeling-voorzieningen

6.2 Compliancevoorzieningen

Met de WUS compliancevoorziening kan een organisatie controleren of haar adapter of programmatuur voldoet aan de WUS koppelvlakstandaard. Met de ebMS compliancevoorziening kan een organisatie controleren of haar adapter of programmatuur voldoet aan de ebMS koppelvlakstandaard.

De volgende compliancevoorzieningen zijn beschikbaar: [28]

- Digikoppeling-WUS compliancevoorziening voor het testen van bevragingen en meldingen op basis van WUS, inclusief grote berichten.
- Digikoppeling-ebMS compliancevoorziening voor het testen van meldingen op basis van ebMS, inclusief grote berichten.

Informatie over de compliancevoorzieningen staat op http://www.digikoppeling.nl.

6.3 OIN register

Logius beheert het OIN register waarin uitgegeven Overheids identificatienummers zijn gepubliceerd. Dit register is openbaar raadpleegbaar. Het OIN register is onderdeel van het Digikoppeling Serviceregister en is te vinden op http://register.digikoppeling.nl.

6.4 Serviceregister[29]

Logius stelt een Serviceregister beschikbaar waarin informatie over landelijke services kan worden opgenomen. Het Serviceregister verbetert de vindbaarheid van services door ze te registreren en te ontsluiten. Logius registreert en beheert deze services.

Het Serviceregister bevat algemene informatie over services zoals de servicenaam, omgeving, status, organisatie, contactpersonen, relevante documentatie en het endpoint van de service.

6.5 CPA Creatievoorziening

De CPA Creatievoorziening wordt gebruikt voor het opstellen van een CPA (servicebeschrijving) voor ebMS uitwisselingen. Een CPA is een formeel xml-document dat de functionele en technische eigenschappen van de ebMS-protocolkarakteristieken vastlegt. Het is dus een format voor afspraken over de gegevensuitwisseling met ebMS.[30]

De CPA Creatievoorziening ondersteunt partijen bij het maken van een CPA (Collaboration Protocol Agreement). Een CPA kan om verschillende redenen zinvol zijn:

- Het is een formeel contract tussen twee partijen die op basis van ebMS gegevens willen uitwisselen.
- Het automatiseert de configuratie van de ebMS adapter (het inlezen van de CPA volstaat).
- Het biedt zekerheid dat beide partijen dezelfde instellingen gebruiken.

De wijze waarop een CPA wordt toegepast staat beschreven in Digikoppeling 2.0 Best Practices ebMS. De CPA Creatievoorziening is beschreven in de Gebruikershandleiding.

---

[28] *Digikoppeling 3.0 Koppelvlakstandaard WUS*
[29] *Digikoppeling 2.0 Architectuur*
[30] *Digikoppeling 2.0 Best Practices ebMS*

7 Vertaaldienst

Een vertaaldienst verzorgt vertalingen van meldingen tussen WUS en ebMS. Dit wordt uitgevoerd namens de serviceaanbieder. Een vertaaldienst kan door een overheidsorganisatie, een sectoraal knooppunt of een ICT-leverancier worden ingericht.
Hieronder staan de eisen aan een vertaaldienst. De translatiespecificatie gaat dieper in op de eisen aan de protocolvertaling door een vertaaldienst.

7.1 Toelichting op End-to-End

*End-to-end is in de context van Digikoppeling van **systeem-tot-systeem**; vanuit een procesperspectief is end-to-end van applicatie tot applicatie.*

Omdat Digikoppeling over systeem-tot-systeem berichtenverkeer gaat worden bepaalde aspecten die op applicatieniveau worden geregeld hier niet nader uitgewerkt. Voor een goede werking van het berichtenverkeer zullen deze aspecten door de partijen nader moeten worden ingevuld. Datzelfde geldt ook voor beveiligingsaspecten. Informatiebeveiligingseisen en risico's dienen op procesniveau voor de gehele keten te worden geanalyseerd. Dit valt buiten de scope van dit document.

7.2 Hoe werkt een vertaaldienst?

Een vertaaldienst gebruikt de Translatiespecificatie als voorschrift om reliable WUS-berichten te vertalen naar ebMS en omgekeerd. Het gaat om een protocolvertaling, de inhoud van een bericht wordt niet vertaald.
ebMS en WUS hebben afwijkende headers. Bij protocolvertaling tussen ebMS en WUS is het daarom niet mogelijk om op protocolniveau een transparante keten (dus zonder wijziging aan berichten) over de vertaaldienst heen te realiseren.Omdat er sprake is van een protocolvertaling, moeten bepaalde eisen die anders op protocolniveau worden geregeld op een andere manier worden geborgd.
Bij het gebruik van een vertaaldienst zijn er twee mogelijkheden om te voldoen aan de eisen t.a.v. beveiliging en vertrouwelijkheid voor de gehele Digikoppeling-keten:

1. De vertaaldienst kan zelf vertrouwd worden door de partijen.
2. Partijen maken gebruik van ondertekening en/of versleuteling van de berichtinhoud zelf als tussenliggende schakels in de Digikoppeling-keten niet vertrouwd zijn.

Een vertaaldienst werkt als volgt:

- De vertaaldienst ontvangt het bericht en pakt het uit.
- De vertaaldienst neemt relevante informatie uit de headers over en voegt die informatie toe aan nieuwe headers voor het uitgaande protocol, overeenkomstig de vertaalspecificatie.
- De vertaaldienst pakt het bericht opnieuw in, met de nieuwe headers, maar bemoeit zich niet met de inhoud van het bericht (payload en attachments).
- Het nieuwe bericht wordt desgewenst door de vertaaldienst digitaal ondertekend en versleuteld.
- Het nieuwe bericht wordt door de vertaaldienst verstuurd.

Indien de applicatie de payload al versleuteld heeft dan laat de vertaaldienst deze versleuteling intact.

7.3 Eisen aan een vertaaldienst

De architectuurkeuzes van de Digikoppeling-keten hebben consequenties voor een vertaaldienst. Een vertaaldienst:

- Legt afspraken vast in serviceovereenkomsten (inclusief bewerkersovereenkomsten en aansluitvoorwaarden), en contracten met serviceaanbieders en serviceafnemers.
- Heeft een eigen identiteit, dus een eigen identificatienummer (identificatie) en een eigen PKIoverheid certificaat (authenticatie).
- Voert periodiek risicoanalyses uit op zijn complete dienstverlening en neemt passende maatregelen op het gebied van informatiebeveiliging.
- Maakt gebruik van de Translatiespecificatie om een fijnmazig verband te configureren tussen de servicedefinities (WSDL of CPA) van de koppelvlakstandaarden waartussen de protocolvertaling plaatsvindt.[31]
    - Geeft de identiteit van verzender en ontvanger door in de berichtheaders.
    - Zorgt ervoor dat het eindresultaat op applicatieniveau hetzelfde is als wanneer dat bericht zonder vertaaldienst zou zijn verstuurd.
    - Voldoet aan de afgesproken beschikbaarheid en performance-eisen.
    - Voorziet in foutafhandeling.
    - Voorziet in sleutelbeheer en beveiliging van sleutels.
- Voorkomt dat berichten verloren gaan door berichten tijdelijk op te slaan:
    - Een bericht is pas betrouwbaar afgeleverd als de ontvanger een ontvangstbevestiging heeft gestuurd en die door de vertaaldienst is ontvangen. Een vertaaldienst moet deze ontvangstbevestiging afwachten voordat het bericht verwijderd mag worden.
    - Houdt bij of er voor meldingen technische ontvangstbevestigingen zijn aangekomen en voorziet in een signalering naar zowel verzender als ontvanger als het bericht niet bij de ontvanger is aangekomen (er is geen ontvangstbevestiging ontvangen van de ontvanger). Afhankelijk van afspraken kan deze signalering ook periodiek en/of via schriftelijke rapportages plaatsvinden.

De volgende functionele eisen worden gesteld aan vertaaldiensten in het algemeen:

- Een vertaaldienst ontvangt, vertaalt en verstuurt berichten:
    - Kan een eventuele ondertekening hiervan valideren.
    - Kan een eventuele versleuteling hiervan ontcijferen.
    - Kan een berichtheader lezen.
    - Kan een bericht omzetten naar een ander protocol.
    - Kan een bericht genereren.
    - Kan een bericht ondertekenen.
    - Kan een bericht versleutelen.
    - Kan een bericht valideren.
    - Kan een bericht versturen.
    - Kan berichtvolgorde handhaven[32].

[31] Zie het document Digikoppeling 3.0 Translatiespecificatie.

[32] Het is mogelijk om berichtvolgorde op protocolniveau te regelen, maar dit is doorgaans een ingewikkelde oplossing. Het is aan te raden om berichtvolgorde aan te geven door middel van berichtvolgnummers of iets vergelijkbaars. Dit kan door partijen onderling worden afgesproken.

- Een vertaaldienst heeft logging, monitoring en een audittrail ingericht en:
    - Registreert individuele berichten in de audittrail op datum en tijdstip/sequence of conversation id/message id/ontvangstbevestiging, evt. foutcodes, en indien beschikbaar de elektronische handtekening.
    - Voorziet in timestamping van alle transacties.
    - Stelt de audittrail van het knooppunt beschikbaar aan de betrokken partijen in de keten.
    - Voorziet in autorisatie voor toegang tot de audittrail. De audittrail zelf is niet wijzigbaar.
    - Voorziet in een exportmogelijkheid voor het exporteren van logfiles, audittrails en andere rapportages[33].
    - Neemt maatregelen om te waarborgen dat de audittrail niet kan worden gewijzigd.
- Een vertaaldienst ondersteunt bewaartermijnen:
    - Opgeslagen berichten worden opgeslagen voor zolang als nodig is om te waarborgen dat het bericht correct is verzonden en ontvangen en dit te kunnen controleren.
    - De audittrail wordt opgeslagen voor zolang als nodig is voor de auditdoeleinden zoals die met partijen zijn overeengekomen.

Naast de bovenstaande eisen zijn de volgende management en beheerfuncties belangrijk bij het inrichten van een vertaaldienst:

- Voorziet in beheerfuncties voor het beheren van de vertaaldienst.
- Voorziet in configureerbare management rapportages.
- Voorziet in autorisatie van beheerders (role-based access control).
- Voorziet in back-up en restore functionaliteit.

7.4 End-to-end identity en authenticatie

Een vertaaldienst heeft een eigen identiteit (dus een eigen identificerend nummer en PKIoverheid certificaat) voor het versleutelen en ondertekenen van berichten.
Dit is nodig omdat het werken met certificaten van verzender en ontvanger door een vertaaldienst als onwerkbaar en onwenselijk wordt gezien. Dit zou inhouden dat de vertaaldienst over het private PKIoverheid certificaat van zowel verzender als ontvanger moet beschikken. Dit vergt een sluitende administratie en beheer van alle toevertrouwde certificaten. Bovendien is de essentie van dit vraagstuk er een van vertrouwen en herkenbaarheid. Als de vertaaldienst ondertekent met het certificaat van de aangesloten dienst, dan is de vraag wie deze dienst feitelijk uitvoert moeilijker te beantwoorden. Bovendien moet de verbinding tussen verzender en vertaaldienst ook worden beveiligd. Het alternatief is dat het vertrouwen tussen partijen wordt afgesproken op business niveau waarbij de vertaaldienst een eigen certificaat en identiteit gebruikt. Dit dient tevens juridisch te worden afgesproken.

7.5 End-to-end security

End-to-end security gaat over de beveiliging van het berichtenverkeer gedurende het transport in de keten van systeem tot systeem. Daarbij gelden de volgende uitgangspunten:

[33] Indien gewenst moet het mogelijk zijn om de audittrail via een derde partij te laten verlopen, opslaan, of auditen.

- Partijen maken onderling afspraken over de organisatorische en procesmatige beveiliging van het berichtenverkeer.
- De partij die een vertaaldienst aanbiedt zorgt voor de technische, organisatorische en procesmatige beveiliging van de vertaaldienst.
- Headers worden zo nodig ondertekend (dit geldt alleen voor signed profielen).
- De berichtinhoud wordt zo nodig als geheel (met bijlagen) versleuteld. Indien berichten via de vertaaldienst worden vertaald dient de versleuteling door de verzender plaats te vinden met de public key van de vertaaldienst.
- Wanneer partijen de berichten inhoudelijk willen versleuteling zonder tussenkomst van een vertaaldienst dan moet de versleuteling op applicatieniveau door de verzender en ontvanger worden geregeld i.p.v. op protocolniveau. Dit is niet gestandaardiseerd door Digikoppeling en partijen dienen hier samen afspraken over te maken.

7.6 End-to-end Betrouwbaarheid

Een betrouwbaar profiel garandeert dat een bericht met zekerheid (slechts één keer) wordt afgeleverd en dat berichten zo mogelijk in de juiste volgorde worden afgeleverd, ook als de ontvanger tijdelijk niet beschikbaar is.

- Een vertaaldienst moet bij meldingen ook zorgen voor een interne betrouwbare verwerking van berichten en protocolvertalingen. Dit vereist monitoring, logging van berichten en ontvangstbevestigingen, persistente storage (opslag van berichten), procedurele afspraken over uitval van berichten (berichten die de ontvanger niet bereiken) en aanvullende service level afspraken hierover.
- Technische ontvangstbevestigingen (acknowledgements) worden door een vertaaldienst bijgehouden/aangeboden.
- Functionele ontvangstbevestigingen zijn geen onderdeel van de protocol en derhalve ook geen onderdeel van de Digikoppeling standaard.

8 Implementatie van Digikoppeling

8.1 Architectuuraspecten van de aansluiting op Digikoppeling

Om gebruik te maken van Digikoppeling zijn een aantal zaken van belang. Zo dient u met uw partners afspraken te maken over de gegevensuitwisseling die via Digikoppeling plaats vindt. Ook dient u in uw organisatie een Digikoppeling-adapter te implementeren waarmee de koppelvlakken worden ingericht. Deze alinea beschrijft enkel de architectuur-aspecten van de aansluiting op Digikoppeling. Meer informatie over de aansluiting zelf vindt u op www.logius.nl/digikoppeling.

8.1.1 Afspraken over de inhoud en interactie van de uitwisseling

Om tot uitwisseling van gegevens te kunnen komen, moeten de uitwisselende partijen afspraken maken over de inhoud en vorm van de gegevensuitwisseling.
Denk hierbij aan de volgende onderwerpen:

- Welk doel heeft de gegevensuitwisseling?
- Welke gegevens worden uitgewisseld?
- Wie is de bronhouder van de gegevens?
- Hoe verloopt de gegevensuitwisseling? Worden gegevens bilateraal uitgewisseld of via een intermediair of knooppunt?
- Welke vorm van interactie wordt gebruikt? Meldingen, bevragingen en/of grote berichten?
- Zijn de service contracten tussen de partijen gedefinieerd?
- Zijn de berichten gedefinieerd?
- Is er sprake van grote berichten (bestanden groter dan 20Mb)?
- Worden er bijlagen meegestuurd?
- Zijn de eindpunten (endpoints) gedefinieerd?
- Maken de partijen gebruik van hetzelfde protocol? Indien nee, hoe wordt voorzien in de protocolvertaling?
- Welke profielen worden toegepast?
    - Betrouwbare (reliable)?
    - Ondertekend (signed)?
    - Versleuteld (encrypted)?
- Hoe worden berichten binnen de organisatie geadresseerd en gerouteerd?
- Gebruiken beide partijen dezelfde codering en karakterset (UTF-8 of Unicode)?
- Beschikken de betrokken partijen over elkaars publieke PKIoverheid sleutel?

8.1.2 Digikoppeling-adapter

Organisaties die beschikken over eigen middleware (een enterprise servicebus, een broker of message handler, of een maatwerk applicatie) kunnen de Digikoppeling aansluiting in het algemeen realiseren door de juiste configuratie van deze producten. Anderen kunnen eenvoudig een van de vele Digikoppeling-adapters die in de markt worden geleverd aanschaffen.

ICT-leveranciers leveren standaard producten en/of diensten voor Digikoppeling. Ook bestaan er open source-oplossingen. Meestal bieden deze producten een Digikoppeling-adapter die vaak automatisch kan worden geconfigureerd conform de eisen van de Digikoppeling-koppelvlakstandaarden en Digikoppeling-profielen.

Per berichtuitwisseling moet worden bepaald welk profiel het meest geschikt is. Als het profiel is gekozen (meestal door de serviceaanbieder) kan de keuze in een servicebeschrijving worden vastgelegd. Deze servicebeschrijving kunnen serviceaanbieder en (meerdere) serviceafnemers gebruiken om hun Digikoppeling-adapter automatisch te configureren. De volgende paragrafen gaan verder in op profielen en servicebeschrijvingen.

8.1.3 Selectie van profielen

Vanwege interoperabiliteit, eenvoud en overzichtelijkheid onderscheidt Digikoppeling per koppelvlakstandaard een aantal standaardprofielen. Elk profiel bestaat uit vooraf gedefinieerde keuzen over kenmerken als synchroniciteit, beveiliging en betrouwbaarheid voor WUS of ebMS. Door toepassing van de Digikoppeling profielen worden deze kenmerken correct afgehandeld en kunnen partijen sneller een koppelvlakstandaard implementeren. De profielen worden nader gespecificeerd in de koppelvlakstandaarden WUS en ebMS.

De volgende kenmerken zijn onderkend voor WUS en ebMS:

- Best effort – geschikt voor bevragingen
- Betrouwbaar (reliable) – geschikt voor meldingen
- Signed – geschikt voor de ondertekening van berichten
- Encrypted – geschikt voor de versleuteling van de payload en attachments

De aanduiding van de profielen kent de volgende systematiek:

- 2W = two-way
- be = best-effort
- rm = reliable
- S of s =signed
- SE of e =signed en encrypted
- osb= overheidsservicebus, de oude naam van Digikoppeling

Invulling voorschriften	WUS-profielen	ebMS-profielen
Bevragingen		
best-effort	2W-be	osb-be
best-effort signed	2W-be-S	osb-be-s
best-effort signed/encrypted	2W-be-SE	osb-be-e
Meldingen		
reliable	2W-R	osb-rm
reliable signed	2W-R-S	osb-rm-s
reliable signed en encrypted	2W-R-SE	osb-rm-e

Tabel 6: Profielen in relatie tot Digikoppeling-voorschriften

NB: De profielnamen komen uit eerdere versies van de koppelvlakstandaarden. Zij moeten gehandhaafd blijven in verband met het feit dat deze standaarden reeds in gebruik zijn bij vele organisaties. Dit verklaart de verschillen in de gebruikte afkortingen tussen de WUS- en ebMS-profielen.

Neem de volgende aspecten mee bij de keuze van een profiel:

- Gaat het om berichten (of bijlagen) groter dan 20Mb? Kies dan voor Grote Berichten.
- Is snelheid belangrijker dan betrouwbaarheid? Kies dan voor bevragingen.
- Is betrouwbaarheid belangrijker, kies dan voor meldingen.
- Bevind zich tussen partijen een niet vertrouwde (transparante) intermediair? Kies dan voor een Signed profiel.
- Mag een niet vertrouwde intermediair informatie niet inzien? Kies dan voor een Encyrpted profiel.
- Gebruikt de verzender een ander protocol, kies dan voor een vertaaldienst.

8.1.4 Servicebeschrijvingen

De berichtuitwisseling wordt vormgegeven door services. Een service bestaat uit een servicebeschrijving (een servicecontract) en berichtdefinitie waarmee de inhoud van een bericht is gespecificeerd. Deze worden op voorhand tussen partijen afgesproken en uitgewerkt.

De servicebeschrijving bevat de gemaakte afspraken over de kwaliteit en vorm van uitwisseling. De berichten zelf zijn in een technisch formaat (XML) beschreven. Servicebeschrijvingen worden opgesteld door een serviceaanbieder (bijvoorbeeld een basisregistratie) en via het Serviceregister beschikbaar gesteld aan gebruikers om hun Digikoppeling-adapter te configureren.

Een servicecontract voor een ebMS service heet een CPA. Dit contract wordt afgesloten tussen de serviceaanbieder en serviceafnemer. Een CPA moet worden gecreëerd via de CPA-creatievoorziening en wordt daarna ingelezen in de systemen van de serviceaanbieder en serviceafnemer.

Een servicecontract voor een WUS service heet een WSDL. Dit contract wordt afgesloten tussen de serviceaanbieder en serviceafnemer(s). Een WSDL voor een bevraging kan door meerdere afnemers worden gebruikt. Een WSDL kan door een aanbiedende partij worden opgesteld.

8.1.5 Gebruik van de Digikoppeling voorzieningen

Digikoppeling bestaat uit een set diensten, afspraken en ondersteunende voorzieningen. Die positionering bepaalt de manier waarop Digikoppeling omgaat met het verschil tussen productie en test.

Digikoppeling-voorzieningen ondersteunen het ontwikkelproces en maken daarom geen onderscheid tussen productie en test[34]. In de berichtuitwisseling moeten organisaties hier wel onderscheid in maken. Wanneer er op een generieke infrastructurele component TLS-terminatie plaatsvindt, zal er in het algemeen slechts met productiecertificaten kunnen worden gewerkt. Dergelijke componenten worden ingezet voor zonering tussen niet-vertrouwde, semi-vertrouwde en vertrouwde netwerkzones. Keten- of pre-productietesten zullen in het algemeen gebruik kunnen maken van generieke infrastructuur.

Daarom geldt:

- De Digikoppeling-voorzieningen zijn bedoeld om te ondersteunen gedurende de ontwikkel- en testperiode.

[34] *Voorzover het de voorzieningen betreft die voor partijen benaderbaar zijn.*

- Certificaten voor productie wijken af van certificaten voor test doordat zij op verschillende 'roots' zijn gebaseerd, respectievelijk 'PKI root Staat der Nederlanden' en 'PKI TRIAL root'.
- Digikoppeling-koppelvlakstandaarden gelden (uiteraard) voor zowel productie als test.
- Het Digikoppeling Serviceregister bevat de informatie van/over productie- en testservices (voor zover extern zichtbaar).

8.2 Relatie met de inhoudelijke laag

8.2.1 Waarom

Deze paragraaf legt zeer beknopt een relatie met de inhoudelijke laag van gegevensuitwisseling en beschrijft welke aspecten door partijen geregeld moeten worden om met Digikoppeling te kunnen werken. Digikoppeling is niet afhankelijk van deze laag maar het gebruik van Digikoppeling heeft weinig nut als deze aspecten niet zijn geregeld.

8.2.2 Informatiebeveiliging

Partijen dienen zelf hun informatiebeveiliging vorm te geven en maatregelen te implementeren in de samenwerking met andere partijen. Daarbij dient rekening te worden gehouden met de keten van partijen, waaronder eventuele intermediairs (met of zonder vertaaldienst). In de samenwerking dienen duidelijke afspraken te worden gemaakt met bewerkers over de verwerking van gegevens en over de maatregelen die hierin genomen dienen te worden.

8.2.3 Bedrijfsprocessen

Partijen definiëren de uitwisseling tussen bedrijfsprocessen vanuit de optiek van de gebruiker en de vereiste doelbinding. Interoperabiliteit op bedrijfsprocesniveau vindt plaats bij de partijen zelf.

8.2.4 Applicatielaag

Het gebruik van gegevens uit andere bronnen wordt intern binnen een organisatie op applicatieniveau vormgegeven. Sommige aspecten, zoals de versleuteling van berichten, kunnen via de applicatielaag worden ingeregeld indien gewenst.

8.2.5 Berichtinhoud en semantiek

Digikoppeling gaat over de uitwisseling van berichten. Binnen Digikoppeling wordt een bericht conform de SOAP[35] messaging protocol samengesteld.
Een bericht bestaat uit de volgende onderdelen:

- Een bericht header (envelop)
- Een bericht payload (inhoud)
- Attachments (bijlagen)

Een bericht voldoet aan de volgende eisen:

- Alle berichten, zowel WUS als ebMS, hebben een unieke identificatie. De gekozen structuur is geldig in de ebMS-omgeving en in de WUS-omgeving. Zo kan dezelfde berichtidentificatie gebruikt worden in 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.
- De payload van een bericht moet beschreven zijn in valide XML36

[35] SOAP (Simple Object Access Protocol) is een computerprotocol dat wordt gebruikt voor communicatie tussen verschillende componenten van systemen.
[36] *Attachments mogen andere formaten hebben.*

- Er moet een contract zijn met de afspraken over de te gebruiken services.
- Het gebruik van een standaard karakterset en standaard codering is verplicht.

Partijen maken onderling afspraken over de semantiek van de payload. Berichtdefinities worden door partijen in overleg opgesteld. De semantische interoperabiliteit (d.w.z. de betekenis van de inhoud) wordt door partijen geborgd door zoveel mogelijk gebruik te maken van (bestaande) gegevensregisters, woordenboeken of catalogi. De standaarden StUF, Suwi-ML en NEN3610 zijn veelgebruikt hiervoor.

8.2.6 Karakterset en codering

De karakterset en codering is in feite een zaak van de 'inhoud' en niet van de logistieke laag. Maar om interoperabiliteit te ondersteunen wordt door Digikoppeling voor alle uitwisselingen het gebruik van UTF-8 voor de codering voorgeschreven.
Voor de karakterset beperkt Digikoppeling zich tot Unicode 2.0 (ISO/IEC 10646), een brede internationale standaard. Niet alle applicaties kunnen de volledige set ondersteunen. Er zullen dus onderling afspraken gemaakt moeten worden over het gebruik van een eventuele subset van de karakterset.

8.3 Relatie met de transportlaag

8.3.1 Randvoorwaarden transport

Digikoppeling stelt ook randvoorwaarden op het niveau van het transport:

- Gebruik van http
- Gebruik van TCP/IP stack.
- Gebruik van HTTPS voor grote berichten.
- Gebruik van tweezijdig TLS voor het veilig transporteren van gegevens via internet (bevragingen en meldingen) is verplicht.

Randvoorwaardelijk wil zeggen dat bovenstaande standaarden nodig zijn om Digikoppeling-koppelvlakstandaarden te kunnen gebruiken.

8.3.2 Waarom

Deze paragraaf legt zeer beknopt een relatie met de beoogde oplossing voor de landelijke voorzieningen op de transportlaag. Die transportlaag regelt de TCP/IP-verbinding, wat geen onderdeel is van Digikoppeling. Dit is echter opgenomen om aan te geven waar deze lagen elkaar raken. Digikoppeling stelt enkele basale eisen aan het transport; deze zijn in deze paragraaf opgenomen.

8.3.3 Transport Level Security (TLS)

Zowel de Digikoppeling-koppelvlakstandaard ebMS als de Digikoppeling-koppelvlakstandaard WUS en Digikopppeling-koppelvlakstandaard Grote Berichten schrijven het gebruik voor van (tweezijdig) TLS om de berichtenstroom te beveiligen. Het protocol TLS heeft betrekking op het communicatiekanaal. De Digikoppeling-koppelvlakstandaarden stellen deze eis dus aan de transportlaag.
In Digikoppeling is ervoor gekozen om PKIoverheid certificaten te gebruiken op het niveau van het communicatiekanaal (TLS) om de directe communicatiepartners te authenticeren (enkele hop). TLS kan niet toegepast worden om end-to-end authenticatie uit te voeren in een multi-hop omgeving; zie daarvoor berichtniveau beveiliging.

8.3.4 Netwerken

Digikoppeling is onafhankelijk van het onderliggende transportnetwerk. Gegevensuitwisseling via Digikoppeling stelt wel enkele eisen aan het transport:

- Digikoppeling is gebaseerd op de TCP/IP stack, dus een TCP/IP transportnetwerk is noodzakelijk.
- Standaarden zijn gebaseerd op 'bindings' – verbindingen of connecties - naar Uniform Resource Identifiers (URI's). Het netwerk moet de 'DNS resolving' [37]van de domeinnaam uit de URI regelen en de routering naar het resulterende IP-adres. Het netwerk en/of DNS-resolving mag ook een lokaal netwerk/host zijn.
- Digikoppeling past SOAP over HTTPS toe. De netwerken (en firewalls) zullen daarom https-transport over TCP/IP moeten toestaan.

Om goed te functioneren heeft Digikoppeling dus alleen basale connectiviteit nodig.

8.3.5 Diginetwerk

Diginetwerk levert de noodzakelijke beveiligde connectiviteit om elektronisch samen te kunnen werken met andere overheidsorganisaties via één standaard koppeling.
Diginetwerk bestaat uit een aantal gekoppelde besloten (koppel)netwerken van diverse samenwerkende overheden die met elkaar worden verbonden door een centrale voorziening (basiskoppelnetwerk). Voorbeelden van nationale koppelnetwerken zijn Gemnet, Suwinet en RINIS. Een internationaal koppelnetwerk is sTESTA. Organisaties die Diginetwerk willen gebruiken sluiten aan op een van de koppelnetwerken. Daarmee kunnen zij alle andere aangesloten organisaties bereiken.
Het voordeel daarvan is dat beschikbaarheid en beveiliging onder eigen beheer valt en dat toegang tot het netwerk gecontroleerd is. Door hergebruik van de aansluiting op Diginetwerk is de implementatie van connectiviteit met andere overheidsorganisaties eenvoudig te realiseren. Diginetwerk biedt een beheerde en afgesloten netwerk voor overheden en is dus een goed alternatief (t.o.v. internet) voor connectiviteit binnen de overheid.

8.3.6 Internet

Internet is een openbaar netwerk waarop velen zijn aangesloten. Het gebruik van TLS en optioneel beveiliging op berichtniveau door Digikoppeling maakt dat het internet goed gebruikt kan worden.
Het voordeel van Internet is dat veel organisaties een aansluiting hierop hebben. Vaak zijn organisaties met vertrouwelijke gegevens en hoge eisen t.a.v. beschikbaarheid en beveiliging terughoudend in het gebruik van Internet hiervoor. Hoewel dus veel organisaties bereikbaar zijn via Internet is toegang tot gegevens niet altijd mogelijk.
De precieze verschillen tussen Diginetwerk en Internet vallen buiten de scope van Digikoppeling en worden hier niet verder beschreven.

[37] *DNS 'resolving' is het opzoeken van de domeinnaam en het bijbehorend IP-adres, conform het DNS protocol.*

Bijlage A: Bronnen

Digikoppeling documentatie
Onderstaande diagram geeft aan hoe de Digikoppeling-standaarden zijn opgebouwd (van globaal naar specifiek). De Best Practices zijn geen onderdeel van de standaarden maar bieden ondersteuning bij het gebruik van de standaarden.

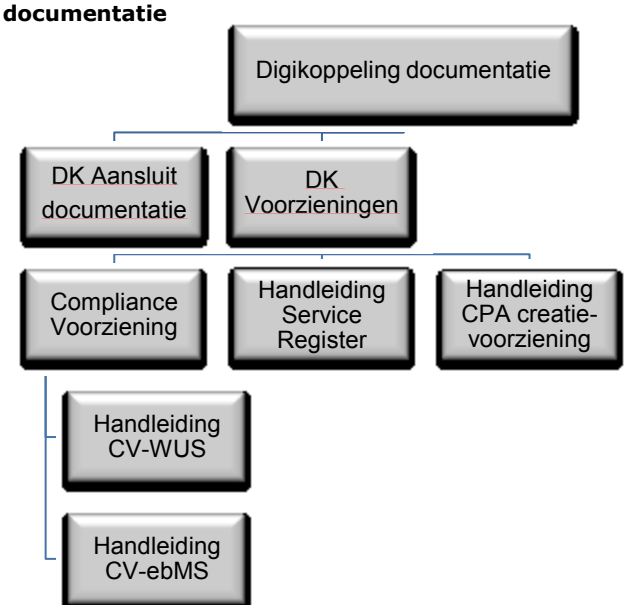
Alle goedgekeurde Digikoppeling documenten zijn beschikbaar op www.logius.nl/digikoppeling.

Digikoppeling-standaarden en gerelateerde documenten

Documentnaam	Auteur(s)	Status
Digikoppeling Identificatie en Authenticatie	Servicecentrum Logius	Definitief
Gebruik en achtergrond Digikoppeling certificaten	Servicecentrum Logius	Definitief
Koppelvlakstandaard WUS voor Digikoppeling 3.0	Servicecentrum Logius	Definitief
Best Practices WUS Digikoppeling 3.0	J. Li	Definitief
Koppelvlakstandaard ebMS: Digikoppeling 2.0	Servicecentrum Logius	Definitief
Best Practices ebMS Digikoppeling 2.0	Servicecentrum Logius	Definitief
Koppelvlakstandaard Grote Berichten: Digikoppeling 2.0	Servicecentrum Logius	Definitief
Best Practice Grote Berichten	Servicecentrum Logius	Definitief
Digikoppeling Translatiespecificatie	Servicecentrum Logius	Definitief
Beheermodel en releasebeleid Digikoppeling	T. Peelen	Definitief

Tabel 6: Digikoppeling-standaarden en gerelateerde documenten

Digikoppeling documentatie



Figuur 8: Digikoppeling documentatie

Overige Digikoppeling documentatie

Documentnaam	Auteur(s)	Status
Handleiding aansluiten	Servicecentrum Logius	Definitief
Serviceniveau overeenkomst (SNO)	Servicecentrum Logius	Definitief
Aansluitvoorwaarden Digikoppeling	Servicecentrum Logius	
Beheerhandleiding Serviceregister	Servicecentrum Logius	
Gebruikershandleiding Digikoppeling Serviceregister	Servicecentrum Logius	Definitief
Gebruikershandleiding compliancevoorziening WUS	Servicecentrum Logius	Definitief
Gebruikershandleiding compliancevoorziening ebMS	Servicecentrum Logius	Definitief
Handleiding CPA Creatievoorziening	Servicecentrum Logius	Definitief

Tabel 7: Overige Digikoppeling documentatie

Overige geraadpleegde bronnen

Documentnaam	Versie	Datum	Auteur(s)	Status
Architectuurschets van het stelsel voor gegevensuitwisseling	1.0	17-06-2013	W. Bakkeren, A. van Weel	Definitief
Verkorte versie Architectuurschets	1.0	17-06-2013	L. van der Knijff, W. Bakkeren, A. van Weel	Definitief
Plan van Aanpak Doorontwikkeling Digikoppeling 3.0	1.0	25-2-2013	L. van der Knijff	Definitief
Digikoppeling Glossary Verklarende woordenlijst Digikoppeling documentatie	1.1	5-1-2010	Logius	Definitief
Expertadvies Digikoppeling v2.0	1.0	12-2-2013	Wolfgang Ebbers Michael van Bekkum	Definitief
Integratielaag LNV en Digikoppeling: Informatiesystemen koppelen via de DICTU-voorziening [Handboek]	Definitief	Ntb	Bert Dingemans Tom Peelen Tony Nolde Henk Vroemen	Definitief
Verfijning en herijking kosten-batenanalyse voor investeringen in gemeenschappelijke voorzieningen in het stelsel van basisregistraties: Grip op centrale en decentrale investeringen en kosten maximaliseert de businesscase [Business Case 2010]	Definitief	23-2-2010	Price Waterhouse Coopers	Definitief
European Interoperability Framework (IDABC)	2.0	16-12-2010	IDABC	Annex 2 COM (2010) 744 final
NORA Principes en afgeleide principes	Ntb	Ntb	Noraonline.nl	Ge-publiceerd
NORA 3.0 Katern Strategie	1.0	19-8-2009	Noraonline.nl	Ge-publiceerd
NORA 3.0 Katern Informatiebeveiliging, 2010	1.0	2010	Noraonline.nl	Ge-publiceerd

NORA 3.0 verantwoording Principes voor samenwerking en dienstverlening	Ntb	29-9-2010	Jasper van Lieshout	Definitief
NORA Beeldtaal	Ntb	13-11-2012	ICTU	

Tabel 8: Overige geraadpleegde bronnen

Bijlage B: Begrippenlijst

Deze begrippenlijst is specifiek voor de *Architectuur Digikoppeling*.

Let op: dit zijn de definities op business niveau. Deze kunnen afwijken van de technische definities die in de protocollen en koppelvlakstandaarden zelf worden gehanteerd. Ook wordt een aantal vaktermen hier niet gedefinieerd zoals http, TCP/IP, netwerk, etc. Hiervoor kunt u andere bronnen via internet raadplegen.

Begrip	Uitleg
Acknowledgement berichten	Protocol-specifieke berichten die gebruikt worden om het ontvangst van een bericht te bevestigen.
Applicatie	Een systeem waarmee gegevens worden geproduceerd, vastgelegd, verwerkt en gebruikt.
Asynchroon	Proceskoppeling zonder onmiddellijke reactie (maar mogelijk wel later).
Attachment	Een bijlage bij een bericht.
Audittrail	Overzicht van de ontvangst, verwerking en verzending van berichten door een vertaaldienst met datum en tijdstip/(sequence of message)id/ontvangstbevestiging en eventueel foutcodes. Heeft als doel om uitsluitsel te geven of een bepaald bericht al dan niet is ontvangen, verwerkt of verzonden.
Authenticatie	Het herkennen van een identiteit van een partij binnen Digikoppeling vindt plaats op basis van een PKI-certificaat en een uniek identificatienummer.
Basisregistratie	Een door de overheid officieel aangewezen registratie met daarin gegevens van hoogwaardige kwaliteit, die door alle overheidsinstellingen verplicht en zonder nader onderzoek, worden gebruikt bij de uitvoering van publiekrechtelijke taken.
Bericht	Een bericht is een informatiedrager waarmee gegevens van een bron via een aanbieder aan een ontvanger worden overgedragen. Een bericht bestaat uit een envelop (header), inhoud (payload) en optioneel een of meerdere bijlagen (attachments).
Berichtdefinitie	De definitie van elementen waar een bericht uit dient te bestaan.
Best effort-profiel	Uitwisselingen die geen faciliteiten voor betrouwbaarheid vereisen.
Betrouwbaar	Garantie dat een bericht met zekerheid (precies één keer) wordt afgeleverd en dat berichten zo mogelijk in de juiste volgorde worden afgeleverd, ook als de ontvanger tijdelijk niet beschikbaar is.
Betrouwbaarheid	De zekerheid dat een bericht aankomt.
Beveiliging	De maatregelen die nodig zijn om te voorkomen dat berichten door onbevoegden worden gewijzigd of onderschept.
Bevraging	Een enkelvoudige vraag die door een serviceafnemer aan een serviceaanbieder wordt gesteld waar direct een antwoord op wordt verwacht.
Bijlage	Ongestructureerde informatie die in de vorm van een bestand kan worden meegestuurd met een inhoud van een bericht. Zie de Koppelvlakstandaarden voor details.
Broker	Een component waarmee berichten worden gegenereerd, aangeboden, afgenomen, gemonitord en verwerkt.
CanSend en	Elementen in het ebMS CPA om aan te geven dat een partij een

CanReceive (CPA)	bepaalde bericht kan ontvangen of versturen.
Compliance-voorziening	Voorziening waarmee partijen kunnen controleren of hun implementatie van Digikoppeling voldoet aan de koppelvlakstandaarden.
Connectivity	Een technische verbinding tussen twee systemen
Contract	Een servicecontract bepaalt de interface (berichtdefinities) van de webservice.
Conversation id	Specifieke element waarde in het ebMS bericht dat gebruikt wordt om meerdere berichten aan een conversatie te koppelen.
CPA	Collaboration Protocol Agreement: Servicecontract voor ebMS services.
'createSequence' bericht	Protocol specifieke bericht van WS-RM om de initiële sequentie creatie uit te voeren.
Dienst	Een geautomatiseerde berichtuitwisseling tussen twee partijen in de vorm van een bevraging, melding of groot bericht.
Digikoppeling	Digikoppeling faciliteert gegevensuitwisselingen tussen overheidsorganisaties door standaardisatie van koppelvlakken (een overeengekomen set middelen en afspraken).
Digikoppeling Architectuur	Het geheel aan principes, voorschriften, eisen en modellen die gezamenlijk Digikoppeling beschrijven.
Digikoppeling Serviceregister	Zie: Serviceregister
Digikoppeling-keten	De uitwisseling van gegevens tussen systemen van partijen via de Digikoppeling-koppelvlakstandaarden.
DK	Digikoppeling
DK Translatiespecificatie	Zie: Translatiespecificatie
DK-adapter	Software die de Digikoppeling-koppelvlakstandaarden implementeert.
DK-koppelvlakstandaard	De Digikoppeling-beschrijving van de ebMS- en WUS-koppelvlakken, die beschrijft hoe deze standaarden in de Nederlandse publieke sector worden gebruikt.
DK-koppelvlakstandaard ebMS	Beschrijving hoe ebMS toegepast moet worden voor Digikoppeling in de logistieke laag.
DK-koppelvlakstandaard Grote berichten	Beschrijving van de standaard voor uitwisseling van grote berichten via Digikoppeling.
DK-koppelvlakstandaard WUS	Beschrijving hoe WUS toegepast moet worden voor Digikoppeling in de logistieke laag.
DK-profiel	Zie: Profiel
DK-standaarden	De Digikoppeling Architectuur, de Digikoppeling-koppelvlakstandaarden en de Digikoppeling Translatie Specificatie.
DK-voorziening	De DK-voorzieningen ondersteunen de implementatie: ze zijn bedoeld om koppelvlakken te testen, voor registratie en om contracten te genereren.
DNS	Domain Name System: een systematiek en protocol voor het identificeren en benoemen van servers (mapping tussen ip adres en naam)
ebMS	ebXML Message (Service) Specification, ISO 15000-2. Onderdeel van ebXML standaard.
Eindpunt	De koppelvlakinterface van de Digikoppeling-adapter.

endpoint persistency	Persisteren van de status van de endpoint op een gegeven moment
Encryptie	Zie: Versleuteling
End-to-end	Binnen de logistieke laag: tussen het systeem van de aanbieder en het systeem van de uiteindelijke afnemer. Op proces- of business-niveau: tussen twee (proces)applicaties.
Endpoint	Zie: Eindpunt
Enterprise servicebus	Zie: Broker
Envelop	De verpakking van het bericht. In het geval van WUS en ebMS komt dit overeen met de 'header' van het bericht.
Exclusiviteit	Zie: Vertrouwelijkheid
Foutafhandeling	Het corrigeren van fouten in de afhandeling van een bericht
Functionele terugmelding	Een asynchrone terugkoppeling op een ontvangen melding.
Gegevensaanbieder	De leverancier van gegevens. Dit kan een andere partij zijn dan de serviceaanbieder (bijvoorbeeld wanneer een derde partij is betrokken).
Gegevensafnemer	De afnemer van gegevens.
Gegevensleverancier	Zie: Basisregistratie / landelijke voorziening
Grote berichten	Uitwisseling van grote bestanden via een melding of een bevraging.
Header	De logistieke informatie van het bericht (afzender, ontvanger, bericht identifier etc.), ook wel 'envelop genoemd'
HRN	Uniek identificatie nummer voor bedrijven (Handelsregisternummer), uitgegeven door de KvK en opgenomen in het Nieuwe Handelsregister.
HTTPS	HyperText Transfer Protocol Secure, afgekort HTTPS, is een uitbreiding op het HTTP-protocol met als doel een veilige uitwisseling van gegevens (Wikipedia).
Identiteit	Identiteit verwijst hier naar een gebruiker (partij) in de Digikoppeling-keten
Inhoud (van een bericht)	Zie: Payload
Integriteit	De inhoud van het bericht kan niet worden gewijzigd.
Interactiepatronen	Vormen van berichtuitwisseling tussen twee partijen. In Digikoppeling: meldingen, bevragingen en grote berichten.
Intermediair	Een partij in de keten die berichten doorstuurt naar de volgende schakel in de keten. Zie ook: transparante intermediair of niet-transparante intermediair.
Knooppunt	Een organisatie(onderdeel) waar verschillende functies zijn samengebracht.
Koppelvlak	De externe interface van een dienst.
Koppelvlakstandaard	De Digikoppeling-beschrijving van de ebMS- en WUS-koppelvlakken, die beschrijft hoe deze standaarden in de Nederlandse publieke sector worden gebruikt.
Landelijke voorziening	Digitale overheidsloketten en -voorzieningen voor burgers en bedrijven
Lifecycle berichten	Protocol specifieke berichten om de sequence lifecycle te beheren
Logging	Mechanisme om berichten individueel te registreren op datum en tijdstip/(sequence of message)id/ontvangstbevestiging en eventueel foutcodes.
Logistieke standaard	Een standaard die de opmaak en de veilige (en zo nodig

	betrouwbare) verzending en ontvangst van een bericht - met header (envelop), inhoud en evt. bijlagen(n) - regelt.
long running transactions	Een transactioneel proces dat over een langere periode kan lopen
mapping	dynamische en statische mapping: 'bericht mapping': contract mapping': Actionmapping: vertaling tussen actions van ebMS en WUS Servicemapping: vertaling tussen services
mapping schema	Een vertaaltabel tussen twee protocollen
Melding	Een verzender stuurt een enkelvoudig bericht naar een ontvanger
Message	Zie: Bericht
Message exchange patterns	Zie: Interactiepatronen
Message handler	Een component dat berichten verwerkt t.b.v. de integratielaag binnen een organisatie.
Message persistency	Persisteren (opslaan) van de ontvangen berichten en de status daarvan bepalen
Middleware	Een Enterprise Servicebus, een broker of message handler, of een maatwerk applicatie die berichten verwerkt; onderdeel van de integratielaag binnen een organisatie.
Monitoring	Het volgen van transacties binnen een applicatie.
Netwerk Time Protocol (NTP)	Netwerk Time Protocol is een protocol voor de synchronisatie van klokken van computers via een netwerk op basis van een gemeenschappelijke tijd (meestal UTC – gecoördineerde wereldtijd).
Netwerk uitval	Situatie dat het netwerk onverwachts niet functioneert
Niet-transparante intermediair	Intermediair die berichten doorstuurt door iets aan het bericht (of berichtheader) te wijzigen.
Non-repudiation	Zie: Onweerlegbaarheid
NORA	De Nederlandse Overheid Referentie Architectuur bevat inrichtingsprincipes, modellen en standaarden voor het ontwerp en de inrichting van de elektronische overheid.
OIN	Zie: Overheidsidentificatienummer
Ontkoppeling	De scheiding van de logistieke laag, de transportlaag en de bedrijfsproceslaag
Ontvanger	De partij die een melding ontvangt.
Onweerlegbaarheid	Achteraf kan niet ontkend worden dat een bericht is verstuurd of dat een bericht in goede orde is ontvangen.
Operation	Functie definitie binnen de webservice specificatie
Out-of-band	Het sturen van aanvullende informatie naar systemen buiten de normale procesgang ('out-of-band') via Grote Berichten.
Overheidsidentificatie nummer (OIN)	Een uniek identificerend nummer voor overheidsorganisaties. Dit is gelijk aan het RSIN uit het Handelsregister.
Partij	(Publieke) organisatie die gegevensdiensten in de vorm van berichten via Digikoppeling aanbiedt aan andere organisaties of afneemt van andere organisaties
Payload	De inhoud van het bericht, bestaande uit XML elementen.
Persistent storage	Opslag van berichten
PKIoverheid certificaat	Een digitaal certificaat van PKIoverheid (Public Key Infrastructure voor de overheid) waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail,

	websites of andere gegevensuitwisseling.
'piggy-backing'	Specifieke techniek om 'mee te liften' op andere berichten om additionele netwerk overhead te voorkomen
Point-to-point	De directe uitwisseling tussen twee Digikoppeling endpoints, op basis van een protocol en zonder andere schakels.
Point-to-point security	Beveiliging van de transportlaag door middel van tweezijdig TLS
Private key	de geheime sleutel van een PKI sleutelpaar (certificaten), nodig voor de ondertekening en ontcijfering van informatie (asymetrische encryptie)
Private sleutel	Zie: Private key
Profiel	Een specifieke invulling van een van de Digikoppeling koppelvlak standaarden die een groep functionele eisen invult.
Protocol	Een set van regels en afspraken voor de representatie van data, signalering, authenticatie en foutdetectie, nodig voor het verzenden van informatie tussen systemen.
protocol-specifiek betrouwbaar verkeer	Betrouwbaar berichten verkeer realiseren door gebruik te maken van protocol technieken als WS-RM en ebMS
Public key	De openbare sleutel van een PKI sleutelpaar (certificaten), nodig voor de vercijfering van informatie (asymetrische encryptie) en controle van de digitale handtekening.
Publieke sleutel	De openbare sleutel van een PKI sleutelpaar (certificaten), nodig voor de vercijfering van informatie (asymetrische encryptie)
RelatesTo	Element in een WUS-header
Reliability	Zie: Betrouwbaarheid
Reliable	Zie: Betrouwbaar
Reliable messaging-profiel	Protocol waarmee SOAP-berichten betrouwbaar geleverd kunnen worden
Sectoraal knooppunt	Intermediair die de gegevensuitwisseling faciliteert tussen partijen in een samenwerkingsverband.
Service	Een geautomatiseerde uitwisseling van informatie tussen twee systemen op basis van berichten.
Serviceaanbieder	De partij die een service aanbiedt.
Serviceafnemer	De partij die een service afneemt.
Servicebus	Integratie-infrastructuur (middleware) die nodig is om een SGA (of SOA) te faciliteren.
Servicecontract	Een technisch formaat voor het vastleggen van afspraken over de inhoud van de gegevensuitwisseling tussen partijen.
Signing	Ondertekening
SOAP	SOAP messaging protocol is een formaat en systematiek voor het opstellen en verwerken van berichten in XML.
sequentie-nummering	WS-RM geeft elk bericht een volgnummer zodat deze uniek geïdentificeerd kan worden
State	Status van een systeem
systeem uitval	Systeem dat niet functioneert (b.v. als gevolg van een storing)
Synchroon	Proceskoppeling waarbij onmiddellijk een reactie volgt op het bericht
Systeem tot systeem ('system-to-system')	Communicatie tussen systemen (op server niveau) van verschillende organisaties

TCP/IP connectivity	Communicatieprotocol voor communicatie tussen computer op het internet.
TLS	Transport Layer Security, protocollen om veilig te communiceren over het internet.
Translatiespecificatie	Beschrijft de beoogde werking van een vertaaldienst en de mapping van elementen tussen de protocollen ebMS en WUS.
Transparante intermediair	Intermediair die berichten doorstuurt zonder iets aan het bericht (of berichtheader) te wijzigen.
Transport	Het doorleveren van data packets via een netwerk
Transportlaag	Zorgt voor het probleemloze transport van data voor de applicaties.
Transportprotocol	Zie Transmission Control Protocol (TCP)
Uniek identificatienummer	Een nummer dat een partij uniek identificeert. Voor overheidsorganisaties is dit het OIN, voor bedrijven en instellingen die in het NHR zijn geregistreerd is dit het HRN.
URI	Unieke adres om een specifieke resource (zoals webpagina, bericht endpoint, download bestand) te benaderen
Versleuteling	Een versleuteld bericht kan alleen gelezen worden als het wordt ontsleuteld met de juiste sleutels. Hiermee wordt vertrouwelijkheid gegarandeerd.
Vertaaldienst	Een voorziening die zorgt voor de protocolvertaling van ebMS naar WUS en andersom.
Vertrouwelijkheid	De inhoud van het bericht (payload +attachments) is alleen voor de ontvanger bestemd en kan niet door derden worden 'gelezen'
Verzender	De partij die een melding verstuurt.
Volgordelijkheid	Berichten op volgorde van verzending ontvangen
VPN	Virtueel privaat netwerk.
Webservice	Een webservice is een verbijzondering van een service waarbij het alleen services tussen applicaties betreft. Die zijn gerealiseerd op basis van de W3C webservice specificatie (in de breedste zin van het woord, niet beperkt tot WS-*) en de service voldoet aan Digikoppeling Koppelvlak Specificatie. Binnen deze context is een webservice een ebMS webservice of een WUS webservice.
WSDL	Servicecontract voor WUS services.
WUS	WSDL/UDDI/SOAP stack. Het is een stelsel uit de W3C WS-* standaarden.
XML	eXtensible Markup Language. Een wereldwijde open standaard voor het beschrijven van gestructureerde gegevens in leesbare tekst.
XSD schema definitie	XML technologie om het formaat van een XML bericht vast te leggen zodat ten alle tijd bepaald kan worden of een XML bericht correct is of niet.

Tabel 9: Gebruikte begrippen

Bijlage C: NORA Architectuurprincipes

De NORA (Nederlandse Overheids Referentie Architectuur) is de bron voor de architectuur principes. NORA definieert 10 basisprincipes[38]:

Principe	Statement	ID
PROACTIEF	Afnemers krijgen de dienstverlening waar ze behoefte aan hebben.	BP01
VINDBAAR	Afnemers kunnen de dienst eenvoudig vinden.	BP02
TOEGANKELIJK	Afnemers hebben eenvoudig toegang tot de dienst.	BP03
STANDAARD	Afnemers ervaren uniformiteit in de dienstverlening door het gebruik van standaardoplossingen.	BP04
GEBUNDELD	Afnemers krijgen gerelateerde diensten gebundeld aangeboden.	BP05
TRANSPARANT	Afnemers hebben inzage in voor hen relevante informatie.	BP06
NOODZAKELIJK	Afnemers worden niet geconfronteerd met overbodige vragen.	BP07
VERTROUWELIJK	Afnemers kunnen erop vertrouwen dat informatie niet wordt misbruikt.	BP08
BETROUWBAAR	Afnemers kunnen erop vertrouwen dat de dienstverlener zich aan afspraken houdt.	BP09
ONTVANKELIJK	Afnemers kunnen input leveren over de dienstverlening.	BP10

Tabel 10: NORA Basisprincipes

[38] *Bron: http://www.wikixl.nl/wiki/nora/index.php/Basisprincipes*

NORA Afgeleide principes	ID	Stelling	Cluster	Realiseert	DK principes
Diensten zijn herbruikbaar	AP01	De dienst is zodanig opgezet dat andere organisaties deze in eigen diensten kunnen hergebruiken.	Diensten-aanbod	Standaard (Basisprincipe)	DK 1. interoperabiliteit
Ontkoppelen met diensten	AP02	De stappen uit het dienstverleningsproces zijn ontsloten als dienst.	Diensten-aanbod	Noodzakelijk	DK 5: Digikoppeling maakt ontkoppeling mogelijk.
Nauwkeurige dienst-beschrijving	AP05	De dienst is nauwkeurig beschreven.	Diensten-aanbod	Transparant Vindbaar	DK is open en beschreven in de architectuur en koppelvlakstandaarden.
Gebruik standaard oplossingen	AP06	De dienst maakt gebruik van standaard oplossingen	Standaard oplossingen	Standaard (Basisprincipe)	DK 2. Standaard oplossingen
Gebruik de landelijke bouwstenen	AP07	De dienst maakt gebruik van de landelijke bouwstenen e-overheid	Standaard oplossingen	Standaard (Basisprincipe)	DK 2. Standaard oplossingen
Gebruik open standaarden	AP08	De dienst maakt gebruik van open standaarden	Standaard oplossingen	Standaard (Basisprincipe)	DK 1. interoperabiliteit
Voorkeurskanaal internet	AP09	De dienst kan via internet worden aangevraagd	Kanalen	Toegankelijk	DK 1. interoperabiliteit
Identificatie informatie-objecten	AP16	Informatieobjecten zijn uniek geïdentificeerd	Informatie	Vertrouwelijk Vindbaar	DK 3. Veiligheid en vertrouwelijkheid
Afspraken vastgelegd	AP28	Dienstverlener en afnemer hebben afspraken vastgelegd over de levering van de dienst	Sturing en verantwoordelijkheid	Betrouwbaar	DK 4. Betrouwbaarheid
De dienst-verlener voldoet aan de norm	AP29	De dienstverlener draagt zelf de consequenties wanneer de dienst afwijkt van afspraken en standaarden.	Sturing en verantwoordelijkheid	Standaard (Basisprincipe) Betrouwbaar	DK 1. interoperabiliteit
Continuiteit van de dienst	AP35	De levering van de dienst is continu gewaarborgd.	Betrouwbaarheid	Betrouwbaar	DK 4. Betrouwbaarheid

Uitgangs-situatie herstellen	AP36	Wanneer de levering van een dienst mislukt wordt de uitgangssituatie hersteld	Betrouwbaarheid	Betrouwbaar	DK 4. Betrouwbaarheid
Identificatie authenticatie en autorisatie	AP37	Dienstverlener en afnemer zijn geauthenticeerd wanneer de dienst een vertrouwelijk karakter heeft	Betrouwbaarheid	Vertrouwelijk	DK 3. Veiligheid en vertrouwelijkheid
Uitwisseling berichten onweerlegbaar	AP40	De berichtenuitwisseling is onweerlegbaar	Betrouwbaarheid	Betrouwbaar	DK 4. Betrouwbaarheid

Tabel 11: Relevante afgeleide NORA principes en mapping naar Digikoppeling (DK) principes

Bijlage D: Niet-functionele eisen

Standaarden op de Pas-toe of leg uit lijst dienen te voldoen aan enkele niet-functionele eisen.
De volgende eisen zijn specifiek voor de Digikoppeling van belang:

- Ontkoppeling inhoud, logistiek en transport.
- Leveranciersonafhankelijke open standaarden.
- Interoperabiliteit.
- Vindbaarheid en openbaarheid: de standaarden en services zijn vindbaar, het beheerproces is openbaar.

Ontkoppeling

De drie lagen (inhoud, logistiek en transport) zijn in hoge mate ontkoppeld en dus onafhankelijk van elkaar. Afspraken over de inhoud van een bericht (payload) staan los van de logistieke laag. Organisaties kunnen dus op generieke wijze berichten uitwisselen, los van onderlinge afspraken over de inhoud.
Afspraken over de inhoud mogen de keuzes in de logistieke laag niet beïnvloeden en omgekeerd. De keuzes in de logistieke laag hebben op hun beurt geen invloed op de inrichting van de transportlaag (bijvoorbeeld transport over internet of eigen verbindingen).
In de context van web-services wordt de logistieke laag vaak gezien als hetzelfde als de envelop van een bericht (SOAP header). Ook in Digikoppeling maakt dit onderdeel uit van de logistieke laag. Daarnaast kan soms ook een deel van de envelop-inhoud (payload) tot de logistieke laag van Digikoppeling behoren. Dit geldt specifiek voor de metadata van Digikoppeling grote berichten.
Behalve een eventuele vertaaldienst heeft de Digikoppeling-keten geen actieve logistieke componenten tussen de adapters van de serviceafnemer en de serviceaanbieder. Als er geen vertaaldienst is, worden performance, snelheid en beschikbaarheid alleen bepaald door het netwerk en door de serviceaanbieder.

Leveranciersonafhankelijkheid

Om de interoperabiliteit te kunnen waarborgen is het essentieel dat Digikoppeling en de koppelvlakstandaarden onafhankelijk zijn van ICT-leveranciers. Dit is nodig om een ‘vendor lock-in’ en maatwerk te voorkomen: de functionaliteit wordt zoveel mogelijk geïmplementeerd met op de markt beschikbare software. Daarom worden de open standaarden van OASIS en W3C gebruikt. Deze organisaties beheren wereldwijde open standaarden, waaronder ebMS en WUS. Zie www.oasis-open.org voor meer informatie.

Interoperabiliteit

De Digikoppeling-standaarden en de Digikoppeling-voorzieningen waarborgen interoperabiliteit op het logistieke niveau van gegevensuitwisseling. Dit houdt in dat organisaties die zich conformeren aan de standaard en hier correct gebruik van maken, onderling gegevens kunnen uitwisseling door de standaard toe te passen. Op deze laag bevinden zich de afspraken betreffende transportprotocollen (HTTP), messaging (SOAP), adressering, beveiliging (authenticatie en encryptie) en betrouwbaarheid. Digikoppeling maakt berichtenuitwisseling mogelijk op basis van de ebXML/ebMS en WUS-families van standaarden, inclusief

bijbehorende andere standaarden. De voor Digikoppeling vereiste interoperabiliteit van de WUS standaarden van OASIS en W3C wordt gebaseerd op de profielen (en tests) van WUS, WS-RM, WS-Security etc. De interoperabiliteit van ebMS is gebaseerd op de standaard ebMS versie 2 (ISO standaard) en de tests/certificering van Drummond.
Aangezien veranderingen tot nog toe bestonden uit uitbreidingen met nieuwe (optionele) functionaliteit, voldoen ook de eerste implementaties aan de nieuwste versie.

Vindbaarheid en openbaarheid

De standaard is vindbaar en toegankelijk op een laagdrempelige manier. De standaard en documentatie wordt gepubliceerd op de website van Logius: www.logius.nl/digikoppeling
De standaard is tevens vindbaar via de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie: https://lijsten.forumstandaardisatie.nl/open-standaarden/digikoppeling.
Wijzigingen op de standaard worden conform het Beheermodel in openbaarheid besproken en beheerd.