Logius - Standaard

Digikoppeling Architectuur 2.1.0

Logius Standaard

Vastgestelde versie 12 augustus 2022

Deze versie:
https://publicatie.centrumvoorstandaarden.nl/dk/architectuur/2.1.0

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

Laatste werkversie:
https://logius-standaarden.github.io/Digikoppeling-Architectuur/

Vorige versie
https://publicatie.centrumvoorstandaarden.nl/dk/architectuur/2.0.1/

Redacteurs:
Pieter Hering (Logius)
Peter Haasnoot (Logius)

Doe mee:
GitHub Logius-standaarden/Digikoppeling-Architectuur
Dien een melding in
Revisiehistorie
Pull requests

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

---

Samenvatting

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 gegevensuitwisseling 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 gegevens (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 OBDO 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 is 'backwards compatible'*. Partijen die Digikoppeling gebruiken, voldoen daardoor automatisch aan de nieuwste versie van Digikoppeling. De nieuwe functionaliteiten en profielen zijn dan echter niet beschikbaar. Voor het beheer van de Digikoppeling standaard en documenten wordt waar mogelijk om SemVer toegepast

De aanleiding van de vernieuwing van dit document is tweeledig: in 2019 is een RFC ingediend over relatie van de Digikoppeling profielen met *bevragen en melden*. Daarnaast is in 2020 een Rest API profiel uitgewerkt en opgenomen in de Digikoppeling Standaard.

De belangrijkste wijzigingen in de nieuwe Digikoppeling Architectuur versie 2.x.x zijn:

- Geen onderscheid meer in 'WUS voor bevragingen' en 'ebMS voor meldingen'
- Toevoegen van een Digikoppeling REST API profiel, gebaseerd op de API Design Rules (uit de Nederlandse API Strategie)
- De Provider bepaalt welk koppelvlak - REST API, WUS of ebMS van toepassing is op de door haar geleverde dienst.

*('Backwards compatibiliteit' geldt niet voor de security eisen, zie hiervoor de actuele versie van [Digikoppeling Beveiligingsdocument])

Status van dit document

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

Inhoudsopgave

Samenvatting

Status van dit document

1. Doel van dit document en leeswijzer
1.1 Inleiding
1.2 Doel
1.3 Doelgroep
1.4 Verantwoording
1.5 Digikoppeling standaarden
1.6 Begrippen

2. Wat is Digikoppeling
2.1 Doel van Digikoppeling
2.2 Context van Digikoppeling
2.2.1 Open en Closed Data
2.2.2 Open en Closed Diensten
2.2.3 Open en Closed Netwerken
2.3 Wanneer moet Digikoppeling toegepast worden
2.4 Functioneel toepassingsgebied
2.5 Organisatorisch werkingsgebied
2.6 Van *'uitwisseling van gestructureerde berichten'* naar *'gestructureerde gegevensuitwisseling'*
2.7 Digikoppeling voor externe uitwisseling
2.8 Digikoppeling voor Closed Data en Open Data via Closed diensten
2.9 Wie communiceert met wie
2.10 Scope van Digikoppeling
2.10.1 Grijs gebied

3. Digikoppeling-architectuurprincipes
3.1 Uitgangspunten
3.2 Architectuurprincipes

4. De Digikoppeling-keten
4.1 Digikoppeling als bouwsteen van de Digitale Overheid
4.2 Opbouw van de Digikoppeling-keten
4.2.1 Partijen en Rollen
4.2.2 Intermediairs
4.3 Componenten in de logistieke Digikoppeling-keten
4.4 Uitwisselingsvormen
4.4.1 Business-behoefte
4.4.2 Digikoppeling-aanbod
4.4.3 Synchrone uitwisseling
4.4.4 Notificaties
4.4.5 Asynchrone uitwisseling
4.4.6 Melding (Transactie)
4.4.7 Grote Berichten
4.5 Geen onderscheid meer in gebruik WUS en ebMS2 voor bevragingen en transacties

5. Transactiepatronen in Digikoppeling
5.1 Synchrone bevraging
5.2 Synchrone Melding
5.3 Asynchrone Melding-bevestiging
5.4 Uitwisselen grote bestanden
5.5 Uitwisseling via een transparante intermediair
5.6 Uitwisseling via een niet-transparante intermediair

6. Digikoppeling-koppelvlakstandaarden en voorschriften
6.1 Overzicht
6.2 Digikoppeling-voorschriften
6.3 REST API's
6.3.1 Digikoppeling REST API voor synchrone requests
6.3.2 OAS: OpenAPI Specification
6.4 WUS
6.4.1 WUS familie van standaarden
6.4.2 Digikoppeling WUS voor synchrone bevragingen
6.4.3 WSDL: Web Services Description Language
6.5 ebMS
6.5.1 ebMS2 familie van standaarden
6.5.2 Digikoppeling ebMS2 voor betrouwbare, asynchone uitwisseling
6.5.3 CPA
6.6 Grote berichten
6.6.1 Werking grote berichten
6.6.2 Standaarden voor grote berichten

7. Overzicht Use Cases
7.1 Hulpmiddel voor een keuze voor een Digikoppeling Koppelvlak
7.1.1 Hoeveel partijen zijn er betrokken bij de koppeling en wat is hun rol?

7.1.2 Wat is de aard van de gegevens/objecten die uitgewisseld moeten worden?
7.1.3 Het uitwisselen van relationele bedrijfsgegevens over objecten, ‘Bedrijfsdocumenten’
7.1.4 Raadplegen of muteren van een bron
7.2 Andere overwegingen voor een keuze van een koppelvlak
7.2.1 Capabiliteit van een organisatie, bestaande infrastructuur
7.3 Overzicht Usecase
7.3.1 Overdracht van verantwoordelijkheid
7.3.2 Abonneren op wijzigingen middels notificaties
7.3.3 End-to-End security
7.3.4 Betrouwbaar berichtenverkeer op protocol niveau (reliable messaging)

8. Digikoppeling-voorzieningen
8.1 Inleiding
8.2 Compliancevoorzieningen
8.3 OIN Register (Centrale OIN Raadpleegvoorziening)
8.4 CPA Register

9. Implementatie van Digikoppeling
9.1 Architectuuraspecten van de aansluiting op Digikoppeling
9.1.1 Afspraken over de inhoud en interactie van de uitwisseling
9.1.2 Digikoppeling-adapter
9.1.3 Selectie van profielen
9.1.4 Servicebeschrijvingen
9.1.5 Gebruik van de Digikoppeling voorzieningen
9.2 Relatie met de inhoudelijke laag
9.2.1 Waarom
9.2.2 Informatiebeveiliging
9.2.3 Bedrijfsprocessen
9.2.4 Applicatielaag
9.2.5 Berichtinhoud en semantiek
9.2.6 Karakterset en codering
9.3 Relatie met de transportlaag
9.3.1 Randvoorwaarden transport
9.3.2 Inleiding transportlaag
9.3.3 Transport Level Security (TLS)
9.3.4 Netwerken
9.3.5 Diginetwerk

10. Bijlage A: Bronnen
10.1 Digikoppeling-standaarden en gerelateerde documenten
10.1.1 Digikoppeling documentatie
10.1.2 Overige geraadpleegde bronnen

11. Bijlage B: Begrippenlijst

12. Bijlage C: NORA Architectuurprincipes

13. Bijlage D: Niet-functionele eisen
13.1 Ontkoppeling van de drie lagen
13.2 Leveranciersonafhankelijkheid

13.3 Interoperabiliteit
13.4 Vindbaarheid en openbaarheid

14. Conformiteit

15. Lijst met figuren

A. Referenties
A.1 Normatieve referenties
A.2 Informatieve referenties

§ 1. Doel van dit document en leeswijzer

§ 1.1 Inleiding

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

§ 1.2 Doel

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

§ 1.3 Doelgroep

De *Digikoppeling Architectuur* 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

Tabel 1.1: Doelgroep Digikoppeling Architectuur

1.4 Verantwoording

§

De *Digikoppeling Architectuur* is tot stand gekomen in samenwerking met leden van het Technisch Overleg Digikoppeling en andere belanghebbenden.

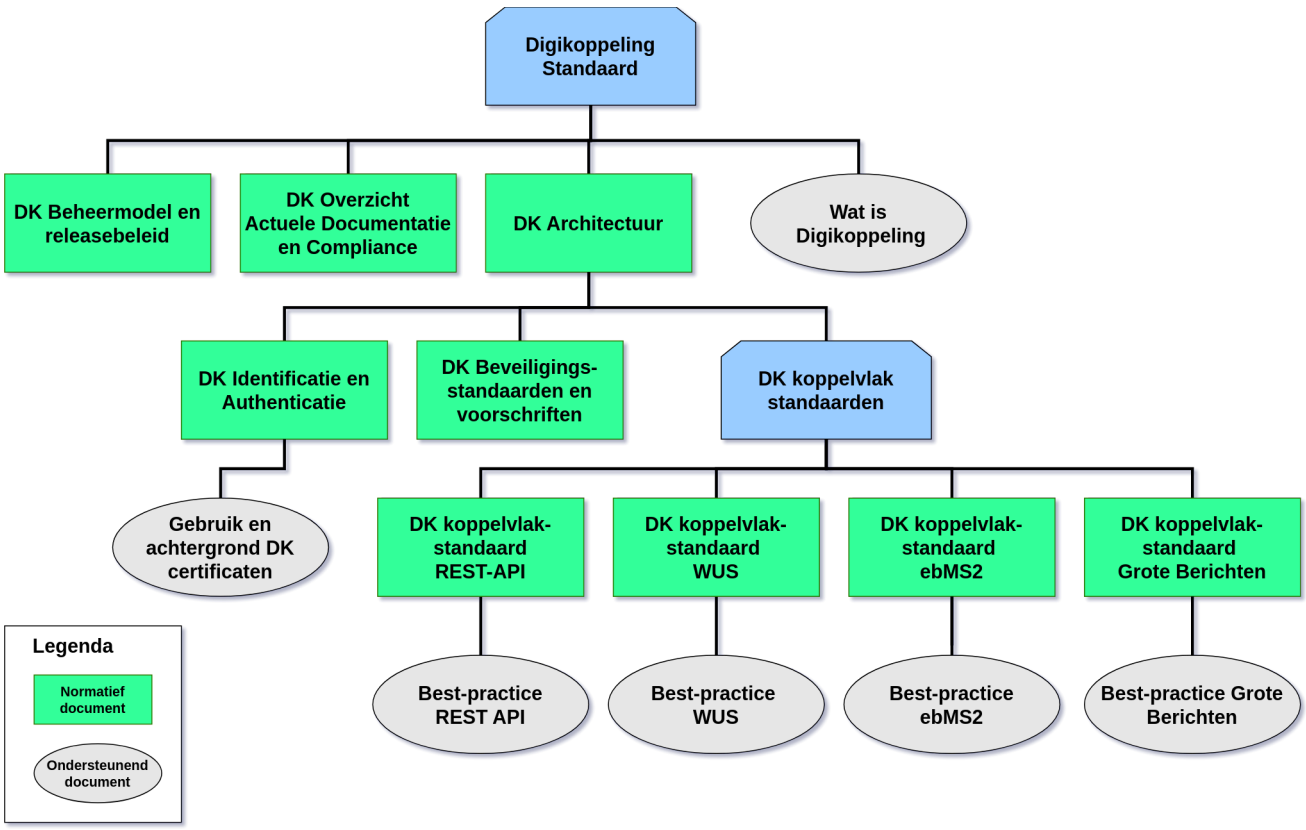
De *Digikoppeling Architectuur* is mede gebaseerd op:

- 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.

§ 1.5 Digikoppeling standaarden

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



Figuur 1 Digikoppeling Standaard

▶ **Tekstalternatief**

- Alle groene documenten vallen onder het beheer zoals geformaliseerd in het [Digikoppeling Beheermodel].
- 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/digikoppeling.

§ 1.6 Begrippen

Belangrijke begrippen en afkortingen zijn opgenomen in *Bijlage B: Begrippen*.

§ 2. Wat is Digikoppeling

In dit hoofdstuk opzet beschrijven we de belangrijkste facetten van de nieuwe Digikoppeling Architectuur.

§ 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. Ook moeten overheden in staat zijn direct elkaars data bronnen te bevragen indien deze data nodig is bij het uitvoeren van hun taken.

Digikoppeling voorziet hierin door de standaarden voor deze uitwisseling te definiëren. Met deze logistieke standaardisatie bevordert Digikoppeling de interoperabiliteit tussen (overheids)organisaties.

§ 2.2 Context van Digikoppeling

Voordat we inhoudelijk op Digikoppeling en haar onderliggende standaarden en de hierbij horende toepassingsgebieden ingaan, is het belangrijk om aantal begrippen uit het gebied van gegevensuitwisseling nader te beschrijven. Zeer belangrijk is ook het toepassings- en werkingsgebied te beschrijven waarmee Digikoppeling op de lijst van verplichte standaarden ('Pas-toe-of-leg-uit') van het Forum Standaardisatie vermeld staat. Met deze ingrediënten formuleren we uiteindelijk de scope van Digikoppeling.

§ 2.2.1 Open en Closed Data

Een concept dat sinds begin 2000 een opmars maakt is het principe van *Open Data*. Open Data zijn gegevens die in een open formaat door iedereen voor alle doeleinden vrij gebruikt, hergebruikt en gedeeld kunnen worden. De nadruk voor Open Data ligt met name bij de gegevens van de overheid. Gegevens die om reden van privacy, veiligheid, wettelijke verplichtingen en dergelijk niet onder de definitie vallen noemen we in dit document *Closed Data*.

§ 2.2.2 Open en Closed Diensten

Naast het onderscheid tussen Open en Closed data is het ook van belang om onderscheid te maken in publieke en afgeschermde diensten. Voor Closed Data biedt een overheidsorganisatie afgeschermde, beperkt toegankelijke closed diensten.

Een bron van open data kan een overheidsorganisatie aanbieden via een voor iedereen toegankelijke open dienst. Die bron kan echter essentieel zijn voor bepaalde publieke ketens. De aanbieder kan er voor kiezen om naast een publieke dienst ook een beperkt toegankelijke dienst te aan te bieden, bijvoorbeeld met een uitgebreide beschikbaarheid, schaalbaarheid of functionaliteit.

- Open Diensten: diensten zonder toegangsbeperking bijvoorbeeld open data.
- Gesloten Diensten: diensten met toegangsbeperking bijvoorbeeld persoonsgegevens en vertrouwelijke gegevens of diensten voor specifieke partijen.

§ 2.2.3 Open en Closed Netwerken

Naast het onderscheid tussen open en closed data en diensten is het ook van belang om onderscheid te maken in publieke en afgeschermde netwerken. Voor closed data en diensten is het deels mogelijk deze via een versleutelde verbinding (TLS) op een open netwerken (het internet) aan te bieden. Digikoppeling voorziet hierbij dan in de beveiliging. Open data en open diensten worden bij vanzelfsprekend aangeboden op open netwerken.

Daarnaast is het ook mogelijk om closed data en diensten over een closed netwerk zoals Diginetwerk of een eigen LAN of WAN aan te bieden.

De aanbieder van de closed data en diensten besluit welke mate van beveiliging wordt toegepast en welke netwerken worden gebruikt.

§ 2.3 Wanneer moet Digikoppeling toegepast worden

Digikoppeling staat op de lijst *verplichte standaarden* van het Forum Standaardisatie. De lijst beschrijft het *Functioneel* toepassingsgebied en het *organisatorisch* werkingsgebied. Met het functioneel toepassingsgebied bedoelt het Forum de toepassing(en) waarvoor het gebruik van de standaard verplicht is of aanbevolen wordt.

§ 2.4 Functioneel toepassingsgebied

Het Forum Standaardisatie definieert het *functioneel toepassingsgebied* van Digikoppeling als volgt:

> Digikoppeling moet worden toegepast bij digitale gegevensuitwisseling die plaatsvindt met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, of die sector overstijgend is. De verplichting geldt voor gegevensuitwisseling tussen systemen waarbij er noodzaak is voor tweezijdige authenticatie. Geautomatiseerde gegevensuitwisseling tussen informatiesystemen op basis van NEN3610 is uitgesloten van het functioneel toepassingsgebied.

bron: [Pas-toe-of-leg-uit]

Daarnaast benoemt het Forum de organisaties waarvoor de verplichting geldt. Dit wordt het *organisatorische werkingsgebied* genoemd. Het werkingsgebied is als volgt gedefinieerd:

§ 2.5 Organisatorisch werkingsgebied

> Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

bron: [Pas-toe-of-leg-uit]

§ 2.6 Van *'uitwisseling van gestructureerde berichten'* naar *'gestructureerde gegevensuitwisseling'*

Digikoppeling heeft zich vanaf het begin van haar ontstaan gericht op het uitwisselen van berichten, en dan specifiek op de 'envelop' van een bericht en niet op de inhoud. Iedere organisatie die Digikoppeling gebruikt kon daarmee de gegevensuitwisseling onafhankelijk van de inhoud inrichten.

Met de toevoeging van het Digikoppeling REST API profiel komt de vergelijking met berichten in enveloppen in het gedrang. Envelop en bericht schuiven in elkaar; de metafoor van enveloppen en postverzending werkt niet meer in alle koppelvlakken van de standaard. Echter, het basisprincipe blijft bestaan: Digikoppeling bemoeit zich niet met de inhoud, Digikoppeling heeft *'Geen boodschap aan de boodschap'*. Het verschil wordt geïllustreerd in onderstaande afbeelding:

Figuur 2 Soap vs. REST APIs bron upwork.com

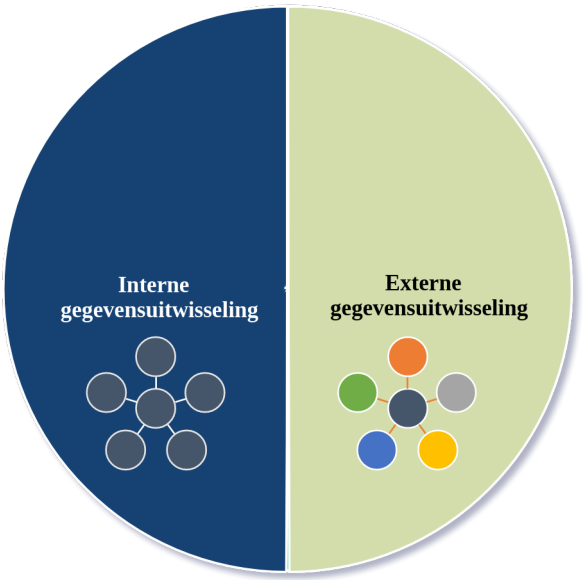
bron: https://www.upwork.com/resources/soap-vs-rest-a-look-at-two-different-api-styles

Het Forum beschrijft dat Digikoppeling gaat over het uitwisselen van gestructureerde berichten. Voor het gebruik van REST API's moet het concept van *berichten* wel erg uitgerekt worden om in deze definitie te passen. Een synchrone JSON response kan als een bericht worden gezien, maar of ook de request die hieraan voorafging als een gestructureerd *bericht* kan worden gezien vergt enige creativiteit. De uitwisseling van gegevens via REST API's is daarentegen in ieder geval wel *gestructureerd*, alleen al omdat elke interactie via een API volgens een protocol, of standaard verloopt, zoals http [rfc7230], https [rfc2818], OpenAPI Specification [openapi] of de (API Design Rules) [API Design Rules].

Voor Digikoppeling verleggen we daarom de focus van berichtenverkeer naar het uitwisselen van gegevens. Vandaar dat we in het vervolg in dit document zullen spreken over gestructureerde *gegevensuitwisseling*, in plaats van gestructureerde berichtenuitwisseling.

§ 2.7 Digikoppeling voor externe uitwisseling

Digikoppeling richt zich dus van oudsher primair op het uitwisselen van gegevens 'met behulp van gestructureerde berichten' en maakt (tot nu toe) geen duidelijk onderscheid tussen Open en Closed Data. Dit maakt het niet duidelijk wanneer Digikoppeling gebruikt moet worden. Reden om dit beter af te pellen en de scope van Digikoppeling eens langs een andere lat te leggen.



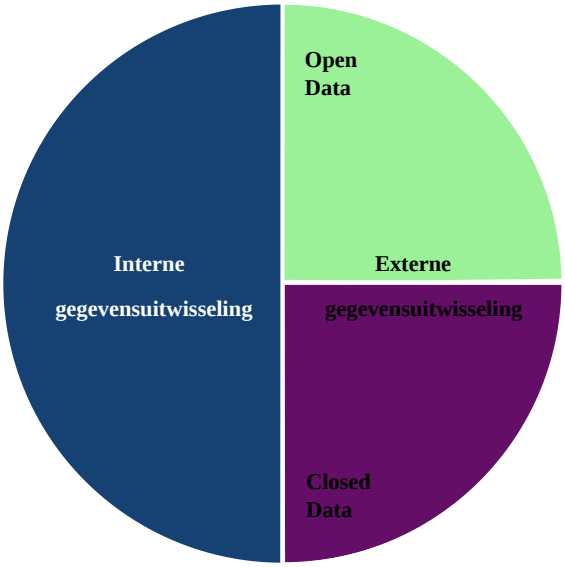
Figuur 3 Interne en Externe Gegevensuitwisseling

Digikoppeling is een standaard voor gegevensuitwisseling *tussen* organisaties, met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, of die sector-overstijgend is.

§ 2.8 Digikoppeling voor Closed Data en Open Data via Closed diensten

Digikoppeling bestaat uit een verzameling standaarden voor elektronisch verkeer tussen overheidsorganisaties. Digikoppeling gaat dus om overheidsgegevens. Openbare informatie van de Rijksoverheid mag worden hergebruikt, bijvoorbeeld op websites en in applicaties. Dit is Open Data.

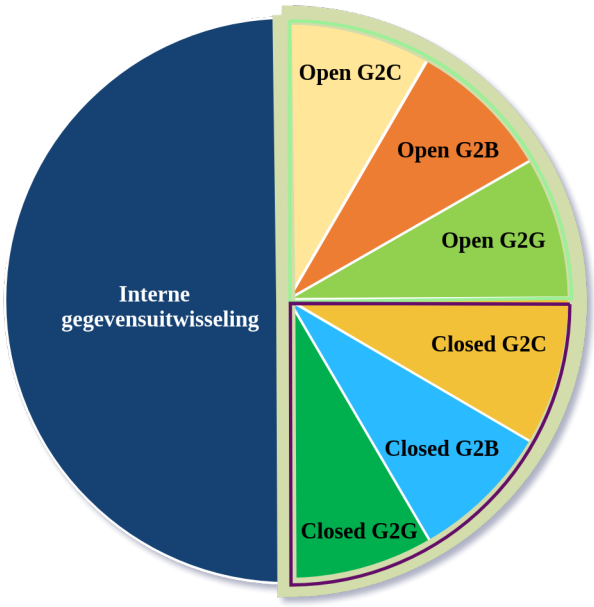
Overheidsgegevens zijn actief beschikbaar als open data voor hergebruik van derden. Behalve als er goede redenen zijn om dat niet te doen. In dat geval noemen we dit Closed Data.



Figuur 4 Open en Closed OverheidsData

§ 2.9 Wie communiceert met wie

Digikoppeling verplicht dat verzender en ontvanger elkaar kennen ([Pas-toe-of-leg-uit] *zie Digikoppeling, paragraaf 'Overig/Waarvoor geldt de verplichting*). Digikoppeling gaat over communicatie tussen de overheden (G2G) en niet over uitwisseling met burgers (G2C). De communicatie tussen overheid en het bedrijfsleven (G2B) is niet gestandaardiseerd.

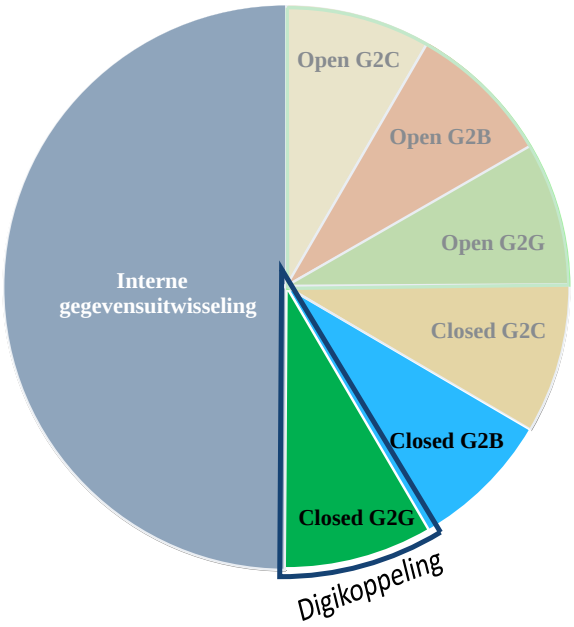


Figuur 5 Segmentering van de communicatie

§ 2.10 Scope van Digikoppeling

Digikoppeling moet worden toegepast voor geautomatiseerde gegevensuitwisseling tussen informatiesystemen en is verplicht voor Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de

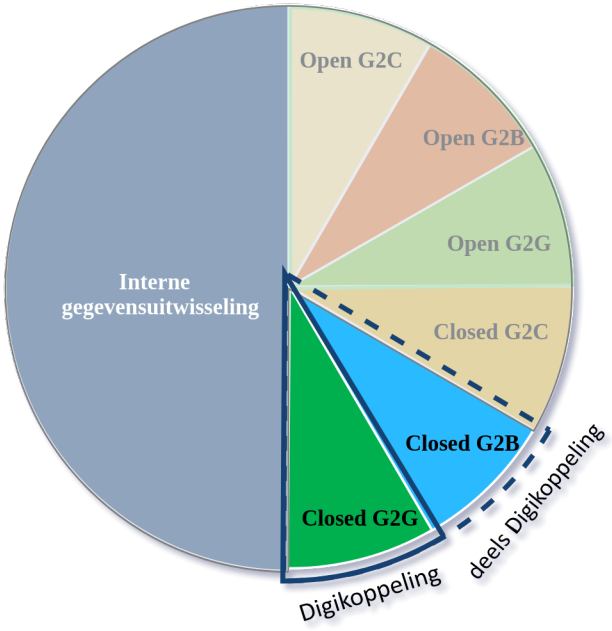
(semi-)publieke sector. Digikoppeling moet worden toegepast wanneer gebruikt gemaakt wordt van Gesloten Diensten. Dat wil zeggen diensten waarbij er noodzaak is om de afnemer te authenticeren.



Figuur 6 Digikoppeling voor Closed Data G2G Uitwisseling

§ 2.10.1 Grijs gebied

De verplichting voor Digikoppeling geldt dus voor communicatie tussen overheden. De praktijk is dat voor communicatie met bedrijven vaak verplichtingen gelden die hun oorsprong hebben in Digikoppeling, zoals het gebruik van het OIN en PKIoverheidscertificaten, of zelfs geïnspireerd zijn op Digikoppeling zoals het Koppelvlak *WUS voor Bedrijven* van Digipoort.



Figuur 7 Digikoppeling voor Closed Data G2B Uitwisseling

§ 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 interoperabel. Zie bijlage D voor uitleg.
2. De Digikoppeling-standaarden ondersteunen veilige gegevensuitwisseling voor:
    - synchrone en asynchrone uitwisseling;
    - berichtenverkeer of op resources gebaseerde uitwisseling;
    - het uitwisselen van best effort of reliable overdracht;
    - het uitwisselen van grote berichten;
3. Dienstaanbieders kunnen kiezen welk interactiepatroon nodig is voor gegevensuitwisseling. Afhankelijk van hun behoefte. Dienstaanbieders bepalen in overleg met de afnemers welke Digikoppeling profielen ze gebruiken.
4. Providers, zoals Basisregistraties en landelijke voorzieningen, bepalen welke Digikoppeling profielen gebruikt wordt voor een door hun geleverde dienst. Per dienst kunnen meerdere Digikoppeling profielen aangeboden worden.

In vorige versies van de Digikoppeling Architectuur werden specifieke profielen gekoppeld aan bevragingen en meldingen. Dit voorschrift bleek in de praktijk niet meer goed bruikbaar. Vandaar dat met ingang van versie `2.0.0` deze relatie is komen te vervallen.

§ 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, moeten serviceaanbieder en serviceafnemer nagaan of de uitwisseling voldoet aan de wet- en regelgeving (in het bijzonder de AVG).
4. **Betrouwbaarheid:** Berichtaflevering 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.

§ 4. De Digikoppeling-keten

Dit hoofdstuk beschrijft Digikoppeling als bouwsteen van de Digitale Overheid. De keten van alle Digikoppeling-gerelateerde componenten die gegevensuitwisseling voor de Digitale Overheid invullen duiden we in dit document aan als de de Digikoppeling-keten. In dit hoofdstuk worden de vormen van gegevensuitwisseling op procesniveau beschreven.

§ 4.1 Digikoppeling als bouwsteen van de Digitale Overheid

De Nederlandse overheid werkt aan betere dienstverlening aan burgers en bedrijven met een basisinfrastructuur voor de Digitale Overheid 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 onder meer
  - **Digilevering** (abonnementen services / Event Driven Notifications) 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 gegevens kunnen uitwisselen.

Digikoppeling maakt het mogelijk om gegevens uit te wisselen, databronnen te raadplegen / bewerken en services aan te roepen. Het is daarmee een essentiële bouwsteen van de basisinfrastructuur van de Digitale Overheid. Organisaties kunnen via Digikoppeling rechtstreeks (bilateraal) informatie met elkaar uitwisselen. Vaak zijn er extra schakels betrokken, zoals een sectoraal knooppunt of een intermediair.

Digikoppeling biedt een standaard voor het veilig uitwisselen van berichten en gegevens 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 gegevensuitwisseling zodat verschillende partijen veilig gegevens kunnen uitwisselen.

§ 4.2 Opbouw van de Digikoppeling-keten

De Digikoppeling-keten bestaat uit:

- Deelnemende publieke organisaties die gegevens met elkaar uitwisselen (partijen). Een partij kan
  - een service of resource 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 en Rollen

Een partij is een (publieke) organisatie die een service 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.

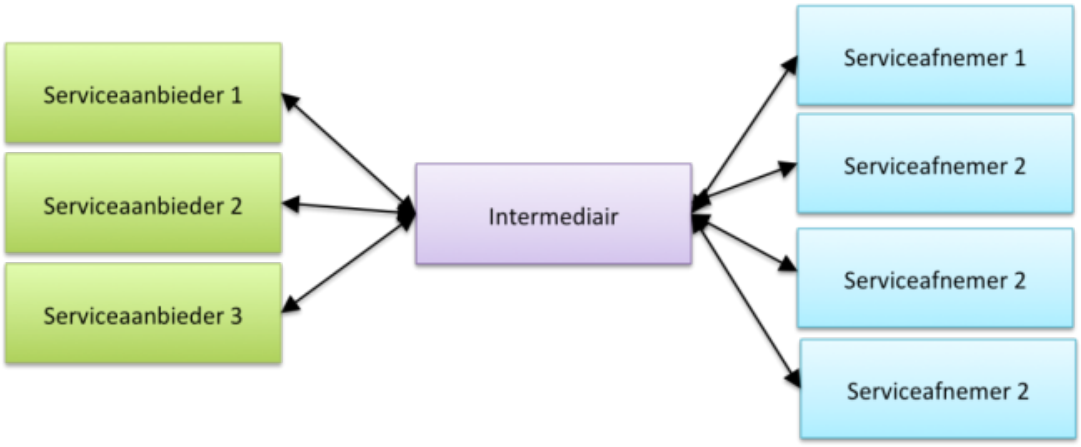
§ 4.2.2 Intermediairs

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 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 8 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.

§ 4.3 Componenten in de logistieke Digikoppeling-keten

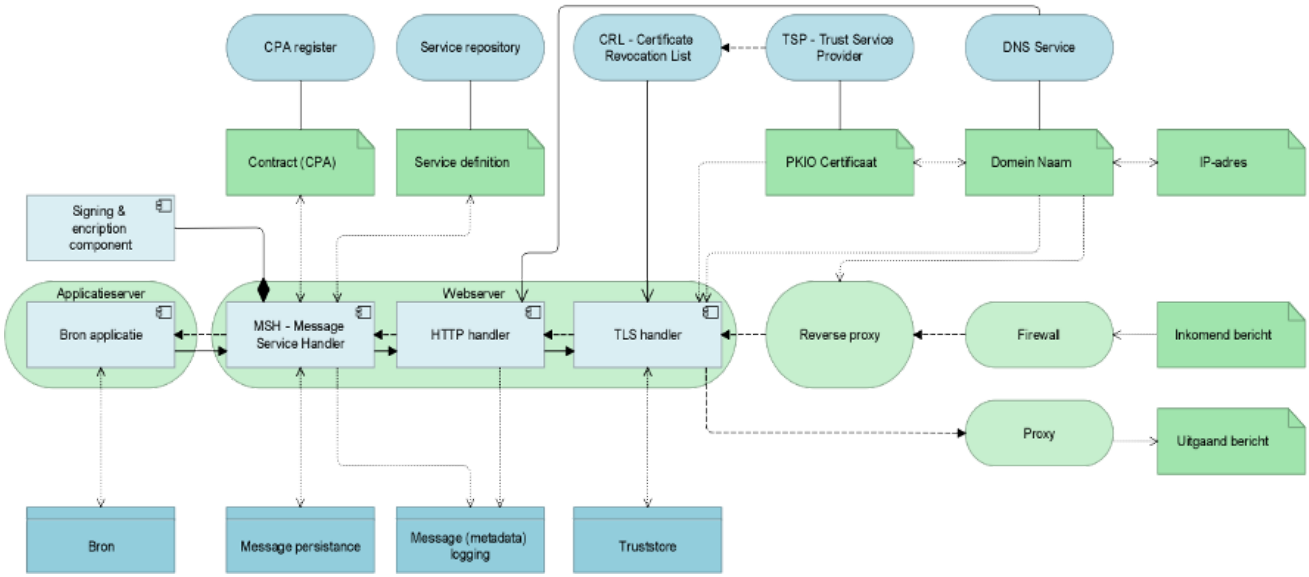
De volgende componenten maken onderdeel uit van de Digikoppeling-keten van gegevensuitwisseling.

Componenten	Toelichting
Applicatie	Een systeem waarmee gegevens worden geproduceerd, vastgelegd en gebruikt.
Broker of Enterprise Service Bus (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 Digikoppeling Gebruik en Achtergrond 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 ebMS2 services), OAS voor Restful API's, en een WSDL (voor WUS services) en wordt ingelezen in de Digikoppeling-adapter. voor de CPA stellen partijen samen een servicecontract op.

Tabel 4.1: Componenten van de Digikoppeling-keten

N.B.: De Digikoppeling-voorzieningen (Het Digikoppeling portaal met de Compliance Voorziening, het OIN register en het CPA register) vormen geen onderdeel van de Digikoppeling-keten maar ondersteunen tijdens de ontwikkel- en testfasen en bij het uitgifte en raadplegen van OIN's.

In meer detail zijn de componenten uitgewerkt in een referentiemodel voor gegvensuitwisseling. Hierin is de opsplitsing en samenhang weergegeven:



Figuur 9 Referentiemodel gegevensuitwisseling

§ 4.4 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.

§ 4.4.1 Business-behoefte

Op business-niveau is er een veelheid aan uitwisselingsvormen waaraan behoefte bestaat. Deze zijn vaak context specifiek. 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.

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 organisatie.
2. Naast deze impact op de service verlenende 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 dit antwoord aan de oorspronkelijke vraag koppelen) 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.

	Synchroon	Asynchroon
Bevraging	Onmiddellijke bevraging	Bevraging met uitstel
Transactie	Onmiddellijke transactie	Transactie met uitstel

Tabel 4.2: primitieve business-interacties

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.

§ 4.4.2 Digikoppeling-aanbod

Digikoppeling onderscheidt verschillende vormen van uitwisseling:

- *synchrone* request-response voor bevraging en bewerking van objecten en in de context van het gebruik van *resources* op basis van het REST patroon.
- *synchrone* request-response met gestructureerde berichtuitwisseling
- *asynchrone* request-response en reliable messaging
- uitwisseling van grote data bestanden en hun metadata

Bij synchrone request-response voor bevraging en bewerking van objecten *data-providers* bieden providers databronnen - of resources- die *data-consumers* kunnen bevragen en bewerken. Een provider vermeldt locatie van en randvoorwaarden voor toegang van de databron en via gestructureerde benadering kan een consumer de resource bevragen of zelfs bewerken.

Bij een synchrone request-response met gestructureerde berichtuitwisseling 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 asynchrone request-response verstuurt de service-requester een bericht 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.

§ 4.4.3 Synchrone uitwisseling

Digikoppeling biedt twee mogelijkheden voor synchrone uitwisseling aan: bij synchrone uitwisseling wacht het vragende informatiesysteem (de requestor) 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.

Synchrone uitwisseling kan worden ingericht op basis van de Digikoppeling-koppelvlakstandaard WUS en het Digikoppeling REST API profiel.

§ 4.4.4 Notificaties

Een alternatieve vorm van synchrone uitwisseling die steeds vaker voorkomt is te omschrijven als notificatie. Hierbij stuurt de *data provider* via het REST patroon een HTTP POST bericht naar de service van de *data-consumer*. Door toevoeging van dit patroon in de gegevensuitwisseling wordt een zogenaamde *Event Driven Architecture* gerealiseerd. Eind 2022 is de Notificatiestandaard bij Logius in beheer genomen onder de noemer NL-GOV-profile-for-CloudEvents.

§ 4.4.5 Asynchrone uitwisseling

Een asynchroon verzoek is een enkelvoudig bericht waarop eventueel enige tijd later een retour-melding volgt. Het gebruikte protocol regelt de betrouwbare ontvangst. Bij asynchrone uitwisseling 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.

Digikoppeling Koppelvlakstandaard ebMS2 biedt specifieke ondersteuning voor asynchrone uitwisseling.

§ 4.4.6 Melding (Transactie)

Een melding is een enkelvoudig bericht waarop eventueel enige tijd later een retour-melding volgt. Het gebruikte protocol kan de betrouwbare ontvangst en de onweerlegbaarheid (non-repudiation) regelen van een bericht. Bij meldingen kan de betrouwbare aflevering van het bericht essentieel zijn. Als een partij het bericht niet direct kan aannemen, kan een protocol erin voorzien dat het bericht nogmaals wordt aangeboden.

Naast het uitvoeren van een transactie met een betrouwbaar - *reliable* - protocol als ebMS2, is het ook mogelijk transacties op *business niveau* te borgen. Dubbel verzonden en ontvangen verzoeken - *duplicate requests* dienen dan door de business applicatie genegeerd te worden. Een vaak geciteerde bron [no-Reliable-messaging] stelt dat betrouwbare aflevering van berichten enkel op het niveau van de verwerkende business applicaties kan worden uitgevoerd. Een eis hiervoor is dat voor update requests *Idempotent* methoden worden gebruikt, meer hiervoor zie regel API-03 uit [API DESIGN RULES].

Praktisch gezien resulteert dit meestal in een conversatie bestaande uit meerdere synchrone uitwisselingen. Conversaties zijn een vast onderdeel van het ebMS2 protocol maar kunnen ook op business niveau worden onderkend. Hiervoor worden attributen aan de synchrone uitwisseling toegevoegd waarmee zowel de provider als consumer - 'out-of-band' - de synchrone uitwisseling later kunnen correleren als 1 conversatie en op deze conversatie als geheel dan bijvoorbeeld compenserende handelingen kunnen verrichten.

4.4.7 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: met de Digikoppeling Koppelvlakstandaard Grote Berichten.

Bij ‘grote berichten’ worden grotere bestanden uitgewisseld via een Digikoppeling uitwisseling in combinatie met een (HTTPS-)down- of upload vanaf een beveiligde website. Grote berichten vormen een functionele uitbreiding op Digikoppeling uitwisseling voor de veilige bestandsoverdracht van berichten groter dan 20 MiB[24].

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.

24: 1 MiB=1024^2 bytes : Voorheen stond hier 20MB. We gebruiken de term MiB om geen enkele verwarring te scheppen over de drempelwaarde. Het verschil tussen 20Mb en 20Mib is echter te verwaarlozen.

4.5 Geen onderscheid meer in gebruik WUS en ebMS2 voor bevragingen en transacties

De Provider bepaalt welk koppelvlak - REST API, WUS of ebMS- van toepassing is op de door haar geleverde dienst.

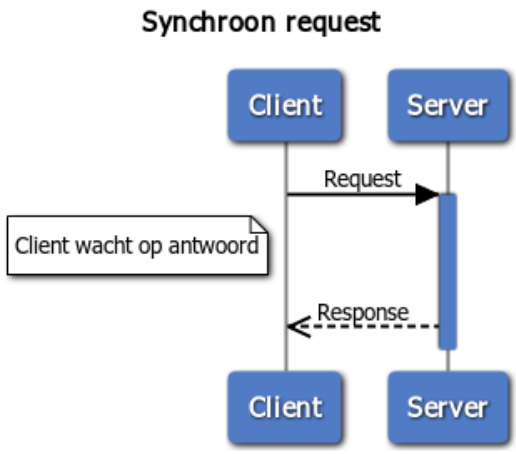
Tot en met 2019 werd in de Digikoppeling Standaard onderscheid gemaakt tussen 'WUS voor bevragingen' en 'ebMS voor meldingen'. In de praktijk bleek dit onderscheid niet altijd goed te werken. Er zijn bijvoorbeeld usecases waarin WUS beter geschikt is voor meldingen dan ebMS. In deze versie van de Digikoppeling Architectuur is dit onderscheid niet meer aanwezig. In plaats daarvan beschrijven we welke Digikoppeling koppelvlakken het best passen bij transactiepatronen en use cases uit de praktijk.

5. Transactiepatronen in Digikoppeling

In dit hoofdstuk beschrijven we de transactiepatronen in gegevensuitwisseling in algemene zin, met een suggestie welk Digikoppeling koppelvlakstandaard hier het best bij aansluit. Voor het opstellen van de volgende transactiepatronen is dankbaar gebruik gemaakt van de conceptversie van de *Edukoppeling Architectuur 2.0*.

§ 5.1 Synchrone bevraging

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). Een synchrone bevraging is in de regel *idempotent*, een request kan opnieuw verstuurd worden zonder gevolgen.



Figuur 10 Synchroon Request

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling WUS	Digikoppeling WUS is geschikt als voor de bevraging gestructureerde berichten (in XML) nodig zijn. Digikoppeling heeft profielen voor signing en encryption.	...
Digikoppeling REST API	Digikoppeling REST API heeft een GET methode waarmee synchrone requests kunnen uitgevoerd. Digikoppeling REST API kent nog geen gestandaardiseerde versies voor signing of encryptie	Bevragen OIN register via de COR API

Tabel 5.1: Synchrone bevraging

§ 5.2 Synchrone Melding

Bij een melding-bevestiging stuurt een service-requester informatie naar de service-provider en de ontvangst wordt synchroon door de service-provider bevestigd. Belangrijk is de schadelijke effecten te voorkomen als een bericht twee keer wordt verzonden (door een time-out) of als meldingen in de verkeerde volgorde binnenkomen.

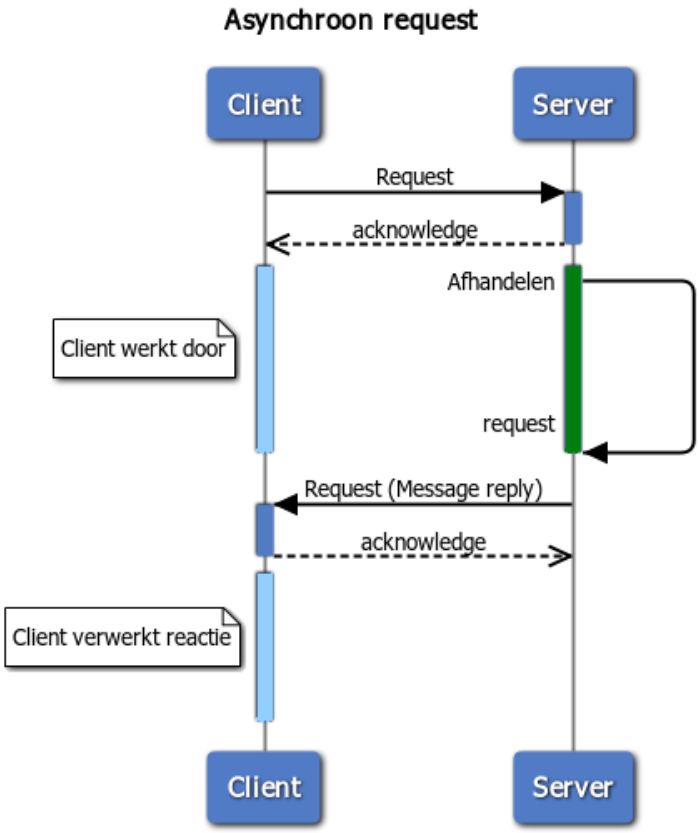
Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling WUS	Digikoppeling WUS is geschikt als voor de melding een gestructureerde bericht (in XML) nodig is. Digikoppeling heeft profielen voor signing en encryption. Voorwaarde is dat de melding *idempotent* is	...

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling REST API	Digikoppeling REST API heeft een PUT methode waarmee synchrone requests kunnen uitgevoerd. Digikoppeling REST API kent nog geen gestandaardiseerde versies voor signing of encryptie Het Digikoppeling REST API profiel kent ook een POST methode. POST is niet idempotent en kan dus niet herhaaldelijk worden verzonden	Binen Haal-Centraal kan een nieuwe resource worden gecreeerd in de Basisadministratie zoals de BAG of de BRP

Tabel 5.2: Synchrone Melding

§ 5.3 Asynchrone Melding-bevestiging

Bij een melding-bevestiging stuurt een service-requester informatie naar de service-provider en ontvangt synchroon een bevestiging dat een bericht is ontvangen. op een later moment kan de ontvanger een bericht sturen dat de melding is verwerkt.



Figuur 11 Asynchroon Request

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling ebMS2	Digikoppeling ebMS heeft reliable profiel (osb-rm) dat de bevestiging van ontvangst borgt	formele overdracht van OLO/DSO naar bevoegd gezag
Digikoppeling WUS	Digikoppeling WUS kent geen reliable profiel. Partijen in de keten moeten met elkaar afspraken	...

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
	hoe een melding wordt bevestigd in een antwoord door de ontvanger op een later tijdstip	
Digikoppeling REST API	Digikoppeling REST API heeft een PUT en een POST methode waarmee synchrone requests kunnen uitgevoerd. Digikoppeling REST API kent geen reliable profiel. Partijen in de keten moeten met elkaar afspraken hoe een melding wordt bevestigd in een antwoord door de ontvanger op een later tijdstip. Eventueel als onderdeel van een conversatie op business niveau	Door middel van de PUT methode kan een nieuw bedrijfsadres worden opgegeven bij de KVK API en d.m.v. POST kan het bedrijf worden genotificeerd over de status van de verhuismelding

Tabel 5.3: Asynchrone Melding-bevestiging

§ 5.4 Uitwisselen grote bestanden

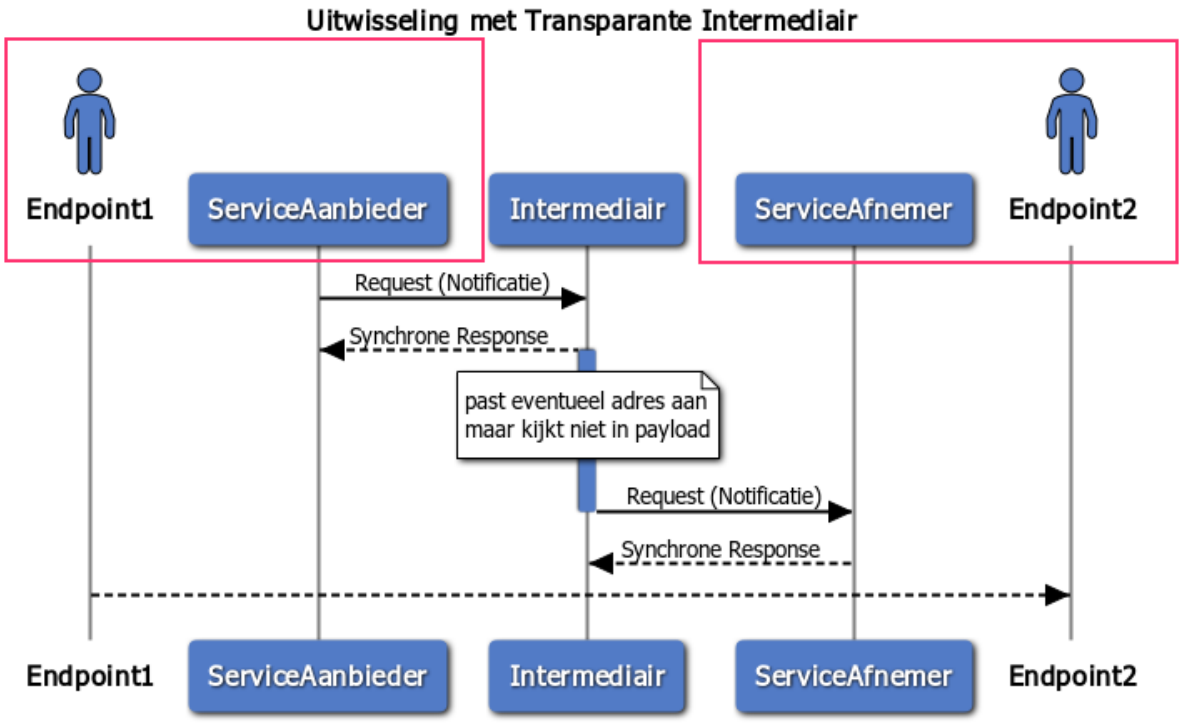
De situatie kan zich voordoen dat een bericht een omvang krijgt die niet meer efficiënt door de Digikoppeling-adapters verwerkt kan worden bijvoorbeeld vanwege de overhead bij eventuele hertransmissies. Ook kan het voorkomen dat er behoefte bestaat aan het sturen van aanvullende informatie naar systemen buiten de normale procesgang ('out-of-band').

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling Grote berichten	Bij ‘grote berichten’ worden grotere bestanden uitgewisseld via een van de Digikoppelingkoppelvlakken in combinatie met een (HTTPS-)download vanaf een beveiligde website. Grote berichten vormen een functionele uitbreiding op de Digikoppelvlakstandaarden voor de veilige bestandsoverdracht van berichten groter dan 20 MiB	Decentrale overheden uploaden hun archief bestanden bij de grote berichten service van het Nationaal archief en dragen via een Digikoppeling koppelvlak de verantwoordelijkheid voor de archiefstukken over

Tabel 5.4: Uitwisselen grote bestanden

§ 5.5 Uitwisseling via een transparante intermediair

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.



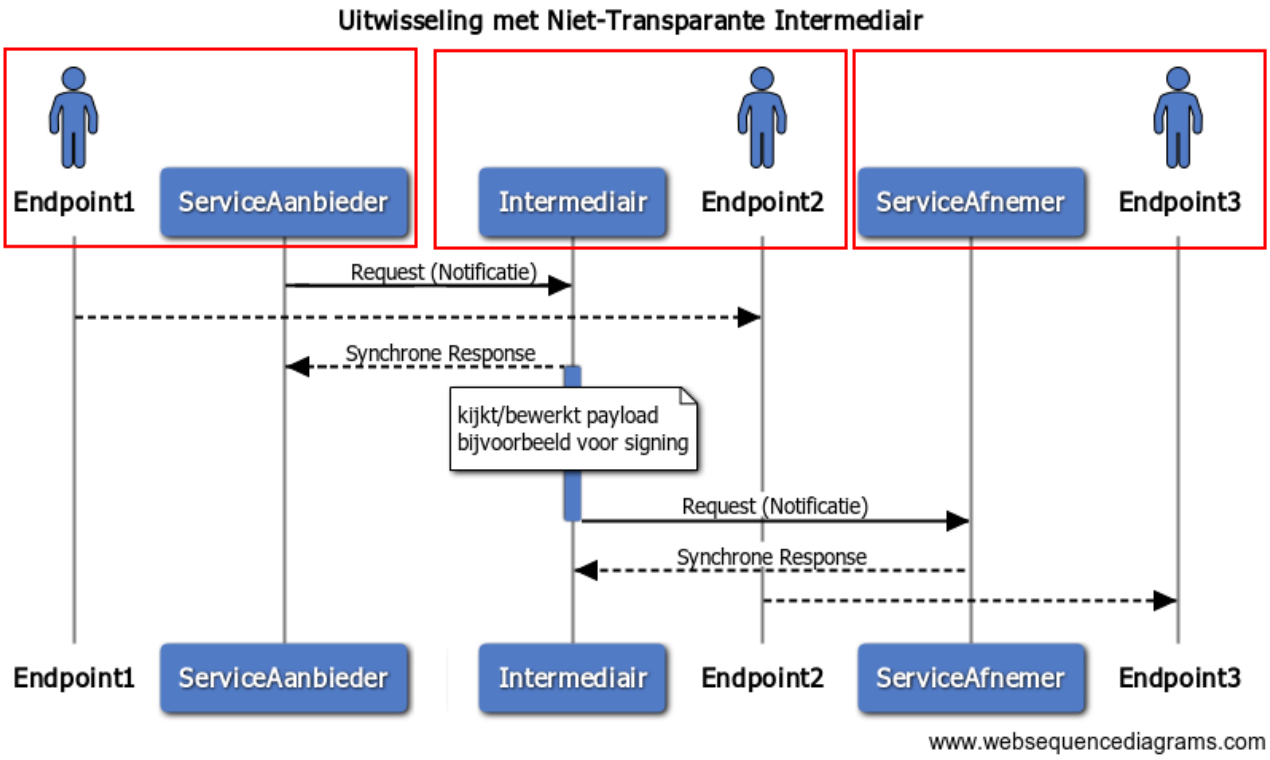
Figuur 12 Transparante Intermediair

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling WUS	Gebruik Digikoppeling WUS header voor routering	...
Digikoppeling ebMS	Gebruik Digikoppeling ebMS header voor routering	...

Tabel 5.5: Transparante intermediair

§ 5.6 Uitwisseling via een niet-transparante intermediair

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 bewerkt moet worden voor verdere verzending.



Figuur 13 Niet-Transparante Intermediair

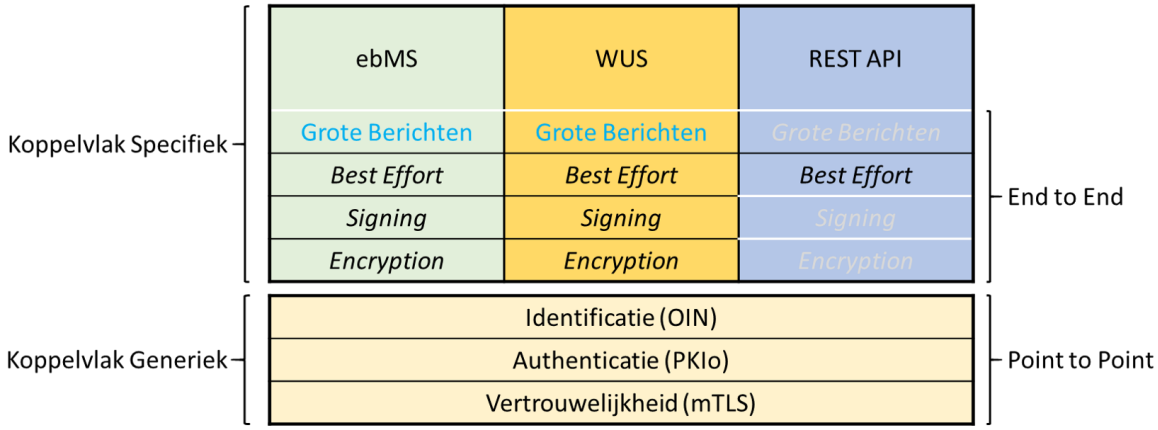
Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling WUS	Gebruik Digikoppeling WUS header voor routering	...
Digikoppeling ebMS	Gebruik Digikoppeling ebMS header voor routering	...

Tabel 5.5: Niet-Transparante intermediair

§ 6. Digikoppeling-koppelvlakstandaarden en voorschriften

§ 6.1 Overzicht

De Digikoppeling Architectuur legde in de eerdere versies grote nadruk op bevragingen en meldingen en legde een verband tussen deze interactiepatronen en de onderliggende standaarden, ('WUS voor bevragingen, ebMS voor meldingen en kennisgevingen'). Dit verband bleek in de praktijk niet altijd werkbaar of wenselijk. In 2020 is daarom besloten om de richtlijnen voor het toepassen van de Digikoppeling standaarden te wijzigen.



Figuur 14 Overzicht Digikoppeling Koppelvlakken

Digikoppeling kent vier koppelvlakstandaarden

- WUS voor synchrone uitwisseling van gestructureerde berichten;
- ebMS2 voor asynchrone uitwisseling voor betrouwbaar berichtenverkeer;
- REST API voor synchrone gegevensuitwisseling met resources;
- Grote berichten voor het uitwisselen van grote bestanden;

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:

- 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 synchrone uitwisseling van gestructureerde berichten en de WUS profielen.
Koppelvlakstandaard ebMS2	Het gebruik van ebMS2 voor asynchrone uitwisseling en de ebMS2 profielen
Koppelvlakstandaard REST API	Het gebruik van REST APIs voor het synchroon raadplegen en bewerken van resources
Koppelvlakstandaard Grote Berichten	De uitwisseling van grote berichten maakt gebruik van WUS, ebMS2 of (indien gewenst) REST met HTTPS bestandsoverdracht

Onderdeel	Toelichting
Beveiligingstandaarden en voorschriften	Beschrijft de beveiligingstandaarden (TLS, signing en encryption) voor de Digikoppeling profielen WUS, ebMS2 en Grote berichten
Identificatie en Authenticatie	Beschrijft de identificatie van partijen, het opzetten van een tweezijdige beveiligde TLS-verbinding en over het ondertekenen en versleutelen van berichten en bijlagen.
Overzicht Actuele Documentatie en Compliance	Overzicht van de actuele versie van de Digikoppeling specificaties (normatief en niet-normatief)
Gebruik en Achtergrond Digikoppeling Certificaten	Beschrijft de werking en gebruik van PKIoverheid Certificaten (niet-normatief)

Tabel 6.1: Digikoppeling-standaarden

§ 6.2 Digikoppeling-voorschriften

Enkele afspraken over de functionaliteit van Digikoppeling hebben betrekking op de Digikoppeling-keten als geheel waar behalve de koppelvlakstandaarden ook partijen, intermediairs 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 (ook intermediairs) 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 medewerkerniveau.	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 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 logistieke 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.

Aspect	Voorschrift	Toepassing en uitleg
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 6.2: Digikoppeling-voorschriften

§ 6.3 REST API's

Het Digikoppeling REST API profiel [Digikoppeling Koppelvlakstandaard REST API] is gebaseerd op de REST API Design Rules die in 2020 door het Kennisplatform API's zijn ontwikkeld.

Een application programming interface (API) is een gestructureerd en gedocumenteerd koppelvlak voor communicatie tussen applicaties. In de laatste 10 jaar heeft *REpresentational State Transfer* (REST) zich ontwikkeld tot een bepalend principe voor het realiseren van API's.

De standaard REST API Design Rules geeft een verzameling basisregels voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST API's aanbiedt. Dit maakt het voor ontwikkelaars gemakkelijker om betrouwbare applicaties te ontwikkelen met API's van de overheid. REST API's kunnen worden gebruikt voor het laagdrempelig bevragen van resources maar ook voor het creëren en muteren van resources.

§ 6.3.1 Digikoppeling REST API voor synchrone requests

[Digikoppeling Koppelvlakstandaard REST API] biedt de volgende functionaliteiten:

- Vertrouwelijkheid
- Identificatie en authenticatie van partijen
- Versleuteling op basis van mTLS conform de Digikoppeling Beveiligings voorschriften
- (Status)Responsecodes en Foutmeldingen

§ 6.3.2 OAS: OpenAPI Specification

Een OpenAPI Specification [openapi] beschrijft de eigenschappen van de data die een API als input accepteert en als output teruggeeft. OAS specificeert alleen welke attributen de API verwerkt en hun datatypen, niet welke implementatie er achter de API schuilgaat.

Voor het beschrijven van DK-Rest API's is het gebruik van OAS verplicht. Op [Pas-toe-of-leg-uit] staat beschreven welke versie toegepast moet worden.

§ 6.4 WUS

6.4.1 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 webservice standaarden uit de profielen van de OASIS “Web Services – Basic Reliable and Secure Profiles” Technical Committee (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.

27: Voorheen Web Services Interoperability (WS-I) organization

6.4.2 Digikoppeling WUS voor synchrone bevragingen

De *Digikoppeling-koppelvlakstandaard WUS* [Digikoppeling Koppelvlakstandaard WUS] ondersteunt het uitvoeren van synchrone requests tussen geautomatiseerde informatiesystemen.

[Digikoppeling Koppelvlakstandaard WUS] biedt de volgende functionaliteiten:

- 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

6.4.3 WSDL: Web Services Description Language

Een WSDL is een formeel xml-document om de gebruikte functionele en technische eigenschappen van de (XML-)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.

§ 6.5 ebMS

§ 6.5.1 ebMS2 familie van standaarden

Digikoppeling maakt gebruik van een familie van standaarden die we “ebMS2” noemen. Deze familie van standaarden is gebaseerd op web-service standaarden uit de profielen van de OASIS “ebXML Messaging Services“ Technical Committee (ebMS2).

Kenmerkend voor de ebMS2-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.

§ 6.5.2 Digikoppeling ebMS2 voor betrouwbare, asynchone uitwisseling

De *Digikoppeling-koppelvlakstandaard ebMS2* [Digikoppeling Koppelvlakstandaard ebMS2] ondersteunt het uitvoeren van asynchrone berichten 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 retourmelding.`

De Koppelvlakstandaard ebMS2 regelt de volgende functionaliteiten: :

- 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 tijdstempel (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

6.5.3 CPA

Een CPA is een formeel xml-document om de gebruikte functionele en technische eigenschappen van de ebMS2 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 ebMS2 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 ebMS2. Het CPA Register ondersteunt partijen in het creëren van een CPA.

6.6 Grote berichten

6.6.1 Werking grote berichten

De situatie kan zich voordoen dat een Digikoppelingbericht een grootte krijgt die niet meer efficiënt door de Digikoppelingadapters en -services verwerkt kan worden. Ook kan er behoefte zijn 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, ebMS2 of eventueel REST wordt referentie (link) verstuurd;
- de referentie verwijst naar de locatie van het grote bestand. Het hangt af van het gebruikte Digikoppeling Grote berichten profiel of de ontvanger het bestand moet downloaden of dat de zender het grote bestand inmiddels als naar de ontvanger heeft geupload.

Het grote bericht zelf zal vaak volledig in het grote bestand zijn opgenomen; het WUS, ebMS2 of REST-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/ebMS2/REST) 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.

6.6.2 Standaarden voor grote berichten

De *Digikoppeling Koppelvlakstandaard Grote Berichten* [Digikoppeling Koppelvlakstandaard Grote Berichten] maakt gebruik van WUS, ebMS2 of REST 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 de andere koppelvlakstandaarden. Ook is het gebruik van transparante intermediairs mogelijk.

[Digikoppeling Koppelvlakstandaard Grote Berichten] regelt de volgende functionaliteiten, in aanvulling op WUS of ebMS2

- 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.

7. Overzicht Use Cases

In dit hoofdstuk beschrijven we een aantal usecases waarbij er een specifiek Digikoppeling Koppelvlak vaak een voorkeur heeft.

Voordat er een keuze wordt gemaakt voor een koppelvlak uit de opties die Digikoppeling biedt, is het belangrijkste dat goed geanalyseerd wordt wat eigenlijk de aard is van de uit te wisselen gegevens of bestanden is en de context waarin deze keuze gemaakt dient te worden. Een keuze voor het een of ander is bij voorbaat eigenlijk nooit goed of fout te noemen. Het gaan om welke implementatie het beste past bij de requirements van de betrokken organisatie(s) en de beschikbare capabiliteiten binnen de organisatie.

7.1 Hulpmiddel voor een keuze voor een Digikoppeling Koppelvlak

Relevante vragen voor het maken van een keuze zijn:

7.1.1 Hoeveel partijen zijn er betrokken bij de koppeling en wat is hun rol?

Voorbeelden:

- 1 service provider, n service consumers. Hier kan een service provider er voor kiezen meerdere koppelvlakstandaarden aan te bieden (bijvoorbeeld REST API en WUS).

- Many to many: Meerdere partijen die allemaal objecten kunnen versturen en ontvangen. Voor deze koppeling worden een REST API koppelvlak vaak gebruikt.
- 1-op-1: twee partijen die onderling objecten uitwisselen. Hierbij kunnen partijen om een specifiek contract af te spreken, zoals in een CPA bij ebMS.

§ 7.1.2 Wat is de aard van de gegevens/objecten die uitgewisseld moeten worden?

Voorbeelden:

- Niet nader gespecificeerde Pdfs die van A naar B moeten, met metadata
- Hele grote Bestanden

Hier kan Digikoppeling Grote Berichten (via ebMS of WUS) gebruikt worden.

§ 7.1.3 Het uitwisselen van relationele bedrijfsgegevens over objecten, 'Bedrijfsdocumenten'

Voorbeelden:

- de volledige gegevens van een GBA inschrijving of de gegevens van een rechtszaak

Hier kan voor Digikoppeling WUS gekozen worden, omdat in deze uitwisseling vaak een gestructureerde berichtformaat wordt gehanteerd in combinatie met WSDL en XSD. Digikoppeling REST API is hiervoor ook mogelijk.

§ 7.1.4 Raadplegen of muteren van een bron

Voorbeelden:

- Een centrale website die een object opvraagt bij op een achterliggende bron.
- Het aanmaken, bewerken of verwijderen van een publicatie op de Staatscourant.

Hier kan Digikoppeling REST API gebruikt worden. Digikoppeling WUS is hiervoor ook mogelijk.

§ 7.2 Andere overwegingen voor een keuze van een koppelvlak

§ 7.2.1 Capabiliteit van een organisatie, bestaande infrastructuur

Wat zijn de capabiliteiten van de organisaties die met elkeaar gegevensuitwisselen. Bijvoorbeeld wordt er al gebruik gemaakt van Digikoppeling WUS of ebMS, of juist niet. beschikt de organisatie over eigen ontwikkelteam, of maakthet gebruik van een partner of leverancier.

- Zijn er al koppelingen in gebruik tussen partijen?.

- Zo ja welke; als hergebruik mogelijk is, kan dat vaak voordelen opleveren omdat men al bekend is met de technieken en de beheerprocessen reeds op volwassen wijze ingericht zijn.

Dit kan een hele valide reden zijn om voor een bepaalde variant te kiezen, ook al zijn er technische argumenten te maken dat een ander type in theorie beter zou passen.

§ 7.3 Overzicht Usecase

§ 7.3.1 Overdracht van verantwoordelijkheid

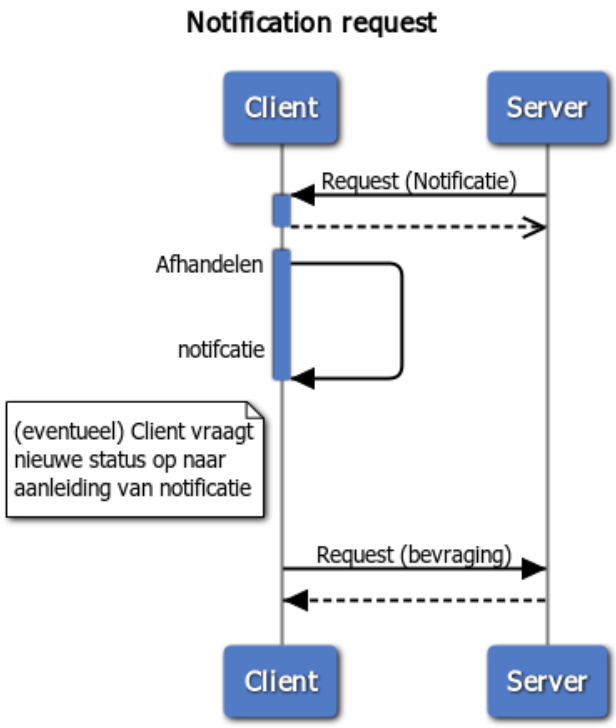
Bij deze case gaat het om een overdracht van verantwoordelijkheden, zoals het bevoegd gezag - bevoegd om besluiten te nemen over een onderwerp - van een overheidsorganisatie naar een andere organsatie. Hierbij is het essentieel dat beide partijen zekerheid over de de overdracht, omdat er bepaalde wettelijke termijnen kunnen bestaan waarin besluiten genomen moeten worden.

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling ebMS2	Digikoppeling ebMS kent een betrouwbaar profiel (osb-rm) dat de bevestiging van ontvangst borgt. Digikoppeling ebMS ondersteunt ook de mogeijkheid van onweerlegbaarheid (non-repudiation) in de vorm van een ondertekende ontvangstbevestiging	formele overdracht van OLO/DSO naar bevoegd gezag

Tabel 7.1: Overdracht van verantwoordelijkheid

§ 7.3.2 Abonneren op wijzigingen middels notificaties

Deze case is bedoeld voor ketens die authentieke informatie willen 'halen bij de bron' in plaats van het synchroniseren van registraties. Hiervoor is het essentieel dat organisaties worden genotificeerd bij wijzigingen.



Figuur 15 Notificatie Request

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling ebMS	Digikoppeling ebMS heeft reliable profiel (osb-rm) dat de bevestiging van ontvangst borgt. Hiermee heeft de aanbiedende partij de zekerheid dat een notificatie door de ontvanger is ontvanger	Digilevering ontvangt gebeurtenisberichten van basisregistraties en zendt deze door naar geabonneerde overheidsorganisaties
Digikoppeling REST API	Een client abonneert zich met POST request op wijzingen in een bepaalde bron van een Provider (en kan muteren met PUT of DELETE request). Een bronhouder informeert een abonnee met een POST request bij een wijzingen. De afnemer haalt de wijzingen op via een GET reequest.	VNG werkt aan afspraken voor decentrale notificatieservices

Tabel 7.2: Notification request

§ 7.3.3 End-to-End security

Een bericht wordt beveiligd tussen de uiteindelijke consumer en de uiteindelijke provider, ook wanneer er zich intermediairs bevinden in het pad tussen die twee. Het betreft hier authenticatie van de consumerorganisatie, conform het Digikoppeling authenticatiemodel, waarbij alleen de identiteit van de consumerorganisatie relevant is(signing), en encryptie van het bericht (payload inclusief attachments) onderweg

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling ebMS	Digikoppeling ebMS kent profielen voor signing en encryption. Digikoppeling ebMS ondersteunt ook de mogeijkheid van onweerlegbaarheid (non-repudiation) in de vorm van een ondertekende ontvangstbevestiging	

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling WUS	Digikoppeling WUS kent profielen voor signing en encryption	

Tabel 7.2: End-to-End security

7.3.4 Betrouwbaar berichtenverkeer op protocol niveau (reliable messaging)

Bij Betrouwbaar berichtenverkeer verstuurt de service-requester een bericht 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.`

Voor betrouwbare uitwisseling op niet-protocol niveau, zie paragraaf melding-transactie.

Koppelvlakspecificatie	Omschrijving	Praktijkvoorbeeld
Digikoppeling ebMS	Digikoppeling ebMS kent profielen voor signing en encryption. (reliability out of the box). Retry maakt bijvoorbeeld onderdeel uit van dit protocol	

Tabel 7.3: Betrouwbaar berichtenverkeer (reliable messaging)

8. Digikoppeling-voorzieningen

8.1 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:

- het Digikoppeling Portaal met daarin de Compliancevoorziening,- WUS en ebMS2 voor het testen van services;
- het CPA Register voor het creëren van een CPA (tbv ebMS2 berichtuitwisseling);
- De Centrale OIN Raadpleegvoorziening (COR) voor het raadplegen van het OIN register. Het OIN staat voor het Organisatie Identificatienummer.

Digikoppeling adapters of applicaties kunnen worden getest op compliance met de koppelvlakstandaarden via de Digikoppeling Compliance voorziening. deze is beschikbaar op de Logius Gitlab omgeving.

Functionaliteit	Uitleg	Invulling
Compliance WUS services	WUS services kunnen worden getest op compliance met de Digikoppeling-koppelvlakstandaard WUS.	Digikoppeling Compliancevoorziening WUS

Functionaliteit	Uitleg	Invulling
Compliance ebMS2 services	ebMS2 services kunnen worden getest op compliance met de Digikoppeling-koppelvlakstandaard ebMS2.	Digikoppeling Compliancevoorziening ebMS2
Compliance Grote Berichten	Grote berichten kunnen in combinatie met WUS of ebMS2 services worden getest op compliance met de koppelvlakstandaarden	Digikoppeling Compliancevoorziening WUS en ebMS2
CPA Register	Een CPA-contract voor ebMS2 services tussen twee partijen kan via het CPA Register worden opgesteld en beheerd.	CPA Register
OIN Register	Het OIN bevat alle uitgegeven Organisatie identificatienummers waarmee organisaties zich uniek identificeren bij het uitwisselen van berichten.	Digikoppeling Portaal – OIN Register (COR)
API Discovery	Op developer.overheid.nl zijn alle API's van de Ned. overheid terug te vinden en is ook na te gaan of de API's voldoen aan de eisen van de API Design Rules. Ben je een developer die iets voor of met de overheid ontwikkelt? Dan vind je hier handige bronnen en de community voor de ontwikkeling van jouw digitale services.	Developer.overheid.nl

Tabel 8.1: Ondersteunende functionaliteiten van de Digikoppeling-voorzieningen

§ 8.2 Compliancevoorzieningen

Met de WUS compliancevoorziening kan een organisatie controleren of haar adapter of programmatuur voldoet aan de WUS koppelvlakstandaard. Met de ebMS2 compliancevoorziening kan een organisatie controleren of haar adapter of programmatuur voldoet aan de ebMS2 koppelvlakstandaard.

De volgende compliancevoorzieningen zijn beschikbaar: [28]

- Digikoppeling-WUS compliancevoorziening voor het testen van synchroon berichtenverkeer op basis van WUS, inclusief grote berichten.
- Digikoppeling-ebMS2 compliancevoorziening voor het testen van asynchroon berichtenverkeer op basis van ebMS2, inclusief grote berichten.

> Informatie over de compliancevoorzieningen staat op [Digikoppeling Compliance Voorziening].

28: Digikoppeling Koppelvlakstandaard WUS

§ 8.3 OIN Register (Centrale OIN Raadpleegvoorziening)

Logius beheert de Centrale OIN Raadpleegvoorziening (COR) waarin uitgegeven Organisatie identificatienummers zijn gepubliceerd. Dit register is openbaar raadpleegbaar en zowel via het web als via een REST API bevraagbaar.

Het OIN register is te vinden op https://portaal.digikoppeling.nl/registers

§ 8.4 CPA Register

Het CPA Register wordt gebruikt voor het opstellen van een CPA (servicebeschrijving) voor ebMS2 uitwisselingen. Een CPA is een formeel xml-document dat de functionele en technische eigenschappen van de ebMS2-protocolkarakteristieken vastlegt. Het is dus een format voor afspraken over de gegevensuitwisseling met ebMS2.[29]

Het CPA Register 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 ebMS2 gegevens willen uitwisselen.
- Het automatiseert de configuratie van de ebMS2 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 Best Practices ebMS2. Het CPA Register is beschreven in de Gebruikershandleiding. Het CPA register is te vinden op https://cparegister.minvenj.nl

29: *Digikoppeling Best Practices ebMS*</sup

§ 9. Implementatie van Digikoppeling

§ 9.1 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 https://www.logius.nl/digikoppeling/.

§ 9.1.1 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, resources en/of interfaces gedefinieerd?
- Is er sprake van grote berichten (bestanden groter dan 20 MiB)?
- 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?

§ 9.1.2 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 gegevensuitwisseling 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.

§ 9.1.3 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 REST API, WUS of ebMS2. 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 ebMS2.

De volgende kenmerken zijn onderkend:

- Best effort – geschikt voor bevragingen (WUS en REST API)

- Betrouwbaar (reliable) – geschikt voor meldingen (ebMS)
- Signed – geschikt voor de ondertekening van berichten (WUS en ebMS2)
- Encrypted – geschikt voor de versleuteling van de payload en attachments (WUS en ebMS2)

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	DK REST API profiel	DK WUS profiel	DK ebMS2 profiel
Bevragingen / Meldingen			
best-effort	1.0	2W-be	osb-be
best-effort signed		2W-be-S	osb-be-s
best-effort signed/encrypted		2W-be-SE	osb-be-e
reliable*			osb-rm
reliable signed			osb-rm-s
reliable signed en encrypted			osb-rm-e

Tabel 9.1: Profielen in relatie tot Digikoppeling-voorschriften

> *Met reliable wordt hier aangegeven of het profiel specifieke functionaliteit biedt voor het herzenden en gegarandeerd afleveren van data als onderdeel van het profiel (dwz bovenop de basisondersteuning van de betrouwbaarheid van het netwerk protocol (TCP/IP) dat voor elk van deze profielen geldt)

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 ebMS2-profielen.

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

- Gaat het om berichten (of bijlagen) groter dan 20 MiB? Stem eerst af met uw ketenpartner of Digikoppeling Grote Berichten gebruikt moet worden.
- Is snelheid belangrijker dan betrouwbaarheid? Kies dan voor een koppelvlakstandaard dat synchrone bevragingen ondersteunt, REST API of WUS.
- Is betrouwbaarheid belangrijker, kies dan voor een koppelvlakstandaard dat reliable messaging ondersteunt (ebMS).
- 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.

§ 9.1.4 Servicebeschrijvingen

Gestructureerde gegevensuitwisseling 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 of antwoorden van een service zelf zijn in een technisch formaat (XML bij WUS en ebMS, JSON bij REST API) beschreven. Servicebeschrijvingen worden opgesteld door een serviceaanbieder (bijvoorbeeld een basisregistratie).

Een servicecontract voor een ebMS2 service heet een CPA. Dit contract wordt afgesloten tussen de serviceaanbieder en serviceafnemer. Een CPA moet worden gecreëerd via het CPA-Register 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 (synchrone request) kan door meerdere afnemers worden gebruikt. Een WSDL wordt door een aanbiedende partij opgesteld.

De beschrijving voor een REST API service heet een OAS. Deze beschrijving wordt opgesteld door de aanbieder van de service. Een OAS voor een API Servicecall kan door meerdere afnemers worden gebruikt.

§ 9.1.5 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[30]. In de gegevensuitwisseling 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.
- 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.

30: Voorzover het de voorzieningen betreft die voor partijen benaderbaar zijn.

§ 9.2 Relatie met de inhoudelijke laag

§ 9.2.1 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.

§ 9.2.2 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. 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.

§ 9.2.3 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.

§ 9.2.4 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.

§ 9.2.5 Berichtinhoud en semantiek

Digikoppeling gaat over de uitwisseling van gegevens. Binnen Digikoppeling wordt een bericht dat uitgewisseld wordt met WUS of ebMS conform de SOAP[31] messaging protocol samengesteld.

Bij het gebruik van het Digikoppeling REST API profiel is er geen sprake van berichtuitwisseling. In dit profiel wordt een service met een Application Programming Interface (API) een resource aangeboden die door een gebruiker kan worden bevraagd of bewerkt, afhangend wat de API en de autorisatie eisen toelaat. De aanroep van een resource vindt plaats met HTTP-request. De HTTP-response bevat JSON of XML.

Een bericht (WUS of ebMS) bestaat uit de volgende onderdelen:

- Een bericht header (envelop)

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

Een bericht (WUS of ebMS) voldoet aan de volgende eisen:

- Alle berichten, zowel WUS als ebMS2, hebben een unieke identificatie. De gekozen structuur is geldig in de ebMS2-omgeving en in de WUS-omgeving. Zo kan dezelfde berichtidentificatie gebruikt worden in zowel een ebMS2-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 XML[32]
- 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.

31: SOAP (Simple Object Access Protocol) is een computerprotocol dat wordt gebruikt voor communicatie tussen verschillende componenten van systemen.

32: Attachments mogen andere formaten hebben.

§ 9.2.6 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.

§ 9.3 Relatie met de transportlaag

§ 9.3.1 Randvoorwaarden transport

Digikoppeling stelt ook randvoorwaarden op het niveau van het transport:

- Gebruik van HTTPS
- Gebruik van TCP/IP stack.

- Gebruik van HTTPS voor grote berichten.
- Gebruik van tweezijdig TLS voor het veilig transporteren van gegevens via internet is verplicht.

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

§ 9.3.2 Inleiding transportlaag

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.

§ 9.3.3 Transport Level Security (TLS)

Alle Digikoppeling-koppelvlakstandaarden 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 beveiliging op berichtniveau (signed of signed en encrypted profielen).

Zie '*Digikoppeling beveiligingsstandaarden en voorschriften'* voor meer informatie over de door Digikoppeling vereiste beveiligingsstandaarden en cipher suites voor signing en encryptie.

§ 9.3.4 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' [33]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 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.

33: DNS 'resolving' is het opzoeken van de domeinnaam en het bijbehorend IP-adres, conform het DNS protocol.

9.3.5 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.

10. Bijlage A: Bronnen

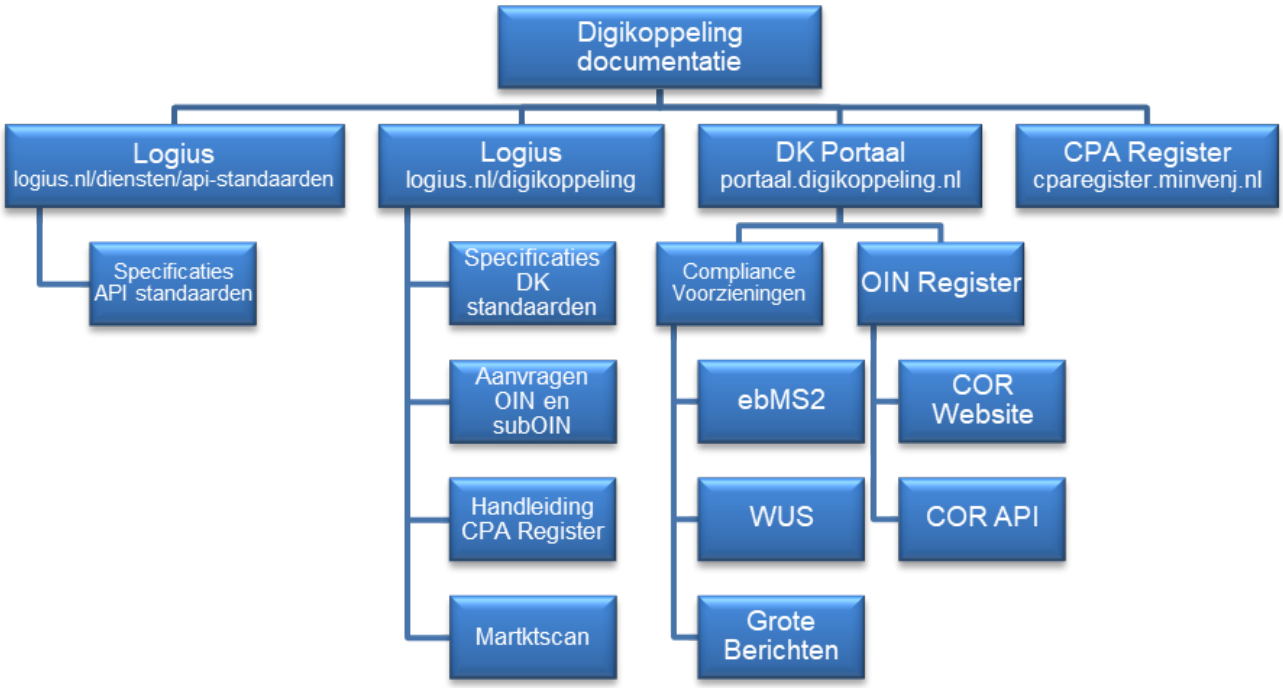
Alle goedgekeurde Digikoppeling documenten zijn beschikbaar op https://www.logius.nl/diensten/digikoppeling/documentatie

10.1 Digikoppeling-standaarden en gerelateerde documenten

Documentnaam	Auteur(s)
Digikoppeling Architectuur (dit document)	Logius Centrum voor Standaarden
[Digikoppeling Koppelvlakstandaard REST API]	Logius Centrum voor Standaarden
[Digikoppeling Koppelvlakstandaard WUS]	Logius Centrum voor Standaarden
[Digikoppeling Koppelvlakstandaard ebMS2]	Logius Centrum voor Standaarden
[Digikoppeling Koppelvlakstandaard Grote Berichten]	Logius Centrum voor Standaarden
[Digikoppeling Beheermodel]	Logius Centrum voor Standaarden
[Digikoppeling Beveiligingsdocument]	Logius Centrum voor Standaarden
[Digikoppeling Identificatie-Authenticatie]	Logius Centrum voor Standaarden
[Digikoppeling Actuele Documentatie]	Logius Centrum voor Standaarden
[Digikoppeling Gebruik Certificaten]	Logius Centrum voor Standaarden
[Digikoppeling Best Practices WUS]	Logius Centrum voor Standaarden
[Digikoppeling Best Practices ebMS2]	Logius Centrum voor Standaarden
[Digikoppeling Best Practices Grote Berichten]	Logius Centrum voor Standaarden

Tabel 10.1: Digikoppeling-standaarden en gerelateerde documenten

10.1.1 Digikoppeling documentatie



Figuur 16 Digikoppeling Documentatie

Overige Digikoppeling documentatie

Documentnaam	Auteur(s)	Status
Handleiding aansluiten	Logius	Definitief
Serviceniveau overeenkomst (SNO)	Logius	Definitief
Aansluitvoorwaarden Digikoppeling	Logius	
Gebruikershandleiding Digikoppeling Portaal	Logius	Definitief
Handleiding CPA Register	Logius	Definitief

Tabel 10.2: Overige Digikoppeling documentatie

10.1.2 Overige geraadpleegde bronnen

Documentnaam	Versie	Datum	Auteur(s)	Status
Architectuurschets van het stelsel voor gegevensuitwisseling	1.0	17-06-	W. Bakkeren, A. van Weel	Definitief

Documentnaam	Versie	Datum	Auteur(s)	Status
		2013		
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	1.0	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	Gepubliceerd
NORA 3.0 Katern Strategie	1.0	19-8-2009	Noraonline.nl	Gepubliceerd
NORA 3.0 Informatiebeveiliging, 2010	1.0	2010	Noraonline.nl	Gepubliceerd
NORA 3.0 vording Principes voor samenwerking en dienstverlening	Ntb	29-9-2010	Jasper van Lieshout	Definitief
NORA Beeldtaal	Ntb	13-11-2012	ICTU	

Tabel 10.3: Overige geraadpleegde bronnen

§ 11. 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.

Begrip	Uitleg
ADR	De API Design Rules zijn een set van normatieve regels die moeten worden toegepast bij het ontwerpen en toepassen van API's
API	API ofwel Application Programming Interface zoals gedefinieerd door de NORA
API Kennisplatform	Samenwerkingsverband tussen overheden om te komen tot een gedeelde API Strategie voor NL.
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 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 CanReceive (CPA)	Elementen in het ebMS CPA om aan te geven dat een partij een 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

Begrip	Uitleg
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.
Developer.overheid.nl (DON)	Developer.overheid.nl is één centraal platform voor de developer die voor of met de overheid ontwikkelt. Het platform focused zich op API's en repositories die developers kunnen gebruiken
Dienst	Een geautomatiseerde gegevensuitwisseling 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-keten	De uitwisseling van gegevens tussen systemen van partijen via de Digikoppeling-koppelvlakstandaarden.
DK	Digikoppeling
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 REST	Beschrijving hoe REST APIs toegepast moeten worden voor Digikoppeling in de logistieke laag.
DK-koppelvlakstandaard WUS	Beschrijving hoe WUS toegepast moet worden voor Digikoppeling in de logistieke laag.
DK-profiel	Zie: Profiel
DK-standaarden	De Digikoppeling Architectuur en de Digikoppeling-koppelvlakstandaarden.
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

Begrip	Uitleg
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 gegevensuitwisseling tussen twee partijen. `todo` 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

Begrip	Uitleg
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.
OAS	OAS ofwel de Open API Specification zoals voorgeschreven op de lijst van verplichte standaarden van het Forum Standaardisatie. OAS wordt gebruikt voor het beschrijven van REST API's.
OIN	Zie: Organisatieidentificatienummer
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.
Organisatieidentificatienummer (OIN)	Een uniek identificerend nummer voor organisaties.
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

Begrip	Uitleg
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
Resource	Oorspronkelijk in de context van het World Wide Web gedefinieerd als documenten of bestanden die met een URL worden geïdentificeerd. Tegenwoordig kan een resource alles zijn dat met een URL kan worden benaderd, zoals een applicatie of voorziening, een lijstje en nog steeds een document of een bestand. *"The HTTP client and HTTP server exchange information about resources identified by URLs. We say that the request and response contain a representation of the resource. By representation, we mean information, in a certain format, about the state of the resource or how that state should be in the future. Both the header and the body are pieces of the representation."* (source:https://code.tutsplus.com/tutorials/a-beginners-guide-to-http-and-rest--net-16340)
REST API	Een REST API ofwel een REpresentational State Transfer API bestaat uit een set van principes voor het vormgeven van een API die faciliteert in de bewerking van de state van een resource.
Sectoraal knooppunt	Intermediair die de gegevensuitwisseling faciliteert tussen partijen in een samenwerkingsverband.

Begrip	Uitleg
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.
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.
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

Begrip	Uitleg
	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 te allen tijde bepaald kan worden of een XML bericht correct is of niet.

Tabel 11.1: Gebruikte begrippen

§ 12. Bijlage C: NORA Architectuurprincipes

De NORA (Nederlandse Overheids Referentie Architectuur) is de bron voor de architectuur principes. NORA definieert 10 basisprincipes[34]

34: *Bron: https://www.noraonline.nl/wiki/Principes*

Overzicht

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

zie ook https://www.noraonline.nl/wiki/Basisprincipes_totaaloverzicht

Tabel 12.1: NORA 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

NORA Afgeleide principes	ID	Stelling	Cluster	Realiseert	DK principes
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
Informatie-objecten systematisch beschreven	AP17	De aan de dienst gerelateerde informatieobjecten zijn, uniek geïdentificeerd, in een informatiemodel beschreven.	Informatie	Vindbaar Toegankelijk	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
Uitwisseling berichten onweerlegbaar	AP40	De berichtenuitwisseling is onweerlegbaar	Betrouwbaarheid	Betrouwbaar	DK 4. Betrouwbaarheid
Beschikbaarheid	AP41	De beschikbaarheid van de dienst voldoet aan de met de afnemer	Betrouwbaarheid	Betrouwbaar	DK 4. Betrouwbaarheid

NORA Afgeleide principes	ID	Stelling	Cluster	Realiseert	DK principes
		gemaakte continuïteitsafspraken.			
Vertrouwelijkheid (principe)	AP43	De dienstverlener zorgt ervoor dat de beoogde toegang tot gegevens en de juiste werking van zijn systemen continu alsook achteraf te controleren is.	Betrouwbaarheid	Betrouwbaar Vertrouwelijk	DK 3. Veiligheid en vertrouwelijkheid

Tabel 12.2: Relevante afgeleide NORA principes en mapping naar Digikoppeling (DK) principes zie https://www.noraonline.nl/wiki/Afgeleide_principes_tabel

13. 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.

13.1 Ontkoppeling van de drie lagen

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 webservices 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.

De Digikoppeling-keten heeft geen actieve logistieke componenten tussen de adapters van de serviceafnemer en de serviceaanbieder. Performance, snelheid en beschikbaarheid worden alleen bepaald door het netwerk en door de serviceaanbieder.

§ 13.2 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.

§ 13.3 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.

§ 13.4 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://www.forumstandaardisatie.nl/open-standaarden/verplicht.

Wijzigingen op de standaard worden conform het Beheermodel in openbaarheid besproken en beheerd

§ 14. Conformiteit

Naast onderdelen die als niet normatief gemarkeerd zijn, zijn ook alle diagrammen, voorbeelden, en noten in dit document niet normatief. Verder is alles in dit document normatief.

§ 15. Lijst met figuren

Figuur 1 Digikoppeling Standaard

Figuur 2 Soap vs. REST APIs bron upwork.com

Figuur 3 Interne en Externe Gegevensuitwisseling

Figuur 4 Open en Closed OverheidsData

Figuur 5 Segmentering van de communicatie

Figuur 6 Digikoppeling voor Closed Data G2G Uitwisseling

Figuur 7 Digikoppeling voor Closed Data G2B Uitwisseling

Figuur 8 Positionering Intermediair/Sectoraal Knooppunt

Figuur 9 Referentiemodel gegevensuitwisseling

Figuur 10 Synchroon Request

Figuur 11 Asynchroon Request

Figuur 12 Transparante Intermediair

Figuur 13 Niet-Transparante Intermediair

Figuur 14 Overzicht Digikoppeling Koppelvlakken

Figuur 15 Notificatie Request

Figuur 16 Digikoppeling Documentatie

§ A. Referenties

§ A.1 Normatieve referenties

[Digikoppeling Actuele Documentatie]
Digikoppeling Overzicht Actuele Documentatie en Compliance. Logius. URL: http://www.logius.nl/digikoppeling

[Digikoppeling Beheermodel]
Beheermodel en releasebeleid Digikoppeling v1.5. Logius. Oktober 2017. URL: https://publicatie.centrumvoorstandaarden.nl/dk/beheer/

[Digikoppeling Beveiligingsdocument]
Digikoppeling Beveiligingsstandaarden en voorschriften. Logius. 2021. URL: https://publicatie.centrumvoorstandaarden.nl/dk/beveilig/

[Digikoppeling Identificatie-Authenticatie]
Digikoppeling Identificatie en Authenticatie. Logius. URL: https://www.logius.nl/diensten/digikoppeling/documentatie

[Digikoppeling Koppelvlakstandaard ebMS2]
Digikoppeling Koppelvlakstandaard ebMS2. Logius. mei 2019. URL: https://logius-standaarden.github.io/Digikoppeling-Koppelvlakstandaard-ebMS2/

[Digikoppeling Koppelvlakstandaard Grote Berichten]
Digikoppeling Koppelvlakstandaard Grote Berichten. Logius. september 2020. URL: https://logius-standaarden.github.io/Digikoppeling-Koppelvlakstandaard-GB/

[Digikoppeling Koppelvlakstandaard REST API]
Digikoppeling Restful API Profiel (Concept). Logius. februari 2021. URL: https://logius-standaarden.github.io/Digikoppeling-Koppelvlakstandaard-REST-API/

[Digikoppeling Koppelvlakstandaard WUS]
Digikoppeling Koppelvlakstandaard ebMS2. Logius. oktober 2020. URL: https://logius-standaarden.github.io/Digikoppeling-Koppelvlakstandaard-WUS/

[openapi]
OpenAPI Specification. Darrell Miller; Jeremy Whitlock; Marsh Gardiner; Mike Ralphson; Ron Ratovsky; Uri Sarid; Tony Tam; Jason Harmon. OpenAPI Initiative. URL: https://www.openapis.org/

[Pas-toe-of-leg-uit]
Lijst Verplichte standaarden. Forum Standaardisatie. URL: https://www.forumstandaardisatie.nl/open-standaarden/verplicht

§ A.2 Informatieve referenties

[API Design Rules]
API Design Rules (Nederlandse API Strategie IIa). Jasper Roes; Joost Farla. Logius. Juli 2020. URL: https://publicatie.centrumvoorstandaarden.nl/api/adr/

[Digikoppeling Best Practices ebMS2]
Digikoppeling Best Practices ebMS2. Logius. 2019. URL: https://www.logius.nl/diensten/digikoppeling/documentatie

[Digikoppeling Best Practices Grote Berichten]
Digikoppeling Best Practices Grote Berichten. Logius. 2019. URL: https://www.logius.nl/diensten/digikoppeling/documentatie

[Digikoppeling Best Practices WUS]
Digikoppeling Best Practices WUS. Logius. 2019. URL: https://www.logius.nl/diensten/digikoppeling/documentatie

[Digikoppeling Compliance Voorziening]
Digikoppeling Compliance Voorziening. Logius. URL: https://portaal.digikoppeling.nl

[Digikoppeling Gebruik Certificaten]
Digikoppeling Gebruik en achtergrond certificaten. Logius. URL: http://www.logius.nl/digikoppeling

[no-Reliable-messaging]
Nobody Needs Reliable Messaging. Marc de Graauw. infoQ. June 18, 2010. URL: https://www.infoq.com/articles/no-reliable-messaging/

[rfc2818]
HTTP Over TLS. E. Rescorla. IETF. May 2000. Informational. URL: https://httpwg.org/specs/rfc2818.html

[rfc7230]
Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing. R. Fielding, Ed.; J. Reschke, Ed.. IETF. June 2014. Proposed Standard. URL: https://httpwg.org/specs/rfc7230.html

↥