

Digikoppeling Restful API Profiel

Logius Standaard

Versie ter vaststelling 24 maart 2021



[Overzicht standaarden](#)

Deze versie:

<https://logius-standaarden.github.io/Digikoppeling-Koppelvlakstandaard-REST-API/>

Laatst gepubliceerde versie:

<https://publicatie.centrumvoorstandaarden.nl/dk/restapi/>

Laatste werkversie:

<https://logius-standaarden.github.io/Digikoppeling-Koppelvlakstandaard-REST-API/>

Vorige versie

<https://publicatie.centrumvoorstandaarden.nl/dk/restapi/1.0-candidate/>

Redacteurs:

Peter Haasnoot ([Logius](#))

Pieter Hering ([Logius](#))

Doe mee:

[GitHub Logius-standaarden/Digikoppeling-Koppelvlakstandaard-REST-API](#)

[Dien een melding in](#)

[Revisiehistorie](#)

[Pull requests](#)

This document is also available in this non-normative format: [pdf](#)

This document is licensed under a [Creative Commons Attribution 4.0 License](#).

Samenvatting

| Naam | Versie | Status |
|--------------------------------|--------|--------|
| Digikoppeling REST API profiel | 1.0 | Draft |

Status van dit document

Dit is een definitief concept van de nieuwe versie van de standaard. Wijzigingen naar aanleiding van consultaties zijn doorgevoerd.

Inhoudsopgave

Samenvatting

Status van dit document

1. Conformiteit
2. Context voor ontwikkeling van het Digikoppeling REST API profiel
3. Toelichting bij de scope van het Digikoppeling REST API profiel
4. Digikoppeling Restful API profiel

- 4.1 Inleiding
 - 4.1.1 Historie
 - 4.1.2 Toepassingsgebied
- 4.2 Digikoppeling REST-API profiel
 - 4.2.1 Algemeen
 - 4.2.2 Koppelvlak Generiek
 - 4.2.2.1 Vertrouwelijkheid
 - 4.2.2.2 Identificatie & Authenticatie
 - 4.2.3 API Design Rules
 - 4.2.3.1 Toelichting aanduidingen
 - 4.2.3.2 Regels
- 4.3 Afspraken API Design Rules extensies

5. BIJLAGE Gebruik van Signing & Encryptie in de context van HTTP / Rest API

- 5.1 Signing in de context van HTTP Rest
- 5.2 Encryptie in de context van HTTP Rest

A. Referenties

- A.1 Normatieve referenties
- A.2 Informatieve referenties

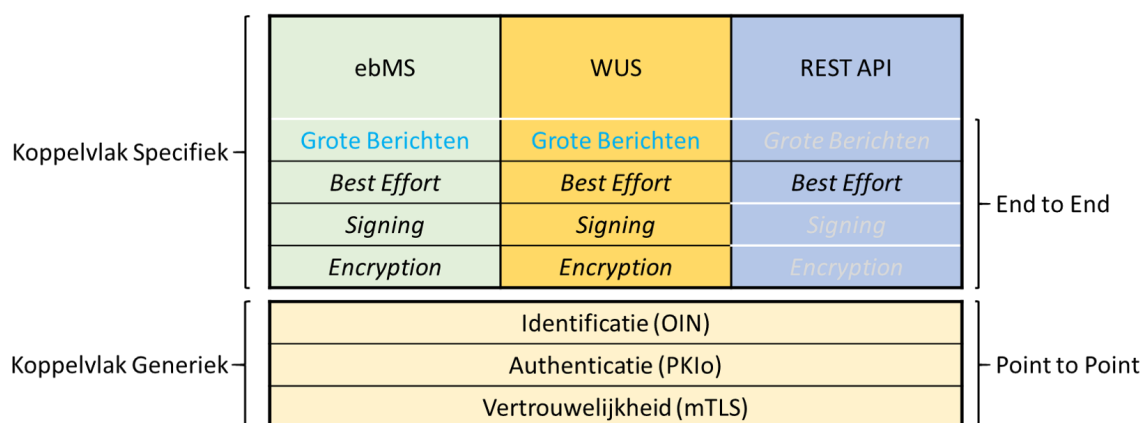
1. Conformiteit

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.

2. Context voor ontwikkeling van het Digikoppeling REST API profiel

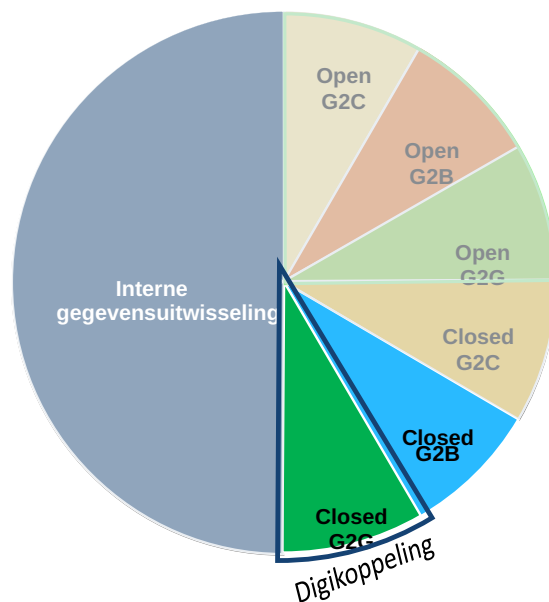
Het Digikoppeling Rest API profiel is gericht op Machine-to-Machine (M2M) en Government-to-Government (G2G) interacties conform de algemene uitgangspunten van de Digikoppeling standaard en het toepassingsgebied van Digikoppeling op de Pas-toe-of-leg-uit lijst (PTLU) van het Forum Standaardisatie;

Opzet Digikoppeling:



Figuur 1 Overzicht Digikoppeling Koppelvlakken

3. Toelichting bij de scope van het Digikoppeling REST API profiel



Figuur 2 Digikoppeling voor Closed Data G2G Uitwisseling

In de figuur wordt onderscheid gemaakt tussen open en gesloten diensten:

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

Het Digikoppeling REST API profiel richt zich op Machine-to-Machine (M2M) gegevensuitwisseling via een gesloten dienst tussen overheidspartijen. Buiten scope van het profiel zijn:

- REST API's voor open diensten van een overheidspartij.
- REST API's voor gesloten diensten van een overheidspartij (direct) aan burgers of bedrijven.

Het Digikoppeling REST API profiel is wat betreft functionele toepassing vergelijkbaar met het Digikoppeling WUS profiel. De client van de dienstafnemer die gebruik maakt van het Digikoppeling REST API profiel is in deze context een systeem (applicatie) en geen internetbrowser.

| Invulling Digikoppeling | 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 |

In versie 1.0 van het Digikoppeling REST API profiel wordt signing en encryptie niet ondersteund. In toekomstige versies van het profiel zal hier wel invulling aan worden gegeven. (Zie ook [Bijlage HTTP Signing & Encryptie](#))

4. Digikoppeling Restful API profiel

HTML versie [Digikoppeling Restful API Profiel](#)

4.1 Inleiding

4.1.1 Historie

Vanuit het TO Digikoppeling zijn al langere tijd de ontwikkelingen rond Restful API's gevolgd. Binnen het Kennisplatform API zijn de REST-API Design Rules (REST ADR) ontwikkeld en de REST ADR standaard is ook opgenomen op de Pas-toe-of-leg-uit lijst van het Forum Standaardisatie. De REST ADR standaard is dan ook als basis genomen voor dit Digikoppeling REST API Profiel dat zich specifiek richt op G2G (Government-to-Government) interactie en M2M (Machine-to-Machine verkeer).

4.1.2 Toepassingsgebied

Het toepassingsgebied is voor Digikoppeling:

Digikoppeling moet worden toegepast op alle digitale gegevensuitwisseling met behulp van gestructureerde berichten die plaatsvindt met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, of die sector-overstijgend is.

Dit profiel is toe te passen bij het aanbieden van REST API's ten behoeve van het ontsluiten van overheidsinformatie en/of functionaliteit.

4.2 Digikoppeling REST-API profiel

4.2.1 Algemeen

Het Digikoppeling REST-API profiel is gebaseerd op de REST-API Design Rules standaard zoals ontwikkeld door het Kennisplatform API's en in beheer gebracht bij Logius Stelsels & Standaarden: [\[API Design Rules\]](#)

Het Digikoppeling REST-API profiel conformeert zich volledig aan het normatieve deel van de REST-API Design Rules.

4.2.2 Koppelvlak Generiek

4.2.2.1 Vertrouwelijkheid

De Digikoppeling Beveiligingsstandaarden en voorschriften gaan specifiek in op het verplichte gebruik van PKIO certificaten [\[PKI Policy\]](#) en 2-zijdig TLS.

- Zie [\[Digikoppeling Beveiligingsdocument\]](#)

4.2.2.2 Identificatie & Authenticatie

Digikoppeling maakt gebruik van het OIN (Organisatie Identificatie Nummer) voor de identificatie van organisaties. Binnen dit DK REST-API profielprofiel zijn er alleen voorschriften m.b.t. het verplicht gebruik van het OIN binnen PKIO certificaten. Voor OIN gebruik binnen payloads (bv JSON) of resource-pad gelden geen specifieke voorschriften.

- Zie [\[Digikoppeling Identificatie-Authenticatie\]](#)

4.2.3 API Design Rules

4.2.3.1 Toelichting aanduidingen

Voorschriften zijn aangeduid met 'Verplicht', 'Aanbevolen' en 'Niet van Toepassing' waarvoor de volgende definities gelden:

| Categorie | Codering RFC2119 | Voorschrift | Toelichting |
|---------------------|------------------|---|-------------|
| Verplicht | MUST | De eisen moeten gevolgd worden. Hier kan niet van afgeweken worden. | |
| Aanbevolen | SHOULD | Aanbevolen is om de eisen conform conform voorschrift te implementeren. Wanneer hier van afgeweken wordt dient een zorgvuldige afweging plaats te vinden | |
| Niet van Toepassing | - | De eisen zijn niet van toepassing | |

(Indeling gebaseerd op [rfc2119](#))

4.2.3.2 Regels

Het Digikoppeling REST-API profiel conformeert zich volledig aan het normatieve deel van de [API Design Rules](#).

| Categorie | Principe | Toelichting | Link |
|-----------|-----------------------|--|--------------------------------------|
| Verplicht | REST-API Design Rules | Het is verplicht te voldoen aan alle (normatieve) eisen van de REST-API Design Rules | [API Design Rules] . |

In onderstaande tabel worden de normatieve eisen van de [API Design Rules](#) weergegeven:

► Normatieve eisen van de REST API Design Rules

4.3 Afspraken API Design Rules extensies

De ADR extensie onderderdelen van dit profiel zijn gebaseerd op: [API Design Rules-Extensions](#).

Hieronder wordt aangegeven welke regels uit de API Design Rules extensies in dit profiel verplicht zijn of worden aanbevolen.

| Categorie | Principe | Extensie | Toelichting | Link |
|---------------------|--|------------------------|--|--|
| Niet van toepassing | 17.1 API-11: Encrypt connections using at least TLS v1.3 | Security | Vervangen door Digikoppeling beveiligingsvoorschriften (*) | [Digikoppeling Beveiligingsdocument] |
| Verplicht | 17.3 API-13: Accept tokens as HTTP headers only | Security Authorisation | | 17.3 API-13: Accept tokens as HTTP headers only |
| Verplicht | 17.5 API-15: Use PKI-overheid certificates for access-restricted or purpose-limited API authentication | Security Authorisation | | 17.5 API-15: Use PKI-overheid certificates for access-restricted or purpose-limited API authentication |
| Aanbevolen | 17.31 API-46: Use default error handling | Error handling | | 17.31 API-46: Use default error handling |
| Aanbevolen | 17.32 API-47: Use the required HTTP status codes | Error handling | | 17.32 API-47: Use the required HTTP status codes |

(*) Wat betreft TLS zijn de Digikoppeling beveiligingsvoorschriften leidend, Zie [Digikoppeling Beveiligingsdocument](#)

5. BIJLAGE Gebruik van Signing & Encryptie in de context van HTTP / Rest API

NOOT

Deze bijlage is informatief en geen normatief onderdeel van het profiel

5.1 Signing in de context van HTTP Rest

Signing van HTTP body en/of header kan gebruikt worden voor *authenticatie*, om de *integriteit* van de request/response berichten te controleren en signing realiseert ook *onweerlegbaarheid*. (Onweerlegbaarheid in de zin van: de verzender van de request/response kan niet ontkennen het bericht verzonden te hebben wanneer deze voorzien is van de digitale handtekening van de afzender).

De berichten kunnen ook samen met de digitale handtekeningen worden bewaard zodat deze bij audits of juridische bewijsvoering gebruikt kunnen worden.

Een HTTP requestbericht is opgebouwd uit de volgende onderdelen:

- Header
 - HTTP operatie (GET, POST etc)
 - Pad / URL resource
 - Protocol
 - Header velden
- Body
 - *data*

Door naast de body data ook onderdelen uit de header digitaal te ondertekenen kan worden gecontroleerd dat bv ook de HTTP operatie en resource specificatie in de request echt van de afzender afkomstig zijn en niet onderweg gemanipuleerd.

Enkele voorbeelden van signing standaarden die in ontwikkeling zijn:

- <https://tools.ietf.org/html/draft-ietf-httpbis-message-signatures>
- <https://www.openbankingeuropa.eu/media/2095/obe-json-web-signature-profile-for-open-banking.pdf>

5.2 Encryptie in de context van HTTP Rest

Voor encryptie is de standaard JSON Web Encryption (JWE) [\[fc7516\]](#) beschikbaar

Zie ook de ADR extensie signing en encryptie:

- <https://docs.geostandaarden.nl/api/API-Strategie-ext/#signing-and-encryption>

A. Referenties

A.1 Normatieve referenties

[API Design Rules]

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

[API Design Rules-Extensions]

[API Designrules Extensions \(Nederlandse API Strategie IIb\)](#). Jasper Roes; Linda van den Brink. Geonovum/Kennisplatform API's. Januari 2020. URL: <https://docs.geostandaarden.nl/api/API-Strategie-ext>

[Digikoppeling Beveiligingsdocument]

[Digikoppeling Beveiligingsstandaarden en voorschriften](#). Logius. 2020. URL: https://www.logius.nl/sites/default/files/bestanden/website/Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v1.3.pdf

[Digikoppeling Identificatie-Authenticatie]

[Digikoppeling Identificatie en Authenticatie](#). Logius. URL: <http://www.logius.nl/digikoppeling>

[PKI Policy]

[Programma van Eisen \(PKIoverheid\)](#). Logius. URL: <https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen>

[rfc7516]

[JSON Web Encryption \(JWE\)](#). M. Jones; J. Hildebrand. IETF. May 2015. Proposed Standard. URL: <https://www.rfc-editor.org/rfc/rfc7516>

A.2 Informatieve referenties

[rfc2119]

[Key words for use in RFCs to Indicate Requirement Levels](#). S. Bradner. IETF. March 1997. Best Current Practice. URL: <https://www.rfc-editor.org/rfc/rfc2119>