Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Technisch Overleg Digikoppeling

Logius

Bezoekadres:
Wilhelmina v Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.logius.nl
servicecentrum@logius.nl

Inlichtingen bij

Pieter Hering

digikoppeling@logius.nl

Datum
25-2-2021

memo

Digikoppeling Rest API Profiel

Inleiding

In de afgelopen periode heeft Logius gewerkt aan een Digikoppeling Rest API Profiel.

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

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.

Het document is publiek geconsulteerd en de resultaten van de consultatie zijn verwerkt:

- *Afkortingen zijn uitgeschreven t.b.v. leesbaarheid*
- *Gebruik van alleen categorie 'Verplicht 'en 'Aanbevolen' en 'Niet van Toepassing'*
- *API Designrules zijn opgenomen in uitklapbare tabel*
- *TLS versies 1.2/1.3: REST API profiel is gebaseerd op de Digikoppeling Beveiligingsstandaarden en voorschriften (zie link : bijlage)*

Digikoppeling Rest API Profiel 1.0:

Integraal:
https://centrumvoorstandaarden.github.io/DigikoppelingRestfulApiProfiel/

Bronbestanden:
https://github.com/centrumvoorstandaarden/DigikoppelingRestfulApiProfiel

Datum
25-2-2021

Vraag aan het TO Digikoppeling

Verleent het TO Digikoppeling goedkeuring aan deze versie van het Digikoppeling Rest API Profiel.

Bijlage TLS 1.3 in Digikoppeling / DK REST API

DK API REST profiel

Bij het DK API REST profiel is een vraag ingebracht mbt TLS:

In Digikoppeling beveiligingsstandaarden en voorschriften hoofdstuk 4.2 nummer TLS004 is het voorschrift als volgt.
Een Serviceaanbieder is verplicht TLS versie 1.2 te ondersteunen, daarnaast is het aanbevolen voor een Serviceaanbieder om TLS versie 1.3 te ondersteunen.
(...)

NCSC geeft aan dat de beste bescherming wordt geboden door TLS 1.3, dit onderschrijven wij ook. Daarnaast heeft deze versie inmiddels het veiligheidsniveau "Voldoende" in plaats van "Goed".

Is het (zeker voor de toekomstbestendigheid) niet beter om hier expliciet voor TLS 1.3 te kiezen?

https://github.com/centrumvoorstandaarden/DigikoppelingRestfulApiProfiel/issues/6

NSCS Beveiligingsrichtlijnen voor TLS v2.1

Daarnaast benadrukt NCSC in de nieuwe versie van de TLS richtlijnen v2.1 specifiek dat TLS 1.3 een toekomstvaste configuratie is:

De vernieuwde richtlijnen helpen toekomstvaste TLS-configuraties te maken op basis van TLS 1.3
Het NCSC heeft besloten TLS 1.2 in veiligheidsniveau af te schalen van *Goed* naar *Voldoende*. TLS 1.3, een grondige herziening van TLS op basis van moderne inzichten, blijft *Goed*. Het NCSC beschouwt TLS 1.2 daarmee nog steeds als veilig, maar minder toekomstvaste optie dan TLS 1.3. Configuraties die voldeden aan de richtlijnen uit 2019 (v2.0) voldoen nog steeds in deze update (v2.1).

Vraag uw leverancier om TLS 1.3 te ondersteunen als onderdeel van een toekomstvaste TLS-configuratie
TLS 1.3 is inmiddels goed beschikbaar in recente versies van softwarebibliotheken. De update van de richtlijnen is een goed moment om uw leverancier te vragen om TLS 1.3 te gaan ondersteunen. Door nu na te denken over een toekomstvaste configuratie, kunnen organisaties zich richten op dreigingen die dagelijkse aandacht verdienen.

TLS 1.3 in Digikoppeling / DK REST API

Het nieuwe API koppelvlak is gebaseerd op de generieke Digikoppeling TLS beveiligingsrichtlijnen, waarbij NCSC gevolgd wordt (en met voor DK voor service aanbieders een verplichte ondersteuning van TLS 1.2 ivm interoperabiliteit).

In lijn met de eerdere besluiten over TLS 1.2 / TLS 1.3 van het TO Digikoppeling is het voorstel op dit punt geen aanpassing te doen voor de 1e release van het Digikoppeling REST API profiel.

Concrete vraag aan het TO m.b.t dit punt:

Is het TO akkoord met dit voorstel of is een aanscherping/aanpassing van de Digikoppeling voorschriften m.b.t TLS versies wenselijk?