

Memo: Advies vaststellen Edukoppeling 1.3

Van: Brian Dommisse (voorzitter werkgroep Edukoppeling)
Datum: 11 januari 2018
Betreft: Advies vaststellen van medior versie Edukoppeling 1.3

Gevraagd besluit

Positief advies van de Architectuurraad ten aanzien het laten vaststellen door de Standaardisatieraad van versie 1.3 van de Edukoppeling afspraak.

Opnemen van afgeleide principes en ontwerpkaders in de ROSA om gegevensuitwisseling te beveiligen los van een specifiek transactieprotocol.

Toelichting

Versie 1.3 is een zogeheten medior versie. Strikt genomen is die niet compatibel met versie 1.2, echter deze versie 1.3 bevat wijzigingen die in de afgelopen periode in de praktijk al zijn geïmplementeerd in het kader van de uitwisselingen tussen het nieuwe BRON (en Verzuim) en diverse LAS-leveranciers in het vo. Die implementatiekeuzes zijn gemaakt omdat de standaard daar geen invulling nog aan had gegeven of omdat alle betrokken partijen het erover eens waren om af te wijken van de standaard. Om die reden zal de impact voor de overstap van 1.2 naar 1.3 voor veel partijen toch gering zijn (men heeft er namelijk al een voorschot op genomen).

Bij nieuwe implementaties zal deze versie 1.3 als uitgangspunt moeten gaan dienen waaronder de transacties tussen het nieuwe BRON en verzuim en de LAS-leveranciers in het po. De bij deze implementatie betrokken partijen hebben behoefte aan het definitief maken van deze versie.

De nieuwe afspraak bestaat uit de volgende specificatiedocumenten:

[2018-12-12 Edukoppeling Architectuur 1.2.2 \(concept\)](#)

[2018-12-12 Edukoppeling Transactiestandaard 1.3 \(concept\)](#)

[2018-09-17 Edukoppeling Identificatie en authenticatie 1.0 \(concept\)](#)

[2017-07-05 Edukoppeling – Begrippen versie 1.0](#)

[2018-12-12 Edukoppeling versie 1.3 – Release Notes](#)

De wijzigingen ten opzichte van 1.2.1 zijn beschreven in de release notes. Binnen het releasebeleid is afgesproken dat de hele set een versienummer krijgt (1.3 in dit geval) maar dat de onderliggende documenten een eigen versienummering hanteren.

Gevolgd proces

De werkgroep Edukoppeling heeft voor de zomer op basis van ervaringen met lopende implementaties en ontwikkelingen rondom de overheidsstandaard Digikoppeling een set van wijzigingen opgesteld. De eerste concepten zijn bij de achterban van de werkgroepleden in eerste instantie gereviewd (VDOD, DUO, Kennisnet (voor uitwisselingen in diverse ketenprocessen)). Eind september heeft dit geleid tot een conceptversie die is gepubliceerd voor openbare consultatie.

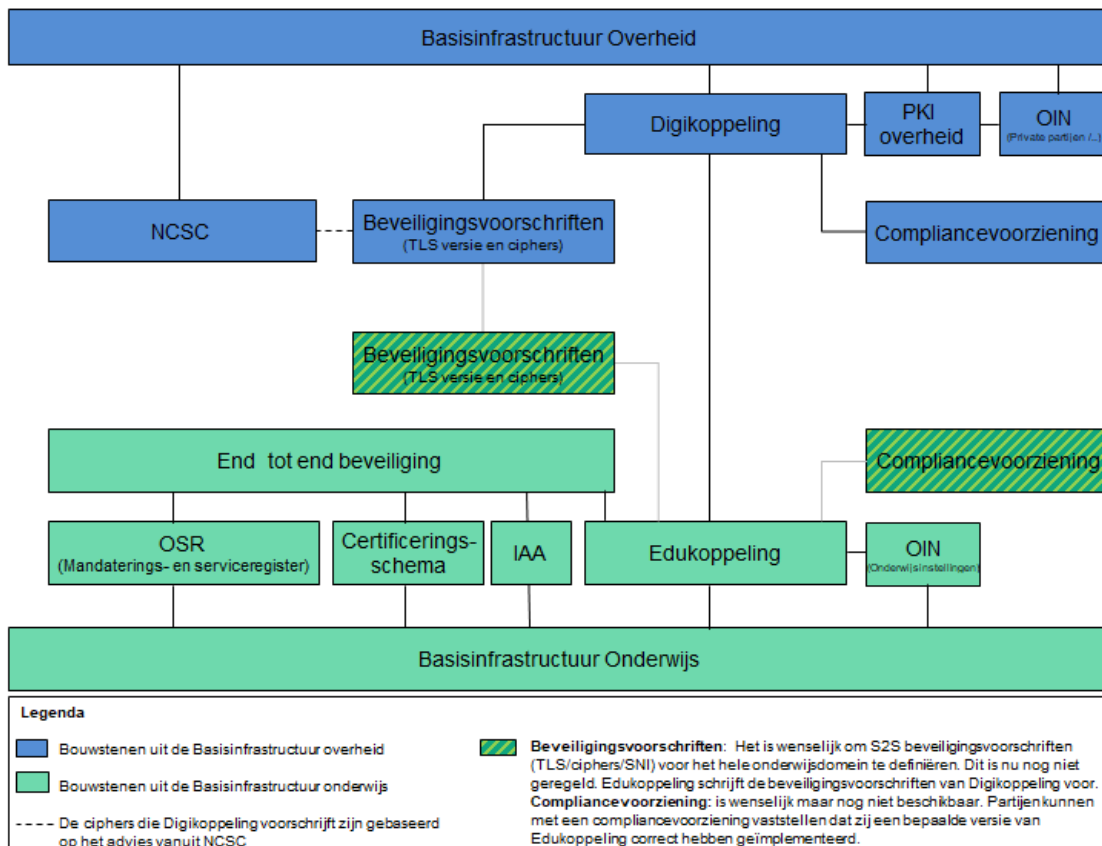
Daarop zijn met name vanuit het programma Doorontwikkelen BRON een aantal aanbevelingen gedaan voor aanpassingen. Ook de laatste ontwikkelingen bij Digikoppeling hebben geleid tot noodzaak tot een kleine bijstelling. De aanbevelingen en bijstelling zijn verwerkt in het nu voorliggende concept.

De werkgroep is van mening dat het vaststellen en hanteren van deze nieuwe versie een goede zaak is. Behalve de verduidelijkingen en aanscherpingen zijn er aspecten die nu in de standaard expliciet zijn geregeld die eerder anders of niet waren verwoord en/of ruimte gaven voor meerdere interpretaties:

- Voor de beveiliging van de uitwisseling en de authenticatie van de uitwisselende partijen is het gebruik van ODOC-certificaten uitgesloten. Alleen PKI-overheid certificaten zijn nog toegestaan.
- De adressering via het OIN (OverheidsidentificatieNummer) van onderwijsinstellingen wordt gebaseerd op de instellingserkenning (BRIN4).
- Verplichting om poort 443 te gebruiken is vervallen.

Architecturaspecten

Edukoppeling is opgebouwd uit een aantal landelijke bouwstenen waarbij de kern wordt gevormd door Digikoppeling. Om binnen het onderwijs bij gegevensuitwisseling end-to-end beveiliging te realiseren wordt gebruik gemaakt van bouwstenen uit de Basisinfrastructuur Overheid en Onderwijs. (zie figuur).



De bouwstenen voor de Edukoppeling Architectuur worden gevormd door zaken die essentieel zijn om beveiligde en betrouwbare gegevensuitwisseling mogelijk te maken. Het gaat hierbij om voorschriften over

- Gebruik van TLS en versies hiervan
- Selectie van gebruikte cyphersuites voor TLS verbindingen
- Gebruik van PKI certificaten

De redenen om deze voorschriften los te willen koppelen van Edukoppeling zelf zijn:

- Het zijn voorschriften zijn op niveau van Transport en niet op het niveau van de Logistiek (zie onderstaande figuur). Dergelijke voorschriften zijn hiermee, afhankelijk van de BIV classificatie van de gegevensuitwisseling, altijd geldig ook als Edukoppeling zelf niet van toepassing is.
- Het beheer van deze standaarden en ligt niet bij Edukoppeling (en ook Edustandaard).

Deze twee constatering hebben in de werkgroep geleid tot de vraag of we ontwerpkeaders voor gegevensbeveiligingen op het niveau van Transport niet expliciet zouden moeten gaan beheren binnen Edustandaard en opnemen in ROSA. Hiermee kunnen we ook voorsorteren op de verwachte uitbreiding van voorschriften op het gebied van beveiliging voor REST uitwisselingen.

