edustandaard

Edukoppeling

M2M gegevensuitwisseling binnen het onderwijs

Werkdocument Architectuur

Met opmerkingen [ER1]: Dit is de eerste versie en we bespreken deze 20 mei. Bevat het de juiste onderdelen, wat ontbreekt, wat is onvolledig, wat moet weg,...?

Met opmerkingen [PL2R1]: Zou zeker nog een haakje verwachten om het concept 'dataspaces' te kunnen ontrafelen. Een deel zit er nu indirect in, maar mag explicieter.

Edustandaard
Datum: 20 mei 2026
Versie: 3.0
Status: concept

edustandaard

Inhoudsopgave

1. Status van dit document

Dit document is een conceptversie van de Edukoppeling Architectuur versie 3.0. Deze nieuwe RESTful-API architectuur wijkt sterk af van de vorige versie[1]. In die versie onderkende we al RESTful API's, maar was nog sterk gericht op webservices en een Digikoppeling-indeling. Verder onderkenden we al patronen die synchrone RESTful API's gebruikte om asynchrone communicatie te implementeren, maar werd niet beschreven hoe deze uitwisseling gestandaardiseerd en zoveel mogelijk ontkoppeld kon plaatsvinden.

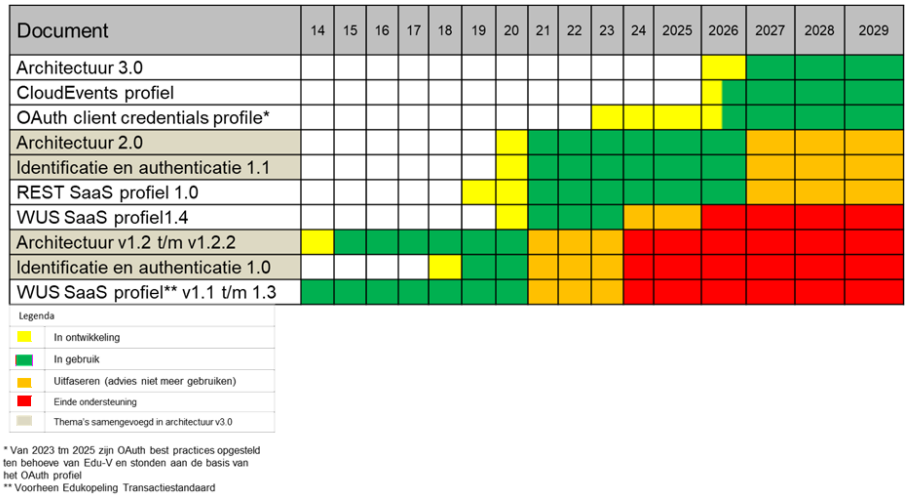
Deze nieuwe architectuur geeft context aan het Edukoppeling OAuth-profiel dat voorschriften de rond beveiliging van API's bevat. We ondersteunen hiermee token-based access. Verder sluit deze architectuur meer aan op ontkoppelde architecturen zoals een Event-driven architectuur (EDA). Hiervoor is een Edukoppeling CloudEvents-profiel opgesteld dat voorschriften bevat voor Asynchrone communicatie via RESTful API's.

1.1. Documenthistorie

Versie	Status	Auteur	Datum	Opmerking
1.2.01	Vervallen	WG Edukoppeling	Maart 2015	Zie document release notes
1.2.93	Vervallen	WG Edukoppeling	Juni 2015	Zie document release notes
1.2.94	Vervallen	WG Edukoppeling	Juni 2015	Zie document release notes
1.2.1	Vervallen	WG Edukoppeling	Juli 2017	Zie document release notes
1.2.2	Vervallen	WG Edukoppeling	December 2018	Zie document release notes
2.0	Vastgesteld	WG Edukoppeling	Februari 2021	Zie document release notes
3.0	Eerste (nog onvolledig) concept	WG Edukoppeling	Mei 2026	• Gehele herziening inhoud en structuur • Toegespitst op token based access (OAuth 2.0) en RESTful API's • Synchrone en asynchrone interacties

[1] https://www.edustandaard.nl/app/uploads/2021/10/2021-02-10-Edukoppeling-Architectuur-2.0-definitief.pdf

1.2. Overzicht actuele documentatie en compliance



Figuur 1 - Overzicht Educkoppeling documenten en versies

2. Inleiding

2.1. Doel van Edukoppeling

Het doel van Edukoppeling is standaardisatie van de technische afspraken op het M2M-koppelvlak waardoor het ontwikkelen van ketensamenwerkingen[2] by design veilig en eenvoudiger wordt. De toepassing van Edukoppeling zorgt ervoor dat, op het niveau van de applicatielaag, gesloten data tijdens transport van de ene naar de andere organisatie niet ongeoorloofd kan worden ingezien of gemanipuleerd. De standaard gaat over de afhandeling van berichten (het transport) en niet over de inhoud van berichten.

De aanleiding voor de introductie van Edukoppeling in het onderwijsdomein is een steeds groter wordende stroom van geautomatiseerde machine-machine uitwisselingen in het onderwijs. Dit wordt veroorzaakt door vernieuwingen in het onderwijs zelf, in wetgeving en in de beschikbare techniek. In toenemende mate lopen de processen over organisaties heen, tussen onderwijsorganisaties (zowel op bestuursniveau als op het niveau van onderwijsaanbieders, de “scholen”) onderling, tussen onderwijsorganisaties en overheidsorganisaties en tussen onderwijsorganisaties en private onderwijsgerelateerde organisaties. En vaak, als er iets nieuws komt, wordt er dan pas nagedacht over de benodigde wijze van koppelen. Als men niet oppast worden er evenveel verschillende soorten van koppelingen bedacht als er geautomatiseerde processen zijn. Dat is nadelig, omdat hiervoor veel kennis nodig is, dit onnodig veel en kostbaar onderhoudt vergt, dit de interoperabiliteit en aanpasbaarheid hindert. Met Edukoppeling verandert dat. Edukoppeling zorgt voor technische interoperabiliteit[3] en is een meervoudig inzetbare wijze van koppelen. Het beheer is binnen Edustandaard publiek-privaat georganiseerd. Verder is Edukoppeling gebaseerd op internationale open standaarden en de onderwijsstandaarden van Edustandaard. Dit alles maakt dat partijen met een lage drempel kunnen deelnemen, wat gunstig is voor het onderwijs

Edukoppeling bestaat uit op zichzelf staande documenten en waar relevant wordt verwezen naar de (volwassen) internationale open industriestandaarden en onderwijsstandaarden (bijvoorbeeld Edustandaard UBV TLS[4]). Edukoppeling wordt onder Edustandaard beheer doorontwikkeld.

2.2. Doelgroep

Dit document is bedoeld voor ICT-specialisten die betrokken zijn bij het ontwerpen en ontwikkelen van systeem-naar-systeem (M2M) koppelingen voor RESTful API’s. Het gaat hier om werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij onderwijsgerelateerde organisaties, zowel in de publieke als private sector. De lezer van dit document willen wij vragen om zaken die ontbreken of onduidelijk zijn te melden bij de beheerorganisatie Edustandaard[5]. Edustandaard is een open platform waar partijen

[2] ROSA definieert een ketensamenwerking als een concrete invulling van een scenario, waarbij er sprake is van een vorm van gegevensuitwisseling (interactie) tussen twee of meer ketenpartners ter ondersteuning van het afhandelen een of meerdere ketenprocess(tapp)en.
3 Edukoppeling gaat over de envelop, niet de inhoud. Procesmatige en semantische interoperabiliteit zijn buiten scope.
[4] https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/
[5] https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/. Reageren kan via info@edustandaard.nl.

binnen het onderwijsveld bij elkaar komen om afspraken te maken. Hier vindt tevens de doorontwikkeling van de standaard plaats. Hiertoe is een werkgroep Edukoppeling[6] ingericht.

2.3. Organisatorisch werkingsgebied Edukoppeling

Edukoppeling schrijft voor hoe onderwijsorganisaties, publieke uitvoeringsorganisaties, dienstverleners[7] en andere ketenpartners gegevensuitwisselingen opzetten. Edukoppeling heeft als scope alle werkingsgebieden vallend onder alle onderwijssectoren. Zie de werkingsgebieden in ROSA[8]. Hieronder vallen dus alle door de overheid erkende onderwijsorganisaties binnen de sectoren po, vo, mbo/bve en ho. Daar waar behoefte is aan technische afspraken op het M2M-koppelvlak, volgens het functioneel toepassingsgebied van Edukoppeling, zijn ketensamenwerkingen binnen deze sectoren verantwoordelijk voor de toepassing ervan. De toepassing buiten het organisatorisch werkingsgebied is toegestaan.

2.4. Functioneel toepassingsgebied Edukoppeling

Het functioneel toepassingsgebied van Edukoppeling is de geautomatiseerde uitwisseling van gesloten data[9] tussen informatiesystemen van onderwijsorganisaties en dienstverleners (onderling, met bedrijven of met de overheid). Deze uitwisseling betreft M2M point-to-point verbinding voor uitwisseling tussen een confidential client en een gesloten API.

Edukoppeling gaat over de afhandeling van de gegevensuitwisseling (het transport) en niet over de inhoud van die uitwisseling (‘berichten’). Het is een functioneel technische standaard, maar zal ook aansluiting moeten vinden op kaders van andere architectuurlagen. Hoe Edukoppeling aansluit op bredere afspraken is aan ketensamenwerkingen[10] waarin de standaard als onderdeel van de afspraak of het afsprakenstelsel wordt gevat.

Edukoppeling regelt de volgende ketenfuncties: identificatie, authenticatie, autorisatie en routering, op de ‘uitwisselingslaag’. Dit om de zorgen dat vertrouwelijke gegevens tijdens transport van de ene naar de andere organisatie, niet ongeoorloofd worden ingezien of gemanipuleerd.

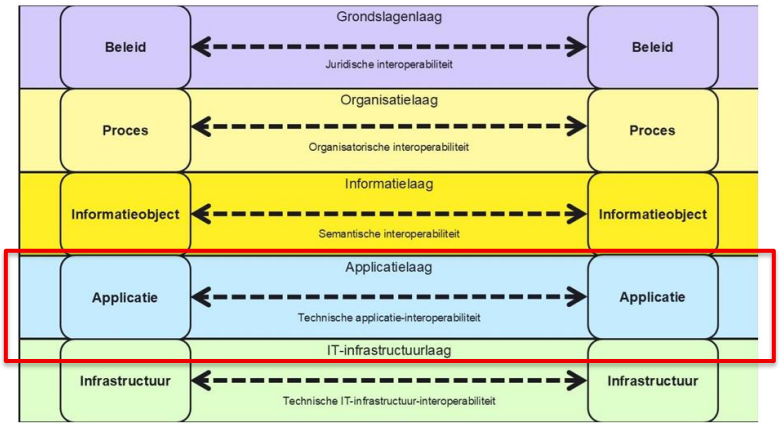
2.5. Positionering van Edukoppeling in het Edustandaard vijflagen model

Het Edustandaard 5-lagenmodel[11] onderkent de volgende lagen:

1. Grondslagenlaag: borgt de juridische basis en beleidskaders waarbinnen gegevensuitwisseling is toegestaan;

[6] Voor meer info over de Edukoppeling werkgroep, zie https://www.edustandaard.nl/standaard_werkgroepen/werkgroep-edukoppeling/
[7] Dienstverleners (ROSA: *Een organisatie die een dienst levert aan een organisatie of een natuurlijke persoon).*
[8] https://rosa.wikixl.nl/index.php/Werkingsgebieden
[9] Het gaat om gegevens waarvoor je geautoriseerd moet worden voor toegang. De gegevens zijn niet voor publiek hergebruik beschikbaar. Dit kan om verschillende redenen zijn, zie https://data.overheid.nl/gesloten-datasets
[10] Ketensamenwerkingen zijn bijvoorbeeld OKE, Edu-V, ROD ec. (zie ook: https://rosa-begrippenkader.wikixl.nl/index.php/Begrip:27a6accf-472d-4415-bc5b-1e9de17bf288#tab=Betekenis)
[11] AMIGO-methodiek-1.1.0-1.pdf en https://rosa.wikixl.nl/index.php/Interoperabiliteit_en_het_Edustandaard_lagenmodel#Opbouw_van_het_lagenmodel

2. Organisatorische laag: ketensamenwerking afspraken over wie welke rol heeft, welke gegevensdiensten, interfaces en interactiepatronen er zijn en welke gegevens onder welke condities uitgewisseld worden;
3. Informatielaag: semantiek, waaronder gegevensdefinities, informatiemodellen en de gebruikte identifiers voor rechtspersonen en natuurlijke personen;
4. Applicatielaag: API's en hun beveiligingsprofielen, berichtspecificaties, payload beveiliging, interactiepatronen en foutafhandeling;
5. IT-infrastructuurlaag: transportprotocollen en technische beveiligingsmechanismen zoals TLS.



Figuur 2 - Edustandaard 5-lagenmodel

Edukoppeling levert binnen het Edustandaard vijflagenmodel belangrijke ondersteuning aan de applicatielaag en heeft een relatie met de IT-infrastructuurlaag. De kaders van Edukoppeling worden opgenomen in het afsprakenstelsel van de betreffende ketensamenwerking[12], waarin ook de kaders van overige architectuurlagen[13] zijn gevat.

Met opmerkingen [PL3]: Is de Edukoppeling-architectuur nog een zuivere M2M-architectuur? Of moeten we toe naar een end-to-end architectuur. Ik snap die positionering vanuit het verleden, maar in de gesprekken en vraagstukken zie ik vraagstukken uit de proces en informatie-laag steeds weer terugkeren (API's, signing). Moeten we eigenlijk niet de end-to-end patronen gaan beschrijven, waarbij we beginnen met een 'user/using party' in de organisatorische laag, die informatieobjecten gebruikt die via de applicatie/technologielaag worden opgevraagd bij een systeem aan de andere kant, waarvoor een andere partij organisatorisch verantwoordelijk is? Met andere woorden: is de rode rechthoek in figuur 2 niet eigenlijk een U, die aan beide kanten de processen en informatieobjecten meepakt (maar niet de horizontale standaardisatie/interoperabiliteit daarvan)

Positionering van dit document

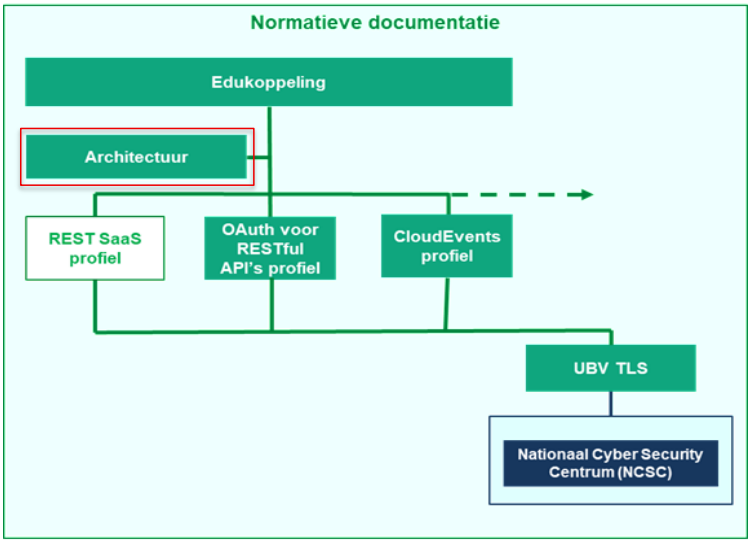
Edukoppeling bestaat uit verschillende documenten en is in beheer bij Edustandaard. Dit Architectuurdocument is één van de normatieve documenten binnen de Edukoppeling-afspraak. In Figuur 3 - Positionering van Architectuur binnen Edukoppeling is een schematische weergave opgenomen.

Dit architectuurdocument geeft context bij de toepassing van de nieuwe Edukoppeling profielen. Het biedt geen ondersteuning aan het oude WUS SaaS profiel[14]. Voor het REST SaaS-profiel[15] geldt dat deze onderdeel is van architectuur versie 2.0. Ook dit profiel wordt niet meegenomen in deze nieuwe architectuur. De toepassing van WUS-SaaS en REST-SaaS valt dus onder de architectuurversie 2.0. We verwachten dat de komende jaren versie

Met opmerkingen [PL4R3]: De profielen en transactiepatronen die je met Edukoppeling vastlegt kun je namelijk alleen begrijpen en kiezen als je begrip hebt van die proces- en informatielaag, en die dus conceptueel meeneemt in je architectuur. En het voorkomt dat we alleen technische endpoints beschrijven ('een IP-adres') ipv ook de organisatorische endpoints ('de verantwoordelijke/verwerker/bronhouder')

[12] Ketensamenwerkingen zijn bijvoorbeeld OKE, Edu-V, ROD ec. (zie ook: https://rosa-begrippenkader.wikixl.nl/index.php/Begrip:27a6accf-472d-4415-bc5b-1e9de17bf288#tab=Betekenis)
[13] Zie Positionering van Edukoppeling in het Edustandaard vijflagen model
[14] Dit profiel is niet meer in beheer (status 'Einde ondersteuning')
[15] Routerings- en mandaatgegevens worden hierbij meegegeven in een querystring

2.0 en bijbehorende profielen minder en minder toegepast zullen worden. Zie Overzicht actuele documentatie en compliance.



Figuur 3 - Positionering van Architectuur binnen Edukoppeling

2.6. Leeswijzer

Dit document is opgebouwd volgens de logische structuur van gegevensuitwisseling binnen een ketensamenwerking. Als eerste worden een aantal architectuurprincipes benoemd waarmee we aansluiten op ROSA en de architectuur kaderen (hoofdstuk 3). Het volgende hoofdstuk geeft de relevantie van een ketensamenwerking weer (hoofdstuk 4). Daarna worden de kernfuncties van de gegevensuitwisseling toegelicht bij interactiepatronen (hoofdstuk 5) en het (voorlopig) laatste hoofdstuk bevat afspraken rond het testen van API's.

Met opmerkingen [ER5]: Afhankelijk van opmerkingen vanuit werkgroep wordt de architectuur aangepast / aangevuld.

2.7. Relevante ontwikkelingen

Ontwikkelingen bij de overheid

Deze nieuwe versie van de architectuur beschrijft hoe binnen een ketensamenwerking op een gestandaardiseerde manier synchroon of asynchroon machine-to-machine gesloten data kan worden uitgewisseld via RESTful API's. Met de toepassing van de OAuth client credentials grant kunnen we toegang nu baseren op basis van tokens met grofmazige autorisaties op basis van scopes. Ook kan in deze flow metadata[16] meegestuurd worden waarmee extra controles kunnen worden uitgevoerd bij de Authorisation Server en/of Resource Server. Deze architectuur staat op zichzelf, maar is geïnspireerd door

[16] Vergelijkbaar met de ondersteuning van de edu-to en edu-from parameters bij het WUS-SaaS en REST-SaaS profiel van architectuurversie 2.0.

verschillende (lopende) initiatieven bij de overheid, zoals het Kennisplatform API's, Digikoppeling en verschillende internationale open standaarden. Deze worden hieronder nader toegelicht.

- **Kennisplatform API's**
  Geonovum[17] is samen met Bureau Forum Standaardisatie, Kamer van Koophandel, VNG Realisatie, Logius en het Kadaster in 2018 het Kennisplatform API's begonnen. Het Kennisplatform API's wil API's beter bij de vraag aan laten sluiten, kennis over het toepassen van API's uitwisselen en de aanpak bij verschillende organisaties op elkaar afstemmen en waar nodig standaardiseren. In werkgroepen die bestaan uit deelnemers uit de publieke en private sector zijn verschillende resultaten behaald. De API-strategie van het Kennisplatform omvat algemene onderdelen, zoals een beschrijving van architectuur en gebruikerswensen. Daarnaast is er een normatief deel[18] dat op de lijst met verplichte standaarden van de Nederlandse overheid staat (Forum Standaardisatie) met o.a. de volgende standaarden NL GOV Assurance profile for OAuth 2.0 (NL GOV OAuth profiel), Open API Specification (OAS) en API Design Rules (ADR).

  Voor Edukoppeling is met name het NL GOV OAuth profiel v1.1.0 relevant. De OAuth best practices[19] die zijn opgesteld ten behoeve van het Edu-V groeifondsprogramma is gebaseerd op deze versie van het NL GOV OAuth profiel. Dit NL GOV OAuth profiel is op zijn beurt weer gebaseerd op het OpenID iGOV OAuth profiel (Draft 03). Beide profielen hebben een brede scope en ondersteunen verschillende use cases[20] en toepassing van zowel confidential als public clients. Op dit moment ontwikkelt OpenID een nieuwe versie van het OpenID iGOV OAuth profiel (Draft 09). Deze gaat in de basis uit van enkel confidential clients. De nieuwe versie van het NL GOV OAuth profiel (Draft March 09, 2026[21]), die nog in ontwikkeling is, is vooralsnog gebaseerd op de vorige versie (Draft 03) van het iGOV OAuth profiel. Voor Edukoppeling is (nu) met name de toepassing van confidential clients en de client credentials grant relevant. Verder hebben we bij het opstellen van de Edukoppeling OAuth Best Practices gemerkt dat documentatie-technisch als beheermatig het lastig is om onze eigen keuzes te vatten in een document dat is afgeleid van het NL GOV OAuth profiel. We zien eerder nadelen dan voordelen. Wel hebben bij het opstellen van het Edukoppeling OAuth profiel onze eigen keuzes gemaakt, waarbij we in eerste plaatst wel naar het NL GOV OAuth profiel hebben gekeken. We blijven de ontwikkelingen van NL GOV OAuth volgen.

  In het Edukoppeling REST SaaS-profiel hebben we destijds het advies opgenomen om de API Design Rules[22] toe te passen. Later hebben we in de OAuth best practices de toepassing van de API Design Rules[23] verplicht gesteld. De werkgroep heeft voor dit document (Edukoppeling Architectuur versie 3.0) en de onderliggende profielen

[17] Kennisplatform API's | developer.overheid.nl
[18] Zie github voor een compleet overzicht van onderdelen van de API-strategie
[19] Zie de voorlopige uitwerking die in 2024 is gepubliceerd (Edukoppeling - Edukoppeling - juni 2024 - Edustandaard).
[20] Client credentials flow en Authorization code flow
[21] Zie editor's draft versie NL GOV Assurance profile for OAuth 2.0
[22] API Design Rules versie 17-01-2020
[23] NLGov REST API Design Rules 2.1.0

besloten om het ontwerp van API's buiten scope te plaatsen en hiermee ook de toepassing van de API Design Rules. We geven ketensamenwerkingen die de API's ontwikkelen wel het advies hun voordeel te doen met het bestaan van de API Design Rules.

- **Logius**
  De vorige versies van Edukoppeling waren gebaseerd op de overheidsstandaard Digikoppeling[24]. We hebben de afgelopen tijd een aantal keer ervaren dat de doorontwikkeling rond deze standaard achter liep op waar we binnen het onderwijs behoefte aan hebben. Dit was eigenlijk ook al de aanleiding in 2014 voor het creëren van de Edukoppeling-standaard. De behoefte voor een profiel voor RESTful API's heeft meer recent geleid tot aansluiting op het Kennisplatform API's[25]. De Edukoppeling OAuth Best Practices zijn zoals eerder aangegeven gebaseerd op het NL GOV OAuth 2.0 profiel[26] van het Kennisplatform API's. We merken dat als we voorlopen, Digikoppeling ons soms volgt, maar men maakt soms daar ook weer (andere) grote stappen waar we als onderwijs (nog) niet op willen of zelfs kunnen aansluiten. Dit is in de huidige situatie aan de orde doordat het Digikoppeling REST profiel[27] de toepassing van Federated Service Connectivity (FSC[28]) verplicht stelt. Dit past (nu) niet goed bij onze huidige afspraken. Hoog over wordt met FSC invulling gegeven aan wat we binnen Edukoppeling al sinds 2014 toepassen. Destijds ging Digikoppeling (WUS/REST) uit van een point-to-point verbinding uit voor de uitwisseling van vertrouwelijke gegevens tussen twee ketenpartijen. De eerste versies van Edukoppeling voegde daar, afhankelijk van het scenario, één of twee ketenpartijen aan toe in de rol van eindorganisatie. De eindorganisatie, over het algemeen de onderwijsorganisatie, geeft de ketenpartijen toestemming om via de point-to-point verbinding de vertrouwelijke gegevens uit te wisselen. Ook FSC ondersteunt verschillende scenario's en rollen[29] waarbij een bepaalde ketenpartij een andere toestemming geeft voor een bepaalde gegevensuitwisseling. Voordat ketenpartijen met elkaar kunnen communiceren, leggen ze afspraken vast in een digitaal contract. Hierin staat precies welke API's door een organisatie gebruikt mogen worden. Deze contracten worden cryptografisch ondertekend, zodat ze niet kunnen worden aangepast zonder toestemming. Juist het gebruik van contracten die met (PKIoverheid) certificaten ondertekend moeten worden levert voor Edukoppeling een probleem op. We zijn met Edukopeling juist afgestapt van het idee dat een onderwijsorganisatie certificaten[30] moet gebruiken. Momenteel is men een HLD Signing service aan het ontwikkelen die een ketenpartij in staat stelt om het contract te ondertekenen zonder dat men over een certificaat hoeft te beschikken. De verwachting is dat op termijn ook in de FSC (core) standaard de toepassing van een ondertekenservice ondersteund gaat worden. We blijven de ontwikkelingen rond het Digikoppeling REST profiel en FSC volgen.

[24] Digikoppeling Overzicht Actuele Documentatie en Compliance 1.12.2
[25] Kennisplatform API's | developer.overheid.nl
[26] NL GOV Assurance profile for OAuth 2.0 v1.1.0
[27] Digikoppeling Koppelvlakstandaard REST-API 3.0.1
[28] Introductie | standaard.nl
[29] De rol van Delegator die aan de Delegatee toestemming geeft, zie FSC - Core 1.1.2
[30] DUO ODOC certificaten

Het Digikoppeling REST profiel ondersteunt ondertekening en versleuteling van de payload[31]. Deze versie van de Edukoppeling architectuur gaat nog uit van scenario's waar er point-to-point verbindingen zijn tussen ketenpartijen. Wanneer er behoefte is aan het ondertekenen en/of versleutelen van de payload dan zullen we meer inhoudelijk naar de opties van het Digikoppeling REST profiel[32] gaan kijken.

Digikoppeling bestaat uit verschillende documenten. Zo is er ook het document Digikoppeling Beveiligingstandaarden en voorschriften 2.0.1. Hierin staan o.a. voorschriften rond identificatie (OIN[33]) en authenticatie (PKIoverheid certificaat), maar ook voorschriften rond (m)TLS. Al sinds 2020 hebben we binnen Edustandaard de voorschriften rond TLS opgenomen in een aparte standaard, UBV TLS[34]. We maken hier sinds 2021 ook binnen Edukopeling gebruik van. We zijn op dit punt dus al enige tijd ontkoppelt van Digikoppeling. Zowel Digikoppeling als de Edustandaard werkgroep IBP zien NSCS[35] als belangrijke bron voor de te maken keuzes rond TLS.

Logius heeft sinds 2022 een NL GOV profile for CloudEvents[36] (NL GOV CloudEvents profiel) in beheer. Deze versie is gebaseerd op de CloudEvents specificatie die is ontwikkeld door de Serverless Working Group van de Cloud Native Computing Foundation. In 2024 is er een publieke consultatie geweest waarna versie 1.0 van het NL GOV CloudEvents profiel is gepubliceerd. Op 17 maart 2026 is versie 1.1[37] vastgesteld. Deze is gebaseerd op *CloudEvents - Version 1.0.1*. Het NL GOV CloudEvents profiel is een set Nederlandse afspraken over het gebruik van de internationale standaard CloudEvents. Het beschrijft hoe een plaatsgevonden gebeurtenis gerapporteerd en uitgewisseld kan worden, zoals een verhuizing of overlijden. Het doel is om gestandaardiseerd en effectief informatie uit te wisselen op een manier waarbij informatie centraal (bij de bron) geregistreerd blijft. Binnen het Groeifondsprogramma Npuls werken Studielink, SURF en MBO Digitaal samen aan het onderbrengen van het huidige Studielink / Cambo in één nieuwe centrale voorziening voor het Aanmelden, Inschrijven en Intekenen (ook wel project AII[38]). Het project heeft behoefte aan asynchrone communicatie via RESTful API's om een zogenaamde Event Driven Architecture (EDA) te kunnen realiseren. De wens is om de NL GOV CloudEvents versie 1.1 als basis hiervoor te gebruiken. Het betreffende nieuwe Edukoppeling profiel wordt momenteel ontwikkeld en zal samen met dit Architectuurdocument worden gepubliceerd.

- **Federatief datastelsel (FDS)**[39]
  In de Meerjarenvisie Digitale Overheid 2025 – 2030[40] wordt aangegeven dat bestaande gegevensuitwisseling binnen de overheid nu vaak als niet transparant genoeg wordt ervaren. En er zijn voorbeelden van gebruik van foutieve gegevens in

[31] https://gitdocumentatie.logius.nl/publicatie/dk/restapi/3.0.1/#signing-encryptie-in-http-rest-context
[32] ADR Modules ADR-HTTP Message and payload signing with JAdES en ADR-HTTP Payload encryption
[33] Digikoppeling ligt de toepassing van OIN en PKIoverheid certificaten nader toe in een apart document Digikoppeling Identificatie en Authenticatie 1.5.0.
[34] https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/
[35] NCSC - Home
[36] Logius | NL GOV profile for CloudEvents
[37] NL GOV profile for CloudEvents 1.1
[38] Aanmelden, Inschrijven, Intekenen | Npuls
[39] Wat is het Federatief Datastelsel? · Federatief Datastelsel · Realisatie IBDS
[40] Meerjarenvisie Digitale Overheid 2025 – 2030 | Versie 2025

registraties, van onrechtmatig gegevensgebruik, of onveilige gegevensdeling. Er worden verschillende oorzaken genoemd en men ziet een organisatie-overstijgend gegevenslandschap als de oplossing. Deze lijn wordt ook in de Nederlandse Digitaliseringsstrategie neergezet. Een verbeterde inrichting van het data-ecosysteem van de Nederlandse overheid wordt gezien in het federatief datastelsel. De Interbestuurlijke Data Strategie (IBDS) is een programma van het ministerie van BZK waar het FDS voor datadeling en integratie wordt ontwikkeld. Het FDS bestaat enerzijds uit een afsprakenstelsel voor de uitwisseling van gegevens en anderzijds uit de standaarden[41] en tools waarmee de uitwisseling ingericht kan worden. Hier wordt in een organisatie-overstijgend gegevenslandschap voorzien dat overheidsorganisaties én private partijen moet ontzorgen rond datadeelvraagstukken. Wijzigingen in opgeslagen gegevens die voor andere overheidsorganisaties van belang zijn, worden via een abonnementsysteem aan de abonnees doorgegeven. Het lijkt er dus op dat FDS o.a. het Digikoppeling REST profiel (met de FSC standaard) en als onderdeel van de EDA architectuur het gebruik van de NL GOV CloudEvents standaard gaan voorschrijven. Voor de Edukoppeling standaard is het van belang om de ontwikkelingen rond FDS en GDI[42] te volgen. We willen niet alleen, waar wenselijk, met Edukoppeling aansluiten op (onderdelen van) overheidsstandaarden, maar willen ook oog hebben voor de grenzen van de werkingsgebieden van relevante overheidsstandaarden en Edukoppeling.

2.8. Uitgangspunten

1 Edukoppeling gaat over technische interoperabiliteit rond vertrouwelijke gegevensuitwisseling[43]
   a. Edukoppeling gaat over de beveiliging van gegevens in transport en de toegang tot API's
   b. Edukoppeling gaat niet over procesmatige of semantische interoperabiliteit en dus niet over de inhoud of het design van API's
2 Open standaarden zijn leidend: De architectuur baseert zich zoveel mogelijk op breed geaccepteerde open standaarden. Edukoppeling kiest daarom voor gangbare internet- en overheidsstandaarden voor API-beveiliging, berichtuitwisseling en interoperabiliteit. Afwijkingen of sectorspecifieke aanvullingen zijn alleen aan de orde wanneer de onderwijscontext daar expliciet om vraagt. Dit uitgangspunt voorkomt onnodig maatwerk en vergroot interoperabiliteit, hergebruik en internationale aansluiting.
3 De ketensamenwerking bepaalt de architectuurkeuze: De inrichting van een koppeling volgt uit de kenmerken van het ketenproces. Aard van de gegevens, mate van actualiteit, aantal betrokken partijen en gewenste ontkoppeling bepalen samen welke interactiepatronen, beveiligingsmaatregelen en vertrouwensmodellen passend zijn.
4 Identificatie: De architectuur onderscheidt minimaal drie identifiers: de identiteit van de organisatie (organisatie identificatienummer[44]), de identifier van de client of applicatie (type is vrije keuze), en indien relevant de identifier van de partij(en)

Met opmerkingen [PL6]: Dat klopt, maar we moeten wel begrijpen hoe die twee interoperabiliteitsaspecten interfereren met Edukoppeling, en ze dus ook in de architectuur meenemen.

Met opmerkingen [PL7]: Tegelijkertijd zijn er mogelijk specifieke sectoreigenschappen die tot structureel afwijken/andere keuzes leiden. Bijvoorbeeld omdat er 7000/700/100 autonome organisaties zijn die elk de architectuur moeten kunnen toepassen, allemaal bronhouder zijn en verwerkingsverantwoordelijk zijn. Of het feit dat dit weliswaar publieke organisaties zijn, maar niet allemaal overheidsorganisaties.

Met opmerkingen [PL8]: Daarin zijn dus wellicht een aantal grotere patronen te ontdekken. Denk aan 100 organisaties die in het Vervolgonderwijs intensief samen gaan werken, vs. 8000 organisaties die allemaal iets met DUO moeten.

Met opmerkingen [PL9]: Dit ondersteunt mijn eerdere punt dat je dus de proceslaag mee moet nemen in je architectuur. Twee van de identifiers bevinden zich namelijk daar (de organisatie en de 'mandaat'-partij. Alleen de client/applicatie-identifier bevindt zich strikt genomen in de applicatielaag.

[41] Standaarden voor het FDS · Federatief Datastelsel · Realisatie IBDS
[42] RE010 - Selectie FDS-standaarden – GDI-standaarden · Federatief Datastelsel · Realisatie IBDS
[43] https://rosa.wikixl.nl/index.php/Id-fd10bf7a-e960-4484-8e19-bd8b86e7d911
[44] OIN, zie Digikoppeling I&A https://gitdocumentatie.logius.nl/publicatie/dk/idauth/

namens wie persoonsgegevens worden uitgewisseld (mandaat/machtiging). Voor elke interactie moet helder zijn welk systeem handelt, onder verantwoordelijkheid van welke organisatie, en indien van toepassing (persoonsgegevens) namens welke organisatie toegang wordt gevraagd, voor welke organisatie de (persoons)gegevens bedoeld zijn.

5 Authenticatie: Er wordt voor authenticatie van een systeem (client) verschillende methodes ondersteund. De private_key_jwt heeft de voorkeur en moet worden toegepast bij een verhoogd risicoprofiel.

6 Autorisatie: Autorisatie is niet alleen gebaseerd op de identiteit van de client, maar ook op de context van het verzoek. Daarbij moet kunnen worden vastgesteld welke handeling wordt gevraagd, voor welke resource of API, namens welke partij wordt gehandeld en voor welke achterliggende partij of dataset de toegang bedoeld is. Autorisatie moet daarmee aansluiten op doelbinding, dataminimalisatie en de functionele afspraken in de keten.

7 Mandaat en delegatie: Wanneer een leverancier of systeem bijvoorbeeld handelt namens een bestuur, onderwijsaanbieder of instelling, moet dit mandaat expliciet zijn vastgelegd. De architectuur gaat ervan uit dat mandaat geen impliciete eigenschap van een client is, maar een gecontroleerde relatie tussen partijen. De identiteit die hierbij wordt gebruikt moet overeenkomen met het niveau waarop het mandaat is verleend. Deze relatie moet door het autorisatiemechanisme afdwingbaar zijn.

8 Vertrouwen: Vertrouwen in de keten is gebaseerd op expliciete afspraken over identificatie, authenticatie. Het vertrouwensmodel kan PKI-gebaseerd, federatief of registry-gebaseerd zijn, afhankelijk van de ketencontext. Edukoppeling ondersteund met PKI-overheidcertificaten een PKI-variant.

9 Transportbeveiliging is altijd verplicht: Alle gegevensuitwisseling vindt plaats over beveiligde transportkanalen. TLS is daarmee een minimale eis voor iedere koppeling. Transportbeveiliging beschermt de vertrouwelijkheid en integriteit van gegevens tijdens verzending.

Begrippen worden zoveel mogelijk overgenomen uit het ROSA begrippenkader[45].
Waar nodig zijn aanvullende begrippen opgenomen in dit document (zie

Met opmerkingen [PL10]: Dit lijkt een tamelijk specifieke keuze voor een architectuur op dit niveau.

Met opmerkingen [PL11]: Dat is dus niet in de applicatielaag.

Met opmerkingen [PL12]: 'handelen namens' is een juridisch begrip (Burgerlijk Wetboek). Technisch intermediair zijn is niet 'handelen'.

Met opmerkingen [PL13R12]: (doet overigens niet af aan het principe dat het expliciet moet zijn hoe de relatie ligt)

Met opmerkingen [PL14]: Het eerste stuk gaat over organisatorisch vertrouwen, en dat gaat over vertrouwen om met elkaar in zee te gaan ('het contract'). Je 'bewijst' dat vertrouwen met technische vertrouwensmiddelen, maar die zijn op zich geen vervanging van organisatorisch vertrouwen.

Met opmerkingen [PL15]: Maar: kunnen we ook een variant bedenken die NIET PKIo is gebaseerd, is daar plaats voor? Ik denk dat dat wel moet, en dat je moet voorsorteren op technisch vertrouwensstelsels waar PKIo NIET de norm is.

Met opmerkingen [PL16]: Mag dus een- en tweezijdig TLS zijn. Geldt ook voor open data, vanwege de integriteit en de zekerheid over de herkomst.

[45] Zie ROSA begrippenkader (https://rosa.wikixl.nl/index.php/Alfabetisch_overzicht_ROSA_Begrippenkader)
https://rosa.wikixl.nl/index.php/Alfabetisch_overzicht_ROSA_Begrippenkader

10 Bijlage A: Begrippen).

3. Architectuurkaders

3.1. Inleiding

De inrichting van deze architectuur wordt bepaald door een aantal belangrijke kaders en randvoorwaarden. Deze kaders komen voort uit wet- en regelgeving, maar ook uit architectuurprincipes en best practices.

- Een belangrijk kader is de privacywetgeving, met name de AVG. Deze stelt eisen aan de verwerking van persoonsgegevens, waaronder rechtmatigheid, doelbinding en dataminimalisatie. Dit betekent dat uitwisseling van persoonsgegevens alleen mag plaatsvinden indien daarvoor een geldige grondslag bestaat en dat alleen de noodzakelijke gegevens mogen worden gedeeld.

- Daarnaast spelen informatiebeveiligingsprincipes een belangrijke rol. Gegevens moeten worden beschermd tegen ongeautoriseerde toegang en manipulatie. Dit vereist een robuust vertrouwensmodel waarin identificatie, authenticatie en autorisatie centraal staan.

- Architectuurprincipes zoals die uit ROSA benadrukken naast IBP het belang van interoperabiliteit, hergebruik en losse koppeling. Dit betekent dat systemen zoveel mogelijk onafhankelijk van elkaar moeten kunnen functioneren en dat gebruik moet worden gemaakt van open standaarden.

Met opmerkingen [PL17]: Dat klopt, en dat heeft gevolgen voor de inrichting van de applicatielaag, maar de rechtmatigheid van de verwerking wordt daar niet bepaald.

3.2. Relevante ROSA-kaders

ROSA IV domein Gegevensuitwisseling[46]
Deze Edukoppeling architectuur gaat (voor een groot deel[47]) uit van het ROSA procesmodel 'Inrichten gegevensinteractie'[48].

ROSA Architectuurprincipes

1. Voorkom onrechtmatige toegang of verspreiding[49]
2. Voorkom aantasting van gegevensintegriteit[50]
3. Doelbinding[51]
4. Dataminimalisatie[52]
5. Unieke en betrouwbare identificatie van entiteiten[53]

ROSA Ontwerpkaders

1. ROSA ontwerpgebied IBP[54]: Ontwerpprincipe: Risicogebaseerde BIV-classificatie en maatregelen[55]

[46] https://rosa.wikixl.nl/index.php/Id-11ba47607fcf4a7b8798280698537737
[47] Er zijn een aantal punten waarop we afwijken. We stellen ook dat we vanuit de Edukoppeling werkgroep de ruimte hebben om dit op punten aan te passen. Wij onderkennen (nu) ook de rol van bronhouder. Deze wordt niet onderkend binnen het ROSA procesmodel 'Inrichten gegevensinteractie'.
[48] https://rosa.wikixl.nl/index.php/Id-7e1e5f972aa04ccd8f92d4ae6da77df7
[49] https://rosa.wikixl.nl/index.php/Id-8771af5f7b7d4cffa7c9f764854243bf`
[50] https://rosa.wikixl.nl/index.php/Id-1019fb234df1431790c567f0acf6e223
[51] https://rosa.wikixl.nl/index.php/Id-87a1dd0192bd49fe9db108ecc27947b8
[52] https://rosa.wikixl.nl/index.php/Id-9eadd4f8f80a4ee9ae92be9b0c8dd741
[53] https://rosa.wikixl.nl/index.php/Id-d0d50170e49d45529c4a0c37d9dab4cc
[54] https://rosa.wikixl.nl/index.php/Ontwerpgebied_IBP
[55] https://rosa.wikixl.nl/index.php/Id-5d847b11cd16491a8b0be3efa92c29d8

   a. Ontwerpkader: Handelingen zijn herleidbaar[56]
   b. Ontwerpkader: Voorkom ongewenste traceerbaarheid en vindbaarheid[57]
2. ROSA ontwerpgebied IBP: Ontwerpprincipe: Bevoegdheden als zeggenschappen en/of toegangsrechten[58]
   a. Ontwerpkader: Lifecyclemanagement van bevoegdheden namens een entiteit[59]
   b. Ontwerpkader: Lifecyclemanagement van bevoegdheden van een entiteit[60]
3. ROSA ontwerpgebied IBP: Ontwerpprincipe: Informatiebeveiliging door ketenpartijen[61]
4. ROSA ontwerpgebied Digitale Identiteiten[62]: Ontwerpprincipe: Unieke en betrouwbare identificatie van entiteiten[63]
5. ROSA ontwerpgebied Interoperabiliteit[64]: Ontwerpprincipe: Technische interoperabiliteit:
   a. Ontwerpkader: Standaarden voor gegevensuitwisseling[65].
   b. Ontwerpkader: Ontkoppeling[66]
   c. Ontwerpkader: Ketenpartijen bepalen zelf de identificerende kenmerken van logistieke punten[67]
   d. Ontwerpkader: Ketenpartijen bieden wederzijdse applicatieservices[68]
6. ROSA ontwerpgebied M2M interactie[69]: Ontwerpprincipe(nieuw): API First
   a. API-first past binnen de huidige beleidsdoelen en de omgeving van de publieke en onderwijssector (API-strategie [70]).
7. ROSA ontwerpgebied M2M interactie: Ontwerpprincipe(nieuw): Gesloten API's voor gesloten data
   a. Gesloten data betreft vertrouwelijke informatie. Dit kunnen persoonsgegeven en/of bedrijfskritische gegevens zijn. Onrechtmatige toegang moet worden voorkomen met toepassing van gesloten API's (zijn beveiligd met een Edukoppeling beveiligingsprofiel[71]).
8. ROSA ontwerpgebied M2M interactie: Ontwerpprincipe(nieuw): De uitwisseling van gesloten data is rechtmatig
   a. Een API-afnemer moet kunnen aantonen op basis van welke geldende regels en besluiten zij van API's gebruik maken.
   b. Een API-aanbieder moet kunnen aantonen op basis van welke regels en besluiten zij API's en data aan API-afnemer(s) beschikbaar stellen.

[56] https://rosa.wikixl.nl/index.php/Id-2fe9add7-dac0-47d8-a2e6-4ec55a62fb65
[57] https://rosa.wikixl.nl/index.php/Id-6905cf44-3de1-41b3-b56f-4b44db4fcb1f
[58] https://rosa.wikixl.nl/index.php/Id-66b82245754b4df1982e3aa9974785ec
[59] https://rosa.wikixl.nl/index.php/Id-5150b0e8bd0f4e2a91c69b442672d4e4
[60] https://rosa.wikixl.nl/index.php/Id-bc05efc2d30a46c0a5b9e480f228c90d
[61] https://rosa.wikixl.nl/index.php/Id-4389b8e6-3291-4819-bd59-41a62a8a056e
[62] https://rosa.wikixl.nl/index.php/Ontwerpgebied_Digitale_identiteiten
[63] https://rosa.wikixl.nl/index.php/Id-33bec441b4b540c9a3a008aa3ff0062c
[64] https://rosa.wikixl.nl/index.php/Id-93ac1579ed1a4ba0b15974da0ec30c5e
[65] https://rosa.wikixl.nl/index.php/Id-88693833712f406f9185c8a5883ba482
[66] https://rosa.wikixl.nl/index.php/Id-f9bcc25632b042b4a02c1c8f6acebd1d
[67] https://rosa.wikixl.nl/index.php/Id-ebaabb65-8416-4277-bd28-64c2dc12eb33
[68] https://rosa.wikixl.nl/index.php/Id-d6c7901d-c46f-4d7e-82a3-c39f7db2e661
[69] https://rosa.wikixl.nl/index.php/M2M-interactie
[70] API Strategie Algemeen (Inleiding)
[71] Deze versie ondersteund de beveiliging van API's met een OAuth client credentials profiel.

4. Ketensamenwerking

4.1. Inleiding

ROSA definieert een ketensamenwerking als een concrete invulling van een scenario, waarbij er sprake is van een vorm van gegevensuitwisseling (interactie) tussen twee of meer ketenpartners ter ondersteuning van het afhandelen een of meerdere ketenprocess(tapp)en. Het (onderwijs)landschap met deze ketensamenwerkingen wordt steeds complexer. Er zijn vele organisaties zoals onderwijsinstellingen, DUO, leveranciers die binnen verschillende ketens[72] gezamenlijk opereren. Er is geen centrale regie over al deze interacties. Deze architectuur is ontworpen in een context van complexe ketensamenwerkingen, waarin meerdere organisaties en systemen samenwerken en afhankelijk zijn van betrouwbare gegevensuitwisseling. De aard van de processen, de juridische kaders en de organisatorische kenmerken van deze ketens bepalen in belangrijke mate de keuzes die worden gemaakt. Edukoppeling biedt ketensamenwerkingen flexibiliteit, maar ook duidelijke kaders om met elkaar te communiceren via een (op logistiek niveau) gestandaardiseerde machine-to-machine (M2M) koppeling.

4.2. Rollen

In ketensamenwerkingen is sprake van een duidelijke scheiding tussen partijen die gegevens beheren en daar verantwoordelijk voor zijn en partijen die gegevens gebruiken. Deze scheiding brengt verantwoordelijkheden met zich mee, zowel op het gebied van gegevenskwaliteit als op het gebied van rechtmatigheid en beveiliging van gegevens in transport. We onderkennen hierin als eerste de rol van gegevensleverancier[73] die ervoor zorgt dat gegevens op een gestandaardiseerde manier beschikbaar worden gesteld via een herbruikbaar gegevensleverend systeem[74]. Anders dan het procesmodel ‘Inrichten gegevensinteractie’[75] onderkennen we binnen Edukoppeling ook de rol van bronhouder voor

Met opmerkingen [PL18]: Dat is dus niet zo op procesniveau. Als twee onderwijsorganisaties samenwerken zijn ze beiden zowel beheerder als gebruiker (en wil je dus symmetrie). Op interactieniveau zul je dan wel (beurtelings) de ene of andere rol hebben.

[72] Dat mogelijk onderdeel is van een groeifondsprogramma (Npuls) of afsprakenstelsel (Edu-V)
[73] Zie https://rosa.wikixl.nl/index.php/Id-3aa58b2e99274fd2b5ac275b01887b33, ook wel gegevensverstrekker https://rosa.wikixl.nl/index.php/Begrip:5b8c9356-5dc7-4655-a0b9-d152babb01b6. In de context van het OAuth-profiel is dit de API-aanbieder.
[74] Zie https://rosa.wikixl.nl/index.php/Id-36c02d762c0e42c999c75564d50e833e, ook wel Applicatieservice (https://rosa.wikixl.nl/index.php/Begrip:D93b7bdc-05c8-4429-90f6-84e0d1038396) of gegevensdienst. In de context van het OAuth-profiel is dit de API van een API-aanbieder.
[75] Zie Inleiding

De inrichting van deze architectuur wordt bepaald door een aantal belangrijke kaders en randvoorwaarden. Deze kaders komen voort uit wet- en regelgeving, maar ook uit architectuurprincipes en best practices.

Een belangrijk kader is de privacywetgeving, met name de AVG. Deze stelt eisen aan de verwerking van persoonsgegevens, waaronder rechtmatigheid, doelbinding en dataminimalisatie. Dit betekent dat uitwisseling van persoonsgegevens alleen mag plaatsvinden indien daarvoor een geldige grondslag bestaat en dat alleen de noodzakelijke gegevens mogen worden gedeeld.

Daarnaast spelen informatiebeveiligingsprincipes een belangrijke rol. Gegevens moeten worden beschermd tegen ongeautoriseerde toegang en manipulatie. Dit vereist een robuust vertrouwensmodel waarin identificatie, authenticatie en autorisatie centraal staan.

de ketenpartij die de gegevens beheerd. Bronhouders zijn verantwoordelijk voor de juistheid en volledigheid van de gegevens die zij beheren. Zij bepalen welke gegevens beschikbaar worden gesteld en onder welke voorwaarden. In een bepaalde context kan de bronhouder ook zelf de rol van gegevensleverancier vervullen. De derde rol is die van gegevensontvanger[76]. De gegevensontvanger verwerkt de gegevens in uiteenlopende processen en moet ervoor zorgen dat deze op een rechtmatige en veilige manier worden verwerkt. Binnen een ketensamenwerking maken bronhouders, gegevensleverancier en gegevensontvanger onderlinge afspraken om ervoor te zorgen dat gegevens optimaal kunnen worden uitgewisseld.

Met opmerkingen [PL19]: Er zijn heel veel bronhouders in het onderwijsstelsel. Elke partij kan in principe elke rol hebben. 'Partij' is een begrip in de organisatorische laag, gegevensleverancier, gegevensontvanger zitten in de applicatie(uitwisselingslaag). Bronhouder lijkt een rol in de proceslaag (je bent bronregistratie, of je hebt brongegevens), die consequenties heeft voor de invulling van de applicatielaag.

Met opmerkingen [PL20R19]: (het lijkt dat hier de herkomst Digikoppeling, met een duidelijke bias naar 'basisregistraties' teveel doorschemert. In het onderwijsstelsel hebben we 1 grote partij die voor iedereen bronhouder is van generieke gegevens (DUO), maar daarnaast 8000 scholen/instellingen die elk ook bronhouder zijn voor hun leerling- en onderwijsgegevens.

4.3. Uitwisseling van persoonsgegevens

Binnen het onderwijsdomein zijn er vele ketensamenwerkingen waarbij persoonsgegevens worden uitgewisseld. Dit betekent dat de architectuur en inrichting moet voldoen aan geldende privacywetgeving, in het bijzonder de Algemene Verordening Gegevensbescherming (AVG). Deze wetgeving stelt niet alleen eisen aan de manier waarop gegevens worden verwerkt, maar ook aan de wijze waarop verantwoordelijkheid en aansprakelijkheid zijn georganiseerd binnen de keten. De verwerkingsverantwoordelijke bepaalt het doel en de middelen van de verwerking, terwijl de verwerker gegevens verwerkt in opdracht van de verantwoordelijke. Gegevens mogen alleen worden uitgewisseld indien daarvoor een geldige grondslag bestaat. De grondslag kan variëren van een wettelijke verplichting tot een contractuele relatie of expliciete toestemming van de betrokkene. In alle gevallen moet het doel van de gegevensuitwisseling duidelijk zijn en moet worden voorkomen dat gegevens voor andere doeleinden worden gebruikt dan waarvoor zij zijn verzameld. Er moet dus bij iedere gegevensuitwisseling duidelijk zijn welke partij optreedt als verwerkingsverantwoordelijke en welke partij als verwerker. Hiermee wordt duidelijk wie verantwoordelijk is voor de rechtmatigheid van de gegevensverwerking. Verder kunnen binnen een ketensamenwerking kunnen meerdere verwerkingsverantwoordelijken en verwerkers betrokken zijn. Een partij kan in de ene relatie verwerkingsverantwoordelijke zijn en in een andere relatie verwerker. Dit maakt het noodzakelijk om binnen een ketensamenwerking deze rollen expliciet vast te stellen. Dit raakt meerdere lagen van het Edustandaard 5-lagenmodel. De Edukoppeling-architectuur ondersteunt de mogelijkheid om via de gegevensuitwisseling extra informatie rond een mandaat/machtiging[77] te delen die geverifieerd kan worden met gegevens uit de grondslagen en/of organisatie laag.

Met opmerkingen [PL21]: En de architectuur moet dus ook de samenhang tussen die lagen beschrijven.

4.4. Proceskarakteristieken

Deze architectuur houdt ook rekening met de karakteristieken van ketenprocessen. Ketenprocessen verschillen onderling sterk in aard en eisen. Een eerste belangrijk onderscheid is dat tussen processen die gericht zijn op het opvragen van gegevens en processen die gericht zijn op het aanleveren of delen van gegevens.

Architectuurprincipes zoals die uit ROSA benadrukken naast IBP het belang van interoperabiliteit, hergebruik en losse koppeling. Dit betekent dat systemen zoveel mogelijk onafhankelijk van elkaar moeten kunnen functioneren en dat gebruik moet worden gemaakt van open standaarden.
Relevante ROSA

[76] Zie https://rosa.wikixl.nl/index.php/Id-4c220210fa6742c3984df16e114bcbef, ook wel gegevensafnemer (https://rosa.wikixl.nl/index.php/Begrip:8817b7b1-80a0-4e7e-97c1-75cb2ec66b59). In de context van het OAuth-profiel is dit de API-afnemer.

[77] Zie **Fout! Verwijzingsbron niet gevonden.**

- Bij het opvragen van gegevens gaat het vaak om situaties waarin een systeem actuele informatie nodig heeft om een beslissing te nemen of een handeling uit te voeren. Deze processen zijn vaak tijdkritisch en vereisen een snelle en betrouwbare respons.
- Bij het aanleveren van gegevens gaat het vaker om het registreren of doorgeven van informatie, waarbij de verwerking niet altijd direct hoeft plaats te vinden.

Met opmerkingen [PL22]: Aanvullen met de gewenste businesstransactie-patronen. One stop shop vereist ander tijdgedrag dan 'long running transaction'. Transacties vereisen een keten van opvragen/aanleveren over meerdere stappen.

Daarnaast zijn er processen waarin veranderingen in gegevens centraal staan. In deze gevallen is het belangrijk dat systemen op de hoogte worden gebracht van wijzigingen, zodat zij hun eigen gegevens kunnen bijwerken of acties kunnen ondernemen.

Met opmerkingen [PL23]: Of dat het procesontwerp zodanig is dat alleen met actuele gegevens gewerkt wordt.

Een derde belangrijk aspect is de dynamiek van gegevens. Sommige gegevens veranderen weinig en kunnen relatief eenvoudig worden opgevraagd wanneer nodig. Andere gegevens zijn sterk dynamisch en vereisen een meer proactieve benadering, waarbij systemen automatisch worden geïnformeerd over wijzigingen. Dit heeft directe gevolgen voor de keuze van interactiepatronen en de inrichting van de architectuur.

De variatie in proceskarakteristieken leidt tot verschillende interactiebehoeften. De Edukoppeling-architectuur ondersteunt deze variatie door geen enkel interactiepatroon te verplichten, maar een kader te bieden waarin per use case een passend interactiepatroon[78] kan worden gekozen.

4.5. Vertrouwen

Gegevensuitwisseling vindt plaats over organisatiegrenzen heen en vaak in een context waarin ketenpartijen elkaar niet volledig kennen of kunnen controleren. Binnen een ketensamenwerking moet vertrouwen niet zijn gebaseerd op aannamen. Er is een vertrouwensmodel noodzakelijk. Edukoppeling gaat ervan uit dat een ketensamenwerking dit heeft ingericht. Het vertrouwensmodel bepaalt hoe partijen elkaar herkennen, accepteren en toegang verlenen. Er kunnen verschillende modellen worden toegepast met elk eigen kenmerken en toepassingsgebieden.

<u>Register</u>
Een vertrouwensmodel kan gebaseerd zijn op een vertrouwt register. Hierbij wordt vertrouwen georganiseerd via een registratievoorziening. In dit register worden clients, organisaties, sleutels en bevoegdheden vastgelegd. Het voordeel van dit model is flexibiliteit. Nieuwe partijen kunnen relatief eenvoudig worden toegevoegd en rechten kunnen fijnmazig worden beheerd.

<u>Federatief</u>
Er is ook een federatief vertrouwensmodel. Hierbij wordt vertrouwen gedistribueerd georganiseerd via een netwerk van partijen die elkaars metadata en beleidsregels vertrouwen. In plaats van één centrale registry delen partijen informatie over identiteit, sleutels en bevoegdheden via een federatie. Het voordeel van federatie is schaalbaarheid en flexibiliteit, vooral in open en internationale ecosystemen. Het nadeel is de complexiteit: governance, trust anchors en validatiemechanismen moeten goed zijn ingericht. Een nieuwe

[78] Zie Transactiepatronen

standaard in deze context is OpenID Federation[79]. Het introduceert een federatief vertrouwensmodel waarin vertrouwen dynamisch kan worden vastgesteld via vertrouwensankers en cryptografisch ondertekende metadata. Organisaties kunnen zogenaamde trust marks (op basis van een JWT) presenteren. Op termijn zou hiermee binnen Edukoppeling een organisatie een door een autoriteit uitgegeven accreditatie of certificering kunnen aantonen. Dit zou mogelijk ook toegepast kunnen worden om een machtiging/mandaat aan te tonen.

PKI
De Edukoppeling-architectuur ondersteunt een op PKI-gebaseerd vertrouwensmodel. Bij een PKI-vertrouwensmodel is vertrouwen gebaseerd op certificaten en een certificaathiërarchie. Organisaties beschikken over digitale certificaten die zijn uitgegeven door een vertrouwde Certificate Authority (CA), zoals PKIoverheid. Door middel van deze certificaten kunnen partijen elkaar cryptografisch identificeren en authenticeren. Het voordeel van dit model is de sterke zekerheid over identiteit en de duidelijke governance via certificaatuitgifte. Nadeel is dat het minder flexibel is: onboarding kan tijd kosten en internationale of kleinere partijen hebben niet altijd toegang tot dezelfde PKI-infrastructuur.

4.6. Beveiliging

Vooraf aan een gegevensuitwisseling moet een ketenpartij maatregelen treffen tijdens de interactie te kunnen vaststellen of rechtmatig toegang kan worden verleend. Hiervoor moeten ketenpartijen elkaar betrouwbaar kunnen identificeren, authentiseren en autoriseren. Deze versie van Edukoppeling leunt stevig op de internationale open standaard OAuth 2.0. Deze standaard ondersteunt meerdere flows, maar gezien Edukoppeling een machine-to-machine interactie betreft, is alleen de client credentials flow[80] van toepassing. Dit mechanisme maakt het mogelijk om systemen (clients) te identificeren en authenticeren en hen gecontroleerd toegang te geven tot RESTful API's. Het gebruik van tokens maakt het mogelijk om autorisatie los te koppelen van authenticatie. Een belangrijk kenmerk van moderne ketens is dat zij steeds vaker een open karakter krijgen. Dit betekent dat nieuwe partijen relatief eenvoudig moeten kunnen aansluiten en dat gegevensuitwisseling niet beperkt is tot een vaste groep deelnemers. Dit stelt hoge eisen aan standaardisatie en interoperabiliteit, maar ook aan het vertrouwensmodel. De toepassing van OAuth 2.0 zorgt voor flexibiliteit en een duidelijke scheiding in rollen zodat rechten flexibel kunnen worden toegekend en beheerd.

Verder onderkennen we dat niet elke ketensamenwerking hetzelfde beveiligingsniveau vereist. Daarom ondersteunt de architectuur meerdere beveiligingsniveaus[81]. Dit maakt het mogelijk om beveiliging proportioneel toe te passen, afhankelijk van de gevoeligheid van de gegevens en de risico's binnen de keten.

4.7. Architectuurstijlen

Een architectuurstijl beschrijft de structurele manier waarop systemen en componenten zijn georganiseerd en samenwerken. We onderkennen hierbij de volgende oriëntaties:

[79] OpenID Federation 1.0
[80] Zie het Edukoppeling OAuth client credentials profiel
[81] Zie Informatiebeveiliging

1. Service-oriëntatie: Bij service-oriëntatie staat de uitvoering van functionaliteit centraal. Systemen roepen services aan om een specifieke handeling uit te voeren. Dit leidt vaak tot synchrone interactiepatronen waarin een verzoek direct wordt verwerkt en beantwoord. Eerdere versies van Edukoppeling hadden een sterk Service Gerichte Architectuur (SGA) met een WUS-profiel waarmee SOAP webservices konden worden geïmplementeerd.
2. Resource-oriëntatie: Resource-oriëntatie richt zich op gegevens als resources die via gestandaardiseerde operaties (zoals CRUD) benaderd kunnen worden. Dit is kenmerkend voor RESTful API's. Gegevensuitwisseling gaat vaak via synchrone interactiepatronen en de focus: ligt niet op de actie, maar op de toegang tot gegevens.
3. Eventoriëntatie: Hier staat het publiceren van gebeurtenissen centraal. Systemen reageren op gebeurtenissen in plaats van deze actief op te vragen. Hierbij staan asynchrone, eventgedreven interactiepatronen centraal wat ontkoppeling en schaalbaarheid oplevert.
4. Berichtoriëntatie: Systemen wisselen vaak via een messaging-infrastructuur berichten uit. Hierbij is de communicatie doorgaans asynchroon ondersteunt een betrouwbare aflevering. We zien dit o.a. terug in het Digikoppeling ebMS profiel.

Event driven architectuur (EDA)

De proceskarakteristieken geven aan dat er behoefte is aan flexibele, schaalbare en robuuste gegevensuitwisseling die zowel synchrone als asynchrone interacties ondersteunt. De traditionele integraties waren vaak gebaseerd op bulk-transacties en synchrone request-response patronen. In toenemende mate zien we echter dat dit niet meer voldoet aan de eisen van moderne (onderwijs)processen. Processen waar gegevens vaak veranderen, meerdere partijen afhankelijk zijn van dezelfde informatie en processen niet strikt sequentieel verlopen, ontstaat behoefte aan een andere benadering van gegevensuitwisseling. Systemen van ketenpartijen reageren op allerlei gebeurtenissen vanuit verschillende bronnen in plaats van het gericht ophalen van gegevens.

Een EDA biedt een passend model. In plaats van systemen die actief gegevens opvragen, staat bij EDA het principe centraal dat systemen reageren op gebeurtenissen. Wanneer een relevante gebeurtenis plaatsvindt binnen een systeem, wordt deze gebeurtenis gepubliceerd als een event, waarna andere systemen hierop kunnen reageren. Dit maakt het mogelijk om systemen losser te koppelen en beter aan te sluiten op de dynamiek van ketenprocessen. Edukoppeling ondersteunt niet alleen passende interactiepatronen die passen binnen EDA, maar ook een CloudEvents profiel om interoperabiliteit te waarborgen over de manier waarop events worden beschreven en uitgewisseld.

EDA heeft in ketensamenwerkingen vaak de voorkeur omdat deze beter aansluit bij de dynamiek, schaal en ontkoppelingsbehoefte van moderne gegevensuitwisseling. EDA vraagt wel om expliciete afspraken over semantiek, governance en beveiliging, omdat context en autorisatie niet impliciet via een directe interactie worden afgedwongen. EDA biedt samen met het Edukoppeling CloudEvents-profiel een robuust en toekomstbestendig fundament voor gegevensuitwisseling.

5. Transactiepatronen

5.1. Inleiding

Binnen Edukoppeling wordt gegevensuitwisseling tussen ketenpartijen vormgegeven aan de hand van gestandaardiseerde transactiepatronen. Deze patronen beschrijven de functionele en technische eigenschappen van de interactie tussen systemen bij het uitwisselen van gegevens en vormen daarmee een essentieel onderdeel van de architectuur voor ketensamenwerking in het onderwijs. Voordat we de transactiepatronen beschrijven worden eerst de kenmerken beschreven die gezamenlijk een bepaald transactiepatroon vormen. Een ketensamenwerking (bedrijfstransactie) maakt op basis van deze kenmerken een keuze welk transactiepatroon het beste past. We onderkennen de volgende kenmerken:

- richting (eenzijdig / tweezijdig);
- initiatief (push / pull);
- interactie (timing);
- koppeling (hecht / los);
- verwerking (synchroon / asynchroon).

Richting

Het perspectief richting maakt onderscheidt tussen eenzijdige of tweezijdige communicatie. Met het perspectief richting geven we (op functioneel niveau) aan of een transactie eenzijdig of tweezijdig is. Bij een tweezijdige interactie heeft een inhoudelijke vraag bijvoorbeeld een inhoudelijk antwoord nodig voor het vervolg van de processtap[82]. De interactie heeft daarmee een vraag-en-antwoordkarakter.

- Bij een eenzijdige transactie communiceert een partij een gebeurtenis, melding of wijziging zonder dat een inhoudelijke reactie nodig is om het proces voort te zetten. De verzender is functioneel niet afhankelijk van de verwerking door de ontvanger.
- Bij een tweezijdige transactie verwacht de initiërende partij wel een inhoudelijk antwoord of resultaat dat noodzakelijk is voor de voortgang van het proces.

Initiatief

Met dit kenmerk beschrijven welke partij functioneel het initiatief neemt tot het uitwisselen van gegevens, gebeurtenissen of gewenste wijzigingen richting een andere partij. Het beschrijft welke rol de regie neemt over het starten van de gegevensuitwisseling en niet de technische vorm waarin deze plaatsvindt. Voor dit perspectief gebruiken we ook de rollen gegevensleverancier en gegevensontvanger[83]. Als een gegevensleverancier initieert betreft het een push, indien de gegevensontvanger initieert spreken we van een pull.

De keuze tussen richting en initiatief zijn binnen een transactiepatroon nauw verbonden. Zo is bijvoorbeeld het transactiepatroon bevraging per definitie tweezijdig en wordt geïnitieerd

Met opmerkingen [PL24]: Dit zijn dus transactiepatronen voor gegevensuitwisseling. DAt zijn niet dezelfde als de patronen voor business transacties. Gegevenstransactiepatronen zijn doorgaans atomair, terwijl bedrijfstransacties juist samengesteld zijn. Onderscheid is essentieel.

Met opmerkingen [PL25R24]: De gegevenstransacties moeten dus altijd zo ontworpen zijn dat de bovenliggende businesstransactie kan worden uitgevoerd.

[82] Binnen Digikoppeling wordt in sommige situaties de aanwezigheid van een technisch responsebericht impliciet geïnterpreteerd als tweezijdige interactie. Edu-V kijkt nadrukkelijker naar het functionele karakter van de transactie en beschouwt meldingen daarom als eenzijdig, ook wanneer technisch een request-response mechanisme wordt gebruikt. Binnen Edukoppeling maken we daarom een duidelijk onderscheidt tussen de technische interactie en het functionele procesmatige perspectief.

[83] Het staat dus los van welke partij (indirect of direct) als bronhouder van de gegevens gezien kan worden. Bij initiatief beschouwen we het enkel vanuit de interactie.

door de gegevensontvanger (pull). Ze zijn geen losstaande keuzes, maar vormen samen een belangrijke basis voor de functionele behoefte die het transactiepatroon invult.

Interactie

Met interactie belichten we de technische wijze van communicatie (communicatieprotocol) tussen systemen en in het bijzonder de afhankelijkheid in tijd tussen verzoek en reactie. We maken hierbij onderscheid in een synchrone en asynchrone interactie. Technisch gezien is het transport afgehandeld wanneer het communicatieprotocol een ontvangstbevestiging heeft verstuurd. We bedoelen hierbij dus niet de verwerking van gegevens. Een melding kan bijvoorbeeld zowel synchroon als asynchroon worden verzonden. De keuze wordt bepaald door de aard van het proces.

- Synchroon: Bij een synchrone interactie wachten verzender en ontvanger tijdens dezelfde sessie op elkaar. De initiërende partij ontvangt direct een response via hetzelfde communicatieprotocol. Dit wordt ook wel een request-response interactie genoemd. De snelheid van afleveren en ontvangst response is vaak belangrijker dan de betrouwbaarheid. Technisch gezien is er een time-out aan verbonden. Het systeem van de gegevensontvanger moet met het optreden van een time-out om kunnen gaan. Deze kan bijvoorbeeld besluiten dat het request opnieuw verstuurt moet worden.

Timing	• Het patroon is synchroon in tijd.
Voordelen	• Eenvoud en voorspelbaarheid van de communicatie. • De autorisatie kan direct worden toegepast op het moment van het request
Nadelen	• De client moet wachten op een antwoord • Over het algemeen een hechte koppeling tussen gegevensontvanger en gegevensleverancier.
Wanneer toepassen	Er kunnen zowel gegevens vanuit het request geleverd worden (push-melding) als vanuit de response (pull-bevraging). Synchrone interactie wordt binnen de Edukoppeling-architectuur gerealiseerd via request-response RESTful API's met directe validatie.

- Asynchroon: Bij een asynchrone interactie zijn gegevensleverancier en gegevensontvanger niet gelijktijdig afhankelijk van elkaar (systemen communiceren losgekoppeld in de tijd). Verwerking en eventuele response kunnen op een later moment plaatsvinden. De gegevensleverancier en gegevensontvanger hoeven niet gelijktijdig beschikbaar te zijn. Asynchrone interactie vermindert afhankelijkheden in tijd en ondersteunt lossere koppeling en schaalbaarheid.

Mapping op oriëntaties	• Het patroon is asynchroon in tijd.
Voordelen	• De mate van koppeling is minder hecht dan bij een synchrone interactie. • Draagt bij aan schaalbaarheid en robuustheid van infrastructuur • Verbeterde interoperabiliteit - lossere koppeling tussen systemen
Nadelen	• Introduceert extra complexiteit. Zo zijn aanvullende maatregelen nodig om autorisatie en authenticatie over meerdere stappen te waarborgen. Naast een client en server is er ook sprake van 1 of 2 intermediairs. Deze complexiteit moet beheersbaar worden gehouden door duidelijke architectuurafspraken en standaardisatie (rationale CloudEvents profiel)
Wanneer toepassen	Het wordt toegepast in situaties waarin systemen onafhankelijk moeten kunnen functioneren. Het is een schaalbare oplossing die goed piekbelastingen kan opvangen.

	Asynchrone interactie kan op verschillende manieren worden gerealiseerd, bijvoorbeeld via[84]: • callbacks of webhooks; • messaging-systeem. Asynchrone interactie wordt binnen de Edukoppeling-architectuur gerealiseerd via het CloudEvents profiel[85].

Koppeling

De mate waarin systemen van elkaar afhankelijk zijn wordt aangeduid als de mate van koppeling. Dit is dus breder dan het kenmerk 'interactie' wat met name de mate van afhankelijkheid in de context van tijd typeert. De mate van koppeling is breder (architectuur) en heeft betrekking op de mate van kennis van elkaars systemen men moet hebben, vaak in de vorm van contracten[86]. Ook de mate van beschikbaarheid en openheid en onafhankelijke implementeerbaarheid spelen hierbij een rol. Zonder al te diep in deze zaken te treden kunnen wel het volgende stellen:

- Bij hechte koppeling zijn systemen sterk afhankelijk van elkaar, zowel in termen van beschikbaarheid als in termen van kennis van elkaars interfaces en gedrag. Hechte koppeling kan leiden tot problemen bij hoge belasting of wanneer de server tijdelijk niet beschikbaar is.

Voorbeeld van een synchrone interactie maar een relatief losse koppeling: Een RESTful API met synchrone interactie, maar de systemen toch relatief los gekoppeld: • gebruik van gestandaardiseerde interfaces; • resource-georiënteerde API's; • versiebeheer; • API gateways; • Partijen/systemen hebben beperkte kennis van elkaars (interne) implementaties.

- Losse koppeling betekent dat systemen zo min mogelijk van elkaar afhankelijk zijn. Zij communiceren via gestandaardiseerde interfaces of via intermediairs, zonder dat zij directe kennis hebben van elkaars implementatie. Een belangrijk aspect van losse koppeling is dat veranderingen in één systeem minder impact hebben op andere systemen. Dit bevordert flexibiliteit, schaalbaarheid en onderhoudbaarheid. Tegelijkertijd vraagt losse koppeling om duidelijke afspraken over gegevensstructuren, semantiek en governance, omdat impliciete afhankelijkheden worden vervangen door expliciete contracten.

Voorbeelden waar een asynchrone interactie wordt gebruikt, maar aspecten zorgen voor een relatief vaste koppeling: • point-to-point messaging; • vaste queues per gegevensontvanger; • strak afgestemde berichtstructuren; • specifieke afspraken per koppeling.

Binnen Edukoppeling is losse koppeling een belangrijk uitgangspunt, maar dit betekent niet dat alle interacties volledig ontkoppeld moeten zijn. In sommige situaties, bijvoorbeeld bij

[84] Polling is niet opgenomen, we zien dit als een antipatroon.
[85] Link naar profiel XXXXXX
[86] Zoals OAS en AAS.

directe bevraging van gegevens, is een zekere mate van koppeling acceptabel of zelfs noodzakelijk.

Verwerking

Het kenmerk verwerking heeft betrekking op de functionele afhandeling van de ontvangen gegevens en niet op de wijze waarop systemen technisch met elkaar communiceren (interactie). Het beschrijft de wijze waarop de inhoudelijke afhandeling van een transactie plaatsvindt: direct binnen dezelfde processtap (synchroon) of losgekoppeld in tijd (asynchroon). Een interactie kan synchroon verlopen, terwijl de verwerking asynchroon plaatsvindt.

Bij synchrone verwerking wordt de inhoudelijke verwerking uitgevoerd binnen dezelfde logische processtap als waarin de interactie plaatsvindt. De initiërende partij wacht op de uitkomst van de verwerking voordat het proces verder kan gaan. Bij asynchrone verwerking wordt de verwerking losgekoppeld van de initiële interactie. De ontvangende partij accepteert een verzoek of melding, maar verwerkt deze op een later moment.

De keuze voor synchrone of asynchrone verwerking moet expliciet worden afgewogen op basis van de proceskarakteristieken en staat in principe los van de te kiezen interactievorm.

Met opmerkingen [ER26]: OF: Edukoppeling stuurt op een “ontkoppeling, tenzij …” aanpak, waarbij bewust en onderbouwd gekozen kan worden om een synchrone / hechte koppeling te accepteren

Willen we sterk(er) aansturen op asynchrone interacties en losse koppelingen?

Met opmerkingen [PL27R26]: Primair op ontkoppeling, want daarmee houdt je de flexibiliteit op je gegevenstransacties. Probeer complexere businesstransacties uiteen te rafelen in losse gegevenstransacties. De hechtheid zit vaak in de bovenliggende businesstransacties (en dat is dus - hopelijk- complexiteit die een eigenschap is van het proces, niet van de gegevensuitwisseling). Overigens vind ik inrichten van channels/queues per partij om specifieke operationele eisen te kunnen halen nog steeds losse koppeling, mits je die maar configureerbaar houdt.

Met opmerkingen [PL28R26]: Wat je in ieder geval NIET moet doen is de sterke koppelingen in het businessdomein verleggen naar het applicatiedomein. Dan krijg je businesslogica op de verkeerde laag. API gateways e.d. zijn soms een goede keuze (namelijk als ontkoppeling tussen intern en extern) of bij de ontkoppeling van twee domeinen met verschillende standaarden en governance.

5.2. Transactiepatronen

De keuze voor een transactiepatroon wordt bepaald door een samenhang van de hiervoor genoemde kenmerken. De kenmerken moeten in samenhang worden beschouwd om te komen tot een bepaald transactiepatroon. Binnen Edukoppeling onderkennen we een aantal gestandaardiseerde transactiepatronen. Dit zijn:

- bevraging;
- opdracht;
- melding;
- melding + bevestiging;
- notificatie + ophalen;
- bulk synchronisatie (dataset-overdracht).

Transactiepatroon	Richting	Initiatief	Interactie	Koppeling	Verwerking
Bevraging	Tweezijdig	Pull	Sync	Gemiddeld / Hecht	Sync
Opdracht	Tweezijdig	Push	Sync of Async	Gemiddeld	Sync of Async
Melding	Eenzijdig	Push	Async of Sync	Los	Async
Melding + bevestiging	Eenzijdig + aparte vervolginteractie	Push (+ optioneel vervolg push/pull)	Async en/of Sync (mixed)	Gemiddeld	Async
Notificatie + ophalen	Eenzijdig en Tweezijdig (hybride)	Push + Pull	Async en Sync (mixed)	Gemiddeld	Async
Bulk synchronisatie	Eenzijdig of Tweezijdig	Push of Pull	Sync of Async	Gemiddeld	Async

Bevraging
Doel: opvragen van gegevens of status
Bij het transactiepatroon bevraging bevraagt de gegevensontvanger de gegevensleverancier gericht om gegevens of statusinformatie. Daarbij is het inhoudelijke antwoord noodzakelijk voor de voortgang van het proces bij de gegevensontvanger. Het patroon wordt toegepast wanneer een processtap afhankelijk is van actuele of gevalideerde informatie, bijvoorbeeld bij het raadplegen van registraties, het controleren van rechten of het uitvoeren van validaties.

- De transactie is functioneel tweezijdig van aard: de gegevensontvanger initieert de interactie en verwacht een inhoudelijke respons van de gegevensleverancier. Het initiatief ligt daarmee bij de gegevensontvanger (pull). Deze kenmerken zijn inherent aan het functionele karakter van een bevraging en vormen geen afzonderlijke ontwerpkeuze.

- De gegevensontvanger vraagt over het algemeen een volledig en consistent beeld op van de gevraagde gegevens of status op een bepaald moment in de tijd. Om deze reden wordt een bevraging meestal gerealiseerd via een synchrone interactie, waarbij de gegevensontvanger tijdens dezelfde interactie wacht op een antwoord van de gegevensleverancier.

- Door de afhankelijkheid in tijd en beschikbaarheid tussen gegevensontvanger en gegevensleverancier kent dit patroon doorgaans een relatief hechte koppeling. Deze koppeling kan echter worden beperkt door gebruik te maken van gestandaardiseerde interfaces, stabiele contracten en generieke API-principes. Hierdoor kunnen systemen onafhankelijker evolueren terwijl de functionele interactie behouden blijft.

- De gegevensleverancier verwerkt het verzoek direct en retourneert het resultaat binnen dezelfde interactie (synchrone verwerking). Interne onderdelen van de verwerking kunnen eventueel asynchroon worden ingericht, zolang dit transparant blijft voor de gegevensontvanger en geen invloed heeft op het overeengekomen gedrag van de interactie.

Opdracht
Doel: initiëren van een wijziging met vereiste terugkoppeling
Bij het transactiepatroon opdracht verzoekt een gegevensleverancier een gegevensontvanger om een wijziging door te voeren. In tegenstelling tot een bevraging ligt de nadruk niet op het verkrijgen van informatie, maar op het doorgeven van een wijziging.

- De transactie is functioneel tweezijdig van aard, omdat de gegevensleverancier verwacht dat de opdracht door de gegevensontvanger wordt geaccepteerd, afgewezen of uitgevoerd. Voor het vervolg van het proces is daarmee een inhoudelijke reactie van belang. Het initiatief ligt bij de gegevensleverancier die bepaalt wanneer de opdracht met wijzigingsgegevens wordt verstuurd (push).

- Afhankelijk van de aard van de opdracht kan de interactie synchroon of asynchroon worden ingericht. Wanneer een proces direct afhankelijk is van de uitkomst van de

opdracht ligt een synchrone interactie voor de hand, waarbij direct een resultaat of acceptatie wordt teruggegeven. Bij een langdurig of complex proces is een asynchrone interactie beter passend.

- De mate van koppeling varieert afhankelijk van de gekozen interactievorm en de wijze waarop systemen samenwerken. Synchrone opdrachten leiden doorgaans tot een sterkere afhankelijkheid in tijd en beschikbaarheid. Bij een asynchrone interactie kan de koppeling tussen systemen worden verminderd. Door gebruik te maken van gestandaardiseerde interfaces en contracten kunnen systemen bovendien onafhankelijker evolueren zonder dat het functionele gedrag van de opdracht verandert.

- Verwerking kan synchroon of asynchroon plaatsvinden. Een opdracht kan direct worden uitgevoerd, maar kan ook eerst worden geaccepteerd en later worden verwerkt. Dit laatste ondersteunt schaalbaarheid en ontkoppeling van systemen.

Melding
Doel: communiceren van een gebeurtenis of wijziging
Bij het transactiepatroon melding communiceert een gegevensleverancier een gebeurtenis of een gegevenswijziging. De gegevensleverancier informeert gegevensontvanger(s) zonder afhankelijk te zijn van een inhoudelijke reactie of directe verwerking. Dit is dus anders dan bij het transactiepatroon ‘opdracht’ waar de gegevensleverancier de opdracht geeft aan de gegevensontvanger en het proces wel terugkoppeling vereist (tweezijdig).

Eventgedreven interactie is met name geschikt voor ketens waarin meerdere partijen afhankelijk zijn van wijzigingen in gegevens, zoals mutaties in registraties of statusupdates. Door de ontkoppeling kunnen nieuwe partijen eenvoudig aansluiten zonder impact op bestaande systemen. Tegelijkertijd stelt dit patroon hogere eisen aan governance, semantiek en beveiliging, omdat de context van events expliciet moet worden vastgelegd en behouden.

- De transactie is functioneel eenzijdig van aard. Het initiatief ligt bij de gegevensleverancier (push), omdat deze bepaalt wanneer een gebeurtenis relevant genoeg is om te publiceren. De gegevensontvanger hoeft geen inhoudelijk antwoord terug te geven om de transactie functioneel compleet te maken.

- Een melding kan zowel synchroon als asynchroon worden verstuurd. Bij synchrone interactie blijft de response beperkt tot een technische ontvangstbevestiging.

- De mate van koppeling is doorgaans relatief los, vooral wanneer meldingen via een intermediair of event broker worden gepubliceerd. Hierdoor hoeven gegevensleverancier geen kennis te hebben van individuele gegevensontvangers en kunnen meerdere gegevensontvangers onafhankelijk van elkaar gebeurtenissen verwerken.

- De functionele verwerking van de melding vindt altijd asynchroon plaats, omdat de gegevensleverancier niet afhankelijk is van het resultaat van de verwerking bij de gegevensontvanger(s).

Binnen Edukoppeling is het van belang dat asynchrone patronen consistent worden toegepast en dat duidelijke afspraken worden gemaakt over statusmodellen, foutafhandeling en herlevering. Daarom is er ook een CloudEvents profiel[87] opgesteld dat bijvoorbeeld meer concreet invulling geeft op Asynchrone publish-subscribe interactie.

Publisch-subscribe: Gegevensontvangers (subscribers) abonneren zich op gebeurtenissen in plaats van actief gegevens op te vragen. Wanneer een gebeurtenis plaatsvindt, publiceert een gegevensleverancier (publishers) een event, waarna een gegevensontvanger deze kan verwerken. De distributie van events verloopt doorgaans via een intermediair, zoals een event broker, die subscriptions beheert en events doorstuurt naar geïnteresseerde partijen.

Melding + bevestiging
Doel: communiceren van een gebeurtenis met latere inhoudelijke bevestiging
Bij dit patroon meldt een partij een gebeurtenis of gegevenswijziging, waarna op een later moment een inhoudelijke bevestiging van verwerking wordt vereist. Het patroon combineert daarmee de eigenschappen van een melding met de behoefte aan formele terugkoppeling over de verwerking.

- De initiële melding (push) is functioneel eenzijdig. Het functionele initiatief ligt bij de gegevensleverancier. De gegevensleverancier bepaalt wanneer de melding wordt verstuurd. Met de melding wordt een wijziging, gebeurtenis of nieuwe toestand gecommuniceerd die door de gegevensontvanger verder verwerkt moet worden.

- De interactie kan zowel synchroon als asynchroon worden verstuurd. Bij synchrone interactie ontvangt de gegevensleverancier direct een technische ontvangstbevestiging via hetzelfde communicatiekanaal. De inhoudelijke verwerking vindt daarna los van deze interactie plaats. Bij asynchrone interactie wordt de melding via messaging of eventing aangeboden zonder directe technische response. Ontvangst en verwerking worden volledig ontkoppeld in de tijd.

- De koppeling tussen partijen is sterker dan bij een eenvoudige melding, omdat een functionele relatie bestaat tussen de initiële melding en de latere bevestiging. Toch blijft de tijdsafhankelijkheid beperkt doordat verwerking ontkoppeld plaatsvindt.

- De verwerking van de melding is asynchroon. De gegevensontvanger verwerkt de gegevens op een later moment

Notificatie gevolgd door ophalen
Doel: signaleren dat gegevens beschikbaar zijn waarna afnemer deze zelf ophaalt
Dit patroon combineert een melding met een daaropvolgende bevraging. Een partij publiceert een notificatie dat gegevens beschikbaar zijn of gewijzigd zijn, waarna gegevensontvangers zelfstandig besluiten om de betreffende gegevens op te halen.

- De notificatie is functioneel eenzijdig. De gegevensleverancier informeert gegevensontvangers (push) dat relevante informatie beschikbaar is gekomen. Het ophalen van de gegevens is daarentegen een tweezijdige pull-gebaseerde interactie,

[87] Link xxxxx

waarbij de gegevensontvanger zelf bepaalt wanneer en welke gegevens worden opgevraagd (pull).

- De koppeling tussen systemen is gemiddeld. De gegevensleverancier hoeft niet te weten wanneer of door welke gegevensontvangers gegevens worden opgehaald, terwijl gegevensontvangers onafhankelijk kunnen bepalen hoe zij notificaties verwerken.

- Dit patroon combineert de voordelen van eventgedreven signalering met gecontroleerde gegevensverstrekking. Het voorkomt dat grote of privacygevoelige datasets direct via notificaties worden verspreid en geeft gegevensontvanger controle over het moment van ophalen (asynchrone verwerking).

Bulk synchronisatie (dataset-overdracht)
Doel: uitwisselen of synchroniseren van grotere datasets
Bulk synchronisatie betreft een transactiepatroon waarbij grotere hoeveelheden gegevens of volledige datasets tussen partijen worden uitgewisseld. Het patroon wordt toegepast wanneer het niet efficiënt of wenselijk is om wijzigingen afzonderlijk via individuele transacties of events te communiceren.

- De richting van de transactie kan variëren. In sommige situaties initieert de gegevensontvanger de synchronisatie door gegevens op te vragen (pull), terwijl in andere situaties de gegevensleverancier periodiek datasets distribueert (push). Afhankelijk van de inrichting kan de interactie daarmee eenzijdig of tweezijdig zijn.

- Het doel is doorgaans het verkrijgen of herstellen van een volledige en consistente dataset, bijvoorbeeld bij initiële systeemvulling of periodieke synchronisatie.

- De interactie kan synchroon of asynchroon plaatsvinden

- De mate van koppeling is doorgaans middelmatig. Hoewel systemen minder afhankelijk zijn van directe interactie, bestaan vaak nog expliciete afspraken over formaat, frequentie en volledigheid van datasets. Bulkverwerking vraagt bovendien aanvullende aandacht voor beveiliging, autorisatie en privacy, omdat vaak grote hoeveelheden gegevens tegelijk worden verwerkt.

- De verwerking vindt in de praktijk vaak asynchroon plaats vanwege de omvang van de datasets en de duur van de verwerking. Hiervoor worden vaak achtergrondprocessen, batchverwerking of tijdelijke opslagmechanismen toegepast.

5.3. Informatiebeveiliging

Edukoppeling schrijft voor de beveiliging van zowel synchrone als asynchrone gegevensuitwisseling de toepassing van het OAuth 2.0 client credentials profiel voor.

- Synchrone interactie: Bij een synchrone interactie gaat het om toegang tot RESTful API's. De client vraagt een access token aan bij het authorization server en gebruikt dit token bij elke API-aanroep. De resource server valideert het token en beslist op basis daarvan of de gevraagde handeling is toegestaan. De authorization server speelt een centrale rol door niet alleen de identiteit van de client te verifiëren, maar ook de autorisatiecontext te beoordelen. Op basis van beschikbare informatie en de geldende toegangsregels bepaalt de authorization server of de client bevoegd is om over een bepaald access token te beschikken. Het access token bevat de benodigde informatie waarmee de resource server zelfstandig kan controleren of een verzoek is toegestaan. Daarmee wordt bereikt dat autorisatie niet uitsluitend plaatsvindt bij de uitgifte van het token, maar ook bij het gebruik ervan.

- Asynchrone interactie: Asynchrone interactie introduceert een andere dynamiek. In plaats van directe communicatie tussen twee partijen, worden gegevens uitgewisseld via berichten of events, vaak met tussenkomst van een intermediair. Dit betekent dat de relatie tussen gegevensleverancier en gegevensontvanger minder direct is en dat de beveiligingscontext over meerdere stappen moet worden gehandhaafd. Binnen een EDA architectuur publiceert een systeem gebeurtenissen zonder vooraf te weten welke partijen deze zullen ontvangen. Dit stelt specifieke eisen aan de inrichting van beveiliging. Allereerst moet worden vastgesteld dat de partij die een event publiceert daadwerkelijk bevoegd is om dat te doen. Dit vereist authenticatie en autorisatie op het moment van publicatie, vergelijkbaar met synchrone interactie.

  Vervolgens moet worden geborgd dat alleen geautoriseerde gegevensontvangers toegang krijgen tot de gepubliceerde events. Dit is de verantwoordelijkheid van de intermediair, die fungeert als broker tussen publishers en subscribers. De intermediair beheert subscriptions en bepaalt op basis van beleidsregels welke partijen welke events mogen ontvangen. Daarbij kan gebruik worden gemaakt van dezelfde autorisatiecontext als bij synchrone interactie, inclusief de informatie over namens welke partij wordt gehandeld en voor welke dataset de gegevens relevant zijn.

  De afwezigheid van een directe request-response relatie betekent dat beveiliging niet kan worden gebaseerd op één enkel interactiemoment. In plaats daarvan moet de beveiligingscontext worden meegenomen in de gehele keten, van publicatie tot consumptie. Dit vraagt om consistente afspraken over hoe deze context wordt vastgelegd en doorgegeven. Dit wordt concreet gemaakt in het Edukopppeling CloudEvents profiel[88].

  Door de distributie van events te scheiden van de publicatie ervan, ontstaat een duidelijke scheiding van verantwoordelijkheden. De publisher is verantwoordelijk voor het correct genereren en publiceren van events, terwijl de intermediair verantwoordelijk is voor de distributie en het afdwingen van toegangsregels. Bij asynchrone interacties hebben beide kanten vaak een intermediair. De toepassing

[88] LINK CloudEvents profiel XXXXX

van het Edukoppeling OAuth profiel vindt dus over het algemeen plaats tussen de intermediair rollen. Wanneer een event via een intermediair wordt verspreid, moet de ontvangende partij kunnen vaststellen namens welke organisatie het event is gegenereerd en voor welke context het bedoeld is. Dit vereist dat de relevante contextinformatie expliciet wordt vastgelegd en wordt meegenomen in tokens, eventmetadata of beide. De authorization server moet de context verifiëren en binden aan de uitgifte van tokens. De intermediair en de resource server moeten deze context vervolgens gebruiken bij hun eigen autorisatiebeslissingen. De opname van contextinformatie zorgt ervoor dat de herkomst en bedoeling van gegevens in de keten is geborgd.

Met opmerkingen [ER29]: Moeten we binnen het Oauth profiel naast de edu-to en edu-from paramters ook parameters definiëren voor events?

Risicoprofielen

We belasten ketens niet onnodig met te zware maatregelen. We onderkennen echter wel dat regelgeving alleen maar toeneemt en dat er op termijn zwaardere eisen gaan gelden. We bieden ketensamenwerkingen dus de ruimte om van het lage risicoprofiel te migreren naar het verhoogd risicoprofiel. Verder wordt het overheidsdomein apart onderkend om in deze ketensamenwerking beter te kunnen aansluiten bij de vanuit de overheid opgelegde standaarden.

- Laag risicoprofiel: De gesloten data bevatten geen of slechts beperkt gevoelige informatie en hebben een beperkte impact bij misbruik, er is een laag risico. Client-authenticatie bij het OAuth token-endpoint gebeurt in dit geval op basis van een gedeeld geheim (client-id en wachtwoord) via HTTP Basic Authentication.

- Verhoogd risicoprofiel: Er geldt een verhoogd risicoprofiel als een API gesloten data ontsluit en de impact bij misbruik hoog zal zijn. Er worden hogere eisen gesteld aan client-authenticatie. In plaats van authenticatie op basis van een wachtwoord wordt nu client-authenticatie uitgevoerd op basis van een ondertekening. De ondertekende JWT dient als bewijs dat de client over de private sleutel beschikt. Deze beveiligingsmaatregelen passen bij ketensamenwerkingen waarin integriteit, traceerbaarheid en schade bij misbruik aanzienlijk zijn.

- Verhoogd risico met toepassing van overheidsstandaarden: In de basis worden de beveiligingsmaatregelen van het verhoogd risicoprofiel toegepast, maar daarnaast worden ook overheidsstandaarden en voorzieningen toegepast, zoals PKIoverheid certificaten. Omdat dit profiel ook al de toepassing van het OIN voorschrijft krijgt men met PKIoverheid ook een sterke identificatie omdat de uitgifte van het certificaat gebonden is aan strikte controles door erkende aanbieders (TSP's) onder toezicht van Logius[89]. Het biedt hiermee hogere mate van betrouwbaarheid en sluit aan op afspraken binnen het overheidsdomein.

Logging, auditing en verantwoording

Naast het afdwingen van toegang speelt ook verantwoording een belangrijke rol. Organisaties moeten kunnen aantonen wie toegang heeft gehad tot welke gegevens en onder welke omstandigheden. Dit geldt zowel voor synchrone als asynchrone interacties.

[89] PKIoverheid-certificaten bevatten het Organisatie-identificatienummer (OIN). De CA's die een PKIoverheid certificaat uitgeven verifiëren de identiteit van de organisatie in het handelsregister (Logius | PKIoverheid)

5.4. Privacy

Bij het uitwisselen van gesloten data kan het om persoonsgegevens gaan. Daarbij kan het zijn dat een ketenpartij (verwerker) namens een onderwijsorganisatie (verwerkingsverantwoordelijke) een gegevensuitwisseling uitvoert. De onderwijsorganisatie is dus verantwoordelijk voor de rechtmatigheid van de gegevensverwerking. De Edukoppeling-architectuur ondersteunt de mogelijkheid om gegevens over de rechtmatigheid (mandaat/machtiging[90]) via de gegevensuitwisseling te delen zodat die in keten geverifieerd kan worden met gegevens in de grondslagen en/of organisatie laag.

Vanuit de rollen binnen een ketensamenwerking kan zowel aan de leverende als de ontvangende kant de verwerkingsverantwoordelijke zelf alle rollen uitvoeren. Een veel voorkomende variant is echter dat de bronhouder de verwerkingsverantwoordelijke is en de gegevensleverancier en de gegevensontvanger de rol van verwerker hebben. De rollen hebben in deze context dan de volgende verantwoordelijkheden:

1. de gegevensleverancier als verwerker is verantwoordelijk voor:
    a. het bepalen van de gegevensleveringscontext;
    b. het bepalen van de rechtmatigheid gegevenslevering;
        i. hieronder vallen tevens de grondslag, doelbinding en dataminimalisatie;
    c. vanuit de verantwoordingsplicht het loggen van de levering;
    d. en het leveren van de gegevens;
2. de gegevensontvanger als verwerker is verantwoordelijk voor:
    a. het bepalen van de gegevensontvangst context;
    b. het bepalen van de rechtmatigheid ontvangst;
        i. hieronder vallen tevens de grondslag, doelbinding en dataminimalisatie;
    c. vanuit de verantwoordingsplicht het loggen van de ontvangst;
    d. het ontvangen van gegevens;
3. de bronhouder als verwerkingsverantwoordelijke is verantwoordelijk voor:
    a. het stellen van randvoorwaarden waaronder de gegevensleverancier en de gegevensontvanger de persoonsgegevens mogen verwerken;
        i. rechtmatige grondslag voor verwerking;
        ii. doelbinding;
        iii. dataminimalisatie;
    b. de kwaliteit en beheer van de gegevens.

ROSA kent een aantal privacy gerelateerde architectuurprincipes[91] die relevant zijn voor Edukoppeling, dit zijn:

1. Voorkom onrechtmatige toegang of verspreiding;
2. Voorkom aantasting van gegevensintegriteit;
3. Doelbinding;
4. Dataminimalisatie;

[90] Zie edu-from en edu-to parameters in het OAuth profiel
[91] https://rosa.wikixl.nl/index.php/Architectuurprincipes

5. Unieke en betrouwbare identificatie van entiteiten.

Voorkom onrechtmatige toegang of verspreiding
Ketenpartners voorkomen onrechtmatige toegang tot of verspreiding van gegevens. Gegevensuitwisseling vindt plaats over organisatiegrenzen heen en vaak in een context waarin ketenpartijen elkaar niet volledig kennen of kunnen controleren. Voordat een ketenpartij kan vaststellen of er sprake is van rechtmatige toegang tot persoonsgegevens moeten ketenpartijen elkaar betrouwbaar kunnen identificeren, authentiseren en autoriseren. Ketenpartners dragen er zorg voor dat hun identiteiten correct worden beheerd en dat cryptografische sleutels veilig worden opgeslagen en dat autorisaties zorgvuldig worden ingericht.

1 Identificatie: Identificatie bepaalt hoe een organisatie uniek herkenbaar zijn binnen de ketensamenwerking.
    a. Een ketensamenwerking moet binnen Edukoppeling het identificatieschema kiezen dat voor identificatie van een ketenpartij gebruikt wordt. Indien mogelijk moet het Digikikoppeling organisatie-identificatienummer (OIN[92]) worden gebruikt.
    b. Een ketenpartij in de rol van gegevensleverancier koppelt de identiteit van de gegevensontvanger aan de identifier van het ontvangende systeem[93] dat interacteert met de RESTful API.
2 Authenticatie: Authenticatie betreft het aantonen dat een partij daadwerkelijk is wie zij zegt te zijn.
    a. Een ketensamenwerking moet binnen Edukoppeling kiezen hoe het ontvangende systeem zich authentiseert. Bij het delen van persoonsgegevens moet het hoogste risicoprofiel[94] worden toegepast.
3 Autorisatie: Autorisatie bepaalt welke acties een geauthentiseerde client mag uitvoeren en welke gegevens toegankelijk zijn
    a. Toegang tot API's moet aansluiten op de juridische grondslag en het doel van de gegevensuitwisseling.
    b. Voor het scenario waar een gegevensontvanger (en hun client) namens een andere organisatie handelt biedt Edukopeling de optie om informatie rond een mandaat/machtiging door te geven waarmee een gegevensleverancier op applicatieniveau kan controleren of de gegevensontvanger, en hiermee het client systeem, toegang mag krijgen tot het gegevens leverend systeem.

Voorkom aantasting van gegevensintegriteit
Ketenpartners voorkomen aantasting van de integriteit van gegevens. In de context van Edukoppeling vereist dit dat (persoons)gegevens zo worden getransporteerd dat aantasting van de juistheid, volledigheid en/of tijdigheid onmogelijk wordt gemaakt. Edukoppeling schrijft voor alle gegevensuitwisselingen het gebruik van TLS voor op basis van de Edustandaard UBV TLS[95] afspraak.

Doelbinding

[92] Zie OIN Stelsel 2.2.1
[93] In deze versie wordt OAuth client credentials gebruikt (zie hoofdstuk xXX) en is het de client die interacteert met de RESTful API.
[94] Zie risicoprofielen bij Informatiebeveiliging.
[95] Zie Edukoppeling profielen

Verwerking van persoonsgegevens moet toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is. Een ketensamenwerking zorgt ervoor dat het ontwerp van de API-specificaties zoveel mogelijk in overeenstemming zijn met de het bovenliggend gestelde doel.

Dataminimalisatie
Verwerking van persoonsgegevens moet toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is. Een ketensamenwerking moet de API-specificaties en hiermee de scopes[96] zodanig ontworpen dat alleen noodzakelijke gegevens worden uitgewisseld.

Unieke en betrouwbare identificatie van entiteiten[97]
Identificatie is onderdeel van toegang. Een ketensamenwerking moet binnen Edukoppeling het identificatieschema kiezen dat voor identificatie van een ketenpartij gebruikt wordt. Indien mogelijk moet het OIN worden gebruikt. Voor het gegevensontvangend systeem (client) is het gegevensleverend systeem (AS/RS) vrij om een keuze te maken in een identificatieschema. Zolang dit systeem binnen het betreffende bereik maar uniek geïdentificeerd kan worden.

[96] In deze versie wordt OAuth client credentials gebruikt (zie hoofdstuk xXX) en de scopes in het Access Token bepalen op grofmazig niveau waartoe de client geautoriseerd is.
[97] https://rosa.wikixl.nl/index.php/Id-d0d50170e49d45529c4a0c37d9dab4cc

6. API-architectuur

Met opmerkingen [ER30]: TODO - API's en standaarden, Bespreken op 20 mei wat we allemaal in dit hoofdstuk willen. Is testbeleid correct/volledig?

Met opmerkingen [PL31R30]: Een deel van de concepten die hier worden geïntroduceerd zijn eigenlijk generiek (niet API-specifiek). In dit hoofdstuk ga je dus eigenlijk een invulling geven van die concepten aan de hand van API's.

6.1. Inleiding

Gegevensuitwisseling werd vaak gerealiseerd via point-to-point koppelingen en batchuitwisselingen. Deze architectuur legt de nadruk op de toepassing van API-gebaseerde interactie. Daarbij worden API's gezien als de technische contracten voor samenwerking binnen ketens. We sluiten hiermee aan op het API-first principe[98] dat betekent dat interacties tussen systemen vooraf worden ontworpen en gestandaardiseerd. Niet de interne werking van systemen staat centraal, maar de contractuele gegevensuitwisseling tussen partijen. Een API beschrijft welke gegevens of functionaliteit beschikbaar worden gesteld, onder welke voorwaarden dit gebeurt en welke beveiligings- en interoperabiliteitsafspraken daarbij gelden. Deze ontwikkeling sluit aan bij bredere ontwikkelingen binnen overheid en bedrijfsleven waarin API's worden beschouwd als de primaire bouwstenen voor digitale dienstverlening en interoperabiliteit.

6.2. Standaarden

De Edukoppeling API-architectuur sluit aan op breed toegepaste internationale open standaarden. Het gebruik van open standaarden voorkomt leveranciersafhankelijkheid, ondersteunt interoperabiliteit tussen ketenpartijen en maakt aansluiting mogelijk op bestaande producten, cloudplatformen en publieke voorzieningen.

RESTful API standaarden

Voor synchrone interacties wordt uitgegaan van RESTful API's die gegevens en functionaliteit beschikbaar stellen via HTTP-gebaseerde interfaces. Daarbij wordt gebruikgemaakt van JSON als primair formaat voor gegevensuitwisseling. Voor de formele beschrijving van RESTful API's wordt aangesloten op de OpenAPI Specification (OAS[99]). Hiermee kunnen API-contracten op een gestandaardiseerde wijze worden beschreven, gepubliceerd en gevalideerd. OAS ondersteunt daarnaast automatische documentatie, validatie en codegeneratie, waardoor interoperabiliteit tussen aanbieders en afnemers wordt vergroot.

EDA standaarden

Voor EDA interacties wordt gebruikgemaakt van CloudEvents als gestandaardiseerd eventmodel. CloudEvents definieert uniforme metadata voor gebeurtenissen, zoals identificatie, bron, tijdstip en type event. Hierdoor kunnen publishers, brokers en subscribers interoperabel samenwerken, onafhankelijk van de gebruikte messaging-technologie. Voor de beschrijving van asynchrone API's en eventstromen wordt aangesloten op de AsyncAPI Specification (AAS[100]). AsyncAPI vervult hierbij een vergelijkbare rol als OAS voor RESTful API's en ondersteunt het formeel beschrijven van eventkanalen, berichtenstructuren en bindings naar messaging-platformen.

Beveiligingsstandaarden

[98] https://docs.geostandaarden.nl/api/API-Strategie/#api-first-strategie
[99] https://swagger.io/specification/
[100] https://www.asyncapi.com/docs/reference/specification/v3.1.0

Voor beveiliging wordt binnen Edukoppeling gebruikgemaakt van OAuth 2.0, specifiek het Client Credentials profiel voor machine-to-machine interactie. OAuth biedt een gestandaardiseerd autorisatiemodel waarbij clients gecontroleerd toegang verkrijgen tot API's via access tokens. Access tokens en client assertions worden gerealiseerd met JSON Web Tokens (JWT). JWT biedt een gestandaardiseerd formaat voor het uitwisselen van claims en autorisatiecontext in een compact en digitaal ondertekend tokenformaat. Door toepassing van asymmetrische cryptografie (clientauthenticatie op basis van private_key_jwt) kunnen tokens betrouwbaar worden gevalideerd zonder dat gedeelde geheimen noodzakelijk zijn.

Voor sleuteluitwisseling en sleutelbeheer wordt aangesloten op JSON Web Key (JWK) en JSON Web Key Sets (JWKS). Hiermee kunnen publieke sleutels op een gestandaardiseerde wijze gepubliceerd en beheerd worden. Deze aanpak ondersteunt automatische sleutelrotatie en beperkt afhankelijkheid van individuele certificaten.

Voor transportbeveiliging wordt gebruikgemaakt van TLS (Edustandaard UBV TLS afspraak). Hiermee wordt vertrouwelijkheid en integriteit van gegevens tijdens transport geborgd. Binnen vertrouwensmodellen kunnen zowel PKIoverheid-certificaten als certificaten van publieke CA's worden toegepast, afhankelijk van de eisen van het ketendomein en de gekozen trustarchitectuur.

6.3. Bouwblokken

De Edukoppeling bevat voorschriften, maar de API-architectuur in de keten bestaat uit een samenhangend geheel van bouwblokken die gezamenlijk veilige, schaalbare en beheersbare gegevensuitwisseling binnen onderwijsketens moeten realiseren. Deze bouwblokken ondersteunen niet alleen de technische connectiviteit tussen systemen, maar ook de organisatorische en bestuurlijke aspecten van ketensamenwerking, zoals beveiliging, governance, mandaat en privacy.

API (gegevensleverend systeem)
Een centraal bouwblok binnen de architectuur is zijn API's. Dit bouwblok stelt gegevens en betreffende functionaliteit beschikbaar via gestandaardiseerde API's en vormt daarmee de gecontroleerde toegangspoort tot gegevensdiensten. Een API abstraheert de achterliggende bronregistratie en biedt een stabiel contract richting gegevensontvangers. Een API-aanbieder (gegevensleverancier) zorgt voor het beschikbaar stellen en beheer van de API.

API Gateway
In een moderne API-architectuur vervult de API Gateway een belangrijke rol als centraal integratie- en beveiligingspunt. De gateway vormt het gecontroleerde toegangspunt voor API-verkeer en ondersteunt functies zoals authenticatie, routering, tokenvalidatie, rate limiting, monitoring en auditing.

Door deze functies centraal te organiseren ontstaat een consistente manier om beveiligings- en governancebeleid af te dwingen. Achterliggende API-services hoeven hierdoor niet individueel alle beveiligingsfunctionaliteit te implementeren. Dit vereenvoudigt beheer en verhoogt de consistentie van beveiligingsmaatregelen binnen de keten.

Binnen Edukoppeling speelt de gateway bovendien een belangrijke rol bij contextuele autorisatie. Hierbij worden niet alleen access tokens gevalideerd, maar ook aanvullende context zoals edu-from en edu-to als die gebruikt worden. Hierdoor kan de gateway controleren namens welke organisatie een client handelt.

Daarnaast ondersteunt de gateway monitoring en auditing van API-gebruik. Omdat veel gegevensuitwisseling binnen onderwijsketens plaatsvindt in de context van persoonsgegevens, is inzicht in gebruik, toegang en ketengedrag essentieel voor verantwoording en beveiliging.

Authorization Server

Een ander essentieel bouwblok binnen de architectuur is de Authorization Server. Dit bouwblok verzorgt authenticatie en autorisatie binnen de API-keten en verstrekt access tokens aan geauthenticeerde clients. Binnen Edukoppeling wordt gebruikgemaakt van OAuth 2.0 Client Credentials. De Authorization Server valideert hierbij de identiteit van clients en verstrekt tokens waarmee toegang tot API's kan worden verkregen.

De Authorization Server vormt daarmee een belangrijk onderdeel van het vertrouwensmodel binnen de keten. Tijdens onboarding worden clients, publieke sleutels, scopes, authorization_details en vertrouwensrelaties geregistreerd. Hierdoor ontstaat een gecontroleerd model waarin expliciet is vastgelegd welke partijen toegang hebben tot welke gegevensdiensten.

Consent- en mandaatregisters

De eerdere versie van de Edukoppeling architectuur ging uit van een centraal Onderwijs Service Register (OSR[101]) voor het vastleggen van mandaten. We zien dat afsprakenstelsels nu dergelijke informatie ook decentraal[102] registreren. In dergelijke registers wordt vastgelegd welke gegevensafnemend systeem toegang heeft en namens welke organisatie wordt gehandeld, welke toestemming is verleend en binnen welke context gegevens mogen worden verwerkt.

Intermediair(s) bij asynchrone interacties

Voor asynchrone interacties en eventgedreven architectuur onderkennen we de rol van een intermediair. Dit bouwblokken ondersteunt het publiceren, distribueren en verwerken van gebeurtenissen binnen de keten. Binnen Edukoppeling wordt voor de standaardisatie van eventmetadata aangesloten op CloudEvents en voor de beschrijving van eventinterfaces op AsyncAPI.

Logging, auditing en monitoring

Omdat veel gegevensuitwisselingen binnen het onderwijs betrekking hebben op persoonsgegevens is inzicht in gebruik, beveiliging en naleving van afspraken belangrijk. Logging-, audit- en monitoringvoorzieningen vormen een belangrijk onderdeel binnen een ketensamenwerking om dit te realiseren. In deze architectuur zijn deze bouwblokken niet uitgewerkt.

Met opmerkingen [ER32]: Is belangrijk, maar valt dit binnen Edukoppeling?

Met opmerkingen [PL33R32]: Ja, want traceerbaarheid is óók een concern voor de applicatielaag.

[101] Welkom bij het Onderwijs serviceregister
[102] Zie Edu-V consentmanagement https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/75268097/Regie+op+gegevens

6.4. Testbeleid

Binnen Edukoppeling geldt dat test- en productieomgevingen strikt van elkaar gescheiden moeten blijven. Deze scheiding heeft niet alleen betrekking op infrastructuur, maar ook op identiteiten, certificaten, datasets en vertrouwensrelaties. Testomgevingen moeten gebruikmaken van aparte clientidentiteiten, aparte OAuth-configuraties en aparte truststores.

Met dit testbeleid creëren we meer uniformiteit hoe ketensamenwerkingen de met Edukoppeling beveiligde API's testen. Een testbeleid is nodig omdat we vernemen dat er in verschillende ketens verschillende keuzes worden gemaakt. Dit is inefficiënt en introduceert onnodige risico's. Een goed ingericht testbeleid draagt bij aan de veiligheid van Edukoppeling-implementaties. Een ketensamenwerking bestaat uit meerdere ketenpartijen en systemen en het testen hiervan is al complex genoeg. Bij het testen van API's gelden de volgende afspraken:

1. Er is een duidelijke scheiding tussen test- en productieomgevingen en voor elk zijn er duidelijke afspraken.
    a. Testomgevingen gebruiken andere certificaten dan in productie (gebruik bij voorkeur verschillende vertrouwensankers[103])
        i. Bij toepassing van PKIoverheid: PKIoverheid vereist de toepassing van een andere root-CA voor testcertificaten[104]. Voor testomgevingen worden TRIAL-certificaten[105] met een PKIoverheid G4 TRIAL root certificaat geboden. Hierbij kan een ketensamenwerking (eventueel in overleg met Logius) een eigen "fauxTSP" CA-certificaat[106] genereren.
    b. Certificaten kunnen verlopen of ingetrokken worden. Het testen van sleutelmanagement is onderdeel van het testprogramma.
    c. Een testomgeving bevat geen productie-data. De productie-identiteit wordt dus niet als testidentiteit gebruikt. Het gebruiken van andere identifiers in testomgevingen verkleint de kans verwarring en draagt bij aan een duidelijke scheiding.
        i. PKIoverheid: Om in testomgevingen geen productiedata te gebruiken bevat een G4 TRIAL certificaat een test OIN[107].
2. Testen is een integraal onderdeel van de ontwikkel- en beheerprocessen. We gaan uit van "security en privacy by design". Beveiliging en privacy worden in de test meegenomen. Testen vindt dus plaats in de gehele lifecycle van de API en niet uitsluitend voorafgaand aan productie.
    a. EDA vraagt extra aandacht bij testen omdat events asynchroon worden verwerkt en meerdere systemen betrokken kunnen zijn. Dit vraagt om het

[103] Een testcertificaat heeft een andere root-CA dan in productie. Testcertificaten worden zo niet impliciet vertrouwd in de productieomgeving
[104] Zie #3 https://gitdocumentatie.logius.nl/publicatie/dk/beveilig/2.0.1/#pkioverheid-programma-van-eisen
[105] GitHub - pkioverheid/g4-trial: Generate TRIAL certificates for the PKIoverheid G4 hierarchies · GitHub
[106] https://github.com/pkioverheid/g4-trial?tab=readme-ov-file#overview
[107] https://gitdocumentatie.logius.nl/publicatie/dk/oin/2.2.1/#prefix-tabel

expliciet testen van replayscenario's, foutafhandeling en duplicaatverwerking. Ontvangers moeten events idempotent kunnen verwerken en correct omgaan met vertraagde of opnieuw aangeboden gebeurtenissen.

3 De tests zijn op maat gemaakt, bijvoorbeeld verschillende typen tests voor verschillende typen interacties.

7. Bijlage A: Begrippen

Met opmerkingen [ER34]: TODO

Met opmerkingen [BD35R34]: De check met het net nieuw opgeleverde NORA/GDI begrippenkader gegevensuitwisseling (https://begrippen.noraonline.nl/gegevensuitwisseling/nl/) moet nog plaatsvinden

Begrip	Definitie	Bron
Open en gesloten 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 Gesloten Data.	Digikoppeling Architectuur 2.1.0
Synchroon		
Asynchroon		
Melding		
API-aanbieder		
API-afnemer		
Bulk-verwerking	Ook wel batchverwerking, betreft het uitwisselen of verwerken van grotere hoeveelheden gegevens in één samenhangende operatie, in plaats van individuele transacties per bericht of API-aanroep.	Edukoppeling
Bronhouder		
Transactiepatroon		