Kennisnet

Nummervoorziening Principes en processen

Pseudonimisering in de leermiddelenketen

Laat ict werken **voor het onderwijs**

Inhoud

Document informatie

Status

Auteur	Kennisnet, Marc Fleischeuers
Versie	1.0.9
Versiedatum	23 jan 2017
Status	Goedgekeurd

Versiehistorie

Versie	Datum	Auteur	Beschrijving
0.9	6 april 2016	Marc Fleischeuers	Samengesteld uit eerdere documenten
0.91	18 april 2016	Marc Fleischeuers	Nav KAT team terugkoppeling
0.92	11 mei 2016	Marc Fleischeuers	Verwoording van encryptie en hashing bij opslag; (A) alleen voor LAS functionaliteit; test- en accreditatieproces, toegangsautorisatie
0.93		Marc Fleischeuers	Consistent met tech voorschriften, paragraaf certificeringsschema, voorschriften aanmelding
1.0	12-7-2016	Marc Fleischeuers	Definitief
1.0.9	23-1-2017	Marc Fleischeuers	Wijzigingen wetgeving (introductie stampseudoniem)
1.0.10	26-10-2017	Marc Fleischeuers	Splitsing Nummervoorziening en ECK ID

Betrokken/geraadpleegd

Betrokken	Rol

Distributie en goedkeuring

Versie	Datum	Goedgekeurd (indien van toepassing)
1.0.9	21-3-2017	Tactisch overleg Toegang tot leermateriaal

1. Samenvatting

Het Doorbraakproject Onderwijs en ICT heeft Kennisnet de opdracht gegeven om een Nummervoorziening te ontwerpen en realiseren. Deze dienst heeft als doel om binnen de leermiddelen keten elke leerling en student een uniek kenmerk (pseudoniem) te geven. Deze dienst wordt gezien als een belangrijke voorwaarde in het streven om de uitwisseling van persoonsgegevens in de leermiddelenketen terug te brengen tot alleen de gegevens die echt nodig zijn, in de situatie waar het echt nodig is (doelbinding en dataminimalisatie ter bevordering van privacy). Verder wordt ook de samenwerking tussen systemen in de keten vereenvoudigd, zodat de ketenprocessen makkelijker verlopen en minder foutgevoelig zijn.

Behalve de feitelijke koppeling tussen leerlingadministratie en Nummervoorziening voor het generen van het ID, zijn er nog een aantal andere taken en verantwoordelijkheden in te vullen om uiteindelijk te komen tot de gewenste dataminimalisatie en verbetering in efficiëntie. In dit overzicht worden de verantwoordelijkheden beschreven, samen met een suggestie hoe ze belegd kunnen worden.

Een aantal verantwoordelijkheden zijn nog nader te bespreken:

- **Correcties verkeerd ketenpseudoniem**. Als een leerling aanvankelijk een verkeerd ketenpseudoniem heeft gekregen (bijvoorbeeld omdat de leerling is aangemeld op basis van een ander BSN of onderwijsnummer) kan de instelling dit corrigeren door opnieuw een ketenpseudoniem aan te vragen. Als het verkeerde pseudoniem echter al in de keten in gebruik is zou deze correctie hier ook doorgevoerd moeten worden. Deze situaties komen niet vaak voor (we vragen ook dat de aanmeld- of inschrijfgegevens gevalideerd worden bij DUO voorafgaand aan de aanvraag van een ECK ID) maar als het gebeurt vragen ze om gecoördineerde actie in de keten. Zie punt 6 op pagina **Error! Bookmark not defined.**.

- **Massale invoering**. Hoe kunnen school en LAS de massale invoering van ECK IDs het beste inrichten. Zowel de 1e niveau hashing in de leerlingadministratie als de hashing door de nummervoorziening kan langer duren dan een interactieve taak. Zie punt 8 op pagina **Error! Bookmark not defined.**.

- **Ondersteunen van de servicedesks**. In situaties dat servicedesks van ketenpartijen met elkaar communiceren over een leerling of individuele acties van een leerling, moet er een manier worden ontwikkeld om de leerling of de transactie onderling te kunnen identificeren. Zie punten 1 en 2 op pagina **Error! Bookmark not defined.**.

In het eerste deel van dit document worden processen en maatregelen rondom het gebruik van het ECK ID in de leermiddelenketen beschreven. In het tweede deel is het beveiligingsbeleid beschreven, hierin worden de voorschriften geformuleerd waaraan de systemen van de Nummervoorziening en ketenpartijen moeten voldoen.

2. Proces van aanmaken van ECK IDs

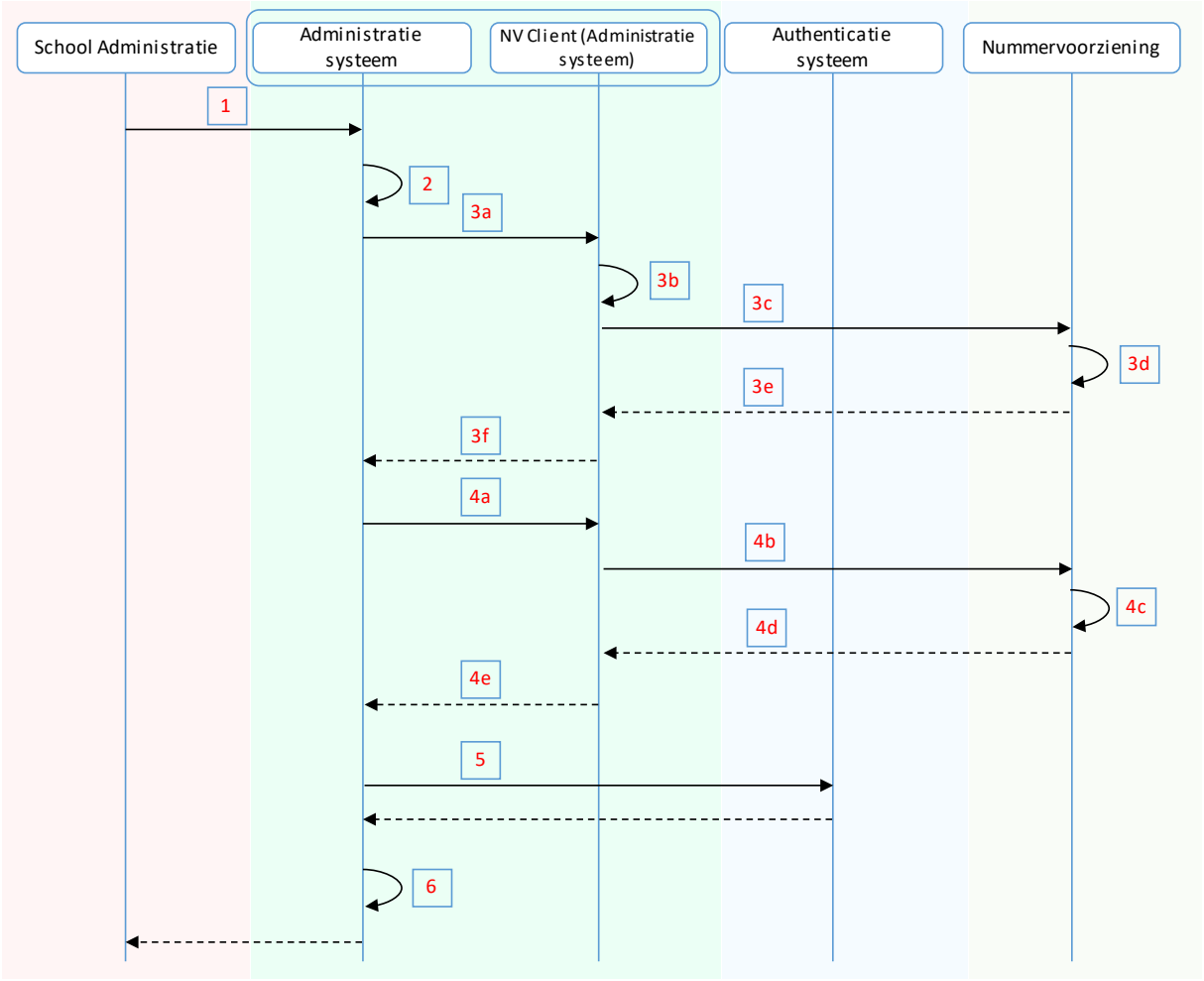
Dit hoofdstuk beschrijft de interactie tussen de betrokken systemen bij het tot stand laten komen van een ECK ID voor een leerling van VO of MBO (het proces voor PO leerlingen verloopt op punten wezenlijk anders, zie de use cases documentatie). Deze interactie vindt doorgaans plaats bij de *aanmelding* van een VO leerling en MBO student op een opleiding of school. Het moment is met name van belang om hen in staat te stellen met een ECK ID materialen te bestellen (na de aanmelding, voorafgaand aan het begin van het schooljaar) en het materiaal te gebruiken (vanaf het begin van het schooljaar)[1]. Dit document bevat voorbeelden die uitgaan van een aanmelding gevolgd door de aanmaak van een ECK ID; in use case documentatie die nu wordt ontwikkeld staan scenario's waarin het aanmaken van het ECK ID op een later tijdstip kan worden ondersteund.

In dit voorbeeld wordt verondersteld dat de school beschikt over een administratiesysteem dat de aanmelding verwerkt, en dat dit systeem gekoppeld is met de Nummervoorziening door middel van een "client" component. Daarnaast beschikt de school over een authenticatiesysteem dat beschikt over de inloggegevens van de leerling. De school beschikt over een systeem waar persoonsgegevens waaronder het PGN veilig zijn opgeslagen; het ECK ID zal hier ook (geencrypt) worden opgeslagen.

Dit is een van de drie belangrijke interacties tussen schooladministratie en de Nummervoorziening. De andere twee interacties zijn de aanvraag van een grote hoeveelheid ECK IDs tegelijkertijd (batch aanvraag) en het melden van een leerling waarvan het PGN is gewijzigd door de autoriteiten. Deze interacties zijn niet uitgewerkt in detailprocessen.

Er zijn scholen waar de verantwoordelijkheden anders over de systemen zijn verdeeld. Dit voorbeeld kan gebruikt worden om de interacties voor elke situatie specifiek uit te werken.

[1] Er zijn alternatieve scenario's mogelijk waarin het ECK ID pas tijdens *gebruik* aan de leerling wordt gekoppeld.



Figuur 1 Sequentiediagram van de verwerkingen van het ECK ID gedurende de aanmaak

De individuele stappen zijn hieronder verder toegelicht. Voor elke stap wordt indien van toepassing verwezen naar maatregelen en voorschriften die genomen moeten worden om de informatieuitwisseling te beveiligen. De voorschriften zijn beschreven in document “Technische voorschriften”. Een (A) markeert maatregelen waar een leerlingadministratie op getoetst (en eventueel geaudit) gaat worden bij toelating.

1. De medewerker van de schooladministratie verwerkt een aanmelding van een VO- of MBO leerling. Tijdens dit proces worden persoonsgegevens van een leerling, onder andere naam, adres, woonplaats en PGN verwerkt. Dit is een bestaand proces. Gegevens van de leerling worden ingevoerd in de leerlingadministratie en geverifieerd bij DUO (niet getoond)

   Maatregelen: (A)

   - Om fouten te voorkomen bij het invoeren van het PGN bij leerlingen, mag het ECK ID pas worden aangevraagd na een succesvolle validatie van de aanmeldgegevens bij DUO[2]. De leerlingadministratie ziet toe op deze controle.
   - Voor docenten en andere niet-leerlingen stelt de leerlingadministratie de basis voor volgens *voorschrift ECKID-1*.

2. Indien nodig bepaalt of bevestigt de medewerker de sector en keten waarvoor een ketenpseudoniem wordt aangevraagd[3]. Zie de servicebeschrijving (servicebeschrijvingen.doc) van service retrieveChains en retrieveSectors voor meer informatie.

[2] Het is met name van belang dat het PGN van de leerling gevalideerd is.

[3] Sector en keten zullen meestal constant zijn voor een instelling, dus het ligt voor de hand dat het administratiesysteem deze waarden in een vaste instelling gebruikt.

Maatregelen: geen bijzondere maatregelen.

3. Om een ECK ID aan te vragen, moet gebruik worden gemaakt van een stampseudoniem van de leerling of docent, die in deze stap wordt aangevraagd. Als de leerlingadministratie al beschikt over een stampseudoniem voor de leerling wordt deze stap overgeslagen.

    a. De leerlingadministratie roept de functie voor het genereren van een stampseudoniem aan in de Nummervoorziening client, en geeft hierbij op het PGN of de gekozen basis voor docenten (zie *Voorschrift ECKID-1* in Technische voorschriften).

    Maatregelen: (A) De leverancier van de leerlingadministratie voorkomt dat het PGN hierbij kan uitlekken.

    b. De client voert 1e niveau hashing van de invoer uit.

    Maatregel: (A) Hashing wordt uitgevoerd volgens *voorschrift NV-1* en conform de referentie-implementatie.

    c. De client roept de service van de Nummervoorziening aan met het gehashte PG om een stampseudoniem aan te maken.

    Maatregel: De koppeling maakt gebruik van EduKoppeling v1.2 volgens *voorschrift NV-2* en TLS volgens *voorschrift NV-4*.

    d. De Nummervoorziening controleert de invoer en maakt het stampseudoniem.

    e. De Nummervoorziening stelt een retourbericht samen dat het stampseudoniem bevat (of een foutmelding, indien een controle faalt) en stuurt dit terug als antwoord op 3c.

    Maatregel: De koppeling maakt gebruik van EduKoppeling v1.2 volgens *voorschrift NV-2* en TLS volgens *voorschrift NV-4*.

    f. De client haalt het stampseudoniem uit het antwoordbericht en retourneert deze aan de leerlingadministratie als antwoord op 3a.

    Maatregel: (A) De leverancier van de leerlingadministratie voorkomt dat het ECK-ID hierbij uitlekt.

4. Op basis van het stampseudoniem, de onderwijssector en de gekozen keten (ECK keten) kan de leerlingadministratie nu een ECK ID aanvragen.

    a. De leerlingadministratie roept de client van de Nummervoorziening aan om een ECK ID aan te vragen, en geeft hierbij het stampseudoniem van de leerling, ID van de gekozen sector en ID van de gekozen keten.

    Maatregelen: (A) De leverancier van de leerlingadministratie voorkomt dat het PGN hierbij kan uitlekken.

    b. De client roept de service van de Nummervoorziening aan met het stampseudoniem, ID van de gekozen sector en ID van de gekozen keten

    Maatregelen: (A) De koppeling maakt gebruik van EduKoppeling v1.2 volgens *voorschrift NV-2* en TLS volgens *voorschrift NV-4*.

    c. De Nummervoorziening controleert de invoer en stelt het ECK ID hiermee samen.

    Maatregel: Maken van het ECK ID wordt uitgevoerd volgens *voorschrift NV-3*. De verwerking wordt gelogd.

    d. De Nummervoorziening stelt een retourbericht samen dat het ECK ID bevat en stuurt dit terug als antwoord op 4b.

    Maatregel: De koppeling maakt gebruik van EduKoppeling v1.2 volgens *voorschrift NV-2* en TLS volgens *voorschrift NV-4*.

    e. De Nummervoorziening client haalt het ECK ID uit het retourbericht en retourneert dit aan de leerlingadministratie als antwoord op 4a.

    Maatregel: (A) De leverancier van de leerlingadministratie voorkomt dat het ECK-ID hierbij uitlekt.

5. Als onderdeel van de aanmelding worden de leerlinggegevens waaronder het stampseudoniem en het ECK ID gekoppeld aan een lokale identificatie.

   Maatregel: geen bijzondere maatregelen

6. De leerlingadministratie beschikt nu over de aanmeldgegevens waaronder het stampseudoniem, het ECK ID en de lokale identifier van de leerling. Het stampseudoniem, het ECK ID en mogelijk andere gegevens worden geencrypt en de gegevens worden geregistreerd in de daartoe aangewezen systemen.

   Maatregel: (A) Opslag van het stampseudoniem en het ECK ID wordt uitgevoerd volgens *voorschrift ECKID-2*.

Scholen zijn vrij om hun administratieve systemen in te richten en dat betekent dat er aanzienlijke variaties zijn in de wijze waarop de Nummervoorziening en het ECK ID voor opslag en gebruik het beste kan worden ingericht. Kennisnet zal samen met zijn partners een aantal handreikingen en voorkeursscenario's ontwikkelen om de scholen en hun partners te helpen bij het goed implementeren van deze processen. Hierbij zal ook aandacht worden besteed aan IDP-last scenario's en andere varianten, zowel voor het aanmaken van het ECK ID als het gebruik.

2.1. Certificeringsschema

De maatregelen en voorschriften die hierin worden genoemd verhouden zich met het Certificeringsschema (zie https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-2017/). Bij invoering van het certificeringsschema zal elke ketenpartij die de Nummervoorziening gebruikt of het ECK ID verwerkt, een BIV classificatie uitvoeren voor de betreffende informatiesystemen, en van daaruit zijn eigen maatregelen formuleren om te voldoen aan de eisen die aan het verwerken van de informatie worden gesteld.

In het volgende overzicht is gemarkeerd welke processtappen en technische voorschriften maatregelen hebben voor ketenpartijen die overlap hebben met maatregelen in het Certificeringsschema. De overige processtappen zijn inherent aan het gebruik van de nummervoorziening of specifiek voor de nummervoorziening.

Processtappen aanvraag ECK ID	**Processtappen gebruik van ECK ID**	**Technische voorschriften**
1 Verwerken aanmelding	1 Openen ELO/Portaal door leerling	1 ECK ID voor docenten
2 Bevestigen sector/keten	2 Inlog door leerling	2 1e niveau hashing ECK ID
3 Aanroep client nummervoorz.	3 Ophalen ECK ID	3 Toepassen EduKoppeling
4 Hashing invoer	4 (optioneel) federatieve authenticatie	4 Hashing nummervoorziening
5 Aanroep nummervoorziening (2x)	5 Leerling is ingelogd	5 Opslag ECK ID administratie
6 Samenstelling stampseudoniem, ECK ID	6 Leerling klikt op link in ELO/Portaal	6 Opslag ECK ID ketenpartij
7 Terugsturen retourbericht Nummervoorziening	7 Gegevens verstuurd naar ketenpartner	7 Toepassen TLS door LAS
8 Client stuurt ECK ID terug	8 Controle gehashte/encrypte ECK ID	8 Toepassen TLS ketenpartner

9 Aanmaken lokaal account	9 Opslag ECK ID	
10 Opslag ECK ID	10 Leerling krijgt toegang	

De gemarkeerde maatregelen gaan over de volgende drie onderwerpen:

- Beveiliging van verbindingen tussen nummervoorziening client en leerlingadministratie
- Beveiliging van verbindingen tussen de nummervoorziening client en nummervoorziening
- Opslag van het stampseudoniem en het ECK ID

De BIV classificatie die we hanteren (en die dus feitelijk door de leverancier van het LAS gemaakt wordt) bij het formuleren van de maatregelen is hierbij: L, M, M voor respectievelijk B, I en V.

Toelichting bij de gemarkeerde stappen voor aanmaken ECK ID:

- Stap 3a, 3f, 4a, 4e: deze stappen veronderstellen bescherming van de vertrouwelijkheid tussen LAS en client van de Nummervoorziening. Het Certificeringsschema stelt eisen aan de vertrouwelijkheid van de verwerking van het ECK ID die hier gelden. De Nummervoorziening zelf heeft op dit punt geen additionele eisen.
- Stap 3b: schrijft 1e niveau hashing van gevoelige persoonsgegevens (d.w.z. het PGN) voor volgens voorschrift 2, om deze minder direct herleidbaar te maken. Het certificeringsschema heeft op dit gebied nog geen eisen, maar zal de eisen uit de technische voorschriften van de Nummervoorziening overnemen.
- Stap 3c, 3e, 4b, 4d: Het certificeringsschema stelt hiervoor specifieke maatregelen voor die overeenkomen met de eisen voor Edukoppeling. Edukoppeling wordt niet vereist voor het certificeringsschema, wel door de Nummervoorziening. Het verkrijgen van een PKI Overheid certificaat, vereist voor Edukoppeling (voorschrift 3), is een zwaardere procedure dan het verkrijgen van een certificaat van een generieke CSP. TLS 1.2 (voorschrift 7) zal voor de Nummervoorziening geleidelijk worden ingevoerd, dit wordt opgenomen in een clausule in het implementatieplan, en is al onderdeel van certificeringsschema.
- Stap 6: Schrijft beveiligde opslag voor het stampseudoniem en het ECK ID in de lokale systemen voor conform *voorschrift 5*. Het certificeringsschema heeft op dit gebied nog geen eisen, maar zal de eisen uit de technische voorschriften van de Nummervoorziening overnemen.

Toelichting gemarkeerde stappen voor gebruik ECK ID:

- Stap 3 Ophalen ECK ID: als het hierbij gaat over transport buiten de beveiligde schoolomgeving, moet deze koppeling voldoen aan beveiligingseisen in Edukoppeling of equivalente eisen in het certificeringsschema.
- Stap 4 Federatieve authenticatie: zal voldoen aan de eisen rondom authenticatie en autorisatie uit het certificeringsschema.
- Stap 6 onderliggend voorschrift 8 is equivalent met eisen aan encryptie / PKI uit certificeringsschema
- Stap 7 onderliggend voorschrift 7 is equivalent met eisen aan encryptie / PKI uit certificeringsschema
- Stap 8 en 9 hashing (voorschrift 6) of encryptie (voorschrift 5) is niet beschreven in het certificeringsschema, maar waar van toepassing zullen de eisen uit de technische voorschriften van de Nummervoorziening worden overgenomen.

2.2. Autorisatie en toegang tot de Nummervoorziening

De Nummervoorziening voert twee onafhankelijke tests uit om binnenkomende verzoeken te autoriseren:

1. Een check of het bevoegd gezag van de bevragende school akkoord is met de gebruiksvoorwaarden van de Nummervoorziening

2. Een check of de leverancier van het bevragende systeem gekwalificeerd is om de Nummervoorziening te bevragen.

Als beide checks positief worden beantwoord, is het binnenkomende verzoek geautoriseerd en wordt het verder verwerkt. Indien dit niet het geval is, retourneert de Nummervoorziening een specifieke foutmelding. Op basis van deze foutmelding kan de aanvragende instelling of zijn vertegenwoordiging met Kennisnet contact opnemen om na te gaan waarom het verzoek niet geautoriseerd kon worden en indien mogelijk, dit te verhelpen.

Voor check 1 houdt de Nummervoorziening zelf een administratie bij van bevoegde gezagen en daaraan gekoppelde scholen. Deze administratie wordt up to date gehouden op basis van synchronisaties met de open data van DUO. Kennisnet administreert hierbij of een bevoegd gezag akkoord is gegaan met de gebruiksvoorwaarden van de Nummervoorziening. De Nummervoorziening identificeert de bevragende school aan de hand van het OIN in de wsa:from header (*voorschrift 3*) in het binnenkomende request.

Voor check 2 houdt de Nummervoorziening een administratie van gekwalificeerde LAS systemen bij. De kwalificatieprocedure zal worden beschreven in 4.5. Kennisnet houdt bij of een systeem gekwalificeerd is voor koppeling aan de Nummervoorziening. De Nummervoorziening identificeert het bevragende systeem aan de hand van het OIN nummer dat onderdeel is van het Subject (Onderwerp) veld is in het certificaat dat het systeem gebruikt on de TLS verbinding (*voorschrift 7*) mee op te zetten.

3. Ondersteunende processen

Om een en ander in ketenbreed te ondersteunen zijn in elk geval onderstaande processen van belang.

3.1. Tegengaan van oneigenlijk gebruik van het systeem

1. *Overbelasten van het systeem met http- en andere requests vanuit verschillende bronnen* (DDOS). De beschikbaarheid voor legitieme gebruikers kan hierdoor worden beperkt.

   Tegengaan of verminderen van de effecten van deze acties vinden plaats buiten het systeem van de Nummervoorziening zelf, in netwerk- en infrastructuur tooling.

   - De verantwoordelijkheid voor het tegengaan van DDOS aanvallen en het beschikbaar houden van de dienst is belegd bij exploitatie en beheer van de Nummervoorziening.

2. *Nagaan of de server wordt aangeroepen door gekwalificeerde leerlingadministratie systemen*.

De Nummervoorziening hanteert aansluitvoorwaarden voor leveranciers, die gecontroleerd worden in een test-situatie.

- Implementatiebegeleiding of servicedesk gebruiken de beheerapplicatie NV om het OIN van leveranciers die zich kwalificeren in te voeren in een tabel van de Nummervoorziening. Deze tabel wordt gebruikt als whitelist in de autorisatie van het systeem.

- Het OIN komt ook voor in het Onderwerp (Subject) veld van het PKIoverheid Services server certificaat dat gebruikt wordt in het kader van EduKoppeling voor de SSL verbinding[4]. De Nummervoorziening gebruikt dit veld voor de verificatie tegen de tabel.

3. *Nagaan of de server wordt aangeroepen door scholen met overeenkomst*.

Besturen van onderwijsinstellingen en Kennisnet gaan een overeenkomst aan, en als gevolg van deze overeenkomst kunnen alle scholen onder dat bestuur gebruik maken van de Nummervoorziening.

Implementatiebegeleiding of servicedesk gebruiken de beheerapplicatie van de Nummervoorziening voor het onderhoud van een tabel waarin alle deelnemende instellingen in zijn opgenomen.

- Het systeem destilleert uit het OIN veld in de WS-Addressing header van het bericht de BRIN (4) van de school. Het systeem onderhoudt een lijst met BRINs en bijbehorende bevoegd gezagen[5], en bij elk bevoegd gezag een aanduiding of alle onderliggende scholen onder een bestuur toegang moet worden verleend of niet. In aanvulling op de beschrijving van de logging in het PvE wordt ook het BRIN (4) en het bevoegd gezag nummer vastgelegd bij elk request.

4. *Nagaan of de aanroepende partij niet een vertaaltabel aanlegt.*

De Nummervoorziening houdt bij of de aanvragen die een leerlingadministratie doet vallen onder “normaal gebruik”. Er worden limieten gehanteerd op de batch opvragingen om tegen te gaan dat er vertaaltabellen kunnen worden opgebouwd. De limieten zijn als volgt:

- Er mogen maximaal 20.000 entries in een batch request worden opgenomen
- Er mogen maximaal 3 batch requests per 24 uur worden opgevoerd
- Er mag maximaal 1 keer per 15 minuten de resultaten van batch requests worden opgevraagd

De servicedesk heeft in de beheerapplicatie zicht op de limieten die een school overtreedt, en kan evt beperkingen opheffen.

[4] Zie https://www.logius.nl/fileadmin/logius/product/digikoppeling/algemeen/Gebruik_en_Achtergrond_Digikoppeling_Certificaten_v1.2.1.pdf. De configuratie van de web server van de Nummervoorziening zorgt dat het veld SerialNumber beschikbaar is als http header veld.

[5] Hiervoor wordt gebruik gemaakt van de onderwijsdata bestanden van DUO, https://duo.nl/open_onderwijsdata/databestanden/

3.2. Test- en accreditatieproces

De Nummervoorziening is beschikbaar voor ketenpartijen in deze omgevingen:

- **Productieomgeving**: regulier gebruik voor geaccrediteerde aansluitende partijen. Voorzien van productie-certificaat.
- **Kwalificatieomgeving**: partijen die willen aansluiten, doorlopen een test-traject op deze omgeving. De versie van de software op deze omgeving is altijd identiek aan de productieomgeving. Voorzien van productie-certificaat. De ECK IDs van de kwalificatieomgeving wijken in versienummer af van valide ECK IDs.
- **Sandbox omgeving:** nieuwe versies van client applicaties kunnen testen tegen de sandbox omgeving. De versie van de software op deze omgeving is altijd identiek aan de productieomgeving. Is voorzien van een self-signed test-certificaat. De ECK IDs van de sandbox omgeving wijken in versienummer af van valide ECK IDs.

Het kwalificatieproces voor leveranciers omvat twee elementen:

1. Een test met een standaard set requests naar de Nummervoorziening. Deze test dekt de services van de Nummervoorziening, en gaat na of de LAS op de services op de juiste wijze aanroept (Edukoppeling, 1e niveau hashing) en correct reageert op foutmeldingen
2. Een inspectie van de met (A) gemarkeerde maatregelen uit hoofdstuk 2 van dit document in de implementatie van de ketenpartij, voor zover niet gedekt door de test hierboven.

4. Principes

Onderstaande principes zijn gebaseerd op

- [A] Doorbraakproject Onderwijs & ICT Eindrapportage roadmap fase II, oktober 2014
- [B] SION IAA Architectuur voor het onderwijs 2014-08-25 v0.5
- [C] Sectorale vraagsturing Leermiddelen Programma van Eisen PO/VO
- [D] ECK Distributie en toegang 2.0 – Principes (0.9)

4.1. IAA Stelsel in context

1. [B] Het onderwijsveld gebruikt voor identificatie, authenticatie één gemeenschappelijk IAA-stelsel.
2. [C] Dit stelsel sluit aan op sectorbrede en/of nationale identiteitsstelsels, zoals DigiD, eHerkenning en het op termijn te realiseren eID NL stelsel, om optimaal gebruik te maken van de door eID uitgegeven authenticatiemiddelen (zoals DigiD accounts en eHerkenning authenticatiemiddelen)
3. [B] Alle lokale informatiediensten worden ontsloten via het gemeenschappelijke IAA stelsel, want we streven naar verkleining van de digitale sleutelbos van de leerlingen, docenten en overige medewerkers

4.2. Diensten van de nummervoorziening

1. [A] Aanmaken Ketenpseudoniemen op basis van externe identiteiten voor ketens en ketenpartners
2. [A,B,C] Koppelen van externe identiteiten aan ketenpseudoniemen
3. [B] Diensten ter ondersteuning van de onderwijsprocessen
    a. (ondersteunen bij) registratie en verstrekken ketenpseudoniemen
    b. (ondersteunen bij) het wijzigen van ketenpseudoniemen als gevolg van het wijzigen van een externe identiteit, in de eigen systemen en in systemen van ketenpartners

4.3. Betrouwbaarheidsniveau van de registratie

1. [A,B] De nummervoorziening functioneert met de betrouwbaarheid van het IAA stelsel waarin hij gebruikt wordt.

4.4. Onderwijsidentiteit

1. [C,D] De nummervoorziening functioneert in aanvulling op en kan gebruikmaken van voorzieningen rondom het persoonsgebonden nummer (ofwel het Onderwijsnummer ofwel het BSN) zoals dat in de wet op het Onderwijsnummer is vastgelegd

4.5. Ketenpseudoniem

Een ketenpseudoniem is een identifier die uniek gekoppeld is aan een individu, dat gebruikt kan worden binnen een bepaalde reikwijdte. Deze reikwijdte kan begrensd zijn in tijd, handeling of tot bepaalde partijen.

1. [B] Een ketenpseudoniem wordt gebruikt als identiteit van een persoon in situaties waar het gebruik van de onderwijsidentiteit niet vereist of niet gewenst is
2. [A,B,D] Een ketenpseudoniem is specifiek voor een gebruikssituatie en een (groep van) ontvangende partijen

Voor gebruik in de Educatieve Content keten wordt een ketenpseudoniem verondersteld dat het ECK ID genoemd wordt. Voor overwegingen ten aanzien van de reikwijdte van het ECK ID, zie “Reikwijdte ketenpseudoniem ten behoeve van toepassing in de leermiddelenketen”. Voor het ECK ID geldt:

3. [D] Een ketenpseudoniem wordt geaccepteerd als voldoende identificatie voor deelname voor alle deelnemende partijen in de reikwijdte van de keten. Een leerling of docent hoeft geen additionele gegevens op te geven om gebruik te kunnen maken van de leermiddelenketen.

4.6. Registratieproces

1. [A] Verstrekking van ketenpseudoniemen door de Nummervoorziening dient al vanaf de eerste registratie (aanmelding, voorinschrijving, voorlopige inschrijving, inschrijving) van een leerling plaats te vinden, of zo spoedig mogelijk daarna[6]. Hierbij dient aandacht gegeven te worden aan het aanmaken en gebruik van een ketenpseudoniem vóórdat met de betrokkene (leerling/student/ouders/medewerker) de nodige (juridische) afspraken zijn gemaakt.

4.7. Doelgroep

1. [B] De Nummervoorziening werkt voor alle onderwijsvolgers en hun wettelijke vertegenwoordigers, onderwijsgevers en ondersteuners in het Nederlandse onderwijs
2. [B] Hierboven bedoelde Onderwijsvolgers en hun vertegenwoordigers kunnen ook leerlingen zonder registratie in de Nederlandse basisregisters zijn
3. [B] Andere natuurlijke personen zoals ouders en medewerkers die een rol vervullen in het onderwijsveld, worden eveneens aangeduid met een (persistent) sectoraal nummer

4.8. Wettelijk kader

1. [C,D] De Wet bescherming persoonsgegevens is bepalend voor inrichtingskeuzes, nader ingevuld door de vuistregels en uitgangspunten van het CBP.
2. [C] De Wet op het onderwijsnummer (Wijzigingswet van enkele onderwijswetten in verband met de invoering van persoonsgebonden nummers in het onderwijs) en sectorale onderwijswetten bepalen de verwerking en het gebruik van het persoonsgebonden nummer (PGN).

4.9. Privacy-gerelateerde maatregelen

Privacy wordt beschermd door

1. [B,C,D] Minimalisatie van uitgewisselde gegevens
2. [B,C] Uitgewisselde gegevens zijn beperkt koppelbaar (vanwege specifieke identifiers)
3. [C] Gebruik van gegevens koppelen aan doelbinding (scope)
4. [C] Bij het gebruik van de nummervoorziening wordt aangesloten bij de afspraken zoals die binnen de sector zijn gemaakt en zijn vastgesteld zoals bijvoorbeeld in het privacy convenant.
5. Partijen die gebruik willen maken van de Nummervoorziening, sluiten een bewerkersovereenkomt af met de scholen waarmee ze willen koppelen, en laten zien dat ze kwalificeren voor een aansluiting op de Nummervoorziening[7].
6. [C] Onderwijsinstellingen informeren studenten/leerlingen en hun vertegenwoordigers over het gebruik van de Nummervoorziening. Ook voor uitoefening van de wettelijke rechten kunnen betrokkenen terecht bij scholen (recht op inzage, correctie, verwijdering, verzet).
7. [D] Deelnemers geven in vrijheid toestemming voor gebruik van de gegevens.

4.10. Proces Leermiddelenketen

1. [A] Een persistente unieke identifier (ketenpseudoniem) wordt gebruikt voor de identiteit van de gebruiker in de hele keten.
2. [D] Besteller, betaler en gebruiker kunnen verschillende personen of instanties (school) zijn.
3. [C] De gebruiksrechten van digitaal leermateriaal worden toegekend aan het ketenpseudoniem van de beoogde gebruiker.
4. [A] Het ketenpseudoniem is tijdig beschikbaar voor gebruik in het bestelproces, dat wil zeggen tijdens of zo spoedig mogelijk na de eerste aanmelding of voorinschrijving van een leerling

[6] Er zijn situaties waarbij een ketenpseudoniem niet online kan worden aangemaakt, zie “Use case ketenpseudoniem aanmaken, opslaan buiten aanmelding (UC1.2)”. Scholen zijn bekend met deze situaties want dit is nu ook al regulier onderdeel van het proces; normaal gesproken is binnen enkele dagen wel mogelijk.

[7] Onderdeel van het – nog in te richten – governance proces is een toets dat de partij op de juiste manier gegevens verwerkt.

4.11. Onderwijsomgeving

1. [C,D] Toegangsadressen van bestelde digitale leermaterialen zijn na een bestelling real-time beschikbaar in het schoolportaal voor de deelnemer (leerling, docent).
2. [C,D] De toegangsadressen zijn gepersonaliseerd voor de deelnemer
3. [C] De deelnemer krijgt bij gebruik van het toegangsadres vanuit het schoolportaal, single sign-on toegang tot het materiaal

4.12. Onderwijsproces

1. [C] Gegevens over de voortgang en prestaties van leerlingen worden alleen geïdentificeerd met het ketenpseudoniem in de omgeving waar deze gegevens ontstaan (d.w.z. de Educatieve Applicatie).
2. [C,D] Additionele persoonsgegevens kunnen worden gebruikt in de Educatieve Applicatie voor specifieke doelen (bijvoorbeeld personalisatie, verlenen van service). Verwerking van deze gegevens valt binnen de grenzen die aangegeven worden voor deze doelbinding.
3. [C] In het sectorale privacy convenant worden afspraken gemaakt over gebruik van de gepseudonimiseerde gegevens over de voortgang en prestaties van leerlingen door uitgevers van Educatieve Applicaties.
    a. Het convenant zal beschrijven hoe uitgevers van Educatieve Applicaties de gegevens over de voortgang en prestaties van leerlingen kunnen verwerken en communiceren met de school van de leerling, in bewerkte, onbewerkte of geaggregeerde vorm. Hierbij gebruikt de uitgever alleen het ketenpseudoniem om de leerling te identificeren.
    b. Het convenant zal de voorwaarden beschrijven die gelden als uitgevers van Educatieve Applicaties de gegevens over de voortgang en prestaties van leerlingen gebruiken voor productontwikkeling.