Kennisnet

ECK-ID Principes en processen

SchoolID services

Laat ict werken **voor het onderwijs**

Inhoud

Document informatie

Status

Auteur	Kennisnet, Marc Fleischeuers
Versie	1.0
Versiedatum	12-7-2016
Status	Definitief

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

Betrokken/geraadpleegd

Betrokken	Rol

Distributie en goedkeuring

Versie	Datum	Persoon	Goedgekeurd (indien van toepassing)

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**. 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 11.
- **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 12.
- **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 11.

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

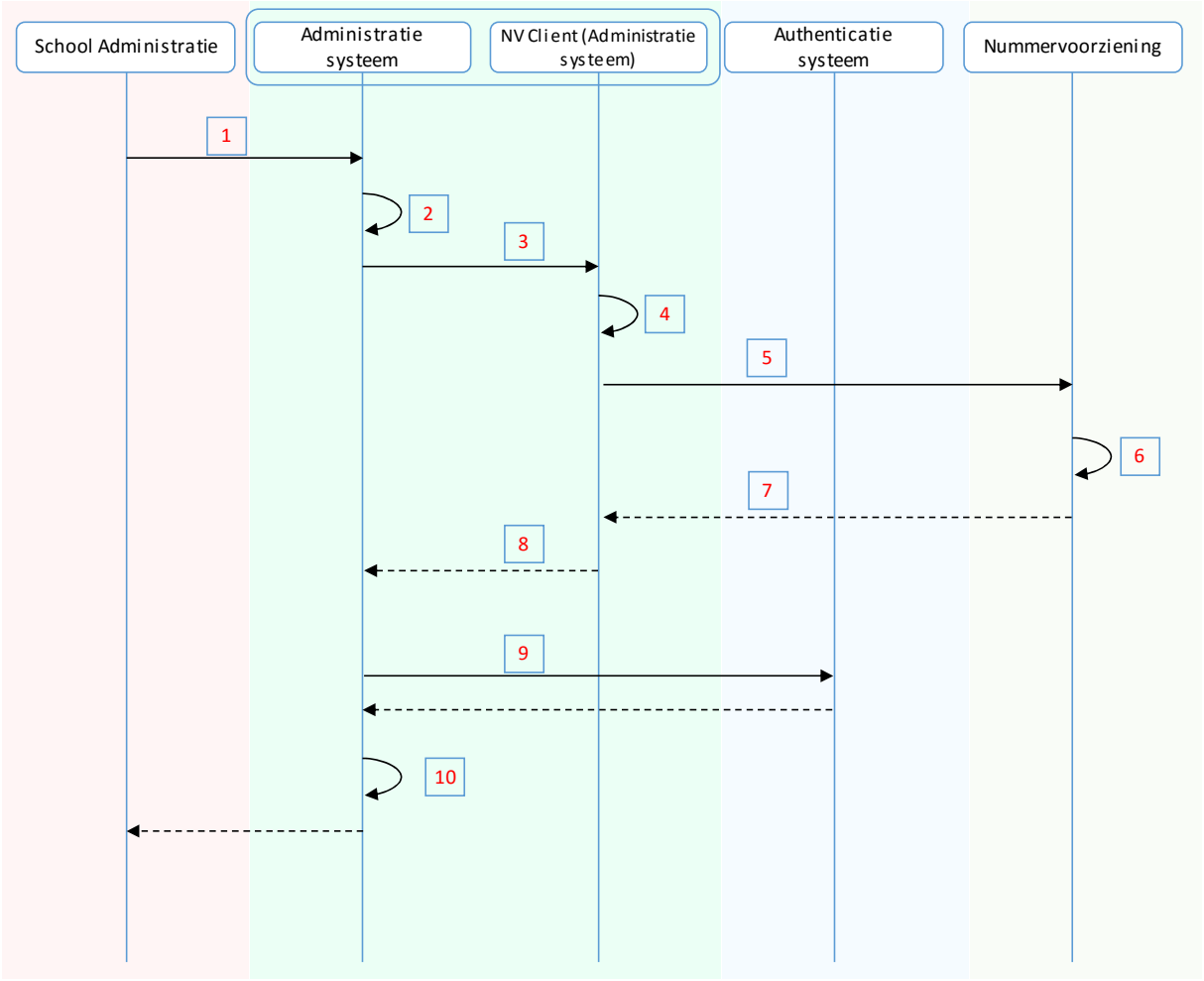
Dit hoofdstuk beschrijft de interactie tussen de betrokken systemen bij het tot stand laten komen van een ECK ID voor een leerling van VO of MBO (het proces voor PO leerlingen verloopt op punten wezenlijk anders, zie de use cases documentatie). Deze interactie vindt doorgaans plaats bij de *aanmelding* 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 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. De leerlingadministratie roept de functie voor het genereren van ECK ID aan in de Nummervoorziening client, en geeft hierbij op het PGN of de gekozen basis voor docenten (zie *Voorschrift 1* in Technische voorschriften), 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.

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

   Maatregelen: (A) Hashing wordt uitgevoerd volgens *voorschrift 2* en conform de referentie-implementatie.

5. De client roept de service van de Nummervoorziening aan met het gehashte PGN, ID van de gekozen sector en ID van de gekozen keten

   Maatregelen: (A) De koppeling maakt gebruik van EduKoppeling v1.2 volgens *voorschrift 3* en TLS volgens *voorschrift 7*.

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

   Maatregel: Maken van het ECK ID wordt uitgevoerd volgens *voorschrift 4*. De verwerking wordt gelogd.

7. De Nummervoorziening stelt een retourbericht samen dat het ECK ID bevat en stuurt dit terug als antwoord op 5.

   Maatregel: De koppeling maakt gebruik van EduKoppeling v1.2 volgens *voorschrift 3* en TLS volgens *voorschrift 7*.

8. De Nummervoorziening client haalt het ECK ID uit het retourbericht en retourneert dit aan de leerlingadministratie als antwoord op 3.

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

9. Als onderdeel van de aanmelding worden de leerlinggegevens inclusief het ECK ID gekoppeld aan een lokale identificatie.

   Maatregel: geen bijzondere maatregelen

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

    Maatregel: (A) Opslag van het ECK ID wordt uitgevoerd volgens *voorschrift 5*.

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, waarvan op dit moment een versie 2.0 wordt ontwikkeld (zie https://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema/2.0/). In principe zal bij invoering van het certificeringsschema, elke LAS leverancier (feitelijk, elke ketenpartij) een BIV classificatie uitvoeren voor het ECK ID en omliggende 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	5 Leerling is ingelogd	5 Opslag ECK ID administratie
6 Samenstelling ECK ID	6 Leerling klikt op link in ELO/Portaal	6 Opslag ECK ID ketenpartij
7 Terugsturen retourbericht	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 lokale 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 ECK ID

De indicatieve 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: geen, 2, 2 voor respectievelijk B, I en V.

Toelichting bij de gemarkeerde stappen voor aanmaken ECK ID:

- Stap 3, 8: deze stap veronderstelt 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 4: 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 5, 7: Het certificeringsschema stelt hiervoor specifieke maatregelen voor die overeenkomen met de eisen voor Edukoppeling, maar 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 10: Schrijft beveiligde opslag voor 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 zodra dit definitief is.
- 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 (voorschfit 6) of encryptie (voorschrift 5) is nog niet beschreven in het certificeringsschema, maar de eisen uit de technische voorschriften van de Nummervoorziening zullen 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.

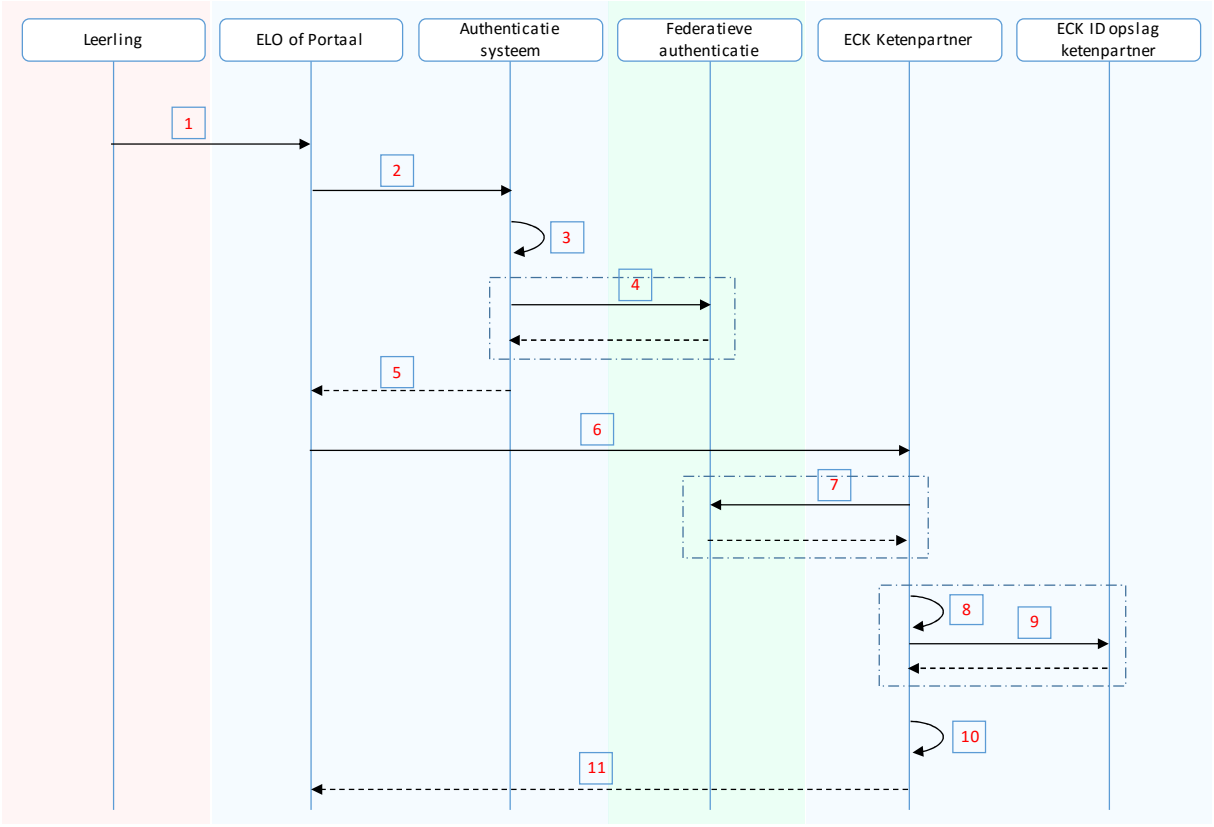
Voor check 2 houdt de Nummervoorziening een administratie van gekwalificeerde LAS systemen bij. De kwalificatieprocedure zal worden beschreven in 4.5. Kennisnet houdt bij of een systeem gekwalificeerd is voor koppeling aan de Nummervoorziening. De Nummervoorziening identificeert het bevragende systeem 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. Proces van gebruik van ECK IDs

Dit hoofdstuk beschrijft de interactie tussen de betrokken systemen bij het gebruik van een ECK ID voor een leerling. Deze interactie vindt plaats als leerlingen inloggen op hun leerlingportaal of ELO en toegang willen naar hun digitaal lesmateriaal, of lesmateriaal willen aanschaffen. Bij deze interacties is de Nummervoorziening niet betrokken.

In onderstaande beschrijving is verondersteld dat de ECK IDs van een instelling worden beheerd in een registratie onder de controle van de school, en dat het ECK ID beschikbaar is voor de ELO of portaal nadat de leerling zich succesvol heeft geauthenticeerd. In de praktijk kan een school de verantwoordelijkheden anders onderverdelen, en in dat geval kan dit voorbeeld worden gebruikt om de interacties voor die situaties specifiek uit te werken.

Dit is een voorbeeld van een *IDP-first* proces, en een dergelijk proces kan werken vanaf het moment dat de leerling beschikt over een account op school en de leerling op school kan inloggen en van daar uit naar de ketenpartner kan navigeren. Er zijn echter situaties waarin dit niet mogelijk is, en voor dergelijke gevallen kan een IDP-last route of een andere, specifieke, flow worden ontwikkeld.



Figuur 2 Sequentiediagram van een voorbeeld toepassing van het ECK ID tijdens gebruik

1. De leerling opent de ELO of het portaal van haar school.
2. De leerling logt in op het voor haar aangemaakte account in het authenticatiesysteem van de school[4].

   Maatregelen: Geen bijzondere maatregelen.
3. Als de het authenticatiesysteem niet al beschikt over het ECK ID, gaat het authenticatiesysteem het ECK ID voor de leerling ophalen. De identifier van het account van de leerling in het authenticatiesysteem

[4] We gaan hierbij uit van het IDP-first scenario

(dezelfde die is aangemaakt in stap 10 uit de flow in Figuur 1) kan worden gebruikt om het ECK ID te identificeren.

Maatregelen: Als de communicatie tussen portaal en ELO of portaal een systeem-systeem koppeling is waarbij de systemen beheerd worden door verschillende partijen, dan is de koppeling beveiligd met Edukoppeling 1.2 of vergelijkbare maatregelen volgens *voorschrift 3* en *voorschrift 7*.

4. Optionele stap: Het authenticatiesysteem start een sessie voor deze leerling bij een federatieve authenticatiedienst, als dit nodig is voor de communicatie met de systemen van de ketenpartijen. Het ECK ID is onderdeel van de set van attributen die de authenticatiedienst uitwisselt met de federatieve dienst.

   Maatregelen: De koppeling beveiligd volgens *voorschrift 7*.

5. De leerling is ingelogd, het ECK ID van de leerling is beschikbaar en er is een sessie bij een federatieve authenticatiedienst voor deze leerling.

   NB Stappen 3 en 4 zijn sterk afhankelijk van de inrichting bij de school zelf, en zijn in dit voorbeeld alleen maar bedoeld ter indicatie. De intentie is om uit te komen in de situatie zoals hierboven beschreven, d.w.z. ingelogd, met een bekend ECK ID en voor zover noodzakelijk voorzien van een actieve sessie in een federatie.

6. De leerling klikt op een link in de ELO of het portaal. In het request zijn een aantal attributen beschikbaar, onder andere het ECK ID, een minimale set persoonskenmerken waarmee de dienstaanbieder zijn dienst kan personaliseren, als er geen gebruik wordt gemaakt van de federatieve authenticatie. Als federatieve authenticatie wel gebruikt wordt bevat het request een kenmerk naar een sessie van het federatieve systeem.

   Maatregelen: De koppeling tussen browser van de leerling en systeem van de ketenpartij is beveiligd *voorschrift 8*.

7. De ketenpartij gaat de leerling in het request identificeren. Indien er een referentie naar een federatieve authenticatiedienst beschikbaar is, kan de ketenpartner de sessie van de leerling verifiëren. De federatieve authenticatiedienst levert extra persoonsgegevens op in het antwoord, tenminste het ECK ID.

   Maatregelen: De koppeling beveiligd volgens *voorschrift 7*.

8. Als de leerling al bekend is, heeft de ketenpartij het ECK ID gehasht of encrypted opgeslagen volgens *voorschrift 6* en gekoppeld aan een eigen interne identiteit. Om na te gaan of de leerling al bekend is, zal het systeem het ECK ID hashen of encrypten.

   Maatregelen: hashing of encryptie vindt plaats volgens *voorschrift 6*.

9. In deze stap kan de ketenpartij de noodzakelijke checks en transacties uitvoeren om de leerling toe te laten tot zijn diensten. Hieronder valt bijvoorbeeld het opzoeken van de interne identiteit van de leerling (dan wel het aanmaken van een nieuwe identiteit, indien de leerling nieuws is), validatie van de licentie enzovoort.

   Maatregelen: als het ECK ID van de leerling wordt opgeslagen in deze stap, dan gebeurt dat volgens *voorschrift 6*.

10. De leerling krijgt toegang tot de gevraagde dienst.

    Maatregelen: de koppeling is beveiligd volgens *voorschrift 8*.

4. Ondersteunende processen

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

4.1. Gebruikersondersteuning

1. *Ondersteunen servicedesk van ketenpartijen (school, boekhandel, uitgever).* Het komt voor dat servicedesks van ketenpartijen met elkaar moeten communiceren over individuele leerlingen. Omdat elke partij het ECK ID met eigen versleuteling opslaat, is het lastig om individuele gebruikers te correleren over organisaties heen[5]. Voor situaties waarin er een probleem is met de identiteit van een leerling, moet een andere weg worden gevonden om ten behoeve van gebruikersondersteuning toch een dergelijke correlatie te kunnen maken.

2. *Correleren van transacties over ketenpartijen (school, boekhandel, uitgever).* Het komt voor dat servicedesks van verschillende partijen met elkaar moeten communiceren over individuele activiteiten van een leerling. Er zijn technische oplossingen denkbaar om te ondersteunen in situaties waarin er een probleem geconstateerd wordt met individuele verzoeken van leerlingen. Dit zou bijvoorbeeld kunnen worden gefaciliteerd door bijvoorbeeld een transactieid te gebruiken.

4.2. Verlenen van toegang voor docenten

3. *Vaststellen van basis voor ECK ID van docenten*. Docenten zijn in het algemeen actief in de educatieve leermiddelenketen vanwege hun aanstelling bij een specifieke school[6]. De school beschikt over de licenties van materialen en toegang tot systemen voor onderwijs en -ondersteuning. De basis voor het ECK ID van een docent zal dan ook een kenmerk zijn dat specifiek is voor de school.

    - School maakt ECK IDs voor zijn docenten aan en levert hiervoor de gegevens. Zie *voorschrift* 1 voor mogelijke werkwijzen om de basis voor ECK IDs voor docenten samen te stellen. Vastleggen gebeurt in een systeem dat toegankelijk is voor de ELO of het portaal dat de docent gebruikt, zodat het ECK ID beschikbaar is als de docent toegang wenst tot de leermiddelenketen.

    - Het LAS systeem ondersteunt de school door de gewenste gegevens voor te stellen.

4. *Docent wil ECK ID voor meerdere scholen gebruiken.* Dit kan voorkomen als een docent eigen materiaal heeft gemaakt en dat op meerdere scholen wil gebruiken. Er zijn geen protocollen voor de overdracht van ECK IDs tussen leerlingadministraties, en het lijkt niet wenselijk om uitzonderingen voor het maken van de basis (zie hierboven) voor specifieke docenten te maken. Er zijn echter workarounds om toch de gewenste situaties te kunnen bereiken.

    - De docent kan in WikiWijs bijvoorbeeld een groep te maken, zichzelf onder meerdere ECK IDs toevoegen aan de groep en alle leden van de groep rechten geven op het materiaal.

5. *Docent wil meerdere ECK ID's binnen een school kunnen gebruiken.* Dit komt voor als een school beschikt over twee gescheiden organisatieonderdelen (bijvoorbeeld PO en VO), en een docent is in beide actief. Deze situatie kan het best worden ondersteund als de docent dan ook beschikt over twee onafhankelijke accounts op het systeem van de school.

    - School kan elk account koppelen aan een eigen ECK ID, gebaseerd op emailadressen die licht zijn aangepast om ze uniek te maken (bijvoorbeeld door er een volgnummer achter te plaatsen).

4.3. Onderhoud van het ECK ID

6. *Herroepen van foutief toegekend ECK ID.* Komt voor als een leerling onder een foutief PGN is aangemeld. Relatief zeldzaam, want ook aanmeldingen worden bij DUO gevalideerd tegen het BAP (Basisadministratie Personen, afslag van het BRP).

[5] Dit is een beveiligingsmaatregel die expliciet voor dit doel is ingebracht.

[6] Scholen kunnen hiërarchisch georganiseerd zijn onder een schoolbestuur. We gaan er hierbij van uit dat een docent dezelfde rechten en mogelijkheden heeft op alle scholen onder een bestuur.

- School herstelt dit door 1. De leerling met het juiste PGN aan te melden of in te schrijven; 2. (automatisch) het juiste ECK-ID op te halen bij de Nummervoorziening met service “ECK ID maken”. Als het foutieve ECK ID al gebruikt wordt in de keten heeft het de voorkeur om het ID gecoördineerd te vervangen.

- Ketenpartners voeren de wijziging door, zodat de leerling met zijn correcte identifier toegang heeft en nog kan beschikken over zijn materiaal

7. *Nieuw ECK ID tgv een gewijzigd PGN.* Komt voor als leerling wordt ingeschreven in het BRP en het eerdere Onderwijsnummer van de leerling vervalt, op dit moment betreft dit enkele duizenden leerlingen per jaar. De Nummervoorziening onthoudt voor deze situaties tijdelijk het oude gehashte PGN, en substitueert dit oude PGN als er een ECK ID voor het nieuwe PGN gevraagd wordt. Het gevolg is dat het ECK ID niet wijzigt, ook als het onderliggende PGN wel wijzigt. Tegelijkertijd blokkeert de Nummervoorziening aanvragen op basis van het oude PGN, dat immers niet meer gebruikt mag worden.

   - School geeft een wijziging aan door in service “Wijzigen ECK ID”, en geeft hierbij het oude en het nieuwe gehashte PGN op.

   - leerlingadministratie leveranciers maken gebruikers duidelijk in de interface dat deze beide situaties verschillen

   - Kennisnet maakt in communicatie naar gebruikers duidelijk wat verschillen zijn, en in welke situatie welke actie van toepassing is

   - Kennisnet servicedesk kan in logfiles nagaan of blokkering en substitutie zijn gebruikt in een bepaalde periode en kan evt entries in subsitutietabel (blacklist) verwijderen.

8. *Massale invoering van ECK IDs.* Komt voor bij initiële vulling van leerlingadministratie met ECK IDs, en wanneer school overstapt op nieuwe leerlingadministratie, tenminste voor situaties waarbij het ECK ID geen onderdeel is van de OSO gegevensset of van een handmatige gegevensmigratie (afhankelijk van wat de school gebruikt).

   - leerlingadministratie leverancier maakt functie om (selecties van) leerlingen in hun administratie te voorzien van ECK IDs. Vanwege de gebruikte 1e niveau hashing (scrypt, zie **Fout! Verwijzingsbron niet gevonden.**) is dit een operatie die enige tijd kan duren (plm 40 minuten voor 5000 leerlingen). Deze functie zal daarom waarschijnlijk in een achtergrondproces verlopen. De verwachting is dat LAS- en andere authenticatiesysteem leveranciers functionaliteit maken om groepen leerlingen en docenten te selecteren om te laten voorzien van ECK IDs.

   - School gebruikt deze functie bij invoering en migratie.

   - Kennisnet servicedesk kan nagaan welke fouten er hebben plaatsgevonden bij het genereren van IDs

   - Kennisnet servicedesk kan evt blokkeringen vanwege overschreden drempels ongedaan maken

4.4. Tegengaan van oneigenlijk gebruik van het systeem

9. *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.

10. *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[7]. De Nummervoorziening gebruikt dit veld voor de verificatie tegen de tabel.

11. *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[8], 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.

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

De Nummervoorziening houdt bij of de aanvragen die een leerlingadministratie doet vallen onder “normaal gebruik”. De criteria hiervoor zijn nog nader te bepalen, en zullen veelal neerkomen op bijhouden van aantallen requests binnen een tijdseenheid (denk aan: niet meer dan 5 requests in een uur; max 5000 gehashte PGNs in een lijst; max 20 per etmaal).

- Product owner: stel limieten vast: requests per uur, requests per etmaal, items in een request.
- Ontwerper: maak configuratie om deze limieten naderhand te kunnen bijstellen.
- De servicedesk heeft in de beheerapplicatie zicht op de limieten die een school overtreedt, en kan evt beperkingen opheffen.

4.5. 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.

[7] 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.

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

5. 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)

5.1. 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

5.2. 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

5.3. Betrouwbaarheidsniveau van de registratie

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

5.4. 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

5.5. 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.

5.6. 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[9]. 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.

5.7. 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

5.8. 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).

5.9. 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[10].
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.

5.10. 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

[9] Er zijn situaties waarbij een ketenpseudoniem niet online kan worden aangemaakt, zie "**Fout! Verwijzingsbron niet gevonden.**". 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.

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

5.11. 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

5.12. 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.