Gebruik van polymorfe pseudoniemen in het onderwijs

Privacy vriendelijke leerling authenticatie bij distributeurs en uitgevers

Eric Verheul

6 November 2015

Eric.Verheul@[cs.ru.nl, keycontrols.nl]

Agenda (verhaal lijn)

Onderdeel	Kernboodschap/-inhoud
1. Inleiding	• Wie ik ben • Architectuur digitale leeromgevingen • Het belang van een landelijk leerling eID stelsel
2. Actuele risico's in leeromgevingen	• Demonstratie risico's in de leeromgeving van mijn dochter
3. Een eenvoudig landelijk leerling eID stelsel	• Een leerling eID stelsel uit de wandelgangen ('Ketenpseudoniemen') • Praktische risico's (koppeling) en privacy bezwaren
4. Een privacy vriendelijk leerling eID stelsel	• Polymorfe pseudonimisering • Privacy vriendelijk stelsel datzelfde *use-cases* ondersteunt
5. Simpele PET Uitbreidingen	• Centrale inzage dienst voor ouders/leerlingen gebruik gegevens • Privacy vriendelijke, centrale attributen diensten
6. Implementatie	• Demonstratie in Microsoft ADFS • Toepassing is praktisch mogelijk bij bestaande producten.

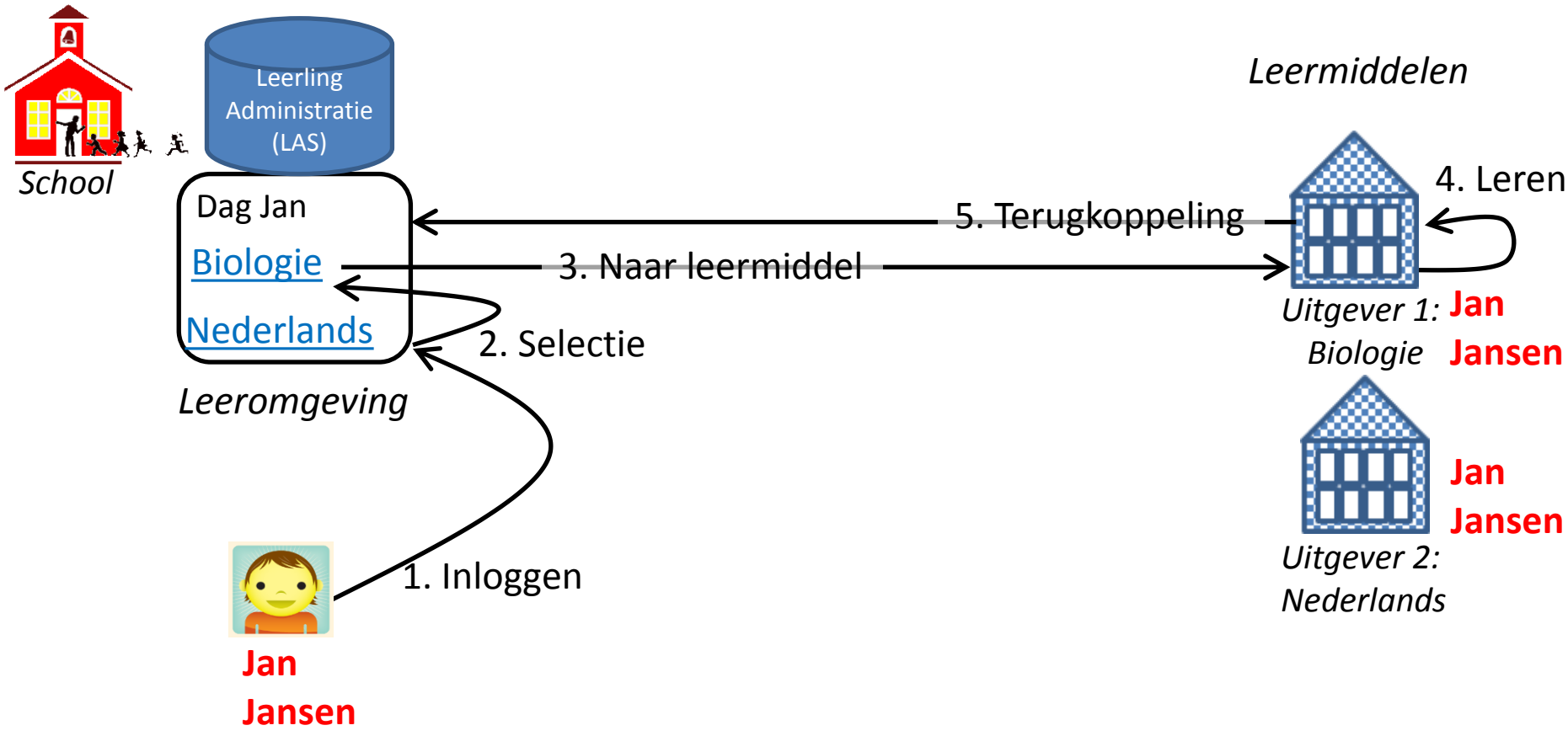
Inleiding: wie ben ik

- Hoogleraar digital security group Radboud Universiteit
- Onafhankelijk adviseur/auditor op het terrein van informatiebeveiliging
- Aandachtpunten zijn security management, cryptografie en *privacy enhancing technologies*
- Ouder van twee kinderen in het middelbaar onderwijs.

Inleiding: context

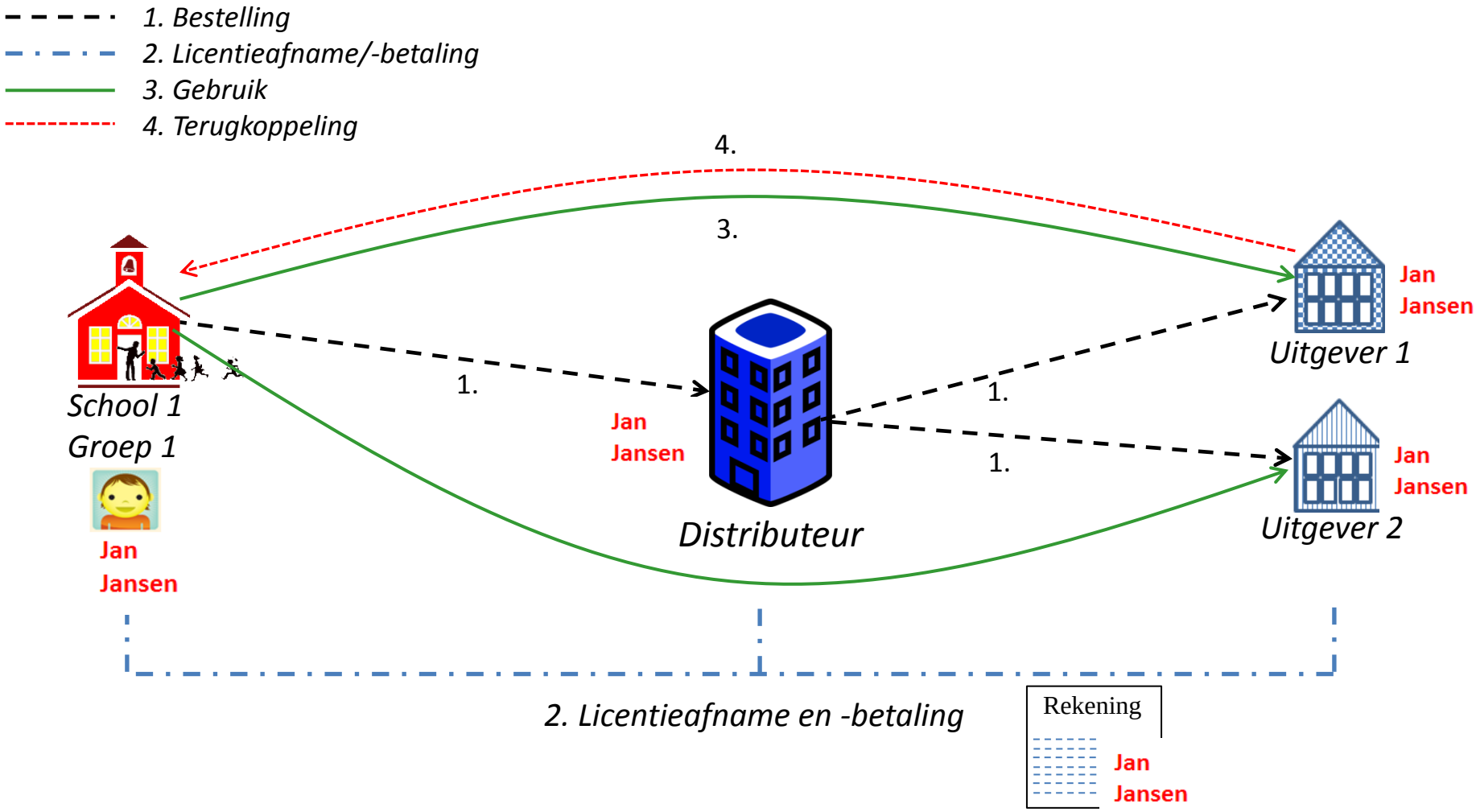
- Toenemend gebruik elektronische leermiddelen in onderwijs.
- Stelsel noodzakelijk tussen scholen en private partijen zoals distributeurs en uitgevers.

Inleiding: context



Herkenning van de leerling bij de verschillende partijen is essentieel.

Basis *Use Cases* gebruik elektronische leermiddelen



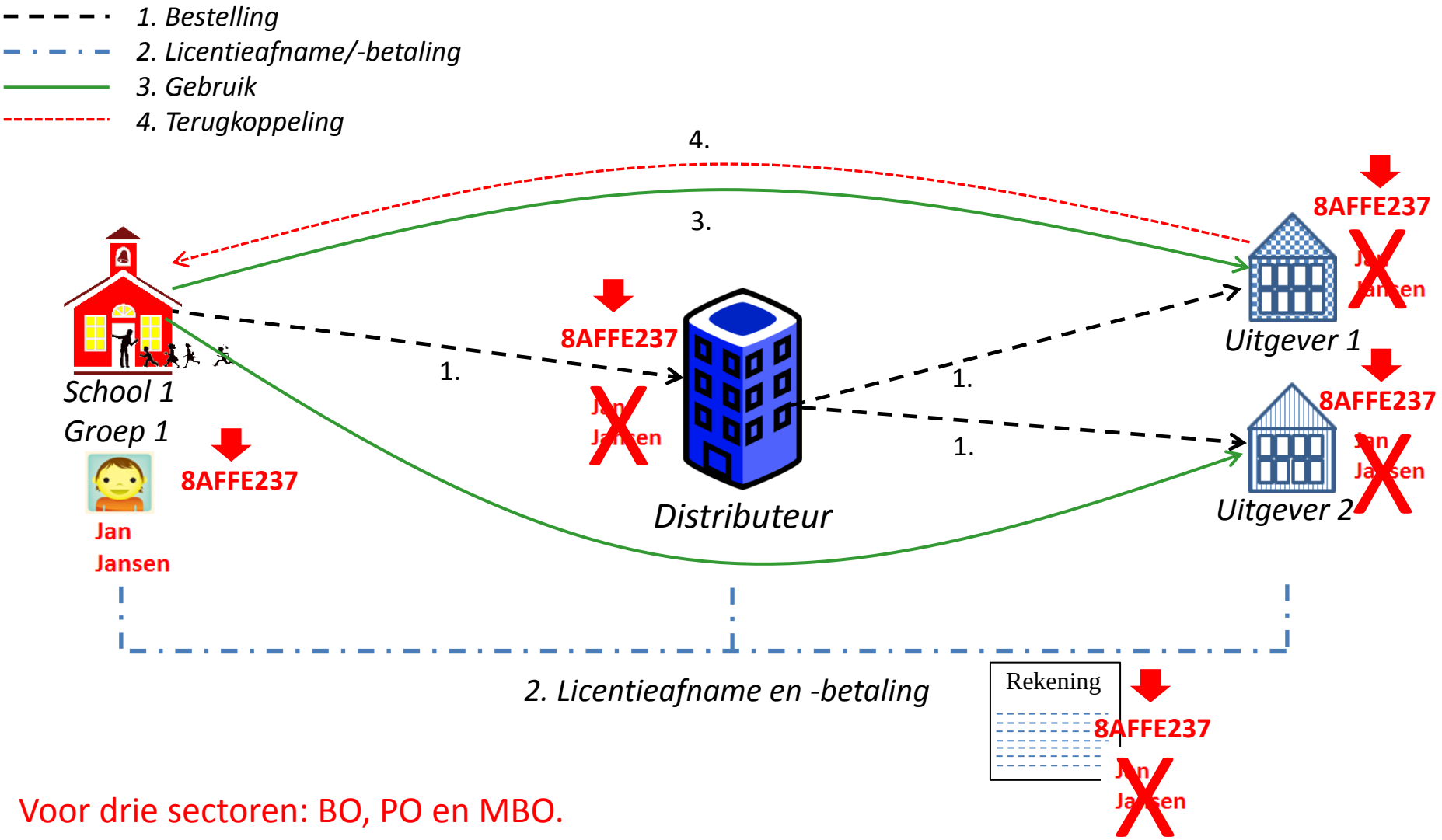
Actuele risico’s in leeromgevingen

Een eenvoudig landelijk leerling eID stelsel

- Op https://www.edustandaard.nl/fileadmin/edustandaard/user_upload/KAT_Edustd_architectuurraad_20150114.pptx (*) staat een functioneel ontwerp voor een landelijk leerling eID stelsel.
- Dit functioneel ontwerp laat verschillende varianten toe, met verschillende privacy beschermende eigenschappen.
- In de volgende slides wordt een variant toegelicht die in de wandelgangen vaak wordt genoemd.
- Het ontwerp noemt een Persoonsgebonden Nummer (PGN). In de praktijk is dat meestal het Burgerservice nummer (BSN) van de leerling.

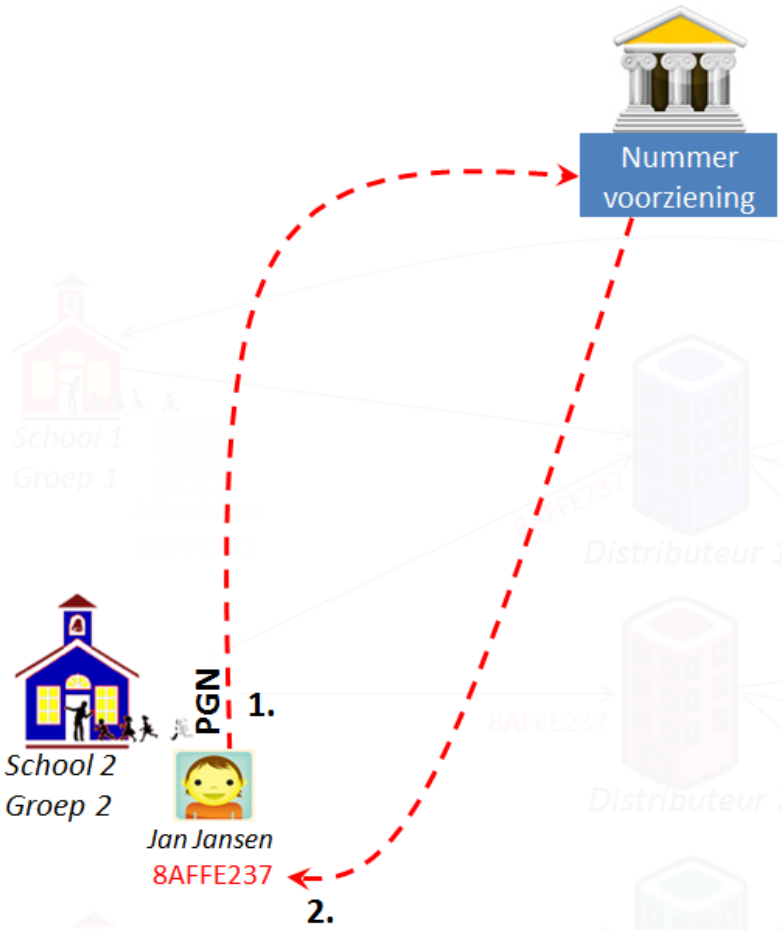
(*) Ook beschikbaar op http://slideplayer.nl/slide/2828232/.

Introductie van ketenpseudoniemen

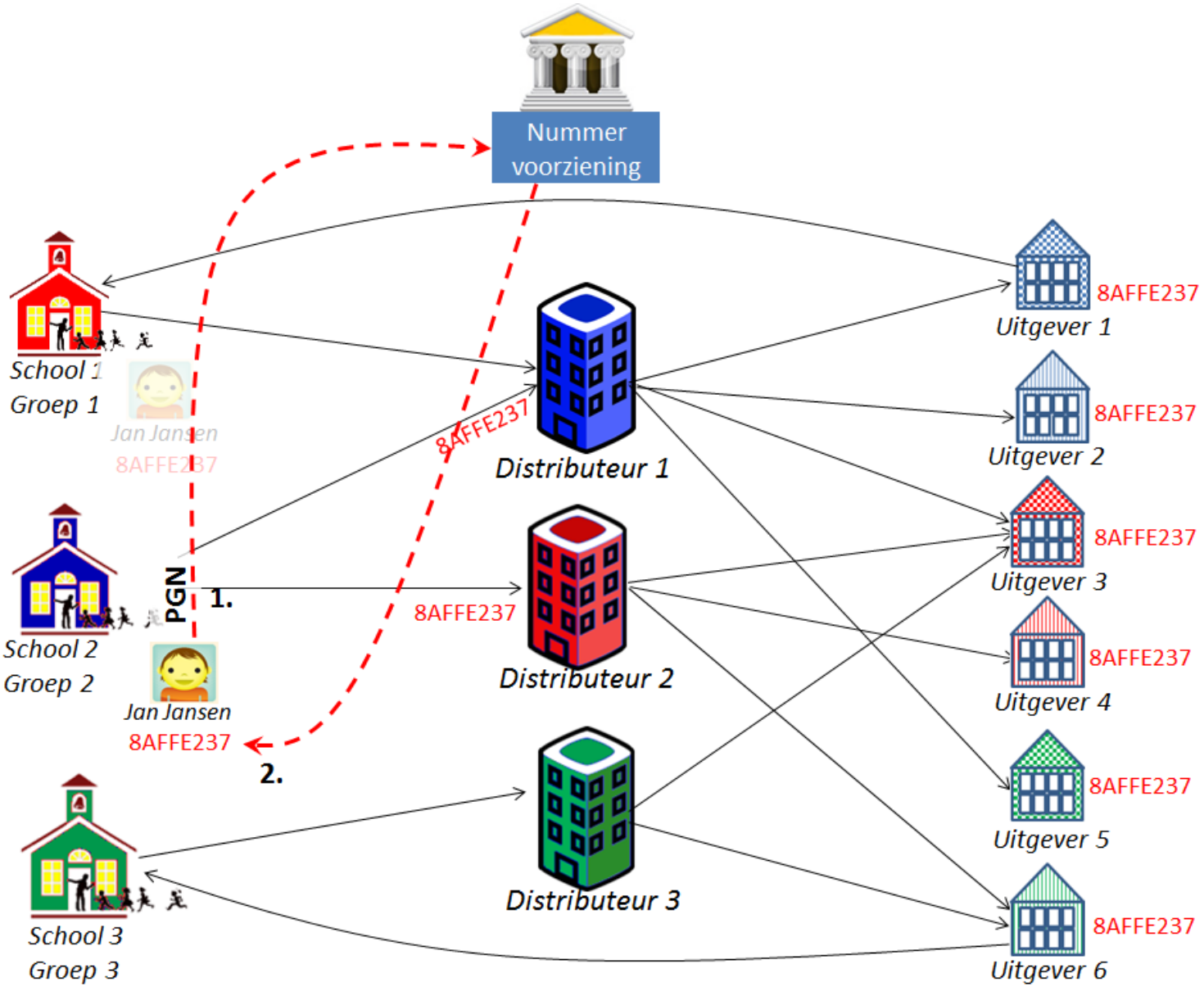


Voor drie sectoren: BO, PO en MBO.

Een eenvoudig landelijk leerling eID stelsel



Een eenvoudig landelijk leerling eID stelsel



Een eenvoudig landelijk leerling eID stelsel

Ketenpseudoniem:

- introduceert risico van koppeling tussen private partijen,
- verhoogt het risico als een private partij wordt gehackt,
- doet geen optimaal recht aan het data minimalisatie beginsel in privacy wetgeving: “persoonsgegevens moeten adequaat en ter zake dienend zijn en beperkt blijven tot datgene wat minimaal nodig is voor de doeleinden waarvoor zij worden verwerkt”.
- geen stand der beveiligingstechniek zoals genoemd in Wbp, art.13

Een ketenpseudoniem is een eufemisme voor drie nieuwe persoonsnummers in het basis, voorgezet en middelbaar beroepsonderwijs die zich ook uitstrekken naar private partijen.

Beschrijving leerling eID stelsel op basis polymorfe pseudoniemen

Beschrijving PP infrastructuur: voordelen

- Een leerling heeft bij elke partij een verschillend pseudoniem. Geen introductie van nieuwe koppelnummers
- Heeft zelfde functionele opzet als de ketenpseudoniem opzet, e.g. heeft ook een centrale Nummervoorziening. Dus al ontwikkelde uitwisseling mechanismen kunnen in stand blijven.
- Sterke privacy bescherming: zelfs de school kent het pseudoniem van zijn leerling bij de uitgever niet; de Nummervoorziening verwerkt alleen versleutelde data en 'ziet' alleen versleutelde PGNs.
- Polymorfe pseudoniemen kunnen ook zonder privacy bezwaar compatibiliteit tussen alle onderwijs sectoren realiseren, ook met het hogere onderwijs; dit maakt meer toepassingen mogelijk.
- Polymorfe pseudoniemen maken ook centrale inzagediensten en privacy vriendelijke attribuutdiensten mogelijk.

Introductie van de drie pseudonieme vormen

De drie essentiële pseudonieme vormen :

- **(Eind) Pseudoniemen bij partijen**

  Een leerling heeft bij elke partij een verschillend pseudoniem.

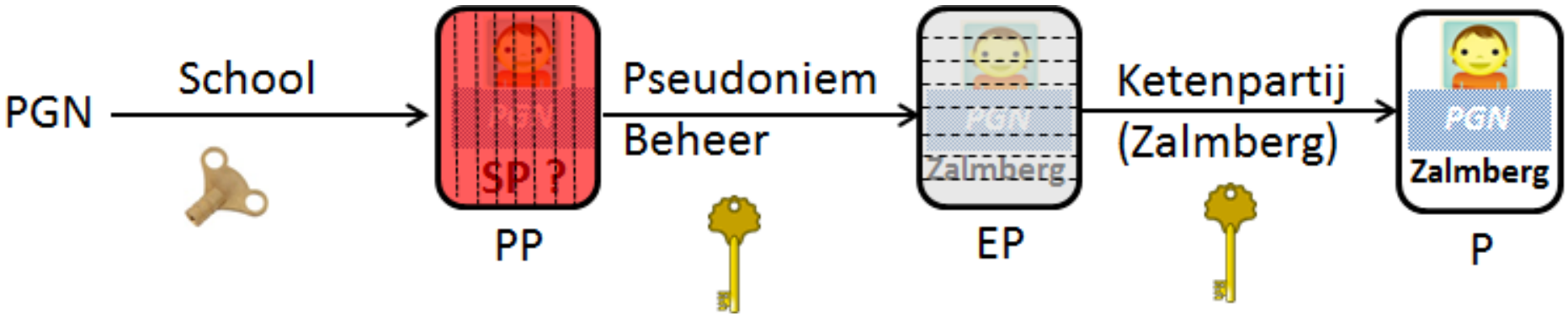
- **Encrypted pseudoniemen**

  Alleen leesbaar voor de bedoelde partij.

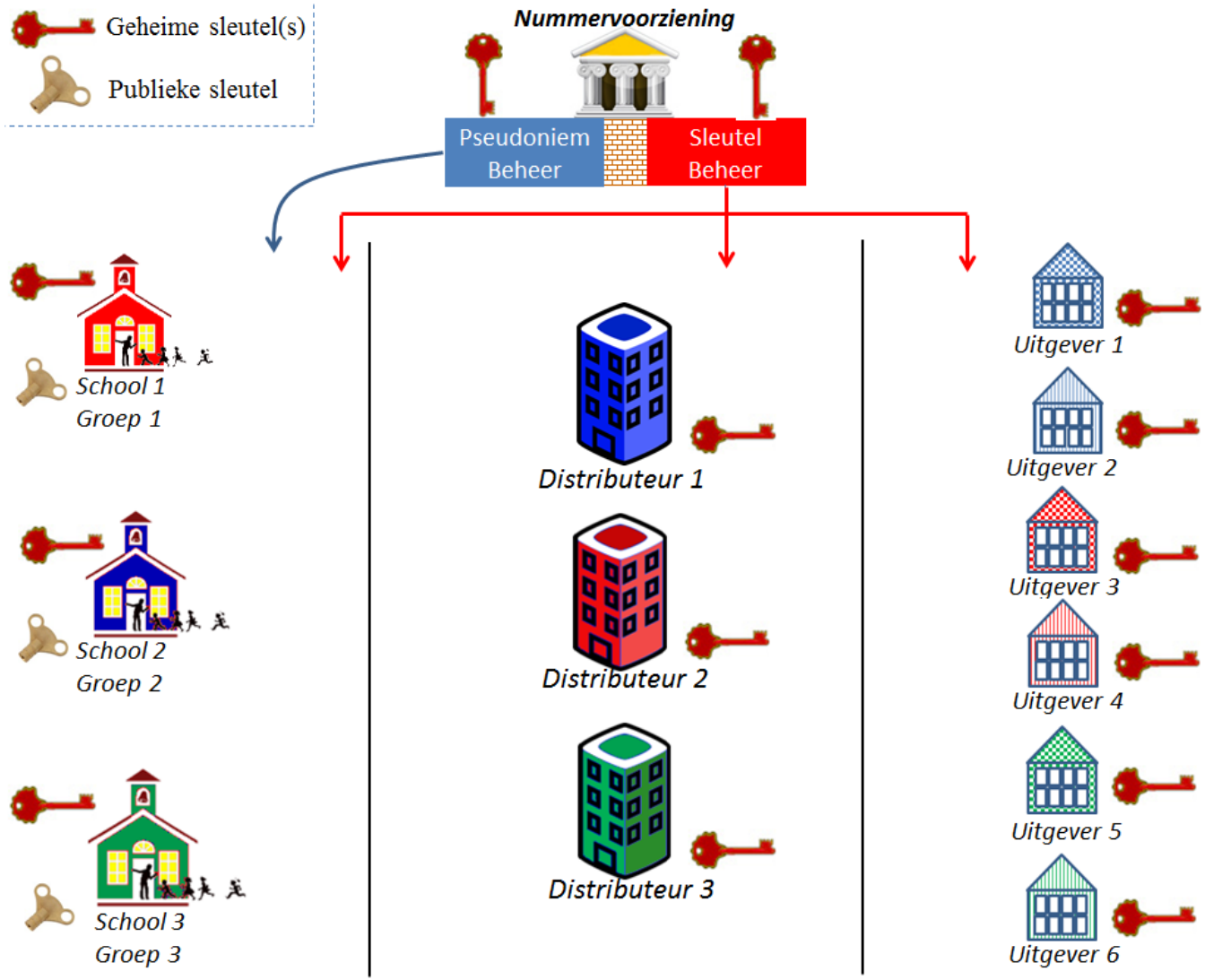
- **Polymorfe Pseudoniemen**

  Versleuteld PGN met een publieke sleutel waarvan niemand de private sleutel kent.

Gebaseerd op ElGamal, het oudste public key systeem.



Beschrijving PP infrastructuur: opzet

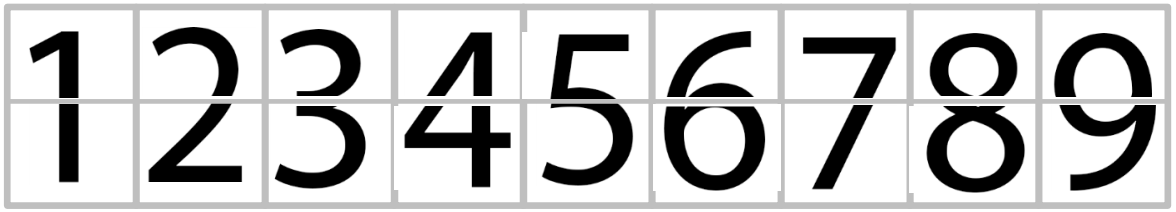


Polymorfe Pseudoniem metafoor

BSN van
Jan Jansen

123456789

BSN geknipt in
stukjes



Plaatsing stukjes
In `schudkluis' voor
de nummer-
voorziening

Polymorf Pseudoniem bij de school

Polymorf Pseudoniem → Encrypted Pseudoniem

Nummervoorziening past `schud instructies' toe voor specifieke partij X

Polymorf Pseudoniem bij de school

Encrypted pseudoniem voor ketenpartij

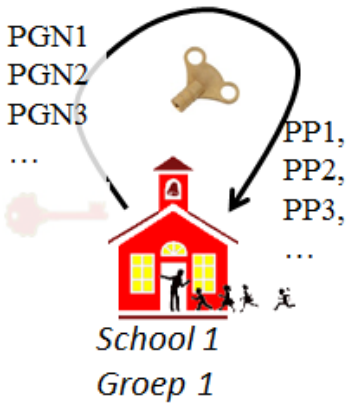
Beschrijving PP infrastructuur: ‘versie’ kopieën

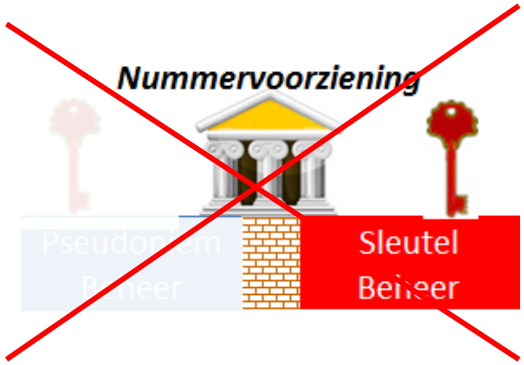
- De pseudoniemen vormen hebben de eigenschap dat ze her-randomiseerbaar zijn.
- Iedereen (m.n. een school) kan een ‘vers’ kopie maken van een PP en EP die weliswaar dezelfde data bevat maar toch niet relateerbaar is aan het origineel.
- Als een school bijvoorbeeld tweemaal een Encrypted Pseudoniem aanvraagt voor dezelfde leerling (m.b.v. ‘vers’ Passe Partout) dan kan de Nummervoorziening niet vaststellen dat het dezelfde leerling betrof.
- Als een school bijvoorbeeld tweemaal ‘vers’ Encrypted Pseudonym stuurt naar een partij van dezelfde leerling dan kan een tussenliggende partij (bijv. Distributeur) dat niet vaststellen.

Toepassing polymorfe pseudoniemen

Leerling registratie in de infrastructuur: PP generatie door school

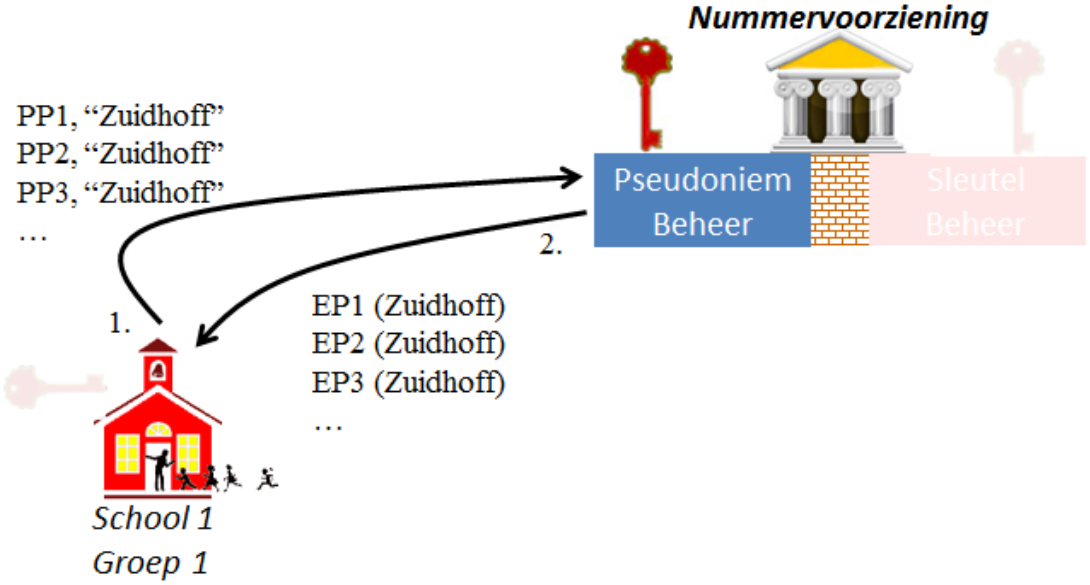
- School maakt Polymorfe Pseudoniemen aan voor de leerlingen die elektronische leermiddelen gebruiken.
- Dit is een publieke sleutel versleuteling PGN en kan zonder interactie met Nummervoorziening.
- Polymorfe Pseudoniemen worden opgeslagen in LAS.





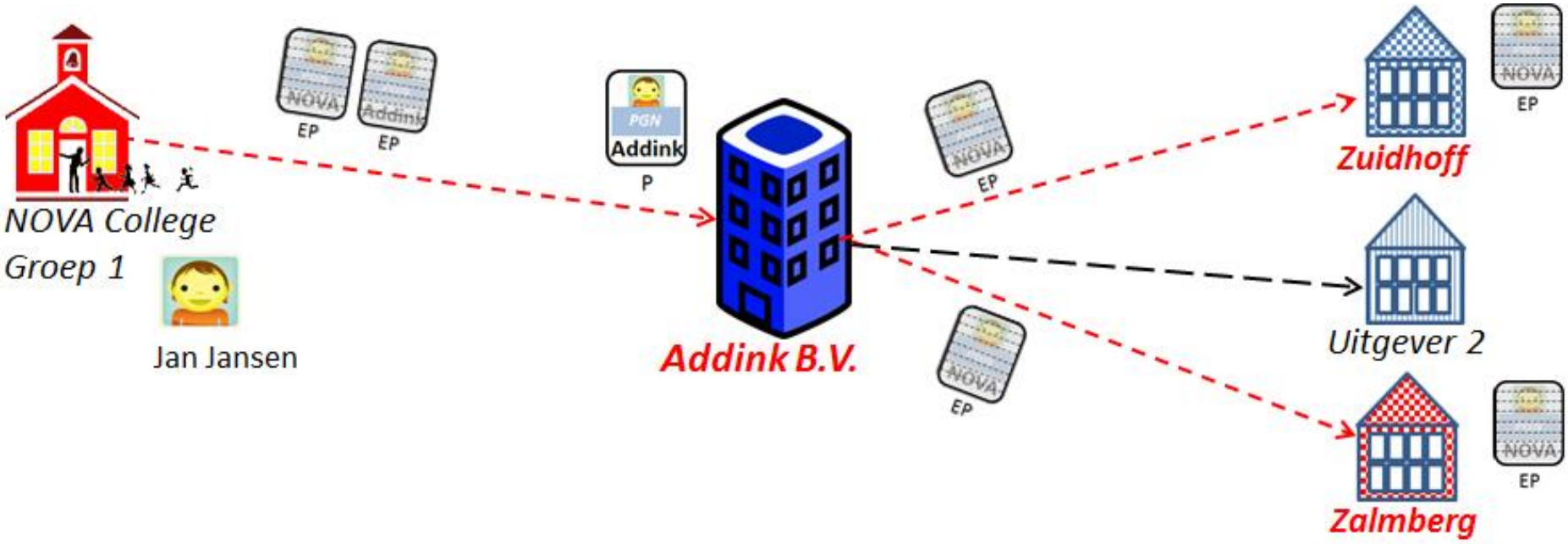
Generatie van Encrypted Pseudoniemen

- School bepaalt partijen (Distributeurs, Uitgevers) die leerlingen moeten kunnen herkennen. Dit gebeurt typisch begin schooljaar.
- School stuurt Polymorf Pseudoniem leerling en de naam van de partij naar de Nummervoorziening en krijgt Encrypted Pseudoniem terug. Nummervoorziening krijgt geen inzage in de identiteit van de leerling (of kan herhalingen constateren).
- Encrypted Pseudonyms worden opgeslagen in LAS (extra kolom).



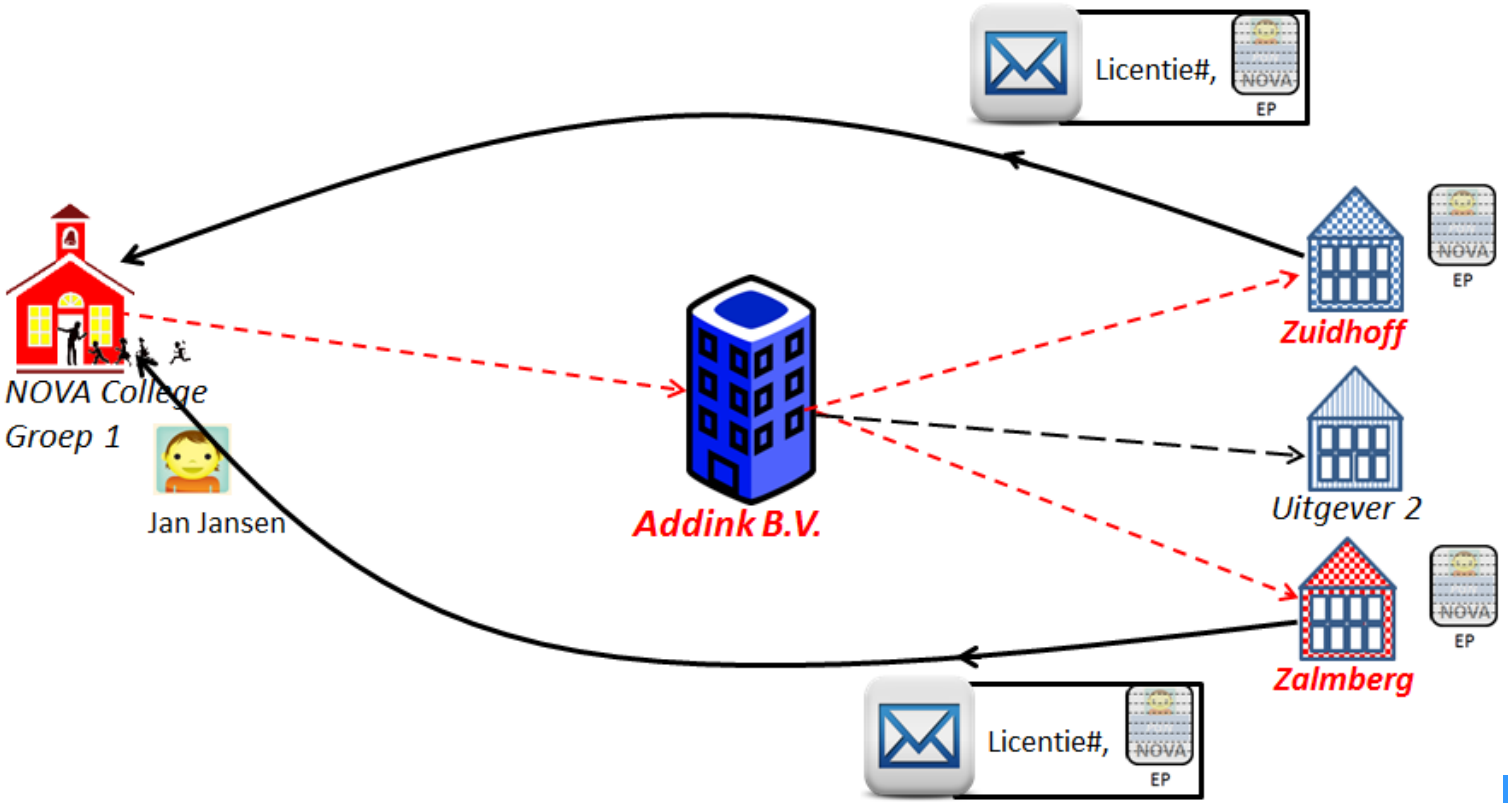
Bestelling van leermiddelen (voorbeeld)

- Leerling logt in bij Distributeur via LAS van school.
- Encrypted pseudoniemen van leerling bij School zelf en Distributeur worden meegestuurd.
- Distributeur ontsleutelt pseudoniem en kan leerling voortaan herkennen.
- Bij bestelling proces richting uitgever stuurt Distributeur Encrypted Pseudoniem van de leerling bij de school mee.



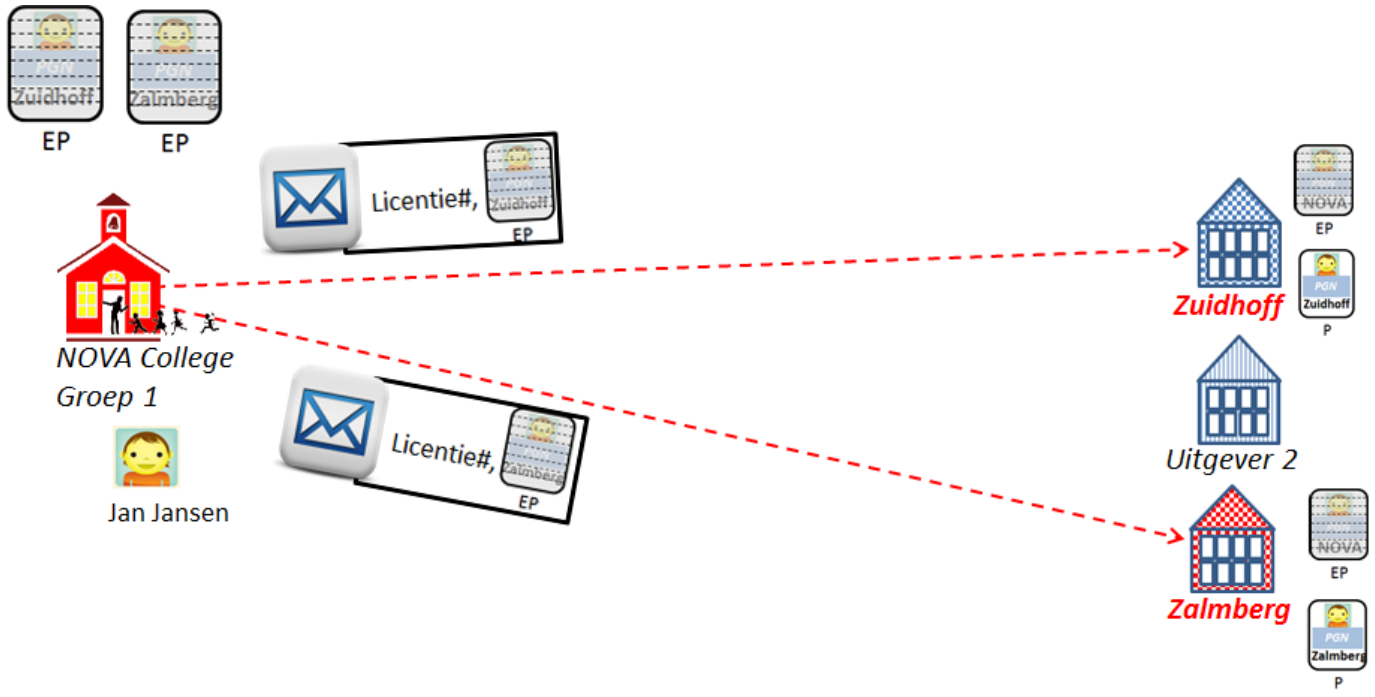
Licentieafname/activatie (voorbeeld)

- School krijgt bericht (bijvoorbeeld via email) van Uitgever/Distributeur met activatiecodes gekoppeld aan Encrypted Pseudoniem leerling bij school.
- School ontsleutelt pseudoniem en herkent leerling.
- School koppelt leerling aan activatiecode in LAS.



Leermiddel gebruik/terugkoppeling naar school (vb)

- Leerling logt in bij Uitgever via LAS van school.
- Activatiecode en Encrypted Pseudoniem van leerling bij Uitgever worden meegestuurd.
- Uitgever ontsleutelt pseudoniem en koppelt dit aan de Activatiecode. Voortaan kan uitgever leerling aan dit pseudoniem herkennen.
- Terugkoppeling testresultaten naar school via Encrypted Pseudoniem van school, vergelijkbaar met de versturing activatiecodes.



PET uitbreidingen met polymorfe opzet

- Centrale logging bij een ‘centrale inzagedienst’ m.b.v. diens encrypted pseudoniemen. Dit biedt leerlingen en hun ouders een inzage mogelijkheid: leerling/ouder logt aan via school.
- Attribuutdiensten zijn ook mogelijk binnen de opzet. De polymorfe techniek laat ook *polymorfe attributen* toe. Dit zijn versleutelde attributen bij de attribuutdienst die deze niet kan inzien maar wel kan omzetten naar encrypted attributen leesbaar voor de bedoelde partijen.
- Verstrekking van de attributen kan ook gelogged worden bij centrale inzagedienst.

Implementatie

- Implementatie van polymorfe opzet kan plaatsvinden door standaard SAML protocollen als transport laag te gebruiken (zoals TCP/IP dat voor HTTP is).
- Dat betekent dat bij standaard SAML implementatie de school (‘Identity Provider’) SAML pre-processing moet doen en de uitgever (‘Service Provider’) SAML post-processing.
- Hans Harmannij (RU) doet hieromtrent afstudeerwerk bij Surfnet. In enkele weken heeft hij een werkende implementatie gemaakt gebaseerd op:
  - Microsoft ADFS bij school als LAS
  - SimpleSAMLPHP en Shibboleth bij uitgever.

Conclusie