edustandaard

Verslag werkgroep Toegang

Aanwezig: Tine de Mik (Studielink), Brian Dommisse (Kennisnet, PO/VO-raad), Peter Clijsters (Surfmarket), Jan Over (SURF/HOSA), Jacob Hop (Aventus, saMBO-ICT/MBO Raad), Frits Bouma (DUO), Freek Nabuurs (Cito), Tom van Veen (Surfmarket), Bram Gaakeer (OCW, voorzitter), Erwin Reinhoud (Kennisnet, Bureau Edustandaard)

Afwezig: Dirk Linden (Kennisnet), Edwin Verwoerd (KBb-E), Rimmer Hylkema (Thiememeulenhoff, GEU)

Datum
18 februari 2021

Agenda

1. Opening en mededelingen
2. Vaststellen verslag vorig overleg en actiepunten
3. Data sharing harmonisation canvas v0.5 (toelichting Jan/Peter/Erwin)
4. Toelichting Federatief SSOn Rijk (toelichting Jan)
5. Casus achternaam Edu-K (toelichting Tonny Plas/ Edwin/Rimmer)

1. Opening

Het 5e agendapunt (Casus achternaam Edu-K) wordt een volgende keer door Edwin toegelicht.

Koppelen eID account voor step up naar eIDAS normenkader
Een dergelijk step-up (via eID/DigiD) lijkt niet mogelijk. Dit koppelen aan eID lijkt alleen toegestaan te worden tussen eID middelen (WDO).

Edustandaard werkgroep Toegang
Op de site van Edustandaard is de werkgroep toegang en architectuuraanpak toegang opgenomen (https://www.edustandaard.nl/standaard_afspraken/architectuuraanpak-toegang/).

Tine geeft aan dat dit de laatste keer is dat ze deelneemt aan het overleg. Er is helaas nog geen vervanger bij Studielink.

2. Vaststellen verslag en actiepunten

Het verslag van 12 januari wordt zonder wijzigingen vastgesteld

Actiepunten

#	Omschrijving	Status	Einddatum	Actie-houder
1	Doornemen Harmonisation canvas tbv discussie in werkgroepbijeenkomst van februari 2021	Afgerond	Feb 2021	Alle leden
2	Is de controle van de gegevens van een WID met de gegevens van een gezaghebbende bron onderdeel van betrouwbaarheidsniveau Laag of Substantieel?	Open		Dirk
3	Toelichten hoe toegang geregeld is bij o.a. ouders, stagebegeleiders en zorgmedewerkers	Loopt		Edwin (po/vo) Jacob (mbo) Peter/Jan (ho)

Actiepunt #3
Jacob heeft de onderstaande use cases voor het mbo aangeleverd.

- Als onderwijsinstelling wil ik ouder(s)/wettelijke vertegenwoordiger(s) van studenten toegang geven tot het KRD/SIS/LAS van de onderwijsinstelling.
    - de student is minderjarig (18-) en de ouder/wettelijke vertegenwoordiger krijgt na identificatie toegang tot gegevens van zoon/dochter
    - de student is meerderjarig en geeft ouder/wettelijke vertegenwoordiger recht op toegang
- Als onderwijsinstelling wil ik een praktijkopleider toegang geven tot het KRD/SIS/LAS van de onderwijsinstelling om de AAR gegevens en de voortgang van de student te kunnen volgen en gegevens/resultaten over BPV te kunnen vastleggen.
- Als onderwijsinstelling wil ik een assessor toegang geven tot het KRD/SIS/LAS van de onderwijsinstelling om examenwerk te kunnen beoordelen en de beoordeling te kunnen vastleggen.

Ouder/wettelijke vertegenwoordiger/praktijkopleider/assessor hebben geen arbeidsrelatie met de onderwijsinstelling en de identiteit wordt dus niet vanuit dienstverband vastgesteld. De relaties tussen deze actoren en de betreffende leerling/student in een betrouwbare digitale vorm die bij toegang gebruikt zou kunnen worden lijken er niet te zijn en dit is een belangrijk aandachtspunt.

Bij het bespreken hiervan wordt duidelijk dat de use cases ook in de andere sectoren spelen. Alleen de use cases waar de ouder/wettelijke vertegenwoordiger ook een rol spelen zijn niet relevant in het ho.

Er wordt besloten om deze toe te voegen aan de bestaande lijst met use cases. Deze lijst was echter onderdeel van het projectplan en we zitten ondertussen in een andere fase. Er wordt besloten om de use cases in een apart document op te nemen. Jacob zal nog aanvullende informatie leveren hoe toegang in het mbo bij deze use cases is ingericht.

3. Data sharing harmonisation canvas v0.5

We willen onderzoeken welke aspecten we uit het canvas kunnen gebruiken. Er is een nieuwe versie van het Data sharing harmonisation canvas[1] beschikbaar. Deze is op de googledrive geplaatst en Peter geeft hierover een toelichting.

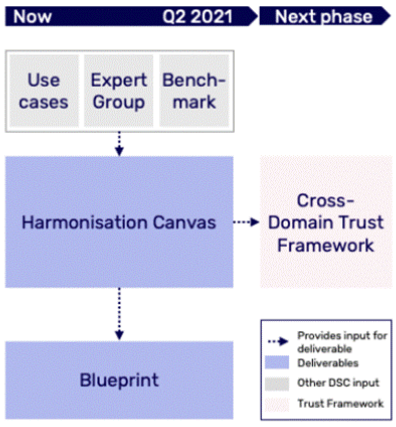


Figure 1: Relationship of the Harmonisation Canvas with other documents

Het document is een eerste aanzet om tot een trust framework te komen. Volgens de planning zou het in Q2 2021 afgerond zijn waarna in een volgende fase een concreet trust framework ingericht kan worden op basis van een BLOFT[2] model.

Het canvas is met name een samenvatting van aandachtspunten die relevant zijn om interoperabiliteit tussen verschillende domeinen te organiseren (cross domain data sharing).

[1] https://drive.google.com/file/d/1ZXAYqf_TS12nWZGhBzBmtWQIE_3taEf6/view?usp=sharing
[2] Business Legal Operational Functional Technical

Proxy's
Het belangrijkste doel van de Data Sharing Coalition[3] is het kunnen uitwisselen van gegevens over domeinen heen. Dit levert vaak interoperabilteitsproblemen op. Een belangrijke pilaar in de oplossing hiervan is de toepassing van een proxy per domein. Dit geeft de partijen in de verschillende domeinen de tijd om te harmoniseren. Na verloop van tijd krijgen de proxy's waarschijnlijk steeds minder functionaliteit. Zo zal op termijn bijvoorbeeld op semantisch vlak worden geharmoniseerd en is translatie tussen het interne en trust framework domein overbodig geworden. De proxy's zorgen er ook voor dat data services gevonden kunnen worden.

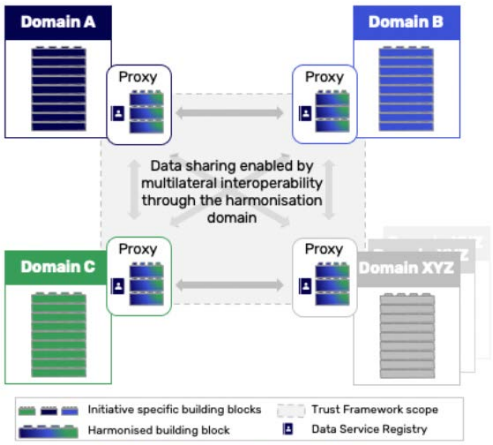


Figure 5: Visual representation Proxy Model

Het proxy model wordt vaak toegepast, ook binnen de onderwijssector. Zo zijn er bijvoorbeeld Entree Federatie en SURFconext die als een implementatie van het proxy model gezien kunnen worden. Ze koppelen het interne (IdP) domein aan het domein van de verschillende diensten (SP). Ook bestaat er een koppeling tussen Entree Federatie en SURFconext. Peter zal een volgende keer hierover wat meer vertellen (actiepunt #4)

Identificatie
Een ander vraagstuk dat in het canvas wordt genoemd is interoperabiliteit rond identifiers. In verschillende domeinen kan dezelfde identifier naar verschillende entiteiten verwijzen. Om tot een eenduidig begrip te komen wordt er voorgesteld om bij dergelijke interoperabiliteitsvraagstukken een (domein)prefix te gebruiken. Zo kunnen de proxy's deze vertalen van het eigen interne domein naar het geharmoniseerde domein van het trust framework en visa versa.

Betrouwbaarheidniveaus
Bij authenticatie speelt mogelijk een interoperabiliteitsvraagstuk rond betrouwbaarheidsniveaus (Level of Assurance). Hierbij wordt voorgesteld om aan te sluiten bij het normenkader van eIDAS. Dit normenkader is tot stand gekomen door te abstraheren naar 3 LoA's (Laag, Substantieel, Hoog) en hieronder in verschillende clusters (cluster policy) aan te geven wat de maatregelen per cluster zijn. Bij notificatie binnen het eIDAS stelsel wordt vervolgens vastgesteld hoe per nationaal eID invulling is gegeven aan de verschillende maatregelen.

Authenticatie
Binnen het trust framework moeten zowel systemen (M2M) als personen (H2M) geauthenticeerd worden. Voor authenticatie van systemen wordt er voorgesteld gebruik te maken van Qualified Website Authentication Certificates (QWAC) die eIDAS voorschrijft. Wat nog niet helemaal duidelijk is hoe (cross domain) authenticatie van natuurlijke personen geregeld wordt. Er wordt aangegeven dat er een vorm van doorsturen van ene naar andere domein mogelijk moet zijn, maar ze gaan nog verder uitwerken wat hier precies wenselijk is en bedoeld wordt.

[3] https://datasharingcoalition.eu/nl/

Autorisatie rollen

In het document worden ook autorisatie rollen beschreven (zie XACML[4]). Op basis van de autorisatie rollen kan aangegeven in hoeverre er mogelijk cross domain interoperabiliteitsproblemen ontstaan. Er zijn naar verwachting twee overheersende verdelingen van autorisatie rollen. Als de autorisatiebeslissing geheel wordt afgehandeld in het autoriserende domein dan worden geen interoperabiliteitsvraagstukken verwacht. Bij een externe PIP (policy information point) ontstaan waarschijnlijk wel interoperabiliteitsvraagstukken. Verder worden bij autorisatie flows twee varianten beschreven die waarschijnlijk nodig zullen zijn. Dit zijn de de Pull en Push variant (RFC 2904 https://tools.ietf.org/html/rfc2904)

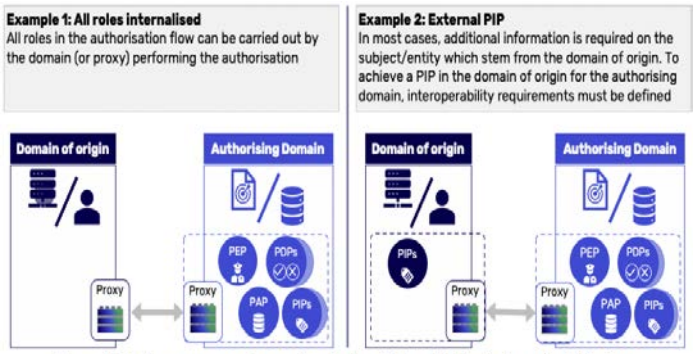


Figure 16: Most use cases can be captured in two different Authorisation role distributions

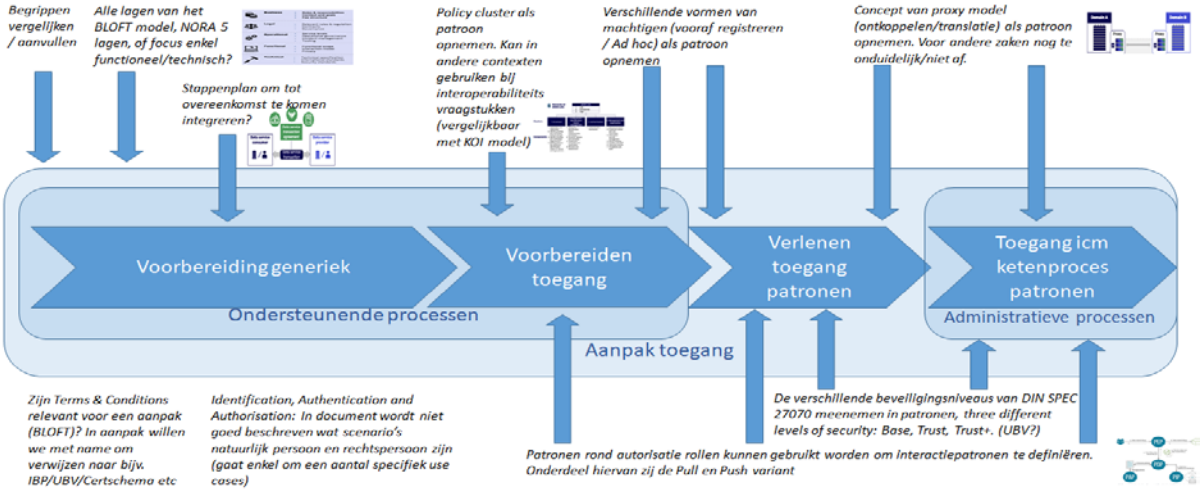
Roles	Responsibilities
PAP (Policy Administration Point)	The Policy Administration Point is where administrators, developers and business users can create and manage AUTHORISATION policies in order to be used by the PDP.
PEP (Policy Enforcement Point)	The Policy Enforcement Point is responsible for protecting the object by executing the access control decision. It intercepts API requests and forwards them on to the PDP.
PDP (Policy Decision Point)	The Policy Decision Point evaluates received AUTHORISATION requests against AUTHORISATION policies using extra information if needed. All decisions reached are returned to the PEP.

Delegated Authority

Het canvas beschrijft een tweetal varianten bij het overdragen van bevoegdheden aan een derde partij. Bij de eerste variant wordt de overdracht vooraf aan het afnemen van de data service geregistreerd en moet over verschillende domeinen gebruikt kunnen worden. De tweede wordt ad hoc overgedragen in het domein en context van de betreffende data service. Deze variant hoeft dus niet in een ander domein gebruikt te kunnen worden.

Conclusie

We hebben naar het canvas doorgenomen om te kijken wat we in onze aanpak kunnen gebruiken. Erwin stelt een aantal zaken voor die mogelijk relevant zijn (zie onderstaande overzicht). Na wat discussie wordt gesteld dat met name de autorisatie rollen en het proxy model relevant zijn. Een volgende keer zal er een voorstel besproken worden wat dit concreet betekent (actiepunt #5).

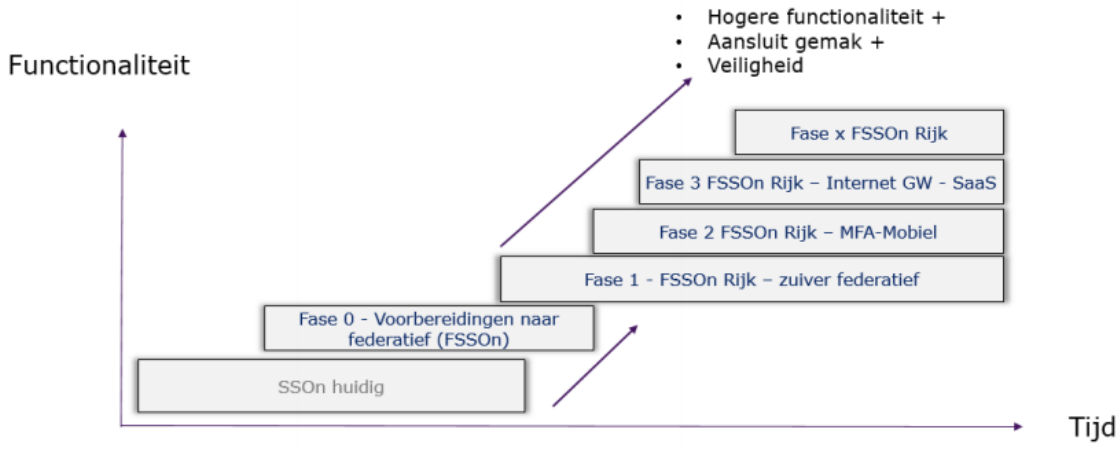


[4] Example Authorisation flow as defined in the XACML standards Source: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

4. Toelichting Federatief SSOn Rijk

Jan is al enige tijd betrokken bij de realisatie van Federatief SSOn Rijk en geeft hierover een toelichting. Sinds 2012 worden Rijksmedewerkers via SSOn Rijk geauthentiseerd en hebben via de voorziening met een enkele aanmelding toegang tot alle noodzakelijke diensten.

Ontwikkelingen zoals het gebruik van cloud-diensten en het gebruik van eigen devices door medewerkers vraagt om doorontwikkeling van SSOn Rijk. Om o.a. deze redenen is er met doorontwikkeling van SSOn Rijk gestart onder de naam Federatieve Single-Sign-On Rijk (FSSOn Rijk). De vernieuwing naar FSSOn zal in fases plaatsvinden.



Bij SSOn Rijk had een medewerker één identifier en één account. Met FSSOn Rijk kunnen medewerkers meerdere accounts hebben, maar hebben nog steeds één identifier.

Als onderdeel van FSSOn Rijk is er ook een eigen normenkader voor betrouwbaarheidsniveaus ontwikkeld. Dit normenkader is gebaseerd op het normenkader van NIST (NIST 800-63 standaard[5]). Onderdeel hiervan is ook een betrouwbaarheidsniveau dat is gekoppeld aan de federatieve hub (FAL[6]). Hierbij gaat het om betrouwbaarheid van de authenticatie en geleverde attributen.

We verwachten dat de verschillende aspecten van FSSOn Rijk de komende tijd nog besproken zullen worden. Zo is er o.a. een relatie met een uniform betrouwbaarheidsniveau voor de onderwijssector.

Rondvraag & afsluiting

Het volgende overleg is op 18 maart van 13:00 tot 15:00 uur.

Er wordt besloten om dit jaar maandelijks te overleggen. Hiervoor zal een datumprikker verstuurt worden.

5. Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder

[5] https://pages.nist.gov/800-63-3/
[6] Federation Assurance Level - the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP). https://pages.nist.gov/800-63-3/sp800-63c.html

2	Is de controle van de gegevens van een WID met de gegevens van een gezaghebbende bron onderdeel van betrouwbaarheidsniveau Laag of Substantieel?	Open		Dirk
3	Toelichten hoe toegang geregeld is bij o.a. ouders, stagebegeleiders en zorgmedewerkers	Loopt		Edwin (po/vo) Jacob (mbo) Peter/Jan (ho)
4	Toelichting koppeling tussen Entree Federatie en SURFconext	Open		Peter
5	Voorstel om aanpak uit te breiden met autorisatie rollen en het proxy model	Open		Erwin

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen