Verslag werkgroep Toegang

Aanwezig: Peter Clijsters (SURF), Tom van Veen (SURF), Freek Nabuurs (Cito), Rimmer Hylkema (Thiememeulenhoff, GEU), Bram Gaakeer (OCW, voorzitter), Erwin Reinhoud (Kennisnet, Bureau Edustandaard)

Afwezig: Dirk Linden (Kennisnet), Edwin Verwoerd (KBb-E), Brian Dommisse (Kennisnet, PO/VO-raad), Frits Bouma (DUO), Jan Over (SURF/HOSA), Paul de Wit (saMBO-ICT/MBO Raad)

Datum
24 juni 2021

Agenda

1. Opening en mededelingen
2. Vaststellen verslag vorig overleg en actiepunten
3. Doorontwikkelen ROSA scan architectuurkaders & beleidskaders

1. Opening en mededelingen

Mededeling: Wijzigingen identiteitskaart /paspoort[1]
De nieuw vormgegeven Nederlandse identiteitskaart bevat:

- een EU-vlag met de letters NL;
- een nieuw Kinegram;
- twee vingerafdrukken van de kaarthouder in de chip;
- **het burgerservicenummer (BSN) in een QR-code op de achterzijde van de kaart (het BSN wordt verwijderd uit de chip).**

Nu staat het BSN nog in de drie regels op de voorkant van het paspoort. Het is niet verboden om een kopie van een paspoort of identiteitskaart te maken, wel wordt aangeraden om het BSN weg te strepen met behulp van de app KopieID. Het is namelijk verboden voor ongeautoriseerde partijen om het BSN te verwerken. Om die reden is besloten het BSN naar de achterkant te verplaatsen. Omdat diverse organisaties het BSN machinaal willen verwerken, wordt een QR-code toegevoegd.

Met de chip op de WID documenten kunnen persoonsgegevens betrouwbaar geregistreerd worden. Omdat hierin ook het BSN is opgenomen verwerken allerlei partijen ook mogelijk het BSN. Met de QR code kan er meer selectief toegang gegeven worden tot het BSN.

2. Vaststellen verslag en actiepunten

2.1. Verslag

Het verslag van 20 mei wordt zonder wijzigingen vastgesteld

2.2. Actiepunten

[1] https://www.rvig.nl/actueel/nieuws/2021/05/20/nieuw-model-nederlandse-identiteitskaart-per-2-augustus-2021
https://magazines.rvig.nl/idee/2021/16/de-nederlandse-identiteitskaart-vernieuwt-verder

Actiepunt #5 Voorstel om aanpak uit te breiden met autorisatie rollen en het proxy model (Erwin)

- Geen voorderingen

Actiepunt #6 (verslag 18 maart) Uitwerken use case / probleemstelling toegang bij meerdere onderwijsinstellingen (Paul)

- Paul is afwezig en Bram zal de status gaan navragen

Actiepunt #8: Kaders voor thema toegang ontwikkelen tbv ROSA scan. We beginnen met principes en we gaan bij voorkeur gebruik maken van bestaande principes voor toegang (Bram/Erwin)

- Agendapunt

Actiepunt #11:Nieuwe versie GO I&A-Machtigen op Drive plaatsen (Frits)

- Zodra er een nieuwe versie beschikbaar is wordt deze op drive geplaatst

Actiepunt #12:Uitwerken welke doelen we willen onderkennen voor identifiers en attributen en deze hieraan koppelen (Peter)

- Peter heeft de tabel met attributen deels aangepast. Het idee is om per attribuut aan te geven wat het doel is. Een attribuut wordt gebruikt om te identificeren, autoriseren, om te tonen op het scherm of voor bepaalde ondersteunende processen (bijvoorbeeld communicatie met helpdesk). Peter zal de nieuwe tabel de volgende keer toelichten (agendapunt) en vooraf op de drive zetten zodat we dit kunnen combineren met actiepunt #13.

Actiepunt #13: Nagaan welke doelen er nu in een ARP opgenomen zijn (Dirk)

- Dit is samen met #12 een agendapunt voor volgende keer. We willen dat vooraf gecontroleerd wordt of de lijst van Peter met attributen en doelen overeenkomt met de doelen die mogelijk in de ARP opgenomen zijn. We kunnen dan deze analyse bespreken als aanvulling op #12.
- Er wordt gevraagd of er in de verwerkersovereenkomst (ECK keten) ook specifiek attributen en doelen zijn opgenomen. Rimmer levert een voorbeeld verwerkersovereenkomst aan zodat we ook dit mee kunnen nemen in de analyse (actiepunt #14)

3. Afspraken thema toegang

We hebben eerder gesproken over de vele verschillende projecten en visies die relevant voor ons kunnen zijn. We weten dat het niet mogelijk is om alles te bespreken, maar in ieder geval wel de ontwikkelingen/afspraken die direct relevant voor ons kunnen zijn. Bram wil daarom een aantal van die afspraken bespreken om te bepalen of ze relevant zijn en om daar dan ook meer gestructureerd mee om te gaan.

<u>Bronnen en thema's</u>

In de visie van BZK wordt gesproken over vier pijlers, dit zijn: 'Betrouwbaar delen persoonsgegevens[2]', 'Digitale Toegang[3]', 'Digitale Bron Identiteit[4]' en 'Wet en regelgeving

[2] Deze pijler volgt de activiteiten in het programma Regie op Gegevens en het voorstel van de EU Data Governance Act.13 (EUR-Lex - 52020PC0767 - EN - EUR-Lex (europa.eu)

[3] Deze pijler volgt de activiteiten van het programma digitale toegang (Kamerstuk 26643, nr. 711 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)).

[4] Een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector.

rond digitaal vertrouwen (Digital Trust Framework)[5]'. Er wordt voorgesteld om deze indeling ook te gaan hanteren binnen onze werkgroep. Deze indeling is ook reeds aangebracht op onze Google drive. We doen dit met de wetenschap dat niet alle stukken conform deze pijlers ingedeeld kunnen worden. Er is vaak sprake van en overlap en zodoende zullen deze mogelijk op meerdere plaatsen te vinden zijn. Daarnaast kan de indeling te hoog over zijn en daarom brengen we hierbinnen ook een verder onderverdeling aan. Zo nemen we bij 'Digitale Toegang' een aantal van de generieke functies van de Gemeenschappelijke Overheidsarchitectuur (GO) op. Ook hebben we een aantal aanvullende (onderwijsspecifieke) thema's, zoals bijvoorbeeld 'Leven Lang Ontwikkelen' die apart benoemd worden. We kunnen zo bij discussies over een bepaald thema direct verwijzen naar relevante bronnen. Verder worden ook de kaders die we nu aan het definiëren zijn geordend conform deze indeling. Het idee is dat we ook nieuwe ontwikkelingen beter kunnen toetsen op deze bronnen en onze eigen stukken.

Reikwijdte van beleidsafspraken
Om tot afspraken van een digital trust framework te komen zullen dienstverleners moeten samenwerken. Hiervoor moet beleid voor worden geformuleerd. Dit beleid richt zich dan bijvoorbeeld op 'Digitale Toegang' of het 'Betrouwbaar delen van persoonsgegevens'. Bij het formuleren van dit beleid moet aandacht worden besteed aan de mogelijke verschillen tussen landen, sectoren, ketens (administratief/primair proces), initieel en post-initieel onderwijs, natuurlijke personen en niet-natuurlijke personen.

Issues
Naast de eerder bewust gekozen verschillen, bijvoorbeeld vanuit het belang van een bepaalde onderwijssector of het belang van de onderwijsvolger versus het belang van de onderwijsinstelling, hebben we ook te maken met enerzijds de huidige situatie (beleidsstukken rond huidige programma's als eID/ programma digitale toegang) en anderzijds de visies (zoals visie BZK). Het analyseren van visies en roadmaps introduceren extra complexiteit. De rol van onze werkgroep moet zijn dat we de alternatieven kunnen vergelijken en kunnen adviseren over de huidige situatie, de middellange en lange termijn.

Na de toelichting van Bram wordt door de werkgroep aangegeven dat men zich kan vinden in deze afspraken. Er wordt wel aangegeven dat het thema IAA lastig blijft en zich niet makkelijk laat vangen. Zo is bijvoorbeeld de impact van het centraal stellen van de persoon enorm, dit raakt in principe alles. Het is een uitdaging om op verschillende benoemde vlakken inzichtelijk te maken wat dit precies inhoudt. Dit nog los van het kunnen adviseren voor de middellange en lange termijn. We zijn het er echter over eens dat hoe meer structuur we hebben hoe beter we deze uitdaging aan kunnen. Zo komen we bijvoorbeeld al tot de conclusie dat zoiets als de digitale bron identiteit juist voor (ongewenste) verkokering kan zorgen. De kans hierop is nog niet in te schatten omdat we geen duidelijk beeld hebben over de kaders die voor afgeleide identiteiten gaan gelden die binnen verschillende overheidssectoren gebruikt gaan worden.

4. Doorontwikkelen ROSA scan architectuurkaders & beleidskaders

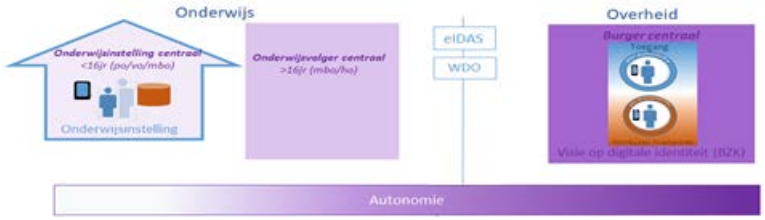
De vorige keer hebben we een aantal ROSA scan architectuurkaders besproken. Tijdens dit overleg worden een aantal van deze kaders afgezet tegen de visie van BZK. Hiervoor zijn een aantal praatplaten opgesteld. Er is er één voor digitale toegang en één voor

[5] Wet- en regelgeving die de uitgangspunten en afspraken rond het delen van gegevens, digitale toegang en het leveren van vertrouwen in de digitale wereld, inclusief de digitale bronidentiteit vastlegt.

attributenuitwisseling. Deze platen kunnen ons helpen om een gedeeld beeld te krijgen over de generieke functies en mogelijke verschillen tussen onze aanpak en de visies.

In de praatplaat voor digitale toegang wordt een vergelijking gemaakt tussen de huidige situatie en de visie van BZK op het vlak van autonomie, privacy en veiligheid. Bij autonomie gaat het om de mate van zelfbeschikking het individu heeft rond zijn digitale identiteit. Bij privacy wordt gekeken naar de generieke functie Identificatie (identifier typen) en bij veiligheid naar de generieke functie authenticatie (betrouwbaarheidsniveau en Single Sign On).

Autonomie



Figuur 1- Digitale toegang (Autonomie)

In Figuur 1 wordt aangegeven dat binnen het onderwijs de onderwijsvolger nu niet of beperkt autonomie geboden wordt. Met name in het po en vo wordt er veel vanuit de school geregeld. De onderwijsinstelling stelt voor de onderwijsvolger een digitale identiteit en authenticatiemiddel beschikbaar. Verder is de digitale identiteit van de onderwijsvolger vaak verbonden met de digitale identiteit van de onderwijsinstelling (in het po/vo wordt bijvoorbeeld de bestelling van leermiddelen) In de plaat wordt aangegeven dat de onderwijsinstelling eigenlijk centraal staat, maar hier is men het niet over eens. In het mbo en ho zien we met de komst van eduID wel meer ondersteuning voor autonomie bij toegang. In de visie van BZK staat de burger centraal. Wat dit concreet betekent is nog niet vastgesteld, maar er wordt aangenomen dat de burger zelfbeschikking krijgt over zijn digitale identiteit bij het afnemen van publieke en private diensten. Het betreft dan bijvoorbeeld welk authenticatiemiddel en/of welke identifier er gebruikt wordt. Het ligt echter voor de hand dat er wel degelijk aan voorwaarden moet worden voldaan. Het zal dus altijd een mate van autonomie zijn die in de betreffende context mogelijk is. Hoe dit in praktijk er uit gaat zien is op basis van de visie nog niet te zeggen. Verder wordt gesteld dat de visie aansluit bij de ontwikkelingen rond eIDAS en dat het waarschijnlijk concreet vorm gaat krijgen als onderdeel van WDO. Hiermee zou de uitwerking van de visie direct een aantal processen binnen het onderwijs gaan raken.

Verder wordt gesteld dat de ‘Wallets’ die bij ‘Mijn attributendiensten’ in de visie van BZK genoemd worden ook een rol zouden kunnen hebben bij toegang (als men bijvoorbeeld aansluit op standaarden rond een Decentralized identifier[6]). Hiermee zou de Wallet ook gebruikt kunnen worden voor toegang[7]. Wat nu ook onduidelijk is of er gesproken moet worden van een wallet of wallets. Er wordt aangegeven dat het onwenselijk is dat er meerdere (te veel) wallets gaan ontstaan doordat bijvoorbeeld elke overheidssector een eigen wallet creëert (deels op basis van afgeleide identiteit) zodat we een vergelijkbare situatie krijgt als met de vele accounts waar men nu mee te maken heeft. Vanuit de werkgroep wordt aangegeven dat het een soort van virtuele wallet moet betreffen die in vele contexten/sectoren te gebruiken is maar verder geen complexiteit in het gebruik introduceert.

---

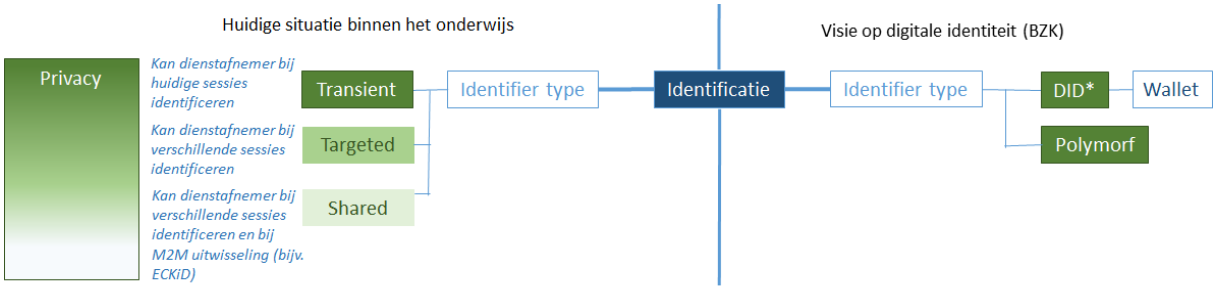
[6] **Decentralized identifier: In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities.*

[7] Dit is deels logisch als voor een bepaalde dienst bijvoorbeeld alleen nodig is om vast te stellen of de dienstafnemer meerderjarig is. Een dergelijk credential wordt logischerwijs ook vanuit de wallet geleverd.

Er wordt besloten dit niet impliciet te laten maar hiervoor een kader te definiëren (actiepunt #15). Verder wordt door leden aangegeven dat een Wallet niet perse een applicatie op een mobiel hoeft te zijn, dit kan wellicht ook een online portaal zijn.

Als een wallet in de context van de visie van BZK ook een rol speelt bij toegang moet er ook de mogelijkheid zijn voor representatie (machtigen). Ook hiervoor willen we een kader opstellen (actiepunt #15).

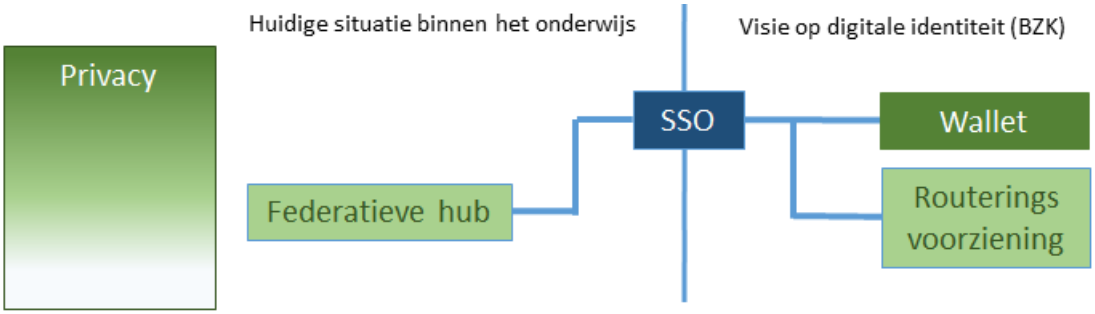
Privacy



Figuur 2 - Digitale toegang – Privacy Identifier type

In Figuur 2 wordt aangegeven dat we binnen het onderwijs (Architectuuraanpak Toegang) drie typen identifiers onderkennen, Transient, Targeted en Shared. Als we vanuit een privacytechnisch oogpunt kijken naar deze typen kunnen we stellen dat een transient identiifer een hogere mate van privacy biedt dan een Targeted identifier. Een Shared idenitifer (zoals een BSN) biedt de minste mate van privacy. Wel zijn er vaak privacy bevorderende maatregelen aan een het verwerken van een shared identifier gekoppeld.

Het eHerkenning (ETD[8]) afsprakenstelsel ondersteunt al een Polymorfe Pseudoniem (PP) identifier en de verwachting is dat deze op de middellange termijn gebruikt wordt binnen programma digitale toegang/WDO. Een PP is eigenlijk geen identifier. Het is een privacy bevorderende maatregel (cryptografisch) om te voorkomen dat partijen binnen het afsprakenstelsel tijdens het transport van het PP het handelen van de gebruiker (makkelijk) kunnen traceren. De polymorfe bewerking kan toegepast worden op alle identifier typen. Als het een Targeted variant betreft wordt het een Polymorfe Pseudoniem[9] genoemd. Als het een Shared variant betreft wordt het een Polymorfe Identiteit (PI) genoemd (in het geval van een BSN). Hoewel het nu nog onduidelijk hoe op basis van de visie van BZK e.e.a. uitgewerkt gaat worden, wordt aangenomen dat er mogelijk ook decentralized identifiers (DID) ondersteund gaan worden. Dit past ook binnen de toepassing van een Wallet.

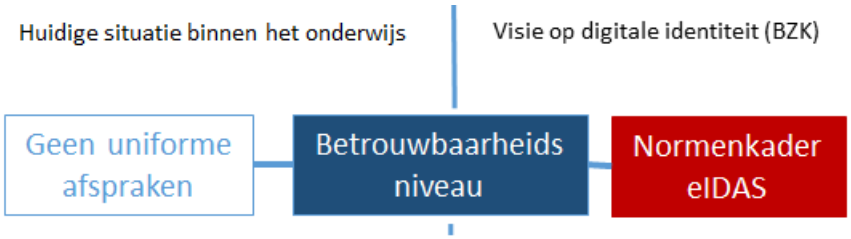


Figuur 3 - Digitale toegang – Privacy SSO

[8] https://afsprakenstelsel.etoegang.nl/display/as/Polymorf+Pseudoniem
[9] Ontvangende Partij specifiek Versleuteld Pseudoniem (VP@OP)

Binnen het onderwijs hebben we nu verschillende Federatieve Hubs, zoals SURFconext en Entree Federatie, die de SSO functie ondersteunen. Vanuit een privacy oogpunt kan gesteld worden dat een Federatieve Hub een redelijke mate van privacy kan bieden afhankelijk van de inrichting. Bij de overheid wordt een dergelijke functie ondersteund via varianten van een Federatieve hub, een Routeringsvoorziening of Makelaar. Als er vervolgens ook gebruik wordt gemaakt van Polymorfe Pseudoniemen kan er door de Federatieve Hub een grotere mate van privacy worden geboden. Als een Wallet ook een rol gaat spelen bij toegang dan is de vraag hoe de SSO functie ondersteund wordt. Wordt dit direct of indirect via een federatieve hub geregeld? De verwachting is dat een Wallet een peer-to-peer koppeling heeft met de verifier en dat er dus geen centrale federatieve hub is. In dat geval zou de wallet dus (een bepaalde mate) van SSO moeten ondersteunen (actiepunt #15). In het geval van een peer-to-peer koppeling kunnen we stellen dat deze optie een nog betere mate van privacy zou kunnen gaan bieden.

Veiligheid



Figuur 4 - Digitale toegang – Veiligheid Betrouwbaarheidsniveau

Als laatste wordt er ook een vergelijking gemaakt rond veiligheid. Dit wordt gerelateerd aan het betrouwbaarheidsniveau van de authenticatie (identifier). Er is binnen het onderwijs nu geen uniform normenkader. Dienstaanbieders kunnen geen risicoanalyse uitvoeren en het betrouwbaarheidsniveau van hun dienst te bepalen. Dienstafnemers kunnen zich niet volgens een bepaald betrouwbaarheidsniveau authenticeren. Bij de overheid wordt (waarschijnlijk) voor de authenticatiemiddelen die onder WDO (en visie BZK) gaan vallen gebruik gemaakt van het normenkader van eIDAS en er is een handleiding voor dienstaanbieders om het betrouwbaarheidsniveau te bepalen. Wat dit betekent voor de visie van BZK (en Wallets als deze ook bij toegang een rol speelt) is moeilijk te zeggen. De credentials die via de Wallet geleverd kunnen worden zullen ongetwijfeld een verschillende betrouwbaarheidsniveau kunnen hebben. Ook in die context zal er dus ongetwijfeld een normenkader beschikbaar zijn. Waarschijnlijk zal dat dit normenkader wel een bredere scope hebben (ook andere credentials dan een identifier, zoals attributen etc.).

De praatplaat rond attributenuitwisseling wordt nog kort toegelicht. Er wordt hierin conform ons architectuuraanpak aangegeven dat er een identifier en (minimale) set attributen via de Federatieve Hub wordt geleverd en dat hiervoor een ARP is geregistreerd. Er is een apart kanaal voor de uitwisseling van overige attributen (bijvoorbeeld om te tonen op het scherm of voor bepaalde ondersteunende processen). Deze attributenuitwisseling verloopt via een apart M2M kanaal waarbij een mandatering is geregistreerd in het OSR. Bij de bespreking van de visie van BZK in de digitale toegang praatplaat is aangegeven dat de manier van uitwisseling voor toegang (identifier van bepaald betrouwbaarheidsniveau) en overige attributen (credentials) mogelijk weer op een identieke manier zal plaatsvinden via de Wallet. De Wallet zal zo mogelijk naast de daadwerkelijke attributenuitwisseling op basis van toestemming ook transparantie kunnen bieden over attributenuitwisseling vanuit een wettelijk kader (actiepunt #15). Als er meer duidelijkheid is hoe de visie van BZK uiteindelijk gerealiseerd wordt kunnen we een beter beeld vormen van de attributenuitwisseling patronen.

Het is duidelijk dat de stellingen rond de visie zijn gebaseerd op aannames en vrije interpretatie. Het is ook duidelijk dat niet alle leden het eens zijn over deze interpretaties. Het lijkt er wel op dat onze architectuuraanpak ons in staat stelt om bijvoorbeeld ten aanzien van aspecten als autonomie, privacy en veiligheid een analyse uit te voeren. De discussie heeft verder de denkbeelden rond een wallet gescherpt en we hebben hiervoor ook een aantal vragen en randvoorwaarden kunnen formuleren (zie actiepunt #15).

5. Rondvraag & afsluiting

Het volgende overleg is op 26 augustus 2021 van 1500 tot 1700 uur. Op de agenda staan dan de volgende onderwerpen:

- Mededelingen en opening
- Verslag 24 juni 2021 & acties
- Probleemstelling toegang bij meerdere onderwijsinstellingen (actiepunt #6)
- Attributenlijst en doelen (actiepunt #12)
- Vervolg ROSA scan kaders (actiepunt #8)

6. Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder
5	Voorstel om aanpak uit te breiden met autorisatie rollen en het proxy model	Open		Erwin
6	Uitwerken use case / probleemstelling toegang bij meerdere onderwijsinstellingen	Open		Paul (en Peter)
8	Kaders voor thema toegang ontwikkelen tbv ROSA scan. We beginnen met principes en we gaan bij voorkeur gebruik maken van bestaande principes voor toegang	Loopt		Bram en Erwin
11	Nieuwe versie GO I&A-Machtigen op Drive plaatsen	Open		Frits
12	Uitwerken welke doelen we willen onderkennen voor identifiers en attributen en deze hieraan koppelen	Open		Peter
13	Nagaan welke doelen er nu in een ARP opgenomen zijn. Analyse of deze doelen overeenkomen met doelen van actiepunt #12	Open		Dirk
14	Voorbeeld verwerkersovereenkomst opleveren	Open		Rimmer
15	Kader definiëren voor een wallet. • We willen wallets in vele contexten/sectoren gebruiken maar dit moet geen complexiteit in het gebruik introduceren vergelijkbaar met het gebruik van verschillende accounts. • Als een wallet ook een rol speelt bij toegang moet er ook een mogelijkheid zijn voor representatie • Als een wallet ook een rol speelt bij toegang moet ook SSO ondersteund worden • Een wallet ondersteunt attributenuitwisseling obv toestemming maar kan ook transparantie bieden over attributenuitwisseling vanuit een wettelijk kader (binnen onderwijssector)	Open		
16		Open		

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen