Verslag werkgroep Toegang

Aanwezig: Peter Clijsters (SURF), Tom van Veen (SURF), Freek Nabuurs (Cito), Edwin Verwoerd (KBb-E), Brian Dommisse (Kennisnet, PO/VO-raad), Frits Bouma (DUO), Bram Gaakeer (OCW, voorzitter), Erwin Reinhoud (Kennisnet, Bureau Edustandaard)

Afwezig: Dirk Linden (Kennisnet), Jan Over (SURF/HOSA), Paul de Wit (saMBO-ICT/MBO Raad)

Datum
26 augustus 2021

Agenda

1. Opening en mededelingen
2. Vaststellen verslag vorig overleg en actiepunten
3. Probleemstelling toegang bij meerdere onderwijsinstellingen (actiepunt #6)
4. Attributenlijst en doelen (actiepunt #12)
5. Vervolg ROSA scan kaders (actiepunt #8 $ #15)

1. Opening en mededelingen

Dirk en Paul zijn afwezig, agendapunten #6 (Paul) en #13 (Dirk) worden een volgende keer besproken.

Actiepunt #14 zou Rimmer oppakken. Er zal bij de GEU worden nagevraagd of een vervanger is voor Rimmer (actiepunt #16). Freek biedt aan om actiepunt #14 op te pakken.

2. Vaststellen verslag en actiepunten

2.1. Verslag

Het verslag van 24 juni wordt zonder wijzigingen vastgesteld

2.2. Actiepunten

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)

- Geen vorderingen

Actiepunt #8: Kaders voor thema toegang ontwikkelen tbv ROSA scan. (Bram/Erwin)

- Agendapunt (combi met #15)

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: Federatieve identifiers en attributen en doelen (Peter)

- Peter geeft aan een update op de google drive te hebben geplaatst. Hiermee is het actiepunt afgehandeld. Een volgende keer wordt dit besproken irt met actiepunten #13 en #14.

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

Actiepunt #14: voorbeeld verwerkersovereenkomst opleveren (Freek)
- Geen vorderingen

Actiepunt #15: Kader voor een wallet.
- Agendapunt (combi met #8), afgehandeld

3. Doorontwikkelen ROSA scan architectuurkaders & beleidskaders (actiepunt #8 & #15)

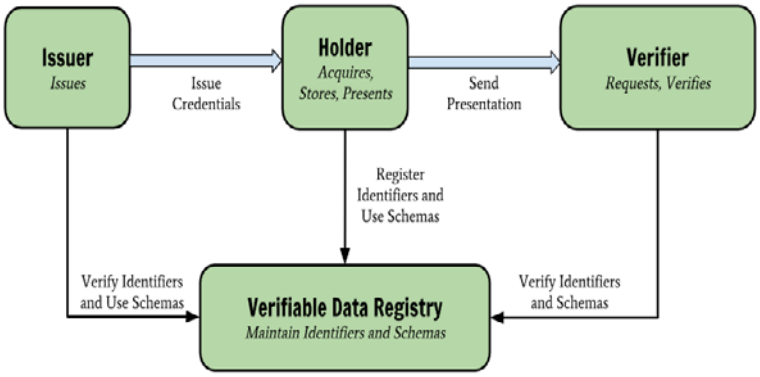
De vorige keer hebben we de kaders besproken vanuit onze architectuuraanpak en deze geprobeerd te relateren aan wat nu bekend is rond de visie van BZK. Een belangrijk onderdeel binnen deze visie is de wallet, maar er is nog veel onduidelijk.

We willen deze keer wat meer duidelijkheid rond het concept van een wallet krijgen. Er is een analyse gedaan op basis van de ambities van eIDAS. We gaan er voorlopig vanuit dat de gedachten rond de wallet van eIDAS aansluiten bij de visie van BZK.

Hieronder zijn een aantal onderdelen uit de presentatie die op de drive[1] staat overgenomen.

De wallet van eIDAS is ook nog erg conceptueel. Het huidige model van eIDAS was te beperkt en men heeft lidstaten een drietal opties voorgelegd om het huidige stelsel aan te passen. Na een consultatie is de meest ambitieuze optie met een wallet gekozen. Om het concept van een wallet te verduidelijken wordt eerst het Verifiable Credentials Data Model[2] van W3C toegelicht.

Verifiable Credentials Data Model
Er zijn verschillende nieuwe standaarden die wat men met een wallet wil bereiken mogelijk maken. Deze definiëren nieuwe rollen, maar zijn deels vergelijkbaar met de voor ons bekende rollen.



Figuur 1 - Verifiable Credentials Data Model (W3C)

1 https://docs.google.com/presentation/d/1muZuZGU2tSGjc_bfJIpurT8Yy1CSGpPO/edit?usp=sharing&ouid=101017003326540547237&rtpof=true&sd=true
2 https://www.w3.org/TR/vc-data-model/

- **Holder**
  A role an entity might perform by possessing one or more verifiable credentials and generating presentations from them. A holder is usually, but not always, a subject of the verifiable credentials they are holding.

- **Issuer**
  A role an entity can perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder.

- **Verifiable data registry**
  A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable credentials.

- **Verifier**
  A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation for processing. Other specifications might refer to this concept as a relying party.

- **Verifiable Credential**
  Een Verifiable Credential is een cryptografisch verifieerbare verklaring van een entiteit (“Issuer”) over een andere entiteit (“Subject”, “Holder”), bijv.:
    - BRP : “Persoon heeft een adres in Amsterdam.”
    - School: “Persoon is alumnus van universiteit X”

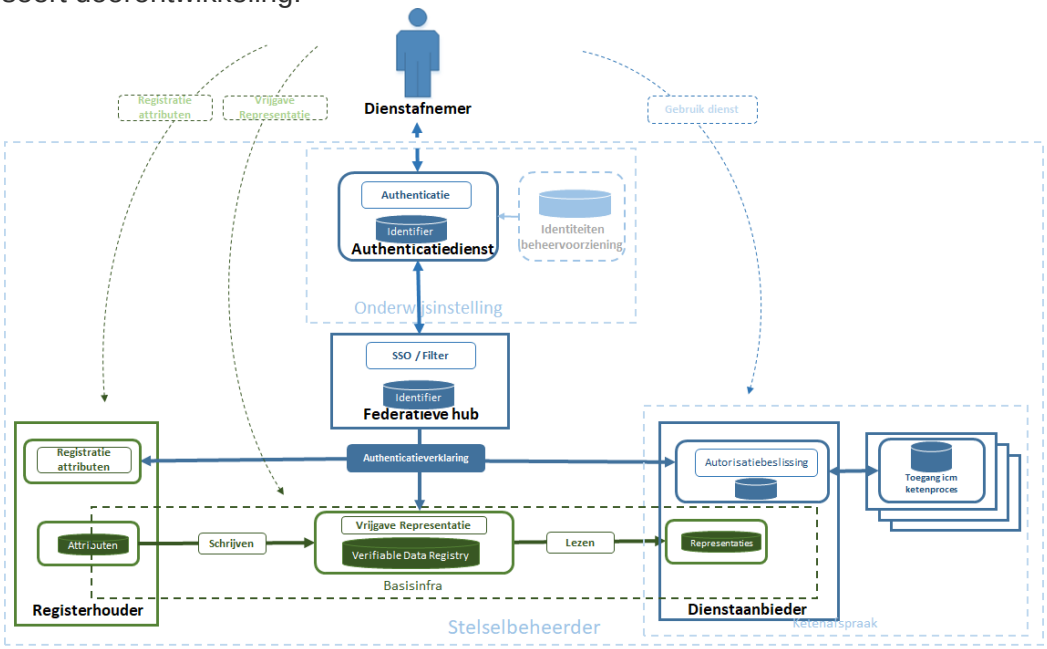
Aanpassing architectuuraanpak toegang praatplaat

Er wordt voorgesteld om de plaat in onze architectuuraanpak aan te passen en deze nieuwe rollen op te nemen. In de huidige plaat hebben we nu de digitale identiteit (met name van onderwijsvolgers en medewerkers) die beheerd wordt vanuit de school en toegang verloopt via een Federatieve hub (perspectief onderwijsinstelling). In de nieuwe plaat is hier attributenuitwisseling aan toegevoegd (in groen aangegeven) zoals die in het eIDAS voorstel mogelijk bedoeld is. De groene basisinfrastructuur is in principe de laag die het gebruik van een wallet ondersteunt. De Holder registreert zijn verifiable credentials en stelt deze aan de verifier beschikbaar. Hiervoor moet de Holder zich authenticeren en dit wordt mogelijk gedaan via de authenticatie applicatie op de mobiele telefoon. Deze functie wordt ondersteund door de rol authenticatiedienst. Er worden (voorlopig) zeven functionele rollen onderkend:

I. Dienstafnemer (gebruiker /holder): Een natuurlijk persoon die gebruik maakt van de dienst. Wil gegevens delen met dienstaanbieder.
II. Dienstaanbieder (relying party / service provider / verifier): De persoon of organisatie die voorziet in het leveren van een afgebakende prestatie (dienst) aan haar omgeving (de dienstafnemers). Een partij die om een interactie of transactie (dienstverlening) aan te gaan bepaalde claims geverifieerd wil hebben vanuit een gezaghebbende bron
III. Identiteitenbeheervoorziening : Registratie en beheer gegevens van een natuurlijk persoon. Levert basis voor digitale identiteit onderwijsvolgers en medewerkers.
IV. Authenticatiedienst (identity provider): Authenticeer de Dienstafnemer aan de hand van een authenticatiemiddel en levert de Dienstaanbieder een authenticatieverklaring (ook wel identiteitsverklaring).
V. Federatieve hub: Ondersteunt SSO en filter functie voor beperkte set attributen. Zorgt voor enkelvoudige koppeling tussen Authenticatiediensten en Dienstaanbieders.
VI. Registerhouder (issuer / attributendienst / trusted source): De partij die gegevens (verifiable credentials) registreert en daarmee een gezaghebbende bron kan vormen.

VII. Verifiable Data Registry. Ondersteunt de creatie en gebruik van verifiable credentials. De dienstafnemer kan een bepaalde dienstaanbieder deze laten lezen (representatie van credential).

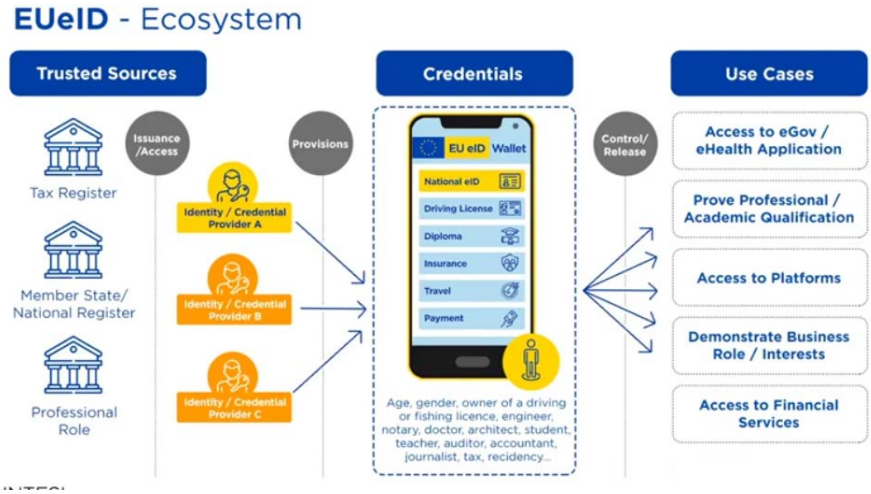
Een 8e niet functionele rol is de stelselbeheerder: Houdt toezicht op compliance en organiseert doorontwikkeling.



Figuur 2 – Architectuuraanpak toegang - praatplaat

European Digital Identity wallet (eIDAS)

Elke lidstaat maakt eigen keuzes rond de te gebruiken wallet(s)[3]. Deze moet door de betreffende lidstaat wel zijn goedgekeurd. Het moet voldoen aan de nog te maken stelseleisen zodat een burger uit een bepaalde lidstaat zijn wallet kan gebruiken voor publieke en private diensten binnen de verschillende lidstaten. Grote platformen zoals Google en Facebook wil men verplichten tot acceptatie van deze eIDAS middelen. Het lijkt dus naast private diensten binnen lidstaten ook te gaan om private diensten buiten Europa. Het volgende is wat we nu (ongeveer) weten.



Figuur 3 - European Digital Identity wallet

[3] Publieke en private partijen kunnen een wallet aanbieden. Een lidstaat moet deze valideren.

Of de voorgestelde wijziging het huidige eIDAS stelsel vervangt is nog niet duidelijk. Wel is in concept beschreven op welke punten de huidige verordening wordt aangepast.

Is de visie van BZK in lijn is met deze aanpassing van de eIDAS verordening?
We weten niet of dit in de governancestructuur geborgd is. De Visie op digitale identiteit van BZK geeft in ieder geval aan dat eIDAS onderdeel is van het juridisch perspectief wat men voor ogen heeft.

Is dit relevant voor ons, het onderwijs? Wanneer gaat het relevant worden?
We verwachten dat dit over een aantal jaren een rol kan gaan spelen binnen het onderwijs. De verwachting is wel dat dit (in eerste instantie) een beperkt aantal use cases betreft en met name in het ho en mogelijk mbo. Als er een wallet beschikbaar is zou DUO het digitale diploma van de student hierop kunnen laten registreren. Zo zou dit en overige gegevens gebruikt kunnen worden bij bijvoorbeeld centraal aanmelden en Studielink. Voor ons is het belangrijk om hier al op vooruit te lopen. De kaders die we definiëren willen we kunnen mappen op de bestaande, maar ook toekomstige inrichtingsvormen. Daarnaast kan een vroegtijdig beeld van het concept en impact ons helpen om tijdig (bij) te sturen waar we dit nodig achten. Of er op sturen dat bepaalde usecases/onderwijssectoren van een bepaalde verplichting uitgesloten worden. We blijven deze ontwikkelingen volgen en een beeld vormen hoe dit in het groter geheel past binnen het onderwijs. We onderkennen echter dat er ook binnen het onderwijs (noodzakelijke) verschillen zijn per sector.

Hoe is onboarding bij een bepaalde registerhouder geregel als de wallet zelf ook een rol bij toegang speelt?
Hoe dit er precies uit gaat zien laat zich raden. Er wordt in ieder geval gesteld dat de wallet een rol heeft bij toegang en het delen van gegevens. Het proces waarbij een verifiable credential van een holder door een registerhouder geregistreerd wordt zodat de holder deze kan “delen” vereisen naar verwachting inderdaad een authenticatie van een hoog betrouwbaarheidsniveau. Zeker in de context van eIDAS. Maar gezien ook private partijen (en platformen zoals Facebook) een acceptatie plicht hebben, kan het zijn dat er in breder zin gebruik wordt gemaakt van de basisinfrastructuur waarbij ook claims (niet noodzakelijk verifiable credetnials) gedeeld kunnen worden. Het is dan ook de vraag of er voor het scenario waar een verifier over een verifiable credential van de holder wil beschikken dezelfde basisinfrastructuur gebruikt kan worden als wanneer een dienstaanbieder over een claim wil beschikken van de dienstaanbieder waarbij minder hoge eisen aan de claim of de uitgever ervan worden gesteld.

Voor de volgende keer gaan alle leden kijken welke hoog over (bestaande) principes we als kader kunnen opnemen en welke mogelijk voor een bepaalde sector, use case of inrichtingsvorm gelden. Zo is er al een IAA visie[4] van SURF dat als basis gebruikt kan worden door leden. Edwin zal de Edu-K casus achternaam met leden delen (actiepunt #17). In de meest recente versie van dit document zijn ook principes opgenomen. Leden zullen eventuele opmerkingen hierover vooraf met Edwin delen.

4. Rondvraag & afsluiting

Het volgende overleg is op 23 september 2021 van 15:00 tot 17:00 uur. Op de agenda staan dan de volgende onderwerpen:

- Mededelingen en opening
- Verslag 26 augustus 2021 & acties
- Vervolg ROSA scan kaders (principes)

[4] visiedocument_iaa_surfnet.pdf

- Terugkoppeling OCW themabijeenkomst Digitale Identiteiten

5. 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	Afgehandeld		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		Freek
15	Kader definiëren voor een wallet.	Afgehandeld		Bram en Erwin
16	GEU vragen om vervanger Rimmer	Open		Bram
17	Edu-K casus achternaam delen met leden	Open		Edwin

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen