Samen aanjagen van vernieuwing

Auteurs: Peter Leijnse, Domeinarchitect HOSA IAM
Menno Scheers, Lead Architect HOSA

Versie: 1.0

Datum: 21 december 2022

Aangejaagd door CIO's van de HO-instellingen, Architectenberaad HO, SURF, ….

Voorwoord

Voor je ligt de HOSA Domeinarchitectuur Identiteit en Toegang. Het eindresultaat van een traject waaraan architecten, informatiemanagers en specialisten van instellingen en sectorpartners over een periode van twee jaar intensief hebben samengewerkt.

De voorliggende domeinarchitectuur schetst hoe het landschap voor identiteit en toegang in onderwijs en onderzoek er over drie tot tien jaar uit zou moeten zien. Daarbij zijn de ambities van de HO-sector, veranderingen rondom onderzoek en onderwijs en internationale (technologische) ontwikkelingen als uitgangspunt genomen. De domeinarchitectuur, te vergelijken met een bestemmingsplan, bevat een visie op de toekomst van het domein en de daarbij behorende processen en systemen. Deze visie vormt tevens de basis voor een roadmap om de domeinarchitectuur te realiseren en te prioriteren. Dit document biedt hiermee kaders voor het uitwerken en toetsen van die vervolgarchitecturen en -ontwerpen.

De andere HOSA-domeinarchitecturen voor Flexibel Onderwijs en Research Data Management maken gebruik van het concept van businessplatforms om in te spelen op de grote behoefte om allerlei vormen van samenwerking te faciliteren. De domeinarchitectuur Identiteit en Toegang is daar ondersteunend aan, en schetst hoe over verschillende businessplatforms heen consistent kan worden omgegaan met identificatie, authenticatie en autorisatie van gebruikers, aanbieders en diensten. Immers, in een flexibele architectuur komen deze in meerdere platformen terug. Dit wordt gedaan met een grote nadruk op publieke waarden.

Het IAM-domein is – met de verschuiving van centrale en federatieve dienstverlener-centrische oplossingen naar decentrale oplossingen waarin de gebruiker leidend is – zeer aan verandering onderhevig. Inmiddels zien we dat een aantal concepten die in deze domeinarchitectuur worden beschreven al neerdalen in het denken binnen de HO-instellingen en ook daarbuiten, bijvoorbeeld in de MBO-sector. Ook zien we dat een aantal beschreven ‘toekomstige’ ontwikkelingen, zoals credentials en wallets, de laatste tijd heel erg snel gaan. In de domeinarchitectuur schetsen we hoe de huidige generaties van IAM-systemen toe kunnen groeien naar een toekomstvaste architectuur.

Het Enterprise Architectuur team bij SURF zal de domeinarchitectuur onderhouden en verder doorontwikkelen samen met de sector.

Inhoud

1 Inleiding

1.1 Aanleiding

De HO-instellingen hebben geconstateerd dat het aantal instellingoverstijgende initiatieven zal toenemen en dat deze een grotere impact gaan hebben op de eigen voorzieningen. De Versnellingsagenda 'In samenwerking onderwijsinnovatie met ICT' van het HO en diverse sectorpartners is zo'n initiatief. Ook UNL onderzoekt in welke onderwerpen de universiteiten gezamenlijk willen gaan investeren, zoals in onderzoeksfaciliteiten, ICT voor onderwijsvernieuwing of duurzame bedrijfsvoering. Daarnaast wordt in het HBO instellingsoverstijgend samengewerkt, bijvoorbeeld rondom het thema onderzoeksondersteuning. De CIO's van instellingen, SURF en een aantal sectorpartners hebben daarom het initiatief genomen voor een gezamenlijke architectuur voor digitale sectorvoorzieningen van de toekomst.

De ontwikkelingen op het gebied van Flexibilisering van Onderwijs, Leven Lang Ontwikkelen (LLO) en datamanagement leiden tot meer instellingoverstijgende samenwerking en organisatie op het gebied van gemeenschappelijke informatie- en ICT-voorzieningen (sectorvoorzieningen). Vragen die hierbij ontstaan, zijn bijvoorbeeld "hoe zorgen we dat sectorvoorzieningen toekomstvast zijn?", "hoe zorgen we voor samenhang in de sectorvoorzieningen?", "hoe maken we hergebruik mogelijk?" en meer recentelijk "hoe borgen, beschermen en bevorderen we publieke waarden bij de digitalisering van onderwijs en onderzoek?".

Sectorpartners als SURF, Studielink, DUO, DANS en NWO proberen alle instellingen hierbij zo veel mogelijk te faciliteren en te ondersteunen. Dit is echter een complex proces, waardoor behoefte ontstaat aan een gezamenlijke architectuur: voor een sectorbrede definitie, ontwikkeling en inzet van Informatie- en ICT-voorzieningen is het noodzakelijk duidelijkheid te verschaffen over de vraag naar die voorzieningen, de eisen die er in samenhang aan gesteld worden, de vormgeving en inrichting ervan en de dienstverlening van ICT-dienstverleners aan instellingen. Dit gemeenschappelijke kader willen we creëren vanuit een architectuurbenadering: de HO Sector Architectuur (HOSA).

1.2 Doelstelling

Het project HOSA heeft als doel een architectuur te definiëren voor sectorvoorzieningen die van belang zijn voor de strategische samenwerkingen tussen HO-instellingen, sectorpartners en marktpartijen. De HOSA kent zodoende als basis een optimale articulatie van de vraag van de sector met betrekking tot sectorvoorzieningen, uitgewerkt in een doelenstructuur (zie 2.4). Het biedt een faciliterend kader voor de interoperabiliteit tussen instellingen en aanbieders van de gemeenschappelijke ICT-voorzieningen. De HOSA moet eraan bijdragen dat lopende en nieuwe initiatieven op het gebied van sectorvoorzieningen sneller, toekomstgerichter en toekomstbestendiger tot stand komen. Sectorpartners en marktpartijen van ICT-voorzieningen kunnen hier met hun dienstenportfolio goed op inspelen.

1.3 Scope van de domeinarchitectuur

De domeinarchitectuur heeft in beginsel als scope de Nederlandse HO-sector met WO en HBO. Daarbij wordt mede naar de internationale context gekeken. De tijdshorizon is op de middellange en lange termijn vooruitkijkend (3 tot 10 jaar), met een inschatting van de functionele behoeften aan sectorvoorzieningen voor de doelstellingen van onderwijs en onderzoek. Wat betreft de architectuur voor ondersteuning van onderwijs en onderzoek wordt er breed gekeken met ook aandacht voor dienstverlening, processen, functionaliteit, gegevens en technologie, governance, eigenaarschap, beheer en ondersteuning. Het betreft een conceptuele beschrijving met richtinggevende kaders voor oplossingen.

Deze domeinarchitectuur is een conceptuele beschrijving van de beoogde inrichting van sectorvoorzieningen ten behoeve van identiteiten en toegang. Onder Identiteit en Toegang (ook wel aangeduid als Identity &

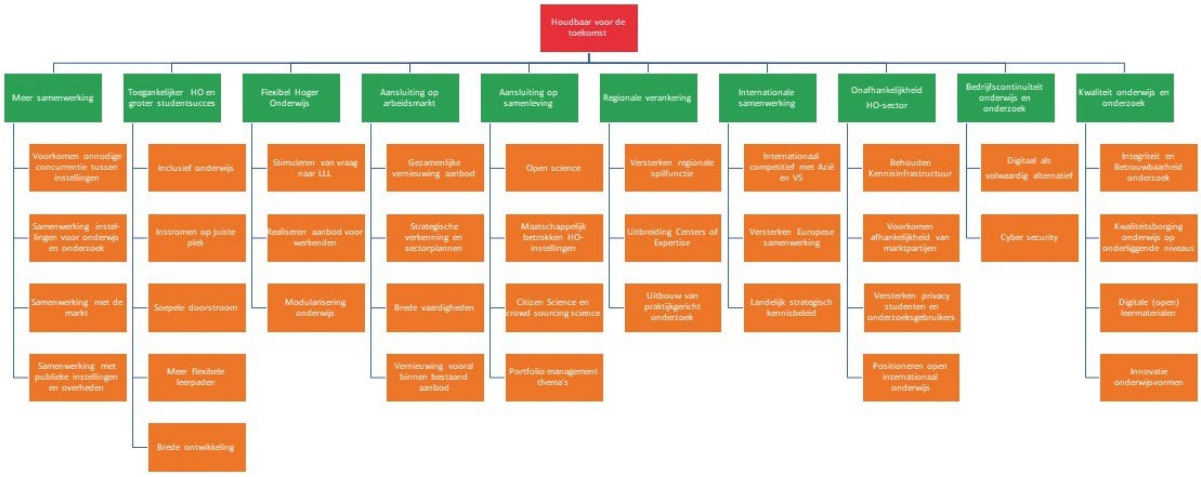
Access Management (IAM)) wordt verstaan het faciliteren dat de juiste “identiteit”, voor de juiste redenen, onder de juiste voorwaarden en op het juiste moment “toegang” krijgt tot de juiste faciliteiten. Identiteit en Toegang is van belang voor het leveren van digitale dienstverlening met drie belangrijke voorwaarden:

- Identificatie, dat we weten wie je bent en welke digitale identiteit van jou is;
- Authenticatie, dat we met een bepaalde zekerheid weten dat jij ook echt degene bent van wie de digitale identiteit is;
- Autorisatie, dat we weten wat je dan mag (al dan niet door een ander gemachtigd), of juist niet mag.

Bij deze domeinarchitectuur Identiteit en Toegang voor het onderwijs en onderzoek wordt er breed gekeken met aandacht voor diensten, dienstverlening, processen, functionaliteit, data en technologie, privacy, informatiebeveiliging, besturing, eigenaarschap, beheer en ondersteuning. Het betreft een conceptuele beschrijving en geeft richtinggevende kaders voor oplossingen.

1.4 De doelenstructuur

De doelen van de sector zijn samengevat in een doelenstructuur[1]. Deze geeft inzicht in de doelstellingen en ambities die de sector heeft gesteld. De basis voor deze doelenstructuur is gelegd door de Strategische Agenda van het Ministerie van OCW. Deze is aangevuld met doelstellingen uit andere beleidsdocumenten en opgenomen in onderstaande diagram.



Figuur 1: de doelenstructuur van de HOSA

Deze domeinarchitectuur Identiteit en Toegang draagt bij aan het realiseren van vrijwel alle doelstellingen (oranje) in het licht van de ambities van de sector (in groen gemarkeerd). Een aantal doelstellingen, zoals ‘Digitaal als volwaardig alternatief’, ‘Voorkomen afhankelijkheid marktpartijen’, ‘Flexibele leerpaden’, ‘Modularisering onderwijs’ en ‘Meer samenwerking’ zijn daarbij drijvers van een andere kijk op Identiteit en Toegang.

[1] Doelenstructuur van de HOSA | SURF.nl

2 Architectuurvisie

HOSA (Hoger Onderwijs Sector Architectuur) geeft een architectuurvisie voor de HO-sector met een horizon van ongeveer drie tot tien jaar. Binnen de HOSA zijn verschillende domeinen onderkend die ieder een verdere invulling geven aan specifieke onderdelen van de architectuurvisie. De architectuurvisie is daarbij gebaseerd op de initiatieven en ambities in de sector en de ontwikkelingen in de markt en samenleving.

2.1 Inleiding

Onderwijs en onderzoek binnen de HO-sector is volop in verandering. Enerzijds zijn er wereldwijde ontwikkelingen die een impact hebben, zoals verdergaande digitalisering, andere vormen van nationaal- en internationaal samenwerken, citizen science, modulair onderwijs en open onderzoek. Anderzijds zijn er technologische ontwikkelingen die veranderingen teweegbrengen, zoals verdergaande inzet van cloud, de opkomst van kunstmatige intelligentie, nieuwe technieken voor betrouwbare decentrale uitwisseling van identiteits- en contextgegevens voor digitale identiteiten.

Nederland heeft zelf een aantal ambities die worden gefaciliteerd vanuit de HO-sector. Regio's zetten in op slimme technieken waarbij ze tezamen met HO-instellingen in de vorm van 'smart regio's' betere aansluiting willen krijgen op de ontwikkelingen. Daarnaast heeft de Nederlandse overheid de ambitie om een datagedreven kenniseconomie te maken, zoals benoemd in het Kennis en Innovatieconvenant[2]. OCW heeft met de sector in de strategische agenda een aantal doelstellingen geformuleerd. De nadruk ligt daarbij op toegankelijker hoger onderwijs, samenwerking tussen instellingen en met andere partijen, flexibel hoger onderwijs, verbeteren van aansluiting op de arbeidsmarkt, aansluiting met de samenleving, regionale verankering en internationale samenwerking. Daarnaast zijn onafhankelijkheid van de HO-sector, bedrijfscontinuïteit van onderwijs en onderzoek en kwaliteit van onderwijs en onderzoek belangrijke aandachtspunten in de sector. Om deze doelstellingen te halen voldoen sectorvoorzieningen in de huidige vorm niet en zijn veelal nieuwe sectorvoorzieningen vereist.

Ook sectorvoorzieningen voor het verlenen van toegang tot online diensten moeten voorsorteren op de ambities van de sector. Het verlenen van toegang balanceert tussen gemak in dienstverlening enerzijds en afscherming tegen ongeoorloofde toegang of onrechtmatig gebruik door onvertrouwde derden anderzijds. Gebruikelijke manier van verlenen van toegang in de huidige situatie is het gebruik van gebruikersnaam, wachtwoord en eventueel een token of tweetrapsverificatie. Op de achtergrond is hiervoor een hele infrastructuur met bijbehorende procesafspraken die dit faciliteert. Veel van deze infrastructuur is 'instellingscentrisch' georganiseerd, terwijl de maatschappelijke en technologische trend is om voor identiteit en toegang veel meer vanuit het perspectief van het individu te redeneren. Dit vraagt om een andere kijk op deze voorzieningen voor Identiteiten en Toegang, zoals in de volgende paragrafen verder wordt uitgewerkt.

Onderwijs en onderzoek zijn in beweging

In onze sector zijn we eraan gewend om te denken vanuit de student, docent en onderzoeker. Bij een student wordt er vaak impliciet vanuit gegaan dat die zich binnen de muren van de instelling bevindt. Bij flexibel onderwijs en leven lang ontwikkelen zal deze zich meer over de muren van instellingen heen bewegen en verschuift de tijdschaal van de duur van een opleiding naar levenslang. Dit terwijl voorzieningen voor het beheren van identiteiten en toegang nu primair binnen een instelling is georganiseerd voor de duur van de opleiding. Er is een mechanisme nodig dat er voor zorgt dat zorgt dat de voorzieningen meebewegen met de ontwikkelingen, over instellingen heen, en over een langere periode

Ook gaat het huidige beeld sterk uit van opleidingen. Als gevolg van flexibilisering en 'leven lang ontwikkelen' komt meer nadruk komen op aanmelden voor en volgen van individuele vakken. Wat moet een instelling eigenlijk van een lerende weten die slechts een vak komt volgen en bij een andere instelling voor een volledige

[2] https://www.topsectoren.nl/innovatie/documenten/kamerstukken/2019/november/12-11-19/kic-2020-2023

opleiding staat ingeschreven? Is het nodig dat deze alle persoonsgegevens nog een keer komt laten zien alsof hij zich voor een voltijdsopleiding aanmeldt? Of is het voldoende dat de persoon aangeeft dat deze student is bij Hogeschool Leiden en dat deze een vak komt volgen? In hoeverre is het noodzakelijk dat er aanvullende gegevens worden gedeeld? In de huidige situatie is er een onboardingsproces voor studenten en medewerkers dat veel vraagt van instellingen. Het is een proces waarin vele zaken getoetst worden. Voor meer flexibel onderwijs en leven lang ontwikkelen is er een behoefte aan een laagdrempelig onboardingsproces dat aansluit op de behoefte van de deelnemer en administratief minder druk legt op de organisatie met lagere kosten en betere doorlooptijden. Bovendien moet dit onboardingsproces geschikt zijn voor lerenden vanuit het buitenland.

Op het gebied van onderzoek heeft de sector de ambitie om de maatschappij meer te betrekken bij onderzoek en de resultaten ervan. Het gaat hier om bedrijven, overheden, burgers, ziekenhuizen en vele andere partijen die regelmatig ook uit het buitenland komen. Dit betekent dat deze partijen toegang moeten kunnen hebben tot bijvoorbeeld faciliteiten voor onderzoek of onderzoeksresultaten. Het regelen van accounts en toegang voor al deze partijen is een omvangrijk vraagstuk. Hoe weet je dat iemand toegang mag hebben? En wie regelt dan het account en de toegang? Dit vraagt om een mechanisme waarmee je op een meer granulair niveau toegang kunt verlenen.

Publieke waarden en 'big tech'

Instellingen binnen de HO-sector bieden onderwijs aan en doen onderzoek. Publieke waarden spelen daarbij een belangrijke rol. Deze publieke waarden gaan bijvoorbeeld over gelijkheid, rechtvaardigheid, duurzaamheid en privacy. Afgelopen jaren zijn deze publieke waarden in toenemende mate onder druk komen te staan als gevolg van de belangen van de internationale techreuzen. Privacy van studenten en de onafhankelijkheid van onderwijs en onderzoek zijn geen vanzelfsprekendheid en komen in het geding. De instellingen dienen mede daarom zo veel mogelijk onafhankelijk te zijn van private marktpartijen.

Het lijkt handig: geïnteresseerden die een cursus willen boeken bij een instelling loggen in met hun Microsoft- of Google-account. De platformen van deze partijen bieden single-sign-on en hebben al vele zaken technisch geregeld. Ook zijn ze breed actief in de sector van hoger onderwijs en onderzoek en hebben aantrekkelijke aanbiedingen om dit eenvoudiger te maken. Het verdienmodel van deze (doorgaans niet-Europese) partijen is vaak gebaseerd op inzicht in gedrag van hun miljoenen gebruikers. Daarmee kunnen maatschappelijk breed geaccepteerde doelen worden nagestreefd (zoals inzicht in een pandemie of opsporen van vermisten na een natuurramp), maar de keerzijde is dat inzicht ook commercieel wordt benut, bijvoorbeeld voor gerichte reclame, maatschappelijke profiling of politieke targeting waarvoor geen acceptatie is bij een groeiende groep gebruikers. In Europa is een beweging gaande waarbij steeds meer het besef indaalt dat de privacy hiermee in het geding komt. Eenmaal weggegeven komt privacy niet meer terug. Daarnaast spelen ook vraagstukken die met bedrijfscontinuïteit te maken hebben: zijn de gegevens die ik op het platform van partij X heb opgeslagen wel makkelijk toegankelijk vanaf het platform van partij Y? Kunnen instellingen eigenlijk nog wel bij hun cruciale onderwijs- en onderzoeksgegevens als het contract met zo'n partij wordt verbroken?

Publieke waarden en het individu

De student in de huidige situatie kennen we en geven we binnen de instellingen of via de instellingen toegang tot allerlei faciliteiten die deze nodig heeft voor de opleiding. Gedurende de opleiding wordt er allerlei informatie gekoppeld aan de student. Hiermee wordt een profiel opgebouwd. Waar komt de student oorspronkelijk vandaan? Wat was de vooropleiding? En welke route heeft de student door de opleiding gelopen? En waar is deze na de studie terecht gekomen? Hiermee bouwen instellingen een profiel op van de student gedurende de periode dat deze zich bij de instelling bevindt. Dit opbouwen van een profiel heeft een doel. Bijvoorbeeld om de student beter te kunnen begeleiden tijdens de studie. Bij leven lang leren ontstaat de vraag hoeveel informatie de instellingen nog zouden moeten opbouwen van hun doelgroepen. Ongewenste traceerbaarheid is bij leven lang ontwikkelen een groter vraagstuk dan bij een vierjarige opleiding. Het persoonlijke profiel dat gedurende een vierjarige opleiding is opgebouwd is al redelijk omvangrijk. Bij leven lang ontwikkelen is dit profiel van de lerende nog vele malen uitgebreider. Het risico ontstaat dat er zonder

expliciete aandacht voor privacy en beveiliging op landelijk niveau een volledig profiel ontstaat dat alle onderwijsgegevens van een persoon bevat en waar het individu zelf geen tot weinig controle over heeft. Het adresseren van dit probleem is een van de doelstellingen van deze HOSA-domeinarchitectuur.

Ook binnen onderzoek is privacy van belang. Rondom onderzoek zijn veel stakeholders betrokken. Veel onderzoeken maken bijvoorbeeld gebruik van proefpersonen die onder afspraken van anonimiteit en privacybescherming mee willen doen aan een onderzoek. Daarnaast zijn er vele burgers, journalisten, artsen en anderen die gebruik maken van de resultaten van onderzoek. Ook hier moet privacy goed geborgd worden en mogen bijvoorbeeld derden geen inzicht opbouwen in wie welke wetenschappelijk content heeft ingezien.

Biometrie

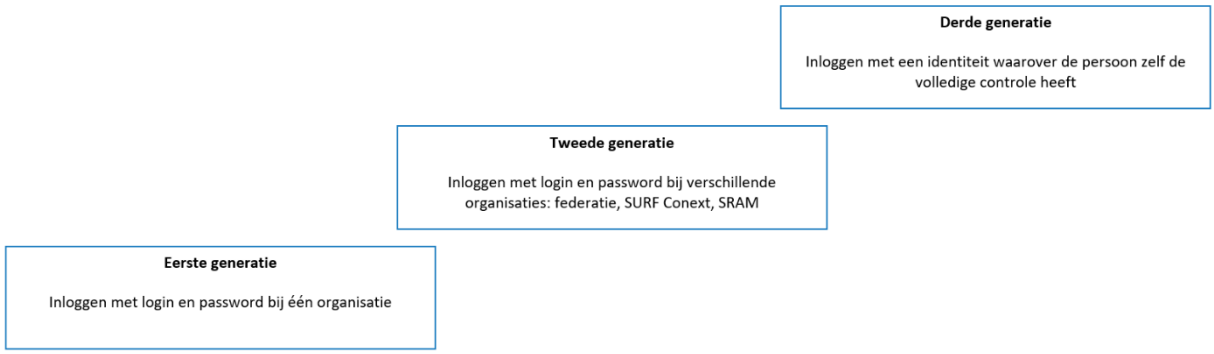
Uitsluitend vertrouwen op een geldige inlog is voor sommige digitale processen onvoldoende. In de fysieke wereld wordt ten behoeve van hoog betrouwbare identificatie vaak direct of indirect gebruik gemaakt van biometrische kenmerken (ben jij degene die op de foto in het paspoort staat). Ook veel digitale processen zijn deels gestoeld op fysieke nabijheid van personen of impliciete controle van biometrische kenmerken. Aanvragen en uitreiken van digitale authenticatiemiddelen vereist veelal fysieke verschijning of een uitgifteproces waarbij fysieke devices een rol spelen.

In een volledig digitale wereld valt een deel van fysieke controles weg. Bij onderwijs op afstand of het inschrijven voor een studie in het buitenland is het praktisch onmogelijk om directe interactie te faciliteren. Gebruik van biometrische kenmerken op afstand biedt dan een mogelijk alternatief. Biometrische kenmerken worden al toegepast bij gebruik van mobiele telefoons of het verkrijgen van toegang tot laptops. Het is aanlokkelijk deze toepassing uit te breiden naar onderzoeks- en onderwijsprocessen die een hoge mate van betrouwbaarheid vereisen, zeker als nationale identiteitsstelsels niet adequaat die hoge betrouwbaarheid kunnen borgen (omdat ze ontbreken, niet erkend zijn of de wettelijke grondslag ontbreekt om ze te mogen gebruiken).

Bij toepassing van biometrie moet echter terdege rekening gehouden worden met de privacy- en securityconsequenties. Het in verkeerde handen raken van biometrische gegevens kan grote, onomkeerbare, gevolgen hebben voor zowel de persoon als voor de beveiliging van organisaties. Gecentraliseerde systemen die biometrische gegevens vastleggen of gebruiken zijn hiervoor zowel vanuit privacy als security fundamenteel ongeschikt, want veel te riskant. Oplossingen waarin biometrische kenmerken worden beheerd en gebruikt op de eigen device lijken voor authenticatie wel geschikt, mits de kenmerken zelf niet worden gedeeld. Een voorbeeld is het vrijgeven van een op de eigen device of in de eigen wallet opgeslagen vertrouwelijke sleutel. Ook bij deze toepassingen geldt een strikt afwegingskader. Dit betekent dat verwerking van biometrische gegevens in beginsel verboden is tenzij hiervoor vrijelijk toestemming is gegeven of inzet van biometrie noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Daarnaast is een aandachtspunt in hoeverre leveranciers van mobiele devices kunnen garanderen dat biometrische gegevens binnen het apparaat blijven.

2.2 Drie generaties van IAM

Een organisatie, bijvoorbeeld een instelling of een bedrijf kan een gebruikersnaam uitgeven aan een burger of klant. De organisatie die deze uitgeeft aan een ander heeft een bepaalde machtspositie. De overheidsorganisatie of bedrijf kan besluiten de gebruikersnaam of bijbehorende rechten weer in te trekken. Hiermee wordt een grote afhankelijkheid gecreëerd van de organisatie of het bedrijf. De persoon zelf is in deze opzet geen eigenaar van de identiteit en heeft weinig zeggenschap erover. Datzelfde geldt voor alle gegevens die aan die identiteit zijn gekoppeld. Wereldwijd is een tegenbeweging gaande waarbij de persoon een eigen identiteit aanmaakt en zelf grip heeft in welke relaties met anderen deze identiteit wordt gebruikt. Dit idee noemen we Self Sovereign Identity. Idealiter heeft de persoon daarbij een identiteit die onafhankelijk is van allerlei formele instanties. Self Sovereign Identity wordt ook wel de derde generatie van Identity and Accessmanagement (IAM) genoemd.



Figuur 2: Drie generaties IAM

De traditionele inrichting van IAM-voorzieningen is gebaseerd op vooraf uitwisselen van gegevens voor identificatie, authenticatie en autorisatie (IAA) binnen de instelling. Dit kan worden gezien als een **eerste generatie** IAM. De uitgifte van toegangsmiddelen, accounts en controle op toegang is hier centraal belegd bij één en dezelfde partij. De identificatie van de gebruiker vindt veelal per instelling plaats, wordt geregistreerd in een bron bij de instelling en deze gegevens worden uitgewisseld met diensten waartoe de gebruiker toegang wenst te hebben. De gebruiker heeft geen kennis en regie over wat precies wordt uitgevoerd met de gegevens. In de dienst (applicatie) worden gegevens opgevoerd voor autorisatie binnen de dienst. De gebruiker krijgt inloggegevens voor toegang tot de dienst.

Het aangaan van federaties van IAM-systemen tussen organisaties kan gezien worden als een **tweede generatie**. Hierbij maken organisaties onderling afspraken om elkaars gebruikers toegang te geven. Uitgifte van toegangsmiddelen en accounts is hier deels gescheiden van de controle op toegang. Techreuzen zijn oplossingen gaan bieden waarmee gebruikers bijvoorbeeld met social login buttons van Facebook of Google kunnen inloggen bij andere dienstverleners. Ook overheden bieden hun burgers vergelijkbare oplossingen aan voor hun dienstverlening, zoals DigiD. De organisaties vertrouwen hierbij elkaar dat ze hun beheer van identiteiten en accounts op orde hebben en geven deze gebruikers dan ook toegang tot de diensten. Hierbij wordt meestal gebruik gemaakt van een trust framework dat uitwisseling van gegevens zowel technisch als juridisch mogelijk maakt. In de HO-sector wordt federatie reeds toegepast met bijvoorbeeld SURFconext en SRAM. Het voordeel hierbij is dat gebruikers met minder accounts gebruik kunnen maken van dezelfde diensten. Voor dienstenleveranciers is een voordeel dat ze relatief dure processen voor uitgifte en het beheer van accounts niet zelf hoeven in te richten. Het nadeel is dat personen afhankelijk zijn van partijen die in staat zijn om hen in hoge mate te volgen in alles wat ze doen. Dit is zeker een issue bij commerciële techreuzen waardoor publieke waarden onder druk komen te staan.

De **derde generatie** van IAM is gestoeld op het concept van Self Sovereign Identity (SSI). In het ideale model hiervan komt het erop neer dat een persoon zelf eigenaar is van de eigen identiteit, controle heeft over waar deze wordt bewaard en zelf beslist met wie hij die identiteit (of onderdelen daarvan) deelt. Ook de mogelijkheid om het gebruik van de identiteit door een ander in te trekken (te revoken) hoort daar bij. De persoon is niet afhankelijk van één centrale partij voor de eigen identiteit. Daarnaast worden principes van privacy-by-design toegepast waardoor de persoon niet gevolgd kan worden. De uitgever van de identiteit ziet namelijk niet waar de identiteit gebruikt wordt om toegang te krijgen. Net zoals de RDW en de gemeente ook niet weten waar de persoon een fysiek rijbewijs heeft laten zien om toegang te krijgen. De HOSA-domeinarchitectuur IAM gaat er van uit dat op termijn Self Sovereign Identity meer gemeengoed gaat worden door mensen in het dagelijks gebruik. Daarmee kunnen we verwachten dat allerlei afnemers van HO-sector zoals leven lang lerenden, proefpersonen of geïnteresseerden in onderzoek gebruik maken van dergelijke voorzieningen.

Een toelichting op SSI

SSI is de onderliggende filosofie die de derde generatie IAM mogelijk maakt. Self Sovereign Identity maakt het mogelijk om autonoom gegevens met hoge mate van zekerheid uit te wisselen. Met deze techniek wordt ook de derde generatie IAM mogelijk: Bring your own ID (ByoID).

Bij de eerste en tweede generatie is er sprake van een grote afhankelijkheid voor de persoon van de andere partij die identiteits- en authenticatiemiddelen verstrekt. Het zijn 'centrale' modellen, waarbij enkele partijen controle hebben over de werking van het geheel. De identiteit én alle kenmerken of attributen leven bij de uitgevende instantie, of bij de partij die authenticatiediensten levert. Deze kunnen bovendien in grote mate volgen wat de persoon doet met de verstrekte middelen. Als deze partij besluit ermee te stoppen of de persoon verliest vertrouwen in de partij, dan verliest de persoon de bijbehorende identiteit en alle gegevens én de mogelijkheid om zich te authenticeren bij dienstverleners die exclusief gebruik maken van de verstrekte middelen.

In het SSI-model, de derde generatie, worden de rollen omgekeerd. Er zijn geen andere partijen dan de persoon zelf die de exclusieve controle hebben over uitwisseling van identiteitsinformatie en daaraan gerelateerde gegevens. De persoon zelf neemt de benodigde informatie mee, en besluit of hij ze wel of niet wil verstrekken aan een dienstverlener. Ongeveer zoals het nu in de fysieke wereld ook is: er is een instantie die paspoorten of rijbewijzen uitgeeft, maar daarna is het document zelfstandig te gebruiken. Credentials zijn essentieel in het model van SSI. Credentials zijn bewijsstukken die iets verklaren over een entiteit. Ze kunnen worden gebruikt als bewijs. De geboortedatum en de pasfoto op een paspoort kunnen gebruikt worden om aan te tonen dat de houder van het paspoort meerderjarig is. Het model van SSI gaat hierin nog een stapje verder. Daar wordt gesproken over verifieerbare credentials. Van een getoond bewijs kan realtime én onweerlegbaar[3] getoetst worden of deze daadwerkelijk is uitgegeven door de uitgever van het bewijs, en of dat bewijs hoort bij de persoon die het toont. Verifieerbare credentials creëren op die manier een basis voor vertrouwen in een digitale wereld.

In het model van SSI heeft een persoon een digitale wallet. Hierin kan de persoon als het ware digitale pasjes bewaren die de persoon gekregen heeft van andere organisaties om iets aan te tonen zoals het bewijs van een lidmaatschap, staatsburgerschap of vaardigheid. Deze pasjes (of de gegevens daarop) worden vaak credentials genoemd. De persoon kan deze pasjes laten zien op het moment dat bijvoorbeeld een organisatie daarom vraagt bij het afnemen van een dienst.

Oplossingen waarbij verifieerbare credentials worden gebruikt bieden een aantal eigenschappen die onderscheidend zijn ten opzichte van de fysieke credentials die we allemaal kennen. De eerste eigenschap is dat verifieerbare credentials 'digital native' zijn, en dus kunnen worden toegepast in situaties waar fysieke credentials onhandig of onbruikbaar zijn. Een tweede eigenschap is dat het model is opgezet vanuit het perspectief van privacy-by-design. De organisatie die vraagt om een bewijs krijgt alleen bewijs voor die specifieke gestelde vraag zonder aanvullende gegevens die onnodig meer prijsgeven over de identiteit. Er wordt bijvoorbeeld aangegeven dat een persoon ouder is dan achttien, maar zonder afgifte van de specifieke geboortedatum. In de fysieke wereld is dit met het paspoort niet mogelijk: om aan te tonen dat je meerderjarig bent, moet je de geboortedatum tonen op een document waarop ook heel veel andere gegevens te zien zijn.

De derde eigenschap is de directe digitale verifieerbaarheid. Bij beantwoording van de vraag wordt meegegeven welke instantie het bewijs heeft afgegeven, inclusief de digitale ondertekening door die instantie. Hiermee kan de organisatie vervolgens toetsen of deze verklaring daadwerkelijk door deze instantie is

[3] Het verschil met een fysieke credential is de onweerlegbaarheid. Een paspoort zit uiteraard vol met echtheidskenmerken, maar slechts een beperkt deel daarvan is 'real-time' te controleren.

afgeleverd, zonder de uitgever van het bewijs daarvoor te raadplegen. De uitgever heeft daarbij niet de mogelijkheid een profiel op te bouwen over de persoon.

Verifieerbare credentials zijn niet alleen bruikbaar voor personen. Ook organisaties, dieren, systemen, natuurlijke objecten en door mensen gemaakte dingen hebben een digitale identiteit, die tot uitdrukking kan komen in credentials[4]. Tussen organisaties en personen kan een veel gelijkwaardiger digitaal proces worden opgestart dan in de huidige situatie, waarbij zowel de organisatie als de persoon zich bij elkaar moeten identificeren. Hiermee kan wederzijds vertrouwen in een digitale wereld worden vormgegeven. Dit in tegenstelling tot de situatie nu waarbij de persoon inlogt bij een website, maar moeilijk kan vaststellen of het gaat om een betrouwbare organisatie. De personen moeten kunnen checken of de site die zich voordoet als 'wetenschappelijk' of 'publieke sector' ook daadwerkelijk betrouwbaar is. Van de personen willen we misschien kunnen checken of het daadwerkelijk personen zijn en geen robots of AI-software. Veel websites maken nu gebruik van Captcha, waarbij je als mens een opdrachtje dient uit te voeren dat voor mensen eenvoudig is, maar voor robots heel lastig (bijvoorbeeld in een raster alle plaatjes met stoplichten moet selecteren.). Dit proces kan gebruiksvriendelijker en betrouwbaarder worden ingericht als een digitaal betrouwbare verklaring 'ik ben een mens' kan worden overlegd.

Wordt alles SSI?

Oplossingen van eerste, tweede en derde generatie zullen komend decennium naast elkaar bestaan. Een cruciaal aspect van SSI is dat het een verandering ondersteunt in de manier waarop identiteit wordt behandeld door bedrijven, gebruikers en overheidsinstanties, en daarmee de weg opent naar vernieuwende vormgeving van bestaande bedrijfsprocessen.

Iedere persoon moet dienstverlening af kunnen nemen van de sector van hoger onderwijs en onderzoek. Dit betekent dat basisdiensten laagdrempelig, maar ook veilig beschikbaar moeten zijn voor alle personen uit de maatschappij. Denk hierbij aan het bezoeken van bepaalde onderzoeksthema's, het gebruiken van open data en publicaties, het oriënteren op onderwijs of het bekijken van kennisclips. Personen kunnen in de gewenste situatie voor laagdrempelige diensten van onderwijs en onderzoek breed terecht in de sector met een eigen Self Sovereign Identity waarmee ze niet meer privacygevoelige gegevens hoeven prijs te geven dan strikt noodzakelijk is. Hierdoor kan vertrouwen en veiligheid worden gecreëerd met behoud van privacy en publieke waarden.

Vanuit publieke waarden is het wenselijk om de mogelijkheden voor instellingsoverstijgend studeren en samenwerken vorm te geven zonder dat deze partijen tot uitgebreide uitwisseling van gegevens over hoeven te gaan. De achterliggende filosofie en principes van SSI worden daarom als leidend genomen in deze domeinarchitectuur. Naast de technologische aspecten zit hier ook een organisatorische verandering voor instellingen aan vast: van een situatie waarin alleen 'eigen' medewerkers en studenten met de 'instellingseigen' identiteiten en toegangsmiddelen (eerste en tweede generatie IAM) gebruik maken van hun faciliteiten en diensten, naar een situatie waar derden en steeds vaker ook deze medewerkers en studenten hun persoonlijke identiteit en middelen meenemen. Hiervoor wordt wel het acroniem Bring Your Own ID gebruikt: BYOID.

Daarnaast is het essentieel om het gebruik van gegevens in de context van IAM te onderscheiden van toepassing van gegevens in daadwerkelijke bedrijfsprocessen. Veel gegevens die nodig zijn voor uitvoering van dienstverlening en onderwijs blijven in de informatiesystemen van de instellingen. Naast interacties waarbij de natuurlijke persoon (in de vorm van zijn 'digital agent', bijvoorbeeld een wallet) direct betrokken is, zullen er ook directe interacties zijn en blijven tussen gegevensbronnen en gegevensgebruikers. In beide scenario's (via

[4] Anders dan 'personen' zijn deze entiteiten natuurlijk niet 'self-sovereign' in de strikte betekenis. Dat laat onverlet dat credentials aan deze entiteiten kunnen worden gekoppeld. In hoofdstuk 5 wordt hier verder op ingegaan.

agent of rechtstreeks) is het noodzakelijk om transparantie te bieden over het gegevensgebruik en de rechtmatigheid daarvan**.**

2.3 Een toepassing op de HO-sector

In de eigen sector zijn er diverse ontwikkelingen die al bewegen richting de concepten van Self Sovereign Identity. Voorbeelden zijn EduMIJ, micro-credentials en EduID. EduMIJ is een idee waarbij een lerende een wallet krijgt waarmee deze bewijs kan leveren van behaalde opleiding of vakken aan potentiële werkgevers. Micro-credentials zijn formeel behaalde credits (EC's) voor behaalde vakken in het onderwijs. Lerenden kunnen deze als bewijs gebruiken voor vrijstellingen. EduID biedt een identiteit aan personen die iedereen zelf kan aanmaken en beheren. Hieraan kunnen bepaalde bewijzen gekoppeld worden, zoals het gegeven dat je werkt of studeert bij een HO-instelling. Nu wordt deze ingezet voor gastgebruik, edubadges en de pilot studentmobiliteit, maar EduID kan ook een opstapbieden naar een HO-brede identiteit.

SSI biedt ook mogelijkheden om de samenwerking tussen organisaties anders vorm te geven. Net zoals een persoon zelf kan beslissen van welke partijen en aan welke partijen deze een credential laat zien, mogen instellingen zelf bepalen aan wie ze de credential verstrekken en aan welke criteria een individu moet voldoen om een credential te ontvangen, en mogen instellingen zelf bepalen welke credentials van welke partijen voldoende betrouwbaar zijn. Deze benadering biedt flexibiliteit die benodigd is om vele verschillende partijen die vaker van buiten de eigen organisatie komen toegang te geven tot bepaalde dienstverlening. Ook houden instellingen hiermee grip op wie ze onder welke condities toegang geven.

De granulariteit die geboden wordt met verifieerbare credentials creëert voor de persoon echter wel het risico op onoverzichtelijkheid. De gebruiker heeft een wallet met potentieel een veelheid aan credentials en dienstverleners vragen daarbij om allerlei verschillende bewijzen. Denken in termen van een conceptuele[5] *digitale* HO-kaart helpt hierbij om overzicht te geven. Een HO-kaart is eigenlijk ook een verifieerbaar credential uitgegeven door een organisatie binnen de sector met als doel om toegang tot bijvoorbeeld online diensten op een efficiënte manier te organiseren. De HO-kaart bevat de meeste regulier benodigde bewijzen en levert daarmee gemak. Voorbeelden in de huidige fysieke wereld zijn een studentenkaart, een campuskaart of een medewerkerspas. Deze kun je net als een rijbewijs tonen om ergens toegang te krijgen. De digitale HO-kaart bevat een set van gegevens die een digitale representatie zijn van een entiteit binnen de HO-sector. Deze entiteit kan voor verschillende situaties een andere set gegevens tonen[6]. Zo kan de HO-kaart voor een onderzoeker anders zijn dan de HO-kaart voor een student.

Iedere persoon die een bredere of meer formele relatie aangaat binnen de sector krijgt in de gewenste situatie een digitale HO-kaart. Hiermee kan de persoon zich binnen en eventueel buiten de sector digitaal identificeren en toegang krijgen tot digitale diensten. De persoon kan de verifieerbare claims op de HO-kaart naar eigen inzicht gebruiken of verborgen houden bij een transactie met een derde partij. Bijvoorbeeld de claim dat deze ingeschreven staat voor een vak. Ook claims van organisaties buiten de sector kunnen worden opgenomen in de HO-kaart. Wie wel of geen HO-kaart krijgt moet nog worden bepaald, maar een voorbeeld zou kunnen zijn dat een persoon die voor plezier open onderwijs bekijkt geen HO-kaart krijgt, terwijl wanneer de persoon aangeeft een microcredential te willen halen voor één vak dan wel een HO-kaart moet aanmaken.

[5] Conceptueel, omdat het niet vanzelfsprekend is dat een digitale HO-kaart als zelfstandig herkenbaar digitaal object zal worden uitgerold. De beoogde functionaliteit uit zich eerder in een afsprakenstelsel binnen de (internationale) HO-sector waarbij de betrokken instellingen de door of namens andere instellingen uitgegeven credentials herkennen en erkennen.

[6] In het VC-datamodel wordt hier gesproken over 'persona': dat deel van de volledige identiteit dat een subject wil tonen in een specifieke context.

Om te kunnen bepalen welk vertrouwen een ontvanger of dienstaanbieder kan stellen in de HO-kaart is er een HO-kaart vertrouwensraamwerk. Het betrouwbaarheidsniveau van de HO-kaart wordt bepaald door de mate van zekerheid die in de gebruikersidentificatie, het authenticatiemiddel en de attributen zijn vastgesteld. Bijvoorbeeld een dienstaanbieder die een zeker besluit wil nemen zoals toegangsverlening tot een bepaalde online dienst of de uitgifte van een diploma heeft gegevens nodig die valide zijn voor dat type besluit. De criteria die de dienstaanbieder hiervoor gebruikt kan en moet deze zelf vaststellen. Dat is ingewikkeld, want hoe kun je weten of de gegevens betrouwbaar genoeg zijn? Om de dienstverleners tegemoet te komen wordt een vertrouwensraamwerk ingericht zodat het voor dienstverleners makkelijker wordt om de validiteit van gegevens die onder zo'n raamwerk worden uitgewisseld en nodig zijn voor een zeker besluit vast te stellen.

Een persoon kan meerdere rollen vervullen, tegelijkertijd of opeenvolgend. Iemand kan student, onderzoeker (stage of afstudeeronderzoek) en werknemer (student-assistent) tegelijk zijn. Gedurende het leven kan iemand wisselen van rol of tijdelijk een extra rol krijgen, bijvoorbeeld een werknemer van een bedrijf die meewerkt aan het onderzoek van een HO-instelling. De sectorvoorzieningen van de toekomst moeten faciliteren dat de persoon de credentials heeft die passen bij zijn rollen op dat moment de daarbij horende credentials kan benutten. Een onderzoeker die stopt bij een instelling zou bijvoorbeeld een verifieerbaar bewijs mee moeten kunnen nemen van de publicaties die op de eigen naam staan, maar in een instellingswallet zijn opgenomen. Een verifieerbaar credential (mits niet ingetrokken) zou dan over te dragen moeten zijn naar een eigen wallet. Hieruit volgt dat de vorm van de credentials niet afhankelijk mag zijn van de gekozen wallet, en dat er interoperabiliteit en overdraagbaarheid tussen wallets moet zijn.

De HO-kaart werkt in de gewenste situatie in combinatie met andere authenticatiemiddelen waarmee bij uitgifte van credentials of bij gebruik van credentials bij digitale diensten kan worden geverifieerd of diegene die zegt een bepaald persoon te zijn dat ook daadwerkelijk is. In de meeste gevallen zal dit niet nodig zijn en zal de HO-kaart afdoende zijn voor authenticatie. Bij het afnemen van een examen kan bijvoorbeeld nog een aanvullende identiteitscontrole nodig zijn via bijvoorbeeld een (digitale) ID-kaart of paspoort.

De HOSA IAM-domeinarchitectuur beperkt zich niet tot een natuurlijk persoon binnen HO-sector. Ook objecten uit de natuur of door mensen gemaakte zaken krijgen in toenemende mate te maken met dat zij zich moeten kunnen identificeren en bepaalde bewijzen moeten kunnen overleggen. Voorbeelden hiervan zijn websites die moeten bewijzen dat ze betrouwbaar zijn en geen phishing-site, datasets of publicaties die hun authenticiteit moeten kunnen aantonen of onderdelen van IoT-netwerken voor onderzoek die zichtzelf moeten kunnen identificeren. Deze onderwerpen lijken nu nog ver weg te liggen, maar bij een verandering van paradigma moeten deze wel meegenomen worden in uitgangspunten die de fundamentele basis gaan leggen voor de technologie.

2.4 De volwassenheid van de technologie en initiatieven

Een paradigmaverandering is niet mogelijk zonder volwassen technologie. De belangen rondom privacy en publieke waarden zijn echter dusdanig groot dat deze domeinarchitectuur hierop voorsorteert in de visie en onderliggende modellen.

SSI is nog volop in ontwikkeling en standaarden zijn nog niet uitgekristalliseerd. Hierdoor zal toepassing op grote schaal nog circa twee tot vijf jaar op zich laten wachten. De meeste bijbehorende technologische concepten zoals distributed computing en cryptografie bestaan jaren en zijn volwassen. De complexiteit zit onder andere in de samenhang waarin de technologieën worden toegepast.

SSI maakt in veel van de huidige implementaties gebruik van Distribute Ledger Technology (DLT). Blockchain is een veelvoorkomend architectonisch onderdeel van SSI-oplossingen. Het gebruik van distributed ledger-technologie zoals blockchain is relatief nieuw met als bekendste toepassing de crypto currencies zoals Bitcoin. Het gebruik van blockchain als cruciaal onderdeel van SSI is niet onomstreden. Het onderzoeksbureau Gartner verwacht dat de technologie tussen 2023 en 2025 een staat van volwassenheid bereikt waarbij brede adoptie

gaat plaatsvinden. Vergelijkbare signalen zijn er vanuit NIST dat aangeeft dat blockchain based identity een fundamenteel architectuurcomponent kan worden van het internet van morgen, maar dat onderwerpen zoals schaalbaarheid, security en privacy goed vertaald moeten worden naar oplossingen.

De W3C-standaarden voor verifieerbare credentials schrijven niet voor hoe de technische realisatie precies wordt ingevuld. goed mogelijk om een SSI-infrastructuur zonder blockchain of andere vorm van distributed ledger te implementeren. Het geheel van de onderliggende samenwerkende technologieën voor SSI is op dit moment niet volledig volwassen om breed in te zetten in de sector. Vraagstukken bestaan bijvoorbeeld nog rondom het intrekken van credentials en mogelijkheden om in te loggen wanneer je offline bent. Ook zijn gebruikersapplicaties nog niet ingericht om te kunnen omgaan met just-in-time provisioning.

Wel zijn er diverse indicatoren dat er breed geïnvesteerd wordt om deze technologie breed toegepast te krijgen. Techreuzen zijn bezig met het ontwikkelen van oplossingen en er verschijnen vele wallets vanuit allerlei leveranciers. Vooralsnog zijn het veel losse initiatieven die leiden tot veel verschillende wallets en protocollen. Organisaties zoals SOVRIN, ToIP, DIF en de OpenID Foundation ontwikkelen modellen, technologie en best practices. Ook zijn wereldwijde standaardisatieorganisatie zoals W3C en NIST bezig met het definiëren en verdiepen van de benodigde standaarden. Dit gaat echter langzaam en vooral de benodigde protocollen zijn nog niet gestandaardiseerd. In Nederland hebben TNO, DUO en SURF eerste ervaringen opgedaan in een experimentele omgeving. Onder druk van o.a. EU-initiatieven rondom wallets en Europese identiteit is convergentie naar toepasbare, samenhangende afsprakenstelsels te verwachten.

Tegelijkertijd zien we dat veelbelovende ontwikkelingen voor de flexibilisering van de sector, zoals rondom microcredentials en open badges ook plaats kunnen vinden zonder een volledige SSI-infrastructuur. Het is niet nodig om te wachten, wel is het nodig om uit te werken hoe de ontwikkelingen aan elkaar kunnen worden gerelateerd.

In de VS zijn verschillende initiatieven zoals Sovrin. Sovrin zou een voorziening voor IAM dienstverlening kunnen worden waarmee wereldwijd self sovereign identities kunnen worden aangeboden. Bedrijven en overheden uit de hele wereld mogen hier tegen betaling gebruik van maken. Het risico is echter dat Europa te afhankelijk wordt van de VS. Een identiteit-infrastructuur wordt gezien als een nutsvoorziening of kritieke infrastructuur voor een land. In Europa wordt dit herkend en zijn er initiatieven ontstaan om eigen identiteitsvoorzieningen te realiseren voor Europa.

De EU en de Nederlandse overheid investeren in identiteitsinfrastructuren die kernwaarden als privacy, autonomie grensoverschrijdende bruikbaarheid voorop stellen. Dit uit zich in voorstellen voor een vernieuwd wettelijk kader in de vorm van (aangepaste) verordeningen en wetgeving zoals eIDAS en de wet Digitale Overheid, waarbij parallel programma's en pilots worden opgestart om de (technische) mogelijkheden van credentials, wallets en regie op gegevens te verkennen.

De Nederlandse overheid ziet in haar visie op digitale bronidentiteit voor zichzelf een cruciale betrouwbare rol als 'uitgever' van digitale bronidentiteit (DBI) voor burgers, vergelijkbaar met de rol bij het uitgeven van paspoorten en identiteitsbewijzen. Deze opvatting kan wringen met het gedachtengoed van SSI, want het risico is dat hiermee de digitale identiteit exclusief wordt uitgegeven door een centrale partij. Het SSI-model laat zien dat een centrale uitgifte van een identiteit niet nodig is. De Nederlandse overheid als 'issuer' van credentials over de identiteit van een burger past prima binnen SSI, en daar kan ook prima gebruik van worden gemaakt in situaties waar een hoog niveau van vertrouwen vereist is[7]. Hier zal dan een relatie gelegd kunnen worden tussen de de HO-kaart met de digitale bronidentiteit. Denk aan de inschrijving voor onderwijs of de uitgifte van een diploma. Voor processen waar dit niet vereist is moeten andere identiteiten van andere

[7] Waarbij wel rekening dient te worden gehouden met de situatie dat in het HO een substantieel deel van de populatie niet de Nederlandse, en zelfs niet een Europese nationaliteit heeft.

issuers gebruikt kunnen worden. Om het risico op ongewenste correlatie van persoonsgegevens en ongewenst volgen van personen te voorkomen is dat zelfs noodzakelijk.

Vanuit de sector is het van belang om deze ontwikkelingen goed te volgen en er op aan te sluiten. Hiermee hoeft de sector niet alle infrastructuur en technologie zelf te ontwikkelen, maar kunnen delen van nationale en internationale organisaties en initiatieven zoals IRMA ingezet worden. De sector kan hiermee de nadruk leggen op welke criteria ze stelt aan wallets en het organiseren van de uitgifte van credentials die breed bruikbaar zijn.

3 Use cases

Voor het verduidelijken van de werking van IAM in relatie tot de beoogde methodiek wordt in een aantal use cases een aantal voorbeelden geschetst voor onderwijs en onderzoek. Binnen deze beschrijvingen wordt soms gebruik gemaakt van termen die binnen bepaalde vakgebieden een vaste definitie hebben. De bedoeling van de use cases is niet om het bovenliggende bedrijfsproces volledig correct te beschrijven, maar om duidelijk te maken hoe verifieerbare credentials en een decentrale identiteit daarin een rol kan spelen. Om dezelfde reden zijn niet alle mogelijke variaties uitgewerkt. Daarnaast zien we in de use cases terug dat niet alleen personen een houder kunnen zijn van identiteiten met bepaalde rollen en attributen, maar dat dit ook geldt voor diensten, apparaten en gegevens die door organisaties worden aangeboden.

3.1 Use cases onderwijs

Use case: Oriëntatie op onderwijs

Iemand is geïnteresseerd in een bepaalde opleiding, bijvoorbeeld na het bezoeken van een beurs of een onderwijskeuze-website, en wil daarom contact onderhouden met een onderwijsaanbieder. De persoon wil nog geen diepgaande relatie aangaan, maar alleen in staat zijn om de onderwijsaanbieder te kunnen volgen. Het liefst wil de persoon hierbij zoveel mogelijk anoniem blijven. De persoon vindt het goed dat de instelling af en toe berichten met informatie stuurt, en daarvoor over de noodzakelijke informatie beschikt, maar liever geeft deze geen adresgegevens, leeftijd en andere persoonsgegevens prijs voor deze basisconnectie.

Door toepassing van SSI is dit mogelijk. De persoon bezit een wallet, waarin o.a. contactgegevens als credential zijn opgeslagen. De persoon scant met een smartphone de QR-code die getoond wordt in de informatieve omgeving van de onderwijsaanbieder (bijvoorbeeld een beursstand of een pagina op een onderwijskeuze-website). De QR-code linkt naar een website die een sessie met de persoonlijke wallet initieert. Na inloggen van de persoon in zijn wallet wordt n een dialoog gevraagd om een minimale set contactgegevens (emailadres of telefoonnummer), waarbij het beoogde gebruiksdoel ‘ontvangen van opleidingsinformatie’ duidelijk wordt aangegeven. Indien de persoon akkoord is, geeft hij een consent af waar in gebruiksdoel en gebruiksduur zijn opgenomen. De instelling heeft nu gevalideerde contactinformatie en bevestigt dit via het opgegeven contactadres.

Indien de persoon niet over een wallet beschikt, zal de dialoog worden afgewikkeld op een website van de onderwijsaanbieder. Omdat de contactgegevens dan niet uit een geverifieerde bron komen, zal een extra stap nodig zijn, bijvoorbeeld het bevestigen van het e-mailadres voordat informatie wordt verstuurd.

Net als bij het communiceren met banken, zal het voor een persoon ook van belang zijn om zekerheid te hebben of hij heeft te maken met een echte universiteit of hogeschool. Een persoon kan zo bijvoorbeeld weten of deze te maken heeft met een betrouwbare instelling of dat het om phishing gaat waarbij criminelen zich voordoen als een instelling. Een correct geïmplementeerde infrastructuur voor verwerken van verifieerbare credentials maakt deze controles mogelijk en legt daarmee een basis voor wederzijds vertrouwen.

Technisch:
Een persoon kan met een digitale wallet gegevens verzamelen vanuit verschillende (vertrouwde) bronnen. Deze gegevens kunnen worden getoond/afgegeven wanneer daar om wordt gevraagd. De persoon kan zelf selecteren welk gegevens uit de wallet worden getoond. Bij de vraag rond

het emailadres kan de persoon dus zelf selecteren welk adres van vertrouwde gegevens die in de wallet zitten wordt afgegeven.

Voor het uitwisselen van wederzijdse credentials zijn verschillende technieken voorhanden. Zo zou het kunnen op basis van DLT's of middels peer-DID's (en bijbehorende DIDComm's).

Use case: Volgen van een enkel vak

Een persoon heeft de eigen oriëntatie voltooid en wil een enkel vak volgen bij een onderwijsinstelling binnen de HO-sector. Deze instelling wil laagdrempelige toegang bieden voor losse vakken en vraagt daarom slechts gegevens van de persoon op het moment dat dit vereist is. Deze instelling biedt de mogelijkheid voor geïnteresseerden om eerst het studiemateriaal online in te zien. Dit vanuit de gedachte van open onderwijs.

De persoon meldt zich aan via een online catalogus. Hiervoor gebruikt de persoon een 'code' die deze gekregen heeft tijdens een onderwijsbeurs. Hiermee wordt direct een link gemaakt en is de persoon (beperkt) bekend bij de instelling. De persoon krijgt een link en heeft hiermee direct toegang tot het vak in de digitale leeromgeving van de instelling. De persoon is door het studiemateriaal zo geïnteresseerd geraakt dat deze besluit het vak te volgen.

Het vak start met een aantal online colleges. Om toegang te krijgen wordt gevraagd om een betaling vooraf. De persoon klikt op de button om het eerste gedeelte van de online colleges te volgen en deze te betalen. De persoon betaalt via de landelijke infrastructuur vanuit het studietegoed. Als betalingsbewijs krijgt de persoon een betalingsbewijs-credential. De persoon toont het credential vanuit z'n digitale wallet bij de digitale leeromgeving van de instelling en krijgt toegang tot de online colleges.

De persoon wil graag het certificaat voor het vak behalen en besluit dat tentamen te doen. De instelling wil bij het afnemen van het tentamen met zekerheid kunnen vaststellen om wie het gaat. Er is een hoger niveau van betrouwbaarheid vereist. De persoon krijgt het verzoek om een credential te tonen die de persoon met een hogere mate van betrouwbaarheid identificeert, bijvoorbeeld gebaseerd op een authenticatie met een middel dat gekoppeld is aan zijn nationale bronidentiteit. Hiermee kan de instelling de resultaten van de toets met hoge betrouwbaarheid koppelen aan de persoon.

Na het slagen voor het tentamen en het voldoen aan alle vereisten heeft de persoon het certificaat behaald. De instelling geeft het certificaat uit in de vorm van een verifieerbare microcredential. De persoon kan hiermee bij derden aantonen dat deze het vak heeft behaald.

Technisch:

Een persoon kan met een digitale wallet gegevens verzamelen vanuit verschillende (vertrouwde) bronnen. Deze gegevens kunnen worden getoond wanneer daar om wordt gevraagd. De persoon kan zelf selecteren welk gegevens uit de wallet worden getoond. Wanneer gevraagd wordt om een identificatiebewijs (van de overheid) kan de persoon zelf een keuze maken uit de digitale wallet. Hieraan wordt verbonden dat de resultaten aan de persoon achter dat betreffende credential worden uitgegeven. In een later proces kan dus ook een ander identiteitsbewijs worden gebruikt.

Indien iemand meerdere nationaliteiten heeft, zijn er meerdere issuers van een nationale identiteit. Deze kunnen als afzonderlijke credentials zijn opgenomen. Het is aan de holder om te kiezen welke deze wil gebruiken en aan de verifier om duidelijk te maken welke deze kan accepteren.

Use case: Onboarding voor een HO-opleiding

De persoon heeft zijn toelatingsdiploma voor het HO met succes behaald en wenst zich aan te melden bij een opleiding van een onderwijsinstelling. In de huidige situatie verloopt dit via Studielink. Dit is onder andere vanwege het terugdringen van de hoge kosten voor onboarding wanneer elke instelling dit afzonderlijk zou regelen. In het huidige proces worden een aantal checks gedaan. Met verifieerbare credentials zijn deze checks op termijn efficiënter en eventueel volledig gedigitaliseerd uit te voeren. Daarbij wel gebruikmakend van een landelijke sectorvoorziening zoals Studielink.

Bij Studielink worden in de huidige situatie door instellingen gegevens gevraagd als aanspreeknaam, emailadres en telefoonnummer. Deze gegevens kunnen in de gewenste situatie met een SSI-infrastructuur als credentials worden uitgegeven aan de persoon en vervolgens kan deze persoon de gegevens bewust verstrekken aan de instelling.

Bij de onboarding zal gevraagd worden of deze persoon reeds een HO-kaart heeft. Deze HO-kaart bevat een aantal identificerende attributen en verifieerbare credentials die de persoon binnen of buiten de HO-sector kan tonen[8]. Denk bijvoorbeeld aan bewijs dat de persoon een student is of bewijs dat de persoon vakken heeft gehaald. De HO-kaart biedt de mogelijkheid om alleen de gegevens te verstrekken die nodig zijn voor de onboarding. De persoon kan bijvoorbeeld laten zien dat deze student is, zonder een burgerservicenummer of de naam van de opleiding of de instelling prijs te geven als dat niet nodig is[9].

Indien de persoon nog geen HO-kaart heeft, kan deze worden aangemaakt bij de sectorale onlinevoorziening. Daarbij kan deze persoon aangeven met welke digitale identiteit deze een connectie wil leggen naar de HO- kaart. Hiervoor kan de Digitale Bronidentiteit (DBI) worden gebruikt of een ander vertrouwd identiteitenstelsel. Deze connecties zijn alleen bij de persoon bekend en worden niet onnodig prijsgegeven.

Daarnaast worden diverse andere zaken gecheckt in het proces. In het proces wordt gevraagd om aan te tonen welke vooropleiding is gedaan. Op termijn kan hier een verifieerbaar credential worden aangeleverd. Een ander voorbeeld is bij buitenlandse deelnemers om aan te tonen dat er voldoende beheersing van de Nederlandse taal (bijvoorbeeld op niveau NT2) is. Hier kan op termijn bijvoorbeeld een verifieerbaar credential van NT2 voor worden aangeleverd, mogelijk in de vorm van een in de sector reeds breed bekende microcredential. Ook Nuffic zou verifieerbare credentials kunnen uitgeven over de gelijkwaardigheid van buitenlandse opleidingen die personen kunnen gebruiken in het proces van inschrijving. Het kenmerk van deze verifieerbare credentials is dat bijvoorbeeld Studielink kan toetsen of de credentials daadwerkelijk zijn uitgegeven en niet zijn ingetrokken. Dit kan worden gedaan zonder dat Nuffic of een andere issuer op de hoogte is dat deze toets wordt uitgevoerd. Hiervoor is het proces ingeregeld volgens de principes van privacy-by-design, waarbij alleen gegevens worden uitgewisseld die voldoen aan het beoogde doel voor verwerking.

Het proces voor digitaal inschrijven bij een onderwijsinstelling maakt het mogelijk om de persoon uniek te verifiëren. Wanneer de verificatie goed is verlopen, kan de instelling de persoon als student registreren. Aan de HO-kaart van de student wordt nu de verifieerbare credential van de opleiding gekoppeld, zodat de persoon de bewering kan toevoegen dat deze staat ingeschreven aan de betreffende opleiding van de onderwijsinstelling.

[8] De HO-kaart representeert dus in termen van het Verifiable Credentials datamodel de ‘HO-persona’, dat deel van de volledige identiteit dat een persoon kan tonen om zich bekend te maken in de HO-sector.

[9] Binnen de huidige wetgeving zal een BSN al snel nodig zijn, en moet Studielink er om vragen vanwege de koppeling met DUO en diverse wettelijke controleprocessen.

Een persoon wenst een aantal jaar na een afgeronde opleiding opnieuw te starten met een studie naast het werk. De persoon heeft nog de HO-kaart en de daaraan gerelateerde credentials. Bij de sectorale voorziening kan de persoon zijn nationale identiteit opnieuw koppelen aan de HO-identiteit. De persoon meldt zich aan bij de opleiding zoals eerder toegelicht. Hiervoor stelt de persoon de instelling via de landelijke sectorvoorziening in kennis van bepaalde HO-kaart gegevens. De instelling kan vertrouwen dat de credentials van de afgeronde opleiding nog steeds geldig zijn.

Technisch:

Een persoon kan met een digitale wallet gegevens verzamelen vanuit verschillende (vertrouwde) bronnen. Voor gegevens die betrekking hebben op onderwijs en onderzoek in de HO-sector worden deze gegevens uitgegeven als verifieerbare credentials die in verschillende wallets kunnen worden ingelezen. De wallets kunnen er vervolgens voor zorgen dat een selectie van attributen uit de credentials als verifieerbare presentatie worden aangeboden aan een verifier. Deze presentaties bevatten uitsluitend die gegevens die nodig zijn en die de holder wil verstrekken. Hiermee kan per verifier een op maat gesneden attributenset worden verstrekt. Dit speelt o.a. bij het bewijzen dat iemand nog een actieve inschrijving heeft als student voor het rechtmatig huren van studenthuisvesting. Daarvoor hoeven slechts beperkte persoonsgegevens uitgewisseld te worden en kan er periodiek een credential worden overhandigd die de actuele status van studeren bewijst.

Use case: Internationale student wil weten of een Nederlandse opleiding geaccrediteerd is

Een internationale student op een buitenlandse onderwijsbeurs moet kunnen zien of een opleiding is geaccrediteerd volgens de Nederlandse overheid. Een SSI-infrastructuur kan hierbij helpen. De officiële status van de opleiding worden bevraagd via een verifieerbare credential van de opleiding. De formele producten in de HO-sector zoals een opleiding kunnen worden gezien als subject waarop de credentials betrekking hebben.

De internationale student gebruikt de QR-code die wordt aangeboden in de stand op de beurs. De Nederlandse instelling vraagt om enkele credentials van de internationale student en de internationale student vraagt om enkele credentials van de instelling. De instelling weet nu dat ze te maken heeft met een echte persoon, zonder dat deze de volledige privacy hoeft prijs te geven. De internationale student weet dat deze te maken heeft met een echte, betrouwbare instelling.

Na het leggen van deze verbinding maakt de internationale student gebruik van de service van de instelling om op te vragen of een opleiding geaccrediteerd is. De chatbot vraagt om welke opleiding het precies gaat. De chatbot toont een bewijs dat de opleiding inderdaad geaccrediteerd is. Het bewijs bevat een sleutel die de ‘agent’ (app op smartphone) van de internationale student kan gebruiken om op de achtergrond te checken of het getoonde bewijs echt is volgens de uitgever van het bewijs.

De uitgever van het bewijs dat de instelling toont betreft een overheidsinstantie (in dit voorbeeld NVAO[10]). Deze heeft het bewijs beschikbaar gesteld aan de instelling en ondertekend. Daarnaast heeft deze in een openbare registry (bijvoorbeeld DUO) gepubliceerd dat dit bewijs daadwerkelijk is uitgegeven. De agent van de internationale student checkt of het bewijs voor de opleiding die deze wil volgen daadwerkelijk is uitgegeven. Dit blijkt het geval en de opleiding heeft het bewijs geleverd geaccrediteerd te zijn.

[10] Nederlands-Vlaamse Accreditatieorganisatie

Use case: Student woont naast een andere campus

In de stad waar de student studeert is het moeilijk om een kamer te krijgen om te wonen. De student heeft wel een andere kamer gevonden op directe loopafstand van een campus van een andere instelling. Deze instelling biedt veel losse cursussen aan en heeft daardoor ook goede faciliteiten voor personen die daar niet een volledige studie volgen.

De student vindt het prettiger om in een omgeving met anderen te studeren en verblijft daarom graag op de campus die op loopafstand is. Om gebruik te kunnen maken van de faciliteiten wil deze instelling wel graag een bewijs ontvangen dat de student een Nederlandse studie volgt. Deze scant een QR-code op de campus en wordt verwezen naar een online portaal. De student toont met enkele gegevens van de digitale HO-kaart uit de wallet aan dat deze onderwijs volgt bij de andere instelling in Nederland. Dit wordt op de achtergrond geautomatiseerd geverifieerd. De student kan nu bijvoorbeeld een studieplek reserveren en heeft toegang tot de bibliotheek.

Na enkele maanden heeft de student de eerste vakken gehaald van de opleiding. De gekozen opleiding heeft een relatief vaststaand curriculum en biedt op meerdere momenten de mogelijkheid om zelf vakken te kiezen. Aankomende periode heeft de opleiding ruimte in het curriculum voor het volgen van extra vakken, eventueel bij andere instellingen. De student heeft inmiddels gevoel gekregen voor het profiel van de campus van de instelling die zich op loopafstand bevindt.

De student besluit zich voor een vak bij deze instelling aan te melden. De student meldt zich aan bij de instelling met de eigen HO-kaart. Er wordt een digitale verificatie uitgevoerd of de beweringen over de status van de student correct zijn. Wanneer de verificatie correct is wordt de digitale identiteit als gaststudent van de tweede instelling uitgereikt en als credential gekoppeld aan de wallet. Op basis van de identiteit als gaststudent op de HO-kaart kan de student nu een studievak selecteren om te volgen. De student krijgt nu toegang tot het studievak op basis van deze digitale identiteit als gaststudent.

Technisch:

Voor de fase waarin de student als gewone gast op de campus van een andere instelling rondloopt, is er geen uitwisseling nodig met de bronsystemen van de thuisinstelling. Alle benodigde gegevens kunnen op dit moment als credential of presentation worden overhandigd door de student. Ook eventuele aanvullende attributen die de gastinstelling nodig heeft (zoals een telefoonnummer of e-mailadres) kunnen direct uit de wallet worden verstrekt.

Bij het aanmelden als student bij een andere instelling, dienen er gegevens uitgewisseld te worden met de hoofdinstelling van de student. Hierbij wordt gebruik gemaakt van sleutels die door de student worden aangeleverd en onder verklaring van consent mogen worden gebruikt om tussen de twee instellingen gegevens uit te wisselen. Hiermee wordt o.a. geregeld op welke wijze er gebruik kan worden gemaakt van onderwijstegoed (zie verderop).

Use case: Leven Lang Ontwikkelen (LLO)

Een professional is vijftien jaar geleden afgestudeerd en is sindsdien werkzaam in het bedrijfsleven. Zij heeft afgelopen zes jaar veel losse vakken gevolgd en daarvoor microcredentials ontvangen. Deze microcredentials zijn in haar persoonlijke wallet opgeslagen. De professional vraagt zich af of de optelsom van al deze behaalde vakken reeds een diploma waard is en welke vakken er nog resteren om een diploma te kunnen krijgen.

Een instelling die modulair onderwijs aanbiedt biedt een app aan waarmee lerenden kunnen nagaan in welke mate zij nog verwijderd zijn van een diploma van die instelling. De professional downloadt de app en start een dialoog. De persoon kan met de gegevens uit de persoonlijke wallet eenvoudig de gevraagde

bewijzen verstrekken. Hierbij hoeven geen privacygevoelige gegevens te worden verstrekt, de claim dat alle microcredentials verbonden zijn aan dezelfde persoon is voldoende.

De app geeft aan dat er een behoorlijke match is met een bepaalde opleiding en geeft bij benadering het aantal vakken en uren die nog resteren op basis van het getoond vakkenpakket. De app vraagt of de persoon een gesprek wil plannen met een studiecoach. Na het gesprek volgt een advies, waarmee de professional akkoord gaat. De studiecoach stuurt het advies en de verzamelde microcredentials digitaal aan de examencommissie van de betreffende opleiding. Deze gaat akkoord en de secretaris van de examencommissie genereert een digitaal toelatingsbewijs voor de opleiding, tezamen met de verstrekte vrijstellingen in de vorm van verifieerbare credentials.

De persoon gaat naar de landelijke sectorvoorziening voor het aanmelden voor de betreffende opleiding. Deze herkent de persoon via gegevens uit de HO-kaart. De persoon kan aan de hand van het digitaal toelatingsbewijs aantonen dat de opleiding akkoord is met zijn inschrijving. Vervolgens kan de sectorvoorziening de persoon verder begeleiden bij het formaliseren van zijn inschrijving.

Use case: Aantonen van vereiste kwalificaties

Een persoon kan bij het communiceren met bedrijven en overheid gevraagd worden om een verifieerbaar bewijs van een diploma of een aantal vakken, bijvoorbeeld bij een sollicitatie of aanvragen van een vergunning. Een persoon beschikt over een wallet waarin deze behaalde diploma's voor opleidingen en microcredentials voor vakken bewaart. Vanuit de wallet kunnen benodigde attributen als verifieerbare credential worden verstrekt. De SSI-infrastructuur zorgt ervoor dat de ontvanger de verklaring kan verifiëren. De uitgevende instelling wordt niet op de hoogte gebracht wanneer een derde partij een credential verifieertUse case: Gebruiken onderwijstegoed
Een professional meldt zich aan voor een cursus. Hij voldoet aan alle vooropleidingsvereisten en heeft ook de voorselectie succesvol doorlopen. Hij kan aan de opleiding beginnen zodra ook de kosten zijn voldaan. Van de overheid heeft hij een leven lang leren-budget gekregen dat hem recht geeft op het volgen van één cursus. Dit staat in de vorm van een credential ('tegoed voor één cursus') in zijn wallet. Hij biedt deze credential aan bij de opleiding. Deze verifieert of de credential van toepassing is op de gekozen opleiding en of deze nog geldig is (niet eerder gebruikt en niet verlopen). Als dat het geval is, mag de professional de cursus starten.
NB: de exacte invulling van de financiële bedrijfsprocessen rondom deze use case valt buiten de scope van het domein IAM. Er zijn verschillende betaalmethoden (bankbetaling, direct afrekenen met onderwijscredits, inwisselen van een studiebudget, eenmalige tegoedbon, vooraf betaald collegegeld, verrekening met studiebudget werkgever) als verschillende mechanismen voor verrekening tussen instellingen (via centrale partij, door bilaterale afspraken, etc.) Ook moet goed nagedacht worden over de wijze waarop de hoogte van een tegoed wordt bijgehouden. In alle gevallen is een (vertrouwde) tussenpartij ('clearing house') die privacyvriendelijk de voorraad studiegoed beheert hier noodzakelijk.

3.2 Use Cases Onderzoek

Burger wil deelnemen aan onderzoek als proefpersoon

In het nieuws komt een bericht over een onderzoek waarbij gezocht wordt naar proefpersonen. Geïnteresseerden kunnen zich op een bepaalde site aanmelden. Een geïnteresseerde zoekt de site op en controleert dat het gaat om een betrouwbare website, onder andere door na te gaan of deze betrouwbare verifieerbare credentials heeft. De SSI-infrastructuur ondersteunt daarbij door verifieerbaar te maken wie er achter de website zit.

De site toont algemene informatie over het betreffende onderzoek en heeft een digitaal certificaat waarmee de geïnteresseerde kan zien dat het een officieel erkend onderzoekstraject betreft. In dit geval is dat een getoonde credential die is uitgegeven door de Nederlandse Organisatie voor

Wetenschappelijk Onderzoek (NWO). De geïnteresseerde is bekend met NWO en gaat ervan uit dat het gaat om een betrouwbaar onderzoeksproject.

De geïnteresseerde besluit zich aan te melden. Daarop wordt vanuit de site gevraagd om enkele gegevens aan te leveren die middels credentials vanuit de wallet van de persoon kunnen worden getoond. Voor het onderzoek is het voldoende om een verklaring van 21+ te ontvangen en een sleutel van uniek persoon, zodat een persoon zich niet via verschillende kaarten (zoals bank, rijbewijs, etc.) meerdere keren als proefpersoon aan kan melden. De persoon hoeft geen leeftijd op te geven om aan te tonen dat deze ouder is dan eenentwintig. Hiervoor kan een credential gebruikt worden dat aangeeft dat de persoon ouder is dan eenentwintig en welke instantie hiervoor instaat.

Hoewel het onderzoek anoniem is, geeft de geïnteresseerde aan dat hij wel informatie over de onderzoeksresultaten wil ontvangen. Hiervoor kan hij vanuit zijn wallet geverifieerde contactgegevens achterlaten. De onderzoeksinstelling draagt er zorg voor dat de contactgegevens en instemming voor het gebruik van de verstrekte gegevens strikt gescheiden blijven van de eigenlijke onderzoeksdata. Na afloop van het onderzoek worden de resultaten gedeeld met de geïnteresseerde. Aangezien de onderzoeksdata gescheiden is gebleven van de contactgegevens kan dit zonder de koppeling tussen geïnteresseerde en zijn aangeleverde onderzoeksdata te leggen.

Citizen scientist wil gebruik maken van data en voorzieningen

Vele vrijwilligers dragen bij aan onderzoek door het ontplooien van activiteiten. Sectorvoorzieningen moeten daar in de gewenste situatie ook mogelijkheden voor bieden. De persoon is in de vrije tijd actief als amateur-meteoroloog. De persoon wil graag lid worden van een Europees netwerk, waarbij amateurs met een eigen weerstation deelnemen. De amateur-meteoroloog wil bij het opzetten van het eigen weerstation in de rol van citizen scientist gebruik maken van data en weermodellen die via het Europese netwerk beschikbaar zijn.

De persoon maakt zich eerst kenbaar als citizen scientist. Het netwerk van onderzoekers vraagt van de deelnemers om voorkennis. De persoon toont een verifieerbaar credential van de opleiding op het gebied van meteorologie die deze jaren geleden heeft afgerond. Als afronding van deze intake gaat hij akkoord met de gebruiksvoorwaarden van de gegevens en modellen. De citizen scientist wordt nu toegelaten tot het netwerk.

Vervolgens meldt hij zijn meteorologische apparatuur aan het netwerk. De voorzieningen die onderdeel uitmaken van dit netwerk zullen ook zelf een identiteit (breder dan alleen een uniek serienummer) hebben, zodat de verschillende citizen scientists erop kunnen vertrouwen dat ze te maken hebben met de juiste gekalibreerde voorzieningen en gecertificeerde voorzieningen. Het voldoen aan deze kwaliteitscriteria kan worden aangetoond op basis van verifieerbare credentials. Zo kan het weerstation van de persoon worden opgenomen in het meetnetwerk en worden de gegevens van dat weerstation meegenomen in de datasets van het netwerk. Mede hierdoor ontstaat een betrouwbaar stelsel van apparatuur met betrouwbare data voor onderzoek. Daarbij kan ook een maximum geldigheid worden meegegeven van het credential, zodat periodiek wordt gecheckt of de apparatuur nog voldoet. Student gebruikt voorzieningen voor een scriptie

Bij het uitwerken van een scriptie wil een student gebruik maken van een aantal voorzieningen die voor het onderzoeksgebied beschikbaar zijn. Om die voorzieningen te kunnen gebruiken moet de student kunnen aantonen bezig te zijn met een gerelateerde studie of als medewerker aan het onderzoek bekend zijn.

Wanneer de student toegang zoekt tot zo'n onderzoeksvoorziening, wordt door de voorziening gevraagd om een bewijs dat de student staat ingeschreven voor een studie binnen een relevant domein. Zo zal voor toegang tot een medische databank gevraagd worden of een student staat ingeschreven op een opleiding in de gezondheidszorg. Dit bewijs kan door de student eenmalig geselecteerd worden uit de set van

verklaringen die vanuit de inschrijving bij de opleiding zijn opgenomen in de wallet van de student. Bij elk volgend bezoek aan de databank zal dit bewijs getoond kunnen worden door het systeem waarbij de student de databank benadert. Belangrijk is hierbij dat de credential 'ingeschreven bij opleiding' een eindige geldigheidsduur heeft.

Fulltime onderzoeker

Een persoon heeft met succes een studie afgerond en blijft als onderzoeker fulltime werken bij een HO-instelling. Deze persoon verrichtte in het kader van zijn afstuderen onderzoek en had in de rol van student-onderzoeker toegang tot een aantal digitale onderzoeksomgevingen van de instelling en een aantal partner-instellingen. De persoon gaat nu in dienst bij de instelling en krijgt daarvoor een credential dat aantoont dat hij nu medewerker is. Om binnen de digitale onderzoeksomgeving direct door te kunnen gaan met de profielen die al aanwezig zijn voor de persoon als student, kan de persoon de verifieerbare credentials aanleveren van de studentgegevens en kunnen de profielen binnen de onderzoeksfaciliteit worden verbonden. Voor de uitschrijving als student wordt aan de persoon kenbaar gemaakt dat de studierechten worden beëindigd, maar dat de bewijsvoering voor de identiteit als student in het verleden nog bevraagd en bewezen kunnen worden.

De onderzoeker werkt een aantal jaren en heeft vervolgens een publicatie in concept gereed. Hij meldt dit aan bij een open science publicator, die zorg draagt voor een onafhankelijke peer review. Na afronding hiervan tekent de onderzoeker voor het eindresultaat, en de reviewers tekenen (anoniem) voor het correct verwerken van hun commentaar Ook een vertegenwoordiger van de instelling ondertekent het eindresultaat van de publicatie. De open science publicator verifieert of alle partijen de publicatie digitaal hebben ondertekend en verifieert of zij beschikken over geldige credentials. Vervolgens genereert de publicator een definitieve versie met de bijbehorende timestamps en credentials. Voor iedereen is nu te toetsen dat diverse betrouwbare organisaties instaan voor de kwaliteit en echtheid van deze publicatie. De onderzoeker ontvangt vervolgens een verifieerbare credential dat aantoont dat deze de auteur is van de wetenschappelijke publicatie, en de instelling een verifieerbare credential dat het onderzoek binnen die instelling is uitgevoerd.

Na vele jaren van dienst gaat de onderzoeker uit dienst. Ook over oude publicaties van de onderzoeker komen nog geregeld vragen en verzoeken binnen. De onderzoeker wil deze na beëindiging van de carrière in het onderzoek graag blijven beantwoorden. De onderzoeker beschikt over een onderzoeksidentiteit, die binnen een SSI-infrastructuur te relateren is aan de publicatie Gedurende de carrière moest gebruik gemaakt worden van communicatiefaciliteiten die door de instelling beschikbaar werden gesteld, waaronder een door de instelling gekozen wallet. Na pensionering wijzigt de onderzoeker de contactattributen behorend bij zijn onderzoeksidentiteit, zodat hij (nu als privépersoon) nog steeds bereikbaar blijft. Omdat de onderzoeksidentiteit zelf niet verandert, hoeven de uitgegeven credentials die zijn auteursrecht bewijzen niet te veranderen.

Technisch:

De onderzoeker maakt gebruik van een instellingsonafhankelijke onderzoeksidentiteit (vergelijkbaar met ORCID[11]). De verifieerbare credentials betreffen bijvoorbeeld credentials voor onderzoeksartikelen, behaalde prijzen en datasets en zijn bijvoorbeeld gekoppeld aan een open identifier-schema zoals ORCID, waardoor deze niet onbruikbaar raken zolang de onderzoeker zijn ID niet wijzigt.
Contactgegevens gerelateerd aan dat ID kunnen wel gewijzigd worden. Belangrijk hierbij is om de privacy van de onderzoeker ook in die situatie te kunnen borgen. Mogelijk moet daarvoor nieuwe functionaliteit ontwikkeld worden binnen ORCID of vergelijkbaar.

[11] Open Researcher and Contributor ID

Als gebruik werd gemaakt van een specifieke HO-wallet, kunnen de credentials naar een persoonlijke wallet worden overgedragen door gebruikt te maken van gedefinieerde transportmechanismen voor overdracht van credentials tussen wallets.

Data delen met een onbekende wetenschapper

Een fulltime onderzoeker bij een universiteit heeft met collega's afgelopen jaren een grote dataset opgebouwd. Ze merken dat er veel vraag is naar de specifieke data die ze verzameld hebben. De Nederlandse overheid heeft de dataset echter bestempeld als *vertrouwelijk*. Dit betekent dat de onderzoeksdata wel door researchinstellingen gebruikt mag worden, maar dat deze niet onbedoeld weg mag lekken naar buiten de EU.

De universiteit van de onderzoeker is aangesloten op de RDM-infrastructuur zoals deze door HOSA is beschreven. Partijen die zijn aangehaakt kunnen datasets uitwisselen met andere partijen of andere partijen toegang geven tot de datasets wanneer de data niet verplaatst kan of mag worden. Verzoeken voor het delen van data komen terecht bij de onderzoeksgroepen die gaan over deze data.

De onderzoeker heeft een verzoek gekregen voor het delen van de dataset. Bij de online intake is aan de indiener van het verzoek gevraagd om een aantal verifieerbare credentials te tonen. De eerste credential die is gevraagd betreft om aan te tonen dat de aanvrager werkt bij een erkende onderzoeksinstelling. Deze credential is overhandigd en onder water getoetst bij de uitgever van de credential. De tweede toets betreft de vraag of de onderzoeksintstelling is gecertificeerd voor het omgaan met vertrouwelijke onderzoeksdata op het vereiste niveau. Ook deze is aangetoond. De laatste verificatie van aangeleverde credentials betreft of de aanvrager een onderzoeker is die door de eigen organisatie is gemachtigd om te werken met vertrouwelijke data en dat deze machtiging niet is ingetrokken.

De onderzoeker kent de aanvrager niet maar heeft door de in samenhang getoonde credentials voldoende vertrouwen om toegang te verlenen tot de dataset. De onderzoeker drukt op de knop om het verzoek te honoreren. Daarna neemt de onderzoeker persoonlijk contact op met de aanvrager om deze alvast bij te praten over het interpreteren van de data.

3.3 Use Cases vanuit perspectief Instelling

Medewerkers van een instelling hebben vaak een rol waarbij zij niet zichzelf, maar de instelling vertegenwoordigen. Daarbij kan de HO-kaart van een instelling gebruikt worden in de communicatie met diensten die door de medewerker worden gebruikt. Dit betekent dat de instelling ook een identiteit heeft. Om gegevens die bij de identiteit horen te kunnen beheren beschikt de instelling over een (company) wallet. Deze biedt bijvoorbeeld functionaliteit om een aantal credentials van de instelling te kunnen bewaren, zoals algemene contactgegevens en status van accreditatie als onderwijsinstelling.

Een aantal medewerkers binnen een instelling krijgt bijvoorbeeld machtigingen om te werken met de HO-kaart van de instelling. De instelling beschikt over (menselijke of geautomatiseerde) medewerkers die bevoegd zijn deze machtigingen aan specifieke medewerkers toe te kennen. Deze medewerkers kunnen de credentials opnemen in hun wallet. Mogelijk stelt de werkgever aanvullende eisen aan een wallet of stelt deze een wallet beschikbaar voor de medewerkers om werkgerelateerde credentials te ontvangen, beheren en delen.

Het vrijgeven van gegevens vanuit een HO-kaart van een instelling moet ook door de persoon van buiten gecontroleerd kunnen worden op de betrouwbaarheid. De persoon kan bij een Nederlandse overheidsorganisatie, bijvoorbeeld DUO, checken of de instelling daadwerkelijk betrouwbaar is. DUO kan als uitgever van deze credentials het bewijs ondertekenen en er zorg voor dragen dat het

publieke deel daarvan is opgenomen in een registry. Hierdoor kan de persoon toetsen of de credentials daadwerkelijk zijn uitgegeven door DUO en of de credential niet is ingetrokken. De persoon weet na deze check of deze te maken heeft met een betrouwbare instelling. Dit hele proces kan in enkele seconden worden uitgevoerd.

4 Bedrijfsarchitectuur

In de use cases zijn voorbeelden gegeven van hoe SSI en verifieerbare credentials zouden kunnen werken in de sector van hoger onderwijs en onderzoek. In de use cases zijn een aantal begrippen naar voren gekomen. Deze worden in komend deel op samenhangende wijze weergegeven. Voor het structureren is gebruik gemaakt van de specificatie voor verifieerbare credentials van de W3C, het Verifiable Credentials-datamodel[12].

Wat is een verifieerbare credential?

Het begrip credential bestaat al in de niet-digitale wereld (identiteitsbewijs, betaalmiddel, diploma, hypotheekakte), en kan dan omvatten:

- Informatie gerelateerd aan de identificatie van een subject (bijvoorbeeld een foto, een naam of een identificerend nummer)
- Informatie gerelateerd aan de uitgevende autoriteit (bijvoorbeeld een gemeente, een overheidsinstelling of een certificatie-autoriteit)
- Informatie gerelateerd aan de aard van de credential (bijvoorbeeld een Nederlands paspoort, een Amerikaans rijbewijs of een ziekteverzekeringspas)
- Informatie gerelateerd aan specifieke attributen of eigenschappen die door de uitgever worden bevestigd (bijvoorbeeld nationaliteit, rijbevoegdheid of geboortedatum)
- Bewijs over de wijze waarop het credential is afgeleid
- Informatie gerelateerd aan beperkingen voor de credential (bijvoorbeeld vervaldatum of gebruiksvoorwaarden)

Een verifieerbare credential is de digitale variant van de ‘analoge’ credential, en kan alle informatie omvatten die daarin is opgenomen. In combinatie met technieken zoals digitale handtekeningen kunnen verifieerbare credentials beter bestand zijn tegen manipulatie en betrouwbaarder zijn dan hun fysieke tegenhangers, en intrinsiek digitaal zijn over te dragen en controleren.

4.1 Overzicht van het ecosysteem

In de use cases hebben de personen, organisaties en dingen verschillende rollen. De specificatie van W3C introduceert de volgende rollen[13]:

- ***Holder*** *(houder of bezitter)* – de rol die een entiteit speelt door een of meer verifieerbare credentials te bezitten[7] en daaruit een of meerdere verifieerbare presentaties te genereren. Voorbeelden van *holders* zijn studenten, werknemers en klanten.
- ***Issuer*** *(uitgever)* – de rol die een entiteit speelt door beweringen te doen over een of meer *subjecten*.
- ***Subject*** *(onderwerp)* – een entiteit waarop claims betrekking hebben. Voorbeelden zijn mensen, dieren en dingen. In veel gevallen is de houder van een verifieerbare credential het *subject*, maar in bepaalde gevallen is dat niet zo. Bijvoorbeeld een ouder kan als *holder* de verifieerbare credentials van een kind (het *subject*) in bezit hebben, of de eigenaar kan als *holder* de verifieerbare credentials van een huisdier (het *subject*) in bezit hebben.
- ***Verifier*** *(verificator of controleur)* – Een rol die een entiteit vervult door het ontvangen van een of meerdere verifieerbare credentials, mogelijk opgenomen in een verifieerbare presentatie, ten behoeve van verwerking. Voorbeelden zijn werkgevers, beveiligingsfunctionarissen en websites.

[12] https://www.w3.org/TR/vc-data-model/

[13] Waarbij nogmaals wordt benadrukt dat dezelfde entiteit afwisselend meerdere rollen kan vervullen.

In een gelijkwaardige interactie kunnen bijvoorbeeld personen of organisaties beurtelings verschillende rollen vervullen. Stel bijvoorbeeld een buitenlands persoon voor die rondkijkt op een onderwijsbeurs en een interessante opleiding ziet. De persoon wil weten en verifiëren of de opleiding daadwerkelijk geaccrediteerd is en heeft dan de rol van verifier. De onderwijsinstelling heeft dan de rol van holder en kan een verifieerbaar credential tonen dat de opleiding daadwerkelijk geaccrediteerd is. Bij inschrijven op de opleiding is dezelfde persoon vervolgens holder en is de instelling verifier voor bijvoorbeeld het verifiëren van de vooropleiding. De persoon heeft een verifieerbaar credential van de vooropleiding en kan deze beschikbaar stellen. Na een succesvolle inschrijving kan de instelling vervolgens een credential uitgeven als issuer, die door de student gebruikt kan worden om bij andere interacties aan te tonen dat hij daadwerkelijk is ingeschreven.

Rollen in het onderwijs

Zoals in de use cases beschreven zijn er diverse scenario's voor onderwijs mogelijk. Verifieerbare credentials kunnen bijvoorbeeld een rol spelen bij het verlenen voor toegang tot onderwijs of onderwijsvoorzieningen, toegang tot de arbeidsmarkt, of het aantonen van kwaliteit van onderwijs. Voor onderwijs zijn er diverse organisaties die betrokken kunnen zijn in de toekomst bij de uitgifte van dergelijke credentials zoals DUO, NVAO, Nuffic, Studielink, de Inspectie van het Onderwijs en de instellingen zelf.

DUO is bijvoorbeeld een voor de hand liggende issuer die op basis van het door instellingen gevulde diplomaregister kan verklaren over behaalde diploma's. In de toekomst kan dit in de vorm van een verifieerbaar credential. DUO is in een andere rol ook verifier van gegevens. Van personen die een diploma-credential opvragen moeten ze bijvoorbeeld controleren of zij daadwerkelijk de bezitter zijn van het diploma. Daarnaast is er ook behoefte aan partijen die registers met verifieerbare (meta)data bijhouden ten behoeve van gebruik in de hele sector. Het gaat hierbij dan o.a. om het publiceren van de schema's voor diploma-credentials en het bijhouden van publiek controleerbare verifieerbare informatie over erkende instellingen en opleidingen. Nadrukkelijk gaat het niet over gedeelde registers met persoons- of bedrijfsgegevens.

Figuur 3: Credentials in het onderwijs

Rollen in het onderzoek

Bij research zijn verifieerbare credentials vereist voor het geven van toegang tot data, digitale diensten en laboratoria aan allerlei vesrchillende actoren zoals bedrijven en burgers. De maatschappij kan zo breder participeren en profiteren van onderzoek. Ook voor het borgen van kwaliteit en betrouwbaarheid kunnen credentials een belangrijke rol spelen. Voor onderzoek zijn er diverse organisaties die een rol spelen in de toekomst bij de uitgifte van dergelijke credentials zoals KNAW, NWO en de instellingen zelf. Rondom onderzoek zullen ook internationale credentials van bijvoorbeeld subsidiegevers, Orcid, open science en uitgeverijen een rol gaan spelen.

Een Europese of nationale subsidiegever kan bijvoorbeeld issuer zijn van het credential ‘gefinancierd onderzoek’. Onderzoekers kunnen dit credential bijvoorbeeld gebruiken als ‘keurmerk’ op de website van het onderzoek zodat burgers kunnen zien dat het om werkelijk bestaand gefinancierd onderzoek gaat. De subsidiegever kan ook in de rol van verifier zitten. Voor de aanvraag van subsidies moeten onderzoekers vele gegevens aanleveren, bijvoorbeeld welke artikelen ze hebben gepubliceerd of welke prijzen ze eerder hebben gewonnen. Deze kunnen in de gewenste situatie aangeleverd worden met verifieerbare credentials. De subsidiegever is dan een verifier van deze credentials.

Figuur 4: Credentials in het onderzoek

4.2 Het vertrouwensmodel

Het verlenen van toegang is gebaseerd op vertrouwen. Aangezien er meerdere partijen een rol spelen in het ecosysteem moeten partijen elkaar vertrouwen. Het vertrouwensmodel voor verifieerbare credentials is gebaseerd op de onderkende rollen en is volgens het W3C-datamodel als volgt:

- De verifier vertrouwt de issuer van een ontvangen credential. Om dit vast te stellen, wordt verwacht dat een credential:
    - Ofwel een bewijs bevat waaruit blijkt dat de issuer de credential heeft gemaakt (dus: het is een verifieerbare credential)
    - Ofwel op een zodanige wijze is overgedragen dat duidelijk is dat de issuer de credential heeft uitgegeven en dat deze niet gemanipuleerd is gedurende transport of opslag. De mate van vertrouwen is dan afhankelijk van een risicoanalyse door de verifier.
- Alle entiteiten vertrouwen dat het register met verifieerbare data bestand is tegen manipulatie en een getrouwe weergave geeft van welke data door welke entities wordt beheerd.
- De holder en de verifier vertrouwen erop dat issuers waarheidsgetrouwe credentials over een subject verstrekken, en dat een issuer credentials snel intrekt wanneer van toepassing.
- De holder vertrouwt erop dat een repository credentials veilig opslaat, deze niet vrijgeeft aan anderen dan de holder, en deze integer en duurzaam bewaart.

In vergelijking met vertrouwensmodellen voor centrale uitgifte van identiteiten wijkt het datamodel voor verifieerbare credentials af in een aantal opzichten. De eerste is dat de issuer en de verifier de repository van de holder niet hoeven te vertrouwen, omdat ze aan de credential zelf kunnen zien dat deze onweerlegbaar is. Ook hoeft de issuer de verifier niet te kennen of te vertrouwen. Het vertrouwensmodel ontkoppelt de rollen van identity provider en verifier die in de eerste en tweede generatie van IAM-oplossingen vaak samenvallen.

Hiermee wordt een flexibel en dynamisch model geïntroduceerd waarin afhankelijkheden van centrale entiteiten worden gereduceerd en keuzemogelijkheden voor de gebruiker toenemen.

4.3 Kernbegrippen van het datamodel

Naast de rollen en hun interacties is de specificatie gebaseerd op een aantal conceptuele kernbegrippen.

Claims – Een *claim* is een bewering over een *subject*. Een *subject* is een 'ding' waarover beweringen kunnen worden gedaan. Claims worden uitgedrukt als een relatie tussen subject, eigenschap (*property*) en waarde (*value*). Met het datamodel kan een krachtige en gevarieerde set beweringen worden opgebouwd. Deze kunnen enkelvoudig zijn of samengesteld uit meerdere aan elkaar te relateren claims in de vorm van een *graph*[11].

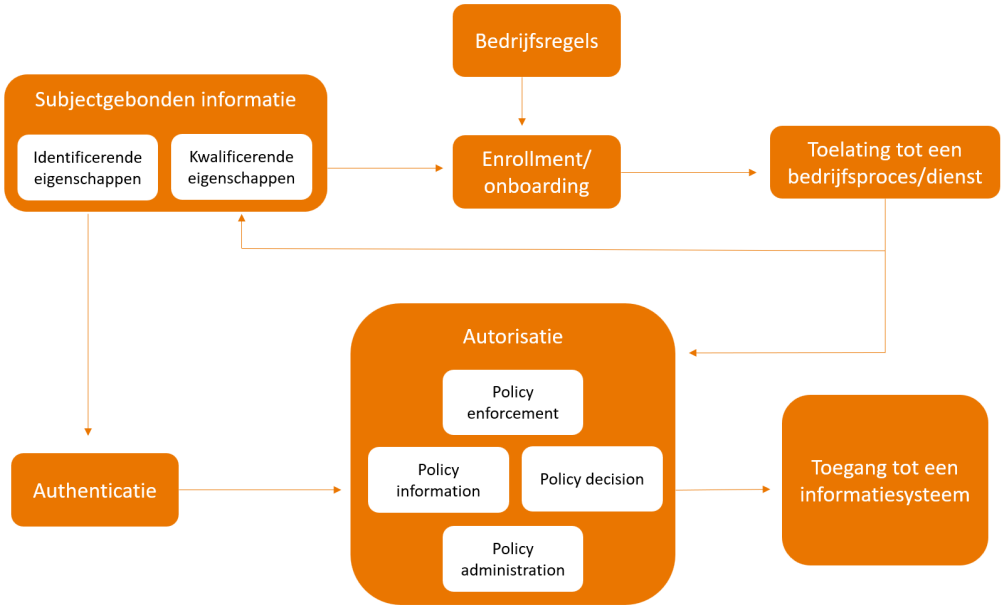
Credentials – Een credential is een set van een of meerdere *claims* die gedaan zijn door dezelfde entiteit. Credentials kunnen daarnaast een identifier bevatten, evenals metadata die eigenschappen van de credential beschrijft, zoals de *issuer*, de vervaldatum, een publieke sleutel ten behoeve van verificatie, het revocatiemechanisme, etc. De metadata kan door de *issuer* ondertekend zijn. Een *verifieerbare* credential is een set van claims die bestand zijn tegen manipulatie, gekoppeld aan metadata en cryptografisch bewijs over de *issuer*, bijvoorbeeld een digitale handtekening.

Presentations – Bevorderen van privacy is een sleuteluitgangspunt voor deze specificatie. Daarom is het belangrijk dat entiteiten in staat zijn om selectief te zijn bij het verstrekken van informatie over hun persona, zodanig dat alleen de informatie wordt onthuld die nodig is in de specifieke situatie. Een entiteit kan afhankelijk van de omstandigheden verschillende persona's gebruiken, zodat er onderscheid is tussen bijvoorbeeld zijn professionele persona, online gaming-persona, gezinspersona en incognito persona.

Verifieerbare presentaties - geven data uit een of meerdere verifieerbare credentials weer, zodanig dat de herkomst (*authorship*) van de data verifieerbaar is. Verifeerbare presentaties kunnen een-op-een overeenkomen met verifieerbare credentials, maar kunnen ook data bevatten die cryptografisch verifieerbaar is afgeleid van credentials. In het laatste geval zijn die verifieerbare credentials zelf geen onderdeel van de verifieerbare presentatie.

4.4 Een conceptuele beschrijving van IAM

Conceptueel zijn er twee aan elkaar gerelateerde processen, een op bedrijfsniveau en een op systeemniveau. Op bedrijfsniveau zijn er twee partijen die een onderlinge relatie aan willen gaan, bijvoorbeeld voor het volgen van onderwijs of het in dienst treden als werknemer. Daarbij gaat het er in eerste instantie om dat op bedrijfsniveau wordt vastgesteld of beide partijen voldoen aan de vereisten en verwachtingen voor het aangaan van die relatie. Tijdens zo'n enrollment/onboarding wordt aan de hand van identificerende (bijv. naam en geboortedatum) en kwalificerende kenmerken (bijv. vooropleiding) en mogelijk andere in bedrijfsregels vastgelegde criteria getoetst of aan de toelatingseisen kan worden voldaan. De uitkomst is een besluit om het subject (de lerende of de werknemer) toe te laten (of niet).



Figuur 5: Functionaliteiten en processen voor IAM

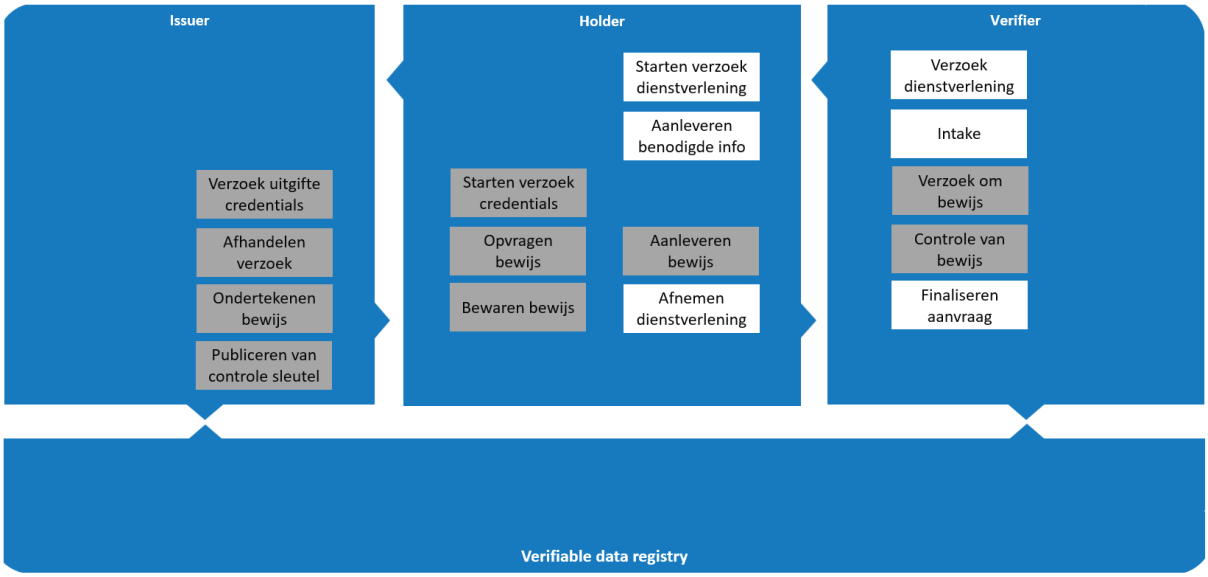
De toelating van het subject resulteert in uitgifte van (authenticatie)middelen aan het subject en toekenning van rechten (autorisaties) om toegang te krijgen tot de informatiesystemen die het subject nodig heeft. Vanaf dat moment lijkt het proces van daadwerkelijk autoriseren en toegang verkrijgen tot informatiesystemen weer heel erg op een bekend autorisatieproces, waarbij nieuwe policies worden gedefineerd en gehandhaafd die aan bestaande toegangssystemen worden toegevoegd. Omdat deze policies over een groot aantal verschillende systemen en organisaties op dezelfde manier moeten werken, zijn hiervoor afspraken en standaarden nodig.

De introductie van verifieerbare credentials leidt tot veranderingen op het conceptuele systeemniveau, maar niet overal in het systeem in gelijke mate. De grootste verandering is uiteraard de wijze waarop wordt omgegaan met subjectgebonden informatie, en nauw daarmee verbonden de authenticatie van het subject. Immers, subjectgebonden informatie is op een andere manier vastgelegd (namelijk in verifeerbare credentials of presentations), de informatie wordt door een andere rol in het ecosysteem verstrekt (door de holder) en kent een ander tijdgedrag (ad hoc verstrekking vs. vooraf vastgelegd). Potentieel worden een aantal stappen in het proces vereenvoudigd of flexibeler, met name als deze berusten op controle van fysieke credentials of complexe centrale administratiesystemen van rollen en rechten. Dit werkt alleen als (tenminste) binnen de Hoger Onderwijs-sector eenduidige afspraken kunnen worden gemaakt over rolinvulling van instellingen en partners.

Tegelijkertijd moet er rekening mee worden gehouden dat er nog heel lang (en wellicht wel altijd) andere manieren zijn voor interactie en uitwisseling van informatie waarbij de identificatie en kwalificatie van het subject niet is gebaseerd op verifieerbare credentials.

4.5 Verifieerbare credentials in een bedrijfsproces

Verifieerbare credentials kunnen leiden tot een hogere automatiseringsgraad. Voor eindgebruikers is het voordeel dat er geen separaat account aangemaakt hoeft te worden. Verzoeken om bewijs kunnen direct afgehandeld worden vanuit de wallet met verifieerbare credentials wanneer de gebruiker daar toestemming voor geeft. De dienstverlener kan in de rol van verifier het getoonde bewijs direct checken via de verifiable data registry zonder dat de issuer hiervan op de hoogte wordt gesteld.



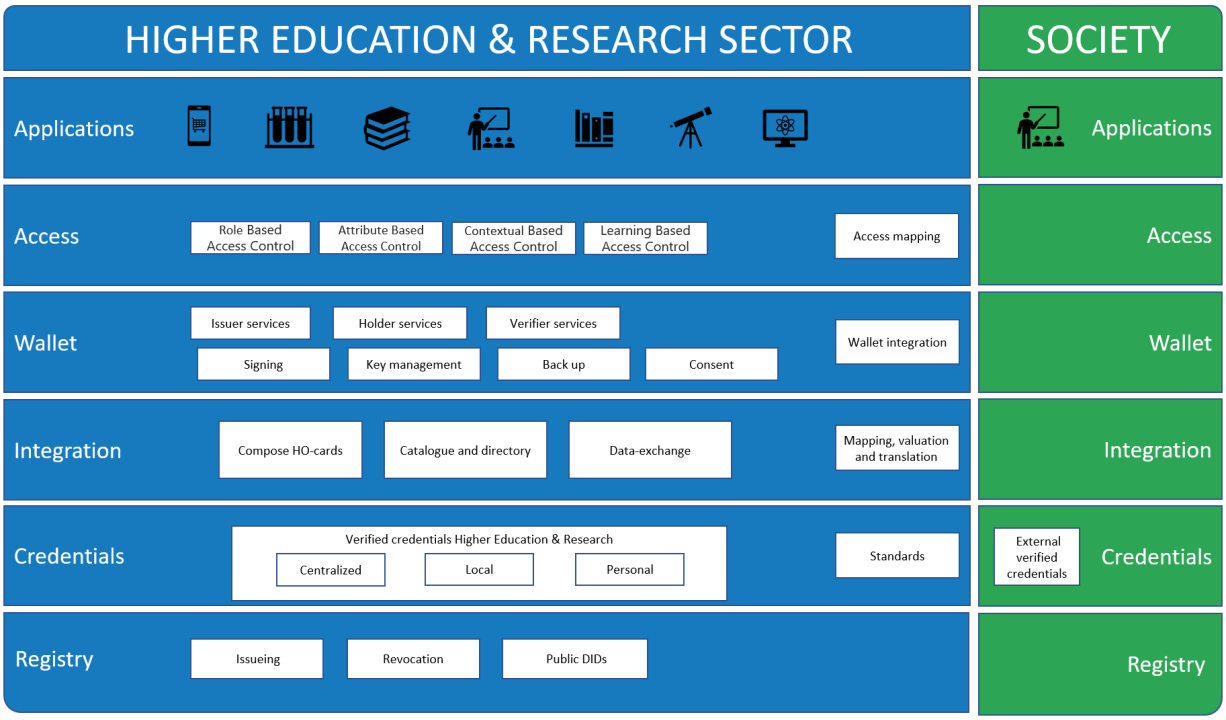
Figuur 6: Toepassing van credentials in een bedrijfsproces

5 Applicatiearchitectuur

Het komende deel geeft een schets van de applicatiearchitectuur weer. Door hetzelfde model voor de applicatiearchitectuur als onderlegger te gebruiken, geeft HOSA overzicht en een gezamenlijk vertrekpunt voor de discussies tussen de vele stakeholders[14]. Daarnaast geeft de applicatiearchitectuur het fundament om diverse initiatieven op een samenhangende wijze weer te geven. De applicatiearchitectuur is zo opgezet dat initiatieven uit tweede en derde generatie IAM in samenhang met elkaar weergegeven kunnen worden. Hierdoor kunnen SSI en het meer traditionele IAM naast elkaar bestaan in het toekomstige landschap.

In de applicatieplaat voor IAM maakt de HOSA onderscheid tussen de maatschappij en de eigen sector. Zoals eerder gesteld verwacht HOSA dat er in de toekomst meer gebruik gemaakt wordt in de maatschappij van een Self Sovereign Identity en zou de sector dit vanuit het belang van publieke waarden ook actief moeten faciliteren. Dit biedt voordelen voor mensen op het gebied van bijvoorbeeld privacy. Het stimuleren hiervan betekent echter dat de sector ook de eigen digitale services en systemen hiervoor naar de toekomst toe geschikt moet maken. Personen (en dingen) kunnen zich met credentials die buiten de sector zijn uitgegeven melden met een verzoek voor toegang tot systemen en diensten binnen de HO-sector. Naar verwachting zal niet alles via SSI worden georganiseerd maar zullen traditionele inlogmiddelen ook blijven bestaan.

De maatschappij beperkt zich echter niet tot de grenzen van ons land en omvat daarnaast meerdere sectoren. Onder de noemer maatschappij (society) schaart HOSA daarom in deze plaat ook overheden, andere sectoren en andere landen. Deze landen, sectoren en overheden maken gebruik van eigen stelsels met eigen regels en technische voorzieningen. Vanuit de HO-sector is het van belang dat we hierop aan kunnen sluiten. Hierdoor ontstaan in de applicatieplaat op de grens tussen de HO-sector en de maatschappij allerlei applicatiefuncties die hier invulling aan kunnen geven.



Figuur 7: Een gelaagde applicatiearchitectuur voor IAM

Binnen de HO-sector zijn voor de beoogde doelstellingen een aantal informatiesystemen vereist. Met de plaat voor de applicatiearchitectuur geeft HOSA een indeling die gebruikt kan worden om overzicht te creëren in de

[14] Bij voorkeur wordt hierbij aangesloten op internationaal geaccepteerde referentiemodellen. Die blijken vooralsnog zeer schaars. Het model van Trust-over-IP (ToIP, trustoverip.org) komt nog het dichtst in de buurt.

benodigde informatiesystemen die samenwerken in het beoogde doel voor toegangsverlening. De plaat is gericht op de toekomst en opgezet langs de beweging richting Self Sovereign Identities (SSI). Ook huidige informatiesystemen uit het IAM-domein kunnen geplot worden op het model. Hiervoor maakt het model onderscheid tussen zes segmenten: Applications, Access, Wallet, Integration, Credentials en Registries.
Elk segment bevat een aantal functies die op zich zelf moeten kunnen staan, en met andere functies en lagen communiceren via welbepaalde koppelvlakken. Dat heeft consequenties voor de uitwerking van de architectuur: oplossingen dienen de elementen niet te vermengen, en er zullen afspraken/standaarden moeten bestaan voor de communciatie tussen de elementen.

Per segment wordt in de volgende paragrafen toegelicht wat HOSA hieronder verstaat.

5.1 Applications

In het segment van Applications staan informatiesystemen die allerlei verschillende digitale diensten verlenen en waarvoor toegang voor eindgebruikers georganiseerd moet worden. In de use cases zijn diverse voorbeelden genoemd, denk aan het intekenen op onderwijs, inloggen op een leeromgeving, het gebruiken van elektronische meetinstrumenten of het verlenen van toegang tot een lab. Deze diensten kunnen geboden worden door instellingen en sectorpartners. Belangrijk kenmerk van sectorvoorzieningen in de toekomst is dat ze veelal de rol hebben binnen marktplaatsen of business platforms. Veel verschillende aanbieders en afnemers komen hier samen voor een breed aanbod aan diensten. Instellingen verlenen bijvoorbeeld diensten aan lerenden, docenten en onderzoekers van andere instellingen of personen die werkzaam zijn bij bedrijven of wetenschap als hobby hebben. Dit zorgt voor grote uitdagingen op het gebied van het verlenen van toegang tot deze services. Wie mag onder welke voorwaarden toegang hebben tot deze service? En welke bewijzen moet deze persoon tonen?

De eigenaar van een Application is ervoor verantwoordelijk dat deze aangeeft welk vertrouwensniveau vereist is voor toegang ertoe. Om dit vertrouwensniveau te bereiken toont de eindgebruiker verifieerbare credentials. Belangrijk uitgangspunt is dat applications zo min mogelijk privacygevoelige gegevens vragen aan eindgebruikers voor het verlenen van toegang. Dit doen de applications door het gebruik van Zero Knowledge Proof te faciliteren. Bij Zero Knowledge Proof stel je bijvoorbeeld alleen de vraag of iemand ouder is dan 18 jaar om vervolgens toegang te verlenen. Met Zero Knowledge Proof wordt alleen een ja of nee gegeven als antwoord. Er wordt geen leeftijd bekend gemaakt. Hiermee worden privacygevoelige gegevens niet onnodig bekendgemaakt aan een verifier.

Daarnaast zal in dit segment van services ook ‘credentialization’ van formele documenten gaan plaatsvinden. Formele documenten worden dan gestructureerd opgebouwd en beschikbaar gesteld op basis van verifieerbare credentials. Denk hierbij bijvoorbeeld aan een diploma waarbij microcredentials van de afzonderlijke vakken gecheckt kunnen worden bij de issuer. Deze trend is bijvoorbeeld zichtbaar in de W3C VC variant van Open Badges.

Gemak en begrijpelijkheid voor de gebruiker zijn belangrijke overwegingen bij het implementeren van applicaties die met credentials werken. Dit is primair vastgelegd in het HOSA-hoofdprincipe ‘Toegankelijk voor iedereen’. Hieronder vallen ook zorgvuldige en duidelijke vormgeving van processen voor het geven van consent en delen van credentials.

Inloggen zonder wachtwoord?

In het concept van Self Sovereign Identity wordt grotendeels afscheid genomen van inloggen met gebruikersnaam en wachtwoord. Binnen de sector van hoger onderwijs en onderzoek zal echter niet alles volledig via SSI gaan verlopen. Services die op lange termijn toegang verlenen via een SSI-wijze worden ingericht zonder het gebruik van wachtwoorden. Hiervoor wordt gebruik gemaakt van decentrale identifiers (DID’s) en verifieerbare credentials. De credentials die hierbij worden uitgewisseld zijn betrouwbaar te gebruiken en hiervoor hoeft binnen de afnemende applicatie geen gebruikersprofiel te worden opgebouwd. De credentials worden na consent bij het gebruik van de dienst meegeleverd bij het activeren van de sessie.

Privacy-vriendelijk & automatisch vullen van formulieren

Op langere termijn kunnen de processen in deze digitale services met behulp van de verifieerbare credentials een veel hogere automatiseringsgraad bereiken dan nu het geval is. Vanuit een wallet kunnen bewijzen automatisch gegeven worden als de gebruiker daarvoor toestemming heeft gegeven. Ook kunnen gegevens geautomatiseerd worden ingevuld in digitale formulieren of kan de gebruiker de agent van de wallet instrueren om gegevens automatisch in te vullen bij een volgend bezoek met aandacht voor privacy.

Verifieerbare reviews

Een groot probleem rondom huidige online diensten wereldwijd is dat reviews over deze diensten niet betrouwbaar zijn. Er kan niet gecontroleerd worden of de auteurs van een review de dienst ook zelf hebben afgenomen. Ook kan het zijn dat iemand tegen betaling vele nep-reviews plaatst. Het stelsel met verifieerbare credentials maakt het mogelijk voor services om te gaan werken met verifieerbare reviews. Hierbij kan men gevalideerde reviews achterlaten zonder dat het ten koste gaat van privacy. In de domeinarchitecturen voor Flexibel Onderwijs en Research Datamanagement spelen reviews ook een rol rondom de business platforms. Hier wordt functionaliteit voorzien voor afnemers op de business platforms voor het geven van reviews.

Verlenen en intrekken van consent

Vanuit de AVG (GDPR)[15] is het geven van toestemming door een eindgebruiker in sommige gevallen vereist bij het verwerken van data. Bij SURFconext en eduID is in de huidige situatie al zichtbaar welk consent door de eindgebruiker wordt verleend aan dienstaanbieders. Een beheerder van een instelling kan afhankelijk van het beleid van een instelling per dienst die gekoppeld wordt kiezen uit drie mogelijkheden: een informatiescherm, een toestemmingsscherm of geen scherm. Bij het concept van Self Sovereign Identity geeft een gebruiker consent voor het verwerken van bepaalde data in de vorm van credentials. Een gebruiker heeft dan overzicht van alle zaken waarvoor deze consent heeft gegeven en is ook in staat om consent in te trekken. Het terugtrekken van die consent is nu nog niet goed geautomatiseerd te ondersteunen binnen SSI[16]. Ook afnemende systemen kunnen nu niet makkelijk verifiëren wat de status van een gegeven consent is. Om een betrouwbaar op credentials gebaseerd SSI-stelsel te maken is dus noodzakelijk dat statussen van consents zijn te raadplegen voor afnemende systemen via de agents van wallets. Bovendien zal via een afsprakenstelsel geregeld moeten worden dat diensten zich hieraan houden.

Het minimum aanleveren op het betreffende moment

Verifieerbare credentials maken het mogelijk om precies het benodigde bewijs aan te leveren voor het nemen van een bepaald besluit. Besluiten op het gebied van toegang worden genomen op basis van het toegangsbeleid van de verifier. Beslisregels worden vooraf openbaar gemaakt zodat personen pas gegevens gaan delen zodra het besluit positief voor hun uitvalt. Daarnaast maken verifieerbare credentials het mogelijk om de bewijzen realtime en actueel te valideren.

Uitwisselen van waarde

Het gedachtengoed van SSI faciliteert scenario's rondom het uitwisselen van waarde, waaronder betalingen. Ook hier speelt vertrouwen een belangrijke rol en wordt er in de financiële wereld onderzoek gedaan hoe SSI ingezet kan worden. Voor HOSA is de uitwisseling van waarde ook benoemd rondom de business platforms in de domeinarchitecturen voor Onderwijs en Onderzoek. Op langere termijn zou dit concept hier potentieel invulling aan kunnen geven.

Permanente verbinding

Wanneer SSI wordt ingezet voor bepaalde services dan komen permanent bestaande connecties in beeld. Deze relaties tussen twee partijen blijven in stand tot één van de partijen besluit om de connectie te verbreken.

---

[15] De Algemene verordening Gegevensbescherming, respectievelijk de General Data Protection Act van de EU.

[16] Ook over de juridische en organisatorische implicaties van een gegeven of ingetrokken consent is niet alles volledig duidelijk. Binnen de context van de IAM-domeinarchitectuur kan ermee worden volstaan dat de architectuur een technisch sluitend consent kan faciliteren, maar zich niet bemoeit met de implicaties van de inhoud van dat consent voor het bovenliggende bedrijfsproces.

Deze permanente verbindingen worden mogelijk gemaakt door de inzet van DID's. Hierdoor is er geen afhankelijkheid meer van een derde partij die functioneert als intermediair.

Relevante ontwikkelingen

- Concepten en technische implementaties van zero knowledge proof
- Large Scale Pilots rondom bijvoorbeeld rijbewijzen, toegang tot overheidsinformatie en openen van een bankrekening[17]
- Verbinden van de standaarden voor OpenBadges met die voor verifieerbare credentials. Open badges zijn ontwikkeld als toepassing voor het kunnen delen van informatie over behaalde onderwijsresultaten, maar worden tot dusverre niet uitgegeven als verifieerbare credential. De onderwijsstandaardisatieorganisatie 1EdTech werkt samen met W3C om dat wel tot stand te brengen.

5.2 Access

In het segment van Access zitten de informatiesystemen die gebruikt worden om toegang tot de applications te organiseren. Aan de hand van policies wordt vastgesteld of een persoon of apparaat toegang mag krijgen tot de application. Voor Access geldt dat er een nieuwe policy-variant bijkomt, maar dat het principe van hoe je toegang verleent niet wezenlijk verandert. Want ook in de huidige implementaties moet er eerst bewijs worden verzameld of aangeleverd, voordat een toegangsbeslissing wordt genomen[18]. De credentials die hiervoor aangeleverd moeten worden komen zo veel mogelijk uit een wallet in het derde segment. In de huidige situatie wordt het verlenen van toegang reeds veelal gedaan op basis van rollen. Dit wordt ook wel RBAC genoemd en voorkomt dat je handmatig rollen en rechten moet uitdelen voor grote groepen. Bekende rollen zijn de rol van student en de rol van medewerker.

Fijnmazigere onderdelen om het recht van toegang op te verlenen werken op basis van attributen of policies (access based control en policy based control; ABAC en PBAC). Ook deze vorm wordt in de huidige situatie al toegepast voor attributen en policies op basis van intern vertrouwde bronsystemen. Een groot deel van de huidige applicatielandschappen heeft in de huidige situatie echter nog moeite om hun interne autorisatiemodel te kunnen vormen naar extern aangeleverde bewijzen. In de toekomst kunnen hierbij nog context afhankelijke attributen aan worden toegevoegd, zoals een extra credential wanneer een dienst buiten kantoortijd wordt gevraagd (Contextual Based Access Control). Deze credential kan de gebruiker aanleveren vanuit de wallet.

Op langere termijn kan ook nog gedacht worden aan mogelijkheden die meer richting kunstmatige intelligentie gaan. Het kan dan gaan om Learning Based Access Control (LBAC) waarbij op basis van patroonherkenning een aanpassing kan worden gedaan in de uitvraag van benodigde credentials. Wanneer er bijvoorbeeld veel internationale studenten vanuit Australië gebruik willen maken van een bepaald meetinstrument hier in Nederland, kan dat komen doordat een docent van een bepaalde universiteit dat heeft opgenomen in z'n lesmateriaal. Met LBAC kan dan geleerd worden dat de overeenkomst van deze studenten is dat zijn van die betreffende universiteit komen en dat het in hun tijdszone binnen kantoortijd valt.

Voorbeelden huidige situatie

Als we kijken naar de situatie zoals die in 2022 actief is rond de tweede generatie systemen voor IAM, dan zien we daar al stappen die richting de functies gaan die we vanuit de derde generatie systemen IAM verwachten. Het gaat dan bijvoorbeeld om de mogelijkheden om autorisatieregels op te geven die toegang tot een applicatie sturen. Deze autorisatieregels kunnen worden gebaseerd op gegevens uit een vertrouwde bron. In

[17] https://www.digital-identity-wallet.eu/

[18] Let wel op dat de volgorde anders wordt: in klassieke systemen begin je met een authenticatie waaruit bijvoorbeeld een identificerend nummer of rol volgt waarbij de juiste attributen voor autorisatie worden gezocht in een intern systeem. In zuiver decentrale systemen komt er een set attributen waaruit identiteit en rol zijn af te leiden door de verifier.

de toekomstvisie van HOSA speelt dit ook een belangrijke rol om SSI identiteiten en credentials als bron te kunnen gebruiken om toegang tot een tweede generatie IAM service mogelijk te maken. De applicatie kan dan als dienst vertrouwen op bijvoorbeeld OIDC vanuit SURFconext die wordt gevuld met credentials die als derde generatie IAM worden aangeleverd vanuit de wallet van de eindgebruiker.

Andersom kan de dienst SURF Research Access Management (SRAM) gezien worden als verbinding tussen 2de generatie IAM identiteiten die een service willen gebruiken die als 3de generatie IAM is ontsloten. De credentials die nodig zijn voor de toegang kunnen dan op basis van gegevens die via SRAM zijn verzameld worden opgebouwd en worden aangeleverd aan de betreffende dienst volgens de standaarden die gelden voor SSI en DID uitwisseling.

Relevante ontwikkelingen

- Het Finse IT Center for Science ontwikkelde een proof of concept voor het gebruik van SSI om toegang te managen tot privacygevoelige human genomic datasets. De proof of concept is gebaseerd op de ELIXIR Authentication and Authorization Infrastructuur (AAI) en een commerciële wallet.

5.3 Wallet

Binnen Self Sovereign Identity wordt vaak gesproken over een wallet. Wallets zijn applicaties die zijn gericht op de eindgebruiker die als doel hebben om persoonlijke data op een afgeschermde, veilige en persoonlijke manier te bewaren en vanuit daar te kunnen presenteren aan verifiers. De wallet is goed vergelijkbaar met hoe een fysieke portemonnee gebruikt wordt in het dagelijks leven. De eindgebruiker kan er bijvoorbeeld pasjes in bewaren waarmee deze zich kan identificeren en valuta om mee te betalen. In het kader van Identiteiten en Toegang is de wallet het mechanisme om combinaties van public en private keys te bewaren. Het bevat de functionaliteit die gebruikt kan worden om de gebruiker met behulp van credentials te authentiseren en heeft ook de functie van een veiligere versie van een wachtwoordmanager. Daarnaast kan de gebruiker berichten ondertekenen vanuit de wallet.

HOSA plaatst de functionaliteit die gebruikers in staat stelt om het werken met credentials mogelijk te maken in het derde segment in het applicatiemodel. Denk hierbij aan het aanmaken, ontvangen, bewaren en ondertekenen van credentials. Zoals in de use cases duidelijk is geworden zijn personen of vertegenwoordigers van organisaties vaak actief in zowel de rol van holder, verifier en issuer. Dit betekent dat de ondersteunende functionaliteit hiervoor beschikbaar moet kunnen zijn in één omgeving.

In voorbeelden functioneren wallets vaak op of worden ze ontsloten via een smartphone. Wallets kunnen ook functioneren op of worden ontsloten via laptops, desktops en andere devices. Naast wallets die functioneren als app zijn er ook wallets beschikbaar die functioneren als webpagina in een browser. Gezien de diversiteit aan use cases is het van belang dat functionaliteit voor wallets zowel als via een app als een browser aangeboden moet kunnen worden. Hiermee wordt een any-device-beleid mogelijk wat toegankelijkheid en inclusiviteit verbetert.

Personal wallet
In de HO-sector is een onderscheid te maken tussen diverse doelgroepen op basis van de betrokkenheid die ze bij de sector hebben. Medewerkers van instellingen zoals docenten en onderzoekers, maar ook studenten zijn nauw en direct betrokken bij diverse processen die toegang vereisen met een hoog betrouwbaarheidsniveau. Voor de sector is het van belang om de eisen die zij stelt aan een wallet helder vast te leggen in afspraken en standaarden. Hierbij sluit de sector aan op standaarden vanuit de publieke sector en EU.

Company wallet
Ook instellingen, sectorpartners en andere partijen hebben zelf de functionaliteit van wallets nodig. Ook de organisaties moeten op basis van credentials laten zien dat ze betrouwbaar zijn. Personen weten zo dat ze te maken hebben met een echte instelling, een echt onderzoek of een geaccrediteerde opleiding. Dit helpt in de toekomst om fraude te voorkomen. Instellingen en sectorpartners beschikken hiervoor over functionaliteit van company wallets. Voor deze company

wallets is integratie met ondersteunende informatiesystemen van belang voor afhandeling van grote aantallen verzoeken. Company wallets vragen om aanvullende mogelijkheden ten opzichte van personal wallets. Denk hierbij aan uitgebreide mogelijkheden voor het toekennen en per direct intrekken van rollen, rechten en permissies via delegatie, een schaalbare onderliggende infrastructuur om vele verzoeken gelijktijdig af te kunnen handelen en aanvullende beveiligingsmaatregelen. Het is waarschijnlijk dat er binnen organisaties verschillende type company wallets ontstaan afhankelijk van het bedrijfsdomein. Voor bijvoorbeeld de afdeling financiën kan specifieke functionaliteit benodigd zijn.

Wallets voor custodians?
Met concepten zoals Self Sovereign Identity krijgen bijvoorbeeld ook dieren, planten of door mensen gemaakte dingen een identiteit. Hiervoor wordt door sommigen een derde mogelijke variant van de wallet, die de functionaliteit biedt om namens iets of iemand bepaalde credentials te managen. Dit wordt ook wel een custodian wallet genoemd. Deze functionaliteit kan overwogen worden bij bijvoorbeeld het bieden van functionaliteit voor ouders van minderjarige studenten. In de huidige ontwikkelingen lijkt echter de voorkeur uit te gaan naar dit op te lossen via credentials in plaats van een extra en specifieke wallet. Dan wordt de holder via een credential ‘gemachtigd’ om namens een andere identiteit te handelen.

Globale functionaliteit

In de gewenste situatie hebben personen en organisaties in veel voorkomende gevallen zowel de rol van holder als verifier, maar dit niet tegelijkertijd voor dezelfde credential. In de use cases zijn voorbeelden genoemd van een persoon die wil weten of een opleiding daadwerkelijk geaccrediteerd is. De organisatie zit dan in de rol van holder van dit verifieerbare credential en de persoon zit in de rol van verifier. Dit betekent dat wallets voor personen en organisaties over functionaliteit moeten beschikken voor beide rollen. Ook de rol van issuer zal regelmatig voorkomen naast de rol van holder en verifier.

Binnen de HO-sector is het nodig tot overeenstemming te komen over de inhoudelijke vereisten aan credentials voor het onderwijs, de regels voor uitgifte en acceptatie en de daarvoor benodigde functionaliteit in wallets om dit te ondersteunen. Dit vereist samenwerking tussen issuers, verifiers en wallet providers in een ‘assurance community’.

Ook zijn functionaliteiten zoals ondertekenen, key management en herstelservices benodigd. Het zetten van gekwalificeerde digitale handtekeningen is vereist om authenticiteit en integriteit te kunnen garanderen van data en documenten. Vaak worden hier cryptografische technieken voor gebruikt zoals PKI. Het kunnen ondertekenen is ook van belang voor betrouwbare digitale gegevensuitwisseling. De verifier kan checken of de ondertekening in een credential nog geldig is. Hiervoor zijn verschillende technieken mogelijk.

Herstelservices zijn vereist voor wanneer een persoon bijvoorbeeld de eigen telefoon verliest, data wil overzetten naar een nieuw toestel, of back-ups maakt vanuit een redundantieperspectief. Een back up kan gebruikt worden om data te herstellen of over te zetten. Bij deze functionaliteit horen vragen als: welke data en metadata neem je mee in de back up,? Waar zet je het neer, of wie kan erbij? Het terugzetten of overzetten van een backup is geen triviale zaak in een decentrale omgeving. Want waar komen de private keys vandaan als de originele verloren zijn? Verwacht wordt dat een deel van de benodigde functionaliteit zal worden ingevuld door wallet providers. Daarnaast moet ook op het niveau van de assurance community worden nagedacht over de mogelijkheid om credentials opnieuw af te geven of te laden. Dat vereist wel dat de uitgevers van credentials de feiten waarover wordt verklaard langdurig bewaren.

Holder

Voor de rol van holder is de wallet de functionaliteit die de holder in staat stelt om privacygevoelige data te verkrijgen, te genereren, op te slaan, te managen, te beschermen en te gebruiken. Voorbeelden van vertrouwelijke gegevens zijn persoonlijke relaties met bijvoorbeeld andere personen en organisaties, wachtwoorden, biografische informatie, persoonlijke contactinformatie, verifieerbare credentials en eventueel kopieën van formele documenten. Persoonlijke relaties kunnen onder andere worden gemanaged met een

DID-manager. Ook het genereren van Zero-Knowledge-Proof credentials is een functie die is te vinden in een aantal wallets.

Verifier

Voor de rol van verifier is functionaliteit benodigd om getoonde credentials te kunnen valideren. Hiervoor zijn bijvoorbeeld checks op het format en de handtekening nodig. De holder presenteert de credentials met een bepaald doel, bijvoorbeeld het verkrijgen van toegang. De verifier moet daarbij een aantal beslissingen nemen. Deze beslissingen worden genomen vanuit het perspectief van bepaalde uitgangspunten of beleidskaders. In het ene uiterste zijn deze beslisbomen vastgelegd in geautomatiseerde procedures. Het voordeel hiervan is dat vele aanvragen tegelijkertijd door een organisatie afgehandeld kunnen worden. Het andere uiterste betreft het handmatig uitvoeren van een aantal checks via een ad hoc procedure. Voor beide varianten is digitale ondersteuning nodig in de gewenste situatie.
Aan de rol van verifier zullen vereisten gesteld moeten worden omtrent het omgaan met credentials en het kunnen aangeven van voldoende onderbouwing voor het ontvangen van bepaalde credentials. Het controleren op deze vereisten voor een verifier zal onderdeel uitmaken van het vertrouwensstelsel waarbinnen de uit te wisselen credentials een betekenis hebben.

Issuer

Voor een issuer zal het in de sector in veel gevallen van belang zijn om verifieerbare credentials in grote hoeveelheden uit te kunnen geven. Verzoeken van holders voor het creëren van verifieerbare credentials moeten online via een geautomatiseerd proces in behandeling kunnen worden genomen. Dit proces zal mogelijk niet volledig in de wallet zelf worden gerealiseerd. Het proces start bijvoorbeeld op de website van de issuer. De holder start hier het proces voor de aanvraag van een verifieerbaar credential. Tijdens het afhandelen van het verzoek moet de issuer de credentials kunnen ondertekenen en de credentials kunnen versturen naar de holder. Daarnaast moet de controle-sleutel die verifiers kunnen checken gepubliceerd kunnen worden.

Wallet integration

Daarnaast zijn er diverse doelgroepen die iets verder afstaan van de reguliere dienstverlening van onderwijs en onderzoek, maar er wel bij betrokken zijn. Denk hierbij aan kenniswerkers, proefpersonen, niet actieve levenlang lerenden of wetenschappers die uit loondienst gaan, maar wel betrokken blijven. Deze worden in de applicatieplaat geplot in het groene gedeelte van de maatschappij. Deze doelgroepen hebben in de gewenste situatie een eigen wallet waarin ze credentials vanuit de HO-sector kunnen managen naast andere credentials. Denk bijvoorbeeld aan microcredentials of andere diploma's die ze gehaald hebben voor onderwijs. Om deze integratie te verzorgen maakt de sector gebruik van een Wallet Integration Gateway.

Deze gateway biedt mogelijkheden om credentials en ook formele documenten te presenteren, uit te geven en te valideren. Dit gebeurt dan wallet-onafhankelijk en zelfs document-onafhankelijk. Deze gateway biedt naast technische interoperabiliteit ook ondersteuning voor integriteit, herkomst en andere garanties. Vanwege de technische interoperabiliteit staat het gebruikers vrij om elke wallet naar keuze te gebruiken, mits deze voldoet aan de standaarden van de gateway. De sector heeft hierdoor niet de volledige technische last van het accepteren van alle mogelijke wallets waarmee personen bij de sector aan kloppen.

Voorbeelden huidige situatie

In de huidige situatie beschikt de sector ook over functionaliteit die je op dit niveau kunt plaatsen. Denk bijvoorbeeld aan de SURFconext Consent Services. Hierbij kan een gebruiker in de huidige situatie aangeven welke gegevens van de gebruiker gedeeld mogen worden met anderen. Een ander voorbeeld is de inzet van SURFteams om groepen te definiëren waarin federatieve accounts bij elkaar kunnen worden gebracht. Dit wordt o.a. gebruikt bij het SURFdashboard. Hier kunnen instellingen aangeven welke medewerkers welke rol hebben richting SURF. Ze kunnen bijvoorbeeld aangeven wie licenties mag bestellen of wie verantwoordelijk is voor het beheer van het netwerk. Deze rollen (bijvoorbeeld "netwerk-beheerder") worden door andere applicaties zoals het Netwerk Dashboard gebruikt voor RBAC: de gebruiker krijgt precies die mogelijkheden in de applicatie die passen bij de rol.

Relevante ontwikkelingen

- European Identity Wallet: Door de EU worden grootschalige pilots uitgevoerd en wordt wetgeving voorbereid (als uitbreiding van de eIDAS-verordening) om een gestandaardiseerde wallet voor alle burgers van de EU beschikbaar te maken.
- eduMij: Afgelopen jaar is een kosten-baten analyse gemaakt over de toevoegde waarde van eduMij. eduMij is oorspronkelijk bedacht als persoonlijke omgeving van waaruit lerenden hun credentials of certificaten kunnen delen met bijvoorbeeld werkgevers.
- Wallet integration gateway: TNO werkt aan een gateway die integratie tussen wallets kan gaan invullen onder de noemer TNO EASSI. Deze gateway ontzorgt aanbieders van wallets zodat ze niet zelf integraties met alle andere wallets moeten onderhouden.
- Solid-project: Solid is een project van Prof. Tim Berners-Lee en MIT. Het idee hierbij is dat personen zelf eigenaar worden van data en dat deze data ook staat opgeslagen in een eigen omgeving, de PODS[19].
- HR Career Wallet: Dit betreft een use case van de DBC (dutchblockchaincoalition.org). In deze coalitie werken de overheid en bedrijfsleven samen aan de ontwikkeling van een gezamenlijke wallet.
- De Global Legal Entity Identifier Foundation (GLEIF) werkt aan een verifieerbaar credential voor de Legal Entity Identiefier (LEI)[20].

5.4 Integration

Credential catalogus

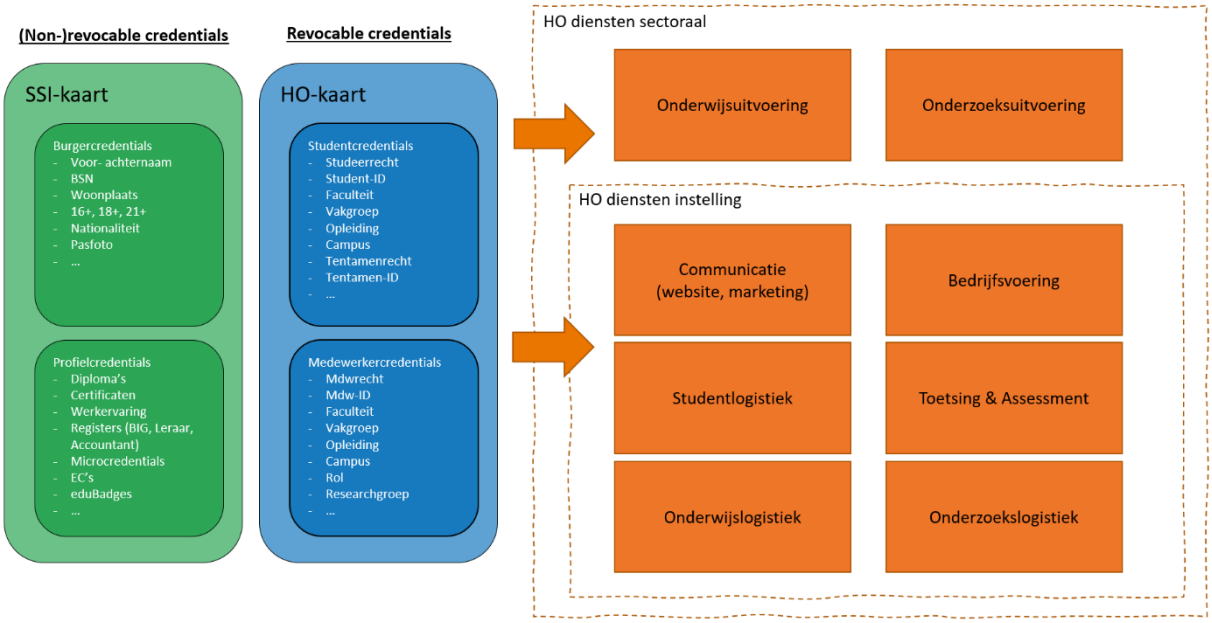
Services in het bovenste segment van het applicatiemodel zullen in de gewenste situatie verifieerbare credentials gebruiken om toegang te verlenen. Bij het inrichten van deze services ontstaat de vraag welke credentials een persoon zou moeten laten zien om vast te kunnen stellen of deze toegang moet krijgen. De sector stelt hiervoor een catalogus beschikbaar. In deze catalogus worden credentials weergegeven die worden uitgegeven in de sector met daarbij een beschrijving, een geadviseerd niveau van vertrouwen en een contactpersoon. Bijvoorbeeld: deze universiteit geeft diploma's uit, in deze vorm, met deze attributen en dit is op basis waarvan wij vaststellen dat dit type credential toegekend kan worden. De credential catalogus wordt vastgesteld in één of meerdere assurance communities. Die kunnen zeker ook spelers van buiten de sector bevatten.

HO-kaarten

Een andere functionaliteit in dit segment betreft het genereren van HO-kaarten. Zoals in de use cases beschreven betreft de HO-kaart een samengesteld geheel van een aantal verifieerbare credentials. Deze kaarten moeten samengesteld kunnen worden als service richting gebruikers in de sector. De wallets beschikken vervolgens over functionaliteit om gegevens van de HO-kaart te kunnen verwerken.

[19] Solid (solidproject.org)

[20] https://www.gleif.org



Figuur 8: Positionering van de HO-kaart

Gegevensuitwisseling

HOSA verwacht dat een deel van de reguliere gegevensuitwisseling die los staat van IAM in de toekomst uitgewisseld gaan worden in de vorm van verifieerbare credentials. Denk aan bijvoorbeeld cijfers voor lerenden of inschrijvingen op vakken. Wanneer een lerende studeert bij twee instellingen dan moeten deze gegevens uitgewisseld kunnen worden. De lerende kan toestemming geven voor deze gegevensuitwisseling via de wallet. Gegevens kunnen vervolgens worden uitgewisseld in de vorm van credentials om bijvoorbeeld vrijstellingen te geven.

Mapping, vertaling en waardering

Gegevensuitwisseling zal niet alleen plaatsvinden binnen de sector maar ook breder richting de maatschappij, waaronder andere sectoren en landen. In andere sectoren en landen worden andere betekenissen toegekend aan begrippen en kennen concepten vaak een andere opbouw, waardoor andere inhoudelijke gegevensmodellen ontstaan. Hierdoor ontstaat de behoefte aan mapping, vertaling en waardering van andere credentials. Ook hier kunnen assurance communities een rol spelen.

Voorbeelden huidige situatie

Ten behoeve van uitwisseling van studenten die zijn aangesloten bij het Erasmus-programma wordt gebruik gemaakt van begrippen die onderling gestandaardiseerd zijn. Op basis van deze standaarden kan eenvoudiger worden bepaald op welke gebieden een student voor uitwisseling in aanmerking komt. In de toekomstvisie van HOSA zou dit geautomatiseerd moeten kunnen door mappings tussen verschillende stelsels door bijvoorbeeld Nuffic te laten beheren en vandaar uit waardes te kunnen bepalen voor het uitgeven van credentials.

Relevante ontwikkelingen

- Actuele ontwikkelingen om betrouwbare stelsel voor uitwisseling van credentials op te bouwen zien we onder andere bij Europass. Daar wordt gewerkt aan het overstappen van papier gebaseerde certificaten naar verifiable credentials die wordt gebaseerd op European Digital Certification Infrastructure[21].

[21] Zie ook: https://europa.eu/europass/en/european-digital-credentials-learning-interoperability

5.5 Credentials

Opbouw van verifieerbare credentials

De W3C beschrijft de opbouw van een verifieerbare credential aan de hand van vier componenten. Deze zijn grotendeels vergelijkbaar met de opbouw van formele documenten zoals rijbewijzen of paspoorten. Het betreft de volgende componenten:

- Credential Identifier: dit betreft een uniek nummer op basis waarvan van het credential geïdentificeerd en opgezocht kan worden.
- Credential metadata: Een voorbeeld hiervan is de datum tot wanneer het bewijs geldig is.
- Claims: elke credential bevat een aantal claims over een subject waarover het credential gaat. Een paspoort kan bijvoorbeeld de claim bevatten dat iemand geboren is op 3 december 1981.
- Issuer Signature: Met de handtekening geeft de uitgever van het credential aan dat de credential daadwerkelijk is uitgegeven. Voor verifieerbare credentials wordt gebruik gemaakt van een digitale handtekening op basis van cryptografie.

Waar bewaren en beschikbaar stellen?

Om het geheel te kunnen laten werken worden er in de gewenste situatie verifieerbare credentials vanuit de sector uitgegeven. Deze credentials worden gegenereerd met behulp van informatiesystemen die kunnen worden gezien als bronsystemen voor deze credentials. De inhoudelijke betrouwbaarheid van de afgegeven credentials is afhankelijk van het bedrijfsproces dat het informatiesysteem vult. Vervolgens ontstaat het vraagstuk via welk scenario's deze credentials kunnen worden uitgegeven. Hiervoor zijn voor onderwijs en onderzoek hoofdzakelijk drie opties.

De eerste variant is dat de credentials op nationaal niveau door een sectorpartner worden bewaard en beschikbaar gesteld. Er is dan één overzicht dat te bevragen is voor dit credential. Dit speelt bijvoorbeeld een rol wanneer de gegevens een hoge actualiteit nodig hebben. Dit zou bijvoorbeeld kunnen gelden voor het afboeken van financieel krediet. Heb je nog voldoende krediet om deze dienst af te nemen?

De tweede variant is dat de credentials lokaal blijven staan bij de instellingen. De gegevens worden niet in één nationaal bestand geplaatst, maar zijn decentraal opvraagbaar bij instellingen. Dit zou bijvoorbeeld het geval kunnen zijn voor het credential of iemand een werknemer is bij een bepaalde instelling. Natuurlijk spelen privacy-aspecten hier een belangrijke rol. Een persoon geeft dan wel consent vanuit de eigen wallet, maar de credentials worden dan beschikbaar gesteld vanuit een lokale instelling.

De derde variant is dat de credential bij de persoon zelf komt te staan en daar op te vragen is. In de visie van Tim Berners Lee[22] zou een gebruiker zelf eigenaar moeten zijn van de eigen data. Het idee daarbij is dat informatiesystemen van organisaties dan geen of veel minder data bevatten over personen. De data wordt dan geplaatst bij de persoon of bij een door de gebruiker gekozen en vertrouwde provider die functioneert als een soort bank voor het beheren van gegevens en credentials. De gebruiker krijgt hierdoor een betere informatiepositie. In het verlengde hiervan zouden credentials dan ook bij de persoon kunnen worden vastgelegd en opgevraagd. Die credentials zijn dan vanuit een andere wallet aan te leveren als (deel)credentials bij nieuw uit te geven credentials binnen de HO-kaart.

Voorbeelden huidige situatie

DUO biedt in de huidige situatie de dienstverlening rondom MijnDiploma's. Een diploma wordt eenmalig afgegeven door een instelling en blijft daarna levenslang geldig. Het feit dat het diploma is behaald wordt vastgelegd bij DUO. Hierdoor kunnen personen digitaal bewijs van hun gehaalde diploma online opvragen. Deze worden in pdf-formaat beschikbaar gesteld, voorzien van een digitale ondertekening op basis van cryptografie. De diploma's kunnen alleen door de personen zelf direct worden opgevraagd en niet door anderen. Wel is het mogelijk om digitaal toestemming te geven aan bijvoorbeeld een werkgever voor het

[22] Solid (mit.edu)

eenmalig ophalen van een diploma. De pdf's gelden als volwaardig alternatief voor de oorspronkelijke diploma's en kunnen door de personen zelf worden gedeeld. Het gebruik van credentials zou in dit geval vergelijkbaar kunnen werken zoals we in de fysieke maatschappij gewend zijn.

Relevante ontwikkelingen

- Europass: Europass biedt European Digital Credentials die gelijkwaardig zijn aan papieren certificaten. Daarnaast beschikt Europass over een aantal standaarden gebaseerd op W3C, zoals Digital Credentials for Learning[23].
- Het datamodel voor Verifieerbare Credentials[24]
- Microcredentials: vanuit de UNL en de VH lopen pilots voor microcredentials. Het idee is dat mini-diploma's voor vakken uitgegeven kunnen worden in de toekomst. Dit betreft een voorbeeld van verifieerbare credentials.
- OOAPI en het datamodel van RIO geven een standaard beschrijving van data zodat deze uitgewisseld kan worden. Deze zou geschikt gemaakt moeten worden voor het beschrijven in termen van credentials.

5.6 Registry

Het gedachtengoed van SSI is veelvuldig toegepast in de wereld van blockchain. Bij blockchain pur sang staan de data over de uitgifte van credentials niet in een database op één plek, maar is de data gedistribueerd over meerdere partijen. Hierdoor kunnen partijen niet ongemerkt data aanpassen. Dat is vooral van belang als de partijen (of de gebruikers) onderling laag vertrouwen. Ook de applicaties kennen daarbij een gedistribueerde opzet. Dit is totaal verschillend met hoe applicaties in de huidige situatie worden opgezet. Veel experts raden daarom aan om voor use cases geen blockchain in te zetten als daar geen goede reden voor is.

Niet alle voorkomende use cases vereisen de inzet van een blockchain. In veel gevallen is het werken met een gedistribueerde append-only database (in blockchain-terminologie een ledger genoemd – een term die overigens is geleend uit de wereld van het boekhouden) niet nodig. Afwegingen hierbij worden gemaakt vanuit de volgende overwegingen:

- Gegevens mogen niet ongemerkt aangepast kunnen worden
- Hoge beschikbaarheid van de gegevens is noodzakelijk
- Delen van data tussen meerdere organisaties is vereist
- Vertrouwen tussen organisaties is vereist om eindgebruiker goed te kunnen bedienen
- Er zijn gedeelde afspraken vereist

In het onderste segment in de plaat plaatst de HOSA de uitgifte en de intrekking van credentials, alsook de sleutels waarmee relaties tussen entiteiten die gelegd kunnen worden door de entiteiten zelf geverifieerd kunnen worden. De inhoud van de credentials zelf en privacygevoelige data mogen nooit op deze laag terecht komen. Het betreft puur de sleutels die als bewijs kunnen dienen dat bepaalde credentials daadwerkelijk zijn uitgegeven.

Relaties tussen entiteiten kunnen door de entiteiten zelf worden gelegd met behulp van decentralized identifiers (DID). Een patroon om privacyvriendelijk te kunnen werken met DIDs is om DIDs zelf niet op te slaan in een publieke registry, maar alleen de hash daarvan. Een verifier kan dan controleren of de hash van de credentials die hem gepresenteerd worden klopt, en de gegevens dus valide zijn. Wanneer iemand bijvoorbeeld een beroep doet op het recht om vergeten te worden, dan kan de relatie tussen de DID en de

[23] European Digital Credentials for Learning | Interoperability | Europass

[24] Verifiable Credentials Data Model v1.1 (w3.org)

hash verbroken worden. De hash is dan niet meer te relateren aan de DID en ook niet aan de gegevens die de DID representeren.

Issuers moeten hun DID opnemen in een registry zodat verifiers weten met welke issuer ze te maken hebben. Issuers gebruiken hiervoor public DIDs. Daarnaast kan een issuer een schema van een credential publiceren in een registry. Hierdoor is de opbouw van een credential openbaar en is helder welke claims een credential van de issuer bevat. Ook een credential definition wordt in een registry beschikbaar gesteld. De credential definition bevat de public DID, een schema en public keys.

Voordat een issuer credentials gaat uitgeven is het van belang dat het kunnen intrekken van credentials goed geregeld is. Denk hierbij aan tijdelijke geldigheid van credentials of het intrekken bij fraude of misbruik. Bij tijdelijke geldigheid worden updates op de credentials en de registry periodiek uitgevoerd. Bij fraude moet het per direct intrekken mogelijk zijn. In de toekomstige situatie zijn aan het intrekken (revoking) van credentials waarschijnlijk extra kosten verbonden bij public registries. Voor het intrekken van credentials is een revocation registry vereist waarbij alleen de holder mag kunnen zien of een credential is ingetrokken. Vanuit privacy-oogpunt wordt ook wel gewerkt met de mogelijkheid voor een holder om een proof of non-revocation te genereren.

Voorbeelden huidige situatie

In de huidige situatie zijn er weinig voorbeelden van initiatieven die reeds functioneren op basis van een registry waar verifiers kunnen checken of credentials daadwerkelijk zijn uitgegeven. Dit heeft met name te maken met de volwassenheid van de technologie zoals beschreven in de visie. SURF voerde een technische verkenning uit naar de werking van een op een ledger gebaseerde Self Sovereign Identity.

Relevante ontwikkelingen

- Sovrin: De Sovrin Foundation is een nonprofit organisatie die de governance regelt rondom het Sovrin Network. Dit is een publieke service die self-sovereign identity op het internet mogelijk maakt.
- IDunion: het doel van IDunion organisation is een open ecosysteem te creeren voor decentralised identity management, dat wereldwijd gebruikt kan worden en is gebaseerd op Europese waarden en regelgeving.
- De European Blockchain Services Infrastructure (EBSI) maakt het mogelijk voor publieke organisaties om toepassingen te ontwikkelen die zijn gebaseerd op verifieerbare credentials. Op termijn kunnen ook commerciële bedrijven aansluiten.
- Non-Fungible Tokens (NFTs). Een NFT is een digitaal object dat in het bezit van een internetgebruiker is. Wanneer je een NFT koopt, word je eigenaar van het digitale object. Dit wordt middels een unieke token vastgelegd op de blockchain. NFT’s kun je online kopen en verhandelen.

6 Principes

De architectuur voor de HO-sector op het vlak van identiteit en toegang is faciliterend aan de verschillende platformen, bijvoorbeeld flexibel onderwijs. De onderstaande principes[25] zijn specifiek voor het onderwijsdomein en vormen deels een verbijzondering van principes die op HOSA algemeen niveau zijn gedefinieerd ten behoeve van identiteit en toegang. Voor de beschreven visie hebben we richtinggevende architectuurprincipes voor identiteit en toegang als richtlijnen voor het inrichten van de gewenste architectuur. Ze dienen als instrument voor en als verantwoording bij inrichtingsbeslissingen.

PRINCIPE: GEBRUIKERS VOEREN REGIE OVER HUN EIGEN DECENTRALE IDENTITEIT

Gebruikers voeren regie over hun eigen decentrale identiteit (waarbij 'decentrale identiteit' in de voorgaande principebeschrijving is gedefinieerd). Je kunt immers geen regie voeren over je eigen identiteit – hoogstens over je eigen partiële identiteit (je zelfbeeld). En doorgaans gaat het erover dat je (slechts) 'in control' bent over de gegevens over jezelf die je hebt gekregen van issuers en met anderen deelt. De 'control' bestaat er dan uit dat je ze (van je eigen 'middel'(en)) kunt verwijderen, en kunt besluiten wanneer je ze met wie gaat delen.

Het invullen van online formulieren wordt door eindgebruikers vaak ervaren als een onnodig tijdrovende en vervelende verplichting.[26] Een significant deel van dit probleem zou niet meer bestaan als diensten en voorzieningen, die nu nog gegevens verkrijgen op basis van door individuele personen (gebruikers) ingevulde formulieren - en deze (soms handmatig) moeten valideren, de betreffende gegevens elektronisch zouden kunnen opvragen en valideren. Er moet dan wel worden voorkomen dat zulke diensten en voorzieningen lukraak gegevens van personen op zouden kunnen gaan vragen, wat niet alleen niet de bedoeling is, maar ook door de Algemene Verordering Gegevensbescherming (AVG) verboden is. De AVG staat vrijwel elke verwerking, waaronder gegevensuitwisseling toe, wanneer de betrokkene (i.e. de persoon op wie de gegevens betrekking hebben) voor een arbitrair, maar wel specifiek en voor de persoon begrijpelijk doel, daarvoor vrijwillig en uitdrukkelijk toestemming heeft gegeven, d.w.z.: dat zelf wil, of: daar zelf de regie over voert. Overigens zijn er ook andere grondslagen waardoor toestemming niet altijd vereist is.

BESCHRIJVING VAN HET PRINCIPE (WAT IS HET)

Wat een organisatie over een persoon weet of meent te weten, blijkt uit de gegevens die over deze persoon zijn geregistreerd. Volgens artikel 15 AVG heeft deze persoon het recht hiervan kennis te nemen. Dit principe voegt hier aan toe dat de persoon zelf mag weten, ofwel de regie voert over wat deze met de opgedane gegevens gaat doen.

IMPLICATIES, CONSEQUENTIES

Het zelf mogen en kunnen voeren van regie houdt in dat eenieder attributen, tenminste die waarvan zij zelf het subject zijn, elektronisch kan verkrijgen bij organisaties die deze uitgeven en zulke verkregen attributen vervolgens al dan niet aan andere vaak digitale diensten en voorzieningen kunnen presenteren als die hierom vragen. Idealiter gebeurt er geen uitwisseling tussen dienstverleners onderling zonder medeweten of toestemming van het subject.

Dit houdt in dat iedereen die gebruik wil maken van diensten van de sector over een middel moet beschikken dat in staat is om verkregen attributen voldoende veilig op te slaan, opgeslagen attributen desgevraagd aan

[25] Met dank aan Rieks Joosten, Senior Scientist bij TNO

[26] Nationale Ombudsman (2019). "Houd het simpel – Een onderzoek naar de gebruiksvriendelijkheid van digitale formulieren van de overheid". Rapportnr 2019/046.

diensten en voorzieningen te presenteren, en over de opgeslagen attributen en uitwisselingen het beheer te voeren op een wijze die bij de persoon past.

Wat een HO-instelling of andere sectorpartner met iemands gegevens kan doen zal in de toekomst strakker geregisseerd gaan worden door de persoon zelf dan nu het geval is. Dit komt door het feit dat de instelling de alleen die elementen van een identiteit gebruikt die nodig zijn voor het beoogde verwerkingsproces.

PRINCIPE: GEBRUIKERS KUNNEN BESCHIKKEN OVER HUN CREDENTIALS ZOLANG ZIJ DIE NODIG HEBBEN

Bij het inrichten van credentials voor bijvoorbeeld diploma's, microcredentials of publicaties is een middel gewenst dat gedurende het gehele leven van de persoon bruikbaar is. Voor het uitgeven van bepaalde credentials dient de gebruiker te beschikken over mogelijkheden voor het verkrijgen, opslaan en gebruiken van credentials die levenslang beschikbaar en portabel moeten kunnen blijven.

BESCHRIJVING VAN HET PRINCIPE (WAT IS HET)

Een gebruiker beschikt op elk moment van diens leven over een wallet dat in staat is om attributen die de persoon zelf betreffen voldoende veilig op te slaan, opgeslagen attributen desgevraagd aan diensten en voorzieningen te presenteren en over de opgeslagen attributen en uitwisselingen het beheer te voeren op een wijze die bij de betreffende persoon past.

IMPLICATIES, CONSEQUENTIES

Een wallet is idealiter de combinatie van een opslag-functie (kluis) en een interface-functie. De opslag-functie kan in de cloud zitten, op een mobiele telefoon, een smart-card, secure usb-stick, enz. De interface-functie kan bijvoorbeeld verweven zijn in een browser, of als een app op een mobiel device. Hij kan 'op maat' zijn gemaakt voor verschillende groepen gebruikers, en de behoeften van de groep accommoderen.

De wallet moet niet alleen met de gebruiker, maar ook met services van andere partijen kunnen interfacen die de rol van issuer of verifier vervullen. De (elektronische) protocollen die hierbij worden gebruikt zijn in de gewenste situatie gestandaardiseerd. We voorzien ook dat er ge-interfaced moet kunnen worden met additionele nieuwe functies, die samenhangen met revocation, het (rechtsgeldig) digitaal ondertekenen van data, documenten, e.d.

Door het grote aantal mogelijke combinaties van uitgevers van credentials, verifiërende partijen en leveranciers van wallets is standaardisatie essentieel. Binnen de EU wordt gewerkt aan regulering om dit te bewerkstelligen.

Bij dit principe is van belang dat gebruikers de componenten die de opslag- en interface-functies vervullen kunnen en willen vervangen: daar zouden issuers en verifiers tegen moeten kunnen. De (onderdelen van) middelen zouden ook vervangen moeten kunnen worden. De gebruiker zou bijvoorbeeld een andere kluis, of een ander soort wallet willen gaan gebruiken. Dat mag de beschikbaarheid van de functionaliteit van het geheel – het kunnen ontvangen, opslaan en gebruiken van credentials bij partijen die daarom vragen – niet beperken. Consequentie is dat de functie behouden moet blijven bij het vervangen van de wallet. De credentials moeten dan middels de nieuwe wallet beschikbaar blijven.

PRINCIPE: CREDENTIALS BEVATTEN NIET MEER DATA DAN NODIG (DATAMINIMALISATIE)

Onder 'dataminimalisatie' wordt door artikel 5 lid 1c AVG verstaan dat gegevens (voor de verwerking – dat houdt ook in: het opvragen/verkrijgen) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Hoe duidelijk dit ook lijkt, in de praktijk kun je hier verschillend naar kijken.

Een manier is om te kijken naar de feitelijke uitvraag van gegevens. Als iemand een boek bestelt en dat bij een afhaalpunt gaat ophalen, is het niet nodig om diens naam, adres, telefoon etc. te vragen. De identificatie van het afhaalpunt, en een (af te spreken) gegeven op basis waarvan de toonder het boek kan afhalen, volstaat. Dit is een zaak van het ontwerp van (informatie)processen – in het bijzonder bij het ontwerp van de uitvraag-(formulieren) waar besluiten worden genomen over welke gegevens uitgevraagd gaan worden en welke daarvan 'verplicht' ingevuld moeten worden om het formulier te kunnen opsturen c.q. in behandeling te nemen. Deze vorm van dataminimalisatie zou binnen elke organisatie een ingesleten gewoonte moeten zijn (en is dat vaak nog niet).

Een andere manier is om te kijken naar de vorm waarin gegevens worden verstrekt. Soms worden gegevens gevraagd die alleen worden gebruikt om er een ander gegeven uit af te leiden: een geboortedatum kan worden gevraagd om vast te stellen of iemand ouder is dan (bijvoorbeeld) 18; een digitale handtekening kan worden gevraagd om vast te stellen dat deze door een specifieke partij is gezet. De gevraagde gegevens leveren echter meer dan de noodzakelijke informatie, en kunnen ook ongewenst of onbedoeld voor andere dingen worden gebruikt. Een maatschappelijk voorbeeld hiervan is bijvoorbeeld selectie van sollicitanten op basis van hun achternaam in plaats van hun kwalificaties.

BESCHRIJVING VAN HET PRINCIPE (WAT IS HET)

Onder 'dataminimalisatie' wordt verstaan dat gegevens die voor een zeker doel worden verwerkt, voor dat doel toereikend zijn, ter zake dienend zijn, en beperkt zijn tot wat voor dat doel noodzakelijk is. Dat is in eerste instantie een zaak van het ontwerp van (informatie)processen en de bijbehorende digitale uitvraag-formulieren. In tweede instantie kan hier ook gaan over dat te specifieke informatie wordt gevraagd terwijl dit niet vereist is.

IMPLICATIES, CONSEQUENTIES

De omvang van digitale formulieren en invulvelden worden beperkt tot het minimum noodzakelijke. Partijen moeten voldoen aan de AVG en dus ook dit principe hanteren. Bewustwording moet vergroot worden bij de ontwerpers van processen en systemen, zodat er meer alternatieven voor ontwerpkeuzes overwogen worden voordat tot een zekere gegevensvraag wordt besloten.

Belangrijk uitgangspunt is dat informatiesystemen zo min mogelijk privacygevoelige gegevens vragen aan eindgebruikers voor het verlenen van toegang. Dit doen ze door het gebruik van Zero Knowledge Proof te faciliteren. De inzet van cryptografische technieken zoals zero-knowledge proofs (ZKPs) maken dit mogelijk.

PRINCIPE: BETROUWBAARHEID IS GEBORGD IN EEN TRUST FRAMEWORK IDENTITEIT, AUTHENTICATIE EN FEDERATIE (LEVEL OF ASSURANCE)

Wanneer mensen gebruik maken van een dienst of voorziening, dan moet de aanbieder daarvan besluiten om dat verzoek in te willigen of af te wijzen. Om dat besluit te kunnen nemen zijn niet alleen gegevens nodig, maar die gegevens moeten ook voldoende gevalideerd zijn, en dat moet worden vastgesteld vóórdat het eerdergenoemde besluit kan worden genomen (omdat ongeldige gegevens tot een ongeldig besluit kunnen leiden). De partij die de dienst of voorziening runt dient dus na te gaan op basis van welke criteria hij gaat besluiten dat gegevens, die nodig zijn om te kunnen besluiten om een verzoek in te willigen, voor dat doel valide (geldig) zijn. Doorgaans hangen de criteria af van de risico's die deze partij denkt te lopen als het besluit ongeldig zou blijken te zijn.

Aanbieders van gegevens (issuers) kunnen zich committeren aan eisen voor het vaststellen en uitgeven van die gegevens, zoals die door zogenaamde 'trust frameworks' zijn gespecificeerd. Deze trust frameworks definiëren niet alleen zulke requirements, maar stellen ook verzamelingen van requirements ('niveaus') vast die elk een oplopende moeilijkheidsgraad hebben om eraan te voldoen. Issuers kunnen dus gegevens uitgeven van een zeker niveau (volgens een zeker trust framework). Het idee is dat deze niveaus het voor voorzieningen- en dienstverleners eenvoudiger maakt om hun validiteitscriteria vast te stellen. De sector sluit aan bij passende frameworks door een helder selectieproces en criteria.

Veel trust frameworks (waaronder eIDAS, NIST 800-63-B, ISO/IEC 29115) beperken zich overigens tot gegevens als identifiers, of NAW-achtige attributen. Die zijn echter vooral bedoeld/geschikt om het risico te mitigeren dat een dienstverlener loopt als hij het nodig vindt de persoon in een juridische procedure te dagen, of te kunnen voldoen aan wettelijke verplichtingen.

BESCHRIJVING VAN HET PRINCIPE (WAT IS HET)

Om (runtime) te besluiten of gegevens op een geldige (valide) manier kunnen worden verwerkt tot een resultaat (zoals het besluit om al dan niet toegang te verlenen tot een dienst of voorziening), moet de partij die de dienst/voorziening levert (design-time) criteria kunnen vaststellen op basis waarvan dat (runtime) besluit (elektronisch) kan worden genomen.

Een trust-framework voorziet in verzamelingen requirements van verschillende 'niveaus' (moeilijkheidsgraad). Verstrekkers van gegevens-sets die aan de vereisten voor een zeker niveau voldoen, kunnen die gegevens als zodanig kenmerken. Voor leveranciers van diensten en voorzieningen die hierop kunnen rekenen, wordt het niet alleen eenvoudig om voor dat type gegevens validiteits-criteria vast te stellen, maar ook gemakkelijk om die run-time te verifieren.

IMPLICATIES, CONSEQUENTIES

In de praktijk zien we dat men vaak voor een of ander framework kiest, omdat anderen datzelfde framework hebben gekozen. Goede keuzes voor frameworks dragen bij aan gebruikersgemak. De sector sluit aan bij passende frameworks door een helder selectieproces en criteria.

Trust frameworks faciliteren de betrouwbaarheid van gegevens die tussen partijen uitgewisseld moeten of kunnen worden. Dat doen ze door verzamelingen van requirements te specificeren en die te labelen (zo'n label noemen we een 'niveau'). Verstrekkers van gegevens kunnen aangeven aan welk niveau hun gegevens voldoen. Een partij die een dienst of voorziening aanbiedt en voor de levering daarvan gegevens van verstrekkers nodig heeft, kan deze niveaus gebruiken als onderdeel van de criteria op basis waarvan hij vaststelt of die gegevens al dan niet geldig zijn om de dienst/voorziening mee te leveren. Het gebruik maken van een beperkt aantal niveaus door een dienst/voorzieningsaanbieder is veel gemakkelijker dan dat hij zelf soms complexe validiteitscriteria gaat opstellen en beheren.

PRINCIPE: BIOMETRIE WORDT TERUGHOUDEND EN GELOKALISEERD TOEGEPAST

Toepassing van biometrie kan in grote mate bijdragen aan de toegankelijkheid en betrouwbaarheid van dienstverleningsprocessen. Koppeling van biometrie aan een decentrale identiteitsinfrastructuur zoals SSI biedt technisch aantrekkelijke mogelijkheden voor hoog betrouwbare identificatie en authenticatie.

Tegenover gebruiksgemak en hoge betrouwbaarheid staan grote gevolgen voor de gebruiker bij lekken en misbruik. Anders dan bij een toegekend identificerend kenmerk (bijvoorbeeld een gebruikersnaam, studentnummer of burgerservicenummer) is het niet makkelijk om de biometrische identificerende kenmerken van een gebruiker te veranderen. Biometrische kenmerken zijn niet los te koppelen van een persoon. Gebruikers kunnen bezwaren tegen gebruik en vastlegging van biometrische kenmerken hebben. Daarnaast is niet voor alle gebruikers biometrie even betrouwbaar (gezichtskenmerken kunnen bijvoorbeeld veranderen – zeker bij jongeren) en levert biometrie nieuwe mogelijkheden op om beveiligingsmechanismen te doorbreken (bijv. het gebruik van een foto of filmpje i.p.v. het echte gezicht).

De verwerking van biometrische gegevens met het oog op unieke identificatie van een persoon is daarom in beginsel verboden. Gebruikers kunnen dus normaliter niet worden verplicht hun biometrische gegevens digitaal te delen. Het aantal gevallen waarin biometrische gegevens *kunnen* worden toegepast (als tweede factor) om de zekerheid over de identiteit van een gebruiker te vergroten is daarom zeer beperkt:

1. Expliciete wettelijke grondslag, of
2. Strikte noodzakelijkheid en proportionaliteit voor de beoogde authenticatie- of beveiligingsdoelstellingen[27], of
3. Uitdrukkelijke *vrijelijke* toestemming van de gebruiker

In de meeste situaties binnen het HO zal de derde mogelijkheid van toepassing zijn. Belangrijk is de vrijelijke toestemming: in een afhankelijkheidsrelatie of machtsverhouding (zoals werkgever-werknemer of instelling-student/leerling) is daarvan geen sprake omdat de betrokkene druk zal voelen in te stemmen. Bovendien moet er een ander alternatief beschikbaar zijn, toestemming moet ingetrokken kunnen worden en aan de weigering mogen geen nadelige gevolgen verbonden zijn.

Het is voorstelbaar dat toekomstige regelgeving biometrie toelaat in specifieke gevallen (bijv. toepassing bij het halen van een bepaald hoog betrouwbaarheidsniveau), echter ook dan blijft aantonen van noodzakelijkheid en proportionaliteit essentieel.

BESCHRIJVING VAN HET PRINCIPE (WAT IS HET)

Biometrie kan enkel in uitzonderlijke gevallen worden gebruikt, en is in alle overige gevallen verboden. Het principe bewerkstelligt dat de juiste afwegingen kunnen worden gemaakt, en dat er wordt nagedacht over oplossingen die het gebruik van biometrische gegevens drastisch beperken.

- *Biometrie* wordt terughoudend toegepast: het is alleen mogelijk, als er aan de voorwaarden van de uitzonderlijke gevallen wordt voldaan. Universele toepassing van biometrie is wettelijk niet toegestaan.
- *Als tweede factor*: toegang tot systemen en processen mag niet enkel op biometrie steunen.
- *Gelokaliseerd*: uitsluitend in oplossingen voor identificatie, authenticatie en beveiliging, in de directe gebruikscontext van de gebruiker, onder directe controle van de eigenaar.

[27] Art. 9(2)(a) AVG; art. 9(2)(g) jo. (4) AVG jo. art. 29 UAVG.

- *Alternatief zonder biometrie is default*: toegankelijkheid voor gebruikers die geen toestemming voor biometrie geven moet geborgd blijven.
- *Uitdrukkelijke vrijelijke toestemming*: wettelijk vereiste, in ieder geval voor toepassingen waar geen zwaarwegend belang is.

Dit principe gaat niet over toepassing van biometrische gegevens in bijvoorbeeld wetenschappelijk of medisch onderzoek. Dergelijk gebruik valt buiten de kaders van IAM.

IMPLICATIES, CONSEQUENTIES

Enrollment/onboarding-processen voor toegang tot onderwijs en onderzoek vermijden direct gebruik van biometrische gegevens. Wel kunnen zij gebruik maken van authenticatiediensten die biometrie toepassen, mits er voor deze diensten een uitdrukkelijke wettelijke grondslag[28] of van diensten met meerdere methoden waarbij de gebruiker vrijelijk heeft ingestemd met toepassing van biometrie. Dergelijke authenticatiediensten passen biometrische gegevens uitsluitend toe bij verificatie van de gebruiker, mits deze niet buiten die context gedeeld worden (met andere woorden: biometrische kenmerken kunnen worden gebruikt in directe, beveiligde interactie met de gebruiker op zijn device, maar worden nooit buiten die sessie gedeeld).

Bij gebruik van biometrie dient daarvoor uitdrukkelijke toestemming gegeven te zijn door de gebruiker en deze toestemming dient te zijn vastgelegd. Inzage en intrekking zijn altijd mogelijk. Gebruikers hebben de mogelijkheid af te zien van gebruik van biometrische gegevens en om op alternatieve manieren hun identiteit aan te tonen.

Authenticatieprocessen waarbij biometrie mag worden toegepast worden zodanig vormgegeven dat er geen verspreiding en opslag van biometrische kenmerken plaatsvindt buiten de sessie waarin de authenticatie wordt gedaan. Biometrie die wordt toegepast voor versterking van de authenticatie mag niet leiden tot uitwisseling van biometrische gegevens die ‘verderop in de keten’ worden verwerkt.

Dataminimalisatie, privacy-by-design en security-by-design zijn hiervoor *essentieel*, net als expliciete verantwoording over en controleerbaarheid van het gebruik van biometrische gegevens. Normenkaders, standaarden, risico-analyses en toetsingen op de daaruit voortkomende maatregelen zijn noodzakelijke elementen. Deels moeten deze normenkaders en standaarden nog worden ontwikkeld.

Gebruik van biometrische gegevens kan een sterke afhankelijkheid creëren van marktpartijen die de (mobiele) devices leveren die zijn uitgerust met biometrische sensoren. Bij inzet van biometrie moet erop gelet worden dat ingezette technologie voldoende toegankelijk is op devices van meerdere aanbieders, aanbieders de normen en waarden van de onderwijs- en onderzoekssector respecteren en implementaties uitsluitend noodzakelijke biometrische kenmerken verwerken, ook al geeft de device meer vrij dan nodig is.

Direct gebruik van biometrie binnen onderwijs- en onderzoeksprocessen blijft beperkt tot gevallen waarvoor een uitzonderingsgrond is. Voorbeelden zijn situaties waarbij een hoge mate van zekerheid over de identiteit van de gebruiker noodzakelijk is, bijvoorbeeld bij inschrijving, toetsing en examinering. Een ander voorbeeld is toegang tot en delen van zeer vertrouwelijke of privacygevoelige gegevens en processen waaronder de eigen wallet, persoonlijke kluizen of andere persoonlijke omgevingen.

Afgeleid gebruik heeft de voorkeur wanneer biometrie wordt toegepast. Hierbij worden de biometrische kenmerken alleen gebruikt in het authenticatieproces, maar daarbuiten niet gedeeld. Het authenticatieproces mag het middel waarover de gebruiker de volledige controle heeft niet verlaten. Bijvoorbeeld het

[28] Op moment van schrijven is een dergelijke grondslag er *niet*!

elektronische identiteitsbewijs en de daarop opgenomen biometrische kenmerken van een persoon hebben bijgedragen aan zeer betrouwbare authenticatie of ondertekening, maar de biometrische gegevens zelf worden niet gedeeld in een afgegeven credential of verklaring.

Bijlagen

Bijlage A: Geraadpleegde personen & gremia

Werkgroep IAM

- Mark de Jong (Inholland)
- Caspar Terheggen (RU)
- Michiel Schok (SURF)
- Tom van Veen (SURF)
- Menno Scheers (VU)
- Mark van Bree (Saxion)
- Stefan Suurmeijer (RUG)
- Maarten van Schie (LU)
- Femke Morsch (SURF)
- Henk Schouten (HHS)
- Jan Over (EUR)
- Alexander Carlucci (WUR)
- Joël van der Elst (UL)

Stuurgroep HOSA

- Jan-Willem Brock (Leiden Universiteit)
- Hans Louwhoff (SURF)
- Anton Opperman (EUR)
- Rose van Iperenburg (HAN)
- John Kropman (Fontys)
- René Schenk (Avans)

Klankbord & brainstormgroep

- Sterre den Breeijen (TNO)
- Johann Schreurs (DUO)
- Jelle Nauta (DUO)
- Niels van Dijk (SURF)
- Menno Nonhebel (KNAW)
- Alexander van den Wall Bake (TNO)

Gesprekken

- Bob te Riele (RvIG)
- Andre de Kok (RvIG)
- Jimmy Snoek (Tykn)
- Christien Bok (SURF)
- Erwin Bomas (Kennisnet)
- Bart Cozijn (BZK)
- Caspar Terheggen (Radboud Universiteit)
- Joris Dirks (Studielink)
- Bart Jacobs (Professor of Security, Privacy and Identity; Radboud Universiteit)
- Frank Snels (Utwente)
- Stephan Okhuijsen (Vrije Universiteit)
- Rieks Joosten (TNO)
- Michiel Kraaij (WUR)
- Frank Niesten (Fontys)
- Nuffic/ Erasmus+
- Andre Koot (Sonicbee)

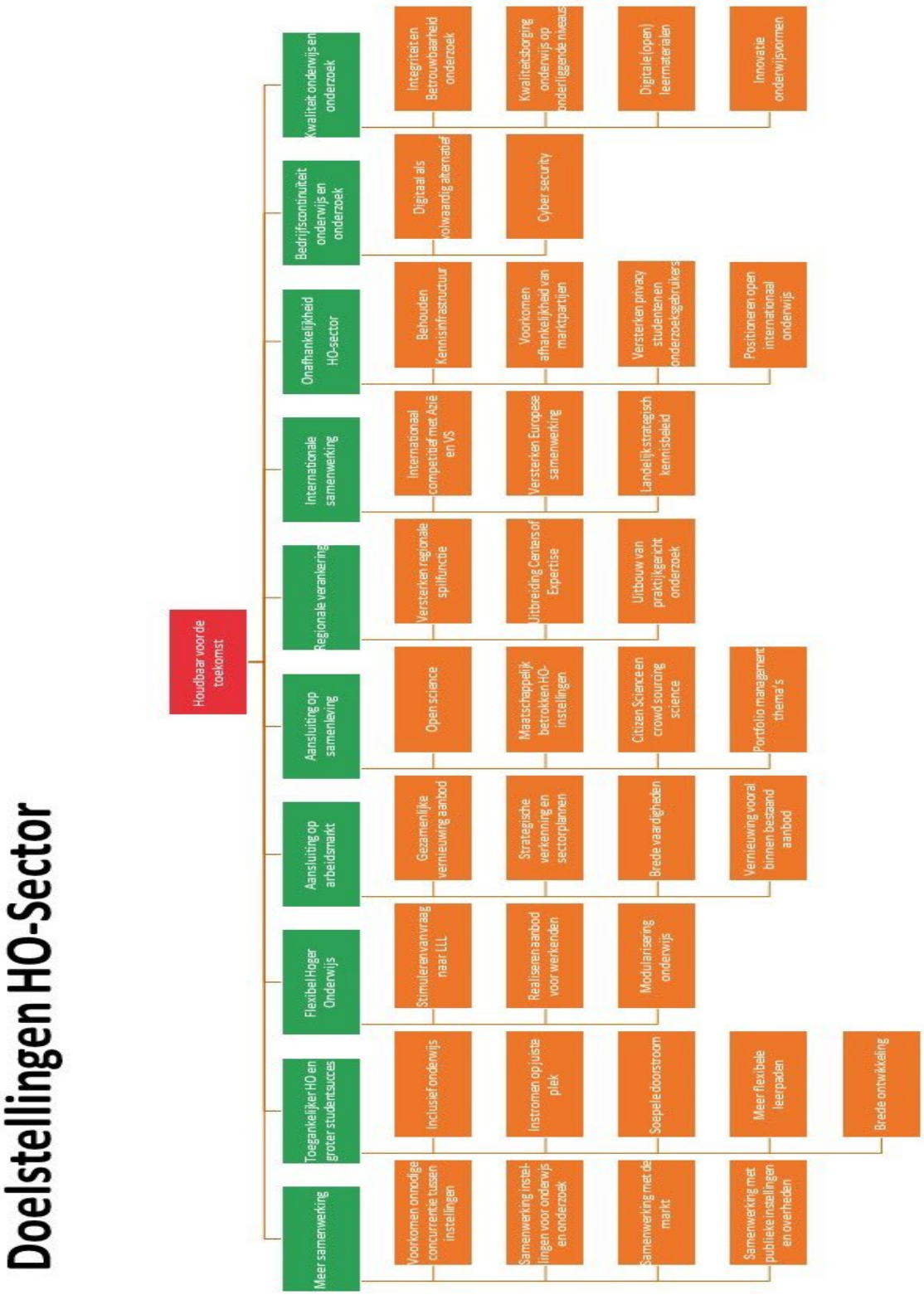
Review

1e. Klankbord & brainstormgroep
2e. SURF Enterprise Architectuur
3e. Werkgroep IAM
4e. Landelijk Architectenberaad HO
5e. Sectorpartners (Studielink, DUO, NWO, KNAW, TNO, MBOdigitaal, Kennisnet)

Sessies

- Presentatie Edustandaard
- Sessie met team eduID
- EWUU
- CSC HBO
- TNO inhoudelijke sessie SSI
- Sectorpartners (Studielink, DUO, KNAW, TNO, MBOdigitaal, Kennisnet)

Bijlage B: Doelenstructuur HO-Sector



Bijlage C: Ambities van de sector

De HO-sector heeft sterke ambities op het gebied van het onderwijs en onderzoek. Er zijn al veel samenwerkingsverbanden en overleggen om hierin stappen te kunnen maken, maar die zijn nog onvoldoende om de ambities op sectorniveau vorm te geven. OCW heeft met de sector daarom een aantal doelstellingen geformuleerd in de strategische agenda hoger onderwijs en onderzoek[29]. Nadruk hierbij wordt gelegd op (regionale, nationale, internationale) samenwerking en onafhankelijkheid van de HO-sector. In de onderstaande paragrafen worden deze ambities kort besproken.

Regionale en Nationale samenwerking

Vanuit de strategische agenda is gesteld dat er o.a. meer regionale en nationale samenwerking moet plaatsvinden tussen de verschillende instellingen binnen het hoger onderwijs. Versterken van de regionale spilfunctie van HO-instellingen om hiermee bijvoorbeeld innovatie en kennisoverdracht te versterken. De regio is geholpen met een eenduidige benadering vanuit het HO. Daarbij dient er geen concurrentie vanuit instellingen op te treden binnen de regio. De HO-sector kan een verbindende rol spelen bij projecten in een regio die discipline overstijgend zijn, zowel op inhoud als op facilitering voor realisatie. Een prominentere plek voor het praktijkgericht onderzoek zal hierbij een rol moeten spelen om de continuïteit in de regio zichtbaar te maken. Een mooi beeld hierbij zou zijn dat studenten uit de regio een invulling kunnen geven die is gebaseerd op kennis en kunde vanuit de landelijke HO-diensten die vanuit de sector worden geboden voor bijvoorbeeld het samenwerken en delen van gezamenlijk onderzoek en ontwikkelingen. Dit kan ook worden gerealiseerd in het LLO door professionals binnen de regio. Voor regionale en nationale samenwerking over de grenzen van de sector heen met bedrijven en overheden is een drempelloze digitale identiteit en gecontroleerde logische toegangscontrole randvoorwaardelijk. Een dergelijke identiteit overstijgt de grenzen van de individuele organisaties en overstijgt ook de grenzen van de HO-sector.

Internationale samenwerking

Er is sprake van toenemende mondiale concurrentie in onderwijs en onderzoek. Onder andere China, de Verenigde Staten maar ook ons buurland Duitsland doen in hoog tempo ambitieuze investeringen in onderwijs en onderzoek. Veel opkomende economieën ontwikkelen zich van lagelonenland tot kenniseconomie. Samenwerking op Europees niveau wordt daarom steeds belangrijker; de veranderende geopolitieke context vereist daarnaast een meer strategisch kennisbeleid. Om competitief te blijven is naast nationale samenwerking internationale, in het bijzonder Europese, samenwerking nodig. Initiatieven als Erasmus Without Papers geven daar al invulling aan. Nederland kent een open en excellent onderzoeksysteem dat in Europa goed scoort en heeft samenwerkingsverbanden met verschillende Europese Universiteiten De volgende Nederlandse universiteiten nemen deel: Eurotech (TU Eindhoven), Aurora (VU), CHARM-EU (UU) en YUFE (UM). Het versterken van de samenwerking binnen de EU om internationaal competitief te kunnen blijven met Azië en de VS. Instellingen werken vaker samen in internationale consortia. Voor internationale samenwerking is een inzet van een erkend internationaal betrouwbare digitale identiteit inzet en gecontroleerde logische toegangscontrole rand voorwaardelijk.

Flexibel hoger onderwijs

Meer flexibiliteit in het hoger onderwijs is nodig om het onderwijs beter te laten aansluiten bij de verschillende kenmerken en behoeften van de diverse doelgroepen. Ook is het nodig omdat de arbeidsmarkt waar het hoger onderwijs op voorbereidt verandert door digitalisering, globalisering en vergrijzing. De trends beïnvloeden het type werk, de kwaliteit van werk en de gevraagde skills en competenties. Modularisering van onderwijseenheden en certificering waardoor studenten flexibel kunnen studeren wat betreft studietempo, locatie, samenstelling van vakken, diepgang van de inhoud en vorm van het leren zullen daarvoor moeten worden ingevuld.

[29] Bron: Strategische agenda hoger onderwijs en onderzoek – Houdbaar voor de toekomst

Met flexibel hoger onderwijs neemt de mobiliteit van onderwijs deelnemers sterk toe en komt de onderwijs deelnemer centraal te staan i.p.v. de instelling. Digitale identiteit wordt persoonsgebonden en onder regie van de onderwijsdeelnemer.

Leven Lang Ontwikkelen

De voortdurende verandering van functies en bijbehorende vaardigheden vereist dat een leven lang gewerkt moet worden aan ontwikkelen van kennis en vaardigheden. Leven Lang Ontwikkelen heeft als doel dat burgers zich voortdurend kunnen ontwikkelen voor veranderende beroepen. Het creëren van het aanbod en de benodigde middelen om dit inpasbaar te maken voor de arbeidsmarkt vraagt om innovatieve oplossingen die het ontwikkelen mogelijk maken. Hiervoor is een aansluiting dicht op de veranderingen benodigd om het aanbod actueel te houden. Leven Lang Ontwikkelen vraagt om het beschikbaar hebben en gebruik van digitale identiteiten die niet alleen instellingsoverstijgend zijn, maar ook HO-sector overstijgend.

Integriteit en betrouwbaarheid

Integriteit en betrouwbaarheid zijn cruciaal voor het vertrouwen van de maatschappij in onderwijs en onderzoek. Bij onderwijs moeten bijvoorbeeld werkgevers er vanuit kunnen gaan dat afgestudeerden beschikken over het juiste niveau van kennis en competenties. Allerlei checks en balances in het proces zorgen voor deze integriteit en betrouwbaarheid. Bijvoorbeeld een examencommissie die ondertekent dat een student heeft voldaan aan de eisen of een auditcommissie die akkoord geeft op de kwaliteit van onderwijs. Naar de toekomst toe worden deze ondertekeningen waarschijnlijk gedigitaliseerd zodat ze op latere momenten weer gebruikt of getoond kunnen worden. Hiermee kan efficiëntie worden gecreëerd, maar ook meer vertrouwen. In onderzoek spelen integriteit en betrouwbaarheid ook een grote rol. Voor burgers is het soms lastig om wetenschappelijke kennis op internet te onderscheiden van fake content. Naar de toekomst toe zal dit alleen maar lastiger worden. Om vertrouwen van de maatschappij in onderzoek te versterken zijn nieuwe digitale hulpmiddelen nodig die bijvoorbeeld herleidbaarheid van wetenschappers organiseren of kunnen aantonen dat een bepaalde website van een wetenschappelijk onderzoek daadwerkelijk betrouwbaar is.

Onafhankelijkheid

Instellingen binnen de HO-sector bieden onderwijs aan en doen onderzoek met inachtneming van publieke waarden. De publieke waarden zorgen bijvoorbeeld ervoor dat onderwijs breed toegankelijk is voor deelnemers aan onderwijs en dat instellingen binnen HO-sector onafhankelijk zijn van overheid of en private marktpartijen. De publieke waarden van het hoger onderwijs niet alleen essentieel voor de instellingen afzonderlijk maar de Nederlandse samenleving. De publieke waarden die voor de HO-sector fundamenteel zijn, komen meer en meer onder druk te staan door de sterke groei van de digitalisering van de HO-sector. De HO-sector maakt op steeds grotere schaal gebruik van clouddiensten van internationale commerciële aanbieders. Hierdoor is de HO-sector steeds meer afhankelijk van de roadmap een beperkte groep van commerciële aanbieders. De HO-sector wil voorkomen dat de onafhankelijkheid van onderwijs en onderzoek verder onder druk komt te staan.

Bedrijfscontinuïteit

In de SURF jaarlijkse publicatie Cyberdreigingsbeeld van 2020-2021[30] wordt een toegenomen dreigingsbeeld geschetst, waarbij bijvoorbeeld cyberaanvallen kunnen uitgroeien tot een heuse crisis. Een crisis die niet alleen van grote betekenis is voor de betrokken instelling, maar die ook impact heeft op de hele sector. Diverse organisaties in de sector hebben te maken gehad met een ransomware-aanval waardoor deze een aantal weken moesten sluiten en de activiteiten volledig stil kwamen te liggen. Ook rondom COVID kwam de businesscontinuïteit in het geding. Instellingen in de sector moesten versneld volledig online onderwijs en onderzoek mogelijk maken en zo continuïteit van onderwijs en onderzoek bieden. Het borgen van businesscontinuïteit is van groot belang voor sectorvoorzieningen van de toekomst waar HOSA de kaders voor schetst.

[30] Bron: CYBERDREIGINGSBEELD 2020-2021 • ONDERWIJS EN ONDERZOEK • SURF

Bijlage D: Ontwikkelingen

Komend deel beschrijft de ontwikkelingen op functioneel en technologisch gebied voor het domein Identiteit en Toegang. Daarbij zijn een aantal zaken geïdentificeerd die mogelijk relevant zijn bij de toekomstige ontwikkelingen binnen de HO-sector. De ontwikkelingen die als mogelijk relevant worden gezien door de werkgroep Identity & Access Management zijn opgehaald uit publicaties vanuit wetenschap, beleidsdocumenten en media.

1. Ontwikkelingen op gebied van Identiteit

Nederlandse Digitale Bronidentiteit

De Nederlandse overheid heeft begin 2021 een visie op digitale identiteit en de bijbehorende infrastructuur gepubliceerd en hierover een kamerbrief gestuurd naar het Nederlandse parlement[31]. De kamerbrief beschrijft de uitdagingen en kansen en schetst een toekomstbeeld waarin de Nederlandse overheid vier activiteiten op zich neemt dan wel uitbreidt: het (mogelijk maken van het) delen van betrouwbare gegevens, het organiseren van toegang tot digitale dienstverlening, het uitgeven van een erkende digitale bronidentiteit en het organiseren van de bijbehorende wet- en regelgeving rond digitaal vertrouwen.

De digitale bronidentiteit is de set basisattributen bij de overheid op basis waarvan identiteitsbewijzen (virtueel en fysiek) en authenticatiemiddelen kunnen worden uitgegeven. De digitale bronidentiteit is voor burgers. Zij kunnen zelf geverifieerde gegevens delen met partijen naar eigen keuze. De Nederlandse overheid werkt voor dit doel aan een gezaghebbende bron: de digitale bronidentiteit. Dit is een digitale versie van de identiteitsgegevens die de Nederlandse overheid van burgers heeft geregistreerd.

Het Wettelijke identiteitsdocument (WID) kun je vergelijken met een fysiek paspoort of identiteitsbewijs. Met de WID word je geïdentificeerd bij een bank voor het verkrijgen van een bankpas of bij de organisatie voor het verkrijgen van een bedrijfspas. Een bankpas en een organisatietoegangspas zijn voorbeelden van zogenoemde afgeleide identiteitsmiddelen. Het beeld is dat afgeleide identiteitsmiddelen in principe uitgeven kunnen worden door partijen in de publieke en private sector.

Burgers krijgen de beschikking over hun gegevens via toegelaten identiteitsmiddelen. Ze gebruiken dus niet de digitale bronidentiteit, maar afgeleide identiteiten in de vorm van een toegelaten identiteitsmiddel. Dit toegelaten identiteitsmiddel gebruikt de digitale bronidentiteit om hun betrouwbaarheid te baseren op de ‘gezaghebbende bron’ van de Nederlandse overheid. Een voorbeeld van een identiteitsmiddel zou een app (wallet) kunnen zijn op een mobiel apparaat waarbij de gebruiker van de app zelf kan bepalen met wie hij delen van beschikbare identiteitsgegevens deelt.

Publieke sector eID

Publieke eID-regelingen worden normaal gesproken door overheden of rechtspersonen met een wettelijke taak aangeboden, zodat burgers een veilige manier hebben om toegang te krijgen tot onlinediensten. Inschrijven bij DUO en studielink gaat met DigiD. Private taken kunnen onder de huidige wetgeving niet met DigiD.

Private sector eID

Vooral social media-bedrijven wedijveren om identity-oplossingen te bieden, maar ze staan niet alleen. Social login is de naam die wordt gegeven aan de identificatie- en loginoplossingen die worden aangeboden door socialmedia-bedrijven. Deze oplossingen scoren meestal hoog in termen van gebruikersgemak en ervaring, aangezien gebruikers doorgaans in staat zijn om met een paar klikken accounts aan te maken en deze opnieuw

[31] https://zoek.officielebekendmakingen.nl/kst-26643-743.html

te gebruiken voor een reeks andere services. Ze scoren echter relatief laag in termen van het niveau van vertrouwen en zekerheid dat ze bieden. Deze accounts hebben doorgaans geen identiteitsbewijsfase waarin gebruikers bewijzen wie ze zijn met een wettelijk identiteitsbewijs en fysieke verificatie. Als zodanig zijn ze niet geschikt voor gevoeligere situaties waarin het essentieel is om te verifiëren wie de gebruiker werkelijk is.

Slechts zes grote internetplatforms domineren social login. Goed voor 87% van de sociallogінmarkt: Facebook, Google Sign-In, Instagram, LinkedIn, Twitter en Amazon. Daaronder zitten Facebook en Google aan het stuur, met respectievelijk 41% en 35% van de Europese gebruikers.

Ook financiële instellingen en banken hebben in deze markt een sterke positie. Zij hebben sterke identificatieoplossingen ontwikkeld zodat klanten toegang hebben tot hun aanbod van internetbankieren. In veel gevallen hebben ze een stap verder gezet om deze identificatieoplossingen voor andere onlinediensten aan te bieden. Daarnaast bieden mobiele netwerkoperatoren hun klanten gewijzigde simkaarten aan die mobiele identificatieoplossingen mogelijk maken. Ten slotte is er een nieuwe reeks speciale digitale identiteitsbedrijven en digitale identiteitsnetwerken ontstaan, die niet noodzakelijkerwijs voortkomen uit een reeds bestaande gebruikersgroep maar een veilige en ongecompliceerde identificatiemethode bieden.

Bring Your Own Identity (eID)

Bring Your Own Identity ”(BYOID) is een groeiende trend in de wereld van digitale identificatie. Het omvat het hergebruik van één digitale identiteit om toegang te krijgen tot een reeks verschillende onlinediensten van zowel de publieke als de private sector. EID-regelingen voor de publieke sector, bijvoorbeeld Chave Móvel Digital in Portugal of de Duitse eID-regeling, zijn een vorm van BYOI. Een groeiend aantal particuliere organisaties biedt echter ook BYOI-oplossingen voor hun gebruikers.

De oorsprong van "Bring Your Own Identity" kan worden gevonden in de wildgroei van digitale diensten die verschillende wachtwoorden vereisen om toegang te krijgen. Veel gebruikers zijn de noodzaak om deze veelvoudige wachtwoorden en identificatieprocedures te onthouden en te beheren beu geworden. Als reactie hierop hebben bedrijven een reeks verschillende identificatie-opties ontwikkeld om een veilige, gebruiksvriendelijke manier te bieden om te bewijzen wie je bent. Deze oplossingen zijn herbruikbaar voor alle diensten, van detailhandel tot bankieren en entertainment.

Groot nadeel van de groei van BYOI is dat grote internetplatforms en bedrijven met grote gebruikersbestanden veel informatie over een gebruiker makkelijk kunnen koppelen en zo grote profielen kunnen samenstellen. Vanuit de HO-sector wordt dit gezien als in strijd met publieke waarden. Daarnaast wordt met een ‘Bring Your Own Identity’ een afhankelijkheid gecreëerd van een intermediaire partij. Deze intermediaire partij bezit veel macht over de relaties die een persoon heeft. Wanneer deze wegvalt of de toegang ontzegt is een persoon alle relaties kwijt.

Self-Sovereign Identities (SSI)

Self-sovereign identity (SSI) is een stroming rondom identiteiten die de volledige beheersing over de eigen identiteit en data terug te geeft aan de individuele gebruiker. SSI is een concept dat steeds populairder wordt volgens marktanalisten. We zien voor SSI verschillende termen zoals blockchain-identiteit, gedecentraliseerde identiteit en draagbare digitale identiteit behoren tot de meest populaire, hoewel deze termen nog steeds beperkingen bevatten bij het beschrijven van SSI. Er kan bijvoorbeeld een gedecentraliseerd identiteitsschema bestaan waarbij het individu niet betrokken is, of hem geen controle geeft over zijn identiteit.

Een cruciaal aspect van SSI is dat het een verandering ondersteunt in de manier waarop identiteit wordt behandeld door bedrijven, gebruikers en overheidsinstanties. De meest pure vorm van SSI gebruikt Distribute Ledger Technology (DLT), waarvan blockchain de bekendste vorm is. Blockchain is een veelvoorkomend architectonisch onderdeel van SSI-oplossingen. Blockchain biedt een onderliggende "betrouwbare" basis voor het bewijs dat uitgewisselde identiteitsgegevens correct zijn en niet vervalst.

Het kan deze basis geven vanwege zijn inherente sterke punten als een gedistribueerd grootboek en een opzet volgens principes van privacy by design. Door een grootboek van transacties toegankelijk te maken voor meerdere partijen kunnen gegevens niet ongemerkt gemuteerd of vervalst worden. Privacy by design wordt bijvoorbeeld georganiseerd door de gebruiker volledige controle te geven over welke data deze delen en de mogelijkheden voor een partij om getoonde credentials te verifiëren zonder dat de uitgever van de credentials hiervan op de hoogte wordt gebracht. Dit werkt vergelijkbaar met een fysiek paspoort waarvan de gemeente ook niet weet als je deze hebt laten zien voor bijvoorbeeld het huren van een auto.

2. Ontwikkelingen op gebied van toegang

Out-of-band authentication (OOBA)

Out-of-band authentication (OOBA) is een authenticatieproces dat gebruikmaakt van een communicatiekanaal dat gescheiden is van het primaire communicatiekanaal met twee entiteiten die proberen een geauthenticeerde verbinding tot stand te brengen. Het gebruik van een afzonderlijk verificatiekanaal maakt het aanzienlijk moeilijker voor een aanvaller om het verificatieproces te onderscheppen en te ondermijnen (d.w.z. via een man-in-the-middle-aanval), omdat de aanvaller daarbij twee communicatiekanalen moet compromitteren. Voorbeelden van vormen van OOB-authenticatie zijn onder meer codes die via sms naar een mobiel apparaat worden gestuurd, authenticatie via een spraakkanaal, codes die via pushmeldingen naar een mobiele app worden gestuurd en codes die worden verzonden naar of worden ontvangen vanuit een vertrouwde uitvoeringsomgeving die is verbonden met het hostapparaat dat probeert een geauthenticeerde verbinding te maken.

OOBA wordt o.a. gebruikt bij SURFsecureID en internetbankieren. Om het inlogproces te voltooien wordt een authenticatiecode via sms naar het mobiele apparaat van de accounthouder gestuurd. OOBA wordt gebruikt voor inloggen met een tweede factor middels een ander kanaal. Een tweede factor voorkomt identiteitsfraude. Hierdoor is het inzetbaar om een hogere betrouwbaarheid toe te kennen aan een identiteit namens een instelling, bijvoorbeeld voor verwerking van cijfers of stagecontracten. Een nadeel hiervan is wel dat mobiel veelal voor de tweede factor gebruikt wordt, maar dat de mobiel wordt ook vaker gebruikt om de functionaliteit te ontsluiten. Er zijn dan wel twee kanalen, maar door een enkel device wordt de veiligheid niet altijd verhoogd.

Continuous authentication

Continue authenticatie is een manier om gebruikers toegang te verlenen tot onlinediensten op basis van aanvaardbare risiconiveaus of contextuele informatie. Continue authenticatie is passief terwijl traditionele authenticatie als actief wordt beschouwd. Hierbij moet de gebruiker in elk geval een authenticatiefactor opgeven (bijvoorbeeld kennis, bezit of biometrie) om toegang te krijgen. Continue authenticatie maakt gebruik van informatie zoals browser metagegevens, gebruikerslocatie, passieve levensdetectie en het tijdstip van de dag om tot een authenticatiescore te komen. Tijdens een onlinesessie komt de waarde van de authenticatiescore voor het verlenen of weigeren van toegang overeen met de risicomodellen van de serviceprovider voor die actie. Het eenvoudig bekijken van accountgegevens kan bijvoorbeeld altijd worden toegekend zolang de risicoscore binnen het vertrouwde bereik ligt, omdat de onderneming het bekijken van de informatie (zelfs door een bedrieger) als goedaardig kan beschouwen. Een financiële transactie tijdens de sessie zal ertoe leiden dat de gebruiker wordt gevraagd om actief een authenticatiefactor te leveren voor de betalingsautorisatie. De onderliggende technologie voor continuous authentication is Artificial Intelligence om een identiteit vast te stellen op basis van een context. CA wordt momenteel veelal gebruikt binnen een organisatie met verschillende onlinediensten van één organisatie en niet in een federatief operationeel model zoals SURFconext.

3. Ontwikkelingen op het gebied van Cloud identity services

Naast de traditionele IAM-oplossingen is de ontwikkeling gaande van vooraf geconfigureerde gestandaardiseerde cloudgebaseerde IDaaS-services voor of als onderdeel van SAAS met logisch toegangsbeheer, eenmalige aanmelding, gebruikersvoorziening, digitale identiteit, compliance en zowel multi-factor als adaptieve authenticatie.

Identity as a Service

IDaaS betreft een platform om identiteiten mee te beheren en toegang te verlenen die geleverd wordt vanuit de cloud. Azure AD Services van Microsoft is hier een goed voorbeeld van. Het kan niet alleen gebruikt worden voor eigen applicaties maar ook voor applicaties van derden. Applicaties kunnen dan in de Private, Public Cloud staan of in een datacenter van een organisatie. Microsoft noemt deze mix van identiteit en toegang voor on-premises en cloudtoepassingen ook wel het Hybride-ID concept. Andere bedrijven zoals Google, AWS, etc. hebben allemaal een vergelijkbare IDaaS functionaliteit beschikbaar.

SaaS met geïntegreerde ID

Cloudapplicatie (SaaS) leveranciers hebben een IDaaS onderdeel geïntegreerd als een onderdeel van hun business Cloudapplicaties, SAP, Salesforce etc. zijn hier een voorbeelden van. Organisaties die hiervoor kiezen worden mogelijk minder flexibel dan wanneer men een losgekoppelde zelfstandige IDaaS had geïmplementeerd. Hiermee kunnen gebruikers de volledige controle over hun identiteit behouden.

Bijlage E: Standaarden en technologie

Digitale transformatie heeft de behoefte vergroot aan robuuste standaarden voor identiteit, toegang en autorisatie die kunnen werken met werken op afstand, multi-cloud omgevingen, IoT, API's en DevOps. Authenticatie voor toegang is een kerncomponent en staat centraal in de beveiliging en het beheer van hedendaagse organisaties.

Authenticatiegebeurtenissen moeten context bieden voor de belangrijkste identiteitsvragen: wie is de gebruiker en/of wat is het apparaat, waar zijn ze geauthentiseerd, wanneer zijn ze geauthentiseerd, hoe zijn ze geauthentiseerd, welke attributen hebben we gegeven en hoe en waarom hebben we deze verstrekt? Alle authenticatieprotocollen moeten antwoord kunnen geven op deze vragen. De industrie heeft jarenlang protocollen ontwikkeld die veilige authenticatie bieden die verder gaan dan de standaard gebruikersnaam en wachtwoorden.

SAML

Security Assertion Markup Language (SAML) is een standaard voor het veilig uitwisselen van authenticatie- en autorisatiegegevens van gebruikers tussen verschillende organisaties. SAML maakt het mogelijk om op een veilige manier via het internet toegang te krijgen tot diensten van verschillende organisaties, zonder dat je per dienst eigen inloggegevens nodig hebt, of bij elke dienst apart moet inloggen. SAML wordt veel gebruikt, zeker in corporate systeemlandschappen, maar wordt als minder geschikt gezien voor mobiele toepassingen.

OAuth 2.0

Wanneer een gebruiker zich met succes authentiseert bij een webapplicatie met een OAuth 2.0-service, geeft de OAuth 2.0-service een token uit voor dit gebruikersaccount zodat de vertrouwende partijen de authenticatie op hun systemen kunnen accepteren. Door de verspreiding van API's die ontwikkelaars in staat stellen applicaties te maken die compatibel zijn met webgebaseerde platforms, is OAuth populair geworden als autorisatieprotocol en wordt het steeds vaker aangetroffen in bedrijfsweb- en desktoptoepassingen om gebruikersaccounts voor verschillende doeleinden toegang te geven tot applicaties.

OIDC

Naast bestaande en veelgebruikte SAML2.0 is OpenID Connect (OIDC) een ander op HTTP-gebaseerd protocol dat vergelijkbaar is met OAuth. OIDC maakt gebruik van OAuth om een robuust authenticatie- en autorisatiepakket te bieden waarmee gebruikersaccounts toegang hebben tot applicaties. Het kan ook eenmalige aanmelding (SSO) voor gebruikers inschakelen voor verschillende webgebaseerde applicaties met behulp van een OpenID-identiteit, waardoor clients de identiteit van een eindgebruiker kunnen verifiëren op basis van de authenticatie die wordt uitgevoerd door een autorisatieserver of identiteitsprovider (IdP). De gebruiker kan een enkele identiteit die aan een vertrouwde OpenID-identiteitsprovider is gegeven hergebruiken en op meerdere websites dezelfde gebruiker zijn. Net als OAuth wordt OpenID gebruikt voor veel consumententoepassingen. De recente openstelling van bankklanteninformatie voor derden maakt uitgebreid gebruik van OAuth- en OpenID-protocollen.

FIDO

De FIDOTM-alliantie (Fast Identity Online) is een non-profitorganisatie die in februari 2013 is opgericht om het gebrek aan interoperabiliteit tussen sterke authenticatieapparaten aan te pakken, evenals de problemen waarmee gebruikers worden geconfronteerd bij het aanmaken en onthouden van meerdere gebruikersnamen en wachtwoorden. De FIDO Alliance heeft specificaties ontwikkeld die een open, schaalbare, interoperabele set mechanismen definiëren, die de afhankelijkheid van wachtwoorden om gebruikers van onlineservices veilig te authentiseren niet meer nodig zijn (passwordless).

Met FIDO-authenticatiestandaarden voor browsers, besturingssystemen, webservers en persoonlijke apparaten kunnen websites en applicaties hun gebruikers de mogelijkheid bieden om cryptografische

inloggegevens te ontgrendelen met eenvoudige ingebouwde methoden zoals vingerafdruklezers of camera's op hun apparaten of door gebruik te maken van easy- om FIDO-beveiligingssleutels te gebruiken.

SCIM

System for Cross-domain Identity Management (SCIM) zorgt ervoor dat identiteitsinformatie van gebruikers systeemoverstijgend op de juiste plek aanwezig is. Hierdoor kunnen gegevens die niet meer in systemen horen te staan, omdat een gebruiker bijvoorbeeld niet langer in dat systeem hoeft te zijn opgenomen, worden verwijderd. Omdat dit geautomatiseerd gebeurt is relatief weinig inspanning nodig om de gewenste toevoeging of verwijdering van gegevens te realiseren. SCIM wordt bijvoorbeeld gebruikt om in de cloud op verschillende plekken informatie over de identiteit van gebruikers te kunnen toevoegen of verwijderen. SCIM maakt gebruik van een Application Programming Interface (API) waarmee een computerprogramma kan communiceren met een ander programma. Deze standaard is gericht op het reduceren van kosten en complexiteit en het voortbouwen op bestaande protocollen. SCIM heeft als doel gebruikers snel, goedkoop en eenvoudig in, uit en tussen clouddiensten te brengen.

Decentralized IDentifier Specification (DID)

De Decentralized identifier specification (DID-Core)[32] beschrijft de architectuur, het datamodel, methoden en syntax voor vastlegging en gebruik van decentrale identiteiten, zodanig dat de eigenaar (controller) van de identiteit daarover kan beschikken, onafhankelijk van derden. De standaard schrijft geen specifieke technische implementaties voor. De specificatie bouwt voort op het Verifiable Credentials Data Model[33].

[32] Decentralized Identifiers (DIDs) v1.0 (w3.org)

[33] Verifiable Credentials Data Model v1.1 (w3.org)

Bijlage F: Huidige situatie

Om een beeld te krijgen van de huidige situatie rondom Identiteit en Toegang is geïnventariseerd welke initiatieven en voorzieningen op het gebied van Identiteit en Toegang bestaan. Hoewel de inventarisatie niet uitputtend is, blijkt dat er al heel veel initiatieven zijn.

De inventarisatie laat zien dat de initiatieven en diensten binnen de sector niet altijd in samenhang met elkaar worden uitgevoerd. Voor het beschrijven van de huidige situatie op het vlak van Identiteit en Toegang gaat deze domeinarchitectuur uit van bestaande voorzieningen en initiatieven vanuit verschillende organisaties en samenwerkingsverbanden in de sector.

Tijdens de inventarisatiefase van de totstandkoming van de domeinarchitectuur zijn via interviews, rapporten en sessies o.a. diverse initiatieven en aandachtpunten rondom Identiteit en Toegang geïnventariseerd. Paragraaf 4.1 beschrijft kort een aantal initiatieven op het gebied van Identiteit en Toegang binnen het onderwijs en onderzoek, paragraaf 4.2 buiten het onderwijs en onderzoek en paragraaf 4.3 beschrijft de belangrijkste aandachtspunten die zijn herkend.

1. Initiatieven binnen Onderwijs en Onderzoek

Rond Identiteit en Toegang voor het Onderwijs en Onderzoek zijn een aantal initiatieven die delen van bestaande vraagstukken adresseren. Een aantal bekende initiatieven worden hieronder beschreven, inclusief de beoogde doelen. De initiatieven die daarbij zijn opgenomen hebben betrekking op bevordering van instelling overschrijdend gebruik van elkaars identiteiten voor het geven van gecontroleerde toegang.

eduID

Onderwijs digitaliseert én flexibiliseert. Studenten willen zelf hun onderwijscarrière vormgeven. Dat zorgt voor logistieke en administratieve uitdagingen. Daarom ontwikkelt SURF samen met de instellingen eduID[34] één identiteit waarmee studenten bij iedere onderwijsinstelling terecht kunnen: voor, tijdens én na hun studie. Met eduID wenst men een overkoepelende digitale studentidentiteit beschikbaar te maken, onafhankelijk van een instelling. eduID is veel meer dan een studentnummer. Het is een voorziening die gekoppeld is aan een persoon. Dit in tegenstelling tot het huidige studentnummer dat gekoppeld is aan een instelling. Studenten, en niet langer de instellingen, hebben de regie over (persoons)gegevens, gevolgde vakken en cijfers. In het eduID-project ontwikkelt SURF één digitale identiteit voor studenten in Nederland. Met dit eduID is een student bekend bij de eigen instelling, maar de student kan het ook gebruiken om zich te identificeren bij een andere instelling of om toestemming te geven om gegevens te delen tussen instellingen.

ORCID

ORCID staat voor Open Researcher and Contributor ID en is een (alpha-numerieke) code die wordt gebruikt om auteurs van wetenschappelijke werken uniek te identificeren. ORCID is een gratis, unieke, persistente identifier die door personen die zich zich bezighouden met onderzoeks-, beurs- en innovatieactiviteiten kan worden gebruikt. Doel van deze identifier is om iedereen die deelneemt aan onderzoek, wetenschap en innovatie te verbinden. De identifier identificeert de deelnemer uniek en verbind de deelnemer met hun bijdragen over disciplines, grenzen en tijd heen.

Achter ORCID staat een non-profitorganisatie, waarvan wetenschappers, instituten en organisaties lid kunnen worden. Deze organisatie is een community gebaseerde organisatie, waarbinnen drie gerelateerde diensten worden aangeboden, te weten: het ORCID-ID, een ORCHID-record gekoppeld aan het ID en een set aan

[34] Bron: Wat is eduID nu precies? | SURF.nl

Application Programming Interfaces (API's) wat de registratie en informatie-uitwisseling met ORCID-records vergemakkelijkt.

Instellingen HO

Meerdere instellingen hebben een eigen IAM-infrastructuur en hebben initiatieven of projecten lopen op gebied van IAM. Naast IAM voor digitale identiteiten en toegang van hun eigen medewerkers en studenten, wenst men ook gecontroleerd toegang te geven aan gebruikers van andere instelling of “gasten” van buiten de onderwijssector. Ook zijn er initiatieven om inloggen met aanvullende tokens mogelijk te maken.

SURF Research Access Management

Onderzoekers werken niet alleen via een instelling en veelal internationaal. De SURF Research Access Management[35] dienst van SURF helpt onderwijs samenwerken bij het organiseren en beheren van toegang tot onderzoeksdiensten. Zo werk je als onderzoeker makkelijker samen met collega's binnen en buiten je instelling. Log in met je instellingsaccount en regel zelf toegang tot diensten voor jouw onderzoekssamenwerking. Het FIM4R-initiatief legde de identiteits- en toegangsuitdagingen vast in een rapport. Als reactie daarop ontstond in Europa het AARC-project (Authentication and Authorization for Research Collaborations), met als resultaat onder andere een ‘Blueprint architecture’ (AARC BPA). SURF gebruikte die architectuur in het project 'Science Collaboration Zone' (SCZ) en ontwikkelde hieruit een dienst: SURF Research Access Management.

Edustandaard werkgroep IAA

De werkgroep Toegang[36] is geïnitieerd door de Standaardisatieraad en heeft als opdracht in kaart te brengen op welke wijze de toekomstbeelden voor toegang binnen de onderwijssectoren op elkaar aansluiten, vast te stellen welke issues problemen geven met de aansluiting en een aanpak voor te stellen waarmee de aansluiting gewaarborgd kan worden. De doelgroep voor toegang beperkt zich niet tot de onderwijsvolger, maar ook de onderwijsprofessional, onderzoeker en medewerker. Werkgroep IAA bestaat uit deelnemers vanuit PO, VO, mbo, hbo, wo, SURF en OCW.

European Student Identifier (ESI)

De European Student Identifier (ESI) [37]is een digitale identificatie waarmee studenten zich op een unieke manier kunnen identificeren. De ESI is opgezet in de context van het Erasmus+ programma. Het heeft feitelijk uitsluitend betekenis binnen de programma’s en diensten die aangeboden worden vanuit Erasmus+ aan deelnemende instellingen. Deze identificatie is nodig wanneer ze online toegang willen krijgen tot diensten die nodig zijn voor studentenmobiliteit in het kader van Erasmus+. Het gaat hierbij in eerste instantie om registratie in de administratieve systemen van betrokken Europese onderwijsinstellingen. Kortom: de ESI ondersteunt en vergemakkelijkt internationale studentenmobiliteit en transnationale samenwerking van instellingen voor hoger onderwijs binnen Europa. Voor toegang tot de Erasmus+ diensten op basis van de European Student Identifier komt er binnen Europa een centraal ESI-koppelpunt beschikbaar, dit koppelpunt wordt de “MyAcademicID Proxy” genoemd. MyAcademicID bouwt voort op eduGAIN, eIDAS, European Student Card (ESC) en European Student Card Number (ESCN).

Diplomas and Credentials European Blockchain Partnership

Vanuit DGDIGIT (EU) heeft de use-case diploma’s afgelopen jaren gedraaid. Een Europees initiatief, ingebracht door Nederland (DUO) en gefaciliteerd door DUO (User Group Diplomas and Credentials European Blockchain Partnership). Een groot aantal deelstaten hebben geparticipeerd in dit initiatief en zijn gekomen tot een aantal use-cases voor het onderwijsveld i.r.t. de digitale identiteit.

[35] Bron: https://www.surf.nl/surf-research-access-management-veilig-en-eenvoudig-toegang-tot-onderzoeksdiensten/wat-is-surf
[36] Bron: https://www.edustandaard.nl/oprichting-werkgroep-iaa-inventarisatie)
[37] Bron: https://wiki.geant.org/display/SM/European+Student+Identifier

2. Initiatieven buiten Onderwijs en Onderzoek

Buiten de sector is een groot aantal initiatieven rondom identity. De belangrijkste zijn hier opgenomen[38].

Europees – eIDAS en EDI

eIDAS[39] staat voor 'Electronic Identities And Trust Services'. Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus[40] en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. Dit kan alleen met een betrouwbare online identiteitscheck aan de voordeur. De eIDAS-verordening is van toepassing op publieke organisaties en private organisaties met een publieke taak. Ze zijn verplicht om Europees erkende inlogmiddelen te accepteren binnen de digitale dienstverlening. De eIDAS verplichting geldt onder andere voor organisaties die gebruikmaken van DigiD en eHerkenning.
Bij introductie van eIDAS heeft SURF instellingen geïnformeerd wat eIDAS zou betekenen voor hun instelling en er is een wiki FAQ beschikbaar: https://wiki.surfnet.nl/display/eIDAS/eIDAS+Home .

De Europese commissie werkt onder de naam European Digital Identity (EDI) aan uitbreiding van de bestaande verordening, onder andere om de Europese digitale identiteit uit te breiden buiten de publieke sector, en om het gebruik van 'attributen' te regelen.[41] Hieruit komen ook initiatieven voort voor de 'European Identity Wallet'.

Digitale bronidentiteit (DBI) - burger

Dit is een digitale identiteit van een burger die door de Nederlandse overheid wordt uitgegeven, erkend en in de wet- en regelgeving verankerd is. De digitale identiteit is voor gebruik in de publieke en private sector. Deze digitale bronidentiteit bevat een minimale set van identiteitsgegevens die nodig zijn in het maatschappelijk verkeer. De overheid creëert met de digitale bronidentiteit een 'gezaghebbende bron' van betrouwbare persoon identificerende gegevens. Dit biedt een belangrijke generieke bouwblok voor vertrouwen in de digitale wereld. De DBI[42] als 'gezaghebbende bron' maakt afgeleide digitale identiteitsmiddelen mogelijk, net zoals je met een fysiek paspoort andere afgeleide identiteiten mogelijk kunt maken.

Virtueel identiteitsdocument (vID)

Een vID is de digitale variant van je vertrouwde paspoort of identiteitskaart in de vorm van een app op je smartphone. Deze digitale identiteit moet in de toekomst voldoen aan dezelfde betrouwbaarheidseisen als je huidige paspoort en identiteitskaart voor het gebruik in de fysieke én digitale wereld. In september 2020 is gestart in het Experiencelab vID. Dit is een samenwerking van diverse overheidsorganisaties, het bedrijfsleven en andere organisaties, waaronder RvIG, Digicampus en TNO. In het lab wenst men verschillende use cases te testen met de uitgifte van een vID bij een gemeentebalie. Ook onderzoeken ze een aantal toepassingen van een vID:

- Online check-in en grenscontrole met een vID op een luchthaven
- Online leeftijdscontrole met een vID in een webshop
- Met een vID identificeren op straat

[38] Voor een recent overzicht, zie https://zoek.officielebekendmakingen.nl/blg-1002922.pdf
[39] Bron: https://www.digitaleoverheid.nl/dossiers/eidas
[40] Bron: https://afsprakenstelsel.etoegang.nl/display/as/Technische+specificaties+en+procedures+voor+uitgifte+van+authenticatiemiddelen
[41] Bron: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0281&from=NL
[42] Bron: Samenwerken aan een digitale bronidentiteit - Digitale Overheid

IRMA

IRMA staat voor “I Reveal My Attributes” en is ontwikkeld door de in Nijmegen opgerichte stichting Privacy by Design van hoogleraar prof. dr. Bart Jacobs. Met IRMA kunnen gebruikers op een veilige en privacyvriendelijke manier een deel van hun identiteit online vrijgeven aan partijen en een digitale handtekening zetten.
Als pilot heeft de gemeente Nijmegen een groep inwoners de mogelijkheid gegeven om hun gegevens uit de basisregistratie personen op te vragen en deze te gebruiken voor hun 'digitale identiteit' in de app IRMA ('I Reveal My Attributes'). Door in te loggen met IRMA hoeft iemand geen gebruikersprofielen meer aan te maken op allerlei websites en apps. De websites krijgen met IRMA alleen nog de gegevens van de gebruiker die echt noodzakelijk zijn. Zij zijn zeker van de betrouwbaarheid van deze informatie, omdat die van officiële instanties komt. De stichting Privacy by Design heeft een samenwerkingsverband met SDIN (beheerder van het .nl-domein) en voert ook het beheer en onderhoud uit van de IRMA technische infrastructuur.

Decentralized Identity (DCI) / Decentralized Identifiers (DID)

DCI/DID biedt een alternatief voor gecentraliseerde IAM-architecturen door vertrouwen in identiteiten en weerbaarheid binnen een algeheel systeem tot stand te brengen, met weinig afhankelijkheid van gecentraliseerde partijen of identiteitsbronnen. DCI/DID biedt een alternatieve aanpak die niet de beveiligings-, privacy- en bruikbaarheidsproblemen heeft die gepaard gaan met traditionele, gefragmenteerde digitale identiteitsbenaderingen. Met DCI/DID krijgen gebruikers controle over hun identiteit en gegevens, waardoor serviceproviders sneller en met meer vertrouwen met gebruikers kunnen communiceren. Op dit moment hamsteren providers doorgaans identiteitsgegevens over gebruikers. Door gebruik te maken van DCI/DID, identiteits- en serviceproviders kunnen de beveiliging en het toegangsgemak voor eindgebruikers worden verbeterd, terwijl de blootstelling aan gegevensdiefstal en mogelijke schendingen van de privacywetgeving wordt verminderd. Binnen w3c is een werkgroep actief die de standaarden voor DID uitwerkt[43]. Partijen die al veel ontwikkelen op het gebied van DCI/DID zijn IBM en Microsoft. Zij hanteren daarnaast ook het gebruik van de identiteiten binnen hun eco-systemen als identiteitsprovider voor andere omgevingen.

IDunion

In april 2021 ging het IDunion Indy-netwerkproject van start in de Europese Unie (EU). IDunion startte begin 2021 een testnetwerk en heeft het geld om later in 2021 het IDunion MainNet te lanceren. Het IDunion-netwerk is bedoeld om alleen gebruikers in de EU te bedienen voor het schrijven van transacties als tegenhanger van Sovrin en Indico die in belangrijke mate georiënteerd zijn op de VS. Natuurlijk kunnen verificateurs noodzakelijkerwijs overal zijn, zodat iedereen ter wereld uit het IDunion-grootboek kan lezen. Het idee van nationale/regionale Indy-netwerken komt voort uit het idee dat naarmate het gebruik van verifieerbare referenties alomtegenwoordig wordt, de betrouwbaarheid van grootboekhulpprogramma's van cruciaal belang wordt. Aangezien de beschikbaarheid van de grootboeken van cruciaal belang is wanneer deze breed gebruikt worden, moeten ze deel uitmaken van de kritieke infrastructuur van een land, net als internet, noodtelefoonsystemen (bijvoorbeeld 911 of 112), het elektriciteitsnet, enz. Andere landen zijn ook begonnen met het verkennen van het creëren van hun eigen grootboek.

[43] https://www.w3.org/2019/did-wg/

Bijlage G: Aandachtspunten

Tijdens de inventarisatiefase van de totstandkoming van de domeinarchitectuur zijn middels interviews, rapporten en sessies diverse knelpunten en ontwikkelingen geïnventariseerd. Hieronder volgt een beschrijving van de belangrijkste aandachtspunten.

Toegang voor gasten

Docenten en onderzoekers kunnen met moeite gastdocenten, collega-onderzoekers of anderen toegang geven tot hun onderwijs of onderzoek vanuit de digitale voorzieningen van de instellingen. Veelal wordt dit bij instellingen opgelost door voor gasten een “not on payroll” registratie in HRM te maken waardoor er automatisch een “gast” account wordt aangemaakt. Voor “gasten” kan een federatieve koppeling ingericht via SURFconext. Over het algemeen is de grootste uitdagingen autorisatie voor deze “gasten”. SURFconext levert veelal de identiteiten van gebruikers bij andere instellingen, of (via eduID) identiteiten van “gasten”, potentieel ‘de hele wereld’. Soms zijn ook samenwerkingen met andere, buitenlandse instellingen gewenst.

Ingericht op nationaal

Europese samenwerking op het gebied van onderwijs is lastig omdat het niet mogelijk is om onderwijsgegevens te delen met andere (Europese) instellingen door het ontbreken van standaarden en afspraken.

Gericht op eigen instelling

Studeren en werken bij verschillende instellingen vraagt meestal om een gebruikersidentiteit per instelling waar je studeert of werkt. De huidige IAM-faciliteiten zijn primair gericht op de eigen instelling. Studeren en werken bij verschillende instellingen vraagt om een sectorbrede gebruikersidentiteit zoals eduID.

HO sector-overstijgende samenwerking

Een samenwerking met gecontroleerde toegang tot applicaties en informatie-uitwisseling tussen een instelling en organisaties buiten de HO-sector (bedrijven, uitgevers, rijksoverheid en ziekenhuizen of instellingen uit PO, VO of MBO) is in de huidige situatie uitdagend.

Privacy en gemak

Voor de HO-sector bestaat het Studielink-nummer dat in een aantal ketenprocessen gebruikt wordt, maar niet in alle ketenprocessen. O.a. omdat het vanuit de AVG/GDPR ongewenst is om hetzelfde centrale onderwijsnummer te gebruiken en meerdere malen op te slaan bij de verschillende ketenpartijen. Daarom wordt de voorkeur gegeven om te werken met pseudoniemen uitgegeven door een partij die ‘te vertrouwen is’ of gebruik te maken van polymorfe pseudoniemen of andere technieken zonder een vertrouwenspartij. De complexiteit van zo’n oplossing is potentieel een stuk groter, en is het van belang om goed te bekijken of het probleem dat rechtvaardigt. Vanuit het oogpunt van de burger of student is het wel wenselijk om het zo gemakkelijk mogelijk te maken, zonder daarbij de privacy van het individu in gevaar te brengen.

Aanmeldproces buitenlandse studenten

Buitenlandse studenten worden per aanmelding op instellingsniveau geverifieerd waardoor veel extra werk ontstaat en kan leiden tot verschillende uitkomsten. Dit aandachtspunt is onderkent door Studielink. Een proces voor Digitale Verificatie van Persoonsgegevens is inmiddels operationeel en werkt voor 60% van de internationale studenten..

Kwaliteitsborging

Instellingen kunnen voor partners en derden niet op een objectieve wijze inzichtelijk maken in welke mate zij het beheren van identiteiten en het verlenen van rechten op orde hebben.

Ongewenste lock-in

Binnen de sector leeft het beeld dat instellingen en onderwijs ongemerkt volledig in de cloudomgevingen van leveranciers verdwijnen die een geïntegreerde eigen digitale cloud-identiteit en toegang aanbieden voor een groot aantal toepassingen. Instellingen zijn dan niet in staat om van identiteit- en toegangsleverancier te veranderen zonder grote impact en ongemak op de cloudapplicatie van de leverancier. Dit is een probleem wanneer instellingen van leverancier wensen te veranderen, omdat er sprake is van een soort gekoppelde levering van verschillende gecombineerde services. Instellingen zijn dan sterk afhankelijk van de roadmap van de leverancier.

Bijlage H: definities en begrippen

In deze bijlage zijn definities en begrippen opgenomen die in de domeinarchitectuur voorkomen. Een aantal begrippen is rechtstreeks ontleend aan een bron, dit is bij het begrip aangegeven. Voor de algemene begrippen is gesteund op het begrippenkader IAM uit de Nederlandse Overheidsrefentie-architectuur (NORA), voor begrippen die specifiek zijn voor virtuele credentials is een vertaling gemaakt uit de W3C-standaard voor verifieerbare credentials (VC Datamodel).

- ***Attribuut:*** een uniek kenmerk of gegeven van een entiteit (bron: NORA)
- ***Authenticatie:*** een proces dat de bevestiging van de identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt. (bron: NORA)
- ***Authenticatiemiddel:*** een middel op grond waarvan authenticatie van een gebruiker kan plaatsvinden. (bron: NORA)
- ***Authenticatiefactor:*** een factor waarvan is bevestigd dat deze gebonden is aan een persoon en die onder een van de drie volgende categorieën valt. • Op bezit gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is. • Op kennis gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt. • Inherente authenticatiefactor: een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit. (bron: NORA)
- ***Autorisatie:*** autorisatie is het proces van vaststelling van het mandaat dat een geauthentiseerde identiteit heeft en de rechten die er bij dit mandaat horen. (bron: NORA)
- ***Betrouwbaarheidsniveau:*** de mate waarin vertrouwen kan worden gesteld in een identificatiemiddel. (bron: NORA)
- ***Bronidentiteit:*** een bronidentiteit (of basisidentiteit) is de identiteit van een (rechts)persoon zoals nu door de overheid vastgelegd en vormgegeven via identificatiemiddelen (identiteitsbewijzen) die in het maatschappelijk verkeer te gebruiken zijn (paspoort, identiteitskaart of rijbewijs of in de toekomst mogelijk meer). (bron: NORA)
- ***Claim:*** Een *claim* is een bewering over een *subject*. Een *subject* is een 'ding' waarover beweringen kunnen worden gedaan. Claims worden uitgedrukt als een relatie tussen subject, eigenschap (*property*) en waarde (*value*). Met het datamodel kan een krachtige en gevarieerde set beweringen worden opgebouwd. Deze kunnen enkelvoudig zijn of samengesteld uit meerdere aan elkaar te relateren claims in de vorm van een *graph*[11]. (bron: Verifiable credentials Datamodel)
- ***Credential***: Een credential is een set van een of meerdere *claims* die gedaan zijn door dezelfde entiteit. Credentials kunnen daarnaast een identifier bevatten, evenals metadata die eigenschappen van de credential beschrijft, zoals de *issuer*, de vervaldatum, een publieke sleutel ten behoeve van verificatie, het revocatiemechanisme, etc. De metadata kan door de *issuer* ondertekend zijn. Een *verifieerbare* credential is een set van claims die bestand zijn tegen manipulatie, gekoppeld aan metadata en cryptografisch bewijs over de *issuer*, bijvoorbeeld een digitale handtekening. (bron: Verifiable credentials Datamodel)
- ***Digitaal/elektronisch identificatiemiddel:*** een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat en die gebruikt wordt voor authenticatie bij een onlinedienst. (bron: NORA)
- ***Digitale/elektronische identiteit*****:** een identiteit in de onlinewereld voor entiteiten. Een digitale identiteit kan bestaan uit verschillende aspecten (attributen) die over een bepaalde entiteit geregistreerd staan. ISO/IEC stelt: een digitale identiteit is een set attributen die te relateren zijn aan een entiteit. (bron: NORA)
- ***Digitale/elektronische identiteitinfrastructuur***: het geheel van stelsels, afspraken, standaarden en voorzieningen, rond de digitale identiteit van (rechts)personen. (bron: NORA)
- ***eID:*** eID staat voor Electronic Identification. (bron: NORA)

- ***eIDAS:*** eIDAS staat voor Electronic Identification (eID) and Trust Services (AS). Het is een initiatief van de Europese Commissie met als doel om elektronische interacties tussen ondernemingen, burgers en organisaties veiliger en efficiënter te maken en alle EU-landen elkaars eID en AS erkennen. (bron: NORA)
- ***Federatief Identity Management:*** een voorziening van de processen, afspraken, standaarden en technologie welke het mogelijk maken om op een gecontroleerde manier digitaal identiteit- en contextgegevens uit te wisselen over (gedeelde/gezamenlijke) instellingsgrenzen heen
- ***Gebruiker:*** iedereen die bekend is en gebruik maakt van de voorziening. Gebruikers kunnen onder meer zijn:
    - *Student, medewerker, onderwijsprofessional, onderzoeker, alumnus:* een natuurlijk persoon van een instelling die een of meer relaties heeft met de HO-sector met een uniek identificatie
    - *Partner:* een natuurlijk persoon van een partnerorganisatie (niet HO-sector) die een of meer relaties heeft met instellingen binnen de HO-sector met een unieke identificatie
- ***Gezaghebbende bron:*** elke bron, ongeacht de vorm ervan, waarvan kan worden verwacht dat deze nauwkeurige gegevens, informatie of bewijsmateriaal biedt op basis waarvan een identiteit kan worden aangetoond. (bron: NORA)
- ***HO-kaart:*** set aan kenmerken die een HO-gebruiker uniek herkenbaar maakt in bepaalde context binnen de HO-sector voor digitale identificatie
- ***Holder*** *(houder of bezitter)*: de rol die een entiteit speelt door een of meer verifieerbare credentials te bezitten en daaruit een of meerdere verifieerbare presentaties te genereren. Voorbeelden van *holders* zijn studenten, werknemers en klanten. (bron: Verifiable credentials Datamodel)
- ***Identificatie:*** het proces van het kenbaar maken van een identiteit. (bron: NORA)
- ***Identificatiemiddel:*** (fysiek of digitaal) middel uitgegeven zodat degene voor wie het is uitgegeven zich kan identificeren. (bron: NORA)
- ***Identiteit:*** een identiteit bestaat uit de geregistreerde aspecten (attributen) die in voldoende mate bepalen wie iemand of iets is. (bron: NORA)
- ***Identity Provider:*** organisatie of een voorziening die borg staat voor de identiteit- en contextgegevens van een gebruiker die toegang vraagt tot applicatie binnen de HO-sector
- ***Issuer*** *(uitgever):* de rol die een entiteit speelt door beweringen te doen over een of meer *subjecten*. (bron: Verifiable credentials Datamodel)
- ***Juridische identiteit:*** een juridische identiteit (of publiekrechtelijke identiteit) is een identiteit die door de wet vastgelegd en gereguleerd is. (bron: NORA)
- ***Persoonsidentificatiegegevens:*** een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld. (bron: NORA)
- ***Registerhouder:*** de partij die gegevens registreert en daarmee een gezaghebbende bron kan vormen. (bron: NORA)
- ***Self Sovereign Identity (SSI):*** Het concept Self Sovereign Identity legt de controle en de macht over een digitale identiteit volledig bij de entiteit die deze digitale identiteit representeert. Dit vereist volledige onafhankelijkheid van een centraal register of centrale autoriteit. (bron: NORA)
- ***Subject*** *(onderwerp):* een entiteit waarop claims betrekking hebben. Voorbeelden zijn mensen, dieren en dingen. In veel gevallen is de houder van een verifieerbare credential het *subject*, maar in bepaalde gevallen is dat niet zo. Bijvoorbeeld een ouder kan als *holder* de verifieerbare credentials van een kind (het *subject*) in bezit hebben, of de eigenaar kan als *holder* de verifieerbare credentials van een huisdier (het *subject*) in bezit hebben. (bron: Verifiable credentials Datamodel)
- ***Verifier*** *(verificator of controleur):* Een rol die een entiteit vervult door het ontvangen van een of meerdere verifieerbare credentials, mogelijk opgenomen in een verifieerbare presentatie, ten behoeve van verwerking. Voorbeelden zijn werkgevers, beveiligingsfunctionarissen en websites. (bron: Verifiable credentials Datamodel)
- ***Verifiable data registry*** *(Register met verifieerbare data)* – Een rol die een systeem kan vervullen door te bemiddelen in de aanmaak en verificatie van identifiers, sleutels (*keys*) en andere relevante data,

zoals schema's voor verifieerbare credentials, revocatieregisters, publieke sleutels (*public keys*) van *issuers*, die nodig is voor het gebruik van verifieerbare credentials. Dergelijke registers kunnen bijvoorbeeld vertrouwde databases, decentrale databases, nationale identiteitenregisters en gedistribueerde ledgers zijn. In een ecosysteem komen vaak meerdere vormen van registers met verifieerbare data voor

- ***Verifieerbare presentatie:*** weergave van data uit een of meerdere verifieerbare credentials, zodanig dat de herkomst (*authorship*) van de data verifieerbaar is. Verifeerbare presentaties kunnen een-op-een overeenkomen met verifieerbare credentials, maar kunnen ook data bevatten die cryptografisch verifieerbaar is afgeleid van credentials. In het laatste geval zijn die verifieerbare credentials zelf geen onderdeel van de verifieerbare presentatie. Net als bij verifieerbare credentials zijn ook hier metadata en bewijs integraal onderdeel van de verifieerbare presentatie.