Samen aanjagen van vernieuwing

De SSI-wallet voor onderwijs en onderzoek

Een technische exploratie

Wallets, ofwel digitale portemonnees met persoonsgegevens, staan in het vizier van vele verschillende partijen, zoals overheid, publieke en private partijen. Niet alleen nationaal, ook internationaal. Voor onderwijs en onderzoek biedt deze oplossing voordelen. De technologie van self-sovereign identity (SSI), die gebruikers meer controle geeft over hun eigen persoonsgegevens, brengt hierbij een grote belofte.

Het team Trust & Identity van SURF doet al enkele jaren onderzoek naar SSI. Die kennis passen we nu toe op het concept van wallets. Met deze kennis ondersteunen we instellingen bij hun IAM-ontwikkeling. Dit rapport is een verkenning van de mogelijkheden van een SSI-wallet voor onderwijs en onderzoek via een proof of concept SSI-wallet.

Inhoudsopgave

1 Introductie SSI

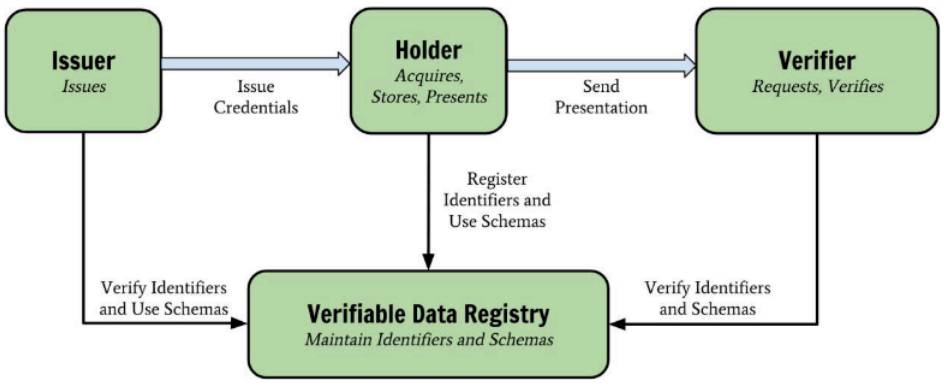
Met deze korte introductie van self-sovereign identity (SSI) geven we de achtergrond waartegen we onze proof of concept (PoC) walletapp hebben ontwikkeld, namelijk SSI-technologie.

Wat is SSI?
SSI is een nieuw paradigma in identitymanagement. Belangrijk verschil met bestaande identitymanagement-ecosystemen, zoals federatief identitymanagement, bijvoorbeeld SURFconext, is dat gebruikers meer controle hebben over het gebruik van hun persoonsgegevens. SSI is echter ook relevant in het bredere speelveld van gegevensuitwisseling, ofwel regie op data. Dit is zichtbaar op nationaal en Europees niveau, onder andere in de nieuwe eIDAS-verordening: een inlogmogelijkheid bedoeld voor Europese burgers en bedrijven die willen inloggen bij Nederlandse diensten met een hun nationale authenticatiemiddel, dus zonder DigiD of eHerkenning.

Hoe werkt SSI?
In het SSI-model geeft de bronhouder, bijvoorbeeld een onderwijsinstelling, gegevens of attributen ('credentials') aan de gebruiker, die deze kan opslaan in een wallet. Deze wallet is meestal een applicatie op de mobiele telefoon van de gebruiker. Wanneer een gebruiker een dienst wil afnemen, vraagt deze dienst de gebruiker om een bepaald bewijs, bijvoorbeeld dat de gebruiker student is. De gebruiker kiest er zelf voor dit vrij te geven aan de dienst – via zijn telefoon.

Rollen in een SSI-ecosysteem
De belangrijkste rollen in het ecosysteem van SSI zijn de volgende:

- Issuers: partijen die attributen (gegevens) over een persoon kunnen uitgeven.
- Verifiers: partijen die iets willen weten over een persoon, zij vragen om attributen.
- Holders: personen die een wallet bezitten en op deze manier regie hebben over attributen.
- Verifiable Data Registries: partijen of plekken waar wordt bijgehouden welke metadata en schema's gebruikt kunnen worden om attributen en *identifiers* te delen.



Rapport technische verkenning naar SSI
In 2021 heeft SURF een technische verkenning naar SSI gedaan. Hierin lees je wat de technische kenmerken, mogelijkheden en uitdagingen zijn van dit concept. Je leest het in dit rapport.
Voor meer informatie over de basisprincipes van SSI, zie: *www.surf.nl/ssi*

2 Ontwikkeling SSI-wallet proof of concept

In dit project grijpen we de mogelijkheid aan te experimenteren met SSI en we leveren een bijdrage aan de ontwikkeling van identity & accessmanagement (IAM) binnen onderwijs en onderzoek. We vinden de aansluiting bij bestaande projecten en diensten en we identificeren relevante trajecten buiten de sector. De focus in deze proof of concept (PoC) ligt op de techniek, functionaliteiten en use cases van een SSI-wallet, waarbij we in de uitvoering hebben gekozen voor prototyping van een werkende applicatie.

2.1 Aanleiding en doelstelling

Binnen SURF doen we al enige tijd onderzoek naar manieren waarop onderwijs en onderzoek kunnen inspelen op ontwikkelingen rond SSI en wallets. Met deze kennis ondersteunen we onderwijsinstellingen bij hun IAM-ontwikkeling en verbeteren we de SURF-dienstverlening. Om het onderzoek naar SSI te kaderen is SURF een SSI-lab gestart waarin we kennis en ervaring met SSI en SSI-technologieën binnen SURF samenbrengen en laagdrempelig delen. In dit lab is deze technische exploratie naar een SSI-wallet voor onderwijs en onderzoek gedaan.

SURF en de sector hebben de wens om te experimenteren met de techniek achter SSI: hoe werkt het en hoe bouwt het voort op huidige SURF-dienstverlening?

We beschrijven hieronder de belangrijkste projecten en diensten waarmee wij raakvlak zien voor onze SSI-wallet PoC:

- eduID, één identiteit waarmee studenten bij iedere onderwijsinstelling terechtkunnen, kan verschillende rollen spelen binnen het SSI-ecosysteem. De ontwikkeling van eduID tot een identity wallet staat op de radar, maar de impact en wenselijkheid hiervan is nog niet duidelijk. We onderzoeken of de huidige functionaliteit van de eduID-app (login, verificatie) is te combineren met SSI-walleteigenschappen.
- Voor de PoC ‘eduWallet’, zoals geformuleerd in Npuls, het achtjarig programma om onderwijs in mbo, hbo en wo te verbeteren door kansen van digitalisering beter te benutten, leveren we input. We zien het uitgeven van microcredentials, zoals edubadges, als een belangrijke use case voor een toekomstige eduWallet en willen dit uitwerken in een experiment.
- Ideeën uit de HOSA IAM, gerelateerd aan SSI, testen we. De HOSA is de Hoger Onderwijs Sector Architectuur. De HOSA-domeinarchitecturen bieden (architectuur)kaders voor gemeenschappelijke sectorvoorzieningen binnen het hoger onderwijs. De domeinarchitectuur Identiteit & Toegang omschrijft kaders voor identity & accessmanagement (IAM).
- In het programma Doorpakken op digitalisering voor het mbo testen we concepten en gebruikerspatronen uit het eigen dossier, zoals geschetst in het programma Doorpakken op digitalisering.
- Concepten en gebruikerspatronen uit het eigen dossier, zoals geschetst in het landelijke programma voor het mbo Doorpakken op digitalisering, testen we.
- We leveren input voor de Europese large scale pilot DC4EU, waar SURF in 2023 participeert, en die bijdraagt aan de implementatie van eIDAS2.0. In DC4EU wordt onder andere gewerkt aan uitgifte van onderwijscredentials en uitwisseling daarvan in Europa via het eIDAS-stelsel.

We zien verder dat, voor het realiseren van de doelen in de digitaliseringsimpuls onderwijs (Npuls), API's en middleware nodig zijn voor toegang tot diensten in het onderwijs ecosysteem. Hiervoor is eenvoudige authenticatie en autorisatie van alle gebruikers een voorwaarde. SSI biedt mogelijkheden om dit onder controle van de eindgebruiker in te richten, maar voor de introductie van deze technologie zal er sprake zijn van een langetermijnpad. Een belangrijk vraagstuk hierbij is hoe een op SSI gebaseerde infrastructuur zich verhoudt tot de huidige federatieve infrastructuur: het meest waarschijnlijke scenario is dat deze twee voorlopig naast elkaar blijven bestaan.

Doel technische proof of concept SSI-wallet
Gezien bovenstaande wensen en vragen is binnen de afdeling Trust & Identity van SURF een technische proef uitgevoerd met als doel:

- technisch ontwikkelen van een walletapp op basis van open source componenten;
- ervaren wat de impact is van de ontwikkeling van een wallet in onderwijs en onderzoek;
- vragen die tijdens de ontwikkeling naar boven komen, in kaart brengen en – waar mogelijk – beantwoorden.

Het doel is niet te komen tot een productiewaardige omgeving. Naast uittesten van SSI gerelateerde use cases, is de wallet gecombineerd met componenten voor federatieve authenticatie (SURFconext, eduID). Dit hebben we expliciet gedaan om te verkennen hoe een mogelijk groeipad voor de instellingen eruit ziet, mocht een ecosysteem van wallets realiteit worden.

Use cases uit onderwijs en onderzoek, doelgroep studenten
De use cases die we onderzoeken zijn gerelateerd aan onderwijs en onderzoek, met als voornaamste gebruikers studenten. Echter, in de sector kunnen docenten en onderzoekers natuurlijk ook een wallet gebruiken. Een belangrijk aspect van SSI is dat gebruikers zelf bepalen welke (onderwijs)gegevens zij uitwisselen en met wie. Deze gegevens zijn nodig om onderwijs te volgen en om gebruik te maken van bepaalde diensten. Denk aan het bewijzen dat je studeert om toegang tot studentenhuisvesting te krijgen. Of, digitaal een diploma of microcredential kunnen aanbieden aan een toekomstig werkgever. Een wallet – een digitale portemonnee met persoonsgegevens – helpt de student hierbij.

Welke gegevens uitwisselen
Aan welke gegevens moeten we denken in onderwijs en onderzoek? Hieronder staan enkele van de belangrijkste attributen die worden uitgewisseld in het SSI-ecosysteem (zie ook hoofdstuk 1 Introductie SSI):

- Affiliatie (ben je student, docent, pre-student etc.)
- Thuisinstelling
- Gastinstellingen
- Diploma's
- Microcredentials
- Identifiers
- Studentnummer
- Toegangsrechten
- Naam
- E-mailadres

Deze lijst is niet uitputtend, maar deze attributen zijn de basis voor veel van de transacties die plaatsvinden bij processen in onderwijs en onderzoek en daaromheen. In paragraaf 2.1 diepen we de use cases verder uit.

Contextexploratie
Op het gebied van wallets is veel ontwikkeling en voortschrijdend inzicht. De exploratie waar dit rapport een beschrijving van is, vond plaats in de periode november 2022 t/m februari 2023. Het onderzoek moet in de context van deze periode worden gezien.

Er zijn inmiddels vele SSI-walletconcepten uitgewerkt in Nederland en internationaal. Door zowel private partijen als (semi-)publieke, denk aan Yivi (voorheen IRMA), Ockto, SOLID en EDI wallet (BZK). In de praktijk zijn de plekken waar dit soort wallets gebruikt worden nog beperkt. Vele vragen zijn daarom nog onbeantwoord:

- Functionaliteit: wat kan je ermee? Wat moet de wallet kunnen doen?
- Gebruikers: begrijpen mensen dat ze regie over gegevens hebben en wat dit betekent?
- Impact op instellingen: hoe verandert SSI het IAM-landschap van instellingen?
- Impact op dienstverleners: hoe verandert SSI de toegang tot dienstverleners?
- Techniek: hoe werkt het? Welke technische standaarden zijn er? Hoe is interoperabiliteit geregeld?
- Policy: wie bepaalt welke persoonsgegevens wanneer met welke partij gedeeld mogen worden? En hoe? Is dit echt alleen aan de eindgebruikers?
- Volwassenheid: in hoeverre is het al toepasbaar? Welke oplossingen zijn er al?
- Businessmodel: wie gaat de transitie naar SSI betalen en is de toegevoegde waarde van SSI voldoende hiervoor?
- Use cases: wat zijn de praktijkvoorbeelden? In welke onderwijscases speelt dit?
- Privacy en juridische aspecten: wat is de rolverdeling in een SSI-ecosysteem? Hoe implementeren we privacy en dataminimalisatie in dit ecosysteem?

Deze vragen hebben input nodig vanuit verschillende domeinen en expertises. Niet alles kunnen we in deze fase beantwoorden. In deze PoC ligt de focus op techniek, functionaliteiten en use cases. Daarnaast besteden we aandacht aan gebruiksvriendelijke ontwerpen. Gebruikersonderzoeken zijn echter nog niet uitgevoerd.

Buiten de sector spelen ook diverse relevant trajecten, onder andere:

- Ontwikkeling van Europese wetgeving rond EU Identity Wallets (eIDAS 2.0).
- Doorontwikkeling van open standaarden, zoals Open Badges 3.0, verschillende W3C standaarden en bij OIDC4VC.

2.2 Methodiek: prototyping

De methodiek voor dit technische onderzoek is prototyping. Het prototype gaat echter verder dan papier, we realiseren een werkende applicatie. Om tot concrete resultaten te komen, ontwikkelen we de applicatie via een agile-methodologie.

Voor het opzetten van een walletapp met bijbehorend ecosysteem van aangesloten entiteiten zijn diverse componenten nodig. Uitgangspunt hierbij is het toepassen van open source componenten, bij voorkeur componenten die aansluiten bij de specificatie van de Europese Commissie voor de eIDAS-referentiewallets (ARF - Architecture Reference Framework) en de al beschikbare componenten van SURF.

Naast het technisch ontwikkelen van een PoC wallet, dient dit project nadrukkelijk ook als middel om verdere vragen over SSI en wallets in kaart te brengen en antwoorden te vinden. De gerealiseerde functionaliteit kan als basis dienen voor pilots en gebruikerstests, en worden doorontwikkeld via verdere iteraties.

3 Use cases, ontwerp en applicatieontwikkeling

Om tot het prototype te komen, hebben we in eerste instantie een ontwerp gemaakt op basis van een aantal use cases en ontwerpprincipes. De principes sluiten aan bij SSI, passen in de context van de sector en voldoen aan de open ontwikkelmethodes van SURF. De benoemde use cases zijn uitgewerkt in benodigde functionaliteiten. Daarna hebben we vastgesteld welke technische componenten wenselijk waren om te gebruiken als basis voor het prototype.

3.1 Toelichting ontwerp

Er is een grote diversiteit aan use cases waarvan we verwachten dat wallets deze kunnen ondersteunen. We hebben een aantal cases omschreven en daarvoor de benodigde technische componenten uitgedacht. Daarnaast hebben we ter inspiratie gekeken naar designs van bestaande walletapps.

3.1.1 Use cases

De meeste use cases waarin een wallet kan ondersteunen, zijn voornamelijk gerelateerd aan de benodigdheden en diensten waar studenten gebruik van maken tijdens hun studietijd. Vooral use cases waarbij flexibilisering van onderwijs centraal staat, of leven lang leren wordt gefaciliteerd, zijn interessant omdat SSI en wallets juist uitwisseling van gegevens over de grenzen van de instelling heen kunnen verbeteren. Dit vertaalt zich in use cases zoals onderstaande:

- Toegang krijgen tot faciliteiten voor studentenhuisvesting.
- Toegang krijgen tot vervolg- of deelopleiding op basis van affiliatie met een instelling.
- Verkrijgen van behaalde diploma’s, microcredentials en skills als professional of student.
- Tonen van behaalde diploma’s, microcredentials en skills aan een (potentiële) werkgever en deel- of vervolgopleiding.
- Verkrijgen van korting op basis van studentstatus bij het kopen van producten of toegangsbewijzen.

Deze lijst aan use cases is niet uitputtend. Er zijn vele variaties te definiëren op basis van de benodigde diensten (aangeboden door *verifiers*) en attributen (aangeboden door *issuers*) zodat de persoon (*holder*) kan doen wat deze wil. We denken dat de basisfunctionaliteiten van een wallet om deze use cases te ondersteunen vergelijkbaar is ondanks de variatie aan use cases.

3.1.2 Functionaliteiten

Bovengenoemde use cases hebben attributen nodig, zoals affiliatie met een instelling, studentnummer en microcredentials die gedeeld kunnen worden via een walletapp. We hebben enkele generieke functionaliteiten gedefinieerd die nodig zijn om de volgende actie te kunnen uitvoeren:

- Activeren van de wallet
- Toevoegen van attributen
- Delen van attributen

Naast deze basisfuncties zijn enkele functies nodig om de persoon regie over de data te kunnen geven:

- Bekijken en bewerken van inhoud (profiel data, attributen)
- Activiteiten inzien (historie van uitwisselingen bekijken)

Het verlopen en intrekken van attributen door de *issuer* (revocatie) zijn ook basisfunctionaliteiten die een wallet moet leveren. Voornamelijk omwille van de haalbaarheid van het prototype binnen de gestelde tijd van het onderzoek hebben we in deze fase van het onderzoek revocatie van gegevens bewust buiten beschouwing gelaten.

3.1.3 Ontwerpprincipes: privacy-by-design

We passen in dit ontwerp privacy-by-design toe: het realiseren van privacyvriendelijke producten door hier al in de ontwerpfase over na te denken. Daarnaast willen we dit doen op een manier waarbij de persoon zelf zoveel mogelijk regie en zelfbeschikking behoudt. Dit borgen we door in het ontwerp de principes van SSI toe te passen.

Dit leidt tot de volgende principes:

- De gebruiker moet zo makkelijk mogelijk privacyvriendelijke keuzes kunnen maken en daarbij geholpen worden via het ontwerp van de applicatie.
- Zo dicht mogelijk aansluiten bij de tien SSI principes:
  1. De gebruiker bestaat en heeft een identiteit.
  2. De gebruiker heeft controle over de identiteit.
  3. De gebruiker heeft toegang tot data.
  4. Systemen en algoritmen dienen transparant te zijn.
  5. De identiteit blijft langdurig bestaan.
  6. Portabiliteit van data en de identiteit.
  7. Interoperabiliteit: de identiteit is zo breed mogelijk inzetbaar.
  8. Consent: gebruiker moet consent geven voor gebruik van de identiteit.
  9. Minimalisatie van data en het vrijgeven daarvan.
  10. Bescherming: de rechten van de gebruiker worden beschermd.

Designsystem

Een van de beoogde doelstellingen was om een wallet specifiek voor onderwijs en onderzoek te toetsen. Dit betekent ook dat de applicatie herkenbaar moet zijn voor doelgroepen in onderwijs en onderzoek. Dit komt tot uiting in de stijl van de applicatie, door waar mogelijk gebruik te maken van het SURF Design System. Het designsystem is in ontworpen voor websites. Het ontwerp van de applicatie levert tegelijkertijd ook input aan een mobiele versie van dit designsystem. Dit leidt tot het principe:

- Herkenbare SURF-stijl gebruiken in het ontwerp van de wallet.

Koppeling met eduID

De wallet moet ook functioneel kunnen interacteren met al beschikbare technische componenten in de sector. Dit komt tot uiting in de identiteit die initieel aan de wallet gekoppeld wordt: eduID. Deze identiteit is bedoeld en beschikbaar voor toepassingen in zowel onderwijs als onderzoek. Daarnaast maken we gebruik van attributen die relevant zijn voor de sector. Dit leidt tot de principes:

- Een identiteit gebruiken die toepasbaar is in de gehele sector (eduID).
- Attributen gebruiken die nodig zijn binnen de sector (zoals edubadges en affiliatie).

Discussiepunt: waar flow starten in app

Een belangrijk discussiepunt voor het ontwerp was waar een flow (de stappen die een gebruiker volgt in de app) in de applicatie moet starten. Wanneer we kijken naar andere walletapplicaties,

zien we dat verschillende aanpakken mogelijk zijn. Wat veel voorkomt, is een trigger waarbij de persoon uitgenodigd wordt om de wallet te vullen met attributen. Dit leidt echter tot het verzamelen van informatie op een nieuwe plek, terwijl hier verder nog geen goede reden (doelbinding) voor is.

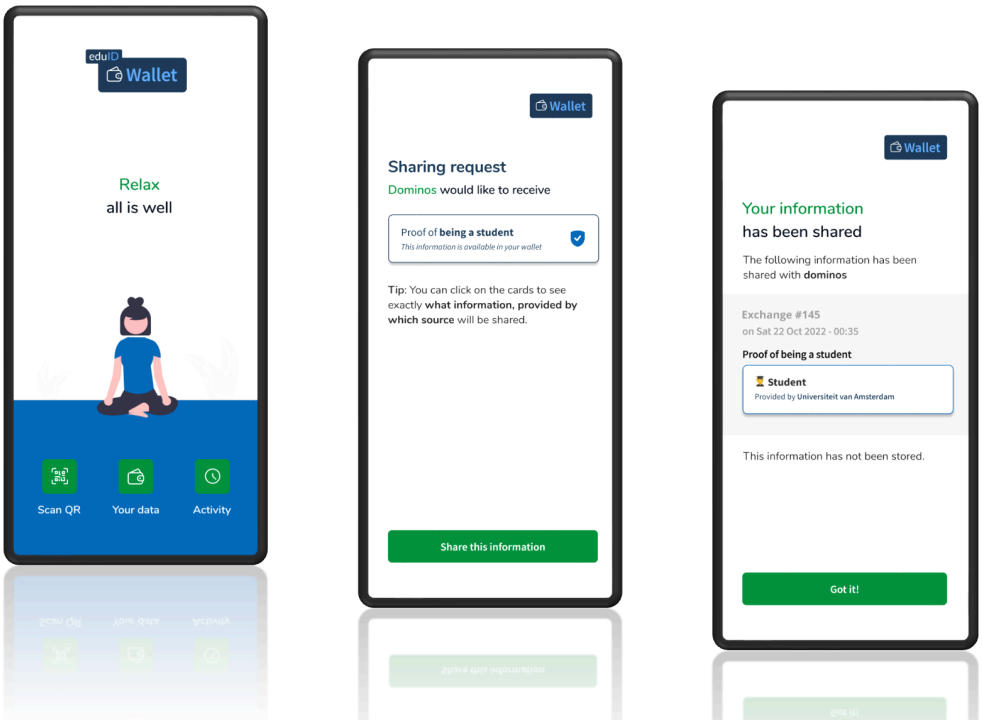
We geven in dit ontwerp de voorkeur aan het starten van flows wanneer de persoon gebruik gaat maken van bepaalde dienstverlening. Dit leidt ertoe dat we starten vanuit de *verifier* (de dienstverlener) en de informatie die nodig is om de specifieke dienst op dat moment mogelijk te maken. Dit betekent ook dat een persoon soms nog attributen bij bronnen moet ophalen, wanneer deze nog niet in de wallet beschikbaar zijn. Dit leidt tot de volgende principes:

- Altijd uitgaan van de persoon die iets wil doen en daarom een actie start.
- Het verzoek van de *verifier* en benodigde attributen zijn leidend in de weergave.

De ambitie is om gebruik maken van open source componenten. Daarnaast willen we waar mogelijk aansluiten bij beoogde standaarden, zoals de EDI wallet van BZK en de specificatie van de Europese Commissie voor de eIDAS-referentiewallets (ARF - Architecture Reference Framework). De referentiewallet gaat verder uit van mobiele applicaties als basis. We verwachten daarnaast dat het gebruik van mobiele apps in de doelgroep studenten gemeengoed is. Dit leidt tot de principes:

- Interactie via mobiele applicatie is de basis.
- Aansluiten bij walletstandaarden waar mogelijk.
- Gebruikmaken van open source componenten.

De ontwerpen tonen aan hoe de wallet de use cases kan ondersteunen. De gerealiseerde ontwerpen worden nader toegelicht in Bijlage 1 Functionele designs.



3.2 Applicatiecomponenten

Het ontwikkelen van de benoemde functionaliteiten doen we zoveel mogelijk op basis van bestaande componenten. Dit doen we om meerdere redenen. Ten eerste ontstaat hiermee een realistische weergave van de werkelijkheid, omdat we dan echt moeten kijken hoe de verschillende onderdelen op bestaande systemen en diensten aansluiten. Ten tweede leidt het gebruik van bestaande componenten ook tot snelheid in het onderzoek, onder andere omdat we op bestaande expertise kunnen voortbouwen. Tot slot is het van belang om input te geven aan bestaande componenten binnen SURF over mogelijke veranderingen die nodig zijn in een walletgebaseerde toekomst.

Om de gewenste functionaliteiten te realiseren, is gebruik gemaakt van:

- Yivi (IRMA): een bestaande open source SSI-wallet die SIDN ontwikkelt in samenwerking met de Radboud Universiteit Nijmegen. Yivi biedt de basis voor het walletcomponent, de benodigde schema's voor attribuutuitwisseling en de opzet van *issuers* en *verifiers* in deze PoC.
- eduID: beschikbaar en bedoeld als identiteit in het onderwijs, ontwikkeld door SURF. Met eduID activeert en koppelt de gebruiker de wallet. Daarnaast maakt eduID het mogelijk om het affiliatieattribuut te verkrijgen.
- SURFconext: bestaande identiteitsfederatie waar dienstverleners en instellingen mee koppelen. Het biedt infrastructuur voor toegang tot onderwijsdiensten en identificatie en wordt in de PoC gebruikt bij het verkrijgen van het affiliatieattribuut vanuit de instelling als dit nog niet binnen eduID bekend is.
- edubadges: het platform voor digitale certificaten voor het Nederlandse onderwijs, ontwikkeld en beheerd door SURF. Met edubadges kunnen gebruikers (*holders*) microcredentials en skills uitwisselen.

We verwachten op basis van deze componenten een goede inschatting te kunnen maken van de uitdagingen en welke keuzes gemaakt moeten worden om een werkbare wallet voor onderwijs en onderzoek te realiseren.

3.3 Gerealiseerde producten

Het onderzoek en de applicatieontwikkeling vond plaats in de periode november 2022 tot en met maart 2023. Tijdens het onderzoek zijn diverse producten gerealiseerd. *Alle producten zijn beschikbaar via de SURF-wiki.*

Designs
Voor alle genoemde functionaliteiten zijn *flows* ontworpen en bijbehorende schermen voor de app ontwikkeld. Ook zijn ontwerpen gemaakt van de *verifiers*. Een overzicht van de verschillende schermen is bijgevoegd in bijlage 1 Functionele designs.

App
Alle schermen zijn geïmplementeerd in een Android-applicatie, waarbij Yivi als back-end gebruikt wordt voor het beheren van de wallet.

Broncodeapp
De app heeft tijdens de ontwikkeling verschillende iteraties doorlopen. De broncode van de app is onder de Apache 2.0-licentie (waar mogelijk) beschikbaar.

Broncode ontwikkelsuite
Voor het testen en ontwikkelen van de verschillende scenario's is veel gebruik gemaakt van de zogenaamde Yivi CLI. Deze applicatie maakt het eenvoudig mogelijk *verifiers* en *issuers* op te zetten en scenario's voor attribuutvrijgave en -opvraging op te zetten en te testen. Alle interacties kunnen met eenvoudige *command line statements* en een JSON-object geïnstantieerd worden. Een voorbeeldbibliotheek van de gebruikte calls in deze pilot, is beschikbaar onder de Apache 2.0-licentie.

Broncode issuer/verifier
Voor het opzetten van de *issuers* en *verifiers* hebben we gebruik gemaakt van SimpleSAMLphp waarvoor eerder een specifieke Yivi-module ontwikkeld was. De broncode en configuratie van deze componenten staan in de SURF-GitHub-repository.

Trustframework
Diverse attributen die in dit onderzoek zijn gebruikt, bijvoorbeeld edubadges, zijn (nog) niet standaard te vinden in de attribuutschema's zoals deze bij Yivi gebruikt worden. We hebben daarom voor zowel eduID als edubadges, specifiek voor deze use cases ontwikkelde schemafiles opgezet. Deze zijn beschikbaar in een *fork*, een kopie, van het Yivi-demoschema.

4 Bevindingen

In dit hoofdstuk lichten we de belangrijkste bevindingen toe. De tussentijdse versies van de applicatie zijn, gedurende het onderzoek, continu door het ontwikkelteam geëvalueerd. In dit stadium is nog niet getoetst onder gebruikers. Waar we in de bevindingen spreken over ‘de gebruiker’ zijn de bevindingen gebaseerd op inschatting van de onderzoekers. We maken onderscheid in bevindingen gerelateerd aan:

- Ontwerp en weergave van de wallet (design bevindingen)
- Bevindingen specifiek voor edubadges
- Bevindingen specifiek voor eduID
- Technische bevindingen gedurende ontwikkeling van de wallet (development bevindingen)
- IRMA-specifieke bevindingen

4.1 Design: ontwerp en weergave van de wallet

Onderstaande paragrafen beschrijven de uitdagingen met het initieel gemaakte ontwerp van de wallet, zoals beschreven in hoofdstuk 3.

4.1.1 Het wallet-login-proces

Het initiële ontwerp hield geen rekening met daadwerkelijk herhaald inloggen in de wallet. Inloggen in de wallet op basis van bijvoorbeeld een pincode of met biometrische gegevens is een vereiste. De wijze van implementatie heeft impact op zowel de gebruikersbeleving als de betrouwbaarheid van de wallet. Dit moeten we tegen elkaar afwegen.

4.1.2 Weergave van uitvraag door verifier

Het huidige ontwerp is gebaseerd op welke attributen de *verifier* vraagt. Daarbij is toelichting vereist op *waarom* de *verifier* deze specifieke attributen nodig heeft. Dit is noodzakelijke informatie voor de gebruiker om een keuze te maken om de vrijgave van de attributen al dan niet te accepteren. Daarnaast is het van belang vanwege het aantonen van doelbinding. Dit is noodzakelijk om te voldoen aan de AVG.
Het is de vraag met welke fijnmazigheid attributen getoond en toegelicht moeten worden aan de gebruiker. Een te diep detailniveau kan tot onduidelijkheid leiden. Bijvoorbeeld als het technische gegevens zijn, zoals *identifiers.* Die hebben voor een gebruiker mogelijk weinig betekenis. Wat de ideale weergave is van een uitvraag moet nader onderzocht worden.

4.1.3 Weergave trusted verifiers

De wallet kan worden gebruikt om het vertrouwen in een *verifier* weer te geven. Het moet duidelijk zijn of een *verifier* vertrouwd en bekend, of juist onbekend, is binnen het ecosysteem. In het ontwerp is hiervoor een vinkje met de term ‘trusted verifier’ gebruikt. Het is op dit moment onduidelijk hoe een dergelijke classificatie tot stand zou moeten komen. Daarbij is het waarschijnlijk dat meerdere van dit soort trustframes naast elkaar bestaan, denk bijvoorbeeld aan een van de overheid en een van de sector. Verdere uitwerking hiervan is essentieel voor een gebruiker om te kunnen bepalen om attributen al dan niet te delen.

4.1.4 Onderscheid in de mogelijke status van een attribuut

Bij het gebruik van een wallet doorlopen de attributen een aantal fases. Denk aan statussen zoals geverifieerd, verlopen, ingetrokken enzovoorts. In het huidige ontwerp hebben we deze

statussen nog niet nader uitgewerkt. De weergave moet de gebruiker duidelijk informeren over de verschillende toestanden waarin een attribuut zich kan bevinden.

4.1.5 Accept en Deny

Voor iedere transactie met data, in of uit de wallet, moet de gebruiker de mogelijkheid hebben deze te weigeren. Dit ligt voor de hand op het moment van uitgifte van gegevens vanuit de wallet richting een *verifier*. Echter, ook bij het inladen van data is het nodig te tonen wat in de wallet opgenomen wordt en de gebruiker expliciet hiervoor om toestemming te vragen. Het kan namelijk zijn, dat de data niet correct is of dat bijvoorbeeld de gebruiker bij nader inzien besluit de uitgevende partij niet te vertrouwen. In het huidige ontwerp van de wallet is dit, behalve in de flow om edubadges op te halen, nog niet consistent toegepast.

4.2 edubadges-integratie

De inzet van edubadges is van belang in de uitwisseling van microcredentials én in het aantonen en verifiëren van extra-curriculaire skills of vaardigheden. Toetsen of een wallet edubadges kan toevoegen en vrijgegeven, is daarbij ook van belang. edubadges ophalen is technisch mogelijk, al zijn de mogelijkheden om edubadges op een goede manier te delen beperkt. Er is meer functionaliteit nodig dan in de huidige variant van de wallet beschikbaar is. Daarnaast vraagt het kunnen opvragen van edubadges om metadata over beschikbare badges. De oplossing voor deze issues ligt niet altijd alleen bij SURF.

4.2.1 Vrijgave van individuele attributen uit één edubadge

In het ontwerp van de wallet kozen we ervoor om losse attributen te tonen aan de persoon. Dit is technisch mogelijk en in lijn met de wens de gebruiker slechts een minimale set attributen te kunnen laten vrijgeven. Echter, een edubadge bestaat uit verschillende attributen die *in samenhang* een betekenis hebben. Losse attributen tonen aan de gebruiker is niet voldoende om tot een zinvolle weergave te komen. Deze losse attribuutvelden zijn daarnaast niet los deelbaar, maar moeten als set vrijgegeven worden. Een mogelijke oplossingsrichting is het implementeren van *verifiable presentations* [1]

4.2.2 edubadges opvragen

Hoe *verifiers* (een collectie van) edubadges kunnen opvragen, is vooralsnog onduidelijk. De *verifier* weet namelijk niet precies welke type edubadges er bestaan en zij weet ook niet welke specifieke vakken en vaardigheden relateren aan specifieke edubadges. Hierdoor is het onmogelijk om te selecteren op edubadges die mogelijk voldoen aan de eisen waarop geselecteerd wordt.
Een oplossingsrichting is Badgeclasses doorzoekbaar te maken, of zoeken op inhoud van de edubadge. Daarbij is de vraag of dat soort complexe logica onderdeel moet zijn van de interactie tussen de wallet en de *verifier*. Of, dat deze geïmplementeerd wordt op een andere wijze, waarna alleen de daadwerkelijke uitwisseling van de edubadges via het walletprincipe verloopt.

[1] *Een verifieerbare presentatie van een verzameling attributen. Zie ook: https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations*

4.2.3 edubadges selecteren als holder

Een mogelijke oplossingsrichting is selectiemogelijkheden ondersteunen om specifieke edubadges te delen door de gebruiker zelf. Dit is een zeer wenselijke functionaliteit voor de wallet. Daarbij is behoefte aan een complexere interface voor selectie van edubadges dan voorzien in het huidige ontwerp van de wallet. Een voorselectie op basis van een bepaald onderwerp door de *verifier* zou dit kunnen ondersteunen. Dit is nu nog niet mogelijk (zie 4.2.2). Vervolgonderzoek moet verder uitwerken hoe het selecteren van badges door de *holder*, zowel technisch als in de weergave, mogelijk gemaakt kan worden.

4.3 eduID-integratie

4.3.1 eduID als basisidentiteit

Het uitgangspunt om eduID als basisidentiteit te gebruiken voor verdere interacties in onderwijs en onderzoek lijkt prima bruikbaar in combinatie met een wallet. Tijdens de PoC hebben we succesvol een Yivi-schema gemaakt en gebruikt om attributen uit te wisselen tussen eduID en de wallet. Ook hebben we attributen toegevoegd aan de wallet die het profiel van de persoon verrijken, bijvoorbeeld de *affiliation* zoals uitgegeven door de instelling.
Belangrijk aandachtspunt daarbij is wel dat eduID (via SURFconext) op dit moment gebruik maakt van gepseudonimiseerde identifiers per aangesloten dienst. Dit gebeurt om linkability van gebruikers tussen diensten tegen te gaan. Diensten die hun gebruikers zowel op de traditionele federatieve manier in een browser als via een wallet willen bedienen, kunnen hierdoor mogelijk de gebruiker niet herkennen.

4.3.2 Walletinitialisatie

Een van de ontwerpkeuzes was dat de gebruiker de wallet altijd met een eduID-basisidentiteit moet vullen. Het leek het eenvoudigste dit al bij initialisatie van de wallet af te handelen (zie ook de flows Activeren wallet in bijlage 1).
We hebben de mogelijke initialisatieflows in kaart gebracht. Omdat de gebruiker verschillende mogelijke beginpunten heeft (eduID-website, eduID-app, walletapp) was het aantal mogelijke routes erg groot en zijn er veel scenario's waar de gebruiker op een dood spoor terecht kan komen. Uiteindelijk bleek geen van de voorgestelde routes haalbaar, omdat deze allemaal zouden leiden tot het vermengen van attributen met verschillende trustframeworks (zie 4.3.2). Vooralsnog is de initialisatie daarom beperkt tot een flow die een 'reguliere' Yivi-issuerflow volgt.

4.3.3 Credentials via de walletapp laden

Met name bij eerste gebruik is het gangbaar de mobiele app te initialiseren, bijvoorbeeld door de app te laten communiceren met een via OAuth afgeschermd REST API. In de context van SSI is het daarbij echter van belang goed na te denken wat de autoritieve bron is voor de gegevens die worden ingeladen. Die bron moet namelijk wel als zodanig binnen het trustframework van de wallet en alle *verifiers* herkenbaar zijn. Momenteel blijkt het om die reden nog niet mogelijk gegevens op een andere manier in te laden dan via een reguliere Yivi-*issuer.* Een vergelijkbaar scenario kan ook spelen als we bijvoorbeeld data afkomstig van een paspoortscanapp in de wallet willen plaatsen.
Het is technisch waarschijnlijk mogelijk, door slim gebruik te maken van *deep link,* om de benodigde complexiteit grotendeels voor de gebruiker te verbergen. Dat vraagt echter om aanpassing van diverse provisioning flows in de eduID-app. Dat viel buiten de scope van deze pilot.

4.4 Development

4.4.1 Complexiteit gebruikersflow

Gebruik van wallets leidt al snel tot complexe ketens van gegevensuitwisseling en daardoor tot mogelijk een complexe flow voor eindgebruikers. Dit probleem treedt op bij het initieel aanmaken van de wallet, maar ook wanneer de flow voor uitgifte van attributen complex is. Bijvoorbeeld wanneer nog extra attributen nodig zijn tijdens een uitvraag door een *verifier*, zeker wanneer de extra attributen bij verschillende *issuers* opgehaald moeten worden. Als het ophalen van een extra attribuut lang duurt, kan dit leiden tot een time-out in de uitgifteflow.

Voor sommige flows moeten gebruikers gebruikmaken van andere apps op hun mobiele devices, denk bijvoorbeeld aan inloggen op een *issuer* via de eduID- of DigiD-app. Deze flow kan voor gebruikers verwarrend zijn.

Er is (veel) samenwerking en afstemming, zowel qua techniek als semantiek, nodig tussen stakeholders om een keten volledig en correct te laten werken voor de gebruikers. Het walletconcept was juist bedoeld om afhankelijkheid tussen partijen en de afhankelijkheid van de gebruiker van partijen te verkleinen. De hoge mate van ontkoppeling tussen de verschillende onderdelen van de keten leidt tot flows met veel uitzonderingen en mogelijke *unhappy* flows. Er is veel expertise nodig om integratie en een goede en consistente gebruikerservaring te realiseren.

4.4.2 Ontwikkelomgeving

Gezien de complexiteit is het – voor het succesvol testen en ontwikkelen van applicaties in dit ecosysteem – van groot belang zoveel mogelijk ketenafhankelijkheden weg te nemen door het inzetten van (mock-)interfaces. In onze pilot is gebruik gemaakt van Yivi CLI. Op deze manier kunnen verschillende ontwikkelaars in verschillende delen van de keten gelijktijdig en zonder onderlinge afhankelijkheid aan de slag.

4.4.3 Trustframework

Yivi maakt gebruik van een op metadata gebaseerd trustframework waarbij SIDN als trusted third party optreedt. Dit concept lijkt sterk op hoe dit voor SURFconext, Entree of eduGAIN federatie geregeld is. We weten daarom dat dit model in principe geschikt is voor gebruik met een (zeer) groot aantal deelnemers. Om echter te schalen tot het niveau dat nodig is voor nationaal, pan-Europees of wellicht zelfs globaal niveau, zijn flinke wijzigingen nodig, zowel in de techniek als in het beheer van de Yivi-metadata. Een mogelijke oplossing is een delegatiemodel te introduceren waarbij voor bepaalde sectoren een andere partij deze rol voor hun rekening neemt. Binnen Nederland liggen SURF en Kennisnet hierbij voor onderwijs en onderzoek voor de hand. Waar in het verleden deze twee federaties los van elkaar opereerden, kan het waardevol zijn te bekijken of een gezamenlijke aanpak in dit nieuwe ecosysteem zinvol is.

4.4.4 Categorisering

Op diverse plaatsen in de app helpt het de gebruikers, als categorisering van de informatie plaatsvindt. Voorbeelden hiervan zijn een weergave van alle ‘naam-’gerelateerde attributen in de wallet (ongeacht *issuer*) of bijvoorbeeld een indicatie dat een bepaalde *verifier* ‘vertrouwd’ is. Gezien het dynamische karakter van een walletecosysteem is het niet praktisch dit soort catalogiseringen vast te leggen in de code van de app, en ligt het ophalen van lijsten of een

vergelijkbaar mechanisme voor de hand. Een dergelijk register heeft echter impact op zowel de schaalbaarheid als mogelijk ook de betrouwbaarheid van de wallet.

4.4.5 Credentialsbinding

Bij het gebruik van een wallet is het voor de *verifiers* van belang dat de credentials die in de wallet beschikbaar zijn, ook daadwerkelijk toebehoren aan de eigenaar van de wallet. In het geval van edubadges bijvoorbeeld, moet de *verifier* kunnen vaststellen dat de edubadge daadwerkelijk is uitgegeven aan een bepaalde persoon. Hiervoor kan de *verifier* vertrouwen op de (policy van) de wallet. Het lijkt echter beter om bepaalde attributen in de edubadges direct te valideren tegen attributen die onderdeel zijn van de identiteit die in de wallet beschikbaar is, bijvoorbeeld via eduID. Een *verifier* kan dan beide sets attributen uitvragen en deze met elkaar vergelijken. De consequentie daarvan is wel dat dit tot een zekere mate van herleidbaarheid leidt, omdat er dan gebruikt gemaakt moet worden van persistente identifiers over meerdere bronsystemen. Aan de andere kant kan het ook voorkomen dat uitgegeven badges in de wallet terechtkomen, die niet gelinkt zijn aan eduID (bijvoorbeeld internationaal uitgegeven badges). Hier zal een andere oplossing voor gevonden moeten worden.

4.4.6 Omgaan met attributen

Het omgaan met en weergeven van attributen is complex. Keuzes in de weergave hebben voor- en nadelen. Onderstaand lichten we twee bevindingen en een uitdaging toe.

Ten eerste is een terugkomend concept in andere walletapplicaties dat van ‘kaarten’ die diverse attributen bevatten – tenminste visueel. Hoe de specifieke attributen aan een gebruiker getoond worden is niet vanzelfsprekend. De data die die de gebruiker te zien krijgt, als zij die willen delen, kan in de huidige situatie nog technisch van aard zijn. De daadwerkelijke eduID-identifier is bijvoorbeeld een ondoorzichtige set karakters. Deze *identifier* is op weinig plaatsen zichtbaar en kan een gebruiker mogelijk verwarren. De gebruiker kan besluiten dit ‘vreemde’ attribuut niet vrij te geven aan de *verifier* omdat de gebruiker niet begrijpt wat het doel van dit attribuut is.

Ten tweede kan het voorkomen dat de *verifier* niet alle data uitvraagt die *in samenhang verstrekt is*. Dit kan leiden tot inconsistente data of gebruik van data zonder context. Een voorbeeld hiervan is een edubadge, waarbij attributen binnen de badge betekenis kunnen verliezen wanneer de gebruiker deze losstaand deelt. Het is van belang om verder te onderzoeken welk niveau van fijnmazigheid in getoonde data gewenst is.

Tenslotte is er een uitdaging met complexe datasets. Sommige data wil een gebruiker wel kunnen delen met een *verifier*, maar leent zich slecht voor transport via een wallet. Denk aan audiovisueel materiaal gemaakt ter ondersteuning van een cv, of bijvoorbeeld een complexe set attributen die een onderzoeker toegang geven tot onderzoeksinfrastructuur, zoals het GA4GH Passport. Tegelijkertijd wil de gebruiker wel de controle houden over de toegang die de *verifier* heeft tot deze data, op vergelijkbare wijze zoals dat met de walletattributen kan. Diverse oplossingen zijn denkbaar voor dit probleem, zoals bijvoorbeeld het combineren van een persoonlijke datakluis voor de opslag met een wallet voor het regelen van de toegang tot deze data in de kluis. Dit zou nader onderzocht moeten worden.

4.5 Yivi-specifieke bevindingen

4.5.1 Centrale keyserver

Yivi gebruikt een centrale keyserver die de helft van de key opslaat die nodig is om de gegevens van een gebruikerswallet te decrypten. Deze informatie wordt bij het opstarten van de wallet opgehaald. De consequentie hiervan is dat verplichte registratie nodig is van de Yivi-wallet bij deze keyserver. Daarnaast vormt de keyserver een risico, omdat gebruikers hun wallet niet kunnen gebruiken als deze server niet beschikbaar of bereikbaar is (single point of failure). Als SURF zelf een wallet zou voeren op basis van dit Yivi-model, dan moeten we een besluit nemen over waar deze infrastructuur gerund wordt.

4.5.2 Gebruik labels door verifier

In het Yivi-ecosysteem kan de *verifier* labels toevoegen aan attributen die ze bevragen. De gebruiker ziet deze in de wallet. Er is echter geen garantie dat deze labels ook daadwerkelijk een relatie hebben met de attributen die een *issuer* in de wallet heeft geplaatst. Dit kan leiden tot verwarring, maar in het ergste geval ook tot misbruik, omdat het mogelijk is onder valse voorwendselen bepaalde attributen aan de gebruiker te vragen. Labels mogen ook gebruikt worden bij zogenaamde disjunctions, waarbij de *verifier* een gebruiker kan vragen om combinatie van gegevens uit verschillende bronsystemen. Echter, gebruik van labels is niet verplicht bij disjunctions, wat voor de gebruiker tot een verwarrende gebruikerservaring kan leiden.

4.5.3 SDK en open standaarden

Het doel van deze technische exploratie was om een wallet voor onderwijs en onderzoek te testen en daarmee ook de wens om een herkenbare SURF-stijl te gebruiken in het ontwerp van de wallet. Dit bleek niet direct mogelijk met Yivi.
De huidige Yivi-app is duidelijk niet gebouwd als een software development kit (SDK). Hierdoor is het combineren van Yivi in of met een andere app bijzonder lastig. Dit blijkt onder andere uit hoe het Yivi-eventmodel geïmplementeerd is en ook is gebleken dat de back-endapplicatie (in GO) technical debt bevat. Het daadwerkelijk combineren van de (reeds bestaande) eduID-app met een Yivi-wallet bleek hierdoor niet mogelijk binnen het tijdsbestek van de pilot.
Yivi implementeert op dit moment geen open standaarden voor de communicatie tussen *issuer*, *verifier* en wallet. Hierdoor is Yivi momenteel een silo. Overigens werkt Yivi wel aan de implementatie van de gestelde interoperabiliteiteisen conform eIDAS 2.0, zoals beschreven in de ARF.

5 Conclusie en vervolgstappen

Gedurende het ontwerp en de ontwikkeling van het prototype zijn we vele design en development issues en bevindingen tegengekomen. Wat zijn de belangrijkste conclusies die we kunnen trekken? Niet alle vragen en issues die we tegenkwamen lagen daarnaast binnen de scope van deze PoC, we definiëren daarom ook vervolgvragen en verdere richtingen voor onderzoek.

5.1 Conclusies

Complexiteit
In een walletecosysteem zijn veel partijen betrokken. De onafhankelijkheid van die partijen is, in theorie, de kracht van SSI. Echter, deze onafhankelijkheid introduceert ook complexiteit en maakt het ingewikkeld om te ontwikkelen en te testen door de gehele keten.

Fijnmazigheid van attributen versus complexe data
Hoewel het wenselijk is dat een gebruiker fijnmazig controle heeft over de vrijgave van attributen, zijn er diverse scenario's waarbij juist een complex data-object (bijvoorbeeld een edubadge) als geheel aan de *verifier* verstrekt moet worden. Het is ook denkbaar bepaalde complexe data-objecten juist te vereenvoudigen tot een ja/nee-vraag. Denk bijvoorbeeld aan de vraag of iemand een student is. De gebruiker kan dit met een simpele ja/nee beantwoorden in plaats van de affiliatie met een specifieke instelling te delen.
Een walletecosysteem moet in meerdere scenario's kunnen voorzien. Hierbij moet duidelijkheid voor de persoon worden gewaarborgd: het vrijgeven van attributen moet eenvoudig zijn, maar ook niet weer te eenvoudig, omdat de gebruiker dan het risico loopt te veel attributen te delen en/of dat deze niet te gebruiken zijn door de *verifier*.

Verbinden van identiteit aan attributen
Het is zeer belangrijk om te kunnen aantonen dat de gegevens in de wallet bij de gebruiker horen. Om dit betrouwbaar te kunnen vaststellen zijn diverse zaken nodig, onder andere het verbinden van deze attributen aan een betrouwbare identiteit. Dit is soms nodig op het moment van uitgifte aan een *verifier* en bij het ophalen van attributen bij een *issuer*. Een voorbeeld hiervan is de opname van de eduID-identifier in een edubadge. De identiteit moet in bepaalde gevallen meegegeven worden als onderdeel van het verzoek om gegevens. Dit vergroot het risico op linkability.

Afhankelijkheid van centrale componenten
Het SSI-ecosysteem is bedoeld om de afhankelijkheid van centrale componenten te reduceren. Diverse functionele wensen, zoals bijvoorbeeld het kunnen groeperen van attributen onder een algemene noemer (weergave van alle 'naam'-attributen in de wallet) of het kunnen tonen van betrouwbaarheid van *verifiers* door te laten zien in welke verschillende trustframes ze deelnemen,bevorderen het gebruikersgemak, maar vereisen waarschijnlijk centrale componenten.

Attributen buiten het trustframe en meerdere trustframes
Het combineren van attributen uit verschillende trustframes is bijzonder lastig, omdat er op dit moment geen manier is om trust tussen verschillende ecosystemen onderling uit te drukken. De

enige praktische route is momenteel het gebruik van proxies die een brug kunnen vormen tussen beide trustframes (bijvoorbeeld SURFconext en Yivi).

Trust (metadata) distributie
Het in Yivi gebruikte trustframe is gebaseerd op een centrale infrastructuur. Dit hoeft geen probleem te zijn, maar kent wel aandachtspunten ten aanzien van de schaalbaarheid.

5.2 Vervolgvragen

5.2.1 Gebruikerservaring

Uit de tests van de walletapplicatie is gebleken dat er complexe interactiepatronen ontstaan. De data die gebruikers te zien krijgen gedurende het proces van data delen is nog technisch van aard. Het niveau van fijnmazigheid in getoonde data en de menselijk interpreteerbaarheid daarvan is geen gemakkelijke keuze.
Het doel van de ontwerpen in deze PoC is om gebruikersvriendelijk en begrijpelijk te zijn. Echter was in dit onderzoek nog geen ruimte om met gebruikers te testen. Het is dus nog een open vraag of de ontwerpen en applicatie voldoen aan de wensen die we op dit vlak hebben.
In vervolgonderzoek is het raadzaam om gebruikers te laten toetsen of de interacties uitvoerbaar en begrijpelijk zijn. En bovenal of gebruikers daadwerkelijk regie over de data ervaren en begrijpen wat ze gedaan hebben.

5.2.2 Regie op gegevens

In de pilot hebben we een aantal verschillende scenario's uitgewerkt. Voor sommige scenario's, zoals het delen van een edubadge, ligt het voor de hand dat de gebruiker zelf directe controle heeft over de uitgifte, zonder dat de instelling daar nog bij betrokken is; een analogie naar het huidige gebruik van een papieren diploma. Voor andere data, zoals bijvoorbeeld de identiteit, is dit minder duidelijk. Stel dat het gebruik van de identiteit bijvoorbeeld tot kosten leidt bij de instelling omdat er een licentie wordt afgenomen. Wie is in dat geval verantwoordelijk voor wat? Waar zit het spanningsveld tussen regie op data door de persoon en de wettelijke taak van de instelling? In hoeverre heeft de instelling het recht en de mogelijkheid om te bepalen waar bepaalde gegevens gebruikt worden? In hoeverre kan/mag de student zelf verantwoordelijk zijn voor uitwisseling van data? Wat zijn de implicaties daarvan? Het zal duidelijk zijn dat dit vragen oproept op functioneel en juridisch vlak.

5.2.3 Technische aspecten

Tijdens de pilot zijn we diverse technische uitdagingen tegengekomen die mogelijk impact hebben op (doorontwikkeling van) bestaande SURF-diensten als we die beter willen aansluiten op een walletecosysteem.

eduID-integratie
Een van de beoogde doelen van de pilot was een integratie van de wallet met eduID en de eduID-app. Het inladen van eduID-attributen in een wallet op basis van SURFconext en een Yivi-issuer bleek vrij eenvoudig. In het ontwerp hadden we echter we een flow beschreven waarbij het inladen van deze credentials al kon plaatsvinden als onderdeel van de initialisatie van de wallet. Het bleek echter lastig de eduID-schermen en API's te gebruiken om dit voor elkaar te krijgen. Omdat er zowel een webbased als mobiele instantie is, ontstaat een zeer complexe set flows, met veel mogelijke edge cases. Daarnaast levert deze manier van vullen van de wallet een

conflict op met betrekking tot het mixen van gegevens van verschillende authoritieve bronnen.

eduID en SURFconext API security
De aanpassingen in eduID en de extra complexiteit die in de walletapp nodig zijn, voor de gewenste integratie vielen niet binnen de scope van deze pilot. Als we streven naar een geïntegreerde app waarin bestaande eduID-appfunctionaliteit en een wallet samen komen, moeten we dit verder verkennen. Omdat eduID gebruik maakt van SURFconext API security zou ook dit in beschouwing genomen moeten worden. Op dit moment biedt eduID een REST API voor het bevragen van de dienst. Het zou een goed idee zijn te onderzoeken of de OpenId4VCI-standaard een mogelijkheid biedt om gegevens via SURFconext API security op een gestandaardiseerde manier uit te wisselen, waarbij we dan direct voorsorteren op een van de standaarden die in de EUID als standaard is aangewezen. Hiermee zouden we ook voor verschillende educatieve diensten, zoals bijvoorbeeld edubadges een basisvoorziening rondom authenticatie en secure access, grootschalig kunnen leveren via SURFconext.

Gebruikers identificeren
Momenteel volgt eduID (en overigens ook SURFconext) de strategie om iedere dienst een eigen pseudonieme identifier te geven om de privacy van de gebruiker te beschermen. Omdat de wallet voor eduID een losstaande dienst is, wordt hier een gepseudonimiseerde identifier aan uitgegeven. Consequentie hiervan is dat de identiteit in de wallet een andere identifier heeft dan de identiteit die gekoppeld is aan de edubadges. Het is hierdoor lastig voor een *verifier* om betrouwbaar vast te stellen of een edubadge wel aan de betreffende persoon is uitgegeven. Dit beperkt de mogelijkheden voor het delen van badges via een wallet.

Levensduur attributen en revocatie
Hoewel we in de PoC op een aantal plaatsen functionaliteit hadden voorzien voor het verwijderen en intrekken van attributen, is dit in de techniek niet verder uitgewerkt. Reden hiervoor is dat het niet duidelijk was hoe dat feitelijk zou moeten en wat de uiteindelijke impact ervan zou moeten zijn op eerder uitgegeven credentials en achterliggende systemen.
Het is duidelijk dat zowel revocatie alsook de levensduur van attributen in een walletecosysteem, in belangrijke mate impact kunnen hebben op de gebruikerservaring én de betrouwbaarheid en veiligheid van het systeem. Omdat hierbij waarschijnlijk zeer tegengestelde belangen gecombineerd moeten worden, is het verstandig hier nader onderzoek naar te doen.

5.2.4 Toepasbaarheid

Deze PoC toont aan dat bestaande oplossingen in de markt als basis kunnen dienen voor de doorontwikkeling van een eduWallet. Dit levert wel diverse uitdagingen op: niet alleen op het gebied van techniek, maar ook op het gebied van governance. Uit de pilot blijkt dat veel mogelijk is met een walletecosysteem. De vraag is voor welke scenario's nu echt een business case is. Pas als daar meer duidelijkheid over is, is het zinvol om te verkennen hoe wallets de gegevensuitwisseling binnen onze sector gaan veranderen.
Een andere uitdaging is de opkomende publieke oplossingen, waaronder de EDI wallet van het ministerie van Binnenlandse Zaken en de EU-referentiewallets. Deze zijn op dit moment nog niet voldoende doorontwikkeld en volwassen om te gebruiken binnen onze sector. Ze zijn echter wel belangrijk en compatibiliteit met deze wallets is gewenst.

Hoe verder?
Afsluitend kunnen we stellen dat een ecosysteem rond wallets alleen werkbaar en schaalbaar is als een zeer hoge mate van technische en semantische standaardisatie wordt bereikt.

Vooralsnog moeten we daarbij rekening houden met het leveren van credentials aan een grote variatie aan wallets. SURF levert hieraan een bijdrage via onderzoek en ontwikkeling op het vlak van SSI en wallets in de onderwijssector. Dit doet SURF op meerdere manieren:

SURF participeert in de EU large scale pilot DC4EU. Deze large scale pilot draagt bij aan de implementatie van eIDAS2.0. Op nationaal niveau experimenteert SURF in het programma Npuls met de ontwikkeling van een 'eduWallet'. In beide trajecten kan SURF voortbouwen op de bevindingen die gedaan zijn in deze PoC. Op langere termijn kan SURF instellingen gaan ondersteunen, door de integratie met deze omgevingen te verzorgen wanneer deze dichter bij realisatie zijn.

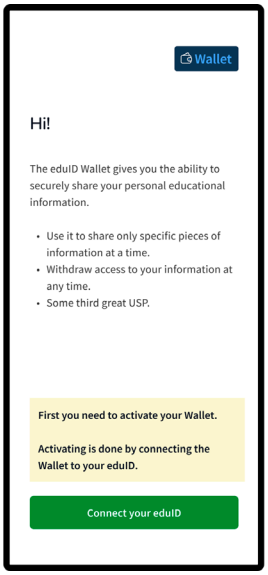
Op korte termijn kan SURF samen met instellingen op basis van specifieke use cases verdere experimenten en pilots uitvoeren. Concreet vervolgonderzoek binnen het SSI-lab van team Trust & Identity is inventariseren wat de beoogde architectuur is wanneer SURFconext ingezet wordt als onderdeel van de dienstverlening voor het uitgeven en verifiëren van *Verifiable Credentials* op basis van OpenID4VCI-standaard. We willen dit doen op basis van realistische use cases in onze sector, waarbij we de stakeholders van deze use cases nadrukkelijk willen betrekken bij het project.

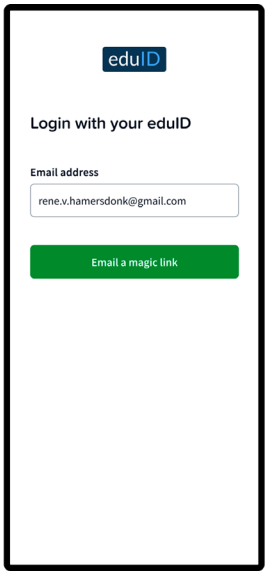
In de genoemde trajecten maar ook daarbuiten, nodigen we instellingen die op dit thema zelf willen deelnemen aan initiatieven nadrukkelijk uit om zich te melden en de opgedane kennis te delen.

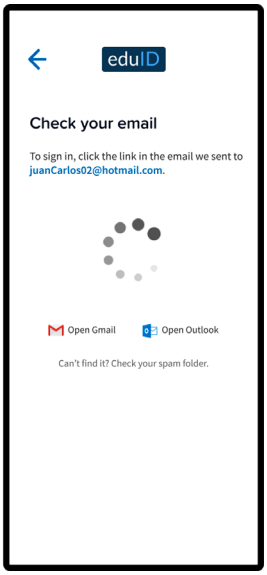
Bijlage 1 Functionele designs

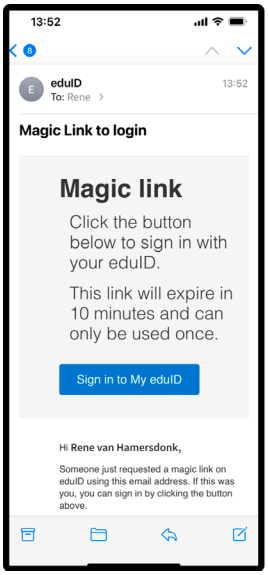
Activeren wallet

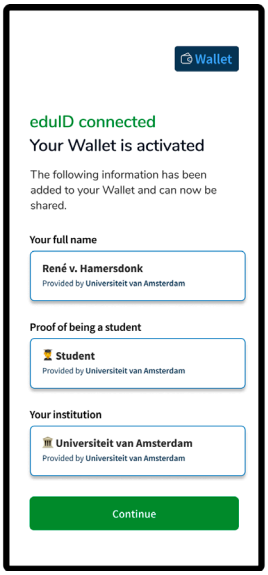
Het activeren van de wallet gebeurt op basis van eduID. Wanneer de persoon de wallet voor het eerst downloadt, is inloggen met eduID vereist. Als deze persoon nog geen eduID heeft, dan moet deze eerst worden aangemaakt. Wanneer deze persoon al bij eduID bekend is of een persoon bij een instelling studeert, kan dit gegeven worden opgehaald tijdens het inloggen met eduID bij de wallet. Voor de kansen en uitdagingen rond de integratie met eduID, zie paragraaf 4.3 eduID-integratie.

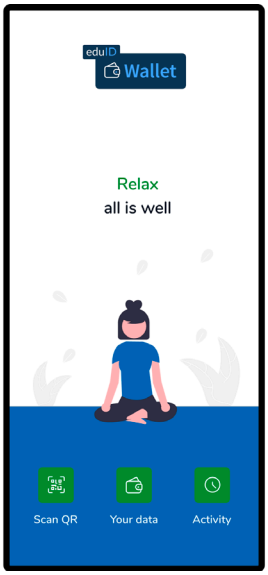


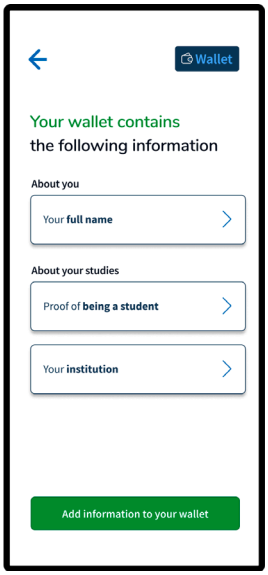






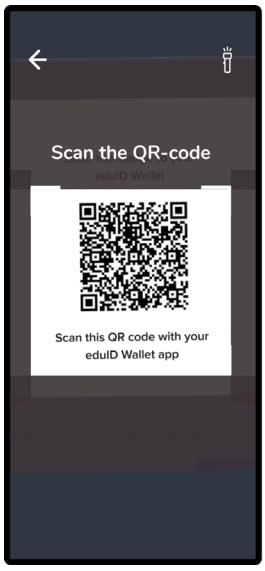


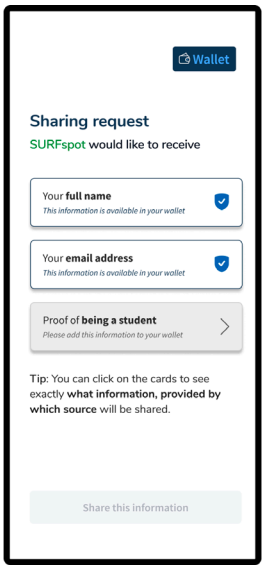


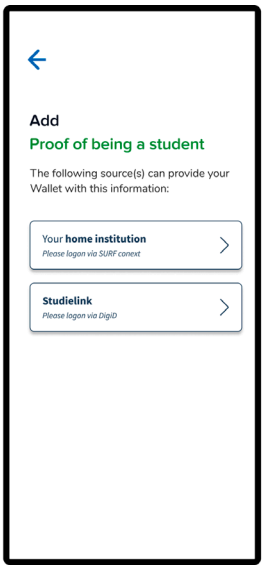


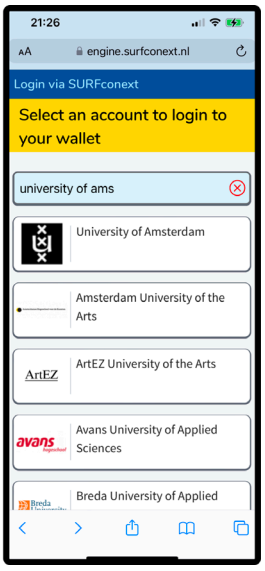
Attributen toevoegen

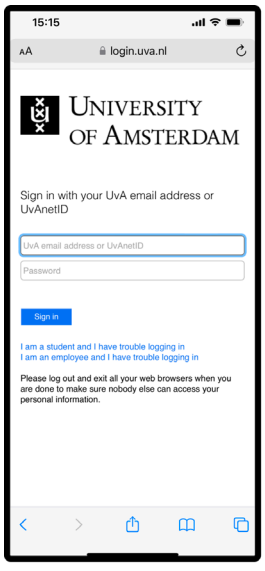
Het toevoegen van attributen zal over het algemeen starten wanneer de persoon actie onderneemt om een dienst te gebruiken. In onderstaand voorbeeld wil de persoon bijvoorbeeld met korting boeken bestellen bij SURFspot. Hiervoor wil SURFspot onder andere weten of de persoon student is en toont een QR-code om de informatie op te vragen vanuit de wallet. In dit geval is het bewijs dat deze persoon een student is nog niet bekend bij de wallet. De persoon haalt dit attribuut op via Studielink of een instelling. De persoon kan daarna de benodigde gegevens delen met – in dit geval – SURFspot.

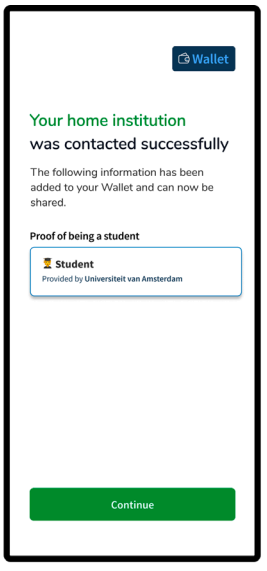


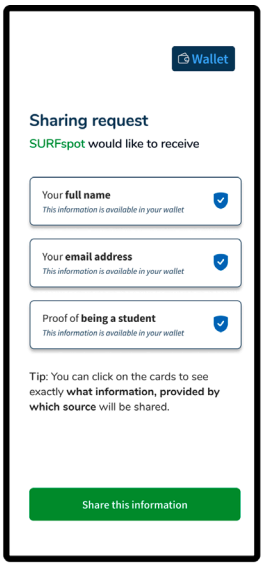


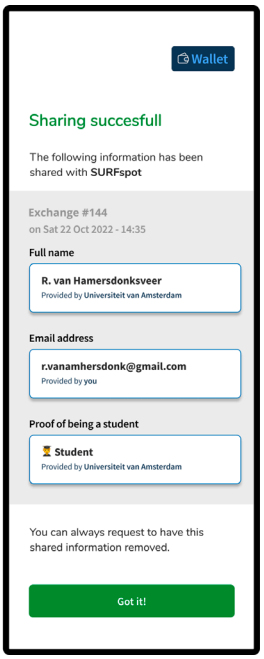






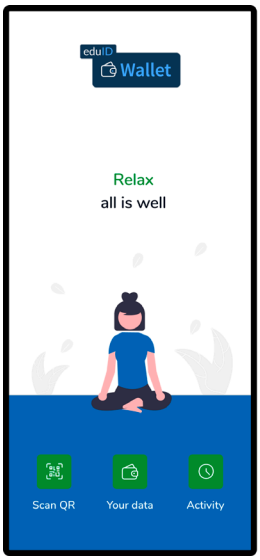


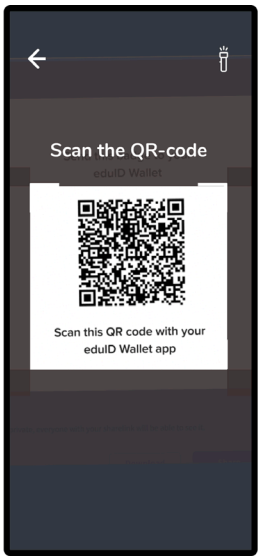


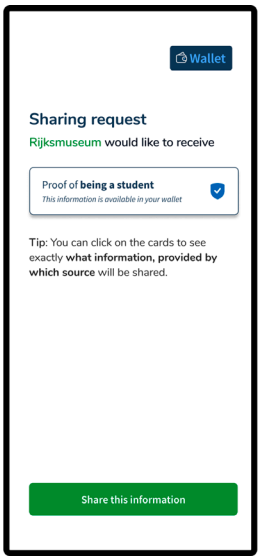


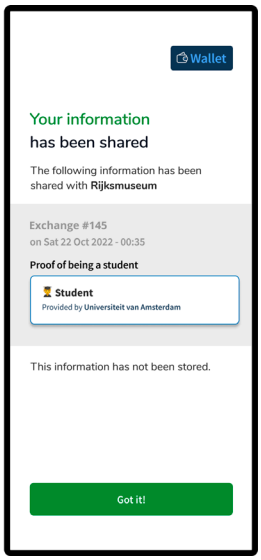
Attributen delen

Wanneer de wallet eenmaal is geactiveerd en de gegevens die nodig zijn voor het gebruiken van een dienst bekend zijn, wordt de flow gemakkelijk. In onderstaand geval wil de persoon bijvoorbeeld een kaartje met korting kopen voor het Rijksmuseum. Hij kan de QR-code scannen die op de balie staat. De persoon kan op dat moment de benodigde attributen delen.



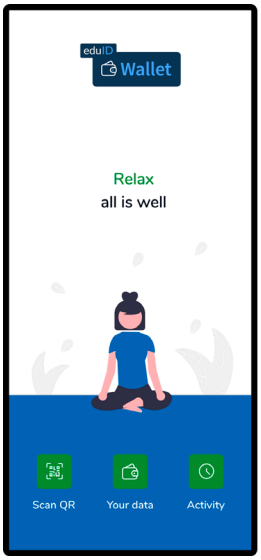


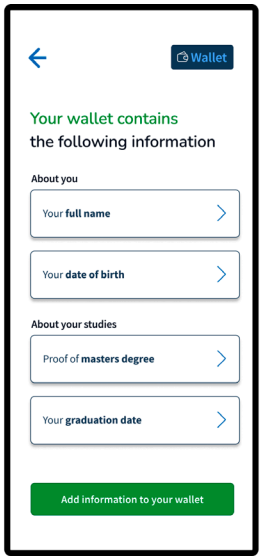


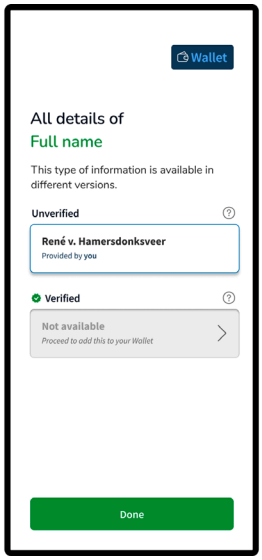


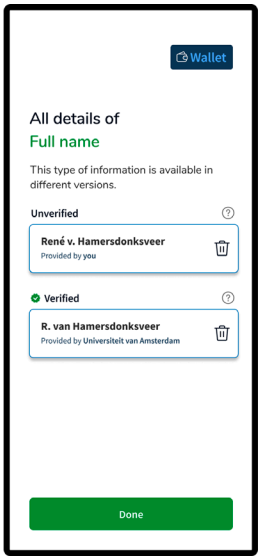
Bekijken en verwijderen inhoud

Inzicht hebben in data die in de wallet staat, en deze kunnen verwijderen zijn noodzakelijke basisfuncties. Deze kan de gebruiker bekijken via ‘Your data‘. Wanneer de persoon dit wil, kan deze hier ook zelf attributen toevoegen.



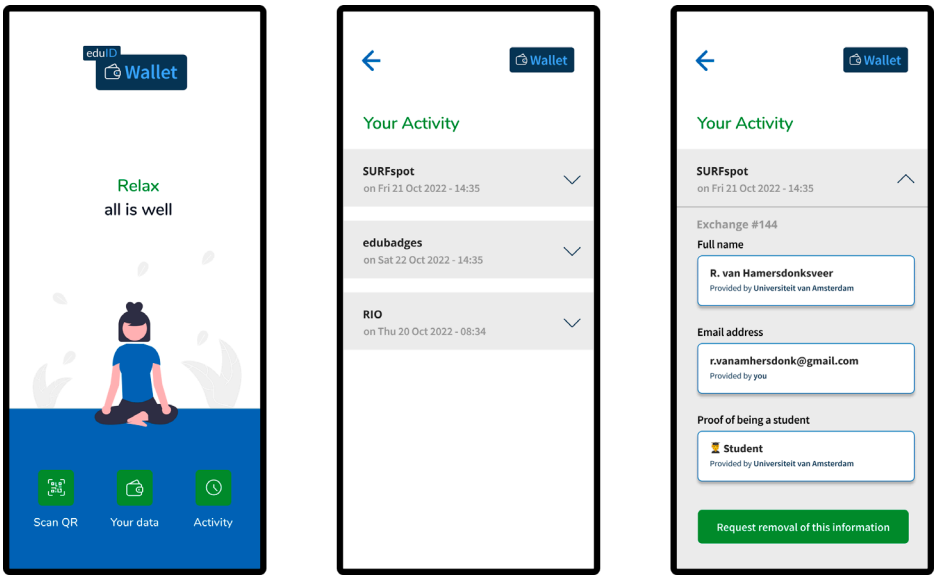






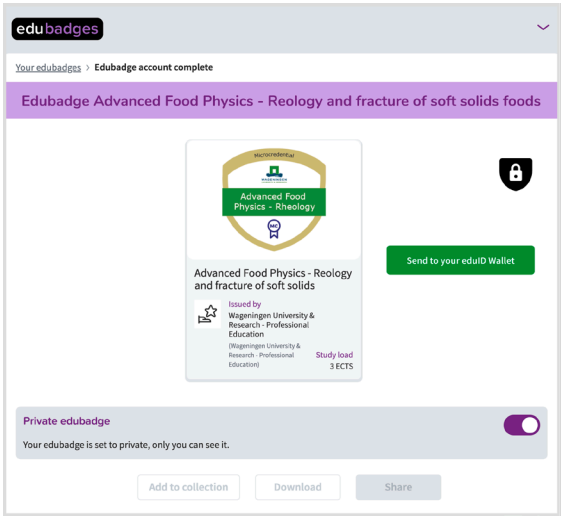
Bekijken activiteit

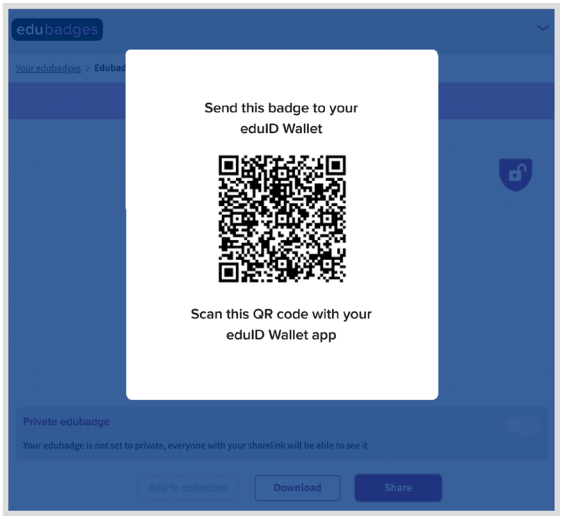
Onder ‘Activity’ staat een overzicht van alle transacties die hebben plaatsgevonden. In de ideale situatie kan de gebruiker hier ook een verzoek tot verwijderen van informatie bij de *verifier* starten. In hoeverre dit toepasselijk is, hangt af van het type inzageverzoek dat heeft plaatsgevonden.

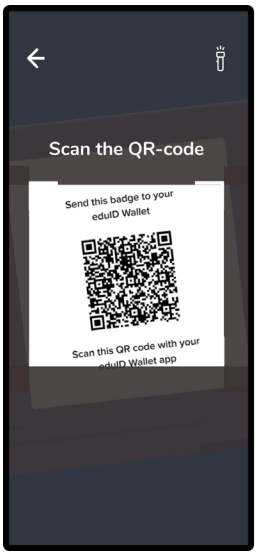


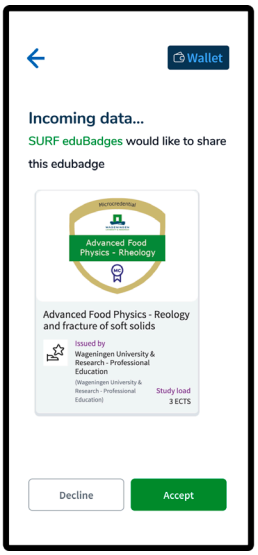
Ophalen edubadges

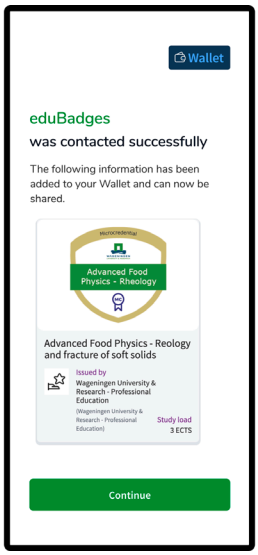
Het toevoegen van edubadges is een activiteit die de persoon zeer waarschijnlijk uit eigen beweging uitvoert. Bijvoorbeeld ter voorbereiding op een sollicitatie, het volgen van een vervolgopleiding of na het behalen van een certificaat.
Op de edubadges-website kan de persoon een QR-code scannen om de informatie op te halen met de wallet. Daarna kan de persoon met de wallet de behaalde edubadges ophalen en toevoegen aan de wallet. De persoon kan vervolgens de behaalde badges delen met de (potentiële) werkgever of instelling. Voor de uitdagingen rond het ophalen en uitvragen van edubadges, zie paragraaf 4.2 edubadges-integratie.

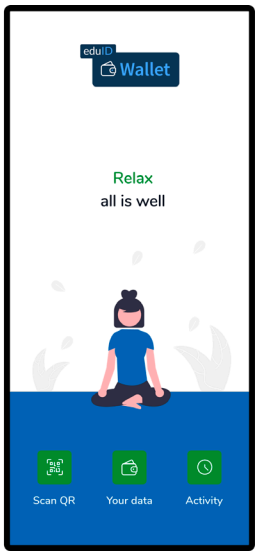












Auteurs
Niels van Dijk, technisch productmanager
Marlies Rikken, productmanager

Dit rapport is een uitgave van SURF
Mei 2023