Advies SURF inrichting
Nederlandse ESI-nummers

SURF
Datum: 3 mei 2021
Status: definitief
Versie: 1.0

Inhoudsopgave

Aanleiding tot deze notitie

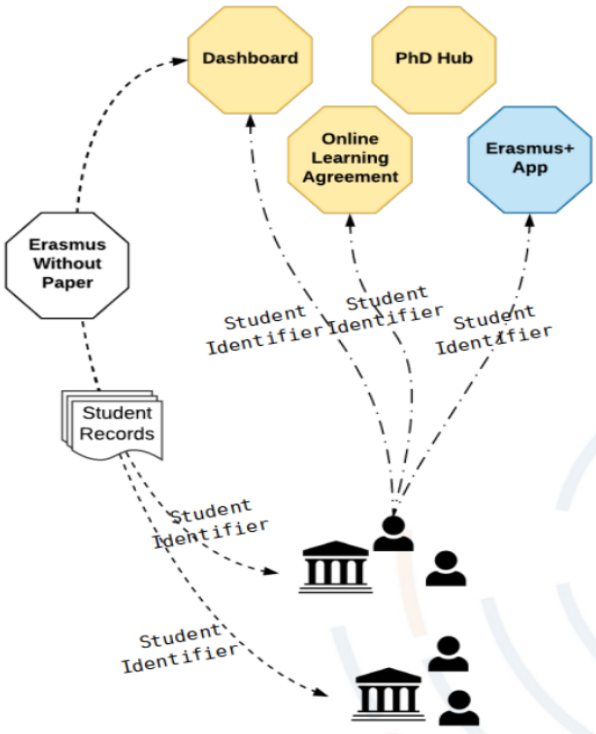
De European Student Identifier (ESI) is een digitale identificatie waarmee studenten zich op een unieke manier kunnen identificeren. Dit betekent dat studenten binnen Europa, waar ze ook studeren, met een en dezelfde identiteit toegang kunnen krijgen. Deze identificatie is nodig wanneer ze online toegang 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.

Nuffic is in Nederland als het Nationaal Agentschap Erasmus+ (NA) aangewezen. Dit betekent dat Nuffic in deze rol de Europese Commissie assisteren bij de uitvoer van het Erasmus+ programma in Nederland. De ESI wordt gerealiseerd als onderdeel van de digitalisering van de processen binnen Erasmus+ (2021-2027)[1]. Eind november heeft het Keten Regie Overleg HO NUFFIC de opdracht gegeven tot een verkenning tot invoering van de ESI en de impact hiervan op de keten. Vanaf augustus 2021 is het voor alle hoger onderwijsinstellingen die deelnemen aan de individuele mobiliteit binnen het Erasmus+ programma een verplichting de ESI mee te sturen om de digitale Erasmus+ diensten te benaderen. Voor Nederland betekent dit dat 58 instellingen (universiteiten en hogescholen) aan deze verplichting moeten voldoen.

Deze verplichting levert ook een technisch vraagstuk op. SURF werkt in opdracht van het hoger onderwijs en onderzoek, heeft kennis van en ervaring met (dit soort technische) vraagstukken rondom Identity & Access Management. Daarnaast heeft SURF technische voorzieningen die de ontsluiting van de ESI naar Europa zouden kunnen verzorgen. Vandaar dat SURF in voorliggende notitie Nuffic van advies voorziet over mogelijke alternatieven voor de implementatie.

[1] blz 26 en 44 Erasmus+ Programme Guide 2021
https://ec.europa.eu/programmes/erasmus-plus/resources/documents/erasmus-programme-guide-2021_en

In de onderstaande afbeelding is de toepassing van de European Student Identifier zichtbaar zoals die is vastgesteld in de architectuur[2] van het ESI-koppelpunt. Dit koppelpunt wordt de “MyAcademicID Proxy” genoemd. Omdat de ESI-architectuur is vastgesteld, geldt deze voor SURF als uitgangspunt bij de uitwerking van dit advies.



Wat is de uitdaging?

- Het inregelen van een technische oplossingen voor de ESI is benodigd voor enerzijds het genereren, administreren, beheren en delen van het identificerend nummer (‘de ESI’) voor studenten die deelnemen aan het Erasmus+ programma en anderzijds de uitwisseling van dit nummer vanuit de onderwijsinstelling met het Europese ESI-koppelpunt (de “MyAcademicID Proxy”).
- Er bestaan in Nederland nog geen ESI-nummers en ESI-specifieke infrastructuur om deze ESI-nummers uit te wisselen. Dit moet in augustus 2021[3] beschikbaar zijn.
- De ESI moet vanuit een Nederlandse onderwijsinstelling kunnen worden uitgewisseld met het Europese ESI-koppelpunt (de “MyAcademicID Proxy”).
- Er zijn 58 Nederlandse onderwijsinstellingen die deelnemen aan het Erasmus+ programma, onderdeel Individuele Mobiliteit, deze dienen daardoor een ESI te kunnen (gaan) leveren.
- Al deze Nederlandse onderwijsinstellingen moeten hier (mogelijk) individueel werk voor verrichten. Het is daarom verstandig te zoeken naar een oplossing met de minste impact op de onderwijsinstellingen.

[2] Details architectuur ESI: https://uni-foundation.eu/uploads/2020_MyAID_Blueprint_Architecture.pdf
[3] Zie slide 49 van de eindpresentatie MyAcademicID: https://drive.google.com/file/d/1brtodoCF3SmTexzIB4Yp-Qv3hs1tGJf

Kenmerken van de European Student Identifier

De definitie[4] van een ESI is: de European Student Identifier is wereldwijd uniek, persistent nummer dat protocol en datatransport neutraal is en niet-specifiek voor een bepaalde dienstverlener.

- Wereldwijd uniek: elke (Erasmus+) student moet uniek worden geïdentificeerd over organisatorische en nationale grenzen heen;
- Persistent: de identifier moet de student volgen terwijl hij / zij op uitwisseling is en mag niet wijzigen zolang dit nummer in gebruik is;
- Niet-specifiek: de identificatiecode moet dezelfde zijn voor alle diensten[5] die vanuit Erasmus+ worden geleverd: ieder van deze diensten herkent de student aan hetzelfde nummer;
- Protocol-neutraal: de identificatie mag niet van de waarde veranderen afhankelijk van het gebruikte technische protocol: het moet hetzelfde zijn ongeacht of bijvoorbeeld de technische standaard SAML of OpenID Connect wordt gebruikt;
- Neutraal gegevenstransport: de identificatie mag niet van waarde veranderen afhankelijk van hoe deze wordt getransporteerd. De studenten moeten bijvoorbeeld met dezelfde ID worden geïdentificeerd ongeacht of dit gebeurt via een federatieve authenticatie of een overdracht van resultaten direct tussen een Erasmus dienst en een onderwijsinstelling.

Kanttekeningen bij de European Student Identifier

De architectuur voor ESI is vastgesteld en daarmee uitgangspunt voor dit advies. Vanuit de privacybescherming van de student wil SURF een kanttekening plaatsen bij een van de kenmerken van de ESI.

Zo is bepaald dat de ESI *'niet-specifiek'* is. Dat betekent dat het identificatienummer van de student dezelfde moet zijn voor alle diensten die vanuit Erasmus+ worden geleverd. Dus ieder van deze diensten herkent de student aan hetzelfde identificatienummer.

In de huidige opzet worden op basis van het ESI de volgende diensten ontsloten: het Online Learning Agreement, Erasmus Without Paper, de European Student Card, de Erasmus+ Mobile App en de European PhD Hub. Het is onduidelijk of het bij deze diensten blijft. Het is niet uit te sluiten dat bij succes van deze oplossing meer diensten gebruik willen gaan maken van het ESI.

Door het toepassen van hetzelfde identificatienummer bij diverse diensten ontstaat de mogelijkheid gebruikers te volgen / profileren bij het gebruik van de diensten. De privacy van de gebruikers kan daardoor worden aangetast. Dit is een onwenselijke situatie, ook al zou dit profileren via een policy en regelgeving worden verboden, het is beter ook technische maatregelen te nemen dit te voorkomen.

[4] https://wiki.geant.org/display/SM/European+Student+Identifier
[5] Details van de diensten: zie Annex I 'e-services in MyAcademicID' (pagina 9) https://uni-foundation.eu/uploads/2020_MyAID_Blueprint_Architecture.pdf

SURF ziet graag dat de architectuur van de ESI op dit punt wordt aangepast. Dat betekent dat als uitgangspunt zou moeten worden opgenomen dat de ESI juist *wel* specifiek is (‘targeted’). Kortom alle diensten die zijn aangesloten op het ESI-koppelpunt (de “MyAcademicID Proxy”) krijgen een ander nummer. Daarbij hoort dan dat deze nummers enkel onder regie van de gebruiker (onderling) te relateren zijn. Bij diensten zoals SURFconext en eduID prevaleert de privacybescherming van de gebruiker en hanteert SURF dit principe.

Door de tijdsdruk op de invoer van de ESI ligt het niet voor de hand dat de architectuur op korte termijn wordt aangepast.

SURFconext

Studenten, onderzoekers en medewerkers maken bij hun dagelijkse werkzaamheden gebruik van veel verschillende clouddiensten en diensten van de eigen instelling. Het is onhandig en onveilig als ze voor elke dienst een account moeten aanmaken. De oplossing is federatief inloggen: gebruikers kunnen dan veilig, vertrouwd en gemakkelijk met hun instellingsaccount inloggen op aangesloten diensten. Om dat mogelijk te maken zijn koppelingen tussen instellingen en de verschillende clouddiensten noodzakelijk. SURFconext voorziet hierin door middel van een afsprakenstelsel en een technische voorziening (centrale gateway).

In het afsprakenstelsel zijn afspraken opgenomen waar zowel de instellingen (Identity Provider, IdP), dienstaanbieders (Service Providers, SP) als de federatie operator (SURF) zich aan moeten houden.Zowel instellingen als (cloud)diensten zijn (technisch) aangesloten op de centrale gateway (Hub) zodat voor elke partij maar 1 koppeling nodig is. Daartoe hebben deze diensten een overeenkomst gesloten met SURF.

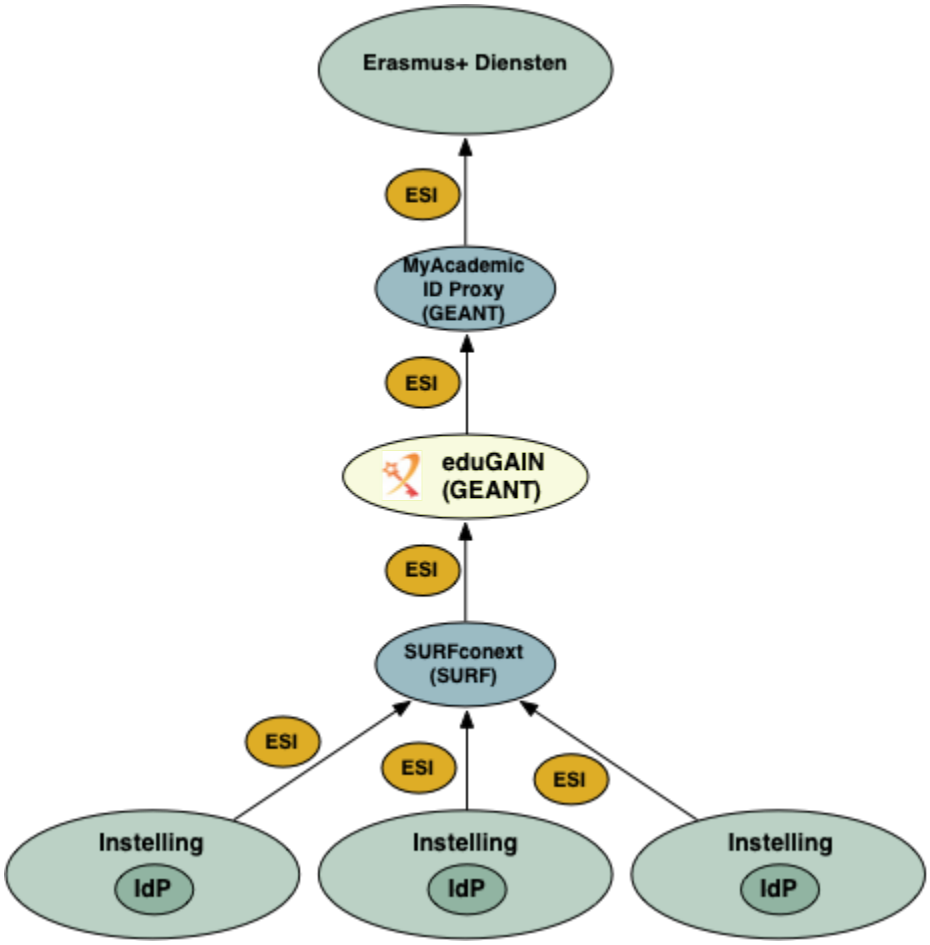
Via eduGAIN is SURFconext verbonden aan andere federaties over de hele wereld die ook deel uitmaken van het eduGAIN-netwerk. Op deze manier krijgen gebruikers gemakkelijk toegang tot clouddiensten uit de wereldwijde onderwijs- en onderzoeksgemeenschap en kunnen diensten vanuit SURFconext gemakkelijk en veilig toegankelijk worden gemaakt voor instellingen uit andere landen. Dit maakt samenwerking met studenten en onderzoekers uit het buitenland eenvoudiger.

De MyAcademicID Proxy is een dienst (Service Provider) in de eduGAIN federatie. Om gebruik te kunnen maken van de MyAcademicID Proxy, is vanuit de architectuur de voorkeursroute dat deelnemende instellingen via hun nationale federatie koppelen. Voor de Nederlandse context betekent dit een aansluiting via SURFconext.

Bij het federatieve inloggen worden een (minimale) set van gegevens over de gebruiker verstuurd. Dit zijn de zogeheten attributen. De ESI is één van de attributen die hierbij nodig is. De waarde van de ESI wordt weergeven in het attribuut `schacPersonalUniqueCode`[6]

[6] https://wiki.geant.org/display/SM/European+Student+Identifier

In de onderstaande afbeelding zijn de verschillende actoren te zien die een rol spelen bij de uitwisseling van de ESI vanuit de instelling met de Erasmus+ diensten.



Uitwerking in varianten

Bij uitwerken van de varianten is het gebruik van SURFconext als uitgangspunt genomen. Deze infrastructuur voor de uitwisseling en transport van attributen zoals ESI biedt grote voordelen: het levert tijdwinst op, voorkomt werk om instellingen technisch aan te sluiten en daarmee kosten. De tijdwinst die het gebruik van SURFconext als infrastructuur oplevert, is relevant in verband met de uitdaging dat in augustus 2021[7] de ESI-nummers en ESI-specifieke infrastructuur om deze ESI-nummers uit te wisselen beschikbaar moeten zijn.

Wanneer SURFconext wordt gebruikt gaat het om nog slechts een paar instellingen waar wat meer aandacht moet komen om de ontsluiting en het transport van een ESI naar de MyAcademicID Proxy mogelijk te maken. Voor het overgrote deel van de onderwijsinstellingen wordt via SURFconext de ontsluiting en het transport van een ESI naar de MyAcademicID Proxy al gefaciliteerd. Daarmee is een belangrijk deel van het vraagstuk opgelost.

Er zijn 58 Nederlandse onderwijsinstellingen die deelnemen aan het Erasmus+ programma, onderdeel individuele mobiliteit, daarvan:

- 50 instellingen zijn volwaardig lid van SURF en aangesloten op de technische voorzieningen van SURFconext en gekoppeld aan eduGAIN. Deze instellingen zijn daarmee in de basis voorbereid voor het ontsluiten en transporteren van een ESI naar de MyAcademicID Proxy.
- 1 instelling is volwaardig lid van SURF en aangesloten op de technische voorzieningen van SURFconext, deze instelling is echter niet gekoppeld aan eduGAIN.
- 3 instellingen zijn geen lid van SURF, maar zijn als non-member in de rol van identiteitsverstrekker (IdP) aangesloten op de technische voorzieningen van SURFconext. Deze instellingen zijn niet gekoppeld aan eduGAIN.
- 4 instellingen zijn geen lid van SURF en hebben geen technische aansluiting op de voorzieningen van SURFconext.

Er zijn ook oplossingsvarianten mogelijk zonder dat SURFconext wordt toegepast. Deze zijn buiten beschouwing gelaten omdat ze meer werk, inspanning en kosten tot gevolg hebben. Bovendien is de tijd krap om 58 instellingen voor augustus 2021 via een andere technische oplossing dan SURFconext te koppelen met de MyAcademicID Proxy.

Bij het samenstellen van het unieke nummer (de ESI) zijn er twee mogelijkheden:

- Optie 1: de ESI baseren op een uniek kenmerk dat de onderwijsinstelling beheert of verwerkt (bv studentnummer of Studielinknummer) en dit unieke deel ook zichtbaar te maken in de ESI. Deze optie is toegepast bij de uitwerking in variant 1,2 en 3.
- Optie 2: de ESI baseren op een uniek kenmerk dat als afgeleide wordt gemaakt van een uniek kenmerk dat de onderwijsinstelling beheert of verwerkt (bv studentnummer, Studielinknummer of een eduID-nummer) waardoor er een ontkoppeling is tussen beide nummers met als positief resultaat meer privacybescherming voor de student. Centraal kan SURF het instellingsspecifieke deel van de ESI (het kenmerkende nummer voor de

[7] Zie slide 49 van de eindpresentatie MyAcademicID: https://drive.google.com/file/d/1brtodoCF3SmTexzIB4Yp-Qv3hs1tGJf_

student) omvormen tot iets dat voldoet de eisen van de ESI. Deze optie is toegepast bij de uitwerking in variant 4 en 5.

Varianten

SURF ziet de volgende varianten als mogelijke inrichtingsvormen voor de Nederlandse inrichting voor ESI met toepassing van SURFconext.

- Variant 1: Instelling genereert ESI op basis van een lokaal studentnummer
  Instellingen genereren zelf een ESI en sturen dit tijdens authenticatie aan SURF. SURF geeft dit ESI onveranderd door.

- Variant 2: SURF genereert ESI op basis van een lokaal studentnummer
  SURF stelt de ESI samen op basis van bestaande informatie (studentnummer, naam van de instelling) die een instelling nu al stuurt tijdens authenticatie.

- Variant 3: SURF genereert ESI op basis van het Studielinknummer
  SURF stelt de ESI samen op basis van bestaande informatie en het Studielinknummer, dat voor dit doel extra wordt doorgegeven tijdens authenticatie.

- Variant 4: Toepassing van eduID via SURFconext voor ESI
  SURF genereert de ESI op basis van een uniek eduID-nummer specifiek voor ESI, nadat de student inlogt met zijn instellingsaccount via SURFconext.

- Variant 5: Toepassing van eduID voor ESI
  SURF genereert de ESI op basis van een uniek eduID-nummer specifiek voor ESI, nadat de student inlogt met zijn eduID.

Een gedetailleerdere beschrijving van deze varianten is in de bijlagen opgenomen.

Vergelijk varianten

Met als doel de varianten onderling vergelijkbaar te maken zijn bij de uitwerking van de varianten een aantal aspecten beschreven. Deze zijn onderstaand kort toegelicht.

Privacyvriendelijk

Het wereldwijd gebruiken van hetzelfde unieke nummer voor het identificeren van een persoon zorgt voor risico's van de privacy van deze persoon. Er ontstaat immers een eenvoudige manier om gegevens aan elkaar te relateren (koppelen van bestanden). Voor ESI is besloten dat er een globaal uniek nummer moet worden toegepast. De privacy van de gebruiker zou (wat) beschermd kunnen worden door de Nederlandse studentnummers te ontkoppelen van de ESI-nummers, bijvoorbeeld door het gebruiken van een identifier die alleen voor ESI wordt gebruikt.

Eenvoud werkzaamheden instelling

Hoeveel moet er aan het Student Informatie Systeem (SIS) en Identity Management Systeem (IdM) worden aangepast om deze oplossing mogelijk te maken. Het hergebruiken van een bestaand studentnummer heeft minder impact op de bestaande processen dan het gebruiken en vertalen van een nieuwe identifier of zelfs het introduceren van een nieuwe identifier in het SIS specifiek voor ESI. Het aanpassen aan bijvoorbeeld een ADFS, om een nieuw attribuut zoals de ESI te genereren, is relatief eenvoudig. Het aanpassen van een SIS voor het opslaan van nieuwe identifier is daarentegen (waarschijnlijk) lastiger.

Eenvoud werkzaamheden SURF

Hoeveel moet er aan de technische voorzieningen van SURF worden aangepast om deze oplossing mogelijk te maken en structureel beschikbaar te stellen/houden. Minder aanpassingen aan de SURF voorzieningen hebben een positief effect op de (structurele) kosten van de oplossing en beheersbaarheid van de centrale componenten bij SURF.

Snel realiseren

Complexe aanpassingen aan SIS en andere informatiesystemen, zoals het introduceren van een nieuwe identifier in het SIS specifiek voor ESI, kosten tijd bij de instellingen. Enkele varianten kunnen door SURF centraal voor alle instellingen geregeld worden en kosten daardoor minder tijd van de instellingen.

Mate waarin de oplossing standaard is

Het hergebruiken van bestaande en standaard oplossingen zorgt voor een kortere doorlooptijd, en een betere oplossing (beheerbaar, onderhoudbaar e.d.) op de lange termijn.

Schaalbaarheid

Is de variant eenvoudig uit te breiden naar meer deelnemers. Zitten er grenzen aan het aantal studenten, instellingen of uitwisselingen?

Toekomstvastheid

Is de variant toekomstvast of toekomstvast te maken.

Score varianten

In onderstaande tabel is per variant de score opgenomen van de aspecten die in de voorgaande paragraaf zijn beschreven. De scores dragen positief (+) of negatief (-) bij aan de waardering/beoordeling van de variant.

Hoe zwaar een criterium doorwerkt (bijvoorbeeld de mate van privacyvriendelijkheid van de oplossing) is van invloed op de totaalbeoordeling van de varianten. Gekozen is alle criteria even zwaar te laten wegen bij het bepalen van de meest gunstige variant. Dat betekent dat Variant 1 de beste oplossing is voor het Nederlandse hoger onderwijs.

Onderwerp	Variant 1	Variant 2	Variant 3	Variant 4	Variant 5
Privacyvriendelijk	--	--	--	+	+
Eenvoud werkzaamheden instelling	+	+	-	+	+
Eenvoud werkzaamheden SURF	++	+	+	--	--
Snel realiseren	-	+	+	--	--
Mate waarin oplossing standaard is	+	+	+	-	-
Schaalbaarheid	+	+	+	+	+
Toekomstvastheid	++	+	+	+	++

Advies

Dit advies heeft betrekking op het genereren van het ESI-nummer en het transporteren van het ESI-nummer naar het Europese ESI-koppelpunt. Hierbij is het gebruik van SURFconext als uitgangspunt genomen. De tijdwinst die het gebruik van SURFconext als infrastructuur oplevert, is relevant in verband met de uitdaging dat in augustus 2021[8] de ESI-nummers en ESI-specifieke infrastructuur om deze ESI-nummers uit te wisselen beschikbaar moeten zijn. Naast het genereren van het ESI-nummer en het transporteren van het ESI-nummer zullen er mogelijk ook aanpassingen benodigd zijn om andere processen te ondersteunen die van belang zijn voor bijvoorbeeld Erasmus Without Papers (EWP) en waar ESI ook een rol bij speelt. Deze zijn niet in dit advies beschouwd.

Alles overziend is SURF van mening dat variant 1, waarbij de instelling de ESI genereert op basis van een lokaal studentnummer, de beste oplossing is voor het Nederlandse hoger onderwijs op de korte termijn, zeker gezien de hoge tijdsdruk die op dit traject staat in de aanloop naar augustus 2021.

- Bij variant 1 hebben instellingen de meeste controle over welk (bron-) nummer zij zelf gebruiken voor het samenstellen van de ESI. Dit kan ieder (administratief) nummer in een SIS zijn. Dit is anders dan variant 2 en 3. Variant 4 en 5 werken volgens een ander mechanisme.
- In variant 1 is het nummer gegarandeerd bekend in de bronsystemen van de instelling, wat behulpzaam is, wanneer het nummer wordt terug gecommuniceerd naar de informatiesystemen van de instelling.
- Variant 1 is het meest eenvoudige model: er is geen inhoudelijke rol en daarmee verantwoordelijkheid voor SURF bij het genereren van een ESI. Deze variant voorkomt centrale bedrijfslogica voor het genereren de ESI in SURFconext, logica die daar (eigenlijk) niet thuishoort. In variant 1 is er minder complexiteit binnen de keten dan bij de overige varianten.
- Het ESI-nummer is (‘by design’) globaal uniek en daarmee privacy-onvriendelijk. Er is echter wel doelbinding gedefinieerd voor het gebruik van het ESI-nummer voor enkel de vastgestelde diensten[9]. Varianten 4 en 5 verbeteren de privacy van de gebruiker (door het ontkoppelen van nummers) als is de meerwaarde beperkt doordat het ESI-nummer zelf globaal uniek is/blijft. Mogelijk dat in de toekomst de varianten 4 en 5 relevant worden wanneer de architectuur van de ESI wordt gewijzigd en de ESI-nummers niet langer globaal uniek zijn.
- Voor variant 1 moeten instellingen wel een nieuw attribuut maken en toevoegen aan de authenticatie. Dit is echter een relatief standaard handeling. Variant 2 ontzorgt de instelling meer op dit punt door hergebruik van bestaande attributen.

[8] Zie slide 49 van de eindpresentatie MyAcademicID: https://drive.google.com/file/d/1brtodoCF3SmTexzIB4Yp-Qv3hs1tGJf_
[9] Het Online Learning Agreement, Erasmus Without Paper, de European Student Card, de Erasmus+ Mobile App en de European PhD Hub.

SURF geeft daarnaast de volgende overige adviezen mee:

- Hanteer in Nederland als opbouw van het ESI-nummer binnen het attribuut schacPersonalUniqueCode de waarde:
  `urn:schac:personalUniqueCode:int:esi:{instelling.nl}:{lokaalnummer}`
  Vervang hierin `{instelling.nl}` door de met SURFconext afgestemde `schacHomeOrganization` en vervang `{lokaalnummer}` door een uniek nummer van de student, bijvoorbeeld het studentnummer.
  Dit levert bijvoorbeeld als ESI op:
  - `urn:schac:personalUniqueCode:int:esi:uva.nl:123456`
  - `urn:schac:personalUniqueCode:int:esi:avans.nl:345678`
- Stem dit advies af met het Architectenberaad HO zodat het advies ook in de bredere (onderwijs-) context kan worden beoordeeld en (eventueel) verankerd.
- Wanneer de architectuur van ESI op termijn zou veranderen, evalueer dan of andere van de beschreven varianten meer relevant worden. Dit speelt in het bijzonder wanneer wordt losgelaten dat ESI ‘niet-specifiek’ is (en dus privacy-onvriendelijk).
- Zodra er meer diensten achter de ESI-proxy komen, evalueer dan of dit extra maatregelen vereist om de privacy van de gebruiker te waarborgen.
- Laat een DPIA opstellen die de gehele ESI-keten beschouwt (zie schema op pagina 6 met ten minste de stakeholders: onderwijsinstelling, SURFconext, eduGAIN, ESI-proxy, diensten)
- Betrek SURF en instellingen nauw bij het vervolgtraject

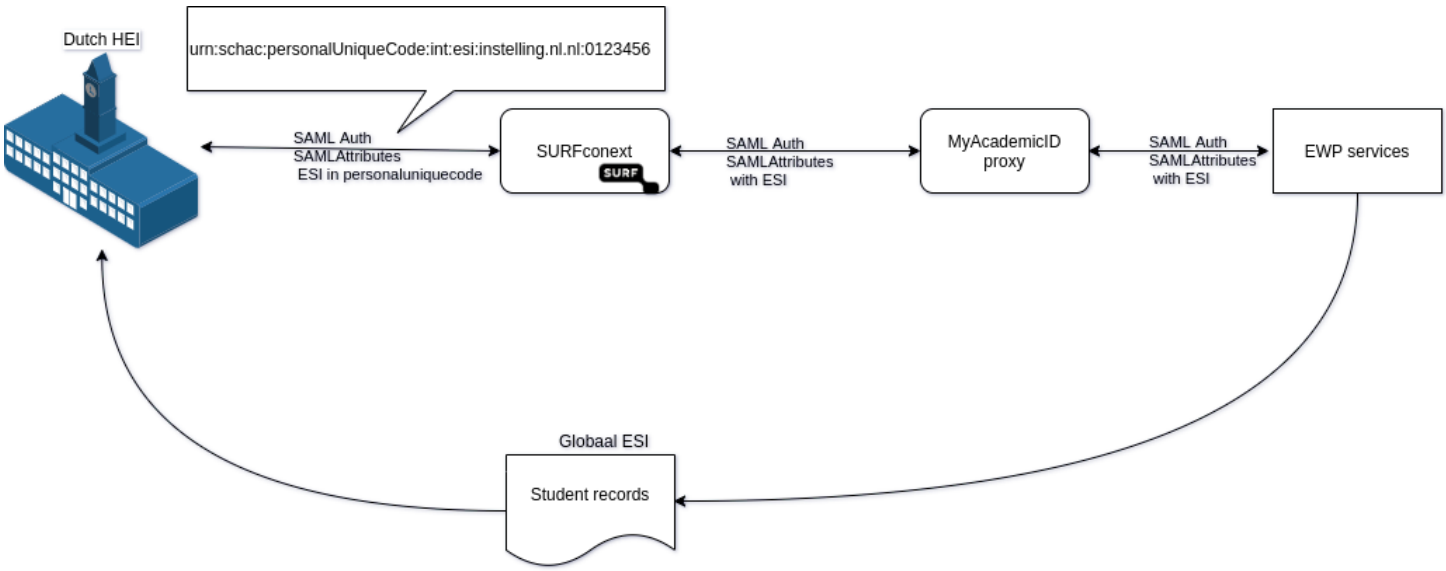
Tot slot

Het ESI-vraagstuk is breder dan alleen het genereren van het ESI-nummer en het transporteren van het ESI-nummer. Er zullen mogelijk ook aanpassingen benodigd zijn om andere processen te ondersteunen. Dit vraagt om coördinatie op alle betrokken onderdelen in de totale keten. SURF is zeer bereid tot nadere toelichting en werkt graag mee aan de vervolgstappen.

Bijlagen

Variant 1: Instelling genereert ESI op basis van een lokaal studentnummer

De instelling genereert een ESI. Dit ESI wordt bij het inloggen doorgegeven aan de EWP-services.



Opmaak:
`urn:schac:personalUniqueCode:int:esi:{schacHomeOrganization}:{lokaal studentnummer}`

Voordelen:

- Nummer zit al in administratie van de instelling
- Eenvoudige SIS implementatie van ESI-nummer, geen tot minimale aanpassing nodig
- Minimale aanpassingen in de (SAML)-koppeling instelling
- Regulier uitgifte en beheerproces van nummer
- Snelheid realisatie afhankelijk van instellings-IdP beheer

Nadelen:

- Niet privacyvriendelijk
- Kleine (configuratie-) aanpassing IdP instelling
- Kans op hergebruik/wildgroei van het ESI-nummer voor andere diensten achter/via ESI, wat een negatieve impact heeft op de privacy
- Externe diensten worden afhankelijk van een intern nummer

Privacy aspecten

- Aandachtspunt: persoonsgebonden nummer wordt gedeeld buiten de instelling/land

Technische aspecten

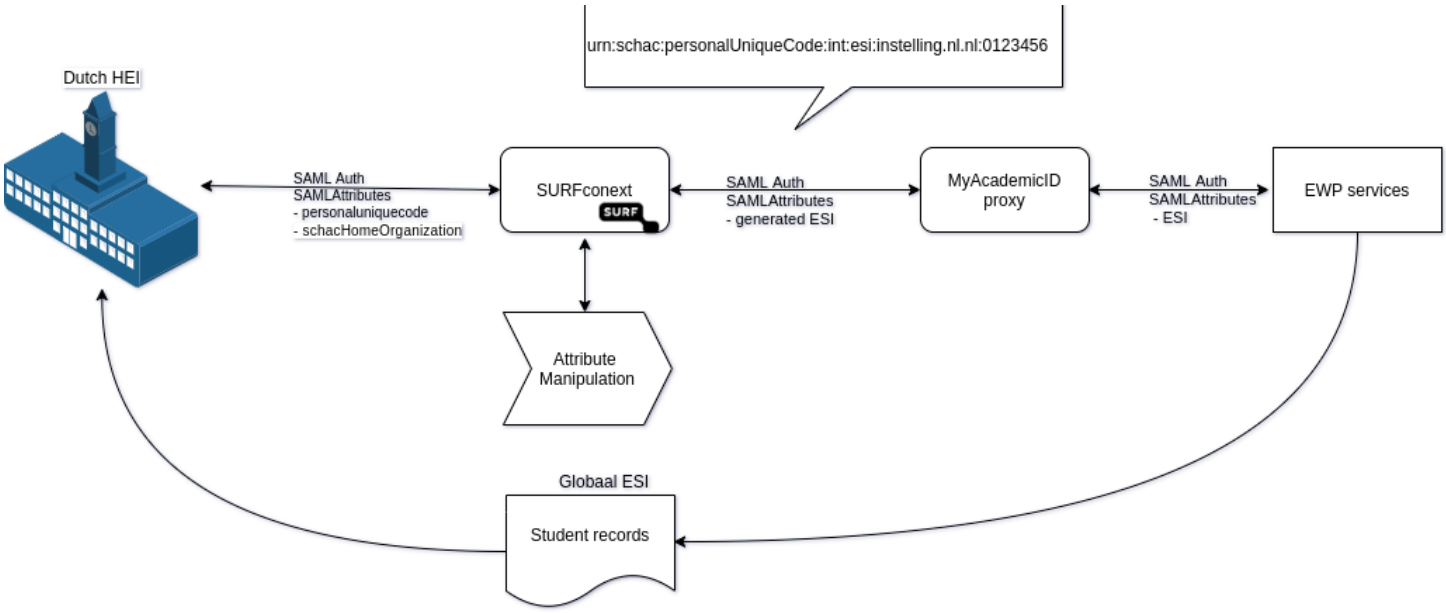
- Eenvoudige implementatie, extra waarde in SAML attribuut vanuit instelling
- SURFconext geeft het attribuut transparant van de in de instellingen (IdP) door aan de MyAcademicID Proxy (SP)

Verdeling inspanningen

- SURF: Reguliere dienstverlening
- Per instelling: Extra waarde maken in IdP systeem
- Nieuwe waarde doorgeven in personalUniqueCode attribuut in de koppeling naar SURFconext
- De instelling moet in het SIS de ESI relateren aan het intern bekende studentnummer

Variant 2: SURF genereert ESI op basis van een lokaal studentnummer

SURF genereert de ESI op basis van de `schacHomeOrganization` en het bestaande lokale studentennummer bij een instelling, de instelling levert hiertoe enkel de `personalUniqueCode`.



Opmaak:
`urn:schac:personalUniqueCode:int:esi:{schacHomeOrganization}:{lokaal studentnummer}`

Voordelen:

- Nummer zit al in administratie van de instelling
- Eenvoudige SIS implementatie, geen aanpassingen nodig m.b.t. ESI-nummer
- Minimale aanpassingen in de (SAML)-koppeling instelling
- Regulier uitgifte en beheerproces van nummer
- Snel te realiseren

Nadelen:

- Niet privacyvriendelijk
- Kans op hergebruik/wildgroei van het ESI-nummer voor andere diensten achter/via ESI, wat een negatieve impact op de privacy heeft
-
- Externe diensten worden afhankelijk van een intern nummer

Privacy aspecten

- Aandachtspunt: persoonsgebonden nummer wordt gedeeld buiten de instelling/land

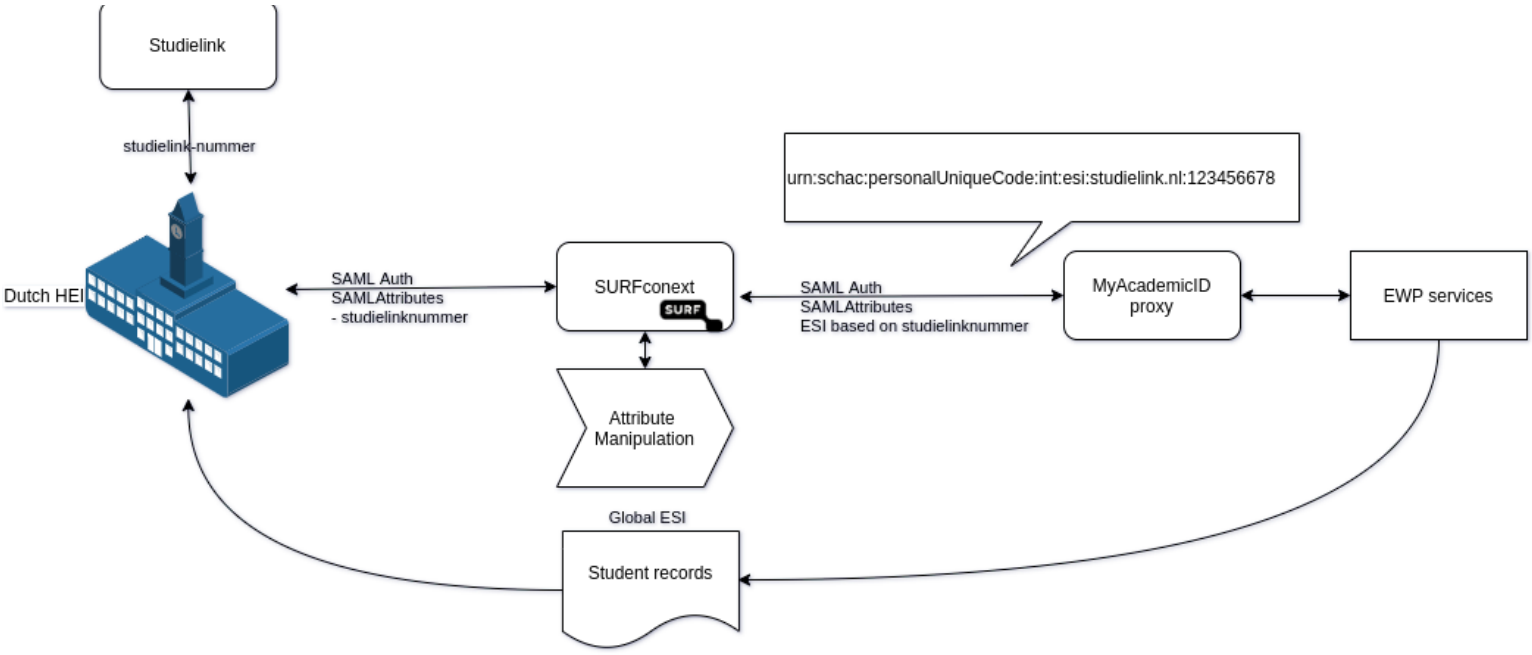
Technische aspecten

- Instelling levert personalUniqueCode in SAML attribuut
- SURFconext ‘bouwt’ de ESI uit het `schacHomeOrganization` attribuut en `personalUniqueCode` attribuut

Verdeling inspanningen

- SURF: inrichten en onderhouden AttributeManipulation om een ESI te genereren.
- Per instelling: twee standaard attributen leveren (als dat nog niet gebeurt), en een koppeling maken met de ESI-dienst via SURFconext. Dit is regulier beheer voor een IdP.
- De instelling moet in het SIS de ESI relateren aan het intern bekende studentnummer

Variant 3: SURF genereert ESI op basis van het Studielinknummer



Opmaak:
`urn:schac:personalUniqueCode:int:esi:studielink.nl:{Studielinknummer}`

Voordelen:

- Nummer zit al in administratie van de instelling
- Geen aanpassingen in het SIS m.b.t. ESI-nummer
- Minimale aanpassingen in de (SAML)-koppeling (extra attribuut doorgeven)
- Regulier uitgifte en beheerproces van nummer via Studielink

Nadelen:

- Niet privacyvriendelijk
- Kans op hergebruik/wildgroei van het ESI-nummer voor andere diensten achter/via ESI
-
- Aandachtspunt: zijn Studielinknummers wel in IAM-systemen -die gekoppeld zijn aan SURFconext- beschikbaar, of alleen in het SIS?

Privacy aspecten:

- Aandachtspunt: persoonsgebonden nummer wordt gedeeld buiten de instelling/land

- Aandachtspunt: Mag het Studielinknummer voor dit doeleind worden toegepast (wat is de juridische status en daarmee de doelbinding van een Studielinknummer)?

Technische aspecten:

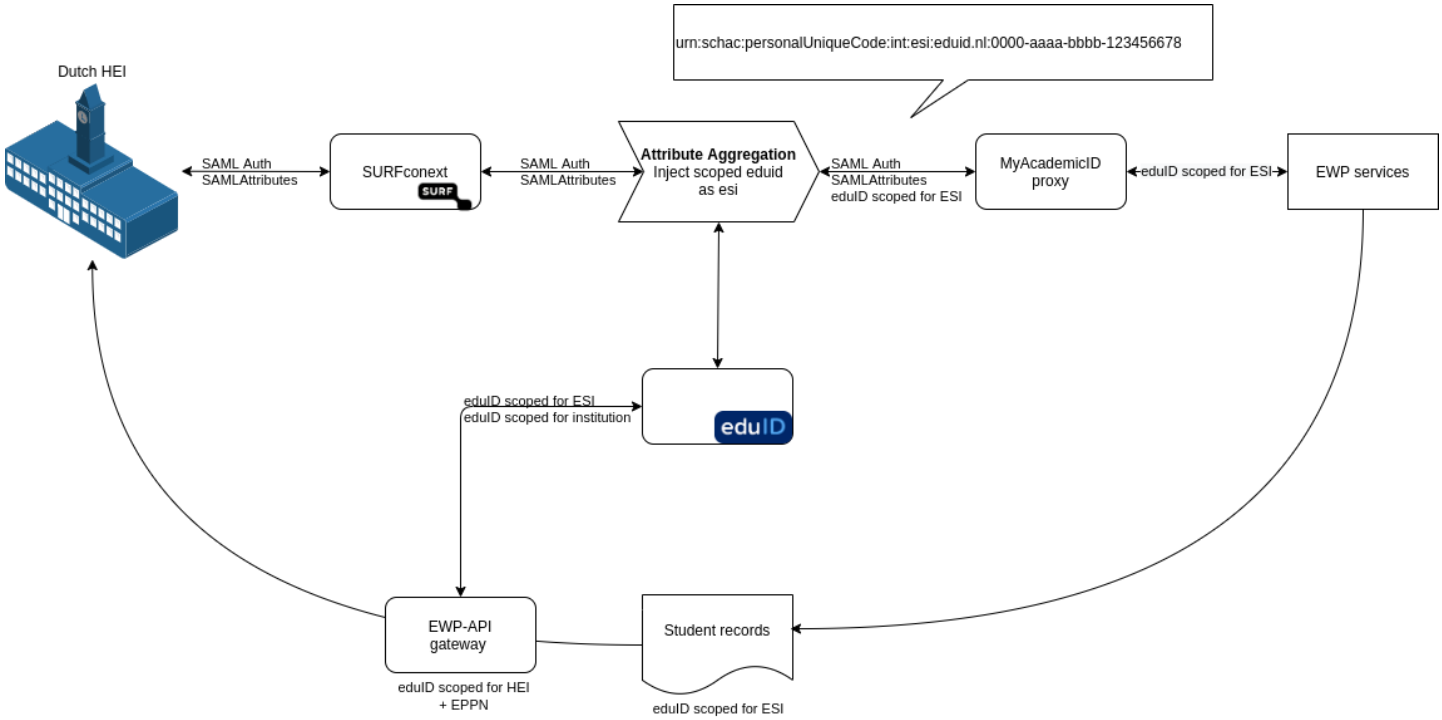
- Eenvoudige implementatie, SAML attribuut
- Instelling levert het attribuut ‘Studielinknummer’
- SURFconext ‘bouwt’ de ESI uit attribuut ‘Studielinknummer’

Verdeling inspanning:

- SURF: inrichten AttributeManipulation om een ESI te genereren.
- Per instelling: een extra attribuut (‘Studielinknummer’) leveren en een koppeling maken met de ESI-dienst via SURFconext. Dit laatste is regulier beheer voor een IdP.
- De instelling moet in het SIS de ESI relateren aan het intern bekende Studielinknummer

Variant 4: Toepassing van eduID via SURFconext voor ESI

Tijdens de SAML authenticatie wordt door SURF een eduID gegenereerd speciaal voor MyAcademicID. Deze wordt opgemaakt als een ESI. In een gateway wordt het eduID voor MyAcademicID omgezet naar een eduID speciaal voor de instelling.



Opmaak:
`urn:schac:personalUniqueCode:int:esi:eduid.nl:{MyAcademicID eduID pseudoniem}`

Voordelen:

- Nummer blijft bestaan, ook na beëindiging studie of wisselen studie
- Geen herbruikbare identifier
- Centrale EWP-API gateway abstraheert complexiteit van identifiers.
- Oplossing positief draagt bij aan privacy van gebruiker
- Oplossing vraagt beperkte aanpassingen aan het SIS

Nadelen:

- Kans op het genereren van een eduID voordat een student bekend is in eduID (door onder water aanmaken van een eduID dat niet gekoppeld is aan een instellingsaccount)
- Oplossing vraagt ontwikkel inspanning van SURF voor het realiseren van een aantal technische componenten en het structurele beheer daarvan (zoals de EWP-API gateway), met als doel verbeteren de privacy van de gebruiker (door het ontkoppelen van nummers) de meerwaarde is echter beperkt doordat de ESI zelf globaal uniek is/blijft

Privacy aspecten:

- Nummer is speciaal voor de ESI-dienst, minder kans op linkability
- De ESI is niet direct herleidbaar tot een persoon

Technische aspecten:

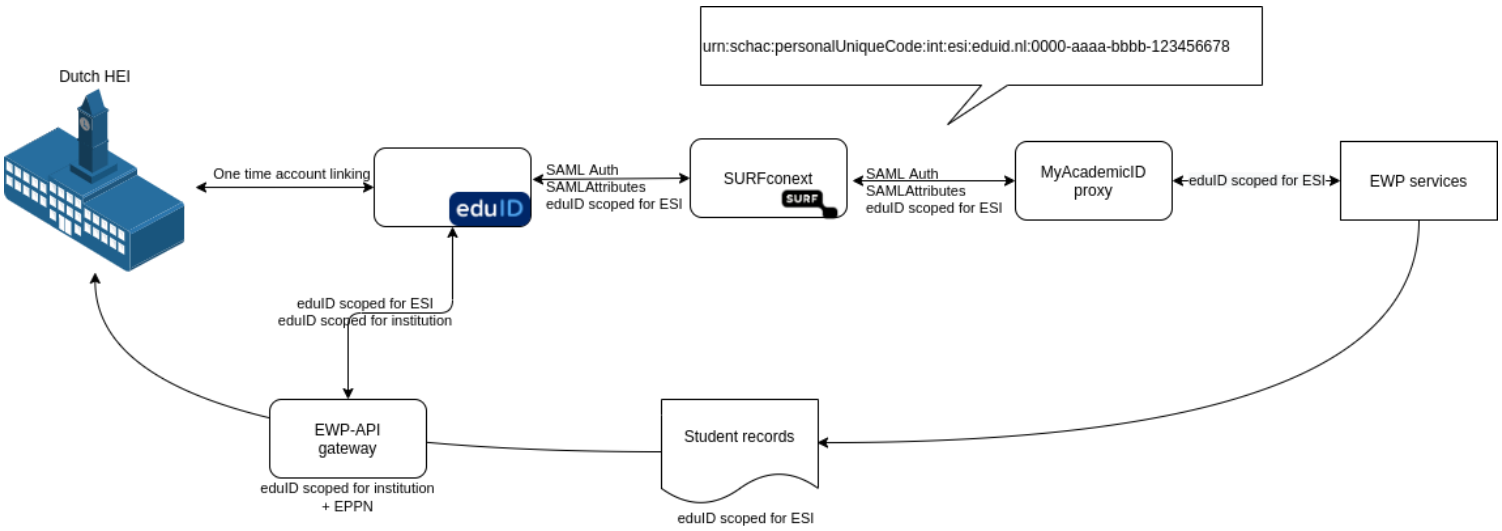
- De ESI is gekoppeld aan de deelnemende instellingen via SURFconext
- Instellingen leveren authenticatie en realiseren een koppeling tussen lokaal student account (via het EPPN) en een eduID (eduID account-linking)
- SURFconext ‘bouwt’ de ESI uit de specifieke eduID identifier
- Eventueel API-gateway voor translatie nummers
- Aandachtspunt: Wat als de instelling de online learning agreement al klaar zet voordat de student ingelogd is?

Verdeling inspanning:

- SURF: inrichten AttributeManipulation om een ESI te genereren en centrale EWP-API gateway ontwikkelen.
- Per instelling: een koppeling maken met de ESI-dienst via SURFconext. Dit is regulier beheer voor een IdP. Daarnaast een koppeling maken met eduID account-linking.

Variant 5: Toepassing van eduID voor ESI

De student logt in via eduID, en koppelt hier een instelling. Tijdens de eduID authenticatie wordt door SURF een eduID gegenereerd uniek voor MyAcademicID. Deze wordt opgemaakt als een ESI. In een gateway wordt het eduID voor MyAcademicID omgezet naar een eduID speciaal voor de instelling.



Opmaak:
`urn:schac:personalUniqueCode:int:esi:eduid.nl:<MyAcademicID eduID pseudoniem>`

Voordelen:

- Nummer blijft bestaan, ook na beëindiging of wisselen studie
- Geen herbruikbare identifier
- Centrale EWP-API gateway abstraheert complexiteit van identifiers.
- Oplossing positief draagt bij aan privacy van gebruiker
- Oplossing vraagt beperkte aanpassingen aan het SIS

Nadelen:

- Aanpassing in SIS voor het vertalen van de MyAcademicID-eduID naar de lokale eduID identifier. Dit kan beter in een centrale gateway worden opgelost.
- Oplossing vraagt ontwikkel inspanning van SURF voor het realiseren van een aantal technische componenten en het structurele beheer daarvan (zoals de EWP-API gateway), met als doel verbeteren de privacy van de gebruiker (door het ontkoppelen van nummers) de meerwaarde is echter beperkt doordat de ESI zelf globaal uniek is/blijft

Privacy aspecten:

- Nummer is uniek en speciaal voor de ESI-dienst, minder kans op linkability
- De ESI is niet direct herleidbaar tot een persoon

Technische aspecten:

- De ESI is gekoppeld aan eduID via SURFconext
- Instellingen leveren enkel eenmalige authenticatie om het account te koppelen
- SURFconext ‘bouwt’ de ESI uit de specifieke eduID identifier
- Eventueel API-gateway voor translatie nummers

Verdeling inspanning:

- SURF: inrichten AttributeManipulation (en optioneel: gateway) om een ESI te genereren.
- Per instelling: de koppeling met eduID account-linking inschakelen