

Generieke IDM-connector

Project ontvlechting IAM – Universiteit Utrecht

Auteur	Albert-Jan Stevens
Contact	A.J.W.Stevens@uu.nl
Versie	1.6

Inhoudsopgave

1	Inleiding.....	3
2	Overzicht van de oplossing.....	4
3	Datamodel.....	5
3.1	Attributen Identity.....	6
3.2	Attributen Person.....	6
3.3	Definitie Engagement (verbintenis).....	7
3.3.1	Configuratie van graceBefore en graceAfter.....	7
3.4	Definitie Trait.....	8
3.5	Definitie Notificatie.....	8
3.6	Definitie Metadata.....	8
4	Interactie overzicht.....	10
4.1	Authenticatie en beveiliging.....	10
4.2	Notificaties.....	10
4.3	Read Identity.....	11
4.4	Updaten van de Bron.....	11
4.5	notifyChange.....	13
4.6	getIdentity.....	13
4.7	getMetaData.....	13
4.8	updateSolisId / updateEmail.....	14
5	SAP.....	15
5.1	Middleware en OData.....	16
1.1	Traits en grace-waarden.....	16
5.2	Metadata objecten.....	17
5.3	Toevoegen business rule.....	17
6	Osiris.....	18
6.1	Traits en grace-waarden.....	19
6.2	Metadata-objecten.....	19
6.3	Processen en berichten.....	20

1 Inleiding

Dit document levert een voorstel om gestandaardiseerd berichten af te leveren aan het Universitaire Identity & Access Management systeem vanuit de bronregistraties. Deze standaard sorteert voor op het inzetten van een integratieplatform en is dan ook zo ontworpen dat de berichten nu, of later, door het integratieplatform afgeleverd kunnen worden.

Dit voorstel is onderdeel van het project 'Ontvlechting IAM'. Het doel van dit project is om de administraties en het IDM-systeem lossier te koppelen en zo de vereiste beheersinspanning te verlagen. Waar nu voor ieder bronsysteem een 'eigen' maatwerk koppeling is gerealiseerd willen wij toe naar een situatie waarin het bronsysteem de data op een generieke wijze beschikbaar stelt voor het IDM proces.

De eerste bronnen die worden aangepast, zijn ook de meest complexe; SAP en Osiris. In het nieuwe model zijn de bronadministraties verantwoordelijk voor het gestandaardiseerd aanleveren van de identiteitsgegevens en het vertalen van interne processen naar het voorgestelde model. Bronadministraties kunnen beter matchen over interne records binnen hun database. Het doel is dat men één identiteit aanlevert per record_id, bijvoorbeeld per studentnummer uit Osiris of Central Person uit SAP. Het IDM-systeem blijft verantwoordelijk voor het linken van deze records over de bronsystemen heen, dus studenten aan medewerkers etc.

De nieuwe koppelmethode is gebaseerd op REST-webservices. Er is gekozen voor veelgebruikte en gestandaardiseerde methoden om zo de noodzaak voor specialistische kennis binnen het IAM-team te verlagen en deze te houden bij de bronadministraties.

2 Overzicht van de oplossing

De complete oplossing is een compositie van de volgende onderdelen:

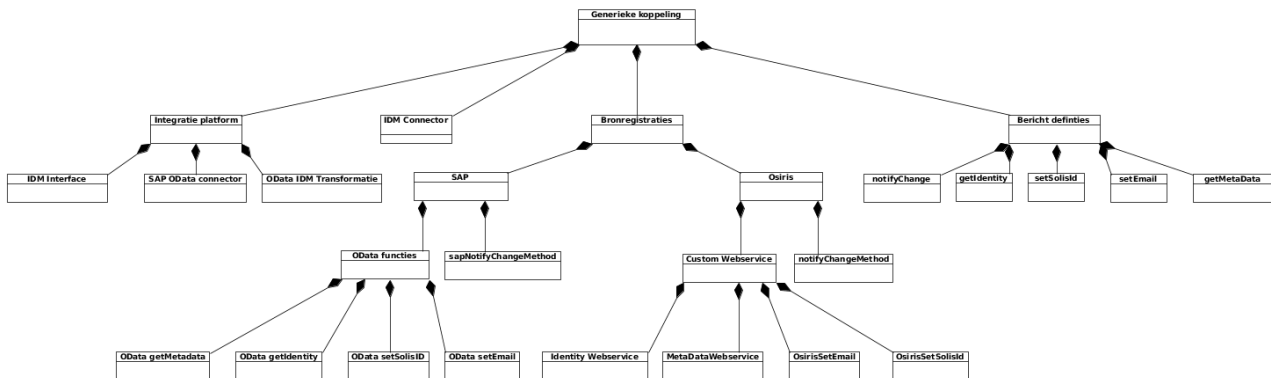


Figure 1: Decompositie in onderdelen

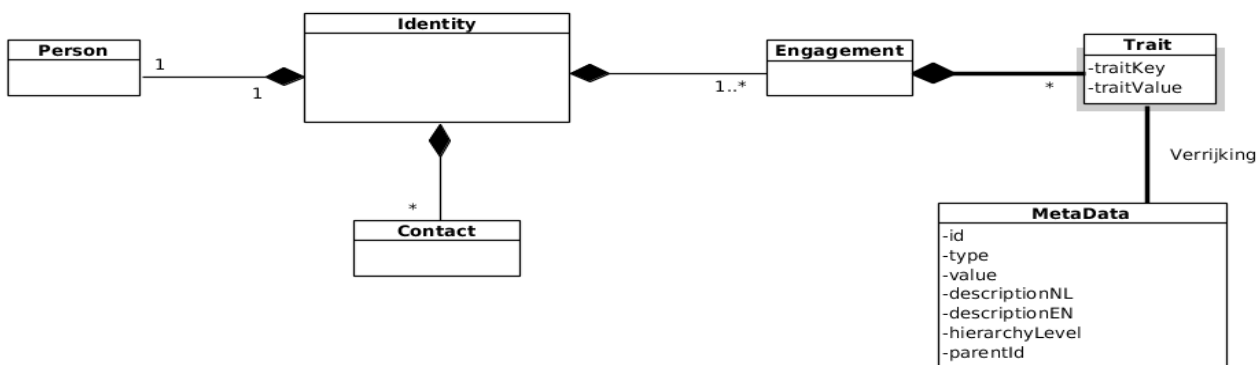
Bovenstaande onderdelen worden kort toegelicht.

Onderdeel	Naam	Omschrijving
0	Generieke koppeling	De generieke koppeling is in dit model de gehele oplossing.
1	Integratie platform	Het UU-integratieplatform
1.1	IDM Interface	Communiqueert met de IDM-connector
1.2	SAP Odata Connector	Communiqueert met het SAP-systeem
1.3	Odata IDM Transformatie	Vertaalt het SAP-Odata bericht naar de door IDM gevraagde definitie.
2	IDM Connector	De IDM connector realiseert de communicatie tussen het IDM systeem en de bronregistraties faciliteert vanuit de IDM kant.
3	Bronregistraties	De bronregistraties leveren de data voor het IDM systeem. Ook ontvangen zij het e-mailadres en SolisID vanuit het IDM systeem.
3.1	SAP	Het SAP systeem huisvest de medewerker identiteitsgegevens
3.1.1	Odata functies	De Odata functies leveren de door IDM gevraagde gegevens. Odata kan gebruikt worden om informatie te lezen maar ook om het SolisID en e-mailadres naar SAP te schrijven.
3.1.1.1	getMetadata	Bevraagd extra informatie over een niet-identiteitsobject: een O, S of C object in SAP.
3.1.1.2	getIdentity	Bevraagd een Central Person op basis van het CP-nummer uit de notificatie. GetIdentity levert de identiteit inclusief persoonsgegevens, aanstelling en formatiegegevens.
3.1.1.3	setSolisID	Zet het SolisID voor één Central Person
3.1.1.4	setEmail	Zet het medewerkers e-mailadres voor één Central Person
3.1.2	sapNotifyChangeMethod	SAP stuurt een notificatie wanneer een identiteit of metadata object wijzigt. De notificatie omvat het type, record_id en de effectieve datum.
3.2	Osiris	Het Osiris systeem huisvest de student identiteitsgegevens.
3.2.1	Custom Webservice	De custom webservice voor Osiris implementeert luisterende webservices zoals in dit document gespecificeerd.
3.2.2	osirisNotifyChangeMethod	Osiris stuurt een notificatie wanneer een identiteit of metadata object wijzigt. De notificatie omvat het type, record_id en de effectieve datum.

4	Berichtdefinities	De berichtdefinities omschrijven de vorm van de te ontvangen data van de IDM connector en web services.
---	-------------------	---

3 Datamodel

Het datamodel is gebaseerd op het interne model van het IDM systeem van de UU. Dit model heeft de volgende structuur.



Hierin is te zien dat een identiteit een compositie is uit één persoon, zijn contactgegevens en verbintenissen met de organisatie. In het beoogde model zijn diverse onderdelen aanwezig, te weten:

Identity	De complete identiteit
Person	De persoonsgegevens van de identiteit
Engagement	De verbintenissen van de identiteit met de Universiteit, bijvoorbeeld een onderwijsovereenkomst of arbeidsrelatie.
Trait	Een 'key-value'-paar welke één eigenschap omschrijft van de verbintenis. Bijvoorbeeld de functie, faculteit, opleiding of soort verbintenis. De vorm wordt per bron afgesproken.
Contact	Een contactgegeven van de persoon gemodelleerd als een type en een waarde.
Address	Een adres van de persoon gemodelleerd als een type en een waarde.
Metadata	Metadata geeft additionele informatie over de trait-waarden. Bijvoorbeeld een SAP o = 500000 omschrijft de Universiteit Utrecht. In het metadata object kan deze informatie éénmaal globaal worden opgeslagen.

Voor iedere identiteit is een Person en Engagement onderdeel verplicht evenals een e-mailadres voor de initiële communicatie. Het doel is om de identiteiten met één 'Identity'-bericht aan te leveren.

3.1 Attributen Identity

Naam	Type	Voorbeeld	Max	Vereist	Toelichting
id	String	0123921093	32	Ja	Uniek identificerend nummer voor de bron. Dit dient een permanente unieke sleutel te zijn voor deze bron.
person	Object	Zie voorbeeld	n.v.t.	Ja	Structuur waarin de persoonsgegevens worden opgeslagen.
engagements	Array Engagement		n.v.t.	Ja	Array van de verbintenissen van de identiteit
contacts	Array Contact		n.v.t.		Array van de verbintenissen van de identiteit
addresses	Array Address		n.v.t.		Uitsluitend werkadressen zijn gewenst

3.2 Attributen Person

Naam	Type	Voorbeeld	Max	Vereist	Toelichting
birthSurname	String		32	Ja	Geboortenaam zonder voorvoegsels. Voor matching
surname	String		64	Ja	Voorkeursnaam zonder voorvoegsels. – max 64 karakters
initials	String	A.I.	12	Ja	Voorletters, uppercase gescheiden door punt. – max 12 karakters
birthSurnamePrefix	String		32		Voor matching
prefix	String		32		
givenName	String	Arie	32	Ja	De roepnaam
givenNames	String	Adrianus	64		De officiële voornaam(en) uit het paspoort.
dateOfBirth	yyyy-MM-dd	1979-03-23	10	Ja	
gender	M F U	M	1	Ja	
preferredLanguage	NL EN	NL	8	Ja	
nationality	String		32		
privateEmail	String	iemand@hotmail.com	64	Ja	
titlePrefix	String	Dr.	32		
titleSuffix	String	MSc.	32		
loginDisabled ¹	Boolean	true	N.V.T.		Zorgt ervoor dat de identiteit niet meer kan authenticeren. Blokkade is direct actief zodra het attribuut is toegekend.
hideAddressList ²	Boolean	false	N.V.T.		De identiteit wordt uit de adreslijsten gehaald.
deceased	Boolean		N.V.T.		
solisID	String	steve008	32		Voor matchingdoeleinden. Wordt uitsluitend bij succesvol

1 Deze velden worden door IAM per bron beschikbaar gesteld. Nu zijn alleen Osiris en SAP in beeld. Er wordt onderzocht of deze velden nog nodig zijn.

2 Deze velden worden door IAM per bron beschikbaar gesteld. Nu zijn alleen Osiris en SAP in beeld.

					matchen overgenomen door het IAM systeem
retentionPeriod	Int				Aantal dagen waarna de gegevens verwijderd worden na de dateEnd. Er is een default waarde vanuit IAM.

3.3 Definitie Engagement (verbintenis)

Een verbintenis betreft één relatie tussen de identiteit en de Universiteit. Om iedere verbintenisvorm te kunnen modelleren is er gekozen voor een simpele structuur.

Naam	Type	Voorbeeldwaarde	Toelichting
Id	String	1	Uniek binnen de identiteit.
dateStart	(yyyy-MM-dd)	2018-01-01	De eerste dag waarop de aanstelling actief is.
dateEnd	(yyyy-MM-dd)	2019-01-01	De eerste dag waarop de aanstelling inactief is.
traits	Array Trait		Kenmerken van de relatie van de identiteit met de Universiteit.

3.3.1 Configuratie van graceBefore en graceAfter

Per verbintenis wordt een graceBefore en graceAfter toegevoegd door IAM. Deze kunnen per bron standaard ingesteld worden. Daarnaast moet het mogelijk zijn om op basis van de kenmerken een waarde toe te voegen. Wanneer de bron het aankan mag deze zelf graceBefore en graceAfter waarden toevoegen. Het IAM-systeem controleert dan alleen dat de waarden beneden een te configureren maximum lopen.

3.4 Definitie Trait

Een trait (eigenschap) slaat willekeurige informatie op over de verbintenis tussen de identiteit en de organisatie. De afdeling, functie, etc. Per bronsysteem zullen afspraken gemaakt worden over welke gegevens als Trait mee te sturen.

Met de waarden uit de kenmerken kan het IDM-systeem keuzes maken voor autorisaties, rollen en configuratie. Een trait is niks meer dan een dynamisch benoemd key-value paar, zij kunnen iedere waarde aannemen. Bijvoorbeeld, de afdeling, faculteit, het type medewerker of student.

Naam	Type	Voorbeeldwaarde	Toelichting
key	string	Faculteit	Het type trait
value	string	GW	De waarde van de trait
<code>{ 'faculty': 'REBO' }</code>			

3.5 Definitie Notificatie

Een notificatie informeert het IDM systeem over een mutatie in de bron. Het IDM systeem kan dan op een later moment een query doen naar het bronsysteem om de gewijzigde waarde op te halen.

Naam	Type	Voorbeeldwaarde	Toelichting
Type	String	Identity	Het type object wat gewijzigd is bijvoorbeeld een SAP o object of een Osiris Faculteit.
Id	String	500000	Het unieke id van de resource. Dit moet gebruikt kunnen worden als een argument voor <code>getMetadata</code>
Effective	String (yyyy-MM-dd)	2020-04-02	De datum waarop de waarde geldig wordt. Het IDM systeem zal op dat moment een query doen aan het bronsysteem.
IsDelete	Boolean	True /false	Kan gebruikt worden om een verwijdering te forceren.

3.6 Definitie Metadata

Een metadata object vertelt iets over een specifieke waarde van een Trait. Deze objecten worden gebruikt om bijvoorbeeld de departmentName en Jobtitle te vullen.

Naam	Type	Voorbeeldwaarde	Toelichting
id	string	10	
type	string	0	Dit refereert aan de Trait Key value. <code>{'faculty' : 'REBO'}</code>
value	string	50000	Dit refereert aan de Trait Value value <code>{'faculty' : 'REBO'}</code>
description_nl	string	Universiteit Utrecht	De Nederlands weergave

description_en	string	Utrecht University	De Engelse weergave
hierarchyLevel	string	0	
parentId	string	-	Het ID van een gelinked object.

4 Interactie overzicht

Interactie is gebaseerd op een notificatie gevolgd door een pull. Het bronsysteem notificeert wat opgehaald kan worden en wanneer. Het IDM-systeem bevroegd daarop het bronsysteem of het UU-IP. Het principe is dat de bron twee zaken organiseert:

- het notificeren van een wijzigingen aan het IDM endpoint. Welk record wijzigt er, vanaf wanneer zijn de waarden geldig?
- Het beschikbaar stellen van webservices welke door de IDM-connector bevroegd kunnen worden, al dan niet met tussenkomst van het UU-integratieplatform.

4.1 Authenticatie en beveiliging

- Voor communicatie van de bron richting het IDM-systeem kan gebruik worden gemaakt van basic authenticatie of een API sleutel als element in het bericht. Op een later tijdstip worden afspraken gemaakt met de ontwikkelende partijen over deze communicatie.
- Voor communicatie vanuit het IDM-systeem richting de bron kan gebruik gemaakt worden van een API sleutel (element of header), basic authentication of het OAuth 2.0 protocol.
- Er wordt gebruik gemaakt van TLS-encryptie op alle verbindingen.

4.2 Notificaties

Het bronsysteem notificeert aan het IDM-systeem de wijzigingen. De wijziging zegt niks meer dan gebruiker **a** gaat wijzigen of is gewijzigd op tijdstip **b**. Het IDM-systeem zal dan de op tijdstip **b** de identiteit bevragen aan de bron.

De bron stelt een web service beschikbaar welke door het IDM-systeem aangeroepen kan worden om de mutaties op te halen. Wanneer het e-mailadres of SolisID wijzigt zal IDM de bron bijwerken.

Wanneer een persoon, zijn verbintenis of andere gegevens wijzigen moet het bronsysteem een call doen naar het IDM-systeem. Hierin staat de volgende informatie:

1. Het tijdstip *X* waarop de mutatie effectief wordt. Wanneer *X* 'null' of in het verleden is, zal het systeem direct een taak plaatsen voor de readIdentity() methode.
2. Het record id *Y* welke wijzigt.
3. Het type record wat wijzigt
4. Of het een delete betreft

Berichten zouden uitsluitend verstuurd moeten worden voor identiteiten welke in scope zijn van het Identity Management systeem.

4.3 Read Identity

Wanneer het tijdstip X is gekomen zal het IDM systeem de nieuwe informatie opvragen via de webservice gekoppeld aan het bronsysteem. Het bronsysteem geeft antwoord middels het standaardbericht. De waarden die teruggegeven worden zijn de waarden zoals die 'nu' actief zijn. Het bronsysteem dient dus deze call te implementeren.

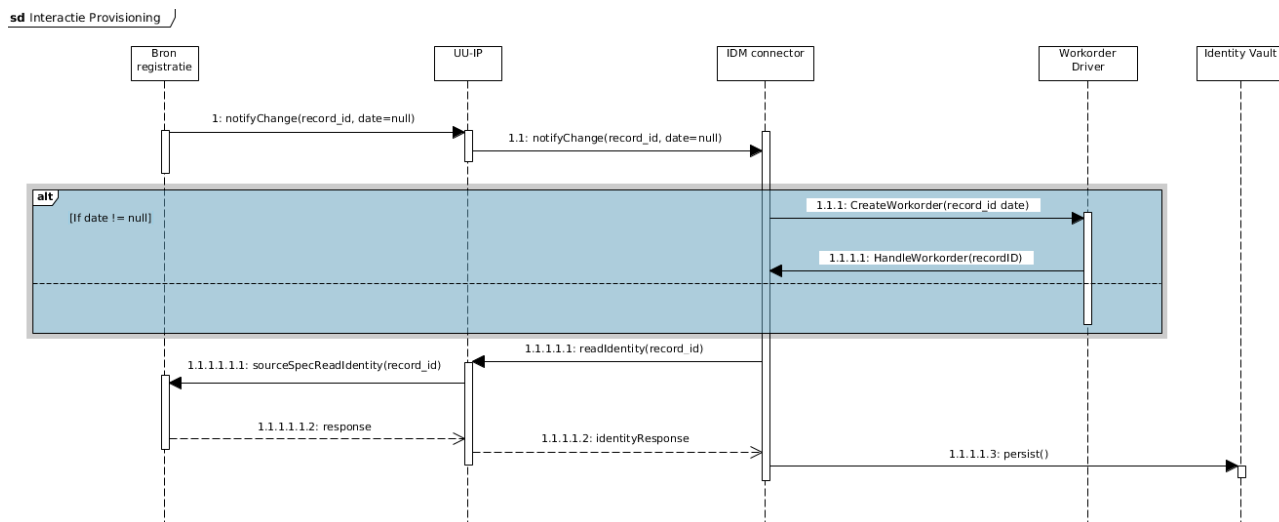


Figure 2: Interactie overzicht. De ESB is hierin optioneel.

4.4 Updaten van de Bron

Met deze call kan het IDM-systeem gegevens updaten in het bronsysteem. De bron kan twee optionele methoden implementeren:

- update email
- update solisid

Het IDM-systeem zal de bron voorzien van de gegevens volgens onderstaande logica. Hier kan het integratieplatform ook tussen worden gezet.

sd Interactie Update bron

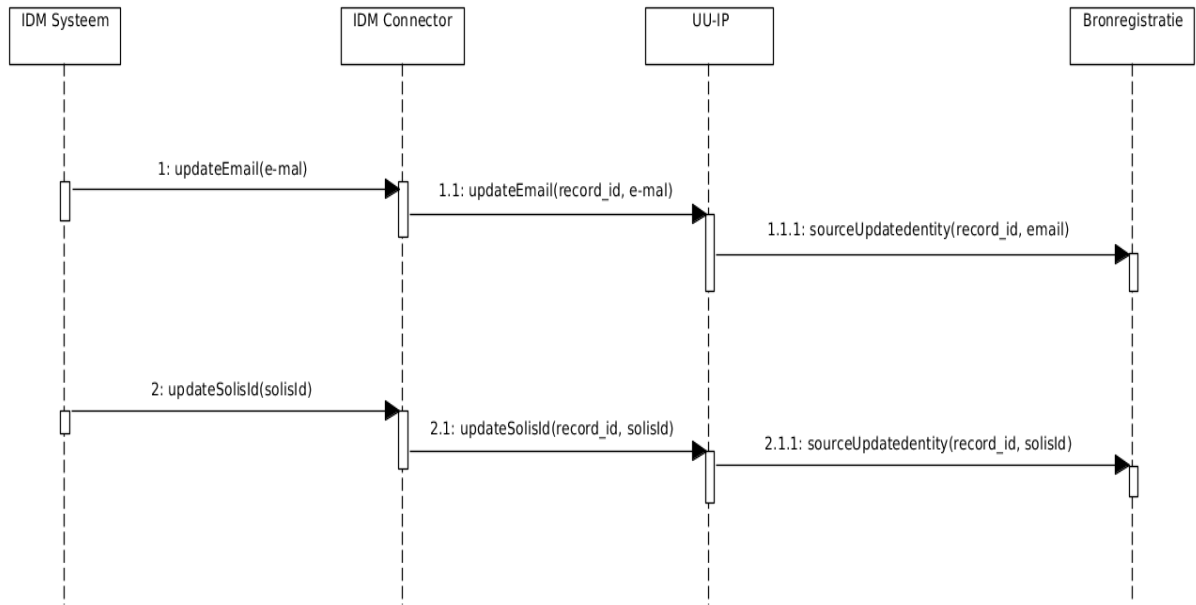


Figure 3: Bijwerken van de bron.

Onderstaande definities van de berichten kunnen gebruikt worden. De implementerende bronregistratie levert een te bevragen endpoint.

Ieder end point begint met een relatieve url bijvoorbeeld. <https://bron.uu.nl/idm/>. Het end point is vanzelfsprekend te configureren.

In onderstaande tabellen wordt met '{}' een dynamische parameter geïd.

4.5 notifyChange

Met notifyChange kan een bron het IDM systeem notificeren over een mutatie in de brongegevens. Dit kan een create of update zijn, er is geen verschil. Het IDM systeem creëert een taak om het gewijzigde record op te vragen.

Method	POST
Request body	<pre>{ 'type': 'identity', 'id': '0000001', 'effectiveDate': 'yyyyMMdd' 'isDelete': false }</pre>
Resources (relatieve URL)	/notification
Response codes	201 (Created) → Success
Response body	Identity bericht

4.6 getIdentity

GetIdentity wordt uitgevoerd door de IDM connector richting het bronsysteem. Het bronsysteem levert de informatie in een response.

GetIdentity moet altijd de 'nu' geldende waarden retourneren. Niet de waarden die pas in de toekomst actief worden. Wanneer een record niet in scope is van IAM kan het systeem een 404 teruggeven.

Method	GET
Request body	-
Resources (relatieve URL)	identity/{record_id}
Response codes	200 → Success 404 → Not found
Response body	Zie Identity bericht

4.7 getMetaData

GetIdentity wordt uitgevoerd door de IDM connector richting het bronsysteem of integratieplatform. Het bronsysteem levert de gevraagde informatie in een response.

Method	GET
Request body	-
Resources (relatieve URL)	metadata/{type}/{record_id}
Response codes	200 → Succes 404 → Not found
Response body	<pre>{ "id", "iets_unieks", "name", "Universiteit Utrecht", "hierarchy_level", "0", "parent_id": null, " }</pre>

4.8 updateSolisId / updateEmail

Met updateSolisID kan het IDM systeem de bronregistratie bijwerken met het door IDM gegenereerde SolisID of e-mailadres. Dit mag individueel of samen in één call.

Om een waarde te legen kan deze met een lege value worden aangeboden.

Method	PUT / POST
Request body	{ "email": " iemand@uu.nl ", "solisid": "steve008" }
Resources (relatieve URL)	identity/{record_id}
Response codes	200 / 204 (No content) → Succes 404 → Not found
Response body	-

5 SAP

Een identiteit uit SAP is een Central Person. SAP stuurt één person element met daarin de persoonsgegevens met alle gekoppelde dienstverbanden/formatieplaatsen en werkadressen. Als SAP ook informatie over uitleen heeft zou dit bijvoorbeeld ook als een eigen engagement ingevuld kunnen worden. De engagements en traits worden gebruikt om de relevante informatie door te geven van de aanstellingen en formatieplaatsen die gekoppeld zijn aan een central person. Hieraan kan het IDM systeem regels koppelen voor autorisaties, groepen of rollen.

Het IDM-systeem wil een engagement per aanstelling, per formatieplaats.

Nu worden in de engagement zaken genoemd als :

- o → organisatieonderdeel
- s → formatieplaats
- c → job / functie
- type → intern / extern / gast /?
- rol → researcher / docent / obp

Voorbeeld Identity bericht SAP

```
{
  "id": "00002",
  "person": {
    "givenName": "Laura Maria",
    "givenNames": "Louise Marijke",
    "initials": "L.M.",
    "surname": "Voorbeeldpartner-van Voorbeeldachternaam",
    "surnamePrefix": "",
    "birthSurname": "Voorbeeld achternaam",
    "birthSurnamePrefix": "van",
    "dateOfBirth": "2000-01-02",
    "titleSuffix": "MSc",
    "titlePrefix": "ir",
    "gender": "m"
  },
  "engagements": [{
    "id": "1232323",
    "dateStart": "2016-07-01",
    "dateEnd": "2019-01-31",
    "graceBefore": 15,
    "graceAfter": 30,
    "traits": {
      "o": "1",
      "c": "3",
      "rol": "docent",
      "type": "intern"
    }
  }],
  "contact": [{
    "id": "1",
    "type": "private_email",
    "value": "someone@me.com"
  }],
  "addresses": [{
    "id": "1",
    "type": "work",
    "country": "Netherlands",
    "state": "Utrecht",
  }]
```

```
"city": "Utrecht",
"street": "Heidelberglaan 8",
"zipcode": "3584CS",
"building": "Bestuursgebouw",
"roomnumber": "2.96"
}]
}
```

5.1 Middleware en OData

SAP heeft een standaard OData interface waarmee records bevroegd, bewerkt en toegevoegd kunnen worden. De IDM connector zal echter geen Odata 'spreken' maar de hier voorgestelde berichten gebruiken. Het integratieplatform zal de berichten transformeren naar het hier omschreven formaat.

Het SAP-team levert de vereiste OData functies die alle gevraagde informatie kunnen opleveren. Concreet betekent dit dat de vereiste middleware zo min mogelijk data transformeert en interpreteert.

1.1 Traits en grace-waarden

De volgende traits en grace-waarden zijn nu gewenst:

Naam	Toelichting
O	De code van de OE op de aanstelling / formatie
S	De code van de formatieplaats
C	De code van de job
Rol	OBP, Docent, Extern etc.. of het persk nummer.
Type	Formatieplaats / Aanstelling
GraceBefore	Deze waarde is nu afhankelijk van het type medewerker 62 voor docenten en 5 voor alle anderen.
GraceAfter	Deze waarde is nu 92 dagen voor alle medewerkers.

De grace-perioden zijn door de bron zelf in te stellen, van de nu geldende standaardwaarden kan dus afgeweken worden mocht dat wenselijk zijn.

Voor medewerkers van GDL kan een andere 'o' trait worden gestuurd zodat zij niet met naam en toenaam bekend worden via bijvoorbeeld Exchange.

5.2 Metadata objecten

Vanuit Osiris verwachten wij twee soorten metadata:

- organisatieonderdeel
- jobs

Hier volgen twee voorbeeld berichten. Let op: de opleiding verwijst naar de faculteit als parentID.

```
{
  "id", "11000000",
  "type": "o",
  "description_nl", "Faculteit Sociale Wetenschappen",
  "description_en", null,
  "hierarchy_level": 2,
  "parent_id": 50007153,
}

{
  "id", "50001666",
  "type": "c",
  "description_nl", "Sportdocent 3",
  "description_en", null,
  "hierarchy_level": null,
  "parent_id": null
}
```

Het IDM systeem wil alle metadata hebben, ook als deze niet toegekend wordt aan medewerkers, zoals het OE onderdeel 'Faculteiten'. De description zou gestript kunnen worden van de niveau-aanduiding dus "Sportdocent 3" → "Sportdocent".

5.3 Toevoegen business rule

Voor SAP is het complex om ook historische data mee te sturen van de aanstellingen. Op het moment dat een aanstelling inactief is zal de 'o' waarde worden vervangen door een algemene waarde. Dit betekent dat er een business rule nodig is om de rechten gedurende de grace-periode te handhaven. De toe te passen regel: wanneer de waarde van de 'o' in een formatieplaats '9999999' is zal deze waarde gestript worden en vervangen door de huidige waarde in IAM. IAM zal dus nooit een persoon kunnen plaatsen op deze o.

6 Osiris

Vanuit Osiris verwachten per studentnummer een identiteit met daarin voor inschrijving een engagement. Het privé e-mailadres is het enige contactgegeven wat wordt verwacht. In de huidige koppeling interpreteert IAM verschillende deelprocessen van de inschrijving. Hoe deze door Osiris zelf geïnterpreteerd kunnen worden met de beschikbare parameters van de verbintenis wordt toegelicht in de paragraaf "Processen en berichten".

Osiris zal worden gekoppeld middels het integratieplatform.

Voorbeeld Bericht vanuit Osiris

```
{
  "id": "00002", ← het studentnummer
  "person": {
    "givenName": "Laura Maria",
    "givenNames": "Louise Marijke",
    "initials": "L.M.",
    "surname": "Voorbeeldpartner-van Voorbeeldachternaam",
    "surnamePrefix": "",
    "birthSurname": "Voorbeeld achternaam",
    "birthSurnamePrefix": "van",
    "dateOfBirth": "2000-01-02",
    "titleSuffix": null,
    "titlePrefix": null,
    "gender": "m",
  },
  "engagements": [{
    "id": "1232323",
    "dateStart": "2018-09-01",
    "dateEnd": "2019-07-31",
    "traits": {
      "faculty": "REBO",
      "study": "BEBM",
      "type": "Bachelor",
    }
  }],
  "contact": [{
    "id": "1",
    "type": "private_email",
    "value": "email@gmail.com"
  }]
}
```

Vanuit Osiris willen wij berichten ontvangen van studenten welke een inschrijving hebben die:

- een einddatum hebben die niet meer dan één jaar in het verleden ligt op een inschrijving die in volledig zijn of een sunrise datum hebben.
- Een volledige inschrijving heeft de volgende processen afgerond of is daar niet in scope voor:
 - toelating
 - matching
 - selectie
- Een sunrise datum wordt opgeslagen in het vrije veld 'SUNRISE_DATUM' en is geldig wanneer deze in net huidige studiejaar ligt voor 15 oktober.

- Wanneer er eenmaal een bericht is gestuurd naar IAM moeten de berichten gestuurd blijven worden naar IAM. Wanneer een aanstelling 'out-of-scope' gaat willen wij nog wel een notificatie ontvangen zodat we de account niet onterecht actief (gaan) maken.

6.1 Traits en grace-waarden

De volgende traits en grace-waarden zijn nu gewenst:

Naam	Toelichting
Faculty	De code van de faculteit van de verbintenis, bijvoorbeeld REBO.
Study	De code van de studie.
Type	Bachelor / Master / Cursus / Sunrise.
GraceBefore	Deze waarde is nu 60 dagen.
GraceAfter	Deze waarde is nu 180 dagen.

De grace-perioden zijn aan te leveren in het bericht mocht dat wenselijk zijn. Er zouden kortere of langere grace-perioden gezonden kunnen worden voor cursisten of deelnemers aan een specifieke studie of bij een bepaalde faculteit of in een bepaalde rol.

6.2 Metadata-objecten

Vanuit Osiris verwachten wij twee soorten metadata-objecten:

- ~~faculteiten~~, Deze metadata wordt niet meer aangeleverd door Osiris maar handmatig beheerd in het IDM-systeem. Wanneer er een wijziging op faculteitsniveau plaats vindt zal IAM aangehaakt worden.
- Opleidingen, we willen de namen weten en bij welke faculteit de studie hoort.

Hier volgen twee voorbeeld berichten. Let op: de studie heeft een verwijzing naar de faculteit als parentID.

```
{
  "id": "REBO",
  "type": "faculty",
  "description_nl": "Faculteit Recht, Economie, Bestuur en Organisatie",
  "description_en": "Faculty of Law, Economics and Governance",
  "hierarchy_level": null,
  "parent_id": null,
}
```

```
{
  "id": "BEBM",
  "type": "study",
  "description_nl": "Bestuur en beleid",
  "description_en": "Public governance",
  "hierarchy_level": null,
  "parent_id": "REBO"
}
```

6.3 Processen en berichten

Osiris moet rekening houden met de status van een persoon binnen het inschrijvingsproces. Het IDM-systeem dient geen inhoudelijke kennis te hebben van deze processen. Dit kan gedaan worden door de begin en einddatum in de verbintenis / engagements te manipuleren of identiteiten niet aan IDM te sturen welke nog niet 'klaar' / in-scope zijn. Osiris stuurt een bericht voor iedere student welke voldoet aan onderstaande regels:

- **Toelating:** zolang toelating vereist is en niet verleend → geen bericht naar IAM
- **Selectie:** zolang selectie vereist is en niet is verleend → geen bericht naar IAM
- **Matching:** zoals matching is vereist en niet afgerond → geen bericht naar IAM
- **Sunrise:** zolang de persoon mag inloggen zonder actieve inschrijving → engagement sunrise datum einddatum is 1 september. > eigen verbintenis. Voorbeeld studenttype → contractant, bachelor, master.
 - dateStart = sunriseDatum
 - dateEnd = 1 oktober in het komende studiejaar
 - graceBefore = 0
 - graceAfter = 0
- **Inschrijving incompleet:** zolang niet compleet (Centrale inschrijving en CSA status niet compleet)
 - dateStart = startdatum inschrijving
 - dateEnd = dateStart + 45 dagen.
 - graceBefore = normaal
 - graceAfter = 0

Wanneer de verbintenis compleet is kan de definitieve verbintenis worden gestuurd met de eigenlijke data.

- **Intrekking vooraanmelding:** → einddatum naar de intrekingsdatum. GraceEnd naar 0.
- **Betalingsachterstand:** wanneer er een betalingsachterstand is kan de Osiris het loginDisabled veld in de Identity naar 'true' zetten.
 - loginDisable = true
- **Overleden / langdurig ziek:** wanneer de identiteit overleden is of langdurig ziek, kan de identiteit aangemerkt worden als 'overleden'. Op deze manier ontvangt de student geen e-mail meer en wordt uit de adreslijsten verwijderd.
 - deceased = true.
- **Delete:** wanneer de studentrecord wordt verwijderd uit Osiris verwachten wij een delete notificatie.