|  |
| --- |
| Vlaamse Overheid – Digitaal Vlaanderen |
| ACM-IDM Onboarding |
| Template: Beveiligen van toepassingen (aanmelden van gebruikers)Vito – WeAre <NAME>Opstartdatum integratie: <DATE> |

|  |
| --- |
| Babak, Galina  |
|  |

Table of Contents

[0 Checklist Integratie ACM 3](#_Toc140146858)

[1 Informatie rond de te ontsluiten toepassing 4](#_Toc140146859)

[1.1 Algemene Gegevens 4](#_Toc140146860)

[1.2 Informatie rond de toepassing 4](#_Toc140146861)

[1.3 Verplichte Contactgegevens toepassing 5](#_Toc140146862)

[1.4 Capaciteitsplanning 5](#_Toc140146863)

[1.5 Registratie buitenlanders/bis register 5](#_Toc140146864)

[2. Specificaties ACM Toegangsbeheer 6](#_Toc140146865)

[2.1 Type ontsluiting acm 6](#_Toc140146866)

[2.2.1 URL’s toepassing 8](#_Toc140146867)

[2.2.2. Callback url OpenID Connect/OAuth 9](#_Toc140146868)

[2.2.2. Entity ID SAML 9](#_Toc140146869)

[2.3 Autorisatie attributen 10](#_Toc140146870)

[2.4 Authenticatiemiddelen 11](#_Toc140146871)

[2.5 Uitgeleverde attributen/scopes 12](#_Toc140146872)

[3. Specificaties IDM gebruikersbeheer 20](#_Toc140146873)

[3.1 Overzicht gebruikersrechten 20](#_Toc140146874)

[3.2 Technische specificaties rechten 21](#_Toc140146875)

[3.3 Technische specificaties interne contexten 22](#_Toc140146876)

[\*Mogelijke keuzes contextenwaarden samenstelling 22](#_Toc140146877)

[3.4 Technische Overdracht IDM 23](#_Toc140146878)

[3.5 DES configuratie\* 24](#_Toc140146879)

[3.6 EAWS specificaties 24](#_Toc140146880)

[3.7 Provisioning webservice specificaties 24](#_Toc140146881)

[3.8 AD groep specificaties 25](#_Toc140146882)

[3.9A Datapower specificaties 27](#_Toc140146883)

[3.9B Datapower (voorbeeld url’s) 28](#_Toc140146884)

[3.10 directory Provisioning specificaties 28](#_Toc140146885)

[3.11 te provisioneren informatie 29](#_Toc140146886)

[3.12A ad groep specificaties (1.1) 30](#_Toc140146887)

[3.12b ad groep specificaties (1.2) 30](#_Toc140146888)

[4. Specificaties SSM Mandatenbeheer 31](#_Toc140146889)

[4.1 algemene beschrijving 31](#_Toc140146890)

[4.2 configuratie mandaattype ssm 31](#_Toc140146891)

[4.3 urls van de toepassing 32](#_Toc140146892)

[4.4 autorisatie attributen mandaten 32](#_Toc140146893)

[6. Metadata 33](#_Toc140146894)

[6.1 SAML-Metadata van de VO-Identity provider: ACM 33](#_Toc140146895)

[6.2 Client Certificaten van datapower 33](#_Toc140146896)

[6.3 Server Certificaten van webservice 34](#_Toc140146897)

[6.4 Public Keys voor Client Authenticatie via JWT 34](#_Toc140146898)

[6.5 endpoints voor Client Authenticatie via JWT via JWKS 34](#_Toc140146899)

[7. Nuttige links ACM/IDM-integraties 35](#_Toc140146900)

[7.1 Overzicht documentatie 35](#_Toc140146901)

[8. Documenteigenschappen 36](#_Toc140146902)

[8.1 Auteurs 36](#_Toc140146903)

[8.2 Geschiedenis 36](#_Toc140146904)

# 0 Checklist Integratie ACM

In onderstaande lijst hebben we, niet exhaustief, al enkele acties opgelijst waar je als klant rekening mee moet houden en opvolgen in je planning, voor een integratie met het toegangs- en gebruikersbeheer. Deze acties zijn niet exhaustief en kunnen verschillen naargelang de functionele en technische behoeften van de toepassing.

1. Aanleveren van de vereiste technische info bij het opstellen van het integratiedossier:
	* SAML: doorgeven van de SAML metadata
	* OpenID Connect: doorgeven van de callbackURI's + post logout URI's
2. Doornemen en goedkeuren van het integratiedossier
3. Als de toepassing zich in DC Atos of VPC overgangszone bevindt; of een locatie achter de VO reverse proxy:
	* aanvragen van de datastromen van de desbetreffende reverse proxy naar de toepassing (bij het netwerkteam)
	* aanvragen van een DNS die verwijst naar de reverse proxy (bij het netwerkteam)
	* aanvragen van een VO PKI certificaat + installatie op de toepassing
	* toevoegen van het IP-adres, poort en URL van de backend-toepassing in het integratiedossier
4. Installatie van de toepassing
5. Configuratie van de ACM-integratie zodra de configuratie langs toegangsbeheer (ACM) zijde voltooid is
6. Als de toepassing niet meer gebruikt wordt, gelieve het integratieteam (integraties@vlaanderen.be) te informeren dat de toepassing uitgefaseerd mag worden uit ACM/IDM. Dit vermijdt een opstapeling van onnodige gebruikersrechten in WebIDM.

Bovenstaande acties en planning geven we enkel ter informatie mee zodat je als klant voldoende rekening kan houden met de planning en opvolging die aan jouw kant verder moet opgenomen worden i.k.v. het integratie-traject. Voor het planningstraject en de technische stappen die nodig zijn aan toepassingszijde is Digitaal Vlaanderen niet verantwoordelijk.

**In het geval van een SAML integratie:**

De certificaten in de SAML metadata zullen na verloop van tijd vervallen. Het is belangrijk om de vervaldatum in het oog te houden en tijdig nieuwe certificaten aan te vragen om nieuwe SAML metadata te genereren.

Gelieve minstens **2 weken op voorhand** het ACM/IDM team te contacteren om de nieuwe SAML metadata te implementeren. Op dit moment moet de nieuwe SAML metadata met de nieuwe certificaten ook geleverd worden.

**Hoe gaan we om met PERSOONSGEGEVENS?:**

Wanneer instanties gebruik maken of beroep doen op het Toegangs- en Gebruikersbeheer van Digitaal Vlaanderen, treedt Digitaal Vlaanderen op als verwerker van persoonsgegevens. De verbintenissen die Digitaal Vlaanderen als verwerker opneemt zijn opgelijst in het [verwerkingscharter](https://overheid.vlaanderen.be/publicaties-toegangs-en-gebruikersbeheer).

[ ]  Ik begrijp en accepteer het verwerkingscharter

**Kleurenlegende:**

Geel gemarkeerd => aan te vullen door integrator/toepassingseigenaar
Groen gemarkeerd => toevoeging door ACM/IDM
~~Rood gemarkeerd~~ => afbouw door ACM/IDM

# 1 Informatie rond de te ontsluiten toepassing

|  |
| --- |
| 1.1 Algemene Gegevens [ ]  ACM overzicht aanvullen op [Sharepoint](https://vlaamseoverheid.sharepoint.com/%3Ax%3A/r/sites/afb/ICT_Klanten/acmidm/ACM/Gedeelde%20%20documenten/toepassingen-entiteiten-201912.xlsx?d=w8ee313aa2a6e4b24b92a6b6c4b67670f&csf=1&e=ii2EUH) |
| **Trajectnaam**Gelieve de entiteit en trajectnaam steeds in het email onderwerp te vermelden bij alle commumicatie.*(bv. DV MijnTraject – draft dossier)* | **PROJECT NAME** |
| **Entiteit** | **ENTITY NAME** |
| **Entiteit – OVO code of KBO-nummer** | **KBO NUMMER** |
| **Korte omschrijving vereisten voor ontsluiting** | [x]  Toegangsbeheer[ ]  Gebruikersbeheer[ ]  Mandatenbeheer (SSM)  |
| **Gewenste datum T&I** | **asap** |
| **Gewenste datum PRD** | **asap** |

|  |
| --- |
| 1.2 Informatie rond de toepassing |
| **beschrijving van de toepassing** | **DESCRIPTION OF APPLICATION** |
| **Doelpubliek** Welke organisaties maken gebruik van de toepassing per doelgroep.Welke acties hebben de organisaties | **GID**  |  |
| **EA** |  |
| **LB** |  |
| **OV** |  |
| **BUR** | **X** |
| **LLN** |  |
| **Informatie indien communicatiecampagne**Hoe zijn de eigen klanten/gebruikers ingelicht? Kunnen wij deze informatie ook ontvangen? |  |

|  |
| --- |
|  1.3 Verplichte Contactgegevens toepassing |
|  **Functie** | **Naam** | **Telefoonnr** | **Emailadres** |
| **Single point of contact** | Click here to enter text. | Click here to enter text. |  |
| **Toepassingsverantwoordelijke\*** |  |  |  |
| **Contact voor support** |  |  | **Functionele mailbox indien beschikbaar** |

\*Persoon zal monitorrechten in Gebruikersbeheer ontvangen

|  |
| --- |
| 1.4 Capaciteitsplanning |
| **Inschatting aantal gebruikers van de toepassing** | **Inschatting aantal authenticaties per dag** |
| [x]  < 100[ ]  100 – 1.000[ ]  1.001 – 10.000[ ]  > 10.000 | [ ]  < 100[ ]  100 – 1.000[ ]  1.001 – 10.000[ ]  > 10.000 |
| **Kantoorurentoepassing** | [ ]  JA [ ]  NEE |
| **Indien geen kantoorurentoepassing, bedrijvigheid tijdens weekend?** | [ ]  JA [ ]  NEE |
| **Wisselende piekperiodes in gebruik** | [ ]  JA [ ]  NEE |
| **Overzicht Piekperiodes voor de toepassing** |  |
| **Van** | **Tot** | **Specificaties** |
| Click here to enter text. | Click here to enter text. | **Drukste periode van het jaar (maandzone)** |
| Click here to enter text. | Click here to enter text. | **Drukste periode van de maand (datumzone)** |
| Click here to enter text. | Click here to enter text. | **Drukste dag(en) van de week** |
| Click here to enter text. | Click here to enter text. | **Drukste tijdszone tijdens dagperiode (uurzone)** |
| Click here to enter text. | Click here to enter text. | **Speciale bemerking rond piekperiodes afwijkend van bovenstaande?** |
| Click here to enter text. | **Documentatie piekperiodes** |
| Click here to enter text. | **Topminuut****(Aantal authenticaties per minuut in de piekperiode)** |

# 2. Specificaties ACM Toegangsbeheer

|  |
| --- |
| 2.1 Type ontsluiting acm |
| **Gebruiksvriendelijke naam van de toepassing**(weergegeven in de authenticatieschermen) | **APPLICATION NAME** |
| **Applicatienummer waarmee applicatie gekend is in WebIDM** | **XXX** |
| **Authenticatieniveau:** deze keuze bepaalt of een gebruiker naar de applicatie gaat voor een specifieke organisatie uit de keuzelijst (organisatieniveau) OF meteen na authenticatie wordt doorverwezen naar de toepassing voor alle organisaties waarvoor hij rechten heeft in het gebruikersbeheer (doelgroepniveau).**\* Authenticatie op organisatieniveau in doelgroep OV is mogelijk op één cruciale voorwaarde: het recht dat toegang geeft tot deze applicatie, mag niet aan één persoon op meer dan 100 verschillende werkrelaties zijn toegekend.** |  | **Organisatieniveau** | **Doelgroepniveau** |
| GID (Medewerkers Vlaamse overheid) | [ ]  | [ ]  |
| Economische actoren | [ ]  | [ ]  |
|  | inclusief wettelijk vertegenwoordigers | [ ]  | [ ]  |
|  | inclusief BTB | [ ]  | [ ]  |
| Lokale besturen | [ ]  | [ ]  |
|  | inclusief wettelijk vertegenwoordigers | [ ]  | [ ]  |
|  | inclusief BTB | [ ]  | [ ]  |
| Onderwijs & vorming\* | [ ]  | [ ]  |
| Burgers |  | [x]  |
| Leerlingen |  | [ ]  |
| Leerkrachten |  | [ ]  |
| Verenigingen | [ ]  | [ ]  |
| **INTEGRATIE eLOKET ONDERNEMEN** | [ ]  JA [ ]  [Dossier eLoket voor Ondernemers](https://vlaamseoverheid.sharepoint.com/sites/afb/ICT_Klanten/acmidm/integraties/Gedeelde%20%20documenten/ACMIDM_Onboarding_AIO_eLoketOndernemersHEADER.docx?d=w1f4861bc5e8e4ad8bf096ad85f65060f) geüpdatet [ ]  [Lijst eLoket voor Ondernemers](https://vlaamseoverheid.sharepoint.com/sites/afb/ICT_Klanten/acmidm/integraties/Lists/Vragen%20aan%20ACM/AllItems.aspx) geüpdatet[x]  NEE |
| **INTEGRATIE Mijn Burgerprofiel** | [ ]  JA[x]  NEE |
| **INTEGRATIE Personeelslid API OV:** heeft Departement Onderwijs & Vorming gevalideerd dat de toepassing mag intekenen op de Personeeslid API OV? | [ ]  JA[ ]  NEE |
| **AUTOSELECT:** Wanneer de keuze van doelgroep/organisatie beperkt is tot 1 mogelijkheid, dient deze keuze dan automatisch gemaakt te worden voor de gebruiker? | [x]  JA[ ]  NEE |
| **AUTHORIZED ONLY:** In de lijst van organisaties, dienen enkel organisaties weergegeven te worden waar de gebruiker ook effectief rechten heeft voor de toepassing? | [x]  JA[ ]  NEE |
| **EXACT 1 AUTHENTICATIEMIDDEL:** Wanneer er slechts één authenticatiemiddel wordt gevraagd (via exact bij SAML of acr\_values bij OpenID Connect), dan moet dat authenticatiemiddel automatisch gekozen worden zonder een keuzescherm met authenticatiemiddellen te tonen. | [ ]  JA[x]  NEE |
| **MOBIELE APP?**  | [ ]  JA[ ]  NEE |
| **Protocol**\* Voorwaarden http header-integraties:- De toepassing ondersteunt geen andere authenticatieprotocollen- De toepassing wordt gehost in een datacenter van de VO | [ ]  GEEN ACM[x]  OpenID Connect[ ]  OAuth[ ]  SAML 2.0 Federatie[ ]  REVERSE PROXY (http Header) \*[ ]  REVERSE PROXY, NIET over HB+ beheerde proxy (NIET-STANDAARD) |
| **Hostomgeving** | [ ]  Intern: VPC Overgangszone, Atos Datacenter[ ]  Extern: Cloud |
| **AUTHENTICATIEMANIER** | [ ]  VIA VLAAMSE OVERHEID[ ]  VIA ACCOUNT BIJ PARTNER (NIET-STANDAARD) |
| **INDIEN AUTHENTICATIE VIA ACCOUNT BIJ PARTNER** | NAAMGEVING TAB | **“Via account bij Partner” of KEUZE** |
| STANDAARD TAB SELECTIE  | [ ]  VIA VLAAMSE OVERHEID[ ]  VIA ACCOUNT BIJ PARTNER |
| **Configuratie OIDC/OAuth**Authorized parties zijn de partijen (ClientID’s) die in naam van deze applicatie tokens mogen opvragen bij het toegangsbeheer | [x]  De toepassing wenst gebruik te maken van refresh tokens |
| Gewenste levensduur refreshtoken (MAX 8 uur)  | **8 uur** |
| [ ]  OIDC Cross client ondersteuning vereist |
| **Authorized parties list T&I** | Click here to enter text. |
| **Authorized parties list PRD** | Click here to enter text. |
| [x]  De toepassing wenst gebruik te maken van end\_session\_endpoint |
| [x]  Het gebruik van PKCE is verplicht bij elke authenticatie |
| **Toegelaten methodes authenticatie client (een of meerdere)** | [x]  Via Client Secret[ ]  Via JSON Web Token (JWT) via JWK[ ]  Via JSON Web Token (JWT) via een JWKS endpoint |
| [ ]  De toepassing wenst gebruik te maken van UserInfo endpoint |
| [ ]  De toepassing mag token exchange doen |
| **Voor (T&I):** | Click here to enter text. |
| **Voor (PRD):** | Click here to enter text. |
| [ ]  De toepassing mag client credentials grant doen (in kader van token exchange) |
| **Voor (T&I):** | Click here to enter text. |
| **Voor (PRD):** | Click here to enter text. |
| **Contactpersoon voor OpenID Connect/OAuth**Naar deze contactgegevens wordt de Client ID en (eventueel) de Client Secret gestuurd bij de integratie | Email adres | Click here to enter text. |
| GSM Nummer | Click here to enter text. |
| [ ]  Klant dient niet per mail verwittigd te worden |

|  |
| --- |
| 2.2.1 URL’s toepassing |
| **T&I** | **ID** | **URL(s)** (starten bij https:// of http:// [localhost]) |
|
| [ ]  | **1** | **https://<ACC ENVIRONMENT>/** |
| [ ]  | **2** | **http://localhost:<FRONT\_END\_PORT>/** |
| **PRD** | **ID** | **URL(s)** (starten bij https://) |
| [ ]  | **A** | **https://<PRD ENVIRONMENT>/** |
| [ ]  |  | Click here to enter text. |

\*Voor de doelgroep Leerlingen wordt er gebruik gemaakt van de authenticatiesleutel LeerID. Deze LeerID sleutel heeft 2 testomgevingen, namelijk een DEV-omgeving en een STAGE-omgeving. Standaard wordt hier geopteerd om met de DEV-omgeving van LeerID te gebruiken. Het is NIET mogelijk om beide omgevingen gelijktijdig te gebruiken.

|  |
| --- |
| 2.2.2. Callback url OpenID Connect/OAuth |
| [ ] **&I** | **ID** | **Client ID** | **Callback URL(‘s)** | **Post logout redirect URI** | **GID** | **EA** | **LB** | **OV** | **BUR** | **LLN\*** |
|  |  |  |  |  |  |  |  |  |  | **DEV (standaard)** | **STAGE** |
|[x]  **1** |  |  https://<API URL ACC>/oidc-redirect,  | https://<API URL ACC>/logged-out, http://localhost:<BACKEND\_PORT>/logged-out |[ ] [ ] [ ] [ ] [x] [ ] [ ]
|[ ]   |  | http://localhost:<BACKEND\_PORT>/oidc-redirect  | Click here to enter text. |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **PRD** | **ID** | **Client ID** | **Callback URL(‘s)** | **Post logout redirect URI** | **GID** | **EA** | **LB** | **OV** | **BUR** | **LLN** |
|[ ]  **A** |  |  https://<API URL PRD>/oidc-redirect | **https://ttp-api.zenjoy.be/logged-out** |[ ] [ ] [ ] [ ] [x] [ ]
|[ ]   |  |  |  |[ ] [ ] [ ] [ ] [ ] [ ]

\*Voor de doelgroep Leerlingen wordt er gebruik gemaakt van de authenticatiesleutel LeerID. Deze LeerID sleutel heeft 2 testomgevingen, namelijk een DEV-omgeving en een STAGE-omgeving. Standaard wordt hier geopteerd om met de DEV-omgeving van LeerID te gebruiken. Het is NIET mogelijk om beide omgevingen gelijktijdig te gebruiken.

|  |
| --- |
| 2.3 Autorisatie attributen |
| **Autorisatiewaarde** | **IDD Attribuut** | **ID URL’s van toepassing** | **GID** | **EA** | **LB** | **OV** |
|  |  | **T&I** | **PRD** |  |  |  |  |
|  |  | **1** | **2** | **3** | **A** | **B** | **C** |  |  |  |  |
| Click here to enter text. | **federatie-applicatiexxx-autorisatiedata** |[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
| Click here to enter text. | Click here to enter text. |[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
| Click here to enter text. | Click here to enter text. |[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

|  |
| --- |
| 2.4 Authenticatiemiddelen |
| **Authenticatiemiddel** | **URN indien SAML** | **Auth****niveau** | **CSAM level** | **Min. CSAM level**\* | **Eidas schaal** | **AuthMechs**Welke authmiddelen mogen standaard getoond worden? |
|  |  |  |  |  |  |  |
| eID en aangesloten kaartlezer | urn:be:vlaanderen:authmech:eid | 35 | 500 | [ ]  500 | High |[x]
| Itsme | urn:be:vlaanderen:authmech:itsme | 30 | 450 | [ ]  450 | High |[x]
| Eidas High \*\*\* | urn:be:vlaanderen:authmech:eidashigh | 30 | 450 |  | High |[x]
| Beveiligingscode via mobiele app (OTP via app) | urn:be:vlaanderen:authmech:csamtotp | 26 | 400 | [ ]  400 | Substantial |[x]
| Beveiligingscode via SMS (OTP via sms) | urn:be:vlaanderen:authmech:csamsms | 25 | 400 |  | Substantial |[ ]
| Eidas Substantial \*\*\* | urn:be:vlaanderen:authmech:eidassubstantial | 21 | 400 |  | Substantial |[ ]
| Beveiligingscode via e-mail (OTP via mail) | urn:be:vlaanderen:authmech:mailotp | 21 | 400 |  | Substantial |[ ]
| CBA (Certificate Based Authenticatie) | urn:be:vlaanderen:authmech:tlsclient | 19 | NVT |  | NVT |[ ]
| Alfa-windows-account \*\* | urn:be:vlaanderen:authmech:kerberos | 12 | NVT |  | NVT |[ ]
| LeerID | urn:be:vlaanderen:authmech:leerid | 10 | NVT |  | NVT |[ ]

\* Dit is het minimale authenticatie level dat aanvaard zal worden voor authenticaties die via single sign-on via CSAM binnen komen.

\*\* Het Kerberos authenticatiemiddel kan in T&I enkel gebruikt worden vanop een PC die gekoppeld is aan het TIALFA-domein en door een gebruiker die gekend is in het TIALFA-domein.

\*\*\* Er dient slechts één keuze gemaakt te worden die het minimum level bepaalt. De keuze houdt impliciet in dat Eidas authenticatiemiddelen met een hogere level ook getoond worden.

Mogelijke BRONNEN: IDD, AD, CLDAP, SSM, BTB, KBO, LeerID, OV Personeelslid API, MBP

|  |
| --- |
| 2.5 Uitgeleverde attributen/scopes |
| **OpenID Connect** |  |
| **Attribuutnaam** | **BRON** | **Attribuut ID** | **scope**  | **claim** | **Doelgroep** |
|  |  |  |  |  |  **GID** | **EA** | **LB** | **OV** | **BUR** | **LLN** |
| **Verplichte scope** |  |  | openid | <n.v.t.> |  |  |  |  |  |  |
| PersoonsID\*\* |  | **<N/A>** | openid | sub |[ ] [ ] [ ] [ ] [x]   |
| VOID | IDD | Vo-idv | vo | vo\_id |[ ] [ ] [ ] [ ]   |  |
| Rijksregisternummer | IDD | vo-pn | rrn | rrn |[ ] [ ] [ ] [ ] [x]   |
| Organisatiecode\* | IDD | vo-org-code | vo | vo\_orgcode |[ ] [ ] [ ] [ ]   |  |
| Organisatienaam\* | IDD | vo-org-naam | vo | vo\_orgnaam |[ ] [ ] [ ] [ ]   |  |
| Doelgroepcode | IDD | vo-doelgroepcode | vo | vo\_doelgroepcode |[ ] [ ] [ ] [ ] [ ]   |
| Doelgroepnaam | IDD | vo-doelgroepnaam | vo | vo\_doelgroepnaam |[ ] [ ] [ ] [ ] [ ]   |
| Taalkeuze | IDD | **<N/A>** | vo | vo\_taalkeuze |[ ] [ ] [ ] [ ] [ ]   |
| Voornaam | IDD | vo-voornaam | profile | given\_name |[ ] [ ] [ ] [ ] [ ]   |
| Familienaam | IDD | sn | profile | family\_name |[ ] [ ] [ ] [ ] [ ]   |
| Emailadres | IDD | vo-email | vo | vo\_email |[ ] [ ] [ ] [ ]   |  |
| Rolleninformatie | IDD | **federatie-applicatiexxx-applicatiedata** | <organisatie\_applicatie> | <organisatie\_applicatie\_rol\_1/2/3d> |[ ] [ ] [ ] [ ]   |  |
| SOLID |
| SOLID WebID\*\*\*\*\*\* | MBP |  | webid | webid |[ ] [ ] [ ] [ ] [x]   |

\* Niet uitleverbaar bij doelgroepniveau authenticatie.

\*\* De persoonsID is een unieke identifier die een gebruiker uniek identificeert: eenzelfde natuurlijk persoon heeft steeds dezelfde identifier over doelgroepen en/of toepassingen heen.

\*\*\* NOT\_FOUND indien geen mandaat // in geval men via mandaat werkt, wordt er geen doelgroepcode meegegeven. De doelgroepcode is niet in alle use cases eenduidig beschikbaar, vandaar. // In geval men via mandaat werkt, wordt er niet aangegeven of de mandaatnemer via Wettelijk Vertegenwoordiger of via IDD binnen kwam.

\*\*\*\* Deze attributen kunnen enkel uitgeleverd worden als Departement Onderwijs & Vorming gevalideerd heeft dat de toepassing mag intekenen op de Personeelslid API OV/LeerID.

\*\*\*\*\* De attributen uitgeleverd onder inschrijving hebben een Base64 encoded JSON-array structuur: “{ [ {“ov\_orgcode”: “xxxxxx”, “claim”: “xxxxxx”} ] }”

\*\*\*\*\*\* Dit is een unieke Identifier die wordt uitgeleverd door Mijn Burgerprofiel. Dit is een url die verwijst naar de unieke solidkluis

# 7. Nuttige links ACM/IDM-integraties

|  |
| --- |
| 7.1 Overzicht documentatie |
| **Onderwerp** | **Beschrijving** | **Handleidingen en Documentatie** |
| **Algemene informatie** |  |
| [Veiligheidsbouwstenen](https://www.vlaanderen.be/digitaal-vlaanderen/onze-oplossingen/informatieveiligheid-en-veiligheidsdiensten) | Overzichtelijke website die het startpunt vormt om het aanbod van veiligheidsbouwstenen te ontdekken. | [Publieke documentatie van alle veilgheidsbouwstenen](https://confluence.voalm.vlaanderen.be/display/GAEP/Applicatie-%2Ben%2BPlatformdiensten) |
| [Gebruikersbeheer (IDM)](https://www.vlaanderen.be/digitaal-vlaanderen/gebruikers-en-rechten-tot-je-digitale-toepassingen-beheren) | Overzichtelijke website met allerlei informatie rond de toepassing gebruikersbeheer (IDM3) met o.a. een overzicht met instructievideo’s over de verschillende mogelijke acties in IDM3: hoe zet ik een werkrelatie op, hoe voeg ik een gebruiker toe, hoe ken ik een recht toe, etc. (zie ook tabje ‘praktisch’). | [Documentatie en handleidingen van het Gebruikersbeheer](https://confluence.voalm.vlaanderen.be/pages/viewpage.action?pageId=22970408) |
| [Toegangsbeheer](https://www.vlaanderen.be/toegangsbeheer) [(ACM)](https://authenticatie.vlaanderen.be/docs/beveiligen-van-toepassingen/integratie-methoden/oidc/technische-info/client-authenticatie/) | Overzichtelijke website met allerlei informatie rond de toepassing toegangsbeheer (ACM) met o.a. een overzicht hoe te koppelen op gebruikers- en toegangsbeheer, de verschillende authenticatiemiddelen, etc. (zie ook tabje ‘praktisch’). | [Technische documentatie van het ACM platform](https://authenticatie.vlaanderen.be/)  |
| [Standaard aansluitingsproces](https://www.vlaanderen.be/acm-idm-standaard-aansluitingsproces) | Geeft een overzicht over een standaardintegratietraject met ACM/IDM. |  |
| [Publicaties Toegans- en Gebruikersbeheer](https://overheid.vlaanderen.be/publicaties-toegangs-en-gebruikersbeheer) | Hier vind je algemene presentaties over onze dienstverlening maar ook specifieke presentaties over Gebruikersbeheer, Mandaten en Toegangsbeheer (o.a. technische documentatie beveiligen API’s en Toepassingen). |  |
| [Incidenten en Servicebeheer](https://confluence.voalm.vlaanderen.be/display/GAEP/Incidenten-%2Ben%2BServicebeheer) | Meer uitleg over incidenten en Servicebeheer. |  |
| **Basispresentaties specifieke doelgroepen** |  |
| [Basispresentatie Lokale Besturen](https://www.vlaanderen.be/digitaal-vlaanderen/informatieveiligheid-voor-lokale-besturen) | Geeft een voor Lokale Besturen op maat gemaakte introductie in Gebruikers- en Toegangsbeheer. |  |
| [Basispresentatie VO-entiteiten](https://www.vlaanderen.be/digitaal-vlaanderen/informatieveiligheid-voor-ambtenaren-van-de-vlaamse-overheid) | Geeft een voor VO-entiteiten op maat gemaakte introductie in Gebruikers- en Toegangsbeheer. |  |
| **Certificatenbeheer** |  |
| [Certificaten](https://www.vlaanderen.be/digitaal-vlaanderen/certificaten-beheren-voor-je-toepassingen-of-apis)  | Geeft informatie over aanvraag van certificaten voor SAML-integratie via VO-DCBaaS | [Documentatie rond het gebruik van het Certificatenbeheer](https://confluence.voalm.vlaanderen.be/pages/viewpage.action?pageId=28543801) |

# 8. Documenteigenschappen

|  |
| --- |
| 8.1 Auteurs |
| **Auteur:**  | Gilles de Schaetzen |
| **Functie:** | ACM-IDM Analist |
| **Contactgegevens:** | integraties@vlaanderen.be |

|  |
| --- |
| 8.2 Geschiedenis |
| **Versie** | **Datum** | **Auteur** | **Wijziging** | **Doc****validatie** |
| 0.1 | 27/11/2023 | Gilles de Schaetzen | Eerste opzet |[ ]
| 0.2 | 15/01/2025 | Frederik Byl | WE ARE TEMPLATE. |[ ]