Referentiearchitectuur IAM

Uitgegeven door: Politie | IV-organisatie | Dienst-ICT | IV Architectuur

Contactpersoon : 5.1.2.e

Telefoon: 06-5.1.2.e

Auteur: IDA/ADA IAM

Status: **Definitief**

30 september 2021 / versie 5.6

Rubricering: Politie Intern

Documentinformatie

De elektronische naam van dit document is: I130405 - Referentie architectuur IAM 5.6.docx

Documentstatus

Documentcode	Versie datum	Versie	5.6	Datum	30-09-2021
Onderwerp	Referentiearchitectuur IAM				
Status	**Definitief**				
Verantwoordelijke lijnmanager	5.1.2.e , 5.1.2.e				
Contactpersoon	5.1.2.e				
Auteur(s)	IDA/ADA IAM				

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
5.0	17 mei 2021	Dit document is een major update van het voorgaande document I130405 – Referentie architectuur 4.1. Het gehele document is zowel qua inhoud als structuur aangepast. Daarnaast is dit document een verdere uitwerking op basis van het IAM politie architectuur overview document. Dit laatste document moet gezien worden als het bovenliggende “paraplu” document.	Gehele document zowel qua inhoud als structuur.
5.1	01 juni 2021	Structuur verder aangepast en in lijn gebracht met de **Enterprisearchitectuur Informatiebeveiliging**	Structuur
5.2	18 juni 2021	Commentaar verwerkt 5.1.2.e , 5.1.2.e .	Diverse punten in het document
5.3	28 juni 2021	Commentaar verwerkt 5.1.2.e	Diverse punten in het document
5.3	20 juli 2021	Commentaar verwerkt IV Architectuur, 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e .	Diverse punten in het document
5.4	4 augustus 2021	Document klaar gemaakt voor ABI Klankbordgroep.	Diverse punten in het document

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
5.5	14 september 2021	Commentaar ABI klankbordgroep verwerkt. Figuur op pagina 15 aangepast deze werd verkeerd geïnterpreteerd.	Diverse punten in het document
5.6	30 september 2021	Laatste aangeleverde commentaar, van 5.1.2.e , 5.1.2.e en 5.1.2.e voor het ABI van september 2021 verwerkt en commentaar van het ABI(V) op 30 september verwerkt	TA-IAM-V15, TA-IAM-V16, TA-IAM-V17 & TA-IAM-V18

Afstemming

Versie	Datum RBR	Naam	Afdeling / Functie
5.1	4 juni 2021	5.1.2.e	IV-architectuur / Security architect
5.1	7 juni 2021	5.1.2.e	IV-architectuur / ICT architect
5.3	21 juli 2021	5.1.2.e	IV-architectuur / ICT architect
5.3	22 juli 2021	5.1.2.e	Infrabedrijf / Solution architect
5.3	22 juli 2021	5.1.2.e	IV-architectuur / ICT architect
5.3	23 juli 2021	5.1.2.e	IV-Architectuur / Enterprise architect
5.3	26 juli 2021	5.1.2.e	IV-architectuur / ICT architect
5.3	27 juli 2021	5.1.2.e	IV-architectuur / ICT architect
5.4	4 augustus 2021	5.1.2.e	Infrabedrijf / Solution architect
5.5	13 september 2021	5.1.2.e	Solution architect
5.5	27 september 2021	5.1.2.e	IV-architectuur / ICT architect
5.5	27 september 2021	5.1.2.e	IV-architectuur / ICT architect

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
5.1	03 juni 2021	IV-architectuur (5.1.2.e , 5.1.2.e , 5.1.2.e)	IV-architectuur / architectuur

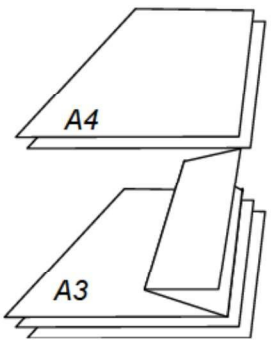
Versie	Verzend datum	Naam	Afdeling / Functie
5.1	12 mei 2021	5.1.2.e	IV-architectuur / architectuur
5.1	07 mei 2021	5.1.2.e	Infrabedrijf / Solutionarchitect
5.1	11 juni 2021	5.1.2.e	IV-architectuur / architectuur
5.2	18 juni 2021	IDA/ADA IAM en PTO IAMnV	Divers
5.3	20 juli 2021	IV-architectuur	IV-architectuur / architectuur
5.4	4 augustus 2021	ABI klankbordgroep	ABI Klankbordgroep

Dit document is vastgesteld door de volgende personen:

Naam	Vertegenwoordiging	Datum	Handtekening
ABI(V)	ABI(V)	30-09-2021	

Leeswijzer

Dit document bevat een aantal grote illustraties. Omwille van de leesbaarheid zijn deze opgenomen in secties die op A3 worden geprint. Wie dit document in papieren vorm wil lezen raden wij aan de A3-secties als volgt in het document op te nemen.



Figuur 1 Vouwwijze A3 secties

Voorwoord

Deze referentiearchitectuur IAM is een verdere uitwerking van IAM politie architectuur overview document. De referentiearchitectuur IAM geeft productonafhankelijke kaders en richtlijnen.

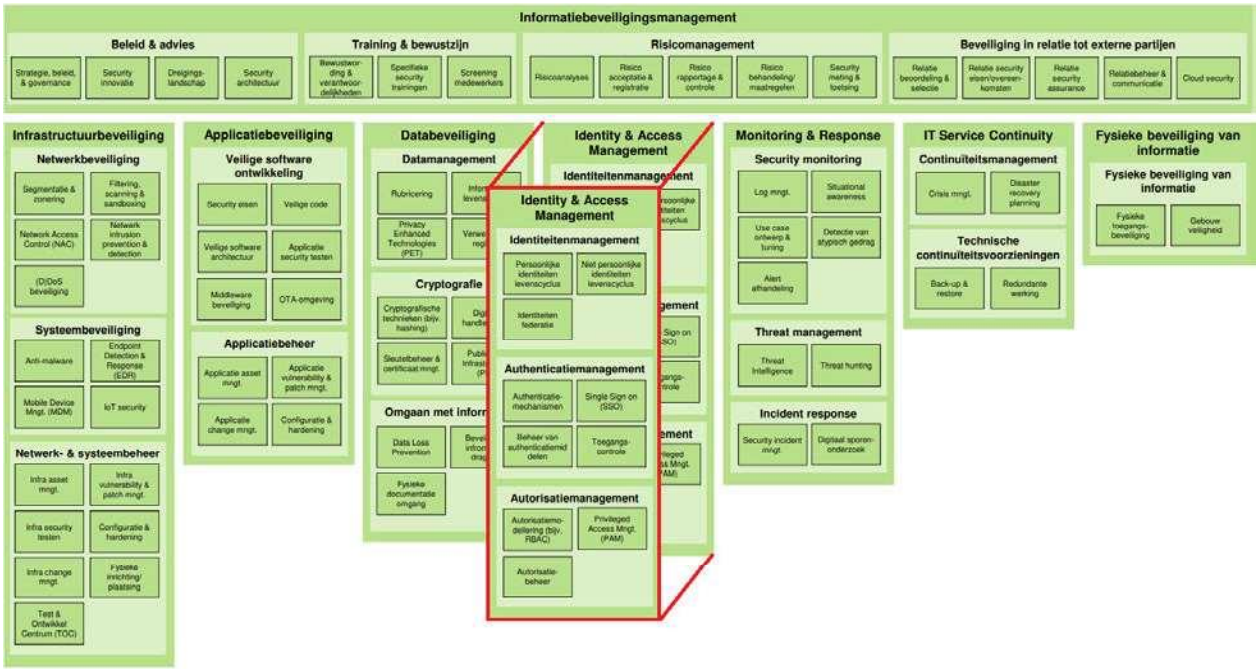
Het IAM-systeem is een complex systeem en bestaat uit diverse componenten en wordt gevoed door diverse bronsystemen en op basis hiervan voedt het continu de diverse doelsystemen. Het IAM-systeem wordt gefaseerd uitgebreid en aangepast omdat er diverse afhankelijkheden zijn, zowel in de huidige techniek (huidige situatie) als in de politieorganisatie (denk aan het verder uitwerken van een landelijk rollenmodel voor de Politie). Dit document wordt dan ook regelmatig herzien en geactualiseerd.

Het IAM-systeem wordt conform beveiligingsniveau politie intern gerubriceerd en ingericht.

In de referentiearchitectuur wordt eveneens stilgestaan bij de relatie met de IV Diensten Catalogus (IDC) en het productiehuis, één van de resources leverancier.

Het productiehuis is één van de leveranciers van apps/applicaties ook wel resources waarvoor autorisaties gerealiseerd moeten worden door middel van IAM. Maar denk ook aan resources die afgenomen worden in de (public) Cloud en resources die aangeboden worden aan derden en vertrouwde partijen.

De IAM referentie architectuur is gepositioneerd in het security gedeelte van IV architectuur. En geeft een verdiepingsslag op het gedeelte Identity & Access Management welke behandeld wordt in dit document.



Inhoudsopgave

1 Inleiding

1.1 Definitie IAM

Identity en Access Management (IAM) is de beveiligingsdiscipline waarmee de juiste personen en geautomatiseerde processen toegang tot de juiste functionaliteiten met bijbehorende gegevens op het juiste moment om de juiste redenen krijgen.

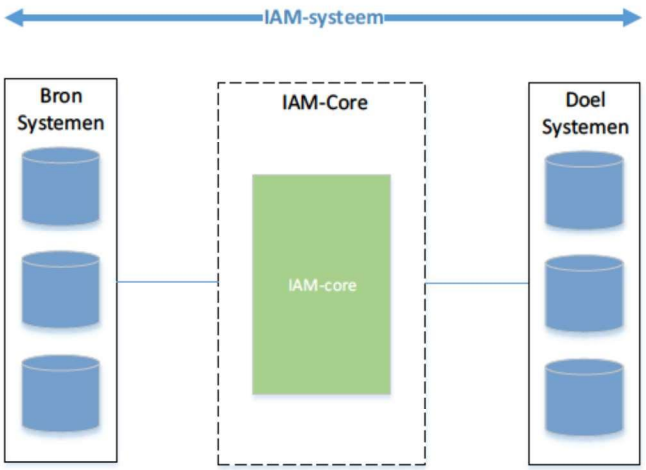
In het document wordt de volgende terminologie gebruikt zie onderstaan figuur:

IAM-systeem bestaat uit:

- Bronsystemen
- IAM-Core
- Doelsystemen

IAM-core bestaat weer uit een aantal componenten:

- Identity repository,
- autorisatie service,
- IAM-policy,
- IAM-role,
- IAM group.



1.2 Doelgroep

De doelgroep voor dit document zijn solution architecten, business/product owners, applicatie ontwikkelaars het SOC, VIK en (IT-)beheerders.

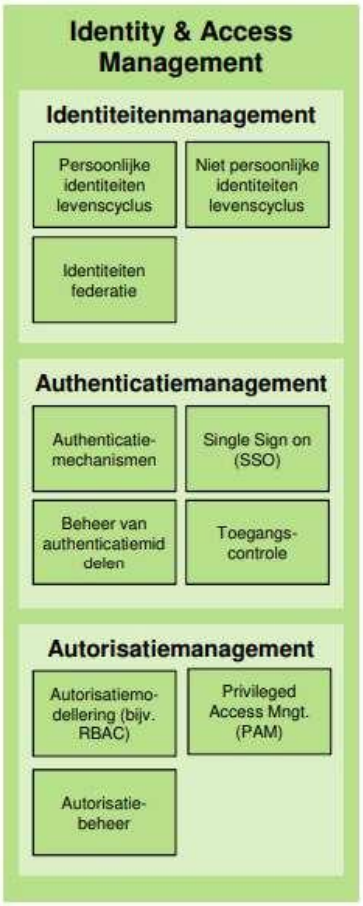
1.3 Brondocumenten

Bij het opstellen van deze referentiearchitectuur zijn de volgende bronnen en referenties gebruikt:

Bronspecificatie
[1] Enterprisearchitectuur Informatiebeveiliging
[2] Baseline Informatiebeveiliging Overheid (BIO)
[3] BIO Addendum: Politie-specifieke maatregelen
[4] IAM politie architectuur overview
[5] Deelarchitectuur Autorisatiemanagement
[6] 181002 - technische referentie architectuur API Management
[7] I210702 – Referentiearchitectuur PAM

1.4 Opbouw document

De IAM referentie architectuur is gepositioneerd in het security gedeelte van IV architectuur. En geeft een verdiepingsslag op het gedeelte Identity & Access Management.



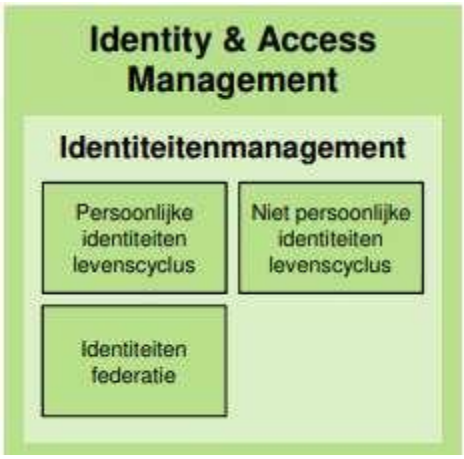
In het figuur hiernaast weergegeven. Alle genoemde componenten worden behandeld in dit document (of er wordt verwezen naar onderliggende documenten).

Het document is als volgt opgebouwd:

- Paragraaf 2 beschrijft Identiteitenmanagement, in de vorm van doelstelling, functionele omschrijving, technische omschrijving, maar ook persoonlijke, niet-persoonlijke en federatieve identiteiten.
- Paragraaf 3 geeft een overzicht van authenticatiemanagement, de bronsystemen van IAM en de daarbij behorende authenticatie mechanismen, SSO enz. in de vorm van o.a. aansluitvoorwaarden.
- In paragraaf 4 worden de componenten van identiteiten-, authenticatie en autorisatiemanagement behandeld. En wordt er een overzicht gegeven uit welke componenten deze bestaat.
- Paragraaf 5 behandelt autorisatiemanagement van de doelsystemen (zoals Privileged Access Management) van IAM en de daarbij behorende aansluitvoorwaarden.
- Paragraaf 6 gaat in op federatie. De paragraaf geeft meer diepgang over het Federatie deel van Identity & Access Management o.a. ook dat van Identiteiten.
- In paragraaf 7 worden de principes van IAM weergegeven.

2 Identiteitenmanagement

2.1 Doelstelling



Identiteitenmanagement: het vaststellen van de identiteiten en de daarbij behorende identiteitskenmerken zoals autorisatierollen en groepsrollen (R2D2). Alles wat over een gebruiker bekend moet zijn om de gebruiker te kunnen authentiseren en autoriseren. Zekerheid over een identiteit is de start van diverse processen.

Eén van deze processen is om zo efficiënt mogelijk gebruikersaccounts te kunnen autoriseren en de-autoriseren voor vooraf gedefinieerde functionaliteit voor de betreffende personen en/of doelgroepen, waarin SSO (middels open standaarden) en RBAC en ABAC (middels gedefinieerde privileges) worden ondersteund.

2.2 Functionele omschrijving

Om Identity en Access management goed te kunnen implementeren is niet alleen de ICT infrastructuur benodigd, maar ook de processen, die nodig zijn om het geheel goed werkend te krijgen. Deze processen komen uit hoger liggende architecturen, Business- en Informatiearchitectuur.

Identity en Access Management, afgekort IAM, is te beschouwen als een systeem (=IAM-systeem) waarbij er logisch centraal identiteitsgegevens worden beheerd en er één logische centrale toegangscontrole[1] is.

Bij het benaderen door een gebruiker van een systeem/applicatie wordt er een controle uitgevoerd.

Elk moment, dat er een controle wordt uitgevoerd op de ID (authenticatie) en autorisatie vraagt het doel-systeem/applicatie dit op bij IAM-core. IAM-core antwoordt met Ja of Nee en regelt eventueel een hoger liggende authenticatie, door bijvoorbeeld een token te vragen en daarna alsnog een Ja of Nee af te geven.

IAM-core wordt o.a. gevoed door de bron-systemen vanuit het HRM-systeem, partners enz.

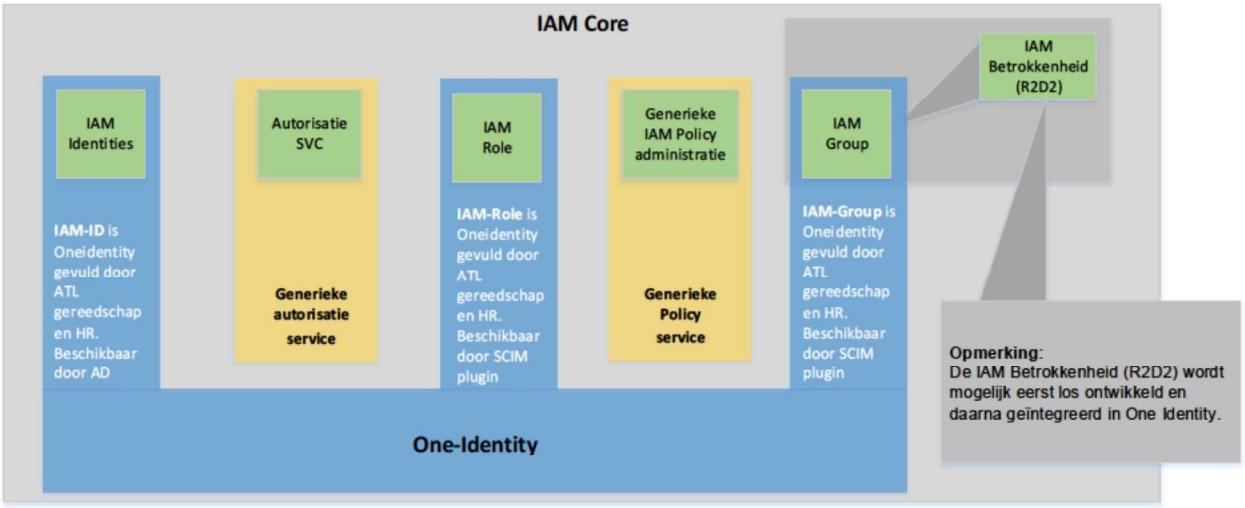
IAM-core bestaat uit verschillende processen en componenten:

- Identificatie en authenticatie (IAM Identities), ofwel het geheel rond de identiteit van een entiteit[2] en de mate van authenticiteit van deze entiteit en richt zich op begrippen als gebruikersnamen, wachtwoorden, aanmeldproces, tokens, etc.
    - Identity Repository ofwel de database waarin de identiteiten, inclusief relevante informatie, worden opgeslagen (lees logisch centraal worden opgeslagen). In de IV-organisatie van de politie wordt de AD hiervoor gebruikt, soms is het in de applicaties zelf ingebouwd.

[1] Er is één bron voor toegang (access) en dat is het IAM-systeem.

[2] Entiteit iets wat wezenlijk bestaat, *(informatica)* een mens, dier of ding waaraan men eigenschappen kan toekennen (attributen) en waarvan deze informatie kan worden opgeslagen b.v. in tabellen

- Autorisatie (autorisatie SVC, IAM role, generieke IAM policy administratie), een aan het geheel rond de identiteit verleend bevoegdheid tot het uitvoeren van een actie op een IT-middel (object). [bron: IB-patronen PvIB].
- Provisioning (IAM groep, IAM betrokkenheid), het geautomatiseerd doorgeven van nieuwe, gewijzigde en verwijderde identiteitsgegevens, vaak inclusief authenticatiegegevens, naar applicaties en diensten met het doel efficiënt en consistent gebruikersbeheer te bewerkstelligen
- Federatie. Het Centraal Netwerkportaal wordt gebruikt voor het gecontroleerd koppelen van partners op IAM-core. Het IAM-systeem fungeert dan als een federatieve oplossing. Voor verder uitwerking en toelichting zie paragraaf 6.



Figuur IAM Core Nationale Politie

Voor meer toelichting hier voor zie document IAM politie architectuur overview.

2.3 Uitgangspunten identiteiten en authenticatiemanagement

De volgende (technische) uitgangspunten moeten gehanteerd worden bij het IAM-systeem:

Uitgangs-punt	Omschrijving
U1.	Er moet gebruik gemaakt worden van gedeelde infrastructurele resources en dus niet zoals in het verleden veelal het geval was de infrastructuur inrichten per projectoplossing en/of applicatieoplossing.
U2.	IAM-core is de single point of truth, voor Identity en Access management.
U3.	IAM-core levert de gegevens voor de ID en access repository, dit wordt gerealiseerd in de landelijke LDAP directory.
U4.	Koppelen met IAM-core geschiedt conform de aansluitvoorwaarden. Dit geldt voor zowel voor SaaS, COTS (Commercial off-the-shelf) als Maatwerk/zelfbouw (eigen gebouwde applicaties/toepassingen), zie hoofdstuk 3.2 aansluitvoorwaarden.
U5.	Koppelen met IAM-core geschiedt op basis van open standaarden en protocollen (OpenID Connect, Oauth en SCIM) en middels de privileges API. Directe LDAP queries en ander maatwerk in de koppeling(en) met IAM-core moet vermeden worden, aangezien anders de complexiteit toeneemt en de beheerbaarheid afneemt. Daarnaast heeft het impact op de life-cycle van het IAM systeem aangezien een nieuwe versie van het product impact kan hebben op de maatwerk koppeling.

Uitgangs-punt	Omschrijving
	De applicatie die zich niet kan conformeren moet zelf een oplossing maken en beheren, buiten IAM.
U6.	De IAM core bevat 1. de gebruikersrepository (IGA, Identity Governance en Administration). De Identity governance en administration component 2. de Authorisation server dat onderdeel is van de API GW suite van de Nationale Politie en een vertrouwenskoppeling met haar keten partners (API Gateway). Deze koppeling wordt via de authorisation server in de API GW suite ter beschikking gesteld. De authorisation server stelt IAM ID en IAM Role informatie ter beschikking via API's maar bevat zelf geen gegevens. M.a.w. de RBAC gegevens. Voor rol-gebaseerde en attribuut-gebaseerde toegang wordt gebruik gemaakt van de standaard autorisatiekenmerken (zoals verwerkingsdoel, verwerkingssubdoel, werkgebied, deelbaarheid, status en rubriceringsniveau). Indien in IAM maatwerk wordt opgenomen voor applicaties van de nationale politie dan heeft dit negatief effect op complexiteit en beheerbaarheid. *De applicatie die zich niet kan conformeren moet zelf een oplossing maken en beheren, buiten IAM.*
U7.	Voor de politie wordt er gekoppeld met het BVI-BV systeem, niet met elke bestaande individuele (HR) omgeving.
U8.	Het IAM-systeem is gerubriceerd conform het politie intern beveiligingsniveau.
U9.	SSO (Single Sign-On) wordt alleen geboden als er aan de aansluitvoorwaarden is voldaan en de te ontsluiten applicatie gekoppeld is aan IAM-core[3] (zowel voor politie als ketenpartners).
U10.	Self-service voor eindgebruikers in de vorm van; bijvoorbeeld wachtwoord resets wordt alleen geboden wanneer er gekoppeld is met en gebruik gemaakt wordt van IAM-core en er volledig is voldaan aan de IAM aansluitvoorwaarden door de te koppelen partij/partner.
U11.	De gegevens in de bronsystemen zijn leidend, de registraties bevatten de gegevens zodat deze door de ICT-omgeving gebruikt kunnen worden.
U12.	Applicatie specifieke rollen worden gefaciliteerd vanuit de Webshop van IAM-core ook wel de ATL tool genoemd (Autorisatie Tool Leidinggevenden).
U13.	De aansturing van IAM moet niet vanuit de techniek gebeuren, maar vanuit de business in samenspraak met techniek.

Toelichting U.6:

IAM-core bevat naast de gebruikersrepository van de Nationale Politie ook een aparte LDAP repository voor niet-politie gebruikers. Bij deze aparte repository voor niet-politie gebruikers moet er gedacht worden aan ketenpartners uit het PODACS regelement die hun identiteit nog niet kunnen aanleveren conform de aansluitvoorwaarden. Daarnaast moet dit ook geregeld worden voor partijen/derden (o.a. schoonmakers) die toegang moeten hebben tot de gebouwen van de politie.

[3] IAM core omvat alle componenten zoals weergegeven in figuur **IAM core Nationale Politie**

2.4 Persoonlijke identiteiten

Er kunnen meerdere systemen zijn van waaruit het verzoek kan komen om een digitale identiteit op te voeren, te veranderen of te verwijderen. Voor politiemedewerkers is dit BVI-BV, echter voor externe inhuur (niet-politie) wordt een apart systeem gebruikt. In IAM-core geldt als regel[4] dat er per natuurlijk persoon slechts één digitale entiteit in de identity repository staat.

Opnamevoorwaarden:

1. Persoonsgegevens worden aangeleverd via een daartoe aangewezen bron.
2. Persoonsgegevens kunnen ook aangeleverd worden door een daartoe geautoriseerde persoon
3. Van een toe te voegen persoon worden minimaal volgende gegevens opgegeven:
    1. Voornaam
    2. Achternaam
    3. Tussenvoegsel
    4. Identiteitsnummer in bronsysteem
    5. email
    6. Startdatum, wijzigings- of einddatum
4. Leidinggevende (iemand die voorkomt in de Identity Repository)
5. Rol(len)
6. Screening en competenties[5]

Binnen de politie zijn de volgende bronsystemen gedefinieerd voor IAM-core:

- HRM systeem (Beaufort)
- Youforce
- Widscan
- Osiris (HRM systeem van Politie Academie)
- BVI-BV (Basis Voorziening Informatie – BedrijfsVoering)
- Webshop (voorheen ATL[6])
- Federatie (voor het autoriseren van ketenpartners en derden)

2.5 Niet-Persoonlijke identiteiten

Voor niet-persoonlijke identiteiten wordt een apart proces gehanteerd binnen de IAM-core. Ook deze niet-persoonlijke accounts worden gefaciliteerd door IAM dat wil zeggen “automatisch” aangemaakt. Dit wordt gerealiseerd door voor elke doelgroep van gerechtige personen (lees beheerders, applicatie eigenaar/verantwoordelijken, functionele beheerders) een webshop aan te bieden waarin ze een niet-persoonlijk account kunnen aanmaken.

Hiervoor zijn de volgende randvoorwaarden van toepassing:

Nr.	Randvoorwaarde
R1.	Voor elke doelgroep moet in de Active Directory omgeving een landingsplaats gecreëerd worden. Denk hierbij aan een OU structuur en groepsstructuur waar deze niet persoonlijke accounts in geplaatst kunnen worden met bij behorende bevoegdheden.

[4] Van deze regel mag afgeweken worden, indien medewerkers twee verschillende functies hebben, zoals bijvoorbeeld een Dienst ICT medewerker die ook politievrijwilliger is. Omdat dit twee identiteiten zijn, met aan elke identiteit verschillende autorisatierollen en dus bevoegdheden.

[5] Screening en competenties is als functionele eis gesteld door de business.

[6] ATL = Autorisatie Tool Leidinggevende

Nr.	Randvoorwaarde
R2.	Er moeten per doelgroep eigenaren/verantwoordelijken aangewezen worden, natuurlijke personen die het “recht” hebben om deze niet-persoonlijke accounts aan te maken.
R3.	Bij niet-persoonlijke accounts waarbij bevoegdheden noodzakelijk zijn waarbij de productieomgeving beïnvloed kan worden moet er een 4-ogen principe worden toegepast. Dat wil zeggen dat een 2e natuurlijk persoon in het proces ook een akkoord moet geven voordat het niet-persoonlijke account wordt aangemaakt.
R4.	Life-cycle van het niet-persoonlijke account moet geborgd worden. Dat wil zeggen dat er o.a. per niet-persoonlijk account een periode aangegeven moet worden waarin het niet-persoonlijk account actief moet zijn. Dit kan zijn een vastgestelde of onbeperkte periode. Hierbij moet door de eigenaar/verantwoordelijke aangegeven worden: - waarvoor het niet-persoonlijke account gebruikt wordt - de periode waarin het niet-persoonlijke account (denk hierbij ook aan automation) actief moet zijn - onderbouwing van de periode - voordat de periode verstrijkt moet de eigenaar/verantwoordelijke op de hoogte gebracht worden (b.v. via mail) zodat deze eventueel (onderbouwd) verlengd kan worden
R5.	Het rouleren van wachtwoorden en/of andere secrets van deze niet persoonlijke accounts moet ondergebracht worden onder PAM[7], zie paragraaf 5.7.
R6.	Voor elke doelgroep moet een webshop beschikbaar worden gesteld, conform de genoemde randvoorwaarden
R7.	Het wachtwoordenbeleid voor service accounts is van toepassing, zoals verwoord in het wachtwoordbeleid.

Onder niet-persoonlijke accounts worden de volgende accounts bedoeld:

- Functionele (applicatie) accounts
- Systeem (o.a. local admin accounts) & applicativeaccounts / OAuth 2.0 client identifiers
- Automation accounts
- Testaccounts
- Accounts voor heimelijken (Door een aanpassing vooraf (Beaufort - BVI-BV) wordt een heimelijken account als normaal account aangeleverd.)

Systeem & applicatieaccounts zijn specifieke accounts (niet-natuurlijke gebruikersaccounts) om het systeem of de applicatie te laten functioneren.

2.6 Federatieve identiteiten

Zie voor federatie en federatieve identiteiten paragraaf 6.

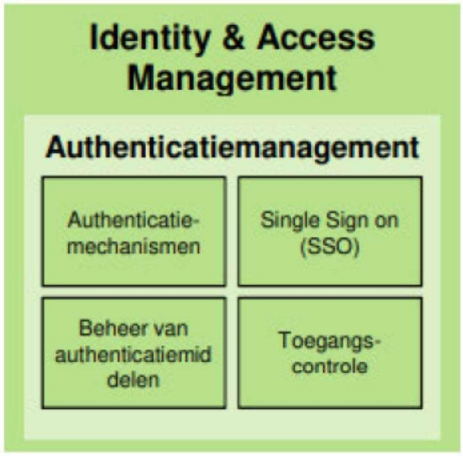
[7] PAM: Privileged Access Management.

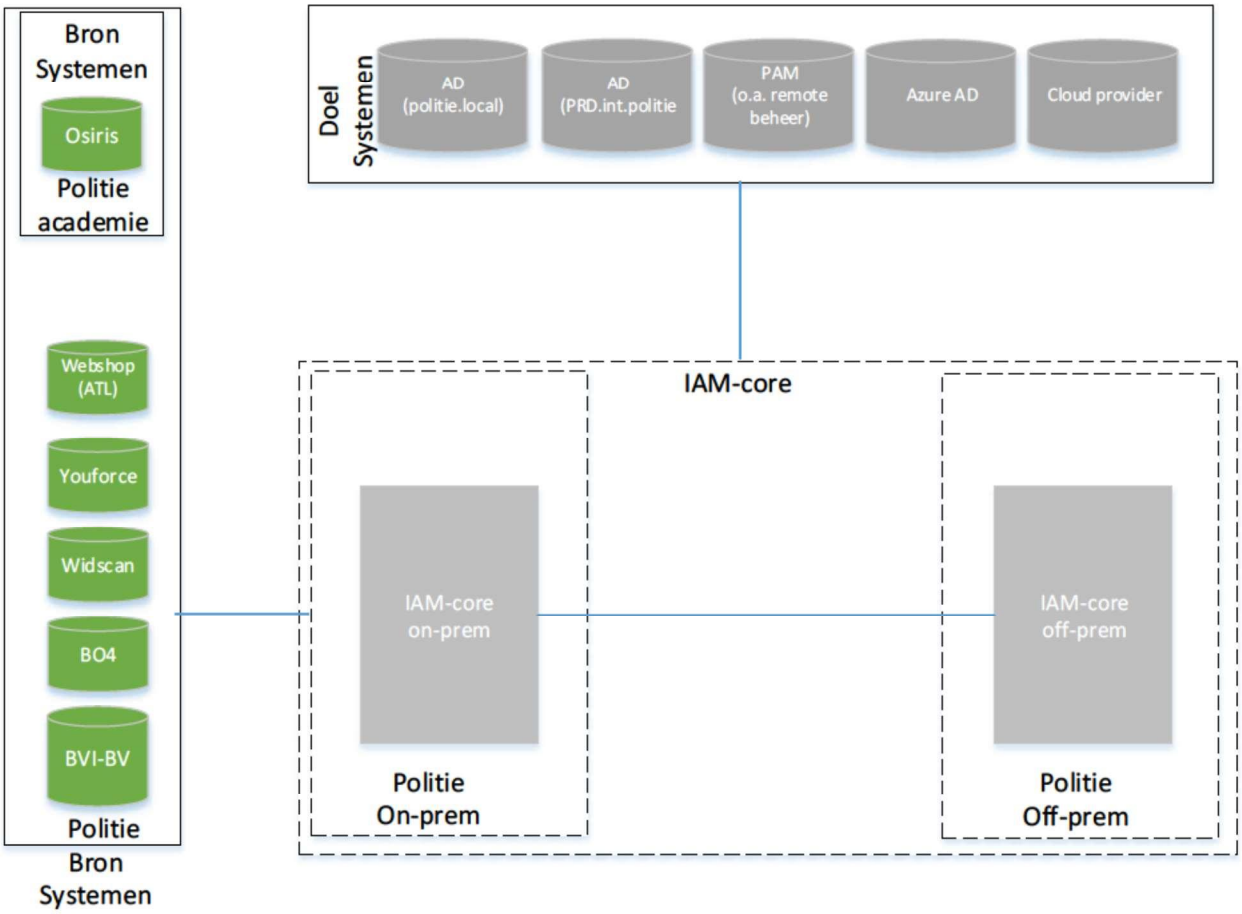
3 Authenticatiemanagement

3.1 Overzicht

Authenticatie management wordt in de eerste fase gerealiseerd door het vaststellen van de identiteiten en de daarbij behorende identiteitskenmerken. De identiteiten en identiteitskenmerken worden aangeleverd door bronsystemen.
Voor de politie worden de bronsystemen gebruikt zoals vermeld in paragraaf 2.4.

Zie hiervoor deelarchitectuur Authenticatiemanagement en gebaseerd op het landelijk autorisatiemodel.





IAM-core bronsystemen

3.2 Aansluitvoorwaarden

De hieronder genoemde aansluitvoorwaarden zijn van toepassing voor Bron naar IAM-core (kern) zowel COTS-producten als maatwerkproducten. Indien er niet voldaan wordt aan de aansluitvoorwaarden dan wordt er niet gekoppeld aan IAM-core. De bron wordt dan niet gekoppeld waardoor de bron IAM functionaliteit zelf moet regelen, beheren en onderhouden.

Opmerking:
Indien de COTS applicatie niet voldoet maar dit toch een eis is van de organisatie dan dient dit apart te worden opgepakt. Dit wordt dan uitgewerkt in een apart document (risicoanalyse) waarin de consequenties en gevolgen voor zowel techniek als organisatie duidelijk geadresseerd worden.

De applicatie bevindt zich in dat geval in een sterfhuisconstructie, totdat er een nieuwe applicatie is gebouwd of gekocht (conform uitgangspunten en aansluitvoorwaarden).

3.2.1 Aansluitvoorwaarden Bronsystemen en IAM Core

Nr.	Aansluitvoorwaarde
BC1.	Koppeling is op basis van open standaarden[8], standaard protocollen en uitwisselingsmechanismes. In paragraaf 5 wordt aangegeven van welke standaarden er gebruik gemaakt wordt.
BC2.	De database providers die door IAM-core worden ondersteund zijn; • ODBC Data Provider [tbv bronsystemen] • OleDbData provider [tbv bronsystemen] • OracleClient Data Provider [tbv bronsystemen] • SQL Client Data Provider [tbv bronsystemen] • dotConnector Oracle [tbv bronsystemen] • Microsoft SQL Server Compact data Provider [tbv bronsystemen]
BC3.	Bestaande en/of lokale ID-repositories, voor applicatie- en functioneel beheer, moeten zijn opgenomen in centrale ID-repository.
BC4.	Het IAM-core maakt geen gebruik van CSV bestanden bij het overhalen van brongegevens maar koppelt direct op het betreffende bronsysteem.
BC5.	De koppeling tussen IAM-core en het bronsysteem moet “real-time” of “near real-time” gerealiseerd worden, dit in verband met de IDU (InDienst, Uitdienst) processen. Vertragingen in de communicatie tussen bronsysteem en IAM-core kan grote gevolgen hebben.
BC6.	Van de koppeling tussen bronsysteem en IAM-core is het bronsysteem altijd de initiator, aangezien bij het bronsysteem de wijzigingen plaats vinden.

[8] Open standaarden zie URL: Forum standaardisatie

3.2.2 Aansluitvoorwaarden Doelsystemen en IAM Core

Nr.	Aansluitvoorwaarde
DC1.	De applicatie & bronsystemen koppelen eenzijdig (single point of data exchange) aan de OAuth2 authorisation server t.b.v. authenticatie en de autorisatie API's t.b.v. autorisatie. Koppeling is op basis van open standaarden[9], standaard protocollen en uitwisselingsmechanismes, OpenID Connect (OIDC). In paragraaf 5 wordt aangegeven van welke standaarden er gebruik gemaakt wordt.
DC2.	De applicatie koppelt via op open standaarden gebaseerde API's (Userinfo, SCIM en privileges API's) aan één ID-repository welke gevoed wordt door IAM-core
DC3.	Applicaties maken eenduidig gebruik van de centrale identity gegevensset (LDAP veldnamen) welke vanuit IAM (centrale ID-repository van de politie of ketenpartners) wordt aangeboden. Applicaties krijgen alleen leesrechten op de centrale ID gegevensset. Bij voorkeur via een API gebaseerd op open standaarden, zoals SCIM[10]. Het initiatief is telkens bij het doelsysteem om de informatie te halen.
DC4.	Mutaties van IAM gegevens worden alleen gedaan vanuit de IAM (beheer)tooling. Self-service voor gebruikersbeheer vanuit applicaties is in strikte gevallen mogelijk, namelijk via de SCIM interface mogen applicaties buiten de IAM-Core aanpassingen doen aan de betrokkenheid (IAM Group) gegevens die zij zelf in beheer hebben.
DC5.	Autorisaties zijn op basis van RBAC en/of ABAC waarbij de rollen in de applicatie (bij voorkeur 1 op 1) matchen met op de rollen in IAM. De applicatierollen zijn gekoppeld met één of meerdere privileges (permissies) in de vorm van combinaties van o.a. attributen.
DC6.	Logging betreffende mutaties in IAM-core (denk hierbij aan Rol wijziging) worden doorgestuurd en verwerkt in de centrale logging en auditing service (LaaS).

[9] Open standaarden zie URL: http://www.forumstandaardisatie.nl/open-standaarden/

[10] SCIM; System Cross domain Identity Management. Meer informatie : https://en.wikipedia.org/wiki/System_for_Cross-domain_Identity_Management

4 Componenten identiteiten authenticatie en autorisatie

4.1 Overzicht

IAM core bestaat uit de volgende componenten:

Nr	IAM Core component	Omschrijving
1	IAM-ID	**IAM-Identity** is het product Oneidentity gevuld door ATL[11] gereedschap en HR. Beschikbaar gemaakt door de Active Directory van de Politie.
2	Autorisatieservice Politie	**Autorisatieservice Politie.** Dit is een generieke dienst voor autorisatiebeslissingen waarvan de toepassingen gebruik maken en heeft o.a. een relatie met de API-GW. Momenteel is dit in onderzoek door het productiehuis.
3	IAM Role	**IAM-Role** is One-identity gevuld door ATL (Autorisatie Tool Leidinggevende), ook wel WebShop genoemd en HR (BO4). Beschikbaar door SCIM plugin.
4	Generieke IAM Policy administratie	**Generieke IAM Policy administratie** heeft vooral als "rol" om bij te houden wat de inhoud is van de autorisatiematrix Politie. Het is als register bevraagbaar door de autorisatieservice Politie. De autorisatieservice Politie handelt autorisatieverzoeken af op basis van de inhoud van de autorisatiematrix Politie en de autorisatieregels in het autorisatiemodel Politie. Generieke IAM Policy administratie is een IAM component welke momenteel (Q1 2021) nog in onderzoek fase. Er wordt gekeken naar Open source producten zoals Open Policy Agent.
5	IAM group	**IAM-Group** zijn varianten (IAM Role en IAM betrokkenheid) van hetzelfde thema: groepen en groepsrollen. Uiteindelijk is alleen IAM group nodig. One-identity gevuld door ATL (webshop) gereedschap, Active Directory (AD) en HR. Interactie met groepen zal plaatsvinden via de SCIM standaard.
6	IAM betrokkenheid (R2D2)[12]	**IAM Betrokkenheid (R2D2)**. IAM betrokkenheid is het IAM component voor het centraal administreren van attribuut gebaseerde autorisaties. De betrokkenheidsadministratie wordt

[11] ATL is een tool waarbij een leidinggevende buiten de standaard autorisatieprofielen om rechten kan uitdelen aan gebruikers (herleidbaar) en dit wordt vastgelegd in de AD.

[12] **IAM Betrokkenheid**. Programma IAM heeft de opdracht voor een vooronderzoek. Hierbij moet een epic opgeleverd worden zodat het dev-ops team het kan bouwen (Bedrijfsvoering)

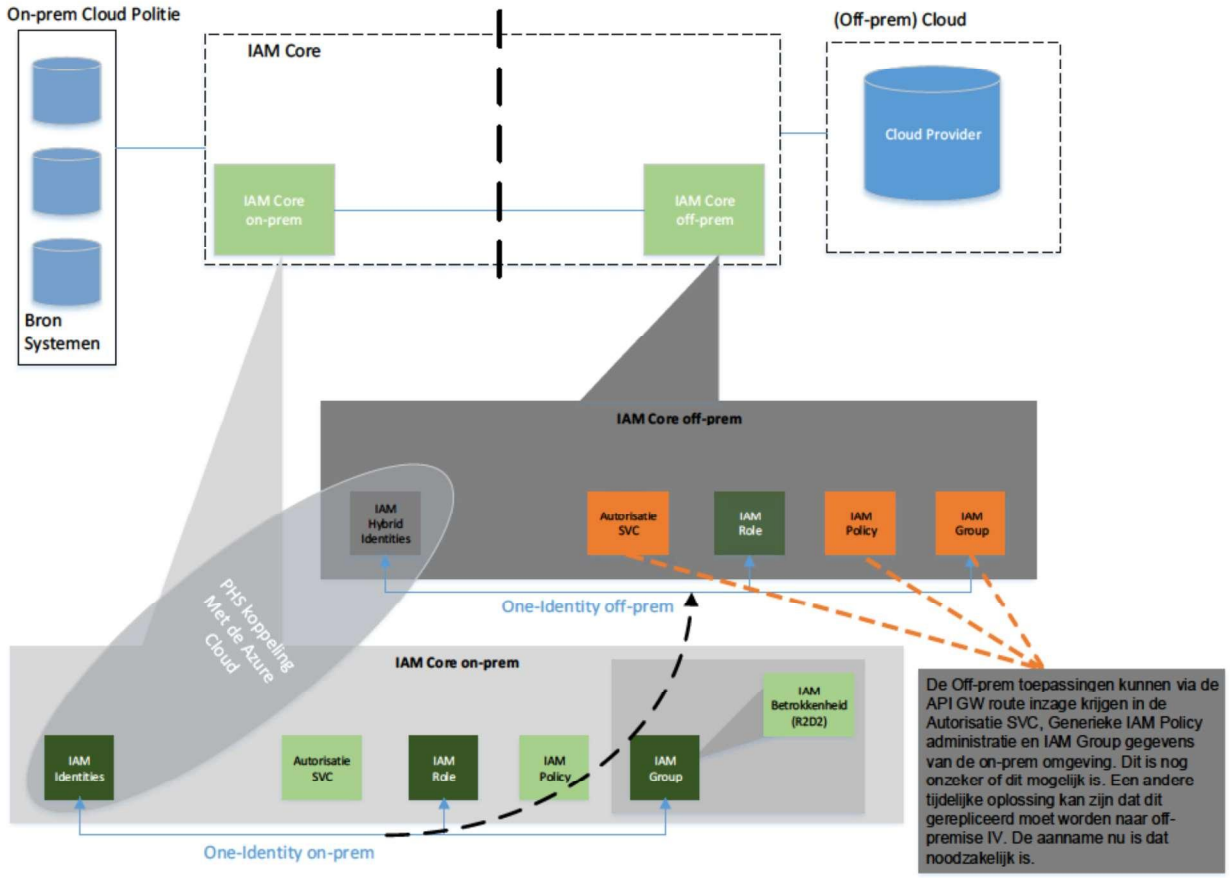
Nr	IAM Core component	Omschrijving
		door de Autorisatieservice Politie gebruikt voor het nemen van autorisatiebeslissingen op basis van de betrokkenheid van een gebruiker bij een registratie.

Opmerking:

De API GW (een doelsysteem) stelt in specifieke gevallen de IAM gegevens beschikbaar voor toepassingen/resoures.

De gegevens zijn de kern, zie Bestemmingsplan 2018 - 2022 Plangebieden en EA van de politie. Er wordt onderscheid[13] gemaakt tussen gegevens die noodzakelijk zijn binnen de on-prem politie cloud en de gegevens die noodzakelijk zijn voor gebruik binnen de off-prem politie cloud[14].
Dit omdat niet alle politiegegevens noodzakelijk zijn voor gebruik binnen de off-prem politie cloud, denk hierbij bijvoorbeeld aan AVG en WPG gegevens. Mede hierdoor wordt de IAM-core logisch opgedeeld in twee delen. Een IAM-core on-prem en een IAM-core off-prem. Dit is verder uitgewerkt in het document Cloud Services in samenwerking met One Identity Manager.

In onderstaande figuur is de IAM core off-prem in de Cloud o.a. weergegeven.



[13] Dit onderscheid wordt bepaald op basis van technische kaders en voorschriften.

[14] Principe " Dataminimalisatie vanuit de AVG" , zie ook het kader P&SbD

4.2 IAM Identity

IAM-Identity is het product Oneidentity gevuld door Webshop (ATL[15]) gereedschap en HR. Beschikbaar gemaakt door de Active Directory van de Politie.

4.3 IAM Role

IAM-Role is One-identity gevuld door ATL (Autorisatie Tool Leidinggevende), ook wel WebShop genoemd en HR (BO4). Beschikbaar door SCIM plugin.

4.4 IAM Group

IAM-Group zijn varianten (IAM Role en IAM betrokkenheid) van hetzelfde thema: groepen en groepsrollen. Uiteindelijk is alleen IAM group nodig.

One-identity gevuld door ATL (webshop) gereedschap, Active Directory (AD) en HR. Interactie met groepen op geautomatiseerde wijze zal plaatsvinden via de SCIM standaard.

4.5 Autorisatie Service

Autorisatieservice Politie. Dit is een generieke dienst voor autorisaties waarvan de toepassingen gebruik maken en heeft o.a. een relatie met de API-GW. Zie hiervoor deelarchitectuur Autorisatiemanagement.

4.6 Generieke IAM Policy administratie

Generieke IAM Policy administratie heeft vooral als “rol” om bij te houden wat de inhoud is van de autorisatiematrix Politie. Het is als register bevraagbaar door de autorisatieservice Politie. De autorisatieservice Politie handelt autorisatieverzoeken af op basis van de inhoud van de autorisatiematrix Politie en de autorisatieregels in het autorisatiemodel Politie[16].

Generieke IAM Policy administratie is een IAM-core component die wordt ingevuld door het Open source product Open Policy Agent. Open Policy Agent is ook in te zetten als Autorisatie Service (zie paragraaf 4.5). De gegevens die door de Open Policy Agent moeten worden vast gehouden zijn:

- de 6+3 autorisatie- en bevoegdheidskenmerken (verwerkingsdoel etc)

- de autorisatie rol, die wordt opgevraagd bij de IAM identiteitskenmerkenservice (userinfo API).

- de vereiste betrokkenheid. Betrokkenheid is één van de 3 bevoegdheidskenmerken uit de 6+3

- en het gebruik, één van de 3 bevoegdheidskenmerken uit de 6+3

Zie Deelarchitectuur Autorisatiemanagement versie 1_0.pdf, paragraaf 3.

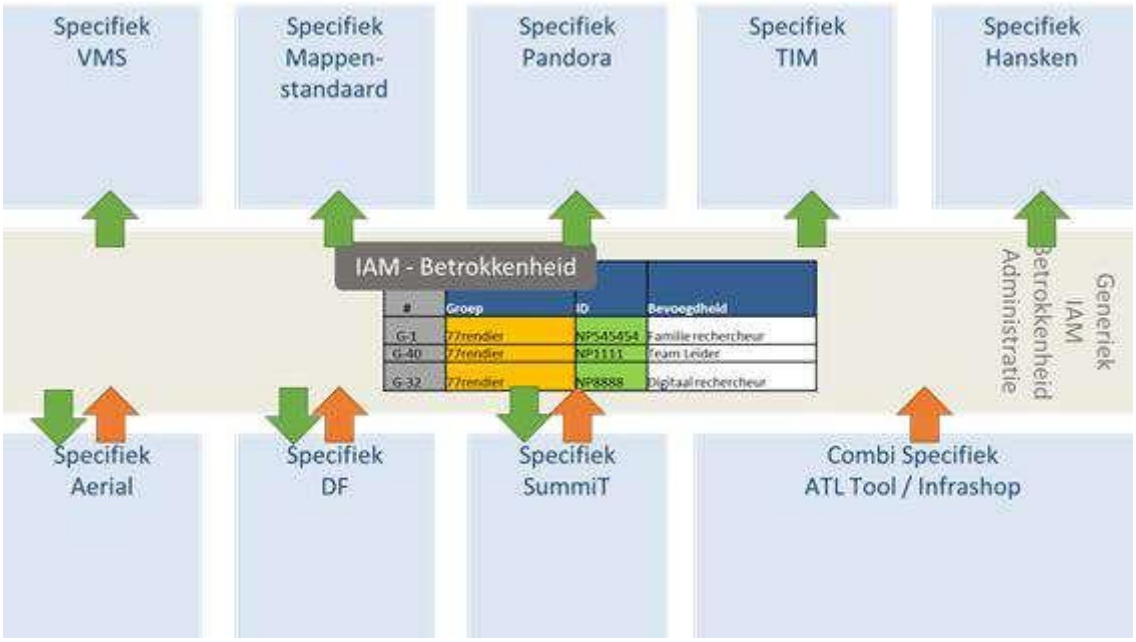
---

[15] ATL is een tool waarbij een leidinggevende buiten de standaard autorisatieprofielen om rechten kan uitdelen aan gebruikers (herleidbaar) en dit wordt vastgelegd in de AD.

[16] De verwijzingen in deze paragraaf zijn nog niet in het ABI vastgesteld. De bron voor de autorisatiematrix is vooralsnog het document Deelarchitectuur Autorisatiemanagement versie 1_0.pdf

4.7 Betrokkenheidsregistratie (R2D2)

IAM Betrokkenheid (R2D2). IAM betrokkenheid is het IAM-core component voor het centraal administreren van fijnmazige autorisaties (op basis van o.a. ABAC). De betrokkenheidsadministratie wordt door de Autorisatieservice Politie gebruikt voor het nemen van autorisatiebeslissingen op basis van de betrokkenheid van een gebruiker bij een registratie.



Zoals aangegeven in bovenstaand figuur is R2D2 zowel een doel als bronsysteem voor IAM.

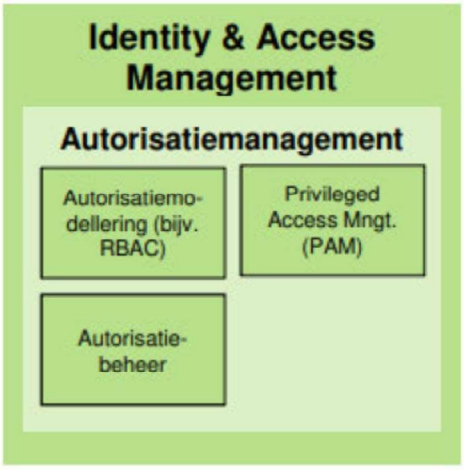
Door SummIT of ATL/Webshop wordt de tabel met betrokkenheid in R2D2 gevuld, aangegeven in bovenstaand figuur door de oranje pijl. IV-diensten als TIM of Hansken halen uit R2D2 deze informatie. Dat gebeurt via de SCIM API, weergegeven door de groen pijl.

5 Autorisatiemanagement

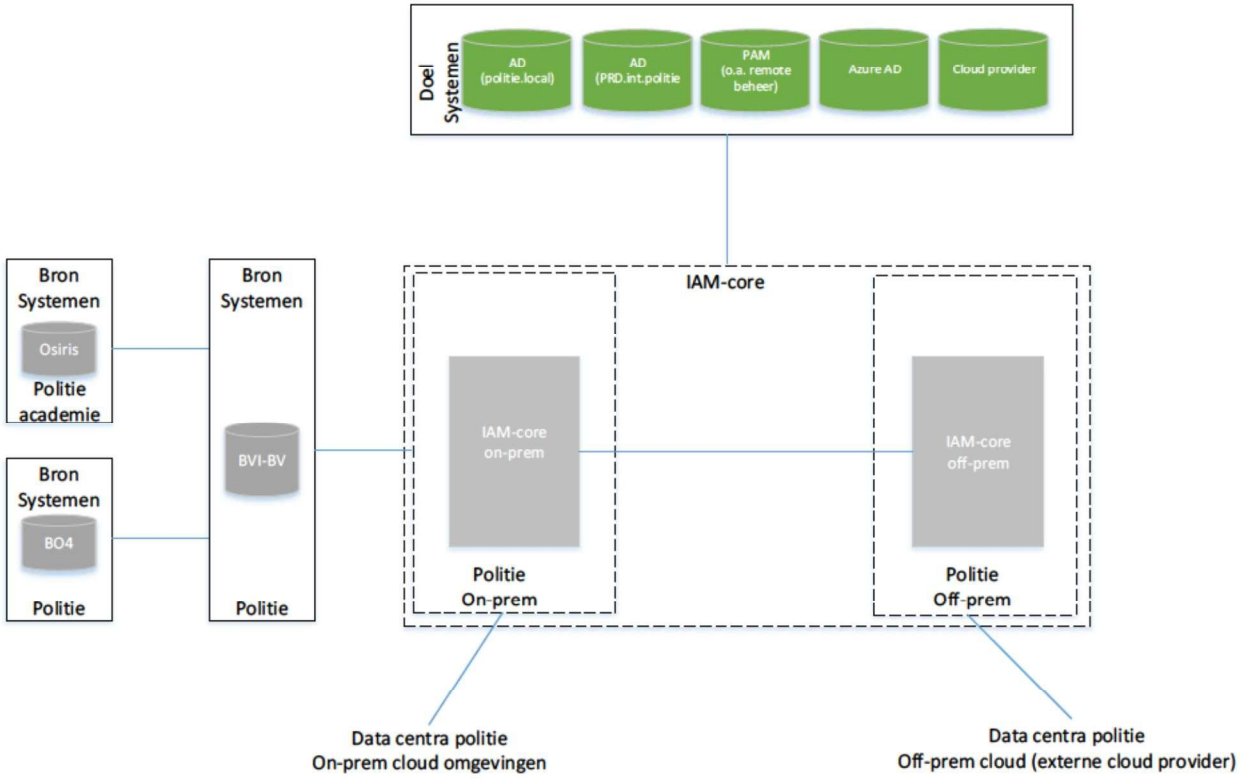
5.1 Overzicht

De huidige (Q1 2021) situatie binnen IAM is als volgt:

- Er zijn autorisatieprofielen opgesteld voor de operatie en dan met name de generieke profielen
- Momenteel (Q3 2021) zijn er de volgende ontbrekende autorisatie profielen:
  - PDC, lees bedrijfsvoering- en OTAP beheer/ontwikkelprofielen
  - THTC
- Voordat deze ontbrekende autorisatieprofielen opgesteld kunnen worden moeten hiervoor de kenmerken vastgesteld worden (zoals autorisatierol, groepslidmaatschap, competenties, werkprocessen, enz.) en de daarbij behorende bronsystemen
- Voor deze bronsystemen (en de nog vast te stellen bronsystemen) is/moet er connectiviteit geregeld worden richting IAM-core (dit is momenteel geregeld voor HRM (BO4, YouForce), BVI-BV en Osiris (PA))
- Momenteel (Q3 2021) wordt de Betrokkenheidsregistratie gerealiseerd



De ATL tool wordt vervangen door een Webshop (Q1/Q2 2021)



Opmerking: bovenstaand figuur bevat voorbeelden van doelsystemen (groen).

5.2 Autorisatiemodellering

IAM-core maakt gebruik van de volgende technieken, conform Deelarchitectuur Autorisatiemanagement:

- Role Based Access Management (RBAM), toegang wordt verleend op basis van de vooraf gedefinieerde rol van een gebruiker binnen een bedrijfsproces.
- Role Based Access Control (RolBAC), toegang wordt automatisch[17] verleend op basis van de rol van een gebruiker binnen een bedrijfsproces.
- Rule Based Access Control (RulBAC), toegang wordt automatisch verleend via toegangsregels (tijdstippen, locaties etc) en niet op basis van de rol van een gebruiker.
- Single Sign-on (SSO), ofwel het mechanisme waardoor een gebruiker slechts één maal hoeft in te loggen om vervolgens meerdere systemen en applicaties te kunnen gebruiken.
- Attribute Based Access Control (ABAC), ook bekend als op policy gebaseerd toegangsbeheer, definieert toegangscontrole waarbij toegangsrechten worden verleend aan gebruikers door het gebruik van policies op basis van een samengesteld aantal attributen.

Voor meer informatie en uitwerking hiervan, zie Deelarchitectuur Autorisatiemanagement.

5.2.1 Autorisatiebeheer via Active Directory

Op basis van de uitgangspunten is de uiteindelijke situatie van de beheeromgeving bepaald.

Er wordt gebruik gemaakt van één landelijke Active Directory, prd.int.politie. Hierin worden alle gebruikersaccounts opgenomen, ook die van beheer. Een beheerder heeft één gebruikersaccount. Wanneer een beheerder zich aanmeldt met zijn/haar account wordt er een aparte beheeromgeving weergegeven (lees PAM), logisch gescheiden van de productieomgeving. In deze logisch gescheiden omgeving zijn maatregelen genomen om de continuïteit en de beschikbaarheid van deze logisch gescheiden beheeromgeving te garanderen. Dit houdt concreet in dat op de generieke infrastructuur een logische beheercontainer (PAM) is gecreëerd. Op deze logische beheer-container zijn de extra beheermaatregelen van toepassing om de continuïteit en beschikbaarheid van deze omgeving te garanderen. Denk hierbij bijvoorbeeld aan een aparte seat (end-point[18]) waarop naast de generieke functionele bodem de beheertoepassingen en applicaties beschikbaar gesteld worden.

In het Windows AD-ontwerp wat hiervoor opgesteld moet worden is het van belang dat deze voor beheer beschikbaar moet blijven wanneer er een storing optreedt in de reguliere KA/productie omgeving.

De werking is globaal als volgt:

1) Een medewerker wordt aangenomen in de functie beheer. Deze wordt opgevoerd in het landelijk HRM systeem.
2) De gebruiker met als functie beheerder wordt in IAM-core vertaald naar de rol beheerder (globaal is dit de reguliere KA functionaliteit aangevuld met de beheer functionaliteit[19]). Deze informatie wordt doorgegeven naar de Active Directory van de politie (prd.int.politie).
3) Deze rolinformatie wordt in de landelijke Active Directory omgeving van de politie vertaald naar een gebruikersaccount[20], met de bevoegdheden voor reguliere KA werkzaamheden en een toegang tot de PAM-omgeving voor de beheerwerkzaamheden.
4) De beheerder kan via het KA-account onder regie van PAM de te beheren omgevingen benaderen. Op basis van de beheerrol (technisch OS, technisch applicatie, functioneel etc.) wordt er toegang verleend tot de te beheren resources met de faciliteiten die van toepassing zijn voor die specifieke rol.

---

[17] Met automatisch wordt bedoeld dat op basis van de rol van de gebruiker in het bedrijfsproces dit automatisch wordt vertaald in toegangsrechten.

[18] Zie hiervoor de technische referentiearchitectuur end-points.

[19] Dit kan via ATL (autorisatie Tool Leidinggevende) verlopen.

[20] De zeven domain admin gebruikeraccounts komen niet voor in het HRM & IAM-systeem deze worden handmatig aangemaakt in de Active Directory.

5.2.2 Autorisatiebeheer End-points applicaties

Dit geldt voor iOS of Android **native** apps en voor **hybride** apps op basis van Cordova, Xamarin of React Native.
De onderstaande voorschriften zorgen ervoor dat de native app intrinsiek veilig draait op het mobiele device, met behoud van de ketenbrede SSO ervaring voor eindegebruikers.

Voorschrift	**Gebruik bij voorkeur een mobiele app voor politiegegevens**
TA-IAM-V-01	
Toelichting	Gebruik voor eindgebruiker applicaties op een mobile device met politiegegevens bij voorkeur een mobile app of een web applicatie. Met behulp van de voorschriften in deze paragraaf wordt een intrinsiek veilige app laag afgedwongen. (met een native gedeelte daarin)
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), veilige software ontwikkeling. Zie ook **TA-IAM-V-18, TA-IAM-V-18, TA-IAM-V-07.**

Voorschrift	**Maak gebruik van één SDK die SSO tussen apps regelt**
TA-IAM-V-04	
Toelichting	Maak gebruik van één SDK (per platform) die SSO tussen apps regelt (op basis van een veilig opgeslagen JWT) en waarbij de SDK met verschillende IDP's overweg kan.
Referentie	Maak zoveel als mogelijk gebruik van marktstandaarden. Bron: Enterprisearchitectuurprincipes Bestemmingsplan IV: Gebruik standaarden

Deze web applicatie voorschriften gelden voor iOS of Android **web** apps.

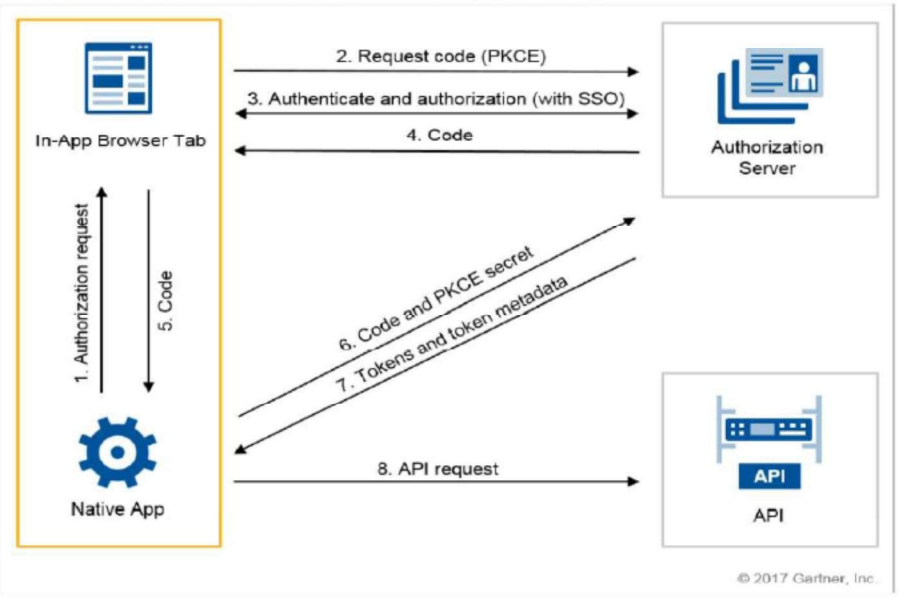
Voorschrift	**Maak gebruik van de OAuth autorisation code voor SSO op applicaties met politiegegevens**
TA-IAM-V-05	
Toelichting	Gebruik voor SSO op politie applicaties de OAuth autorisation code grant type. Alleen indien niet anders mogelijk mag hiervan worden afgeweken en één van de andere OAuth grant types worden gebruikt; (SAML/JWT bearer of ROPC). Hoe dan ook moet OAuth worden toegepast.
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), maak gebruik van intrinsiek veilige protocollen. Maak zoveel als mogelijk gebruik van marktstandaarden. Bron: Enterprisearchitectuurprincipes Bestemmingsplan IV: Gebruik standaarden

Voorschrift **TA-IAM-V-15**	**Gebruik voor het authenticeren van de applicatie een veilig opgeslagen key of secret. Gebruik OAuth 2.0 om het secret op het Token Endpoint in te wisselen voor een token.**
Toelichting	Mobiel apps: • Zorg dat een app gebruik maakt van een veilig opgeslagen secret. Zorg dat deze met een dynamic registration wordt uitgegeven: https://publicatie.centrumvoorstandaarden.nl/api/oauth/#native-client-with-user-delegation • Zorg dat de app beschikt over een veilig opgeslagen private key tbv mTLS Web applicaties: • Zorg dat de webapplicatie applicatie op container infrastructuur gebruik maakt van een veilig opgeslagen private key. Bijvoorbeeld in een secure vault zoals Conjur of Hashicorp. Gebruik: • Stuur het secret niet mee met de tokenaanvraag naar de token aanvraag maar gebruikt het secret of private key voor signing (gebruik de OAuth Client authentication methoden “private_keyt_jwt” of “client_secret_jwt”) Maak gebruik van bewezen en gecertificeerde oplossingen en cryptografische technieken. Zie referentie hieronder. N.B. Het is NIET toegestaan om alléén een API key als authneticatie/autorisatie te gebruiken dat in ieder request wordt meegegeven en in de resource server of back-end wordt gevalideerd wordt. In plaats daarvan MOET het OAuth 2.0 access_token worden meegegeven. Deze is vooraf verkregen via het OAuth 2.0 Token endpoint De redenen hiervoor zijn schaalbaarheid, securtity en centraal toegangsbeheer: 1. De voorkeur is dat API’s generiek inzetbaar zijn maar soms kunnen bepaalde API’s client specifiek zijn: d.w.z. en niet meer generiek inzetbaar voor alle client applicaties. De doelarchitectuur is dat systeem autorisatie centraal beheerd wordt middels OAuth scopes: zie **TA-IAM-V-17** 2. Door Oauth toe te passen kan het blokkeren van clients geregeld met generieke NL GOV OIDC API’s zoals dynamic registration, bijvoorbeeld via de API developer portal of andere beheerapplicaties die de generieke OIDC Dynamic Registration API’s aanroepen. 3. De API key komt in iedere API call terecht. Daardoor kan deze door onbevoegde beheerders onderschept worden of komt mogelijk in de logging terecht.
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), deelarchitectuur cryptografie. SEC-D2-P-04 Encryptiesleutels en digitale certificaten worden gedurende de gehele levenscyclus op een veilige wijze toegepast en beheerd. SEC-D2-P-01 Bij het toepassen van encryptie moet gebruik worden gemaakt van goedgekeurde cryptografische technieken.

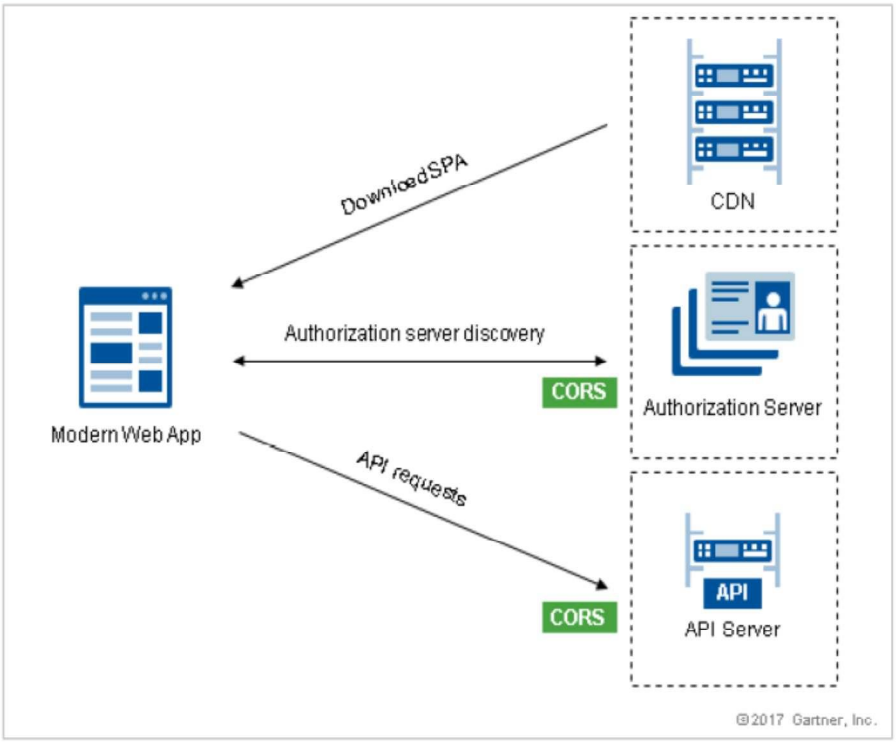
5.2.3 Autorisatiebeheer Cloud platform applicaties & services

In grote lijnen kunnen de rollen onderverdeeld worden in twee groepen, namelijk beheerders en applicaties/services. Deze paragraaf gaat over applicaties/services.

Voorschrift **TA-IAM-V-02**	**Maak gebruik van de OAuth autorisation code flow**
Toelichting	Gebruik de OAuth autorisation code flow, deze werkt met veilige token uitwisseling
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), maak gebruik van intrinsiek veilige protocollen.

Voorschrift **TA-IAM-V-03**	**Maak gebruik van de OAuth2 PKCE extensie**
Toelichting	Gebruik ook de OAuth2 PKCE extensie (RFC6750) 
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), maak gebruik van intrinsiek veilige protocollen. Maak zoveel als mogelijk gebruik van marktstandaarden. Bron: Enterprisearchitectuurprincipes Bestemmingsplan IV: Gebruik standaarden

Voorschrift **TA-IAM-V-06**	**Maak gebruik van CORS**
Toelichting	Maak gebruik van Cross-Origin Resource Sharing (CORS) API's, zodat er onderscheid gemaakt kan worden van de static content. Dit om Cross Site Request Forgery en gerelateerde risico's te mitigeren. Implementeer en controleer de CORS headers in de API gateway. Gebruik CORS headers in de web applicatie.

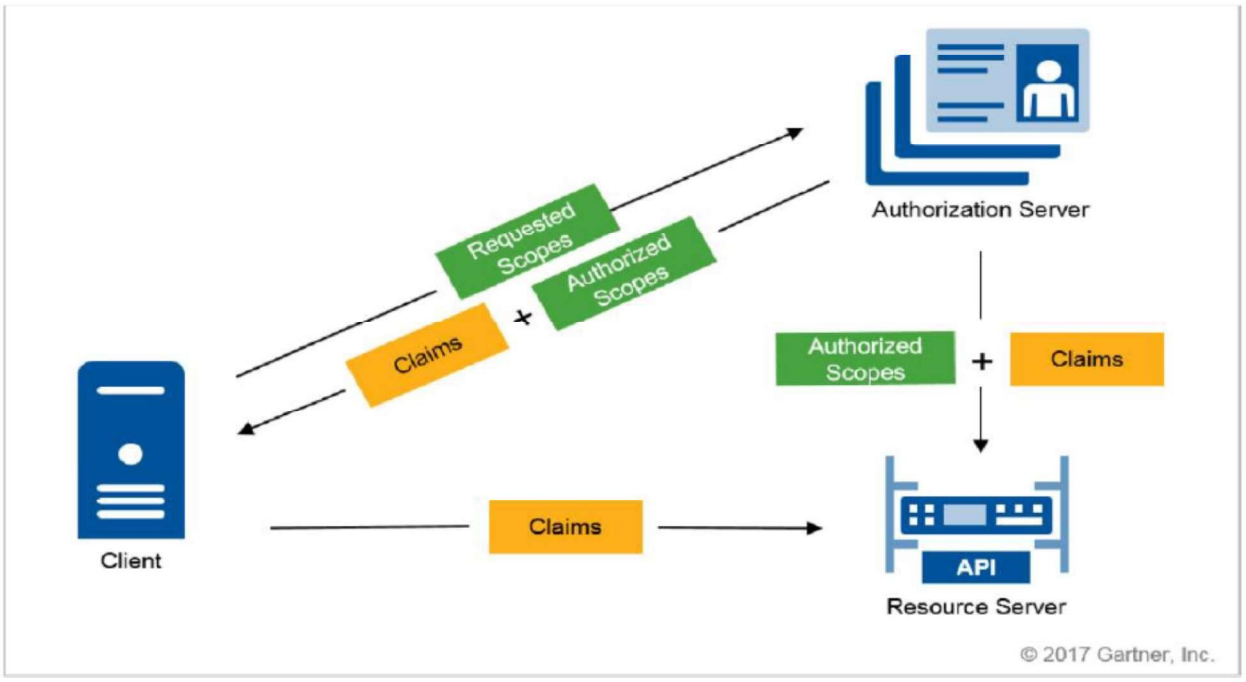
	
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), maak gebruik van intrinsiek veilige protocollen. Maak zoveel als mogelijk gebruik van marktstandaarden. Bron: Enterprisearchitectuurprincipes Bestemmingsplan IV: Gebruik standaarden

Voorschrift **TA-IAM-V-07**	**Systeemautorisaties voor services worden vastgelegd in OAuth2 scopes**
Toelichting	De autorisatie van een applicatie (in de vorm van een OAuth 2.0 API key met secret en scopes moet voldoende zijn om alle functies van de applicaties en webservices uit te kunnen voeren.
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), maak gebruik van intrinsiek veilige protocollen. Maak zoveel als mogelijk gebruik van marktstandaarden. Bron: Enterprisearchitectuurprincipes Bestemmingsplan IV: Gebruik standaarden

Een client applicatie (of worker) die een RESTfull service wil aanroepen wordt geïdentificeerd door een API key welke resulteert in een set OAuth2 scopes. De scopes voor een service of worker (zie autorisatie Scope) worden geregistreerd in het IAM systeem, en ontsloten via de API gateway (specifieke[21] worden geregistreerd in de API gateway). Tijdens de systeem authenticatie van de worker/client met Oauth 2.0 client credentials grant type – met API key en secret - tegen het token endpoint van de OAuth2 authorisation server op de API gateway worden de scopes gekoppeld aan een OAuth token met een

[21] Met specifieke wordt bedoeld niet generiek en standaard. Als alle specifieke ook in het IAM systeem worden opgeslagen dan wordt het IAM systeem complex en onbeheersbaar, denk aan life-cycle omdat per applicatie de specifieke settings bijgehouden moeten worden. Dit kan beter in de applicatie zelf en via een API ontsloten worden.

bepaalde geldigheidsduur. Het benodigde client secret wordt veilig opgeslagen (bijvoorbeeld met een secure vault op de client) en alleen uitgewisseld tussen de client en de token service op de API gateway bij het ophalen van een nieuw token.



Services moeten de OAuth scopes valideren. Dit kan worden belegd in een Resource server.
(Microservices kunnen dit uitbesteden aan een Microgateway, die onderdeel is van een microservice.)

Voorschrift **TA-IAM-V-08**	**Indien de aan te roepen service ook gegevensautorisatie moet doen op basis van applicatie en/of rollen, moet de identiteit van de eindgebruiker worden gepropageerd bij aanroepen van systeemkoppelingen**.
Toelichting	De standaard die hier wordt gebruikt is JWT (en OpenID Connect). De onweerlegbare vertrouwensketen wordt daarbij ingevuld middels een digitaal ondertekend JWT (id_token), uitgegeven door de authorisation server. Het access_token wordt gebruikt om de identiteit te propageren.
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), identity & access management NL_GOV OIDC standaarden.

In voorgaande versies van de referentie architectuur was dit Kerberos.
In dat geval moet de Resource server ook het ontvangen JWT signature en audience restriction valideren.
(Microservices kunnen dit uitbesteden aan een Microgateway, die onderdeel is van een microservice.)
Alle acties die gedaan worden door een enkele gebruiker (medewerker, medewerker van een publieke organisatie, burger, medewerker van een ketenpartner organisatie) MOETEN gebruik maken van autorisatie op de persoon met behulp van de autorisatie services en de identiteit in het JWT.

De Autorisatie SVC van de IAM Core kan zowel aan de server kant als in de (MASA) apps worden aangeroepen, zodat de autorisatie consistent werkt in de server-side (n-tier) registratieve applicaties en in de vele kleine MASA apps. De autorisatie moet worden gelogd.

Voorschrift	**Voor de geldigheidsduur van sleutels en het sleutel-uitwissel mechanisme, wordt JWKS gebruikt.**
TA-IAM-V-09	
Toelichting	JSON Web Key Set (JWKS) is een set met sleutels die de openbare sleutels bevatten die gebruikt worden om een JSON Web Token (JWT) te verifiëren die is uitgegeven door de authorisation server.
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), maak gebruik van intrinsiek veilige protocollen. Maak zoveel als mogelijk gebruik van marktstandaarden. Bron: Enterprisearchitectuurprincipes Bestemmingsplan IV: Gebruik standaarden

Voorschrift	**Toegang tot gegevens binnen een database en andere componenten of SOAP services waar OAuth2 niet wordt ondersteund - vindt plaats op basis van de (generieke) rol die is vastgelegd in het centrale IAM systeem.**
TA-IAM-V-10	
Toelichting	N.v.t.
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), identity & access management

IAM binnen een database

Dit is een ongewenste situatie en is een legacy oplossing. Maar omdat er nog wat business critical applicaties worden gebruikt wordt dit toch in dit document besproken.

Traditioneel kennen de meeste RDBMS-en een interne identity repository. De interne repository bevat alleen interne RDBMS-(systeem)accounts die onlosmakelijk verbonden zijn met het functioneren van het RDBMS. Deze worden voor zover mogelijk gedisabled voor interactief gebruik. Voor de overige accounts is de centrale IAM-repository leidend. Hoe dit in het ontwerp wordt uitgewerkt is afhankelijk van de mogelijkheden die het RDBMS hiervoor biedt. Het gaat hierbij om een beperkt aantal identiteiten, namelijk beheerders en service accounts. Interne RDBMS-accounts worden niet in de centrale IAM-repository vastgelegd, maar dat geldt wel voor service accounts die worden gebruikt in de JDBC/ODBC/OLEDB datasources vanuit applicaties, services en beheertools.

Opmerking:

Wanneer er gebruik gemaakt wordt van systeembeheerders accounts met hogere bevoegdheden in o.a. een database wordt er gebruik gemaakt van PAM (Privileged Access Management, zie paragraaf 5.7).

Specifieke applicatie autorisaties voor eindgebruikers worden geregeld met de autorisatiematrix. Voor gegevens- en functionele autorisatie wordt de LDAP niet direct aangeroepen, maar wordt de Autorisatie SVC van de IAM Core gebruikt, waar bevoegdheden/permissies van de gebruiker vanuit applicatierollen worden vrijgegeven in de vorm van consistente ABAC attributen.

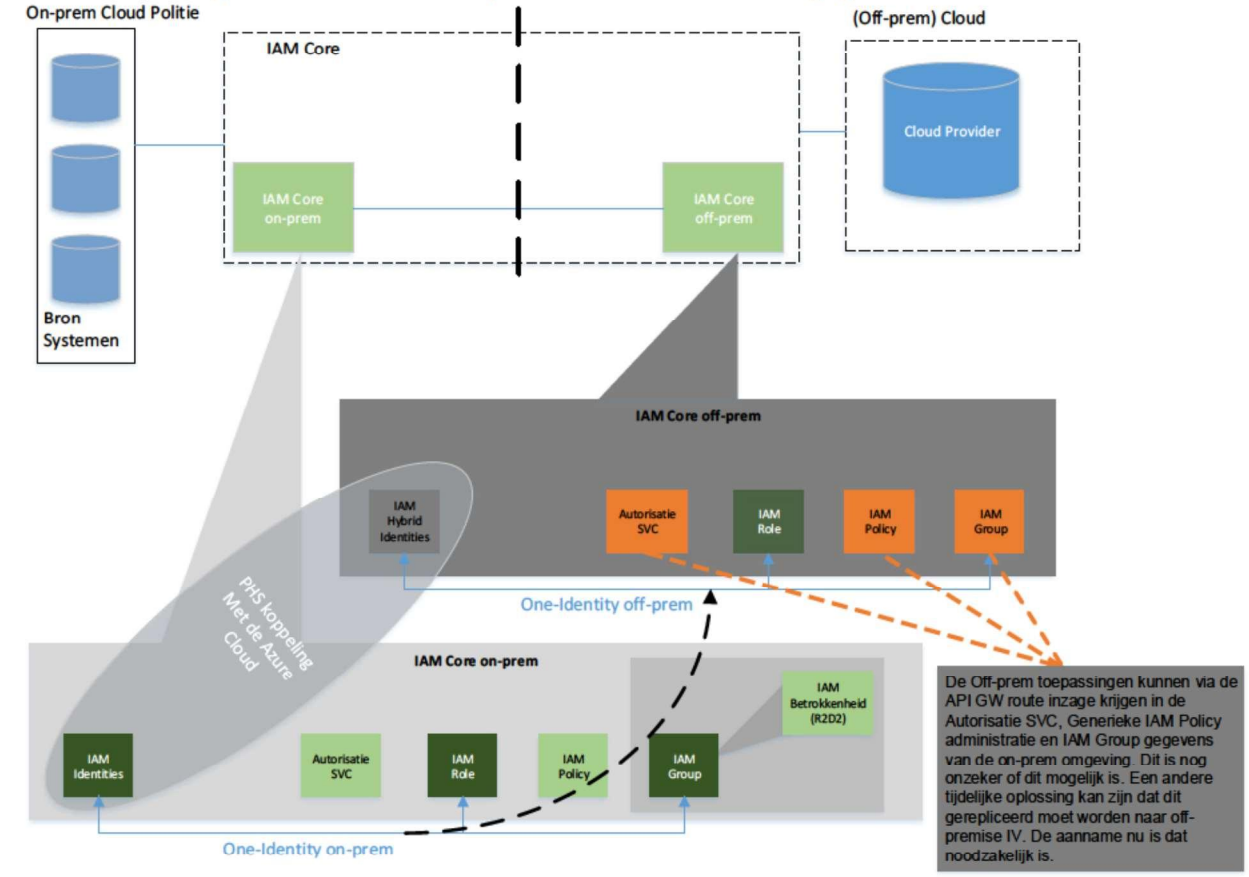
.

5.2.4 Autorisatiebeheer off-prem Cloud Platform applicaties & services

Er wordt onderscheid gemaakt tussen gegevens die noodzakelijk zijn binnen de on-prem politie cloud en de gegevens die noodzakelijk zijn voor gebruik binnen de off-prem politie cloud.

Dit omdat niet alle politiegegevens noodzakelijk zijn voor gebruik binnen de off-prem politie cloud, denk hierbij bijvoorbeeld aan AVG en WPG gegevens. Mede hierdoor wordt de IAM core logisch opgedeeld in twee delen. Een IAM core component on-prem en een IAM core component off-prem. Dit is verder uitgewerkt in het document Cloud Services in samenwerking met One Identity Manager.

In onderstaande figuur is de IAM core off-prem in de Cloud o.a. weergegeven.



Voor meer informatie hierover zie documenten:

- Document IAM politie architectuur overview
- Document Cloud Services in samenwerking met One Identity Manager

5.2.5 Autorisatiebeheer via PAM

Autorisatiebeheer Privileged Access Management wordt behandeld in een apart document; I210702 – Referentiearchitectuur PAM.

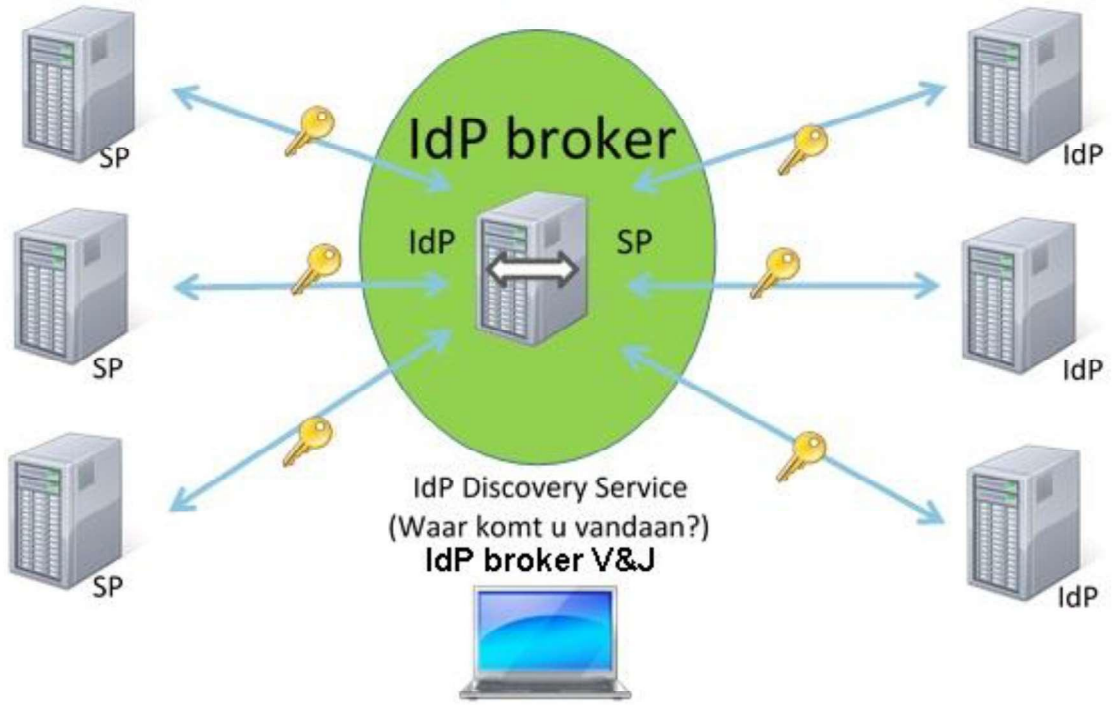
6 Federatie

Federatietechnologie brengt een beveiligde, gestandaardiseerde manier om SSO domeinoverstijgend te faciliteren. SSO (Single Sign-On) is een IAM-functie om eindgebruikers toegang te verschaffen die tevens gerelateerde risico's beperkt. Dit betreft ook de inzet van federatietechnologie om SSO[22] voor on-premise en cloud (zowel on- en off-premise) gebaseerde toepassingen in mobiele en traditionele werkomgeving te faciliteren.

6.1 Rijksbreed federeren

Conform de Cloud adoptie[23] van de politie zal de politie in de komende jaren vaker gebruik gaan maken van clouddiensten van andere overheidsinstanties.

De politie biedt ook clouddiensten aan, via de Open data API. Zie https://www.politie.nl/algemeen/open-data.html. Om de authenticatie (en een beperkte vorm van autorisatie[24]) uniform beschikbaar te stellen maakt de politie gebruik van IdP-broker van V&J, zie onderstaand figuur:



Doordat alle overheidsinstanties gebruik gaan maken van de IdP-broker hoeven deze instanties enkel hun IdP en services aan de IdP-broker kenbaar te maken, zonder dat de overheidsinstanties onderling een vergelijkbare koppeling moet aanleggen. De IdP-broker voorkomt hiermee een complexe onderlinge

[22] SSO wordt op de applicatie toegepast na het authenticeren op de IDP van de politie.

[23] Cloud adoptie document: I150203-Cloud Adoptie-110. *Dienst ICT,* 5.1.2.e *, versie 1.1, 9 februari 2016*

[24] Met beperkte vorm van autorisatie wordt o.a. de toegang tot een bepaalde toepassing bedoeld. Ook wel toegang tot de "voordeur" genoemd.

verbindingenstructuur (full mesh[25]) welke lastig te onderhouden is en dwingt gebruik van een standaard federatiefkoppelvlak af. Direct B2B[26] koppelingen moeten zo veel als mogelijk voorkomen worden en moeten dus lopen via het federatiefkoppelvlak.

De oplossingsrichting om rijksbrede diensten toegankelijk te maken vanaf een politiewerkplek i.c.m. een federatieve koppeling levert dus uniformiteit op voor authenticatie en deels voor autorisatie. De authenticatie voor de politiemedewerker wordt geregeld door middel van een IdP van de politie. Hierbij wordt gebruik gemaakt van de KA-credentials van de politiemedewerker zodat SSO[27] gerealiseerd kan worden en de politiemedewerker zich niet opnieuw hoeft aan te melden.

De daadwerkelijke autorisatie wordt gerealiseerd conform inbound en outbound federatie zoals beschreven in paragraaf 6.2 & 6.3.

De IdP-broker zorgt tevens voor het koppelvlak naar de publieke authenticatie service, E-herkenning voor de commerciële markt en DigiD voor de burgers.

De IdP van de politie zorgt voor het politie specifiek koppelvlak naar andere IdP's zoals die van Microsoft & Google.

Ondanks de doelarchitectuur om koppelingen via de V&J broker te laten lopen zullen er ook directe SP koppingen vanuit de Politie naar ketenpartners liggen. Dit bekent dat deze omgezet moeten worden.

6.1.1 Koppelvlak

Het rijksbrede IdP-broker-koppelvlak is gebaseerd op open standaarden. De volgende open authenticatiestandaarden worden ondersteund:

- OpenID[28] Connect (OIDC)
- Oauth2
- SAMLv2

De markt trend[29] is dat er meer implementaties beschikbaar zijn op basis van OIDC dan met SAMLv2. De code ten behoeve van OIDC authenticatie zijn in programmeertalen makkelijker te implementeren dan de code ten behoeve van SAML authenticatie. Hierdoor is minder implementatiewerk nodig. De technische aansluiting verloopt ook eenvoudiger: in plaats van het uitwisselen van metadata is het voor een dienstaanbieder voldoende eenmalig bij het platform te registreren. Het SAML-protocol is uitermate geschikt voor webapplicaties[30], maar minder voor mobiele apps. Dit houdt in dat voor mobiele apps OAuth v2 ondersteund moet worden. OAuth v2 is een open standaard voor autorisatie (Open Authorization)[31].

Voorschrift	**De uitgifte van OAuth2 Tokens worden centraal belegd, voor federatieve ontsluitingen**
TA-IAM-V-11	
Toelichting	Er wordt op één centrale plek binnen de ICT infrastructuur de uitgifte van OAuth2 tokens gefaciliteerd.

---

[25] Full mesh zie: https://en.wikipedia.org/wiki/Network_topology#Mesh

[26] B2B: Business to Business koppeling.

[27] SSO: https://nl.wikipedia.org/wiki/Single_sign-on

[28] OpenID Connect is een RESTful API-like service; het is minder complex dan SAML. Zie: http://openid.net/connect/

[29] Bron: Gartner Mobile SSO for native apps

[30] Bron: https://blog.runcloud.io/2018/12/26/php-authentication-with-oauth-saml-openid-explore-which-solution-to-use-and-when.html

[31] OAuth, bron: https://nl.wikipedia.org/wiki/OAuth

	Het proces voor het vrijgeven beheren van de OAuth client vindt gedelegeerd plaats via de API developer portal (self-service en autorisatieworkflow) en/of specifieke clients die gebruik maken van de API's (Dynamic registration, aangevuld met API developer Portal API's) De secrets behorende bij de API key's worden ontsloten via een secure vault (bijvoorbeeld Conjur). Externe client moeten gebruik maken van een private key als client authentication method ("private_key_jwt" mechanisme)
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), maak gebruik van intrinsiek veilige protocollen. Maak zoveel als mogelijk gebruik van marktstandaarden. Bron: Enterprisearchitectuurprincipes Bestemmingsplan IV: Gebruik standaarden

Bij voorkeur wordt er gebruik gemaakt van OpenID Connect (OIDC), dit heeft als voordeel dat er van één protocol gebruikt wordt gemaakt voor toegang tot politiegegevens. Dit geldt zowel voor toegang via een webbrowser als via een mobiele app.

Hiervoor wordt het "NL GOV Assurance profile for OAuth 2.0" en het NL GOV Assurance profile for OpenID Connect 1.0 toegepast, overeenkomend/aangevuld met voorschriften verderop in dit hoofdstuk.

Doordat de server (en gegenereerde inlogpagina) wordt gebruikt als client (bij voorkeur OIDC-client) richting de ketenpartners, wordt die complexiteit niet neergelegd bij de individuele webbrowser apps en de mobiele apps.

Voor het netwerkkoppelvlak wordt gebruik gemaakt van de bestaande partnerkoppeling; PolJus Koppeling.

6.1.2 Algemene voorschriften

Voorschrift **TA-IAM-V-12**	**Federatie naar ketenpartner IdP's (of de V&J broker) wordt geïnitieerd via de authorisation server (niet direct vanuit de app)**
Toelichting	Afhankelijk van de ketenpartner kan dit met SAML of met OAuth. Token uitwisseling gaat voor de rubricering geheim (politiegegevens) via de server en niet via de browser, dus met SAML artifact binding of met OAuth Authorisation code flow. (Uitsluitend voor bedrijfsvoeringtoepassingen binnen een veilige container is het toegestaan om het token via de browser uit te wisselen.) De reden hiervoor is dat we het de applicatie developer (van een ketenpartner of de politie) zo eenvoudig mogelijk willen maken om fedratief inloggen aan te zetten in een applicatie (in een poging om het kopiëren van gegevens over de keten te ontmoedigen) 1. De app developer werkt met één OAuth provider om bij alle politie en ketenpartner IDP's te kunnen authentiseren. De IDP keuze wordt tijdens de registratie worden aangevinkt. 2. Geen koppeling naar de IDP broker per nieuwe app, een nieuwe app kan per ommegaande wordenaangemaakt 3. Geen SAML in de client applicaties In de OAuth client registratie wordt bijgehouden welke applicatie van welke IDPen/of 2FA middel gebruik mag maken. Dit kan door een developer zelf worden aangegeven. Goedkeuring daarvan loopt via aanvraagproces ondersteund door een API developer Portal. (Indien nodig kan dynamisch worden geregistreerd uitgevraagd middels "default_acr_values"). Indien de client twee of meer toegestane IDP's of inlogniveaus ondersteund dient door de client

	applicatie - middels het “acr_values” veld - aangegeven te worden welke moet worden gebruikt.
Referentie	Maak zoveel als mogelijk gebruik van marktstandaarden. Bron: Enterprisearchitectuurprincipes Bestemmingsplan IV: Gebruik standaarden https://logius.gitlab.io/oidc/#authentication-context

Voorschrift **TA-IAM-V-13**	**Notificeer de gebruiker van zijn inlog acties**
Toelichting	Toon de gebruiker de laatst inlog en uitlog tijdstippen. Notificeer de gebruiker indien deze inlogt op een nieuwe app (of groep MASA apps), bijvoorbeeld middels een consent pagina. Notificeer de gebruiker bij uitzonderlijk gedrag (nieuwe devices, uitzonderlijke locaties etc.)
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB)

Voorschrift **TA-IAM-V-14**	**Identiteitsattributen van de ketenpartnergebruiker worden opgehaald met de userinfo API**
Toelichting	Identiteitsattributen van de ketenpartnergebruiker zelf kunnen worden opgehaald met de een userinfo API (of WhoAmI).Op de server wordt bepaald of deze in de SAML token stonden of opgehaald moeten worden met een userinfo SCIM API call bij de ketenpartner. Identiteitsgegevens van andere (ketenpartner) gebruikers worden opgehaald met de SCIM API.
Referentie	Maak zoveel als mogelijk gebruik van marktstandaarden. Bron: Enterprisearchitectuurprincipes Bestemmingsplan IV: Gebruik standaarden

Voorschrift **TA-IAM-V-16**	**Maak in applicaties op End-points gebruik van pseudoniemen**
Toelichting	Maak (in het JWT dat gebruikt wordt) in de applicaties op End-points gebruik van een pseudoniem van het userID van de gebruiker. Maak in het by-value access_token (een JWT dat gebruikt gebruik van een pairwise pseudoniem van het userID van de gebruiker als “sub”). https://publicatie.centrumvoorstandaarden.nl/api/oauth/#jwt-bearer-tokens (Als de applicatie het userid nodig heeft, kan dit worden vrijgegeven met een OAuth scope, bijvoorbeeld “prefererend_username”.) In het access_token staat dus geen userID.
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB), identity & access management

Voorschrift TA-IAM-V-17	**Hanteer verschillende OAuth 2.0 scopes voor de systeemautorisaties van een applicatie**
Toelichting	Maak voor de systeemautorisatie aparte scopes. De scopes dienen bij voorkeur samengesteld te zijn uit een aantal elementen, zoals: 1. Een grofmazige definitie van de te ontsluiten gegevens te bevatten (bijvoorbeeld referentiegegevens, WPG artikel 8, etc.) 2. Optioneel een meer fijnmazige definitie van de te ontsluiten gegevens (vaak gelijk aan de API). Bijvoorbeeld Locatie, Melding, Signalering, Digibon, etc. 3. De toegestane gebruikersactie (meestal is onderscheid tussen 'read' en 'write' voldoende) De scopes moeten zo grofmazig mogelijk zijn, maar niet zo grofmazig dat de applicaties véél te veel systeemrechten hebben voor het doel van de applicatie. ("overentitled"). Te fijnmazige scopes leidt tot een onbeheersbaar aantal scopes (Helaas bevat de OIDC standaard zelf al een aantal te fijnmazige scopes, hier hebben we geen invloed op.) Wijs deze toe aan de apps en controleer deze in de resource server.
Referentie	Enterprise Architectuur InformatieBeveiliging (EAIB) Voorbeelden: • https://consumerdatastandardsaustralia.github.io/standards/#authorisation-scopes • https://api.slack.com/scopes

Voorschrift TA-IAM-V-18	**Hergebruik van OAuth 2.0 access_tokens**

Toelichting	• Je mag een OAuth 2.0 access_token alleen hergebruiken voor een nieuwe API call als de oorspronkelijke cliënt applicatie die call ook zelf zou mogen doen.
	• Je mag een token alleen hergebruiken als het niet tot een heel andere business transactie leidt / er sprake is van een ander rubriceringsniveau van de gegevens.
	  ○ Als het token bijvoorbeeld leidt tot een API call naar een lager/ander rubriceringsniveau (bijvoorbeeld van geheim naar confidentieel of vanuit burger naar politie confidentieel/intern, moet hiervoor een token uitwisseling plaatsvinden.
	  ○ Het is niet toegestaan om verschillende ketens (zoals immigratie, forensisch onderzoek, ondermijning etc. vanuit één client te initiëren. Dan moet je daar een andere client met andere scopes voor gebruiken. Dat leidt automatisch tot een ander access_token.

Referentie	Gebruik standaarden zoals OAuth JWT of SAML bearer grant type of RFC8693 Token exchange wordt altijd centraal geïmplementeerd op of via de OAuth autorisation/token server. (niet in een API)

6.2 Inbound federatie

6.2.1 Globale stappen

Bij een inbound federatieve SSO-koppeling authenticeren externe gebruikers met de credentials (aanmeldgegevens) van de externe partij zich bij de Resource Provider van de politie.

Bij externe partijen moet bijvoorbeeld gedacht worden aan partnerorganisaties of identiteitaanbieders zoals overheidsinstellingen.

Hierbij maakt de client-applicatie[32] gebruikt van politiegegevens, de authenticatie van de externe partij wordt vertrouwd en geaccepteerd, waarmee er contact gezocht met het politiedomein om data te benaderen van de politie. De client-applicatie kan zowel door de politie als door een ketenpartner worden gerealiseerd, conform de beveiligingseisen van de politie (en verificatie daarvan).

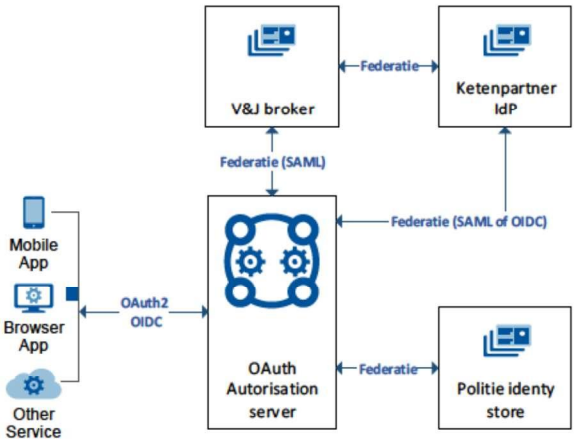
Afspraken

In de trust policy tussen de politie en de vertrouwde partij moet worden vastgelegd dat:

- Beide organisaties elkaar vertrouwen;
- De authenticatie van de vertrouwde organisatie wordt vertrouwd en geaccepteerd. Voor verschillende rubriceringsniveaus gelden er verschillende eisen ten aanzien van authenticatie;
- Welke gebruikers-attributen[33] er gebruikt moeten worden om toegang te verlenen tot de applicaties van de politie. De afspraak hierin is dat de politie bepaalt welk autorisatieprofiel gebruikt wordt. De ketenpartner geeft zijn eigen context mee, en op basis daarvan zijn afspraken gemaakt tussen politie en ketenpartner over toegang tot gegevens. De invulling daarvan is aan de politie. Het autorisatieprofiel bepaalt de autorisatierol(len) die de gebruiker met dat profiel zijn toegekend. Aan een autorisatierol zijn weer bevoegdheden toegekend, op basis waarvan de autorisatieservice Politie een autorisatiebeslissing kan nemen.
- Het technisch koppelvlak vastleggen (welke protocollen worden er gebruikt, Cryptografische verbinding). Zoals verderop wordt toegelicht is er een voorkeur om de tokens niet via de browser uit te wisselen, maar via een backchannel.
- Er moeten afspraken gemaakt worden over het gebruik van welke Rijksbrede attributen.
- De Authorisation server als onderdeel van de API GW suite vertaalt de tokens van de ketenpartner (veelal SAML, soms OIDC) naar politietokens (OAuth2 en IODC)

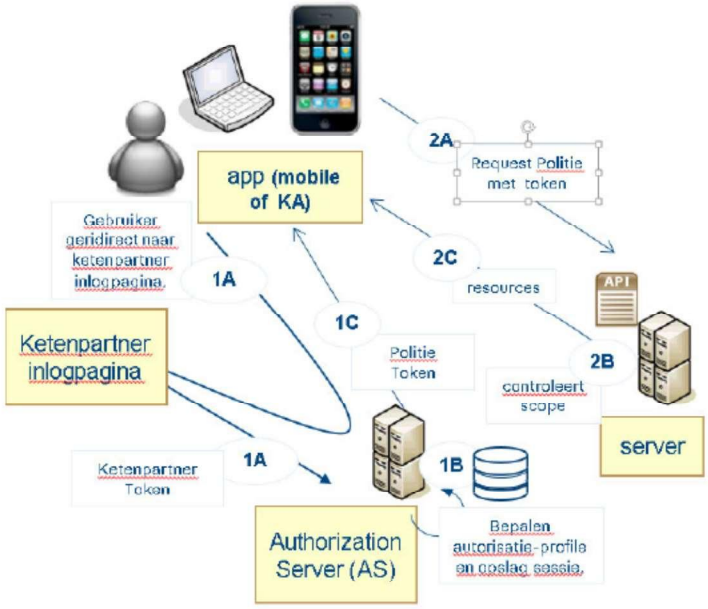
[32] Met client applicatie wordt bedoeld: een mobiele app, of een desktop applicatie of een browser-based app

[33] Dit in afstemming met o.a. SEMA team en het ontologie team



6.2.2 Inlogproces inbound

1. Aanvraag van een token door de app
   A. De gebruiker van de vertrouwde organisatie selecteert op de app de IDP van de eigen organisatie (op de inlogpagina die al is gepresenteerd door de Authorisation server als onderdeel van de API GW suite.
   De App redirect de gebruiker via de Autorisatie server naar de inlogpagina van de ketenpartner (eventueel via de V&J broker). Gebruiker logt in (of heeft al een token).
   B. De autorisatieserver controleert het token van de ketenpartner en bepaalt het autorisatieprofiel (aan de hand van het userID en groupID in het token)
   C. Vervolgens genereert de autorisatieserver een politie-token met scopes retour en slaat de SSO-sessie lokaal op (met het token en/of de attributen los). Autorisatieserver retourneert een code (die het token vertegenwoordigt) naar de app.



2. Gebruik van een token om toegang te krijgen tot resources
   A. De OAuth resource-server (onderdeel van APIM) valideert het token is uitgegeven door de Autorisatie-server (signature validatie)
   B. De Back-end server (niet getekend) voert met behulp van de Autorisatie SVC van de IAM Core de autorisatie uit (selecteert het record) aan de hand van de ABAC-attributen en het subjectID (user) en retourneert de politiegegevens.
   C. Wanneer de autorisatie succesvol is wordt er toegang verleend tot de resources

6.3 Outbound federatie

Bij een outbound federatieve SSO-koppeling authenticeren (interne) politiegebruikers zich bij een externe Service Provider met credentials vanuit de politie-organisatie, en niet met credentials vanuit de externe organisatie. Hierbij vertrouwt de externe organisatie de Nationale Politie. Bij een externe organisatie moet ook gelezen worden van interne omgevingen binnen de politieorganisatie (denk hierbij bijvoorbeeld aan de opleiding, SURF-omgeving van de politieacademie[34]).

Outbound federatie is de meest voorkomende federatieve toepassing. SSO zorgt voor toegang tot meerdere systemen zonder dat de gebruiker zich op ieder systeem hoeft aan te melden. Bij toenemend gebruik van SaaS-toepassingen zullen meer gebruikers toegang moeten krijgen tot applicaties buiten de politie-organisatie.

6.3.1 Globale Stappen

1. Maak gebruik van een identity provider, bij communicatie met de overheid gaat de voorkeur uit naar de IdP broker van VenJ. Er zijn twee verschillende SSO protocollen met hun eigen terminologie: SAML 2.0 en OpenID Connect 1.0 / OAuth2. Beiden maken gebruik van de identity provider waarmee de gebruikers zich kunnen authenticeren. Een federation identity Provider (IdP) (in SAML termen) of “OpenID identity provider (OP)” (In OpenID Connect termen) genereert de identiteitsaspecten, die meestal bestaan uit bepaalde attributen over de persoon, zoals naam of e-mailadres. De *IdP* heeft een verbinding met de attribute provider (AP) en/of de ID-repository[35]. De *IdP* gebruikt enkel een deel van de informatie uit deze ID-repository om te voldoen aan het authenticatieverzoek.
2. De SAML *IdP van de politie* of OpenID identity provider) heeft een koppeling met de attribute provider (AP). De AP krijgt de identiteitsgegevens en bepaalde informatie (attributen) over de gebruiker aangeleverd vanuit de bestaande ID-repository. De *IdP* / OP bevat dus slechts een subset van informatie over de gebruikers.
3. Tussen de externe organisatie waarmee gefedereerd moet worden en de politie wordt een cryptografisch vertrouwen gecreëerd. Hiervoor wordt er gebruik gemaakt van een public key infrastructure (PKI), die zorgt voor versleutelde communicatie tussen de politie en de vertrouwde organisatie. Bij authenticatie/versleuteling tussen twee interne organisaties, wordt er gebruik gemaakt van de interne PKI van de Nationale Politie. Voor de authenticatie/versleuteling tussen een interne en externe organisatie wordt er gebruik gemaakt van een externe PKI. Hierbij is de PKI-overheid de certificaatleverancier. PKI wordt gebruikt voor:
    - Het ondertekenen van het token naar de ketenpartner (dit kan een OpenID Connect id_token of een SAML 2.0 token zijn)
    - Het encrypten van het kanaal waarover het token wordt uitgewisseld. Dit is tweezijdig TLS. Zie volgende punt.
4. Voor federatieve toegang Voor SAML en OpenID Connect bestaan er verschillende profielen. Sommige daarvan (SAML Artifact Binding en OpenID Connect basic profile) wisselen het token uit via een API in plaats van via een browser redirect. Dit heeft als voordeel dat de tokenuitwisseling minder kwetsbaar is voor browser redirect gebaseerde aanvallen:
    - OpenID Connect 1.0 (OIDC): Het id-token wordt door de politie-autorisatieserver (‘client’, vanuit het perspectief van de uitwisseling met de ketenpartij) opgehaald met een authorisation-code die via de browser wordt opgehaald. Daarbij moet de client zich

[34] SURF zie https://www.surf.nl/

[35] Hier wordt de AD van de Nationale Politie (politie.local) bedoeld.

authenticeren met een PKIO client-certificaat en/of met een client-secret. Dit heet de “OpenID Connect basic profile”

- SAML 2.0: Het SAML 2.0 token wordt door de politie autorisatie-server (service provider in SAML termen) opgehaald met een SAML artifact die via de browser wordt opgehaald. Daarbij moet de client zich authenticeren met een PKIO client-certificaat. Dit heet de “SAML artifact binding”

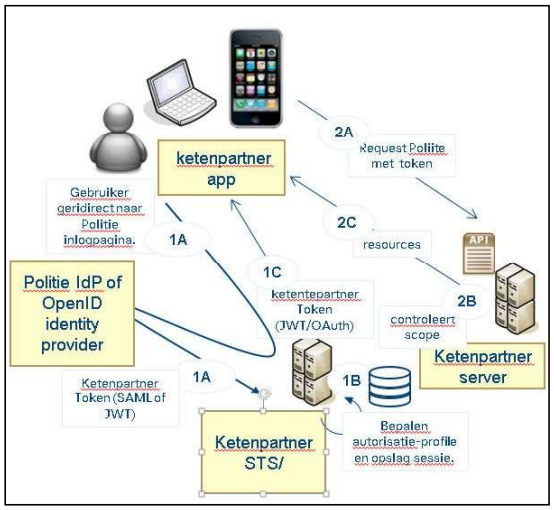
Voor outbound koppelingen zijn het de resources van de ketenpartijen die worden vrijgegeven.

Daarom wordt de beslissing welk profiel wordt gebruik, genomen door de ketenpartner.

1. Autorisatie zorg dat de politiegebruikers toegang krijgen tot de toepassingen van de ketenpartners. Federatie middels een IdP (ook wel OP genaamd bij uitwisseling via OpenID Connect) zorgt dat de identiteit uit het prd.int.politie domein gebruikt kan worden voor toegang tot een toepassing uit een andere, externe organisatie. Om te zorgen dat een *IdP* met de verschillende soorten authenticatieformaten overweg kan is een Security Token Service (STS) noodzakelijk. De STS transformeert de diverse authenticatietokens naar standaard formaten, zoals Kerberos[36], SAML[37] (Security Assertion Markup Language). Het gebruik van meerdere STS’s is mogelijk
2. De ketenparter heeft een SAML service provider (SP) of OpenID Connect Provider (CP). Deze verleent toegang tot de toepassing of service op basis van de afgesproken identiteitsattributen. Het token wordt (door de politie SAML IdP of OpenID Connect identity provider) uitgegeven voor een bepaalde ketenpartij (“audience”)

6.3.2 Inlogproces outbound

Voor inloggen van politie medewerkers bij een ketenpartner app, gelden de volgende stappen.



1. Aanvraag van een token door de app
   A. De app van de ketenpartner redirect de politie gebruiker via de autorisatieserver naar de inlogpagina van de politie. De gebruiker logt in (of heeft al een token).
   B. De STS van de ketenpartner (afhankelijk van het protocol heet dit de Service Provider of ResourceProvider) controleert het token van de politie en bepaalt de toegang tot hun applicatie.
   C. Vervolgens genereert de autorisatieserver van de ketenpartner een eigen token voor die organisatie/app.
2. Gebruik van een token om toegang te krijgen tot resources
   A. De OAuth resource-server (onderdeel van APIM) valideert het token is uitgegeven door de Autorisatie-server (signature validatie)
   B. De Back-end server (niet getekend) voert de autorisatie uit (selecteert het record) aan de hand van de ABAC-attributen en het subjectID (user) en retourneert de politiegegevens.
   C. Wanneer de autorisatie succesvol is wordt er toegang verleend tot de resources

[36] Kerberos, bron: https://nl.wikipedia.org/wiki/Kerberos_(protocol)

[37] SAML, bron: https://nl.wikipedia.org/wiki/Security_Assertion_Markup_Language

Koppelbaarheid

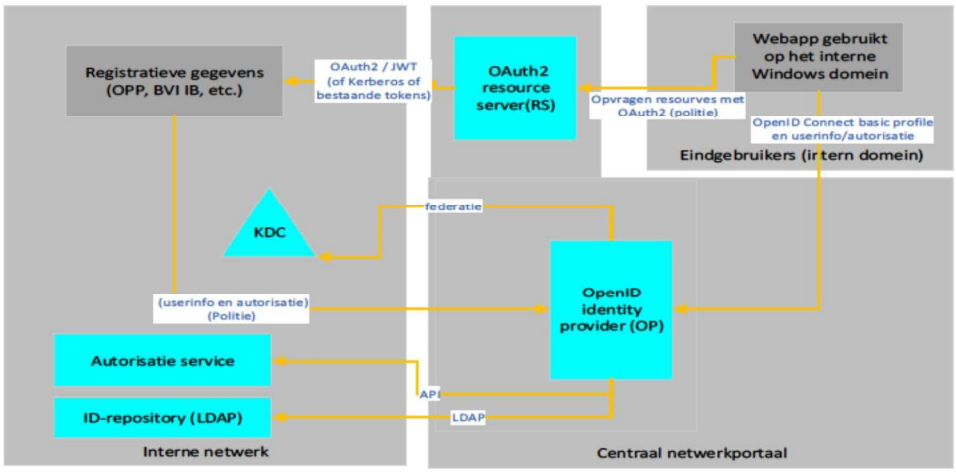
- De federatieve koppeling moet aansluiten op de functionaliteit van aanbieder/afnemer, maar moet technologisch voor de Nationale Politie generiek inzetbaar blijven. Het gebruik van SAML of OpenID Connect als standaard authenticatieprotocol is daar een voorbeeld van.
- De IdP of OpenID provider wordt ingezet als een generieke politie IdP. De politie IdP wordt opgezet als een generieke IdP en is onderdeel van IAM-core (Ondergebracht in de API-M component). De IAM Identity en IAM Role onderdelen van de IAM CORE hebben de invulling van de IdP functies gedelegeerd aan het API-M doelsysteem voor federatie.
    - Voor Outbound vanuit SaaS/ketenpartner applicaties/APIs (data van bijv. ketenpartners zoals DJI) waarop politiemedewerkers inloggen.
    - Voor Inbound vanuit perspectief van de politie apps (politie gegevens) waarop ketenpartners inloggen.
- De voorkeur gaat uit dat de Politie IdP met behulp van Federatie verbonden is met de IdP van ketenpartners (o.a. de IdP van V&J). Voor overheid instanties wordt hier de generieke IdP Broker van de overheid gebruikt.
- Dit betekent dat alle inbound federatieve afnemers gebruik maken van één generieke SAML of OpenID Connect functie. De generieke IdP gebruik maar één URL. De afnemers worden op basis van URL's gescheiden.

6.4 Interne federatie binnen politie

6.4.1 Authenticatie eindgebruikers

Voor applicaties die intern op het politie-Windows domein draaien kan Kerberos worden gebruikt, waardoor gebruikers SSO ervaren met hun Windows-login.

- Voor applicaties die OAuth2 en/of OIDC gebruiken en geen Kerberos, is federatie nodig, zie paragraaf 6.1.1.
- Voor applicaties binnen het politie Windows domein die op Kerberos draaien is dit niet van toepassing. Het doel is in de toekomst alle systemen op basis van OAuth2 en openID Connect te laten werken.



IAM logische functies/building blocks geraakt in de Kerberos flow

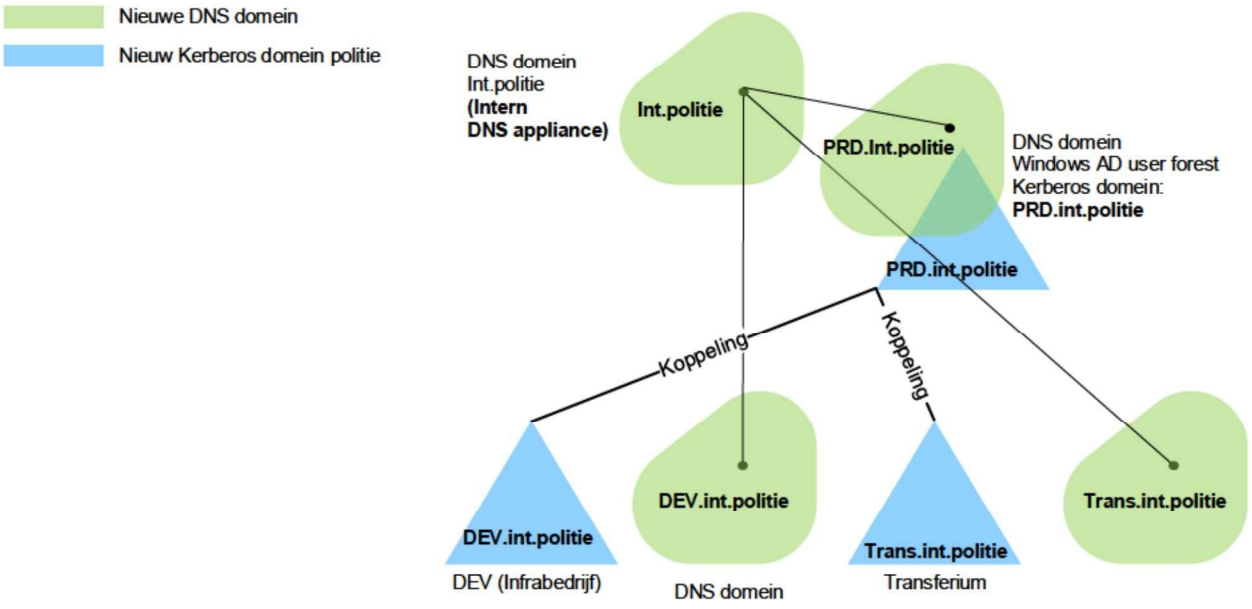
Overige systemen

De flow verschilt met die van de flow in stappen 2a t/m 2c in paragraaf 6.2.2. Hiervoor in de plaats wordt Kerberos-authenticatie gedaan. Het andere verschil is dat de identiteitsattributen en het autorisatieprofiel aan de hand van het gebruikersID in de LDAP worden opgezocht.
De software architectuur is o.a. gebaseerd op deze interne federatieve koppeling. Deze koppeling is in de voorgaande paragraaf 5.6 verder uitgewerkt.

6.4.2 Kerberos-realm politie SOLL

In de uiteindelijke situatie wordt er gebruik gemaakt van het nieuwe gTLD[38] **.politie**. Onder deze gTLD worden de Kerberos-domeinen van de politie gepositioneerd.

Naast het huidige Kerberos-domein, **politie.local** wordt het nieuwe domein **PRD.int.politie** opgebouwd. Beide domeinen hebben geen invloed op elkaar, de systemen/diensten/services kunnen elkaar vinden zowel in 'oud' als in 'nieuw'. Zie onderstaand figuur:



De onderbouwing waarom er gebruik gemaakt wordt van de diverse subdomeinen is in onderstaande tabel toegelicht:

Domein	Functie	Onderbouwing
PRD.int.Politie	User repository politie domein	• In dit domein zijn alle gebruikers opgenomen van de politie; • Het is als apart domein gepositioneerd om het een klantdomein betreft met een beveiligingsbeleid gebaseerd op politie Intern en Confidentieel; • In dit domein zijn de productieresources opgenomen van de politie; • Geënt op stabiliteit, continuïteit en hoge beschikbaarheid.
DEV.int.Politie	Ontwikkel, Test en	• De infrabedrijf OTA-resources (denk hierbij aan Ontwikkel, Test en Acceptatie van AD, IAM, PAM enz.) moeten afgeschermd worden

[38] gTLD; Generic Top Level Domain (Wikipedia)

Domein	Functie	Onderbouwing
	Acceptatie resource domein (infrabedrijf)	omdat deze infrabedrijf-werkzaamheden impact hebben op het productiedomein.
Trans.int.Politie[39]	Transferia resources domein	• Dit domein is apart gepositioneerd omdat de bevoegdheden in deze omgeving ruimer zijn. De afnemer heeft vaak volledige bevoegdheden op zijn of haar omgeving; • Geënt op flexibiliteit en snelheid van implementatie; • Computers en servers binnen Transferia zijn niet standaard en mogen geen "last" krijgen van binnen PRD.int.politie opgelegde veiligheidsmaatregelen zoals policies; • De afnemers beheren zelf de door de afnemer gerealiseerde omgeving (of hier zijn afwijkende afspraken voor gemaakt).

[39] Momenteel (Q2 2021) gebruikt het Transferium vooral digi.intern. Deze moet omgezet worden naar trans.int.politie tijdens het onboarding proces waarbij het transferium als resource domein wordt gepositioneerd onder prd.int.politie

7 Principes IAM

Nummer Principe	Enterprisearchitectuur Informatiebeveiliging principes
SEC-EA-P-02	Identificatie en autorisatie: Toegang tot politie-informatie is altijd uniek herleidbaar tot een persoon.
SEC-EA-P-03	Autorisatie: Aan gebruikers wordt toegang tot de informatievoorziening verleend op basis van uitvoering van de aan hen opgedragen werkzaamheden
SEC-EA-P-04	Metagegevens: Gegevens worden bij opslag en verdere verwerking voorzien van kenmerken die nodig zijn om de correctheid en rechtmatigheid van de gegevensverwerking te kunnen waarborgen.
SEC-EA-P-05	Registratie van handelingen: De informatievoorziening voorziet in de registratie van handelingen van gebruikers en activiteiten van systemen.
SEC-EA-P-06	Beschikbaarheidsfuncties: De benodigde beschikbaarheid ten aanzien van moedwillige beschikbaarheidsverstoringen van informatiediensten dient voorafgaand aan de bouw te worden vastgesteld.
SEC-EA-P-07	Gelaagde Beveiliging: De informatievoorziening wordt door meerdere onderling complementaire typen beveiligingsmaatregelen beschermd.
SEC-EA-P-08	Koppelvlakken: De koppelvlakken tussen onderdelen van de informatievoorziening (compartimenten) worden beheerd met specifieke beveiligingswaarborgen waarbij geen afbreuk wordt gedaan aan de verschillende beveiligingsniveaus van de compartimenten.

7.1 Specifieke principes

In deze paragraaf wordt ingegaan op de voor de IAM geldende specifieke principes en richtlijnen. Algemene principes alsmede principes op het vlak van beheer en beveiliging zijn niet meegenomen.

Principe **TA-P-IAM-01**	**De IAM functionaliteit dient ook ketenpartners te ondersteunen**
Referentie	Zie **SEC-EA-P-02, SEC-EA-P-03, SEC-EA-P-05 & SEC-EA-P-08**
Toelichting	De Nationale Politie werkt nauw samen met Ketenpartners. Er wordt onderling informatie uitgewisseld. Hierdoor moet het mogelijk zijn dat wederzijds informatie opgevraagd en gedeeld kan worden.
Rationale	In de Openbare Orde en Veiligheidsketen is samenwerken en wederzijdse informatie bevraging en uitwisseling cruciaal. Zie ook het authenticatiemechanisme wat door de rijksoverheid is voorgeschreven: OpenID Connect id_token of een SAML 2.0 token[40].

[40] Bron: http://www.logius.nl/fileadmin/logius/product/digid/documenten/Koppelvlakspecificatie_SAML_DigiD4_v2.2.pdf

Implicaties	Identity en Access Management moet dusdanig ingericht worden dat dit de samenwerking tussen ketenpartners bevordert. Indien dit niet meegenomen wordt dan worden er diverse puntoplossingen gerealiseerd die de werkbaarheid en samenwerking tussen de Nationale Politie en Ketenpartners bijna onmogelijk maakt. Dit dient te gebeuren op een manier dat politie of ketenpartner developers geen technische implementatie hoeven te doen - behalve gebruik te maken van het standaard OAuth 2.0 authorization code aansluitpatronon - als zij een app bouwen waarmee ketenpartner gebruikers toegang krijgen tot politie gegevens. Wel moeten zij rechten aanvragen: • Indien nodig nieuwe rollen voor ketenpartner gebruikers en autorisaties in de autorisatiematrix • Systeemrechten voor de ketenpartner IDP (zgn. loa_values) aanvragen in de API developer portal Zie ook **TA-IAM-V-12.**

Principe **TA-P-IAM-02**	**Ketenbreed dient wachtwoordmanagement ingeregeld te zijn**
Referentie	**SEC-EA-P-03, SEC-EA-P-08 & SEC-EA-P-10**
Toelichting	Wachtwoordmanagement moet ingeregeld zijn zodat: - Tijdig geïnformeerd wordt bij verlopen wachtwoord; - Afdwingen wachtwoord wijzigen bij verlopen wachtwoord; - Wachtwoord wijzigen op elk willekeurig moment; - Transport van wachtwoord(en) geschiedt versleuteld
Rationale	Bij IAM is het inregelen van wachtwoord management cruciaal
Implicaties	Wachtwoord management is binnen een eigen organisatie/domein vaak ingeregeld en op orde. Ketenbreed is dit vaak een probleem. Om er voor zorg te dragen dat elke manier van ontsluiting ketenbreed ondersteund wordt moet dit mee genomen worden in de IAM oplossing. De frequentie van het wijzigen moet beperkt worden om geautomatiseerde wachtwoord aanvallen met libraries te voorkomen.

Principe **TA-P-IAM-03**	**Elke tot een natuurlijke persoon herleidbare gebruiker heeft één identity**
Referentie	Zie **uitgangspunt U2** & **SEC-EA-P-02**
Toelichting	Elke tot een natuurlijke persoon herleidbare gebruiker heeft één identiteit dit in verband met auditing, logging, traceerbaarheid, beheerbaarheid enz..
Rationale	Elke gebruiker die tot een natuurlijke persoon herleidbaar is heeft één identiteit.
Implicaties	Voor medewerkers die twee verschillende functies hebben, zoals bijvoorbeeld een Dienst ICT medewerker die ook politievrijwilliger is, geldt op dit principe een uitzondering. Omdat dit twee identiteiten zijn, met aan elke identiteit verschillende autorisatierollen en dus bevoegdheden.

	Vaak heeft een tot een natuurlijke persoon herleidbare gebruiker meerdere identiteiten dit omdat de persoon toegang moet hebben tot meerdere domeinen. De IAM oplossing moet dit adresseren ketenbreed.

Principe **TA-GNI-P-01**	**Single Sign-On**
Referentie	Zie **uitgangspunt U5, SEC-EA-P-07 & SEC-EA-P-08.**
Toelichting	Omdat er OOV breed samengewerkt wordt en informatie gedeeld moet worden is Single Sign-On een “must have”. Dit in verband met gebruiksgemak maar ook vanuit beveiliging. Aangezien er anders diverse wachtwoorden bewaard moeten worden door de gebruiker die hiervoor diverse oplossingen gaat zoeken. Denk hierbij bijvoorbeeld aan “geeltjes” onder het toetsenbord.
Rationale	Samenwerken en informatie uitwisseling wordt bevorderd bij single sign on
Implicaties	Single sign on heeft naast de technische uitdagingen ook organisatorische uitdagingen deze zijn veelal te herleiden op vertrouwen. Vaak is er geen vertrouwen tussen de diverse keten partners waardoor er diverse technische punt oplossingen worden gerealiseerd die qua beheer een grote impact hebben op bruikbaarheid van de ketenbrede diensten. Om dit mogelijk te maken moet er gestandaardiseerd gewerkt worden zowel aan de O- als aan de T-Kant. Denk aan standaard authenticatie protocol (OpenID Connect) maar ook het terug brengen van het aantal identity repositories. De organisatorische implicatie gaat deze referentiearchitectuur IAM niet oplossen.

Principe **TA-P-IAM-04**	**Rolgebaseerd autorisatiemodel**
Referentie	**SEC-EA-P-03**.
Toelichting	Op basis van de functie en de daarbij behorende rol van de gebruiker wordt het rolgebaseerde autorisatiemodel ingericht
Rationale	Bij een functie en daarbij behorende rol hoort een autorisatierol, bij een autorisatierol horen toegekende bevoegdheden.
Implicaties	Bij de inrichting van IAM dienen op basis van de verschillende functies de rollen van de bijbehorende identiteiten bekend te zijn. Alleen op basis van deze rollen kan IAM gerealiseerd en ingericht worden.

Principe **TA-P-IAM-05**	**Eén logische centrale plaats voor toekennen autorisaties**
Referentie	Zie **uitgangspunt U2** & **SEC-EA-P-03**
Toelichting	Bij bepaalde rollen horen bepaalde bevoegdheden deze bevoegdheden worden toegekend op basisautorisaties. Een autorisatie is een bepaald bevoegdheid dat een rol heeft op een resource.
Rationale	Eenvoudiger en daardoor veiliger en beter beheerbaar
Implicaties	Momenteel zijn er diverse autorisatie systemen zowel centraal als decentraal. De diverse plaatsen waar autorisaties plaats vinden moeten terug gebracht worden naar één logische centraal plaats.

Principe **TA-P-IAM-06**	**Elke applicatie die enige vorm van IAM nodig heeft, dient gebruik te maken van de standaard userInfo API (OpenID Connect) SCIM en pivileges API in plaats van deze zelf te implementeren.**
Referentie	Zie **uitgangspunt U5** & **SEC-EA-P-06 &** Deelarchitectuur Autorisatiemanagement
Toelichting	Daarnaast dient de Applicatie voor de implementatie van authenticatie en autorisatie gebruik te maken van de ABAC/RBAC attributen (gegevensdomein, subdomein, bereik, gebruik, privacyStatus, embargo, afscherming en verwerkingsstatus). Op deze wijze ontstaat er geen afhankelijkheid tussen de broncode en de toegepaste Identity Repository. Deze kan dan via configuratie parameters gekozen en veranderd worden. Bovendien is er geen afhankelijkheid met de RBAC rollen en is de autorisatie middels een eenvoudig generiek mechanisme zonder hard-gecodeerde regels af te leiden.
Rationale	Identity Repository, de OAuth2 Authorisation server en de OpenID Connect attributeprovider (AP) zijn centraal landelijk belegd.
Implicaties	Momenteel bevatten veel legacy applicaties een eigen identity repository en mechanisme voor identity propagatie en sessiebeheer. Deze moeten eerst gesaneerd worden voordat er gekoppeld wordt met IAM-core via de beschreven OAuth2 en OIDC profielen en richtlijnen voor mobiel apps, webapplicaties en systeemkoppelingen Voor gegevens en functionele autorisatie moeten applicaties gebruik maken van de Autorisatie SVC van de IAM Core.

Principe **TA-P-IAM-07**	**Eén repository voor IAM met metagegevens**
Referentie	Zie **uitgangspunt U5, U2** & **SEC-EA-P-06 & SEC-EA-P-08**
Toelichting	Er is één repository voor IAM met de metagegevens van de gebruikers. Hierbij moet gedacht worden aan gegevens zoals rol, e-mail adres enz..
Rationale	Meta gegevens zijn beschikbaar vanuit één single point of truth.

Implicaties	Meta gegevens van de gebruikers zijn her en der verspreid binnen de ICT Infrastructuur en applicaties. Daarnaast zijn er ook verschillende bronnen. Bij de implementatie van IAM moeten de single point of truth bron(nen) voor meta gegevens bekend zijn. Deze bronnen zijn de userInfo API en de SCIM API.

Principe **TA-P-IAM-08**	**Eén generieke Identiteit & Toegang Management dienst**
Referentie	Zie **uitgangspunt U5, U2** & **SEC-EA-P-02 & SEC-EA-P-04**
Toelichting	Er moet maar één IAM-systeem beschikbaar zijn binnen één domein/organisatie. Deze centrale toegangscontrole geschiedt op basis van bijvoorbeeld locatie, (generieke) wijze van authenticatie (conform NORA), gebruik van 'strong-authentication' indien …. enz.
Rationale	Het centrale IGA mechanisme "IAM core" is voor Identiteit & Toegang single point of Truth.
Implicaties	Momenteel zijn er meerdere "IAM" systemen aanwezig binnen de Nationale Politie. Dit moet terug gebracht worden tot één.

Principe **TA-P-IAM-09**	**IAM-core ondersteunt alleen standaard koppelingen**
Referentie	Zie **uitgangspunt U3** & **U4, SEC-EA-P-08**
Toelichting	Het IAM-systeem levert geen extra intelligentie. Dit geldt ook voor de koppeling (denk hierbij aan transities, vertalingen, conversies enz..).
Rationale	Een koppeling moet generiek en gebaseerd op standaards zijn. • De ondersteunde standaarden zijn OAuth2, OpenID Connect. • De systeem- en functionele autorisatie wordt gerealiseerd middels OAuth scopes. • De gegevens autorisatie zijn beschikbaar via autorisatie services (waaronder de autorisatie beslissing en betrokkenheden / R2D2 API)
Implicaties	Indien de koppeling met IAM-core voorzien wordt van extra intelligentie en/of maatwerk dan heeft dit impact op beheer en complexiteit van IAM-core. Tevens kan het gevolgen hebben voor het de product life-cycle van IAM. Aangezien de implementatie van een nieuwe versie tot gevolg kan hebben dat de maatwerkkoppeling niet meer functioneert. *Wanneer dit toch een eis is van de organisatie dan dient dit apart te worden opgepakt. Dit wordt dan uitgewerkt in een apart document waarin de consequenties en gevolgen hiervan zowel voor techniek als organisatie duidelijk geadresseerd worden.*

Bijlage A Definities & Begrippen

Zie hier voor de IV-architectuur website; termen en begrippen.

Bijlage B IAM en Keycloak

administratie voeren en integratie verzorgen rondom authenticatie.

Het omtrent identiteiten administratie voeren en integratie verzorgen rondom authenticatie is er beleid om met een centrale bron van gebruikers en identiteiten te werken. Deze wordt met IAM toepassing One Identity i.c.m. o.a. Webshop (ATL) volledig en juist gehouden.

Identiteiten administratie voeren en integratie verzorgen rondom authenticatie moet bij gebruik van Keycloak worden voorkomen.

Het ontwikkelteam moet gebruik maken van deze centrale bron. Daartoe moet er een verbinding aangegaan worden.

De centrale bron (voor identiteiten administratie) wordt aangeboden via standaard oplossingen als AD en OAUTH2/API-Mgt. Indien de standaard oplossing niet gebruik kan worden, treedt er architectuurschuld op. “Comply or Explain” is hier van toepassing en accordering van ABI(V).

Wanneer er onderbouw en geaccordeerd geen gebruik gemaakt kan worden van de standaard oplossing dan heeft de voorkeur dat er tijdelijk (of permanent mist dit geaccordeerd is in het ABI(V)) gebruik gemaakt wordt van Keycloak.

De volgende oplossing wordt gehanteerd:

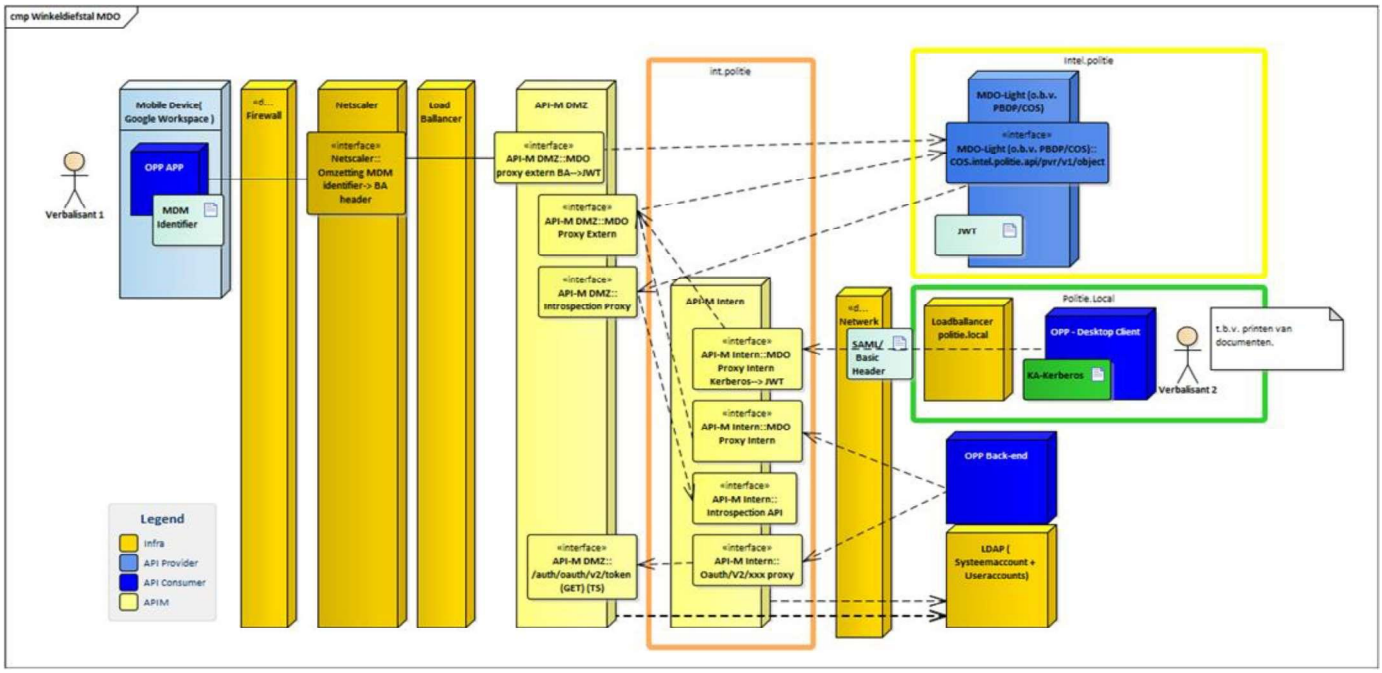
1) Het ontwikkelteam dat SSO wil ontwikkelen met Keycloak moet aangeven hoe Keycloak ingezet wordt
2) Hierna wordt dit getoetst hoe Keycloak wordt ingezet
3) Als Keycloak vooral integratie doet dan is dit geen probleem. Als het echter ook identiteiten administratie doet dan moeten we dat aspect wegnemen (direct, maar eventueel met een tijdslijn).

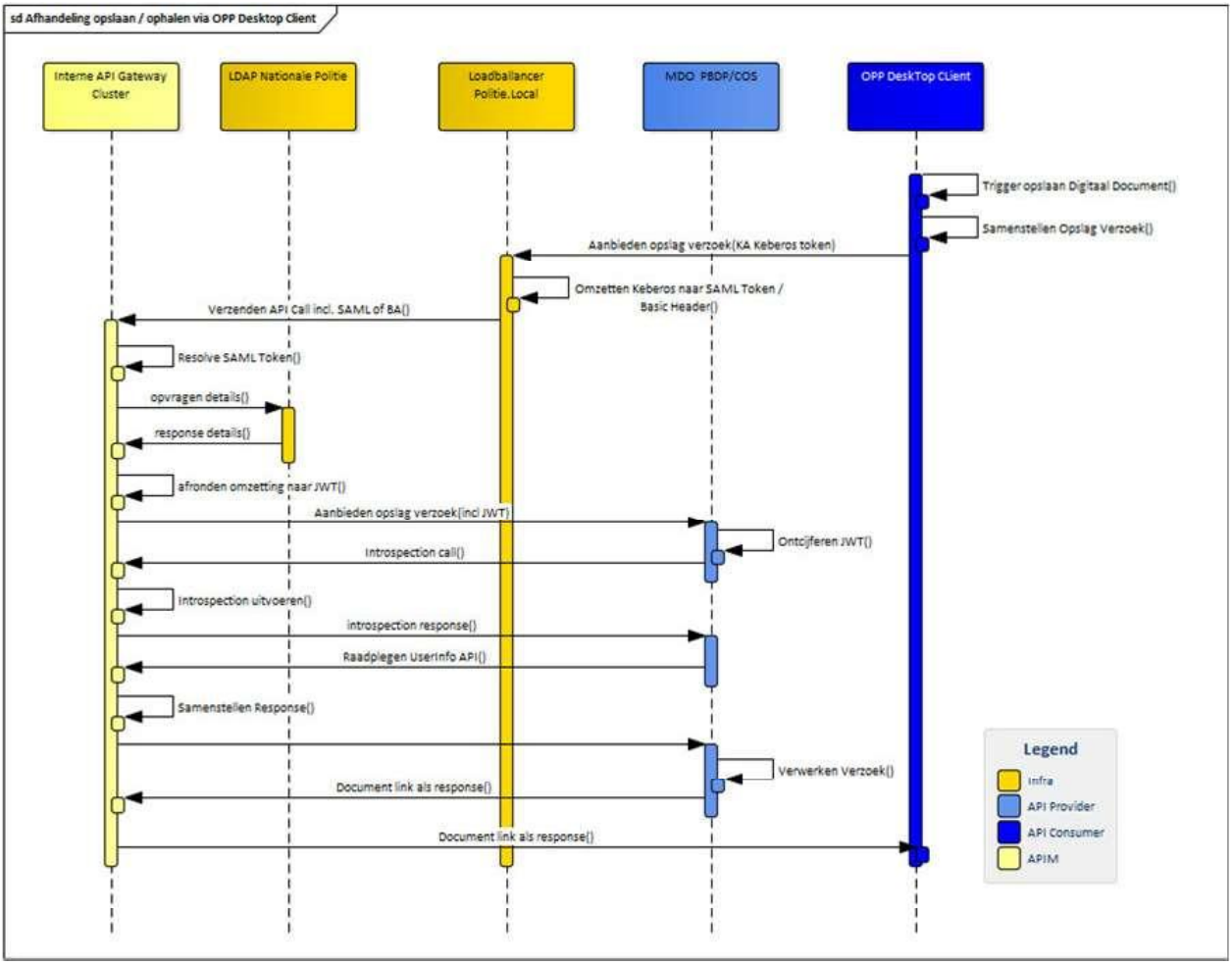
NB.

Een overzicht van de functies https://www.keycloak.org/ en de markering welke functie in ieder geval niet gebruikt mag worden.

Bijlage C Tijdelijke federatieve koppeling F5-API-GW

Gegeven het feit dat er geen Kerberos keytab kan worden ingelezen op de API-gateway is de onderstaande tussenoplossing uitgewerkt.




sd Afhandeling opslaan / ophalen via OPP Desktop Client
Interne API Gateway Cluster
LDAP Nationale Politie
Loadballancer Politie.Local
MDO PBDP/COS
OPP DeskTop CLient
Trigger opslaan Digitaal Document()
Samenstellen Opslag Verzoek()
Aanbieden opslag verzoek(KA Keberos token)
Omzetten Keberos naar SAML Token / Basic Header()
Verzenden API Call incl. SAML of BA()
Resolve SAML Token()
opvragen details()
response details()
afronden omzetting naar JWT()
Aanbieden opslag verzoek(incl JWT)
Ontcijferen JWT()
Introspection call()
Introspection uitvoeren()
Introspection response()
Raadplegen UserInfo API()
Samenstellen Response()
Verwerken Verzoek()
Document link als response()
Document link als response()
Legend
Infra
API Provider
API Consumer
APIM

Bijlage D Roadmap IAM 2021-2022