



Aanbesteding IAM/IGA

Bijlage G Casussen en demonstratie IAM-VRU



Inhoud

1. Inleiding.....	3
2. Uitgangssituatie	4
3. Opzet rollenmodel	5
Casus 1: Standaard IDU-proces.....	6
Casus 2: Monitoring, audit, rapportage	7
Casus 3: Rol leidinggevende.....	8
Casus 4: Rol medewerker.....	9
Casus 5: Rol beheerder, nieuwe rol	10
Casus 6: Rol beheerder, nieuwe applicatie.....	11
Casus 7: Ketenpartner of piketmedewerker.....	12



1. Inleiding

Dit document bevat de casussen die tijdens de demonstratie worden getoond. Ze geven Opdrachtgever inzicht in de manier waarop de aangeboden oplossing invulling geeft aan de eisen en wensen.

Hoofdstuk 4 tot en met 7 volgen de zeven casussen uit de bijlage bij de aanbesteding: de rol van de leidinggevende, de medewerker en de beheerder. Hoofdstuk 8 tot en met 10 zijn aanvullende casussen over het standaard IDU-proces, andere partijen en rapportage. Die laten zien hoe de rollen in de dagelijkse praktijk van een veiligheidsregio worden toegepast.

In de uitwerking wordt ook gekeken naar gebruiksvriendelijkheid en naar wat functioneel beheer zelf kan doen. Datums, afdelingen en accountnamen in de casussen zijn voorbeelden. In de demo-omgeving worden deze vooraf klaargezet.



2. Uitgangssituatie

De casussen gaan uit van de huidige inrichting bij de Aanbestedende Dienst:

- Active Directory (on-premises) is leidend. Accounts en groepen worden door de IAM-oplossing in AD aangemaakt en gewijzigd.
- Entra ID wordt via hybride synchronisatie gevuld vanuit AD. Wijzigingen in AD komen na de volgende synchronisatiecyclus in Entra ID en M365.
- M365-licenties worden toegekend via groepen, zodat ook licenties vanuit de IAM-oplossing gestuurd worden.
- Het HR-systeem is de bron voor medewerkers. Vrijwilligers, inhuur en medewerkers van andere partijen staan niet (altijd) in het HR-systeem en worden via een formulier in de IAM-oplossing opgevoerd.
- Applicaties worden aangesloten via een connector (API, SCIM, database). Waar dat niet kan, loopt de toekenning via een taak voor beheer met terugmelding.
- Voor applicaties zonder API en voor identiteiten die niet in het HR-systeem staan, ondersteunt de oplossing import en export via CSV-bestanden. Accounts en rechten worden periodiek ingelezen. Wijzigingen worden als bestand klaargezet voor de applicatie.

Identiteitstypen

Type	Bron	Toelichting
Medewerker	HR-systeem	Vast of tijdelijk dienstverband
Vrijwilliger	HR-systeem of formulier	Bijvoorbeeld vrijwillig brandweerpersoneel
Inhuur	Formulier	Met verantwoordelijke en verplichte einddatum
Andere partij	Formulier	Medewerker van een ketenpartner, leverancier of andere overheidsorganisatie
Functioneel account	Formulier	Gedeelde mailbox, service- of systeemaccount, altijd met eigenaar



3. Opzet rollenmodel

Het rollenmodel is de basis voor alle scenario's. De opzet is bewust eenvoudig gehouden, zodat het voor leidinggevendenden begrijpelijk en voor beheer onderhoudbaar blijft. We werken met drie lagen.

Laag	Wat	Voorbeeld
Basisrol	Wat iedereen van een bepaald identiteitstype krijgt	Account, mailbox, M365-licentie, intranet
Functierol	Bundel van rechten voor een afdeling of functie, automatisch toegekend op basis van HR-gegevens	Medewerker Risicobeheersing, Piketfunctionaris crisisbeheersing
Applicatierecht	Een los recht in een applicatie of een AD-groep. Onderdeel van een functierol of los aan te vragen	Crisisapplicatie gebruiker, GIS-viewer, roosterapplicatie planner

Wat bij een rol wordt vastgelegd

- Naam en omschrijving in gewone taal, zodat een leidinggevende begrijpt wat de rol inhoudt.
- Eigenaar van de rol (meestal het afdelingshoofd) en wie de rol inhoudelijk mag wijzigen.
- Voorwaarden voor automatische toekenning, bijvoorbeeld afdeling, functie, type dienstverband of piketfunctie uit het HR-systeem.
- De applicatierechten en AD-groepen die aan de rol hangen, en per recht of dit automatisch gaat of een handmatige handeling vraagt.
- Wie de rol mag aanvragen als deze niet automatisch wordt toegekend, en wie moet goedkeuren.
- Eventuele conflicten met andere rollen (functiescheiding).

Aanpak

We beginnen met de basisrollen en een beperkt aantal functierollen voor de grotere afdelingen. De bestaande AD-groepen en het HR-systeem gebruiken we om met role mining voorstellen te doen voor rollen. Die voorstellen worden met de leidinggevendenden doorgenomen voordat ze actief worden. Rechten die maar bij een paar mensen voorkomen blijven losse aanvraagbare rechten en worden niet in een rol gestopt. Zo voorkomen we een model met honderden rollen die niemand meer overziet.

Bij de naamgeving van groepen in AD houden we een vaste conventie aan, zodat direct zichtbaar is of een groep door de IAM-oplossing wordt beheerd. Bijvoorbeeld een prefix voor rolgroepen en een prefix voor applicatiegroepen.



Casus 1: Standaard Instroom Doorstroom Uitstroom (IDU)-proces

Beschrijving proces:

Een nieuwe medewerker wordt in het HR-systeem geregistreerd en komt over drie weken in dienst bij de afdeling Risicobeheersing. Binnen de organisatie werkt al een collega met dezelfde naam. Bij de registratie is de achternaam verkeerd gespeld, dit wordt later door HR gecorrigeerd. De VOG is bij registratie nog niet binnen.

In dezelfde casus nemen we een doorstroom en een uitstroom mee. Een medewerker die via inhuur bij Bedrijfsvoering werkt, komt in vaste dienst bij Crisisbeheersing en krijgt een piketfunctie. Een andere medewerker gaat uit dienst en moet nog een paar maanden bij zijn loonstroken en jaaropgave kunnen.

Wat Opdrachtgever in de demonstratie wil zien:

Nr	Functionaliteit
a.	AD-account en e-mailadres worden aangemaakt volgens de naamconventie, inclusief de afhandeling bij een naamconflict.
b.	Controle op dubbele identiteiten en de afhandeling daarvan.
c.	Correctie van de achternaam in het HR-systeem en de verwerking in de IAM-oplossing, AD en Entra ID.
d.	Toekennen van autorisaties op basis van bedrijfsregels: - account wordt inactief aangemaakt bij registratie, zodat middelen aangevraagd kunnen worden; - account en M365-licentie worden actief per datum in dienst; - functierol op basis van afdeling; - geen autorisaties als de VOG per datum in dienst niet is aangeleverd, met melding aan de verantwoordelijke.
e.	Met één handeling alle autorisaties van een identiteit deactiveren en weer heractiveren.
f.	Doorstroom: bestaande identiteit en account blijven behouden, rollen worden aangepast, oude rechten ingetrokken en conflicterende rechten gesignaleerd.
g.	Uitstroom: account blokkeren, autorisaties en groepen intrekken, verwerking in gekoppelde systemen en een uitzondering voor bepaalde autorisaties.
h.	Logging en audittrail van alle stappen.



Casus 2: Monitoring, audit, rapportage

Beschrijving proces

De Aanbestedende Dienst heeft verschillende gebruikers; Leidinggevenden, beheer, de security officer en de auditor hebben ieder hun eigen behoefte aan overzicht. In de demo-omgeving is een medewerker rechtstreeks in AD aan een groep toegevoegd, en staan er accounts in AD en Entra ID die niet via de IAM-oplossing zijn aangemaakt.

Wat de Aanbestedende Dienst in de demonstratie wil zien:

Nr	Functionaliteit
a.	Overzicht van wie, wanneer en met welke bevoegdheden toegang heeft gehad en hoe deze verkregen is. Zoeken, sorteren en filteren op identiteitsgegevens, rollen en autorisaties.
b.	Periodieke attestatie door eigenaren, inclusief intrekken van een recht met reden en notificatie.
c.	Afwijkingen tussen het rollenmodel en de werkelijke rechten in AD en applicaties, en de afhandeling daarvan.
d.	Accounts die rechtstreeks in AD of Entra ID zijn aangemaakt en niet via de IAM-oplossing.
e.	Bewaking van openstaande taken voor leidinggevenden, HR en beheer.



Casus 3: Rol leidinggevende

Situatie

Een leidinggevende wil zien welke rollen er voor de eigen afdeling bestaan, welke rechten daaraan hangen en welke medewerkers in welke rol zitten. In dit voorbeeld is dit het hoofd van de afdeling Risicobeheersing.

Wat de Aanbestedende Dienst in de demonstratie wil zien:

Nr	Functionaliteit
1.	Inzien van de rollen voor de eigen afdeling.
2.	Inzien wat een rol betekent: welke toekenningen van applicaties en rechten hangen hieraan, gaat dit automatisch of is er een handmatige handeling vereist.
3.	Per rol bekijken welke medewerkers deze rol hebben.
4.	Per medewerker bekijken welke rollen en toekenningen de medewerker heeft.



Casus 4: Rol medewerker, Serviceportaal

Situatie

Een medewerker vraagt toegang tot een applicatie via een losse aanvraag. In het voorbeeld vraagt een medewerker van Bedrijfsvoering toegang tot een applicatie waarvoor een aparte licentie nodig is.

Wat de Aanbestedende Dienst in de demonstratie wil zien:

Nr	Functionaliteit
1.	Medewerker logt in op de oplossing.
2.	Medewerker selecteert de gevraagde autorisatie uit een lijst en vraagt deze aan.
3.	Eigenaar (leidinggevende en/of beheerafdeling) accordeert of weigert de aanvraag.
4.	Systeem controleert indien mogelijk op beschikbare licenties.
5.	Toegang wordt automatisch geregeld.
6.	Medewerker ontvangt een notificatie.
7.	Aanvullend: signaleren van conflicterende rechten en het tijdelijk toestaan daarvan.
8.	Aanvullend: tijdelijke toegang met einddatum en automatisch intrekken.
9.	Aanvullend: vervanging van de goedkeurder bij afwezigheid.



Casus 5: Rol beheerder, nieuwe rol

Situatie

De beheerder richt een nieuwe rol in en voegt daar autorisaties aan toe. In het voorbeeld gaat het om een rol voor medewerkers met een piketfunctie in de crisisorganisatie. Daarnaast wordt een bestaande rol aangepast.

Wat de Aanbestedende Dienst in de demonstratie wil zien:

Nr	Functionaliteit
1.	Maak de rol aan.
2.	Voeg de bevoegdheden aan de rol toe.
3.	Stel in onder welke voorwaarden de rol wordt toegepast. Aanvullend: eigenaarschap, aanvraagbevoegdheid en conflicterende rollen vastleggen bij de rol.
4.	Pas de bevoegdheden van een bestaande rol aan.
5.	Toon een overzicht van de toe te passen wijzigingen.
6.	Verwerk de wijzigingen.



Casus 6: Rol beheerder, nieuwe applicatie

Situatie

De beheerder sluit een nieuwe applicatie aan. In het voorbeeld is dit een SaaS-applicatie voor registratie van incidenten, die al een tijd in gebruik is. Er bestaan dus al accounts en rechten in de applicatie.

Wat de Aanbestedende Dienst in de demonstratie wil zien:

Nr	Functionaliteit
1.	Sluit de applicatie aan.
2.	Lees de bestaande rechten uit (indien van toepassing).
3.	Systeem geeft suggesties voor het toevoegen van rechten aan bestaande of nieuwe rollen binnen de oplossing.
4.	Beheerder verwerkt de rechten naar bestaande of nieuwe rollen.
5.	Test de werking: rechten tot de applicatie of in de applicatie worden toegevoegd voor de medewerker.



Casus 7: Ketenpartner of piketmedewerker

Situatie

Niet iedereen die toegang nodig heeft staat in het HR-systeem. Denk aan een medewerker van een ketenpartner die meedraait in de crisisorganisatie, of een externe piketmedewerker die voor een periode wordt ingezet. Deze personen worden in de IAM-oplossing zelf opgevoerd, met een verantwoordelijke binnen de veiligheidsregio en een einddatum.

Opvoeren kan op twee manieren. Een losse medewerker wordt via een formulier in het serviceportaal opgevoerd. Levert een ketenpartner een lijst aan met meerdere medewerkers, bijvoorbeeld de piketbezetting voor het komende jaar, dan wordt die lijst in één keer ingelezen via de CSV-import zoals beschreven in hoofdstuk 2. Voor beide manieren gelden dezelfde verplichte velden en controles.

In het voorbeeld wordt een externe piketmedewerker opgevoerd die toegang nodig heeft tot de crisisapplicatie. Er zijn twee varianten: de medewerker krijgt een account in AD van de veiligheidsregio, of logt in met het eigen account van de eigen organisatie als gast in Entra ID.

Wat de Aanbestedende Dienst in de demonstratie wil zien:

Nr	Functionaliteit
1.	Opvoeren van de identiteit in de IAM-oplossing in plaats van in het HR-systeem, met verplichte velden: naam, organisatie, functie, verantwoordelijke binnen de veiligheidsregio, ingangsdatum, einddatum en rol.
2.	Vastleggen van eigenaarschap: wie is verantwoordelijk voor de identiteit en wie keurt de toegang goed.
3.	Toekennen van de piketrol en de bijbehorende rechten.
4.	Variant met account in AD en variant met inloggen als gast via het eigen account.
5.	Notificaties aan de verantwoordelijke bij het naderen van de einddatum en verlengen van de toegang.
6	Automatisch intrekken van de toegang bij het verlopen van de einddatum of bij vertrek bij de eigen organisatie.