



Aanbesteding IAM

Casus en demo



Inhoud

1.	Inleiding	4
2.	Casus: Standaard IDU-proces	5
3.	Casus: Niet-medewerker	6
4.	Casus: Selfservice	7
5.	Casus: Monitoring, audit, rapportage	8
6.	Casus: Beheer	9

1. Inleiding

Dit document bevat een aantal casussen die Opdrachtgever inzicht moet geven in de wijze waarop invulling gegeven wordt aan de eisen en wensen. Per regel is ook expliciet een verwijzing naar één of meerdere eisen benoemd. In de uitwerking van de casussen wordt ook gekeken naar de mate van gebruikersvriendelijkheid van het IAM-systeem.

2. Casus: Standaard IDU-proces

Beschrijving proces:

Het is 5 oktober en in YouForce/Beaufort wordt een nieuwe medewerker geregistreerd die per 1 november bij de partnerorganisatie op de marketingafdeling in dienst komt. De desbetreffende medewerker heet Jan Janssen en daarvan is al een identiteit bekend van een medewerker die al jaren bij dezelfde partnerorganisatie werkt. De nieuwe medewerker krijgt een basisrol met een M365-account en moet toegang krijgen tot één extra applicatie.

Wat Opdrachtgever in de uitwerking wil zien:

Nr	Functionaliteit	Eis
a.	AD-account en E-mailadres wordt aangemaakt volgens conventie van de partnerorganisatie. Gebruik voor conventie AD-account een willekeurige conventie. Gebruik voor conventie E-mailadres voorletter + "." + achternaam + domeinnaam.	2
b.	Uitvoeren van een controle op dubbele identiteiten per partnerorganisatie en de afhandeling in geval een dubbele identiteit ontstaat.	4
c.	In dit geval was de achternaam niet juist geregistreerd in Beaufort en deze moet worden gecorrigeerd. Laat zien hoe deze correctie in IAM-systeem en doelsysteem wordt afgehandeld.	2
d.	Hoe op basis van de volgende bedrijfsregels autorisaties worden toegekend: - Account wordt per 5 oktober inactief aangemaakt zodat middelen via TOPdesk aangevraagd kunnen worden. - M365-Account wordt actief per datum in dienst, 1 november, inclusief licentie - Toegang tot een marketingapplicatie - Geen autorisatie wordt verleend indien de VOG per datum in dienst niet is aangeleverd en hoe de verantwoordelijke hierover geïnformeerd wordt.	10 24
e.	Hoe bij een identiteit met 1 druk op de knop alle autorisaties gedeactiveerd worden en ook hoe dit weer geheractiveerd kan worden.	13

3. Casus: Niet-medewerker

Beschrijving proces

Een gemeente werkt veel samen met (keten)partners. Dit kan een veelheid van verschillende publieke en private partijen zijn. Deze partijen werken in los of vast verband, soms namens de gemeente. Daarvoor is vaak ook toegang tot applicaties van de gemeente nodig.

In deze casus werkt een gemeentelijke medewerker samen met medewerkers van de Nationale politie. Voor het bestrijden van ondermijning zijn er specifieke applicaties die informatiedeling mogelijk maken. Een medewerker van de nationale politie moet toegang tot deze ondermijning-applicatie verkrijgen en daarom bekend worden gemaakt in ons IAM-systeem. De politiemedewerker heeft het mailadres nomen.nomad@politie.nl en inlogaccount ISC09776. De Nationale politie beschikt over Quest One Identity als IAM oplossing.

In de casus willen we graag terugzien hoe er een koppeling wordt gerealiseerd tussen de Nationale Politie en de IAM oplossing van het SSC ONS op zo'n wijze dat het een robuuste manier van identiteit ontlenen is.

In de uitwerking zien we twee scenario's van de casus:

1. hoe de politiemedewerker een volledige desktop met partner-account inclusief autorisatie tot de ondermijning-applicatie krijgt.
2. hoe de politiemedewerker geen partner-account krijgt, maar wel de mogelijkheid krijgt om met het politie-account (extern) in te loggen op de ondermijning-applicatie. We nemen aan dat de ondermijning-applicatie vanuit extern te benaderen is. Voor de rest worden eventuele aannames onder de 'best case scenario' meegenomen.

Wat Opdrachtgever in de uitwerking wil zien:

Nr	Functionaliteit	Eis
a.	Hoe de identiteit van de politiemedewerker met de volgende gegevens wordt opgevoerd, waarbij (v) verplichte velden zijn: achternaam(v), tussenvoegsels, voornaam(v), samengestelde naam(afgeleid), organisatie(v), afdeling(v), functie, locatie, leidinggevende(v), ingangsdatum(v), einddatum(v), rol(v). Hoe een identiteit volgens scenario-1 wordt aangemaakt.	6 5
b.	Hoe een identiteit volgens scenario-2 wordt aangemaakt.	5

4. Casus: Selfservice

Beschrijving proces

Het IAM-systeem wordt gebruikt door verschillende gemeenten die diensten afnemen bij SSC Ons. Standaard krijgt een medewerker een basisrol en autorisaties volgens bedrijfsregels en RBAC. Deze casus moet laten zien

- hoe het aanvraagproces van een autorisatie verloopt in geval rollen of autorisaties handmatig via een selfservice worden aangevraagd
- hoe gebruikersvriendelijk dit proces voor de aanvrager is.
- welke configuraties uitgevoerd moeten worden

Wat Opdrachtgever in de uitwerking wil zien:

Nr	Functionaliteit	Eis
a.	Hoe wordt vastgelegd bij een rol, wie aanvraagbevoegd is.	19
b.	Op welke manier leidinggevend en bij het handmatig aanvragen van autorisaties/rollen voor een nieuwe medewerker worden geholpen door het IAM-systeem.	22
c.	Hoe conflicterende rollen tijdelijk toegestaan worden.	18
d.	Hoe een medewerker tijdelijk autorisatie aanvraagt op een hoog-risico-applicatie via selfserviceportaal.	10
e.	Hoe een leidinggevende een notificatie hiervan krijgt en goedkeurt.	39
f.	Hoe een applicatie-eigenaar een notificatie krijgt van de aanvraag door de medewerker en deze autorisatie-aanvraag afwijst, inclusief notificatie en reden van afwijzing.	22
g.	Hoe een leidinggevende het goedkeuren van taken tijdelijk delegeert aan een collega.	8
h.	Hoe een eigenaar van de ondermijningsapplicatie zelf kan opvragen aan wie autorisaties zijn uitgegeven.	52

5. Casus: Monitoring, audit, rapportage

Beschrijving proces

Zowel SSC-ONS als de partnerorganisaties hebben behoefte aan rapportages. De ene operationeel, andere strategisch. Alle stakeholders moeten worden voorzien in hun rapportagebehoefte. De volwassenheid van deze behoefte is wisselend.

Laat in deze casus zien welke rapportages standaard in het IAM-systeem geleverd worden.

Wat Opdrachtgever minimaal in de uitwerking wil zien:

Nr	Functionaliteit	Eis
a.	Hoe een overzicht eruit ziet waarbij inzichtelijk wordt wie, wanneer en met welke bevoegdheden toegang heeft gehad, en op welke wijze deze verkregen is. Laat zien hoe in dit overzicht gezocht, gesorteerd en gefilterd kan worden op identiteitsattributen, rollen en autorisaties.	51 44
b.	Hoe voor gedefinieerde rapportages t.b.v. attestatie periodiek naar systeemeigenaren gestuurd worden. Laat zien hoe eenvoudig de systeemeigenaar een autorisatie kan intrekken, inclusief notificatie met reden.	49
c.	Hoe de afwijkingen tussen autorisaties volgens het autorisatiemodel en de werkelijk geregistreerde autorisaties laat zien, Laat zien hoe deze afwijkingen afgehandeld kunnen worden.	57 58
d.	Welke accounts zijn rechtstreeks AD/AAD aangemaakt en niet via IAM.	55
e.	Voor verschillende gebruikers van het IAM-systeem zullen taken openstaan, voor functioneel beheer HR, voor leidinggevenden, rolbeheerders bij de verschillende partners. Hoe worden openstaande taken bewaakt.	43

6. Casus: Beheer

Beschrijving proces

De Opdrachtgever SSC Ons werkt voor verschillende partnerorganisaties. In deze aanbesteding gaan wij ervan uit dat het functioneel beheer van het IAM-systeem door SSC Ons uitgevoerd wordt. SSC Ons krijgt daarmee veel configuratieverzoeken van autorisatieprofielen die in het IAM-systeem in productie gebracht moet worden. Daarvoor is het voor beheer belangrijk om eenvoudig onderscheid tussen de partnerorganisaties te maken. We willen voorkomen dat configuratie A voor partner B geïmplementeerd wordt.

Laat in deze casus zien hoe het voor SSC Ons zo eenvoudig mogelijk gemaakt wordt om een grote hoeveelheid aan wijzigingsverzoeken voor rollen/profielen te configureren voor verschillende partnerorganisaties.

Wat Opdrachtgever in de uitwerking wil zien:

Nr	Functionaliteit	Eis
a.	Laat zien hoe autorisatieprofielen gemaakt worden.	26
b.	Laat zien hoe koppelingen met doelsystemen geconfigureerd worden, zowel SAAS als on-prem-systemen. Welke technieken worden toegepast en welke kennis is nodig?	25 29 9
c.	Laat zien op welke wijze het IAM-systeem in 1 centraal systeem meerdere organisaties en meerdere tenants kan ondersteunen.	31
d.	Laat zien dat een rolbeheerder van de gemeente Zwolle alleen inzicht heeft in de identiteiten, rollen en autorisaties van de gemeente Zwolle. Log in als rolbeheerder van de Provincie en laat zien dat alleen de identiteiten, rollen en autorisaties van de Provincie zichtbaar zijn.	28
e.	Log in als beheerder van SSC Ons en laat zien dat de beheerder alle Laat zien dat een beheerder van Opdrachtgever eenvoudig het beheer, dus niet te veel muisklikken, en ook minimale kans op fouten taken kan uitvoeren. B.v. Het aanmaken van rollen.	28