SOC Team
Zwarte Woud 2
3524 SJ Utrecht
Telefoon 030 252 3004
Email soc@ggdghor.nl

Onboarding Applicatie – Checklist

Aansluiten nieuwe dienst via GGDGHOR IAM aan de AccountProviders

Versie: 0.04

Opdrachtgever	Peter de Koning	Manager SOC GGD GHOR
Auteur	Mesut Kumas	IAM GGD GHOR

Rapportnummer	
Classificatie	Intern
Status	Voorlopig
Datum	21 april 2021
File Naam	Onboarding Applicatie – Technisch IAM

Voorlopig versie 0.02

Inhoud

Documentbeheer

Versiebeheer

Versie	Datum	Auteur	Omschrijving verandering	Status
0.01	07-04-2021	Mesut Kumas	Initiële opzet	Concept
0.02	22-04-2021	Mesut Kumas	Commentaar IAM team verwerken	Voorlopig
0.03	06-07-2021	Michiel Hoogenraad	Certificaat eisen toegevoegd	Voorlopig
0.04	23-12-2021	Michiel Hoogenraad	Versiebeheer aangepast	Voorlopig

Gecontroleerd door

Versie	Datum	Naam	Functie

Geautoriseerd door

Versie	Datum	Naam	Functie
		Peter de Koning	Manager SOC

Gerelateerde documenten

Documenttitel	Omschrijving

Volgende review en/of herziening, plus accordering (tenzij eerdere update)

Datum	Functie voor bewaking
01-06-2021	Manager SOC

1. Inleiding

Met dit document wil GGD GHOR het technisch onboarden van nieuwe applicaties structureren en zorgdragen dat relevante stukken op de juiste plaats worden opgeslagen.

Dit document biedt informatie en een checklist voor het toevoegen van nieuwe applicaties aan de GGDGHOR IAM oplossing (The Identity Hub) om gebruik te maken van de Identity & Access Management (o.a. authenticatie, SSO, Multi-Factor-Authentication) mogelijkheden.

1.1. Scope en doelgroep

Dit document is van toepassing op ***alle*** applicaties die door GGDGHOR, de decentrale GGD's en andere landelijke partners zoals SOS/CED/ANWB/etc. worden ontsloten via de IAM oplossing van de GGDGHOR, namelijk The Identity Hub.

De doelgroep bestaat uit de projectleiders van de aan te sluiten applicatie en de technische projectmedewerkers van de applicaties en de Account Providers.

Dit document beschrijft het onboardingsproces van een applicatie in termen van activiteiten en verantwoordelijkheden tussen de applicatieleverancier, GGDGHOR IAM team, de Account Providers en de projectleider voor de aansluiting.

1.2. Rollen en verantwoordelijkheden

Het IAM team van GGD GHOR is verantwoordelijk voor de inhoud van dit document.

Het IAM-team is verantwoordelijk voor het correct uitvoeren van de handelingen conform dit document.

1.3. Review of audit door het SOC

Desgewenst kan het SOC een review of audit uitvoeren op een applicatie. Dit wordt met name geadviseerd voor applicaties die gevoelige persoonsgegevens verwerken of die onderdeel zijn van een essentieel bedrijfsproces bij een GGD of andere ketenpartners.

1.4. Onderhoud van dit document

Het IAM-team onderhoudt dit document en communiceert deze naar de betrokken medewerkers van het IAM-team en projectmedewerkers.

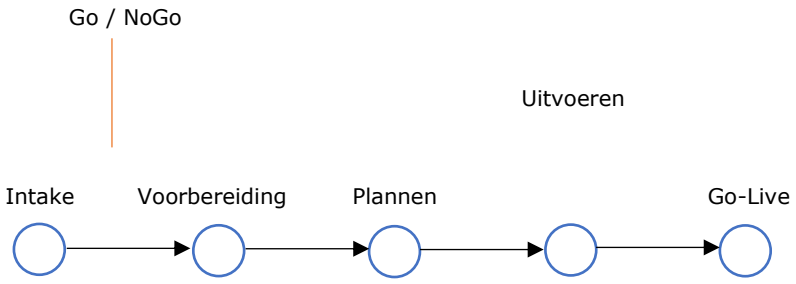
2. Proces onboarding

Het onboardingsproces voor applicaties is een wijzigingsverzoek dat GGDGHOR volgt om een nieuwe dienst toe te voegen aan de IAM oplossing, The Identity Hub (TIH).

Ingang is mail of een Topdesk melding. Een IAM teamlid maakt een wijzigingsverzoek aan namens de aanvrager. Dit teamlid is dan ook de coordinator van de wijziging. De aanvraag wordt concreet gemaakt tijden de intake fase, waar de nodige informatie wordt verzameld om de haalbaarheid te beoordelen. Na de intake wordt het wijzigingsverzoek gehonoreerd (geautoriseerd) of afgewezen. Indien geautoriseerd gaat men verder met de voorbereiding.

Processtappen voor onboarding applicatie
De stappen binnen het proces zijn:

1. **Intake**
2. **Voorbereiding**
3. **Plannen**
4. **Uitvoeren (Inrichten+Testen)**
5. **Go-Live**



Figuur 1

2.1. Intake

De eerste stap is om het wijzigingsverzoek te beoordelen op de volledigheid en correctheid van de informatie. De informatie moet dit ingevulde onboardingsdocument en optioneel metadata-gegevens van de applicatie bevatten. Een medewerker van het IAM-team neemt contact op met de aanmelder en neemt het proces door en de context rondom de aansluiting van de nieuwe applicatie.

Randvoorwaarden

- Applicatie is goedgekeurd door de informatiemanager.
- Applicatie is goedgekeurd door GGDGHOR SOC team.
  i) Het applicatie onboarding document van SOC is volledig ingevuld.
  ii) Er zijn geen showstoppers bekend die de onboarding tegenhouden.
- De aanvrager is een geautoriseerd persoon, bijv de informatiemanager.
- Het applicatie onboardingdocument van IAM (dit document) is volledig ingevuld
- Excel document '**Application Onboarding - Technisch IAM – ClaimMapping**' is ingevuld met de juiste claims/rollen en claimmappings.

Deliverable

- Bevestiging naar de aanmelder dat het wijzigingsverzoek compleet en correct is en naar de volgende fase (Voorbereiding) overgaat.

2.2. Voorbereiding

Zodra de gegevens beschikbaar zijn, zal het IAM-team de wijziging voorbereiden en de verstrekte informatie in detail bekijken. Als de inhoud van de gegevens is gevalideerd en alle details beschikbaar zijn voor implementatie kan de wijziging worden ingepland.

Randvoorwaarden

- Metadata gegevens van aan te sluiten applicatie (SP: Service Provider)

Deliverable

- Bevestiging naar de aanmelder dat de aangeleverde metadata gegevens compleet is en naar de volgende fase (Plannen) overgaat.

2.3. Plannen

De wijziging wordt ingepland door het IAM team samen met de aanmelder. Er wordt door het IAM-team uitgezocht en geregistreerd wat de omvang, timing en risico's zijn van de geplande inzet.

Randvoorwaarden

- Geen

Deliverable

- Plannen van uitvoerdatum van de wijziging

2.4. Uitvoeren

In de uitvoerfase wordt de applicatie aangesloten samen met de applicatie beheerder of leverancier en het IAM team van GGDGHOR. Wanneer de onboarding van de applicatie is voltooid, verwachten we dat ketentesten door de aanmelder in overleg met de applicatiebeheerder en de Account Providers uitgevoerd wordt. Er dienen test-accounts bij de Account Providers en eventueel in de applicatie geregeld te zijn. Het IAM team GGDGHOR kan standby staan en eventueel hierin ondersteunen, de verantwoordelijkheid ligt bij de aanmelder.

Randvoorwaarden

- Testaccounts zijn geregeld in de Applicatie en Account Provider(s)

Deliverable

- Een aangesloten applicatie aan TIH en een succesvol uitgevoerde ketentest.

2.5. Go-Live

In deze fase wordt de aangesloten en succesvol geteste applicatie live gebracht. Hierbij is het belangrijk dat het IAM-team ruim op tijd op de hoogte wordt gebracht van de Go-Live datum zodat de juiste resources vanuit het IAM-team en de IAM-leverancier ingepland kunnen worden. Authenticaties en autorisaties kunnen dan ook gemonitord worden en waar nodig snel geschakeld kunnen worden.

Het informeren of communiceren van de projectorganisatie of serviceorganisatie is niet de verantwoordelijkheid van het IAM team.

3. Applicatie checklist

Deze checklist is noodzakelijk voor de juiste aansluiting aan de IAM oplossing, TIH, van GGDGHOR. Op basis van onderstaande gegevens kan de applicatie SSO aangesloten worden met onder andere de volgende standaarden: SAML, OAuth 2.0, OpenID Connect. Voor alle andere federatieve opties dient u via Topdesk een wijzigingsverzoek in bij het IAM team.

3.1. Contactgegevens

Gegevens van de aanmelder/projectleider

#	Item	Antwoord
1	Naam	
2	Functie	
3	Telefoon	
4	Email	
5	Naam GGD	
6	/ Naam Partner	

Gegevens van de informatiemanager (van GGDGHOR):

#	Item	Antwoord
1	Naam	
2	Functie	
3	Telefoon	
4	Email	

Gegevens van de contactpersoon van de applicatie leverancier (functioneel en/of technisch)

#	Item	Antwoord
1	Naam	
2	Functie	
3	Telefoon	
4	Email	

Gegevens van de applicatie beheerder (functioneel en/of technisch)

#	Item	Antwoord
1	Naam	
2	Functie	
3	Telefoon	
4	Email	

Gegevens van de productowner

#	Item	Antwoord
1	Naam	
2	Functie	
3	Telefoon	
4	Email	

3.2. Applicatie details

#	Item	Omschrijving	Antwoord
1	Naam	Naam van de applicatie	
2	Omschrijving	Wat voor app is het, en waar wordt het voor gebruikt?	
3	Versie	Versie van de applicatie	
4	Documentatie	Documentatie-URL van de applicatie	
5	SSO Methode	SAML/OAuth/OIDC	
6	SLO Methode	Single Logout vereist? Hoe?	
7	User identifier	UPN? Email? Username? Of…	
8	Gebruikersaantallen	Hoeveel gebruikers heeft de app?	
9	Userstore	De applicatie heeft een eigen userstore?	Ja/Nee
10	Pre-provisioning	Is een account binnen de app een randvoorwaarde voor de werking van SSO? Of is dit JIT (Just-In-Time)?	Ja/Nee
11	Authenticatie (huidige situatie)	Hoe wordt de authenticatie nu geregeld?	
12	Autorisatie (huidige situatie)	Hoe worden de autorisaties nu geregeld?	
13	Locatie app	Waar draait de app? Bij de GGD on-premise? Bij een Third-Party (cloud)?	
14	App bevat persoonsgegevens	Persoonsgegevens zoals NAW gegevens worden gebruikt in de app	Ja/Nee
15	Welk domeinnaam gaat gebruikt worden?	Voor de aanvraag van het certificaat is het van belang welk domeinnaam gebruikt wordt.	
16	Welke rollen/veiligheids-groepen gaan gebruikt worden	Een applicatie dient minimaal één rol/veiligheidsgroep te hebben om een gebruiker te autoriseren voor een applicatie. Graag alle rollen vermelden die gebruikt gaan worden.	
17	Welke organisaties gaan gebruik maken van de app?	Een volledig overzicht met alle organisaties die gebruik gaan maken van de applicatie.	
18	Maakt de applicatie gebruik van regiocodes?		

3.3. Applicatie claimmapping

Zie meegeleverd Excel bestand. Graag invullen en meesturen met dit document naar het IAM-team. Zonder ingevulde Excel bestand kan de onboarding niet gerealiseerd worden.

3.4. SSO gebaseerd op SAML 2.0

Vul de volgende gegevens in als de aan te sluiten applicatie gebruik maakt van het SAML protocol.

Is er een metadatabestand aanwezig van de applicatie en is deze publiekelijk beschikbaar? Dan vernemen we graag welke URL's dit zijn. Als deze als XML bestand aangeleverd kan worden per omgeving dan kan dat naar IAM@ggdghor.nl verstuurd worden.

#	Omgeving	Federation Metadata URL
1	DEV	
2	TEST	
3	ACC	
4	PROD	

Graag per omgeving invullen:

#	Item	Omschrijving	Antwoord
1	Issuer *entityID*		
2	Federation Metadata *url*		
3	SSO endpoint *HTTP-POST*		
4	SSO endpoint *HTTP-REDIRECT*		
5	SLO response *url*		
7	nameID		
8	Shared attributes	Welke lijst van minimale attributen verwacht de applicatie?	
9	ACS url	Welk URL wordt gebruikt als ACS-URL. Inclusief ConsumerType (HTTP-POST, HTTP-REDIRECT **not supported**)	
10	Certificaat	Het publieke certificaat graag hier als tekstwaarde plakken	

3.5. SSO gebaseerd op OAUTH 2.0 / OpenID Connect

Vul de volgende gegevens in als de aan te sluiten applicatie gebruik maakt van het OAuth protocol.

#	Item	Omschrijving	TEST	ACC	PROD
1	Client ID	*clientID wordt door GGDGHOR aangeleverd, kan niet gekozen worden.*			
2	Client Secret	*Secret wordt door GGDGHOR aangeleverd, kan niet gekozen worden.*			
3	Scope(s)				
4	Default scope(s)				
5	redirectURL(s)				
6	Signing/Encryption method	RS256 (public/private keys nodig) HMAC, HS256 of een andere…			
7	Token lifetime (access_token)	Hoelang dient een access_token geldig te zijn?			
8	Token lifetime (refresh_token)	Hoelang dient een refresh_token geldig te zijn?			