FOD Beleid & Ondersteuning
SPF Stratégie & Appui

FAS
-
Onboarding Guide

.be

Version 6.4

Inhoudstafel

Algemene informatie

Hieronder wordt "**gebruiker**" gebruikt om te verwijzen naar de klant van FOD BOSA die een online beveiligde overheidsapplicatie ter beschikking stelt, die op zich gebruik maakt van de FAS om de eindgebruikers van deze applicatie te authentificeren. De "**eindgebruiker**" is dus inderdaad de persoon die zich aanmeldt via de FAS op de online beveiligde overheidsapplicatie van de bovenstaande gebruiker.

Beschrijving van het Onboarding proces

Fase	Beschrijving	Opleveringen
1	Aanvraag doen	Een aanvraag doen door het webformulier in te vullen op : https://digital.belgium.be/iaf/hil/bosa/fas-onboarding/?lng=nl
2	Invullen van het Onboarding document	De gebruiker vult het onboarding document in en stuurt het terug door te antwoorden op de e-mail waarmee dit in te vullen document werd gestuurd.
3	Configuratie in de integratie omgeving	Configuratie en testen op basis van de informatie in het Onboarding document. Validatie van de onboarding door FOD BOSA.
4	Configuratie in de productie omgeving	Configuratie en testen op basis van de informatie in het Onboarding document. Validatie van de onboarding door FOD BOSA. In dienst nemen door de gebruiker.

Identificatie van de contactpersonen bij de gebruiker

De mensen die vermeld staan onder "Opzet" worden alleen gecontacteerd tijdens de onboarding fase. Operationele contactpersonen worden op de hoogte gehouden van updates en eventuele onderbrekingen.

BELANGRIJK || **Minimum één contactpersoon** wordt gevraagd voor de fasen "Opzet" en "Operationeel".

Fase	Rol	Naam	E-mail	Telefoonnummer
Opzet	Project Manager			
	Functioneel Analyst			
	Architect			
Operationeel	Eigenaar van de service			
	Service Manager			
	Data Protection Officer (DPO)			
	Service Desk			

Toegang tot de onlinedienst van de gebruiker

Bij elke onboarding wordt slechts één enkele URL en/of URI geautoriseerd per onlinedienst (en omgeving).

BELANGRIJK | | De waarde voor de **productieomgeving** is verplicht.

Omgeving van de gebruiker	De URL van de onlinedienst van de gebruiker	Publiek toegankelijk (Ja / Nee)
Test		
Acceptatie		
Productie		

OIDC – Technische Details

BELANGRIJK || Dit gedeelte hoeft alleen ingevuld te worden als uw dienst het OpenID Connect-protocol (OIDC) gebruikt. OIDC is de verificatiemethode die door onze diensten aanbevolen wordt.

Gegevens van de leverancier van de diensten

Omgeving	Data	
Test & Acceptatie	**Identifier van de gebruiker (client_id)**	Geleverd door FOD BOSA VD via **Securedtransfer**[1] (Formaat: *client_application*)
	Redirectie link(en) (URIs)	Voorbeeld: *https://yoururl-testenvironment/oauthFAS/auth*
	Redirectie link(en) na *logout* (URIs)	Voorbeeld: https://yoururl-testenvironment/logout
	Security mechanisme om de gebruiker te identificeren	client_secret_basic Geleverd door FOD BOSA VD via **Securedtransfer**[1] (Formaat: *client_application*)
Productie	**Identifier van de gebruiker (client_id)**	Geleverd door FOD BOSA VD via **Securedtransfer**[1] (Formaat: *client_application*)
	Redirectie link(en) (URIs)	Voorbeeld: *https://yoururl/oauthFAS/auth*
	Redirectie link(en) na *logout* (URIs)	Voorbeeld: https://yoururl/logout
	Security mechanisme om de gebruiker te identificeren	client_secret_basic Geleverd door FOD BOSA VD via **Securedtransfer**[1] (formaat: *client_application*)

[1] Securedtransfer is een onlinedienst van FOD BOSA voor het delen van gevoelige informatie zoals client-id en client-secret. Gebruik de "file download link" via https://apps.digital.belgium.be/securedtransfer/, met een door jezelf gekozen "geheime sleutel" die je per e-mail toegestuurd werd. Deze link is nodig om de gegevens veilig naar de ontvanger te sturen.
De gekozen "geheime sleutel" moet veilig worden bewaard en mag niet worden vermeld in het onboarding ticket.
Vervolgens communiceert FOD BOSA via het onboarding ticket een nieuwe URL vanwaar de inloggegevens kunnen worden gedownload met behulp van de sleutel die ingevoerd werd bij het aanmaken van de downloadlink.

Scopes

Gelieve alleen de “Scopes” te selecteren die u echt nodig hebt. Als u nog vragen hebt, kan u met ons contact opnemen via het CSM portaal https://bosa.service-now.com/csm?id=csm_taxonomy_topic&topic_id=307b393087fee5102d55964cbbbb35d7.

Scope	Beschrijving	Nodig ? (J/N)
openid	Deze scope is **verplicht**. Enkel het protocol *OpenID Connect* wordt ondersteund.	(Altijd) J
profile	Deze scope gaat de volgende attributen teruggeven: `surname`, `givenName`[2], `prefLanguage`[2], `mail`[2]	J | N
egovnrn	Deze scope gaat het attribuut `RRN/NRN` (egovNRN) of `BIS`-nummer van de geauthentificeerde eindgebruiker bevatten.	J | N
certificateInfo	Als de eindgebruiker zich authentificeert met eID en de scope *certificateInfo* wordt gevraagd, dan worden volgende attributen teruggegeven: `cert_issuer`, `cert_subject`, `cert_serialnumber`, `cert_cn`, `cert_givenname`, `cert_s`, `cert_mail`	J | N
roles	Geeft de rollen van de geauthentificeerde eindgebruiker terug. Noteer dat de scopes *roles* en *enterprise* samen gebruikt dienen te worden.	J | N
enterprise	Geeft aan dat de aanvraag gedaan wordt in naam van een onderneming. Noteer dat de scopes *roles* en *enterprise* samen gebruikt dienen te worden.	J | N
citizen (default)	Geeft aan dat de aanvraag gedaan wordt in eigen naam (geauthentificeerde eindgebruiker als fysieke persoon. Deze scope is niet compatibel met de scopes *roles* en *enterprise*. Deze scope is de default scope als de Relying Party niet de scope *enterprise* aangeeft.	J | N

[2] This field may not have a value and therefore not be returned by the system.

SAML – Technische details

BELANGRIJK || Dit gedeelte hoeft alleen ingevuld te worden als uw dienst gebruik maakt van het Security Assertion Markup Language (SAML2) protocol. SAML2 blijft ondersteund, maar wordt niet langer verder ontwikkeld. OIDC is de authenticatiemethode die door onze diensten wordt aanbevolen.

Uitwisseling van gegevens (attributen)

Persoonlijke identificatie-informatie wordt gebruikt om de werkelijke identiteit van een eindgebruiker vast te stellen. FedID (unieke ID) en Context zijn altijd meegegeven.

Attribuut	Authentieke bronnen	Nodig voor de gebruiker ? (J / N)
FedID (urn:be:fedict:iam:attr:fedid)	FOD BOSA	Altijd meegeleverd
Context (urn:be:fedict:iam:attr:context)	FOD BOSA	Altijd meegeleverd
Nationaal rijksregisternummer (egovNRN)	Nationaal Register	J / N
Voornaam (givenName)	Nationaal Register	J / N
Achternaam (surname)	Nationaal Register	J / N
Taalvoorkeur (PrefLanguage)	Profiel SMA[3]	J / N
Persoonlijk e-mailadres (mail)	Profiel SMA[3]	J / N
Rollen (roles)	FOD BOSA	J / N

Metadata

Om ervoor te zorgen dat u het dataformaat gebruikt dat de FAS vereist, vragen we u om het tool dat we u ter beschikking stellen, te gebruiken om deze metadata te genereren. Zie hieronder: Metadata Generator Tool.

[3] Self Managment Applicatie (SMA) staat ter beschikking om gebruikers in staat te stellen hun profiel te beheren en hun voorkeuren aan te geven. Deze onlinedienst is toegankelijk in de integratieomgeving op https://iamapps.int.belgium.be/sma en in de productieomgeving op https://iamapps.belgium.be/sma.

Identiteitsprovider (IdP / FOD BOSA)

Ter informatie zijn hieronder de links naar de FOD BOSA-metadatabestanden:

Omgeving	URL
Integratie	https://iamapps-public.int.belgium.be/saml/fas-metadata.xml
Productie	https://iamapps-public.belgium.be/saml/fas-metadata.xml

Leverancier van de diensten (of Service Provider (SP) Onlinedienst)

Deze metadata moeten openbaar worden gemaakt via een URL of aan ons overgedragen worden via uw FAS Onboarding ticket (ServiceNow CHGxxxxxx).

Omgeving	URL
Integratie	*https://your-public-url/SP-fas-metadata.xml*
Productie	*https://your-public-url/SP-fas-metadata.xml*

Tool om metadata te genereren

Het formaat van metadata van verschillende software-implementaties kan verschillen. Het openbaar ter beschikking gestelde demonstratietool van FAS dient gebruikt te worden om de metadata in het juiste formaat om te zetten:

https://iamapps.belgium.be/demo1/generatemetadata

Lijst van definities en afkortingen

Concept	Beschrijving
Change	Zodra een wijziging in de configuratie van een bestaande klant op een zeker platform uitgevoerd dient te worden (bijvoorbeeld een wijziging in meta-data) wordt gesproken over een change.
Context	Een activiteitensfeer waarin de toegang van een gebruiker tot een bepaalde toepassing kadert, namelijk de context ondernemingen en de context burger.
Eindgebruiker	Persoon die de beveiligde online overheidsapplicatie gebruikt die de gebruiker van de FAS (van FOD BOSA) ter beschikking stelt.
FAS	Federal Authentication Service
Gebruiker	Klant van FOD BOSA die een beveiligde online overheidsapplicatie ter beschikking stelt die gebruik maakt van de FAS om de eindgebruikers te authentificeren. Een klant kan uit meerdere Relying Parties bestaan.
IAM	Identity and Access Management
IDP	Identity Provider
OAuth2	Protocol OAuth2 (Open Authorization)
OIDC	Protocol OpenID Connect
Onboarding	Onboarding is het proces dat FOD BOSA heeft gedefinieerd waarin een nieuwe of bestaande Relying Party op het FAS-platform wordt geplaatst. Onboarding bestaat uit de functionele intake (informatieverzameling en -analyse), het daadwerkelijk configureren van de Service Provider en het in productie nemen.
Onlinedienst	Software van de klant waarvoor de toegang via de FAS wordt geregeld. FOD BOSA en haar leveranciers hebben hier uit principe geen verantwoordelijkheid voor / behoeven deze in principe niet te kennen. Een of meerdere onlinediensten kunnen aan een Relying Party verbonden zijn.
Relying Party	Een contactpunt voor de FOD BOSA FAS. Een Relying Party is aan maximaal één klant gebonden.
SAML2	Protocol Security Assertion Markup Language 2.0
Service Provider	Tot voor kort werd deze term gebruikt in de plaats van « Relying Party ». In alle nieuwe communicaties zal deze term in principe niet meer gebruikt worden.
SLO	Single Log Out – Log out op alle onlinediensten waar een gebruiker op ingelogd is zodra de gebruiker op één van deze onlinediensten uitlogt.
SMA	Self Management Application – is een onlinedienst voor de eindgebruikers dat gebruikt wordt om hun profiel te beheren, bijvoorbeeld om zijn digitale sleutels te beheren. Deze onlinedienst is toegankelijk via de adressen https://iamapps.belgium.be/sma voor de productieomgeving en https://iamapps.int.belgium.be/sma voor de integratieomgeving.
SSO	Single Sign On – Automatisch inloggen op een onlinedienst, zonder dat de gebruiker zich opnieuw hoeft te authentificeren op basis van een al bestaande authenticatiesessie bij FOD BOSA.