|  |  |
| --- | --- |
|  | *FAS Onboarding*  *(Federale authenticatiedienst)* Organisatie: Toepassing:  |

## Inhoudstafel

[Inhoudstafel 2](#_Toc124773541)

[1. algemeen 3](#_Toc124773542)

[1.1. Beschrijving van het onboardingsproces 3](#_Toc124773543)

[1.2. Identificatie van de contactpersonen bij de klant 3](#_Toc124773544)

[1.3. Toegang tot de toepassing 3](#_Toc124773545)

[2. SAML onboarding - Technische details 4](#_Toc124773546)

[2.1. Authenticatiemogelijkheden 4](#_Toc124773547)

[*2.1.1.* *LOA Levels* 5](#_Toc124773548)

[2.2. Gegevensuitwisseling (attributen) 5](#_Toc124773549)

[2.3. Metadata 6](#_Toc124773550)

[*2.3.1.* *URL’s van de Identity Provider metadata (IdP / FOD BOSA)* 6](#_Toc124773551)

[*2.3.2.* *Metadata van Service Provider (SP / de toepassing)* 6](#_Toc124773552)

[*2.3.3.* *Metadata generator tool* 6](#_Toc124773553)

[3. OIDC onboarding - Technische details 7](#_Toc124773554)

[3.1. Data van Service Provider 7](#_Toc124773555)

[3.2. Scopes: 8](#_Toc124773556)

[4. Lijst met definities en afkortingen 9](#_Toc124773557)

1. **algemeen**
	1. **Beschrijving van het onboardingsproces**

|  |  |  |
| --- | --- | --- |
| **Fase** | **Omschrijving** | **Deliverables**  |
|  1 | Aanvraag indienen | * Aanvraag door invullen van Webform op: <https://apps.digital.belgium.be/forms/show/bosa/fas-onboarding?lng=nl>
 |
|  2 | Invullen onboardingsdossier | * Invullen van onboardingsdossier door de klant en deze mag teruggestuurd worden naar de verzender dewelke u dit document bezorgd heeft
 |
|  3 | Configuratie in de integratie omgeving | * Configuratie en test op basis van de informatie uit het dossier
* Validatie van onboarding door FOD BOSA
 |
|  4 | Configuratie in de productie omgeving | * Configuratie en test op basis van de informatie uit het dossier
* Validatie van onboarding door FOD BOSA
* Ingebruikname door klant
 |

* 1. **Identificatie van de contactpersonen bij de klant**

Contacten onder ‘Opstart’ zullen enkel worden gebruikt tijdens de onboardings fase.

Operationele contacten zullen worden geïnformeerd over updates en mogelijke onderbrekingen. Er dient **minimum 1 persoon**, zowel bij de “**opstart**” en “**operationeel**”, verplicht ingevuld te worden.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Rol** | **Naam** | **E-mail** | **Telefoonnummer** |
| **Opstart** | Projectmanager |  |  |  |
| Functioneel Analist  |  |  |  |
| Architect  |  |  |  |
| **Operationeel** | Service Owner  |  |  |  |
| Service Manager |  |  |  |
| Data Protection Officer (DPO) |  |  |  |
| Service Desk  |  |  |  |

* 1. **Toegang tot de toepassing**

Bij elke onboarding is er slechts één URL en/of URI toegestaan per toepassing (en omgeving) en binnen de context van de onboarding.

.

|  |  |  |
| --- | --- | --- |
| **Klantenomgeving** | **URL’s van de toepassing** | **Publiek toegankelijk** |
| **Test**  |  |  |
| **Acceptatie** |  |  |
| **Productie** (verplicht) |  |  |

1. **SAML onboarding - Technische details**

Dit hoofdstuk dient vervolledigd te worden voor service providers die het SAML protocol hanteren.

* 1. **Authenticatiemogelijkheden**

FAS ondersteunt 3 methodes om authenticatiemogelijkheden te presenteren in CSAM bij een SAML onboarding:

1. Door een Level of Assurance (LoA) in het SAML authentication request te definiëren.

Deze methode heeft de **voorkeur**. Zie 2.1.1 voor de geassocieerde authenticatiemiddelen.

Snippet SAML request:

 …

<saml2p:RequestedAuthnContext Comparison="minimum">

<saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:be:fedict:iam:fas:citizen:Level300</saml2:AuthnContextClassRef>

</saml2p:RequestedAuthnContext>

…

1. Door een lijst van authentication contexts in het SAML authentication request te definiëren (minimum 1).

Deze methode laat toe individuele authenticatiemiddelen te tonen.

Snippet SAML request:

…

 <samlp:RequestedAuthnContext xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Comparison="exact">

<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:be:fedict:iam:fas:citizen:eid</saml:AuthnContextClassRef>

<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:be:fedict:iam:fas:citizen:bmid</saml:AuthnContextClassRef>

<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:be:fedict:iam:fas:citizen:myid</saml:AuthnContextClassRef>

<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:be:fedict:iam:fas:citizen:totp</saml:AuthnContextClassRef>

<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:be:fedict:iam:fas:citizen:token</saml:AuthnContextClassRef>

</samlp:RequestedAuthnContext>

…

1. Door geen authentication context meesturen in het SAML authentication request**. In dit geval dient de klant op te geven welk LoA gewenst is**, dit wordt hardcoded gedefinieerd.
	* 1. *LOA Levels*

|  |  |  |
| --- | --- | --- |
| **Securitylevel**  | **Authenticatie Means**  | **Technisch Level**  |
|  **High**    **Low**  |  eID **(1)** | urn:be:fedict:iam:fas:citizen:Level500 **(3)**  |
|  itsme®  **(1)** | urn:be:fedict:iam:fas:citizen:Level450 **(3)**  |
|   myID.be®   Authenticator App  Mail OTP  SMS OTP **(2)**   | urn:be:fedict:iam:fas:citizen:Level400 **(3)**  |
|   Token **(4)**  | urn:be:fedict:iam:fas:citizen:Level300 **(3)**  |
|   Gebruikersnaam/Paswoord   | urn:be:fedict:iam:fas:citizen:Level200 **(3)**  |
|  Zonder identificatie   | Zelfregistratie zonder gebruik te maken van rijksregisternummer  | urn:be:fedict:iam:fas:citizen:Level100 **(3)**  |

**(1)** De digitale sleutels **eID en itsme®** dienen bij elke onboarding **verplicht** **aangeboden** **te worden.**

 Kiest de klant een bepaald level, dan dienen ook de sleutels met een hoger technisch level aangeboden worden.

(vb klant kiest level 400, dan toont het FAS scherm de sleutels van het level 400, 450 en 500).

**(2)** SMS OTP: optionele digitale sleutel.

De klant betaalt de kost voor het versturen van de SMS bij een authenticatie met deze sleutel. Dit vereist een overeenkomst tussen de klant en de mobiele operator, die de kost rechtstreeks aan de klant factureert.

Hebt u interesse om de digitale sleutel ‘code via SMS’ aan te bieden, vraag dan het addendum hiervoor aan bij BOSA.

**(3)** Vervang in het Technisch Level ‘*citizen’* door ‘*enterprise’* context, indien u het toegangsbeheer via rollen wenst te gebruiken. De

aanvraag van rollen gebeurt via een afzonderlijk formulier.

(Vb. urn:be:fedict:iam:fas:enterprise:Level400)

**(4)** Het token is in status ‘*phase out’*.

Er kunnen geen nieuwe tokens meer geactiveerd worden door eindgebruikers sinds 25/09/2020.

* 1. **Gegevensuitwisseling (attributen)**

Persoonlijke identificatie-informatie laat toe om de effectieve identiteit van een gebruiker vast te stellen. FedID (unieke ID) en Context worden altijd meegeleverd.

|  |  |  |
| --- | --- | --- |
| **Attribuut** | **Authentieke bron** | **Gewenst door klant?** |
| **FedID** | FOD BOSA | Standaard geleverd |
| **Context** | FOD BOSA | Standaard geleverd |
| **Rijksregisternummer** | Rijksregister | Y / N |
| **Voornamen** | Rijksregister | Y / N |
| **Familienaam**  | Rijksregister | Y / N |
| **Voorkeurstaal** | SMA profiel | Y / N |
| **Persoonlijk e-mailadres** | SMA profiel | Y / N |
| **Rollen** | FOD BOSA | Y / N |

* 1. **Metadata**
		1. *URL’s van de Identity Provider metadata (IdP / FOD BOSA)*

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

* + 1. *Metadata van Service Provider (SP / de toepassing)*

Deze metadata moet publiek gepubliceerd worden op een URL, of opgeladen worden naar je ticket voor de FAS Onboardings (ServiceNow CHGxxxxxx).

|  |  |
| --- | --- |
| **Omgeving** | **URL** |
| **Integratie** | [*https://your-public-url/SP-fas-metadata.xml*](https://your-public-url/SP-fas-metadata.xml) |
| **Productie** |  [*https://your-public-url/SP-fas-metadata.xml*](https://your-public-url/SP-fas-metadata.xml) |

* + 1. *Metadata generator tool*

De metadata van verschillende software implementaties kan in formaat verschillen. Bij twijfel kan de publieke demotool van FAS gebruikt worden om metadata naar het correcte formaat te transformeren:

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

1. **OIDC onboarding - Technische details**

Dit hoofdstuk dient vervolledigd te worden voor service providers die het OIDC protocol hanteren.

* 1. **Data van Service Provider**

|  |  |  |
| --- | --- | --- |
| **Environnement** | **Data** |  |
| **Test & Acceptation** | **Client\_id** | Geleverd door BOSA DT via **Securedtransfer** **(\*)**(format: *client\_application*) |
| **redirect URl(‘s)** | example “ [*https://yoururl-testenvironment/oauthFAS/auth*](https://yoururl-testenvironment/oauthFAS/auth) *“* |
| **Post-Logout Redirect URI(‘s)** | example “ <https://yoururl-testenvironment/logout>*“* |
| **Security mechanism for client authentication** | client\_secret\_basicClient secret geleverd door BOSA DT via **Securedtransfer** **(\*)**(format: *client\_application*) |
| **Production** | **Client\_id** | Geleverd door BOSA DT via **Securedtransfer** **(\*)**(format: *client\_application*) |
| **redirect URl(‘s)** | example “[*https://yoururl/oauthFAS/auth*](https://yoururl/oauthFAS/auth)*”* |
| **Post-Logout Redirect URI(‘s)** | example “ <https://yoururl/logout>*“* |
| **Security mechanism for client authentication**  | client\_secret\_basicClient secret geleverd door BOSA DT via **Securedtransfer** **(\*)**(format: *client\_application*) |

**(\*)** *Securedtransfer* is een applicatie aangeboden door BOSA om gevoelige informatie zoals een client id en client secret te delen.

Gelieve een “file-upload-link” aan te maken via <https://apps.digital.belgium.be/securedtransfer> met een zelf te kiezen “geheime sleutel”. Dit genereert een URL die volledig dient vermeld te worden als antwoord op het origineel onboarding ticket (ServiceNow). Deze link is nodig om de credentials veilig te adresseren naar de ontvanger.

De gekozen “geheime sleutel” dien je veilig te bewaren en **niet** in het ticket te vermelden.

Hierna communiceert BOSA via het onboarding ticket een nieuwe URL waarvan de credentials gedownload kunnen worden, gebruikmakend van de sleutel die initieel werd ingegeven bij de aanmaak van de uploadlink.

* 1. **Scopes:**

Gelieve enkel de velden te “selecteren” dewelke u werkelijk nodig heeft. Mocht u nog bijkomende vragen hebben hieromtrent dan kan u ons contacteren via servicedesk.dto@bosa.fgov.be

|  |  |  |
| --- | --- | --- |
| **Scope** | **Description** | **Needed ?** |
| **OpenID** | This scope is a MUST. Only the OpenID Connect protocol is supported | Always Y |
| **profile** | This scope will contain the following claims: *surname ; givenName ; PrefLanguage ; mail* | Y | N |
| **egovnrn** | This scope will contain the RRN/NRN or BIS number claim of the authenticated user | Y | N |
| **certficateInfo** | If the user authenticates using eID and the scope certificateInfo is requested we’ll return the following claims: *cert\_issuer ; cert\_subject ; cert\_serialnumber ; cert\_cn ;cert\_givenname ; cert\_s ; cert\_mail* | Y | N |
| **roles** | This is an explicit request from roles of the authenticating end-user (roles and enterprise should be combined) | Y | N |
| **enterprise** | States that the request is made in the name of an enterprise (roles and enterprise should be combined) | Y | N |
| **citizen** (default) | States that the end-user authenticates as a natural person (this scope is currently incompatible with the enterprise and roles scope). This scope is default if a RP doesn't request the enterprise scope. | Y | N |

1. **Lijst met definities en afkortingen**

|  |  |
| --- | --- |
| **Concept** | **Beschrijving** |
| Applicatie | Software van de klant waarvoor de toegang middels 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 applicaties kunnen aan een Relying Party verbonden zijn. |
| Context | Een activiteitensfeer waarin de toegang van een gebruiker tot een bepaalde toepassing kadert, namelijk de context ondernemingen en de context burger. |
| 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. |
| Circle Of Trust | COT. Een groep van applicaties die elkaar wederzijds vertrouwen, wat het mogelijk maakt om zonder extra controles informatie (data) uit te wisselen of een Single Sign On toe te staan. |
| Customer | Zie klant |
| Domein | Functionele groepering van rollen |
| IAM | Identity and Access Management |
| Klant | Klant van FOD BOSA. Een Customer kan uit meerdere Relying Parties bestaan. |
| Onboarding | Onboarding is het proces dat FOD BOSA heeft gedefinieerd waarin een nieuwe of bestaande Relying Party op een nieuw FAS-platform wordt geplaatst. Onboarding bestaat uit de functionele intake (informatieverzameling en -analyse), het daadwerkelijk configureren van de Service Provider en in productie nemen. |
| Relying Party | Een contactpunt voor de FOD BOSA FAS. Een Relying Party is aan maximaal één customer gebonden. |
| Service Provider | Deze term werd tot voor kort gebruikt in plaats van Relying Party. In nieuwe communicatie wordt deze term in principe niet meer gebruikt. |
| SSO | Single Sign On – Automatisch inloggen op een applicatie, zonder dat de gebruiker zich opnieuw hoeft te authenticeren op basis van een reeds bestaande authenticatiesessie bij FOD BOSA. |
| SLO | Single Log Out – Log out op alle applicaties waar een gebruiker op ingelogd is zodra de gebruiker op één van deze applicaties uitlogt. |
| Application ID | SAML2 entity ID |
| FAS | Federal Authentication Services |
| OIDC | OpenIDConnect |
| OAuth2 | OAuth2 protocol |