|  |  |
| --- | --- |
|  | *FAS Onboarding*  *(Service fédéral d'authentification)*Organisation: Application:  |

## Table des Matières

[Table des Matières 2](#_Toc124773925)

[1. Généralités 3](#_Toc124773926)

[1.1. Description du processus d’onboarding 3](#_Toc124773927)

[1.2. Identification des personnes de contact auprès du client 3](#_Toc124773928)

[1.3. Accès à l'application 3](#_Toc124773929)

[2. Onboarding SAML - Détails techniques 4](#_Toc124773930)

[2.1. Possibilités d’authentification 4](#_Toc124773931)

[*2.1.1.* *Niveaux LOA* 5](#_Toc124773932)

[2.2. Échange de données (attributs) 5](#_Toc124773933)

[2.3. Métadonnées 6](#_Toc124773934)

[*2.3.1.* *Les URL du « Identity Provider metadata » (IdP / SPF BOSA)* 6](#_Toc124773935)

[*2.3.2.* *Métadonnées du fournisseur de services (ou Service Provider (SP)/ l’application)* 6](#_Toc124773936)

[*2.3.3.* *Metadata generator tool* 6](#_Toc124773937)

[3. Onboarding OIDC - Détails techniques 7](#_Toc124773938)

[3.1. Données du fournisseur de services 7](#_Toc124773939)

[3.2. Scopes: 8](#_Toc124773940)

[4. Liste de définitions et d'abréviations 9](#_Toc124773941)

1. **Généralités**
	1. **Description du processus de l’onboarding**

|  |  |  |
| --- | --- | --- |
| **Phase** | **Description** | **Produits livrables**  |
|  1 | Introduire la demande | * Demande en complétant le formulaire web sur : <https://apps.digital.belgium.be/forms/show/bosa/fas-onboarding?lng=fr>
 |
|  2 | Compléter le dossier d'onboarding | * Le client replit le dossier d'onboarding et celui-ci le re-envoie à l'expéditeur qui vous a fourni ce document.
 |
|  3 | Configuration dans l'environnement d'intégration | * Configuration et test sur la base des informations du dossier
* Validation de l’onboarding par le SPF BOSA
 |
|  4 | Configuration dans l'environnement de production | * Configuration et test sur la base des informations du dossier
* Validation de l’onboarding par le SPF BOSA
* Mise en service par le client
 |

* 1. **Identification des personnes de contact auprès du client**

Les personnes mentionnées dans la rubrique « Lancement » ne seront contactées que pendant la phase d’onboarding. Les personnes de contact opérationnelles seront informées des mises à jour et interruptions éventuelles.

**Un minimum d'une personne**, pour "**Lancement**" et "**Opérationnel**", doit être obligatoirement renseigné.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Rôle** | **Nom** | **E-mail** | **Nr de téléphone** |
| **Lancement** | Gestionnaire de projets |  |  |  |
| Analyste fonctionnel  |  |  |  |
| Architecte  |  |  |  |
| **Opérationnel** | Propriétaire du service  |  |  |  |
| Gestionnaire du service |  |  |  |
| Data Protection Officer (DPO) |  |  |  |
| Service Desk  |  |  |  |

* 1. **Accès à l'application**

Pour chaque onboarding, une seule URL et/ou URI est autorisée par application (et environnement) et dans le contexte de l’onboarding.

|  |  |  |
| --- | --- | --- |
| **Environnement client** | **Les URL de l'application** | **Accessible publiquement** |
| **Test**  |  |  |
| **Acceptation** |  |  |
| **Production** (obligatiore) |  |  |

1. **Onboarding SAML - Détails techniques**

Ce chapitre doit être complété pour les fournisseurs de services qui utilisent le protocole SAML.

* 1. **Possibilités d’authentification**

Le FAS soutient 3 méthodes pour présenter des possibilités d’authentification dans CSAM en cas d’onboarding SAML :

1. En définissant un « Level Of Assurance » (LOA) dans la requête d’authentification SAML.

Il s’agit de la méthode **privilégiée**. Voir le point 2.1.1 pour les moyens d'authentification associés.

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. En définissant une liste de contextes d’authentification dans la requête d’authentification SAML (minimum 1).

Cette méthode permet d’afficher des moyens d'authentification individuels.

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. En n’envoyant pas de contexte d’authentification dans la requête d’authentification SAML. **Dans ce cas, le client doit indiquer quel LOA est souhaité**. C’est défini de manière figée dans le code (« hardcoded »).
	* 1. *Niveaux LOA*

|  |  |  |
| --- | --- | --- |
| **Securitylevel** | **Authentication Means** | **Niveau Technique** |
|  **Élevé** **Faible** | eID **(1)** | urn:be:fedict:iam:fas:citizen:Level500 **(3)**  |
| itsme® **(1)** | urn:be:fedict:iam:fas:citizen:Level450 **(3)**  |
| myID.be® Authentication AppMail OTPSMS OTP **(2)**  | urn:be:fedict:iam:fas:citizen:Level400 **(3)**  |
| Token **(4)** | urn:be:fedict:iam:fas:citizen:Level300 **(3)**  |
| Nom d'utilisateur/mot de passe | urn:be:fedict:iam:fas:citizen:Level200 **(3)**  |
| Sans identification | Auto-enregistrement sans utiliser de numéro de Registre national | urn:be:fedict:iam:fas:citizen:Level100 **(3)**  |

(1) Les clés numériques **eID et itsme® doivent être présentes** à chaque onboarding.

 Si le client choisit un certain niveau, les clés avec un niveau technique supérieur doivent également être proposées.

 (p.ex.: le client choisit le niveau 400, puis l'écran FAS affiche les clés des niveaux 400, 450 et 500).

(2) SMS OTP : la clé numérique en option.

 Le client paie le coût de l’envoi du SMS lors de l'authentification avec cette clé. Cela nécessite un accord entre le client et

 l'opérateur mobile, qui facture le coût directement au client.

 Si vous êtes intéressé par l'offre de la clé numérique 'code par SMS', veuillez demander l'annexe correspondant à BOSA.

(3) Remplacez *'citoyen'* par le contexte *'entreprise'* si vous souhaitez utiliser le contrôle d'accès via les rôles. Les rôles sont demandés

 par un formulaire séparé.

 (p.ex.: urn:be:fedict:iam:fas:enterprise:Level400)

(4) Le token est en mode ‘*phase out’*.

 Aucun nouveau token ne peut être activé par les utilisateurs finaux depuis le 25/09/2020.

* 1. **Échange de données (attributs)**

Les informations personnelles relatives à l'identification permettent de constater l'identité effective d'un utilisateur. FedID (ID unique) et Contexte sont toujours inclus.

|  |  |  |
| --- | --- | --- |
| **Attribut** | **Source authentique** | **Souhaits du client ?** |
| **FedID** | SPF BOSA | Fourni par défaut |
| **Contexte** | SPF BOSA | Fourni par défaut |
| **Numéro de Registre national** | Registre national | O / N |
| **Prénoms** | Registre national | O / N |
| **Nom de famille**  | Registre national | O / N |
| **Choix de langue** | Profil SMA | O / N |
| **Adresse e-mail personnelle** | Profil SMA | O / N |
| **Rôles** | SPF BOSA | O / N |

* 1. **Métadonnées**
		1. *Les URL du « Identity Provider metadata » (IdP / SPF BOSA)*

|  |  |
| --- | --- |
| **Environnement** | **URL** |
| **Intégration** |     |
| **Production** |  <https://iamapps-public.belgium.be/saml/fas-metadata.xml>    |

* + 1. *Métadonnées du fournisseur de services (ou Service Provider (SP)/ l’application)*

Ces métadonnées doivent être publiées publiquement sur une URL ou chargées vers votre ticket pour les Onboardings FAS (ServiceNow CHGxxxxxx).

|  |  |
| --- | --- |
| **Environnement** | **URL** |
| **Intégration** | [*https://your-public-url/SP-fas-metadata.xml*](https://your-public-url/SP-fas-metadata.xml) |
| **Production** |  [*https://your-public-url/SP-fas-metadata.xml*](https://your-public-url/SP-fas-metadata.xml) |

* + 1. *Metadata generator tool*

Le format des métadonnées de diverses implémentations logicielles peut être différent. En cas de doute, l’outil de démo public du FAS peut être utilisé pour transformer des métadonnées dans le format correct :

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

1. **Onboarding OIDC - Détails techniques**

Ce chapitre doit être complété pour les fournisseurs de services qui utilisent le protocole OIDC.

* 1. **Données du fournisseur de services**

|  |  |  |
| --- | --- | --- |
| **Environnement** | **Données** |  |
| **Test & Acceptation** | **Client\_id** | Fourni par BOSA DT via **Securedtransfer** **(\*)**(format: *client\_application*) |
| **redirect URl(‘s)** | exemple “ [*https://yoururl-testenvironment/oauthFAS/auth*](https://yoururl-testenvironment/oauthFAS/auth) *“* |
| **Post-Logout Redirect URI(‘s)** | exemple “ <https://yoururl-testenvironment/logout>*“* |
| **Security mechanism for client authentication** | client\_secret\_basicFourni par BOSA DT via **Securedtransfer** **(\*)**(format: *client\_application*) |
| **Production** | **Client\_id** | Fourni par BOSA DT via **Securedtransfer** **(\*)**(format: *client\_application*) |
| **redirect URl(‘s)** | exemple “[*https://yoururl/oauthFAS/auth*](https://yoururl/oauthFAS/auth)*”* |
| **Post-Logout Redirect URI(‘s)** | exemple “ <https://yoururl/logout>*“* |
| **Security mechanism for client authentication**  | client\_secret\_basicFourni par BOSA DT via **Securedtransfer** **(\*)**(format: *client\_application*) |

**(\*)** *Securedtransfer* est une application fournie par BOSA pour partager des informations sensibles telles que le client-id et client-secret.

Veuillez créer un "lien de téléchargement de fichier" via <https://apps.digital.belgium.be/securedtransfer/> avec une "clé secrète" choisie par vous-même. Cela génère une URL qui doit être entièrement référencée dans le ticket d'onboarding original (ServiceNow). Ce lien est nécessaire pour transmettre en toute sécurité les credentials au destinataire.

La "clé secrète" choisie doit être conservée en sécurité et ne **pas** être mentionnée dans le ticket d’onboarding.

Ensuite, BOSA communique via le ticket d'onboarding une nouvelle URL à partir de laquelle les credentials peuvent être téléchargées, en utilisant la clé initialement saisie lors de la création du lien de téléchargement.

* 1. **Scopes:**

Veuillez ne "sélectionner" que les champs dont vous avez réellement besoin. Si vous avez d'autres questions, veuillez nous contacter à l'adresse 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. **Liste de définitions et d'abréviations**

|  |  |
| --- | --- |
| **Concept** | **Description** |
| Application | Logiciel du client pour lequel l'accès est réglé au moyen du FAS. Le SPF BOSA et ses fournisseurs n'assument en principe aucune responsabilité en la matière/ne doivent en principe pas le connaître. Une ou plusieurs applications peuvent être connectées à une « Relying Party ». |
| Contexte | Une sphère d'activités dans laquelle s'inscrit l'accès d'un utilisateur à une application spécifique, à savoir le contexte Entreprises et le contexte Citoyen. |
| Changement | Dès qu'une modification doit être effectuée dans la configuration d'un client existant sur une certaine plate-forme (par exemple une modification de métadonnées), on parle de changement. |
| *Circle Of Trust* | COT. Un groupe d'applications se faisant mutuellement confiance, permettant ainsi, sans contrôles supplémentaires, d'échanger des informations (données) ou d'autoriser un « Single Sign On ». |
| *Customer* | Voir client |
| Domaine | Groupement fonctionnel de rôles |
| IAM | Identity and Access Management (gestion de l'identité et de l'accès) |
| Client | Client du SPF BOSA. Un « Customer » peut consister en plusieurs « Relying Parties ». |
| *Onboarding* | L'*onboarding* est le processus défini par le SPF BOSA dans lequel une « Relying Party » nouvelle ou existante est placée sur une nouvelle plate-forme FAS. L'*onboarding* consiste en un *intake* fonctionnel (collecte et analyse d'informations), en la configuration effective du Service Provider et en la mise en production. |
| « Relying Party » | Un point de contact pour le FAS du SPF BOSA. Une « Relying Party » est liée à un « Customer » au maximum. |
| *Service Provider* | Jusqu'à il y a peu, ce terme était utilisé en lieu et place de « Relying Party ». Dans toute nouvelle communication, ce terme ne sera en principe plus utilisé. |
| SSO | Single Sign On – Connexion automatique à une application, sans que l'utilisateur ne doive à nouveau s'authentifier sur la base d'une session d'authentification existante au SPF BOSA. |
| SLO | Single Log Out – Déconnexion de toutes les applications auxquelles un utilisateur est connecté dès qu'il se déconnecte de l'une de ces applications. |
| Application ID | SAML2 entity ID |
| FAS | Federal Authentication Services (services fédéraux d'authentification) |
| OIDC | OpenIDConnect |
| OAuth2 | Protocole OAuth2 |