FOD Beleid & Ondersteuning
SPF Stratégie & Appui

FAS
-
Integration Guide
Frequently Asked Questions

.be

Version 6.4

Table of Contents

Frequently Asked Questions **1**

Table of Contents **2**

About this Document **3**

General Information **4**

Contact the helpdesk 4
About the onboarding procedure 4
OIDC, SAML or both? 5
Browser Requirements 5

Technical Information **6**

About the Single Sign-On (SSO) functionality 6
About the SAML Metadata 6

About this Document

This guide is a complement to the **FAS OIDC Integration Guide** and **FAS SAML Integration Guide**. It has been created to provide best practice guidance, provide additional information that might be useful and answer the most common questions received by the helpdesk team.

Please, reach out to the helpdesk if you have any additional question via the ServiceNow CSM portal https://bosa.service-now.com/csp?id=bosa_csm_unauthenticated_form&form=dg-vd-csam&lang=en.

Underneath "**user**" is used to refer to a customer of FPS BOSA who makes available via OIDC a secured online public application that uses the FAS for the authentication of end-users. The "**end-user**" is indeed the person that makes use of this secured online public application of the above-mentioned user. See also the schema underneath. A user might consist of several "**Relying Parties**".

General Information

Contact the helpdesk

The helpdesk can assist you in your onboarding journey with the FAS. Make sure you have read this FAQ and consulted the available documentation, the answer you are looking for might be right there.

The ServiceNow CSM portal https://bosa.service-now.com/csp?id=bosa_csm_unauthenticated_form&form=dg-vd-csam&lang=en.

About the onboarding procedure

The onboarding procedure consists of two workflows:

- The first one contains the contractual agreements between FPS BOSA and the user. The necessary contracts are put in place to establish the trust relationship between the user and FPS BOSA. Once this is completed and contracts are signed, the next workflow can be started.
- The second one is the technical onboarding based upon the FPS BOSA onboarding document. During this step, the technical implementation is carried out to make the FAS environment ready for the user. The customer will, together with FPS BOSA, prepare the onboarding specification.

The workflows are split in four (4) phases:

Phase	Description
1 – Onboarding Request	The onboarding request is initiated by filling out the following online form: https://digital.belgium.be/iaf/hil/bosa/fas-onboarding/?lng=en
2 – Technical Details	You will be asked to provide technical details about your environment and service.
3 – Integration Onboarding	Onboarding and test in the Integration (INT) environment.
4 – Production Onboarding	Onboarding and test in the Production (PRD) environment.

OIDC, SAML or both?

The preferred federation method is **OpenID Connect (OIDC)**.
If you have the choice, we strongly recommend choosing OIDC. SAML should be your choice if and only if your environment doesn't allow you to do otherwise.

Also, **stick to one option** if possible. The federation method is transparent to the user during the authentication, having both doesn't bring any additional value. If you are not required to support both, only one is enough.

Browser Requirements

The user interface of FAS has been created using Vue and the browser requirements are defined as follows:

- Browsers versions with global usage statistics **greater than 1%**
- The **last two** versions of each browser
- **NOT Internet Explorer** with a version number **below 11**

It's important to note that **any browser that does not meet the above requirements**, **is not supported**. This also includes embedded browsers.

Technical Information

About the Single Sign-On (SSO) functionality

Single Sign-On may or may not be applied. It is the FAS' SSO engine that decides to apply SSO based on multiple criteria. The decision is based on information gathered from:

- The incoming **federation request.**
- The **active session** (resulting from a previous authentication).
- The Relying Parties' configuration.

Single Sign-On **will be denied** and authentication will be required in the following cases:

1. The incoming federation request explicitly requests to go through the whole authentication process with a *Force Authentication*.
2. The configuration of the Relying Party forbids the usage of SSO. It can be requested in the onboarding document.
3. The technical level of the authentication method used in the previous authentication is lower than the technical level in the current federation request.
4. The authentication method used in the previous authentication is not allowed in the current federation request.
5. The authentication method used in the previous authentication is not allowed to perform Single Sign-On authentication.

Single Sign-On should work by default otherwise.

About the SAML Metadata

To make sure the metadata file is compliant with the FAS requirements, it's recommended to generate the metadata file using the generator tool provided by FPS BOSA.

Consult the Onboarding Guide and SAML Integration Guide for more details.

Metadata Generator Tool: https://iamapps.belgium.be/demo1/generatemetadata