FOD Beleid & Ondersteuning
SPF Stratégie & Appui

FAS
-
SAML
Integration Guide

21 February 2025

Version 6.5

Table of Contents

Contents

Table of Contents **2**

About this Document **3**

SAML Provider **4**

Authentication Context 4
Attributes 6
Metadata 10

Authentication Request **14**

Request 14
Response 15

Logout Request **18**

Request 18
Response 19

About this Document

The purpose of this document is to provide the relevant technical information to complete the integration with the Federal Authentication Service (FAS) via the SAML protocol.

Underneath "**user**" is used to refer to a customer of FPS BOSA who makes available via SAML 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. Such a user might consist of several Relying Parties. To avoid confusion with the different terminologies a "user" is therefore also called a "**Relying Party**".

This document focusses on the support for governmental organisations in the implementation and connection of their systems with FPS BOSA IAM. The governmental organisations are Relying Parties who rely on FPS BOSA IAM as a Trusted Third Party and as such form a Circle of Trust.

The most important way of connecting to FPS BOSA IAM is via the Federal Authentication Service (FAS). Relying Parties can use this service to identify and authenticate the end users to their online services. The FAS service can also provide relevant attributes and roles to enable the Relying Party to make an authorization decision.

SAML Provider

Authentication Context

The Authentication Context Class Reference (ACR) has been made mandatory because that way, the system allows you to login with eID, even in case our database becomes unavailable.

To access the FPS BOSA IAM Services, several ways of authentication are possible:

- eID
- Application MyGov.be
- Recognised electronic identifier (partner): itsme®
- Authenticator App (TOTP)
- Email (OTP)
- SMS (OTP)
- Username + Password

Depending on the target audience of the application (citizen / enterprise), these authentication methods are translated in SAML into “context” and “contract”. A contract is a technical SAML definition to define the requested authentication method.

FAS works with “Levels of Assurance” (LOA). This means all authentication means equal or higher than the level sent by the authentication request will be available. Setup is done by adapting the SAML authentication request parameters.

The list of supported values between a RP and the FAS is given below:

- `urn:be:fedict:iam:fas:<context>:Level500`
- `urn:be:fedict:iam:fas:<context>:Level450`
- `urn:be:fedict:iam:fas:<context>:Level400`
- `urn:be:fedict:iam:fas:<context>:Level300`
- `urn:be:fedict:iam:fas:<context>:Level200`
- `urn:be:fedict:iam:fas:<context>:Level100`

Below you find a table, containing an overview of all authentication means offered and supported by FPS BOSA:

Level of Assurance	Authentication Means	Authentication Contract[1]
High	eID[2]	`urn:be:fedict:iam:fas:<context>:Level500`
	MyGov.be[2]	
	eIDAS High[2]	
	Itsme[2] High	`urn:be:fedict:iam:fas:<context>:Level450`
Substantial	eIDAS[2] Substantial	`urn:be:fedict:iam:fas:<context>:Level400`
	Itsme[2] Substantial	
	Authenticator App	
	Mail OTP	
	SMS OTP[3]	
Low	Username / Password	`urn:be:fedict:iam:fas:<context>:Level200`
Weak	Self-registration without NRN	`urn:be:fedict:iam:fas:<context>:Level100`

Table 1 Authentication contracts with corresponding authentication means and security levels

[1] If the customer chooses a certain level, the keys with a higher technical level must (will) also be offered as well.
E.g.: the customer chooses level 400, then the FAS screen displays the keys of levels 400, 450 and 500.
[2] The digital keys, **eID**, **MyGov.be** and **itsme®**, **must** be present at each onboarding.
[3] The digital key **SMS OTP** is disabled by default and should be requested to be used.

Note:

- The target audience (`context`) **MUST** be specified in your request. It has **citizen** or **enterprise** as a value. E.g.: An authentication contract with a technical level value of 400 will either be `urn:be:fedict:iam:fas:citizen:Level400` or `urn:be:fedict:iam:fas:enterprise:Level400.`

- **Enterprise** context is required to retrieve roles. Note that requesting roles may add calls to external dependencies and the processing of the request may take longer.

Remark: **iframes** technology has never been supported by FAS and is not compatible actually.

Attributes

The FPS BOSA IAM Service also contains a service that can provide some additional attributes, embedded in the SAML response, which can be used to decide upon the authorization to the application. This service is called the Attribute Service (AS).

The exchanged attributes are defined on FAS for each Service Provider (during the onboarding). There is a distinction between context aware attributes and context-free attributes.

This service can deliver attributes related to private information of the principal or related to the role the principal achieved.

Personal Attributes

Attribute	Description
Name ID	The NameID code is a unique identifier for the principal during a session. FAS expects a transient NameID. This value changes each session per principal. E.g.:

	<**saml:NameID** Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="https://idp.iamfas.ta.belgium.be/fas" SPNameQualifier="https://iamapps.ta.belgium.be/demo1"> 656964.58c14e71-ec3e-4f4c-8a46-7739f2c27d27 </**saml:NameID**>
Fed ID	A unique value for the principal within a certain context. This value can be used as a unique identifier without the use of the national number
Target Group (context)	Citizen or Enterprise E.g.: <saml:Attribute Name="**urn:be:fedict:iam:attr:context**"> <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"> **urn:be:fedict:iam:context:citizen** </saml:AttributeValue> </saml:Attribute>
National Registry Number (egovNRN)	The national registry number of the principal, namely RRN. The attribute's name is **egovNRN.** E.g.: <saml:Attribute FriendlyName="egovNRN" Name="**egovNRN**"> <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">92020202020</saml:AttributeValue> </saml:Attribute>
Given Name	The given name of the principal. E.g.: <saml:Attribute FriendlyName="givenName" Name="**givenName**"> <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"> John </saml:AttributeValue> </saml:Attribute>
Last Name	The surname of the principal.

	E.g.:
	
	`<saml:Attribute FriendlyName="surname" Name="surname">`
	`  <saml:AttributeValue`
	`  xmlns:xs="http://www.w3.org/2001/XMLSchema"`
	`  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
	`  xsi:type="xs:string">`
	`  Doe`
	`  </saml:AttributeValue>`
	`</saml:Attribute>`

Preferred Language	This is the language which the principal defined as preferential in his SMA User Interface.

Preferred Local Language (`locale`)	The preferred language of the principal as it's registered in FPS BOSA IAM.
	
	E.g.:
	
	`<saml:Attribute Name="urn:be:fedict:iam:attr:locale">`
	`  <saml:AttributeValue`
	`  xmlns:xs="http://www.w3.org/2001/XMLSchema"`
	`  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
	`  xsi:type="xs:string">`
	`  nl`
	`  </saml:AttributeValue>`
	`</saml:Attribute>`

Personal Email Address	The personal email address as registered in FPS BOSA IAM.

Authentication Method	Describes the authentication method used. This allows applications to offer different functionalities based on authentication methods.
	
	E.g.:
	
	`<saml:Attribute`
	`  Name="urn:be:fedict:iam:attr:authenticationmethod">`
	`  <saml:AttributeValue`
	`  xmlns:xs="http://www.w3.org/2001/XMLSchema"`
	`  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
	`xsi:type="xs:string">`
	`  urn:be:fedict:iam:attr:authenticationmethod:Level500`
	`  </saml:AttributeValue>`
	`</saml:Attribute>`
	
	`<saml:Attribute Name="authenticationmethod">`
	`  <saml:AttributeValue`
	`  xmlns:xs="http://www.w3.org/2001/XMLSchema"`
	`  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
	`xsi:type="xs:string">`
	`  Eid`
	`  </saml:AttributeValue>`

	</saml:Attribute>

Table 2 Personal attributes with sample values

Role Attributes

These attributes hold all the role information for the principal specific for the Relying Party. The information is base64 encoded and has an XML structure.

The XML format uses a scheme to deliver the role information with a set attribute "`role-name`" and one or more possible parameters.

```
<rol:RoleResult xmlns:rol="http://be.fedict.rolemgmt/RoleXMLSchema">
  <rol:Role name="<application_role>"
xmlns:role="http://be.fedict.rolemgmt/RoleXMLSchema">
    <rol:RoleAttribute name="CompanyId">999999999</rol:RoleAttribute>
    <rol:RoleAttributename="FEDictDomain">SOMEDOMAIN</rol:RoleAttribute>
  </rol:Role>
</rol:RoleResult>
```

During role definition, the user can request 3 additional **standard attributes** (described below) which are related to the role, namely OrganizationID, RefOrganizationID and professional email-address. During role-onboarding, the user can also define and request additional **non-standard attributes** that can be added to the specific role.

Attribute	Description
OrganizationID	The company number of the company will be returned.
RefOrganizationID	The company number of the master company A. will be returned e.g., the number of Company A which delegates services to their accountant company B.
Professional email-address	The professional email address of the logged-in user will be returned, e.g., the accountant's company's email address.

Table 3 Role attributes

Metadata

For each URL/application that the client wants to get access to FAS, metadata is expected in xml-format. The structure of the metadata is based on the SAML v2 metadata schema.

Reference: http://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd

Identity Provider's Metadata

The standard URLs to add in the metadata are :

Environment	Path
Integration	https://iamapps-public.int.belgium.be/saml/fas-metadata.xml
Production	https://iamapps-public.belgium.be/saml/fas-metadata.xml

Table 4 FAS metadata URL per environment

Service Provider's Metadata

Below are some guidelines to follow when creating your metadata for SAML 2.0.

Parameter	Description
EntityID	The entityID must be unique for every Relying Party and is specified in the entitydescriptor. It can be the url of the application or any unique identifier that contains preferably the name of the organization and application. E.g.: ▪ fediam.minfin.fgov.be (applicationname.organisation) ▪ btb.csam.be (applicationname.organisation) ▪ https://kbo-bce-wi.economie.fgov.be/kbo/ (url of the application)
SPSSODescriptor	The Service Provider SSO Descriptor contains: ▪ the *AuthenticationRequestSigned* attribute, which preferably must be set to true, ▪ the certificate ▪ the Single Logout Service o Binding where there are the following options available in SAML 2.0: ▪ SAML SOAP Binding (Limited support, only for artifact) ▪ http Redirect Binding ▪ **http Post Binding** ▪ http Artifact Binding o Location: Endpoint Location for Single Logout Requests

	○ ResponseLocation: Endpoint Location for Single Logout Responses (Optional) ▪ NameIDFormat: only transient is supported ▪ AssertionConsumerService Binding: ○ this contains the type of binding ○ and the location

Table 5 - Relying Party's metadata structure

Note :

- About the bindings, there is very limited support to all except **`HTTP POST binding`**. The usage of any other binding is not recommanded.

Sample EntityDescriptor

```
<EntityDescriptor
    xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    ID="I5bf4e6f87a221b0a"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    entityID="entityID_of_RP"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata
        http://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd">
    <SPSSODescriptor AuthnRequestsSigned="true"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>
                        <!-- Certificate of RP used for signing SAML messages
                            (must be issued by a CA with a public OCSP)  -->
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>

        <SingleLogoutService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="<!-- Endpoint Location for Single Logout Requests -->"
            ResponseLocation="<!-- Endpoint Location for Single Logout Responses
(Optional) -->" >
        </SingleLogoutService>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</NameIDFormat>
        <AssertionConsumerService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="<EndPoint Location for HTTP POST SAML Assertion Messages"
            index="0"
            isDefault="true"></AssertionConsumerService>

        <AssertionConsumerService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="<!-- EndPoint Location for HTTP Redirect SAML Assertion
Messages -->"
            index="1"
            isDefault="true">
        </AssertionConsumerService>
    </SPSSODescriptor>
</EntityDescriptor>
```

Figure 1 Sample EntityDescriptor in XML

Authentication Request

In the simplest use case, the Service Provider asks a certain AuthenticationContext for a session of the principal and the FAS delivers certain identity attributes, no privilege information to the Service Provider.

Request

Method	Path
GET	/fas/SSORedirect/metaAlias/idp

Table 6 Authentication request

Parameter		Value
SAMLRequest	Mandatory	Base64 encoded request
SigAlg	Mandatory	Signature algorithm
Signature	Mandatory	Signature value
locale	Optional but recommended	One of: “en” “de” “fr” “nl”. The default value is “nl”.

Table 7 Authentication request parameters

Sample Request

A typical request looks as follows. The important attributes are highlighted: **`ForceAuthn`**, **`Issuer`**, **`NameIDPolicy`** and **`RequestedAuthnContext`**.

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    ID="s2fbfcec03a12c05e5fcc7a07e2b02c00b4c742fec"
    Version="2.0" IssueInstant="2023-12-04T12:07:12Z"
    Destination="https://idp.iamfas.ta.belgium.be/fas/SSORedirect/metaAlias/idp"
    ForceAuthn="false"
    IsPassive="false"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

AssertionConsumerServiceURL="https://iamapps.ta.belgium.be/demo1/fedletapplication">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        https://iamapps.ta.belgium.be/demo1
    </saml:Issuer>
    <samlp:NameIDPolicy
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
        SPNameQualifier="https://iamapps.ta.belgium.be/demo1"
        AllowCreate="true" />
    <samlp:RequestedAuthnContext
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
        Comparison="minimum">
        <saml:AuthnContextClassRef
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            urn:be:fedict:iam:fas:citizen:Level500
        </saml:AuthnContextClassRef>
        <saml:AuthnContextClassRef
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            urn:be:fedict:iam:fas:citizen:IAL500
        </saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Figure 2 Sample authentication request

Response

A typical response would look as below. The important attributes are:

- The combination of **`Destination`**, **`ID`** and **`InResponseTo`** are used to prevent replay attacks and abuse of captures responses.
- Status Code (`samlp:StatusCode`)
- `AuthnContext`
- The content of attribute statement (`saml:AttributeStatement`)

Sample Response

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  Destination="https://iamapps.ta.belgium.be/demo1/fedletapplication"
  ID="s2305c13e9c4324dbb16ab9b802ecc60f3cf0716c5"
  InResponseTo="s23c4cd1d56655287744a690d3f2ac3833994d105f"
  IssueInstant="2023-12-05T07:44:04Z" Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    https://idp.iamfas.ta.belgium.be/fas</saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
      <ds:Reference URI="#s2305c13e9c4324dbb16ab9b802ecc60f3cf0716c5">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

<ds:DigestValue>+s5oY54+hvGZ73xWJq61wH0v8H1HoEhNeqGP2RYN4jY=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>s5OsQT7n0seIY...oP3c3CLD+8DDrZlmpK3aw=</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIIlDCCBny...3MX7rROKJtINx3nbg==</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </samlp:Status>
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2e1ed4292c0d2d496a6b4d1a84bb65f78188331cf"
    IssueInstant="2023-12-05T07:44:04Z"
    Version="2.0">
    <saml:Issuer>https://idp.iamfas.ta.belgium.be/fas</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
        <ds:Reference URI="#s2e1ed4292c0d2d496a6b4d1a84bb65f78188331cf">
          <ds:Transforms>
            <ds:Transform
              Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

<ds:DigestValue>sY1A7Ll+iv5L3YOK8Bl8jpMLG8pBK11u06bPwdhiJww=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
```

```
      <ds:SignatureValue>NRCJURVc3DOQC1a...R827EbHiqlUSk/SHX2Y=</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>MIIIlDCCBnAw...0INx3nbg==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>
      <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
        NameQualifier="https://idp.iamfas.ta.belgium.be/fas"
        SPNameQualifier="https://iamapps.ta.belgium.be/demo1">
        656964.58c14e71-ec3e-4f4c-8a46-7739f2c27d27</saml:NameID>
      <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData
          InResponseTo="s23c4cd1d56655287744a690d3f2ac3833994d105f"
          NotOnOrAfter="2023-12-05T07:54:04Z"
          Recipient="https://iamapps.ta.belgium.be/demo1/fedletapplication"/>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2023-12-05T07:34:04Z"
      NotOnOrAfter="2023-12-05T07:54:04Z">
      <saml:AudienceRestriction>
        <saml:Audience>https://iamapps.ta.belgium.be/demo1</saml:Audience>
      </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2023-12-05T07:44:04Z"
      SessionIndex="s29576bd741ff712a0eed35f6b022851907cdd8601">
      <saml:AuthnContext>
<saml:AuthnContextClassRef>urn:be:fedict:iam:fas:citizen:Level500</saml:AuthnContext
ClassRef>
      </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name="uid">
        <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:type="xs:string">john.doe</saml:AttributeValue>
      </saml:Attribute>
      ...
      <saml:Attribute Name="authenticationmethod">
        <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:type="xs:string">eid</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```

Figure 3 Sample authentication response

Logout Request

The SAML Simple Logout (SLO) request follows the typical SAML message but also includes the name ID of the user to log out.

Request

Parameter		Value
Issuer	Mandatory	Issuer
NameID	Mandatory	User identifier
SessionIndex	Mandatory	Session identifier
locale	Optional but recommended	One of: “en” “de” “fr” “nl”. The default value is “nl”.

Table 8 Logout request parameters

Sample Request

```
<samlp:LogoutRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    ID="s2d1cdf8aa8b3063edb026b7ce86efda77ed52417b"
    Version="2.0"
    IssueInstant="2015-01-28T19:35:27Z"
    Destination="https://idp.iamfas.belgium.be/fas/IDPSloRedirect/metaAlias/idp">

    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        https://iamapps.belgium.be/
    </saml:Issuer>

    <saml:NameID
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        NameQualifier="https://idp.iamfas.belgium.be/fas"
        SPNameQualifier="https://iamapps.belgium.be/"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
        myNs4TJ12S7I6OW3gGk6uA7Fvb/a
    </saml:NameID>

    <samlp:SessionIndex
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
        s21d268460527f0c526f9591e3398642d04 85ba112
    </samlp:SessionIndex>
</samlp:LogoutRequest>
```

Figure 4 Sample logout request

Response

A typical response would look as follows:

Attributes		**Value**
Issuer	Mandatory	The requested scopes
Status	Mandatory	The status of the request

Table 9 Logout response attributes

Sample Response

```
<samlp:LogoutResponse
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    ID="s63732ba858c3fd3c394faf58f3fa4833de1a9727"
    Version="2.0"
    IssueInstant="2015-01-28T19:35:27Z"
    Destination="https://iamapps.belgium.be/fedletSloPOST"
    InResponseTo="s2d1cdf8aa8b3063edb026b7ce86efda77ed52417b">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        https://idp.iamfas.belgium.be/fas
    </saml:Issuer>

    <samlp:Status
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
        <samlp:StatusCode
            xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
            Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
</samlp:LogoutResponse>
```

Figure 5 Sample logout response