Technical specifications
Identity & Authorization Management (I.AM)
SP Shibboleth – Upgrade

Migration from IDP v1.3 to IDP v2

Version 1.0

This document is provided to you free of charge by

The eHealth platform

Willebroekkaai 38 – Quai de Willebroeck 38
1000 BRUSSELS

Table of contents

1 Document management

1.1 Document history

Version	Date	Author	Description of changes / remarks
1.0	11/07/2013	eHealth	Initial version

2 Introduction

2.1 Introduction

The eHealth IDP has received a major upgrade (v1.3 → v2) and is now part of the eHealth I.AM Federation.

To ease migration of legacy components, communication between existing SPs and the new eHealth IDP may remain similar as before.

However, during a transition period, existing SPs are requested to perform a few updates.

Some of them are required, others are optional.

This document describes for existing Shibboleth SP partners the specific changes they should perform to update their SP to integrate well with the eHealth I.AM Federation IDP.

If you want more information on the different configuration sections or if you don't use a Shibboleth SP yet, please consult the cookbook 'eHealth I.AM – SP Shibboleth' which contains a full setup description and various HOWTOs for additional configuration.

Existing Shibboleth SP partners have a working integration with the eHealth IDP v1.3.

The eHealth I.AM IDP v2 supports all the protocols and bindings that were used in the v1.

However, there are changes to be done by the SPs in the near future: some optional, some required.

They are listed in the sections below.

2.2 Goal of the document

This document is not a development or programming guide for internal applications. Instead it provides functional and technical information and allows an organization to integrate and use the eHealth service.

But in order to interact in a smooth, homogeneous and risk controlled way with a maximum of partners, eHealth partners must commit to comply with the requirements of specifications, data format and release processes described in this document.

Technical and business requirements must be met in order to allow the integration and validation of the eHealth service in the client application.

2.3 eHealth document references

All the document references can be found in the support section of the eHealth portal[1]. These versions or any following versions can be used for the eHealth service.

ID	Title	Version	Date	Author
1	Glossary.pdf	1.0	01/01/2010	eHealth

2.4 Service history

This chapter contains the list of changes made to the service with respect to the previous version.

Previous version	Previous release date	changes
	DD/MM/YYYY	

Remark: = "None" when the major version = 1

[1] www.ehealth.fgov.be

3 eHealth contact

eHealth ContactCenter:

02 / 788 51 55

- Mail: support@ehealth.fgov.be
- Web form:
    - Dutch version: https://www.ehealth.fgov.be/nl/contactform/website/home/contactform.html
    - French version: https://www.ehealth.fgov.be/fr/contactform/website/home/contactform.html

4 Changes

4.1 Shibboleth SP version (optional)

The past years, Shibboleth team has upgraded a few times its software for Service Providers (SP).

At this time of writing, the latest version is v2.5.1, released on 10 December 2012[2].

A roadmap with status and fixes of the Shibboleth SP software can be found on the Shibboleth WIKI[3].

As announced on the Shibboleth WIKI, it is advised to subscribe to the Shibboleth Announcement mailing list[4]. This is where announcements about new releases, end-of-life of past releases, and security advisories are distributed.

4.1.1 Upgrade 2.x

If you are running an older v2 version, you are advised to upgrade to the latest version.

It should be fairly simple if you are running a Windows or Linux version as automated installation and upgrade is available from the Shibboleth site. For other distributions it might be a bit harder.

See the Native Service Provider section on the installation page[5] of the Shibboleth WIKI. You will find links for installation of the software on the different supported Operating Systems.

4.1.2 Upgrade from 1.3 to 2.x

If you still run a v1 version, we strongly advise you to upgrade to the v2.x series.

However, no automated upgrade is available.

See the upgrade page on the Shibboleth WIKI[6].

[2] http://shibboleth.net/community/news/20121210.html

[3] https://wiki.shibboleth.net/confluence/display/DEV/SPRoadmap

[4] http://shibboleth.net/community/lists.html

[5] https://wiki.shibboleth.net/confluence/display/SHIB2/Installation

[6] https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPUpgradeOlder

4.2 IDP Metadata updates (required)

To setup communication between the SP and IDP v1.3, a SAML 2.0 Metadata file was used: ehealth-metadata-idp.xml.

It contained information on the locations of the IDP Services and certificates used.

It was sent to the partners everytime the file was updated and the partners needed to update manually their local installation.

The eHealth I.AM IDP v2 also comes with a SAML 2.0 Metadata file which is very similar to the one of the IDP v1.3 but it contains more information and the locations of the IDP services are different.

To ease migration for the existing SPs, the old locations at the eHealth Platform are temporary routed to the new locations.

However, you must start using the new IDP Metadata so in time all SPs will contact directly the right locations.

To start using the new metadata, you should plan an update of the section of the MetadataProvider in the shibboleth2.xml configuration file.

As the new metadata of the eHealth is available online, you only need to do this update once. Your Shibboleth SP will keep a local cache up to date. Future updates of the metadata will no longer require interventions by the partner.

To receive automatic metadata updates of the eHealth IDP v2, replace your current MetadataProvider section in the shibboleth2.xml configuration file of your distribution by the MetadataProvider section below.

```
<MetadataProvider type="XML"
       uri="[idp-root]/profile/Metadata/SAML"
       backingFilePath="[workdir]/ehealth-metadata-idp-iam.xml"
       maxRefreshDelay="86400">
</MetadataProvider>
```

Note:

- **Idp-root**: Location of the eHealth IDP webapplication. Please use the location of the IDP in the eHealth environment you wish to integrate with (int, acc, prod)[7]. The content will be different for each environment.
- **Workdir**: A Location of your choice where the Shibboleth SP can store a cached version of the online metadata. Defaults to [SHIB_HOME]/var/run/shibboleth.
- **maxRefreshDelay**: This is a synonym for the reloadInterval setting, and determines the maximum allowed refresh interval (in seconds) when polling a remote resource for changes.

[7] For production, this will be https://www.ehealth.fgov.be/idp

For more information on the content of the metadata and the reload process, see the documentation on Federation Metadata[8] and the Shibboleth WIKI[9].

4.3 eHealth Attributes (required)

The eHealth IDP v1 returned all identity and authorization information in one SAML Attribute 'urn:behealth:data' (or 'authorisationResponse' for WS-Federation).

It contained a CDATA section with an xml element <AuthorisationResponse> (from the eHealth metadata.xsd).

The eHealth IDP v2 returns all identity and authorization information in separate SAML Attributes: mostly simple string values, one for each identity or authorization element.

For the time being, the IDP still sends the 'legacy' attribute 'urn:behealth:data' so partners have the time to start using the new attributes.

As the Shibboleth SP filters out everything that is not specifically mapped in its configuration, your SP will keep using the legacy attribute 'urn:behealth:data' (as you always received it) and filter anything else out until you update your configuration mapping and filtering as described in sections below.

4.3.1 Mapping

The attribute-map.xml configuration file of your SP now probably contains something like this (as described in the old cookbook):

```
<Attributes xmlns="urn:mace:shibboleth:2.0:attribute-map"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <Attribute name="urn:behealth:data" id="Shib-Behealth-Data" />
</Attributes>
```

You should stop mapping the urn:behealth:data attribute as it is deprecated and start mapping the new attributes supported in the eHealth I.AM Federation.

Please read section 'Update <shib-sp>\etc\shibboleth\attribute-map.xml' of the 'eHealth I.AM – SP Shibboleth' cookbook on how to.

[8] See document 'eHealth I.AM – Federation Metadata'.

[9] https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMetadataProvider

Filtering

The attribute-policy.xml configuration file of your SP now probably contains something like this (as described in the old cookbook):

```
<afp:AttributeFilterPolicyGroup xmlns="urn:mace:shibboleth:2.0:afp:mf:basic"
xmlns:basic="urn:mace:shibboleth:2.0:afp:mf:basic" xmlns:afp="urn:mace:shibboleth:2.0:afp"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <afp:AttributeFilterPolicy>
    <!-- This policy is in effect in all cases. -->
    <afp:PolicyRequirementRule xsi:type="ANY" />
    <afp:AttributeRule attributeID="Shib-Behealth-Data">
      <afp:PermitValueRule xsi:type="ANY" />
    </afp:AttributeRule>
  </afp:AttributeFilterPolicy>
</afp:AttributeFilterPolicyGroup>
```

Once you stopped mapping the urn:behealth:data attribute to Shib-Behealth-Data, you should stop filtering for the Shib-Behealth-Data attribute as it will no longer be there.

You should start filtering the new list of attributes (or stop filtering at all).

Please read section ‘Update <shib-sp>\etc\shibboleth\attribute-policy.xml’ of the ‘eHealth I.AM – SP Shibboleth’ cookbook on how to.

4.3.2 Authorization

The `<AuthorisationResponse>` in the urn:behealth:data Attribute contained a ‘NOT AUTHORIZED’ error message and ticketnumber if the user was not authorized by eHealth.

In the eHealth IDPv2 this is no longer used.

Please consult the HOWTO ‘enforce eHealth-Authz-Decision’ of the cookbook ‘eHealth I.AM – Shibboleth SP’ to learn how to enforce the authorization decision that was made by ehealth.

Don’t forget to update your authentication/authorization component (not part of the Shibboleth Software) which expected the `<AuthorisationResponse>` variable or header, made available by the Shibboleth SP. This component will now have to look for the other variables or headers you will map in the configuration file attribute-map.xm.

See HOWTO ‘Attach an Access Control Policy’ if you want to perform authorization rules at the level of the Webserver or Shibboleth SP.

4.4 SAML Protocol, Profile and Binding (optional)

The Shibboleth SP v2.x series support all SAML 1.1 and SAML 2.0 Web Browser SSO profiles.

The eHealth IDP v1.3 supported only the following profiles:

- SAML 1.1 Browser/POST (push)
- SAML 1.1 Browser/POST, proprietary Shibboleth (pull – with callback AttributeQuery)
- WS-Federation: Web (Passive) Requestor

For this reason, the old cookbook requested to specify SAML 1.1 Browser/POST as default profile.

As configured at the eHealth IDP, this included for most SPs the callback AttributeQuery.

This means you probable have something like below configured in your shibboleth2.xml:

```
<Sessions lifetime="28800" timeout="3600" checkAddress="false"
            handlerURL="/Shibboleth.sso" handlerSSL="false"
         exportLocation="http://localhost/Shibboleth.sso/GetAssertion" exportACL="127.0.0.1"
idpHistory="false" idpHistoryDays="7">

<SessionInitiator type="Chaining" Location="/Login" id="sso" relayState="cookie"
entityID="http://idp.smals-mvm.be/shibboleth">
        <SessionInitiator type="Shib1" defaultACSIndex="5"/>
        <!-- others: not supported by ehealth for now -->
</SessionInitiator>

<md:AssertionConsumerService Location="/SAML/POST" index="5" isDefault="true"
                Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"/>
```

The eHealth IDP v2 now also supports all SAML 1.1 and SAML 2.0 Web Browser SSO Profiles.

This means you can leave your configuration as it is or you can choose to upgrade to SAML 2.0.

eHealth has no plans yet to remove the SAML 1.1 profiles, they remain supported.

However, since SAML 2.0 is the successor of SAML 1.1, we advise you to consider an upgrade to a SAML 2.0 profile.

Since SAML 2.0 supports encryption (SAML 1.1 does not), this also opens the possibility to eliminate the need for the AttributeQuery callback if you choose the SAML 2.0 HTTP-POST profile.

A communication between SP and IDP would then be simplified to one redirect from SP to IDP and one POST back from the IDP to the SP with all the requested information in an encrypted SAML 2.0 Assertion.

Your SP will take care of everything so you do not need to worry about that.

This is the profile eHealth suggests by default.

If you plan to migrate to this or another profile, please read HOWTO ‘Switch default SAML Profile using SessionInitiators’ of the ‘eHealth I.AM – SP Shibboleth’ cookbook on how to switch SessionInitiators.

If you upgraded your SP to at least version 2.4, you can also remove all <SessionInitiator> elements and use the simplified notation with an <SSO> element as specified in the section 'Update <shib-sp>\etc\shibboleth\shibboleth2.xml' of the cookbook.

Please contact eHealth development team before you test so we can make sure the profile is configured for your ServiceProvider at the IDP.