ISA Action 1.17: A Reusable INSPIRE Reference Platform (ARE3NA)

Authentication, Authorization and Accounting for Data and Services in EU Public Administrations

D3.3c – Deployment of a Shibboleth Service Provider

Pieter De Graef

Andreas Matheus

Dirk Frigne

Reijer Copier

Jan De Moerloose

Robin S. Smith

Joint
Research
Centre

This publication is a Deliverable of Action 1.17 of the Interoperability Solutions for European Public Administrations (ISA) Programme of the European Union, A Reusable INSPIRE Reference Platform (ARE3NA), managed by the Joint Research Centre, the European Commission's in-house science service.

The study contributing to this publication has been undertaken by Pieter De Graef, Andreas Matheus, Dirk Frigne, Reijer Copier and Jan De Moerloose in collaboration with Robin S. Smith and Michael Lutz from the EC Joint Research Centre.

Disclaimer

The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

Copyright notice

Bibliographic Information:
De Graef P, Matheus A, Frigne D, Copier R, De Moerloose J, Smith RS. Authentication, Authorization and Accounting for Da-ta and Services in EU Public Administrations D3.3c – Deployment of a Shibboleth Service Provider. European Commission; 2015. JRC98196

Table of Contents

Glossary

AAA	Authentication, Authorization, Accounting
AAAI	AAA Infrastructure
ABAC	Attribute-Based Access Control
ACM	Access Control Management
ADFS	Active Directory Federation Service
AMF	Access Management Federation
AP	Attribute Provider
ARE3NA	A Reusable INSPIRE Reference Platform (ISA Action 1.17)
BIWG	Business Interoperability Working Group of the UK Location Programme
CAS	Central Authentication System
CERN	European Organization for Nuclear Research
COBWEB	Citizen OBservatory WEB
CORS	Common Resource Sharing
Corve	e-Government Cell of the Flemish Government
COTS	Commercial Off-The-Shelf Software
CBO	Cross Border Operation
CSW	OGC Catalog Service for the Web
DARIAH	DigitAl Research Infrastructure for the Arts and Humanities
DOV	Database Underground Flanders of the Flemish Government
DS	Discovery Service
DNS	Domain Naming System
EAP	Extensible Authentication Protocol
EC	European Commission
ECP	Enhanced Client or Proxy
EGI	European Grid Infrastructure
EU	European Union
EUDAT	European Data Infrastructure
FEDICT	Federal ICT (Belgium)
GDI-DE	The Spatial Data Infrastructure of Germany
GeoPDP	Geographically extended Policy Decision Point
GEOSS	Global Earth Observation System of Systems
GSI-SSH	Grid Security Infrastructure – Security Shell
GUGiK	Head Office of Geodesy and Cartography, Poland
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICT	Information and Communication Technology
IDF	Identity Federation
IDM	Identity Management
IdP	Identity Provider
IE	Interoperability Experiment
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGN-BE IGN-FR	Institut Géographic National (France and Belgium)
INSPIRE	Infrastructure for Spatial Information in the European Community
ISA	Interoperability Solutions for European Public Administrations

JRC	Joint Research Centre
LNE-ACD	Environment, Nature and Energy Department of the Flemish Government, Central Data Management Unit
LoA	Level of Assurance
LoT	Level of Trust
NREN	National Research and Education Network
NTP	Network Time Protocol
OASIS	Advancing Open Standards for the Information Society
OGC	Open Geospatial Consortium
OpenSSL	An open-source implementation of the SSL and TLS protocols
OSS	Open Source Software
PAOS	Reverse SOAP binding
PEP	Policy Enforcement Point
PRACE	Partnership for Advanced Computing in Europe
PVP	PortalVerbund Protocol , a specific Austria protocol for secure access
RADIUS	Remote Authentication Dial In User Service
SAML	Security Assertion Markup Language
RFC	Request For Comments
SDI	Spatial Data Infrastructure
SP	Service Provider
SSL	Secure Sockets Layer
SSO	Single Sign-On
STORK	Secure idenTity acrOss boRders linked
SWOT	Strengths, Weaknesses, Opportunities and Threats
TLS	Transport Layer Security
URL	Uniform Resource Locator
VO	Virtual Organisation
W3C	World Wide Web Consortium
WFS	OGC Web Feature Service
WMS	OGC Web Map Service
WAYF	Where Are You From
WSS	52North Web Enforcement Service
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
XRI	Extensible Resource Identifier

1 Introduction

This document is one of the deliverables of the project *"Authentication, Authorization and Accounting for Data and Services in EU Public Administrations"* launched by the Joint Research Centre of the European Commission (Contract n°389834). The project is part of ARE3NA, one of the actions of the ISA Programme (Action 1.17), aiming to create a Re-usable INSPIRE reference platform. The general objective of the project is to assist the Joint Research Centre (JRC) of the European Commission in preparing a study, workshop and testbed on standards, technologies and best practices for the Authentication, Authorization and Accounting (AAA) of data and services to support secure data exchange by public administrations in Europe, including INSPIRE data and services.

The particular objectives for the project can be summarized as follows:

1. To identify and assess the current standards and technologies that would help to guarantee secure data exchange between public administrations, with particular focus on INSPIRE data and services, as well as those relevant in the context of the ISA programme and the Digital Agenda for Europe.
2. To identify and assess best practices in Europe with regard to the application of those standards and technologies for data and service sharing in order to better understand what works well, what not and what elements are missing or could be improved.
3. To design, develop and deploy an AAA-testbed using open source technology, based on existing INSPIRE and SDI components in three Member States taking into account the organisational, legal and technical settings.
4. To involve actively Member State representatives on the proposed AAA-architecture and testbed and to collect feedback from them.

As a key part of the project (Task 3), this document *"D3.3c – Deployment of a Shibboleth Service Provider"* contributes to the testbed activities noted in points 3 and 4, above. Acting as a guide, it describes the technical aspects of the access management federation that is to be put into place during the testbed phase of the project, focussing on how to put in place the Shibboleth technology for an Service Provider (SP), alongside other documents covering setup for an Identity Providers (IdP, who provides access credentials) and a Coordination Centre (CC) who helps the trusted exchange of access details in the access federation). In developing the testbed as Task 3 of the project, the work has been divided into the following three phases :

1. **Testbed development** : where the consortium will first develop the testbed on local servers.
2. **Testbed implementation** : In this phase, the testbed is extended to include the supporting organizations. It is important to note that the supporting organizations do not create a new federation, but join the existing federation set up during the testbed development phase.
3. **Testbed assessment** : This is a continuous phase in which we assess all steps taken in the first 2 phases.

This technical document, therefore, acts as a part of a series of guides for anyone trying to set up a similar testbed (or federation) for INSPIRE or other sectors interested in accessing geospatial data.

The remaining sections outline the resources and prerequisites for the SP setup (Section 2). This is followed by a section explaining how to install the Shibboleth SP (Section 3), SSL certificates & Apache configuration (Section 4) and configuration of the Shibboleth SP (Section 5), with details for configuring session initiation and metadata for the intranet (Section 6) and federated (Section 7) cases. This is followed by Metadata Adaption, including settings such as IdP display name, and company/contact information (Section 8). Settings are also described for the removal of the SAML1 handler, including from metadata (Section 9). Two sections then outline how to protect a resource (Section 10) and issues of protecting a web service (Section 11). The document closes with a description of the run and test settings (Section 12) and firewall settings (Section 13).

1 Resources and Prerequisites

This document describes a Linux Server specific installation of a Shibboleth identity Provider 2.4 and its configuration specific for the ARE3NA AAA Federation. In-depth information on any aspect of Shibboleth can be found online starting at this link: https://wiki.shibboleth.net/confluence/display/SHIB2/Installation

The Shibboleth Service Provider (SP) 2.5 is implemented in is implemented in C/C++ as an Apache authentication module mod_shib and a separate daemon shibd.

The following values are used in this guide:

$DOMAINNAME = The common domain in which the IdP is a subdomain.

$HOSTNAME = idp.$DOMAIN (“The DN of the Resource Service Provider”)

Before starting to install and configure the Shibboleth Identity Provider, ensure that the following prerequisites are met:

- Apache HTTP 2.2.x with OpenSSL (*https://www.openssl.org/*) is installed
- A proper certificate for providing a Transport Layer Security (TLS) connection to the Apache web server hosting the protected resource is required.
- The Shibboleth Service Provider will use a self-signed certificate.
- Network Time Protocol (NTP) is installed and activated on the server. Servers running Shibboleth must have their system time synchronized in order to avoid clock-skew errors.

2 Installation of the Shibboleth IdP

How to install the IdP software; please follow the process outlined for your operating system here:

https://wiki.shibboleth.net/confluence/display/SHIB2/IdPInstall

3 SSL certificates & Apache configuration

As explained in the prerequisites, the web server hosting the IdP and the protected endpoints must support HTTPS with SSLv3 or TLSv1.

Please note that if you want to deploy the IdP in the same domain, it might be cheaper to order a SSL Wild Card certificate. Assuming that the SP and the IdP will be deployed in the same domain, the wild card certificate must cover ***.$DOMAINNAME**.

Please use your preferred Certificate Authority to order the certificate.

Please follow the instructions that you receive with the certificate or follow the configuration instructions available for Apache to enable HTTPS properly. A successful installation of the certificate should be tested using either an online SSL checker (e.g. http://www.sslchecker.com) or use the openssl command available with linux:

```
#root> openssl s_client --connect https://$HOSTNAME
```

4 Configuration of the Shibboleth SP

This section covers the specific configuration of the Shibboleth daemon for the ARE3NA AAA Federation.

1.1 shibboleth2. Xml

shibboleth2.xml is the main file for configuring your Shibboleth Service Provider. Edit the **/etc/shibboleth/shibboleth2.xml** file and make sure you update the file to reflect the changes outlined in the following subsections.

4.1.1 ApplicationDefaults

This configuration element describes the basic behaviour of the SP. Please make changes to reflect the following (remember to replace **$HOSTNAME** with the actual value). Set the **entityID**: This is a unique identifier for your Service Provider. Typically, this is **https://$HOSTNAME/shibboleth .**

```
<ApplicationDefaults entityID="https://$HOSTNAME/shibboleth"
    authType="TLS" signing="true" encryption="false"
    requireConfidentiality="true" requireTransportAuth="true"
    REMOTE_USER="eppn persistent-id targeted-id">
```

4.1.2 Sessions

We keep the default session times (maximum length is 8h and the maximum time before a session becomes inactive is 1h), but we enforce the use of HTTPS by setting the `handlerSSL`. This also requires that we change the default cookie configuration using the `cookieProps`.

```
<Sessions lifetime="28800" timeout="3600"
    relayState="ss:mem"
    checkAddress="false" handlerSSL="true"
    cookieProps="; path=/; secure">
```

5 Configuring session initiation and metadata (intranet case)

This section covers the configuration for the intranet case. This must be up-and-running before moving to the federated case.

2.1 SessionInitiators

The following simple Simple Sign-On (SSO) setup for browser clients can be used for testing with a local IdP:

```
<SSO entityID="https://$IDP_HOSTNAME/idp/shibboleth">SAML2</SSO>
```

3.1 MetadataProvider

The local IdP must be configured by putting its metadata in a local file:

```
<MetadataProvider type="XML" file="partner-metadata.xml"/>
```

The file **partner-metadata.xml** should be present in the **/etc/shibboleth** folder and contain the advertised metadata of the IdP. Just download the contents of the metadata URL and put it in the file:

https://$IDP_HOSTNAME/idp/profile/Metadata/SAML

6 Configuring session initiation and metadata (federated case)

Important! Make sure you have the intranet case working before attempting the federated case.

4.1 Basic configuration

6.1.1 SessionInitiators

The session initiation for the ARE3NA AAA Federation must reflect the requirements because OGC Web Services are provided and because they are to be consumed by web-based and desktop clients. In order to support automatic SSO, the only session initiation is possible via the SAML protocol. To enable this, the appropriate Discovery Service (DS) URL must be provided in the **discoveryURL: https://ds.aaa.secure-dimensions.de/DS**

In order to enable the desktop clients to connect, the ECP support must be enabled. This can be achieved by using the **ECP** attribute.

For the Browser SSO Profile, it is important that you verify that the session initiation is taking place using the Artefact Binding. This can be configured using the **acsIndex**. Please make sure that the index used actually matches the index for artefact binding, as listed in the metadata for the SP.

```
<SSO acsByIndex="true" acsIndex="3" ECP="true" discoveryProtocol="SAMLDS"
     discoveryURL="https://ds.aaa.secure-dimensions.de/DS">SAML2</SSO>
```

6.1.2 MetadataProvider

For this federation, the signed metadata is hosted at

http://www.aaa.secure-dimensions.de/metadata/aaa-metadata.xml or

https://www.aaa.secure-dimensions.de/metadata/aaa-metadata.xml

The signature verification is possible by obtaining the public key used by the Coordination Centre for signatures: https://www.aaa.secure-dimensions.de/metadata/AAA.pem

You can use the following command to obtain the public key:

```
#root> curl https://www.aaa.secure-dimensions.de/metadata/AAA.pem \

       -o /etc/shibboleth
```

We keep the maximum validity for the metadata at 28 days[1].

```
<MetadataProvider type="XML"
    uri="http://www.aaa.secure-dimensions.de/metadata/aaa-metadata.xml"
    backingFilePath="aaa-metadata.xml" reloadInterval="7200">
 <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
 <MetadataFilter type="Signature" certificate="AAA.pem"/>
</MetadataProvider>
```

6.1.3 Errors

It is possible to customize the page and settings to reflect how an organization wishes to present itself online. The following example reflects the Secure Dimensions SP Proxy for GDI-BY. It uses the default Shibboleth style but advertises the Secure Dimensions email address for support.

```
<Errors supportContact="support@secure-dimensions.de"
    helpLocation="/about.html" styleSheet="/shibboleth-sp/main.css"/>
```

[1] This ensures that the CC must refresh the metadata a couple of times throughout the project. It also allows that the effectiveness of the automatic establishment of the circle of trust via the centrally hosted metadata can be tested. To test this, the CC will – with warning to the federation members – fail to sign the metadata.

6.1.4 Attribute Mapping and Acceptance

Attributes received from the IdP have to be mapped from the standard “wire[2]” naming convention to domain specific attribute names. This is configured in the attribute-map.

For simplicity and the ease of configuring access rights, all SPs of the ARE3NA AAA Federation use the same identical attribute mapping, with the CC hosting that file online. Each SP will load any changes once the refresh time is up. The URL for the attribute map is:

https://www.aaa.secure-dimensions.de/metadata/sp-attribute-map.xml

Please use this URL to configure the attribute mapping, as shown below:

```
<AttributeExtractor type="XML"
  uri="https://www.aaa.secure-dimensions.de/metadata/sp-attribute-map.xml"
  backingFilePath="attribute-map.xml" reloadInterval="7200"/>
```

5.1 attribute-policy.xml

The **attribute-policy.xml** file describes rules to filter received attributes. The rules may reflect individual trust relationships with IdPs. This means that, typically, the filter configuration is maintained locally. For this federation, each SP must be configured to accept all attributes.

```
<AttributeFilter type="XML" validate="true" path="attribute-policy.xml"/>
```

6.1 Logging

There are two different Shibboleth related log files you can access for troubleshooting.

- **native.log**: located in **/var/log/httpd** and can be configured in **/etc/shibboleth/native.logger**
- **shibd.log**: is located in **/var/log/shibboleth** and can be configured in **/etc/shibboleth/shibd.logger**

Important! Make sure that the right processes have write permissions to the log files!

As the shidb process is owned by the shibd user, it is recommended to create the logfiles and change ownership, as follows:

```
#root> touch /var/log/httpd/native.log

#root> chown shibd /var/log/httpd/native.log

#root> touch /var/log/httpd/shibd.log

#root> chown shibd /var/log/httpd/ shibd.log
```

The level of logging detail can be adjusted inside the **/etc/shibboleth/shid.logger** file.

[2] For this federation, a set of attribute names to be exchanged must be determined. It is recommended to use the ones listed in the eduGain paper.

7.1 Layout

Shibboleth ships with some default html pages. These can be found in the **/etc/shibboleth** folder. For this federation, we do **not** change these files:

- **accessError.html**
- **bindingTemplate.html**
- **globalLogout.html**
- **localLogout.html**
- **metadataError.html**
- **postTemplate.html**
- **sessionError.html**
- **sslError.html**

7 Metadata adaption

The metadata, generated by the default installation, does not reflect the project specific needs regarding the correct display of logos and explanatory text.

As the AAA Test Federation is using the SWITCH Discovery Service it is recommended (for proper design) to make the following additions to the metadata before sending it to the Coordination Centre.

8.1 SP Display Name and Logo

When a user logs in with their IdP, the logo and the description of the SP that the user is trying to initiate a session with, is displayed at the IdP login page. The information for the SP (name, description and logo) is taken from the SP metadata.

9.1 Company and Contact Information

It is good practice to include company and contact information in the metadata. Please add the following XML snippet before the closing tag `</EntityDescriptor>`

```
<md:Organization>
    <md:OrganizationName xml:lang="en">Secure Dimensions GmbH</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="en">SD</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en">http://www.secure-dimensions.de/</md:OrganizationURL>
</md:Organization>
<md:ContactPerson contactType="technical">
    <md:GivenName>Andreas</md:GivenName>
    <md:SurName>Matheus</md:SurName>
    <md:EmailAddress>mailto:am@secure-dimensions.de</md:EmailAddress>
</md:ContactPerson>
<md:ContactPerson contactType="administrative">
    <md:GivenName>Andreas</md:GivenName>
    <md:SurName>Matheus</md:SurName>
    <md:EmailAddress>mailto:am@secure-dimensions.de</md:EmailAddress>
</md:ContactPerson>
```

8 Removal of SAML1 Support

For the AAA Project Federation, there is no need to support SAML1. It is therefore recommended practise to remove SAML1 support. This can be achieved in three steps: (i) remove the SAML1 related handler, (ii) remove the exposure of SAML1 handlers, and (iii) remove SAML1 support indication in the metadata. We outline each step in the following sections.

1.1Remove SAML1 Handler

The handler configuration can be found in the **shibboleth2.xml** document. Removal of SAML1 support can be achieved by changing the <SSO> element by deleting the SAML1 value as illustrated below.

```
<SSO acsByIndex="true" acsIndex="..." ECP="true"
     discoveryProtocol="SAMLDS" discoveryURL="https://ds.aaa.secure-dimensions.de/DS">
  SAML2
</SSO>
```

10.1 Remove SAML1 Handler from Metadata

The exposed URL endpoints are automatically adopted from the **shibboleth2.xml** configuration after a shibd restart. The metadata can be obtained by using the SP metadata exposure URL:

https://$HOSTNAME/Shibboleth.sso/Metadata

9 Protect a resources

You can protect a resource with Shibboleth per URL by configuring your Apache webserver. Edit the file **/etc/httpd/conf.d/shib.conf** to reflect your needs. For this federation, we keep the default-protected path **/secure** for simplicity and use the configuration for any additional locations to protect individual service endpoints.

```
<Location /secure>
    AuthType shibboleth
    ShibRequireSession On
    require valid-user
</Location>
```

To create some content for the /secure link, add an index.html file to the following location (for document root **/var/www/sp**, use your own document root if applicable):

```
/var/www/sp/secure
```

10 Protect a Web Service – The CORS Issue

Setting up the endpoint for a Web Service (such as OGC WMS or WFS) can be achieved in the same fashion as for a resource. However, it is important to note that the use of the service in a Web Browser type application is constrained by the Browser security sandbox. The common limitation implemented by all vendors is “same origin”.

In cases where, however, the service shall be consumed in a web mapping application such as an OpenLayers application, the need arrives to relax the “same origin” security sandbox. The W3C recommendation Common Resource Sharing (CORS) addresses this by introducing web server side access control triggered by HTTP headers.

Essentially, the idea behind CORS is server side access control based on white listing. Whenever a Web Browser based application is making a cross domain call, it sends the HTTP Origin with the request. Based on this header, the web server called must determine if access shall be granted. Where access is granted, the web server will return the HTTP header Access-Control-Allow-Origin. If the Origin and the Access-Control-Allow-Origin values match, then the browser allows the application to use the data received.

To support Single-Sign-On using cookies, the web server must also return the HTTP header Access-Control-Allow-Credentials with the value true.

The CORS whitelisting is a common issue when establishing access control to Web Server URLs that are protected by SAML. This is not the case in the context of a federation.: In order for a client application to execute the web service the user must be authenticated first. In that sense, the whitelisting is (*defacto*) null and a simple Apache configuration can be used to support CORS, as illustrated below.

```
 SetEnvIf Origin (.+) ORIGIN=$1
Header set Access-Control-Allow-Origin "%{ORIGIN}e" env=ORIGIN
Header set Access-Control-Allow-Credentials true
```

11 Run & Test

To run and test the SP the details below need to be followed.

On CentOS, export the **LD_LIBRARY_PATH** first:

```
#root> export LD_LIBRARY_PATH=/opt/shibboleth/lib64:$LD_LIBRARY_PATH
```

You can now test the configuration by entering the following command:

```
#root> /usr/sbin/shibd -t /etc/shibboleth/shibboleth2.xml
```

The configuration is acceptable if the output /overall configuration is loadable. The console needs to be checked for non-fatal problems.

You can now start/stop/restart the shibboleth daemon using the following commands:

```
#root> service shibd start | stop | restart
```

To make sure the Apache web server has loaded the mod_shib, you can restart the service with this command:

```
#root> service httpd restart
```

To verify that the mod_shib was loaded successfully, you can grep the listing of loaded apache modules with this command:

```
#root> apachectl –M | grep shib
```

A simple test to check that the overall configuration is executable and that the Apache is communicating with the shibboleth daemon, involves checking the status returned by this URL: https://localhost/Shibboleth.sso/Status

Please note that by default, the status URL can only be accessed from **localhost** as you can tell by the following configuration:

```
<Handler type="Status" Location="/Status" acl="127.0.0.1"/>
```

You may temporarily remove this section if you are not able to access the URL from localhost but this must be put back after testing.

If you do not have an X enabled session, you can either use the wget or curl command to execute the URL.

12 Firewall settings

This federation uses the SAML Artefact Binding for session initiation. This requires specific firewall related adjustments:

- inbound:

  - Apache web server: port 443 used by any browser-user (usually open already)
- outbound:
  - Shibboleth daemon (shibd): has to be able to connect to each remote IdP in the federation on port 8443 for attribute fetching. (n.b. This may already be enabled)
  - NTP: Port 123 to connect to remote ntp server (If this is not already configured)

13 References

- Apache HTTP OpenSSL included - Download:
  - *http://httpd.apache.org/download.cgi*
- Apache HTTP - General documentation:
  - *http://httpd.apache.org/docs/2.2/*
- Apache HTTP - SSL documentation:
  - *http://httpd.apache.org/docs/2.2/ssl/*
- Apache HTTP - Authentication, Authorization and Access Control documentation:
  - *http://httpd.apache.org/docs/2.2/howto/auth.html*