ISA Action 1.17: A Reusable INSPIRE Reference Platform

(ARE3NA)

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

D3.3b – Deployment of a Shibboleth Identity 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 Data and Services in EU Public Administrations D3.3b – Deployment of a Shibboleth Identity Provider. European Commission; 2015. JRC98194

Table of Contents

Glossary 3

1 Introduction 5

2 Resources and Prerequisites 6

3 Installation of the Shibboleth IdP 6

4 SSL certificates & Apache configuration 7

5 Tomcat Configuration 8

6 Configuration of the Shibboleth IdP (intranet case) 9

1.1 relying-party.xml 9

7 Configuration of the Shibboleth IdP (federated case) 9

2.1 relying-party.xml 9

3.1 attribute-resolver.xml 10

4.1 attribute-filter.xml 12

8 Metadata Adaption 14

5.1 IdP Display Name and Logo 14

6.1 Company and Contact Information 14

9 Removal of SAML1 Support 15

7.1 Remove SAML1 Handler 15

8.1 Remove SAML1 Handler Exposure 15

9.1 Remove SAML1 Handler from Metadata 16

10 Run & Test 16

11 Installation and Configuration of uApprove 17

12 Firewall settings 17

13 References 17

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 *"D3.3b – Deployment of a Shibboleth Identity 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 Identity Provider (IdP), alongside other documents covering setup for a Service Providers (SP, who provides access to data) and a Coordination Centre (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 IdP setup (Section 2). This is followed by a section explaining how to install the Shibboleth IdP (Section 3), SSL certificates & Apache configuration (Section 4) and Tomcat Configuration (Section 5). The document also contains a description of configuration of the Shibboleth IdP in the intranet (Section 6) and federated (Section 7) cases before outlining 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, exposure configuration (including from metadata; Section 9). The document closes with a description of the run and test settings (Section 10), the installation and configuration of the uApprove for privacy settings (Section 11) and firewall settings (Section 12).

2 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 Identity Provider (SP) 2.4 is implemented in Java and get deployed as a Java application on Apache Tomcat using the file idp.war.

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.
- Java 1.6 or 1.7 is installed
- Apache Tomcat 6 is installed
- Network Time Protocol (NTP) is installed and activated on the server (ntpd deamon running). Servers running Shibboleth must have their system time synchronized in order to avoid clock-skew errors.

3 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

After the initial installation of the IdP software, the following steps are required:

- load SAML metadata (for intranet configuration, this is your local SP, see next)
- configure an authentication mechanism

For a typical LDAP based authentication, 2 files should be modified in the configuration folder `/opt/shibboleth-idp/conf.`

In the file `login.conf`, the following should be added:

```
edu.vt.middleware.ldap.jaas.LdapLoginModule required
      ldapUrl="ldap://localhost"
      baseDn="<your base DN for users>"
      ssl="false"
      userFilter="uid={0}";
```

In the file `handler.xml`, put `RemoteUser` in comments and uncomment `UserNamePassword`:

```
<ph:LoginHandler xsi:type="ph:UsernamePassword"
                 jaasConfigurationLocation="file:///opt/shibbo-
leth-idp/conf/login.config">

<ph:AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:classes:Password-
ProtectedTransport</ph:AuthenticationMethod>

</ph:LoginHandler>
```

4 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 SP 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**.

If the certificate is not a wildcard, a specific subdomain like IdP should be prepended to the domain name: **idp.$DOMAIN**. Another subdomain may be chosen, but IdP will be suggested by default by the installation script.

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
```

For the ARE3NA AAA Federation, Artefact Binding must be supported. This requires that the IdP provides a so called secure Back-Channel to all other SPs. The standard deployment of the Shibboleth IdP uses port 8443 for this.

Based on the standard IdP deployment, the same key for SAML signatures and port 8443 SSL communication is used. However, it is possible to use the same private key used in Section 4 for port 443 SSL communications. Depending upon the configuration, it is important to make sure that Apache picks up the correct key for the HTTPS communication of port 443 and 8443. A typical virtual host configuration section may look like this (this configuration uses IP virtual hosting):

```
(ssl-geosparcidp443.conf)
Listen 188.121.63.200:443
<VirtualHost 188.121.63.200:443>
DocumentRoot "/var/www/idp"
ServerName geosparcidp.com:443
SSLCertificateFile /etc/pki/tls/certs/geosparcidp.crt
SSLCertificateKeyFile /etc/pki/tls/private/geosparcidp.key
SSLCertificateChainFile /etc/pki/tls/certs/geosparcidp-bundle.crt

(ssl-geosparcidp8443.conf)
Listen 188.121.63.200:8443
<VirtualHost 188.121.63.200:8443>
DocumentRoot "/var/www/idp"
ServerName geosparcidp.com:8443
SSLCertificateFile /opt/shibboleth-idp/credentials/idp.crt
SSLCertificateKeyFile /opt/shibboleth-idp/credentials/idp.key
```

In order to connect Apache to the IdP software hosted on Tomcat, please add the following configuration to the configuration for both port 443 and 8443:

```
ProxyPass /idp ajp://localhost:8009/idp
```

The following example illustrates the configuration for port 8443 to protect the ECP endpoint (it uses the HTTP BASIC login which needs to be changed to LDAP):

```
<Location "/idp/profile/SAML2/SOAP/ECP">
    Order allow,deny
    Allow from all

    AuthType Basic
    AuthName "Secure Dimensions Identity Provider Authentication"
    AuthUserFile /etc/httpd/conf.d/user-passwords
    Require valid-user
</Location>
```

It is important to note that IdP and SP domain names should be bound to a different IP address. They can both be hosted on the same machine by giving the machine multiple IP addresses and using IP virtual hosting in the Apache configuration.

5 Tomcat Configuration

For security reasons, it is not recommended to make any Tomcat endpoints directly accessible to the Internet. Instead, Apache should be used to reverse proxy the IdP endpoints hosted on Tomcat.

As Tomcat is not operating as standalone, it is recommended to deactivate the standard connector on port 8080. In the /etc/tomcat6/server.xml file please comment the following connector, as outlined below:

```
<!--
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
-->
```

The ECP SOAP endpoint of the IdP must be protected using HTTP BASIC Authentication. This must be achieved in the Apache configuration. It is important to note that the Tomcat AJP connector for port 8009 must be configured to accept the Apache authentication. Please make sure the 8009 connector looks like the example below:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
           tomcatAuthentication="false"/>
```

Finally, it is good practice to run the Tomcat as a non-privileged user, e.g. tomcat6. Please make sure that your configuration of Tomcat reflects this.

The IdP war can be deployed as described in the Shibboleth documentation by putting a context file in the **<TOMCAT_HOME>/Catalina/localhost** folder. Add **auto-deploy=false** to this context if you want to avoid that Tomcat removes this file when the idp.war is removed:

```
<Context docBase="/opt/shibboleth-idp/war/idp.war"
         privileged="true"
         autoDeploy="false"
         antiResourceLocking="false"
         antiJARLocking="false"
         unpackWAR="false"
         swallowOutput="true" />
```

The consequence of this setup is that the idp.war is not unpacked. Any changes to it have to be done by either changing the source code in the idp war configuration directory **<IDP_INSTALL_HOME>/src/main/webapp** and calling install.sh again (choose the option to preserve the existing configuration, make a backup of **/opt/shibboleth-idp** to be sure) or by setting **unpackWAR** to true and make the changes in-place (the unpack will happen in the webapps directory of Tomcat).

6 Configuration of the Shibboleth IdP (intranet case)

This section covers the specific configuration of the Shibboleth IdP for the intranet case.

1.1 relying-party.xml

In the configuration folder, make a file system reference to your local SP metadata:

```
<metadata:MetadataProvider id="SPMD"
    xsi:type="metadata:FilesystemMetadataProvider"
    metadataFile="/opt/shibboleth-idp/metadata/sp-metadata.xml"
    maxRefreshDelay="P1D" />
```

We refer to the SP configuration for establishing the SP metadata. The metadata can typically be downloaded from the following exposure URL: https://$SP_HOSTNAME/Shibboleth.sso/Metadata

7 Configuration of the Shibboleth IdP (federated case)

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

2.1 relying-party.xml

The IdP must load the federation metadata from a HTTP URL and verify the digital signature on it.

In order to achieve the loading of the metadata, please use the following snippet for configuration of the **MetadataProvider**:

```
<metadata:MetadataProvider id="URLMD" xsi:type="metadata:FileBackedHTTPMetadataProvider"
    metadataURL="http://www.aaa.secure-dimensions.de/metadata/aaa-metadata.xml"
    backingFile="/opt/shibboleth-idp/metadata/aaa-metadata.xml">
    <metadata:MetadataFilter xsi:type="metadata:ChainingFilter">
        <metadata:MetadataFilter xsi:type="metadata:RequiredValidUntil"
            maxValidityInterval="P7D" />
        <metadata:MetadataFilter xsi:type="metadata:SignatureValidation"
            trustEngineRef="shibboleth.MetadataTrustEngine"
            requireSignedMetadata="true" />
        <metadata:MetadataFilter xsi:type="metadata:EntityRoleWhiteList">
            <metadata:RetainedRole>samlmd:SPSSODescriptor</metadata:RetainedRole>
        </metadata:MetadataFilter>
    </metadata:MetadataFilter>
</metadata:MetadataProvider>
```

In order to achieve the verification of the metadata, please use the following snippet for configuration of the **MetadataProvider**:

```
<security:TrustEngine id="shibboleth.MetadataTrustEngine" xsi:type="security:StaticExplicitKeySignature">
    <security:Credential id="AAAFederationCredentials" xsi:type="security:X509Filesystem">
        <security:Certificate>/opt/shibboleth-idp/credentials/AAA.pem</security:Certificate>
    </security:Credential>
</security:TrustEngine>
```

The **AAA.pem** file can be obtained via this URL:

https://www.aaa.secure-dimensions.de/metadata/AAA.pem

Please make sure that the backup file (aaa-metadata.xml) has write permission for the user running the IdP. This is typically the Operating System user that starts the Apache Tomcat. As an example, use the following commands (assuming that Tomcat is started by user “tomcat” and the IdP installation is in **/opt/shibboleth-idp**):

```
#root> cd /opt/shibboleth-idp/metadata
#root> touch aaa-metadata.xml
#root> chown tomcat aaa-metadata.xml
#root> chgrp tomcat aaa-metadata.xml
```

3.1 attribute-resolver.xml

Attributes released by the IdP have to be mapped from the domain specific names to a standard “wire[1]” naming convention. This is configured in the file **attribute-resolver.xml**.

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

Unlike for SPs, this mapping is domain specific and, therefore, no common mapping can be provided for the ARE3NA AAA Federation. As the concrete set of attributes is still a topic for discussion, it is a good start to enable a set of common ones:

transientId	= urn:oasis:names:tc:SAML:2.0:nameid-format:transient
eduPersonScopedAffiliation	= urn:oid:1.3.6.1.4.1.5923.1.1.1.9
eduPersonAffiliation	= urn:oid:1.3.6.1.4.1.5923.1.1.1.1
organizationName	= urn:oid:2.5.4.10
persistentid	= persistentId
uniqueID	= uniqueID
givenName	= urn:oid:2.5.4.42
surname	= urn:oid:2.5.4.4

A complete LDAP-based configuration may look as follows:

```
<resolver:AttributeDefinition id="transientId" xsi:type="ad:TransientId">
         <resolver:AttributeEncoder xsi:type="enc:SAML2StringNameID" nameFor-
mat="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
    </resolver:AttributeDefinition>

    <resolver:AttributeDefinition xsi:type="ad:Scoped" id="eduPer-
sonScopedAffiliation" scope="geosparcidp.com" sourceAttributeID="eduPerso-
nAffiliation">
        <resolver:Dependency ref="staticAttributes" />
         <resolver:AttributeEncoder xsi:type="enc:SAML2ScopedString"
name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" friendlyName="eduPersonScopedAffilia-
tion" />
    </resolver:AttributeDefinition>

     <resolver:AttributeDefinition xsi:type="ad:Simple" id="eduPersonAffilia-
tion" sourceAttributeID="eduPersonAffiliation">
        <resolver:Dependency ref="staticAttributes" />
        <resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" friendlyName="eduPersonAffiliation" />
    </resolver:AttributeDefinition>

    <resolver:AttributeDefinition xsi:type="ad:Simple" id="organizationName"
sourceAttributeID="o">
        <resolver:Dependency ref="myLDAP" />
         <resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:2.5.4.10" friendlyName="o" />
    </resolver:AttributeDefinition>

    <resolver:AttributeDefinition xsi:type="ad:Simple"  id="persistentId"
sourceAttributeID="computedID">
        <resolver:Dependency ref="computedID"/>
      <resolver:AttributeEncoder xsi:type="enc:SAML2StringNameID" nameFor-
mat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"/>
 </resolver:AttributeDefinition>

    <resolver:AttributeDefinition xsi:type="ad:Simple" id="uniqueID" sourceAt-
tributeID="uid">
        <resolver:Dependency ref="myLDAP" />
      <resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:0.9.2342.19200300.100.1.1" friendlyName="uniqueID" />
    </resolver:AttributeDefinition>
    <resolver:AttributeDefinition xsi:type="ad:Simple" id="givenName"
sourceAttributeID="givenName">
        <resolver:Dependency ref="myLDAP" />
        <resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:2.5.4.42" friendlyName="givenName" />
    </resolver:AttributeDefinition>

    <resolver:AttributeDefinition xsi:type="ad:Simple" id="surname" sourceAt-
tributeID="sn">
        <resolver:Dependency ref="myLDAP" />
        <resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:2.5.4.4" friendlyName="sn" />
    </resolver:AttributeDefinition>

    <resolver:DataConnector id="myLDAP" xsi:type="dc:LDAPDirectory"
        ldapURL="ldap://localhost"
        baseDN="ou=Users,dc=geosparc,dc=com"
        principal="cn=shibboleth,ou=system,dc=geosparc,dc=com"
        principalCredential="*******">
        <dc:FilterTemplate>
            <![CDATA[
                (uid=$requestContext.principalName)
            ]]>
        </dc:FilterTemplate>
    </resolver:DataConnector>
   <resolver:DataConnector id="staticAttributes" xsi:type="dc:Static">
        <dc:Attribute id="eduPersonAffiliation">
            <dc:Value>member</dc:Value>
        </dc:Attribute>
        <dc:Attribute id="eduPersonEntitlement">
            <dc:Value>urn:example.org:entitlement:entitlement1</dc:Value>
            <dc:Value>urn:mace:dir:entitlement:common-lib-terms</dc:Value>
        </dc:Attribute>
    </resolver:DataConnector>

    <resolver:DataConnector xsi:type="dc:ComputedId"
                            id="computedID"
                            generatedAttributeID="computedID"
                            sourceAttributeID="uid"
                            salt="***********">
        <resolver:Dependency ref="myLDAP" />
    </resolver:DataConnector>
```

4.1 attribute-filter.xml

The attribute-filter.xml file describes rules to filter release of attributes. For this federation we use a simple "release to all" policy:

```
<afp:AttributeFilterPolicy id="releaseToAnyone">
    <afp:PolicyRequirementRule xsi:type="basic:ANY"/>

    <afp:AttributeRule attributeID="transientId">
        <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>

    <afp:AttributeRule attributeID="eduPersonScopedAffiliation">
```

```
        <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>

    <afp:AttributeRule attributeID="eduPersonAffiliation">
        <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>

    <afp:AttributeRule attributeID="organizationName">
        <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>

    <afp:AttributeRule attributeID="persistentId">
        <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>

    <afp:AttributeRule attributeID="uniqueID">
        <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>

    <afp:AttributeRule attributeID="givenName">
        <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>

    <afp:AttributeRule attributeID="surname">
        <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>

</afp:AttributeFilterPolicy>
```

8 Metadata Adaption

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

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

5.1 IdP Display Name and Logo

The Discovery Service (DS) provides a list of possible IdPs to the user for selecting the home organization’s IdP. The name to use for this display is taken from the IdP Metadata. In case no display name is provided, the DS must use the IdP identifier as included in the metadata.

For completeness, a logo URL for an organization can be added. Please make sure that you use the http**s** scheme!

At the top, please find the `<Extensions>` element and add the `<mdui:UIInfo>` element as illustrated below in bold. The `<shibmd:Scope>` element is already generated **=> Do not change it!**

Please add the following XML snippet to the IdP Metadata, located in **idp-metadata.xml**

```
<Extensions>
    <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
        <mdui:DisplayName xml:lang="en">The Name of YOUR IdP - e.g. Geosparc IdP</mdui:DisplayName>
        <mdui:Logo height="45" width="99">https://geosparcidp.com/images/logo.jpg</mdui:Logo>
    </mdui:UIInfo>
    <shibmd:Scope regexp="false">DONT CHANGE THIS</shibmd:Scope>
</Extensions>
```

6.1 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>
```

9 Removal of SAML1 Support

For the ARE3NA AAA 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.

7.1 Remove SAML1 Handler

The handler configuration can be found in the **handler.xml** document. Removal of SAML1 support can be achieved by commenting the lines as illustrated below.

```
<ph:ProfileHandler xsi:type="ph:ShibbolethSSO" inboundBinding="urn:mace:shib-
boleth:1.0:profiles:AuthnRequest"
outboundBindingEnumeration="urn:oasis:names:tc:SAML:1.0:profiles:browser-post
urn:oasis:names:tc:SAML:1.0:profiles:artifact-01">
<ph:RequestPath>/Shibboleth/SSO</ph:RequestPath>
</ph:ProfileHandler>

<ph:ProfileHandler xsi:type="ph:SAML1AttributeQuery" inboundBinding="urn:oa-
sis:names:tc:SAML:1.0:bindings:SOAP-binding"
outboundBindingEnumeration="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-bind-
ing">
<ph:RequestPath>/SAML1/SOAP/AttributeQuery</ph:RequestPath>
</ph:ProfileHandler>

<ph:ProfileHandler xsi:type="ph:SAML1ArtifactResolution" inboundBind-
ing="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
outboundBindingEnumeration="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-bind-
ing">
<ph:RequestPath>/SAML1/SOAP/ArtifactResolution</ph:RequestPath>
</ph:ProfileHandler>
```

8.1 Remove SAML1 Handler Exposure

The handler exposure configuration can be found in the **relying-party.xml** document. Removal of SAML1 support can be achieved by commenting the lines as illustrated below.

```
<!--
<rp:ProfileConfiguration xsi:type="saml:ShibbolethSSOProfile" includeAttrib-
uteStatement="false"
    assertionLifetime="PT5M" signResponses="conditional" signAsser-
tions="never"
    includeConditionsNotBefore="true"/>

<rp:ProfileConfiguration xsi:type="saml:SAML1AttributeQueryProfile" asser-
tionLifetime="PT5M"
    signResponses="conditional" signAssertions="never"
    includeConditionsNotBefore="true"/>

<rp:ProfileConfiguration xsi:type="saml:SAML1ArtifactResolutionProfile" sign-
Responses="conditional"
    signAssertions="never"/>
-->
```

9.1 Remove SAML1 Handler from Metadata

The exposed URL endpoints can be found in the **idp-metadata.xml** document. Removal of SAML1 URLs can be achieved by commenting the lines, as illustrated below.

```
<!--ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bind-
ings:SOAP-binding" Location="https://idp.aaa.secure-dimen-
sions.de:8443/idp/profile/SAML1/SOAP/ArtifactResolution" index="1"/-->

</IDPSSODescriptor>
...
<!--NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat-->
...
</IDPSSODescriptor>

<!--SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRe-
quest" Location="https://idp.aaa.secure-dimensions.de/idp/profile/Shibbo-
leth/SSO"/-->

<!--AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-bind-
ing" Location="https://idp.aaa.secure-dimensions.de:8443/idp/pro-
file/SAML1/SOAP/AttributeQuery"/-->

<AttributeAuthorityDescriptor>
...
<!--NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat-->
...
</AttributeAuthorityDescriptor>
```

Removal of SAML1 protocol support can be achieved by removing the attribute from the `<AttributeAuthorityDescriptor>` element:

```
<AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oa-
sis:names:tc:SAML:2.0:protocol">
```

10 Run & Test

You can test the configuration by entering the following command:

```
#root> wget https://$HOSTNAME/idp/profile/Status
```

The configuration is acceptable if the output is

```
OK
```

You can now start/stop/restart the Shibboleth IdP via Tomcat using the following commands:

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

Your metadata should be visible here:

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

For a full test including the SP, make sure your SP is correctly configured first (starting with the intranet configuration).

11 Installation and Configuration of uApprove

Although outside the scope of the project, it is useful to demonstrate compliance to privacy regulations. It is likely that many IdPs that releases personal attributes may only do so after user approval. One option to do so is to deploy the uApproave module on top of the Shibboleth IdP.

Please follow the instructions for installing and configuring uApprove from: http://www.switch.ch/aai/support/tools/uApprove.html

12 Firewall settings

The ARE3NA AAA federation uses SAML Artefact Binding for session initiation. This requires specific firewall related adjustments:

- inbound:
  - Apache web server: port 8443 used all SPs
- outbound:
  - NTP: Port 123 to connect to the remote ntp server (in case 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*