ISA Action 1.17: A Reusable INSPIRE Reference Platform

(ARE3NA)

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

D4.1.5 – Final technical report

Danny Vandenbroucke

Andreas Matheus

Dirk Frigne

Pieter De Graef

Reijer Copier

Robin S. Smith

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 Danny Vandenbroucke, Andreas Matheus, Dirk Frigne, Pieter De Graef and Reijer Copier in collaboration with Robin S. Smith and Michael Lutz from the EC Joint Research Centre.

Disclaimer

Copyright notice

Bibliographic Information:

Vandenbroucke D, Matheus A, Frigne D, De Graef P, Copier R, Smith RS. Authentication, Authorization and Accounting for Data and Services in EU Public Administrations D4.1.5 – Final technical report. European Commission; 2015. JRC98201

Executive Summary

This final report describes the results of the study 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. The focus was on lowering e-barriers in Europe and in particular accessibility of protected data from the download- and view-services being deployed for the INSPIRE Directive (2007/2/EC). The report covers the whole study, including several aspects of a technical nature.

Key results of the study

- A concrete, well thought-through proposal for standards, software and technology to be used for AAA, including an Open Source software stack;
- A testbed demonstrating the proposed standards, software and technologies by means of several use-cases including a cross-border use-case;
- Comprehensive documentation on the set-up of the AAA testbed.

Key lessons learnt

- AAA mechanism is best facilitated by means of a European Access Management Federation (AMF) instead of a centralised access control approach. This implies single sign-on and the possibility to control access based on not only identity but also certain attributes of a user and even controlled access to selections of data for certain user-groups.
- Consensus seems to exist on which standards need to be used. For Authentication the widely accepted standard is SAML. For Authorisation there is consensus on the use of XACML as well as GeoXACML for cases where spatial criteria are important.
- For all components Open Source software was available except for the tool to work with GeoXACML. This can be well tackled by establishing a separate open source project to realise and promote the missing component.
- The selected standards and technology appear to be “open” for re-use;
- Existing security infrastructure of organisations can be integrated;
- The AAA mechanism is suitable for web-clients and desktop applications. For the latter an additional modification can be implemented;
- A coordination centre plays a pivotal role. The coordination centre needs to define attributes, roles and rules and to set up agreements with the participating organisations of the federation.

Expectations

- Organisations are more eager to provide access to their resources if the access is controlled and managed by the AAA solution. This sharing may lead to improved data quality and services. More users with different expectations and needs accessing INSPIRE data and services trigger organisations to meet higher service levels (metadata, availability, performance, inter-operability, etc.).
- To have a fully formed federation, decision-makers need to be made aware of the limitations of the current data access situation and the possibilities offered by being part of a federation. Involvement can be organic, as new organizations can join the federation over time. As a result, a potentially vast amount of data, services and applications can be made available in a controlled, secure and convenient way for a range of users, from the general public to professionals at local, cross-border and European levels.
- AAA solutions may not be needed in all cases for accessing INSPIRE services and Open Data approaches should be encouraged. Further discussion with INSPIRE stakeholders is needed to decide if an AMF approach will be the best solution for all partners.

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
CERN	European Organization for Nuclear Research
COBWEB	Citizen OBservatory WEB
COTS	Commercial Off-The-Shelf Software
DARIAH	DigitAl Research Infrastructure for the Arts and Humanities
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
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
OASIS	Advancing Open Standards for the Information Society

OGC	Open Geospatial Consortium
OSS	Open Source Software
PAOS	Reverse SOAP binding
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
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
WAYF	Where Are You From
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
XRI	Extensible Resource Identifier

1 Introduction

This final report contains the summary of the main achievements and results, the key lessons and the recommendations formulated in the context 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 (JRC; Contract n°389834). The project is part of A Reusable INSPIRE Reference Platform (ARE3NA) Action 1.17 of the EU's ISA Programme. The general objective of the project is to assist the JRC in carrying out a study, conducting a workshop and the setting-up of a 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.

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

- 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.
- 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.
- 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 and technical settings.
- To involve actively Member State representatives on the proposed AAA-architecture and testbed to collect feedback from them.

All relevant outputs have been made available in a dedicated space on the ISA Programme's JoinUp platform[1].

1.1 Initial Evidence Gathering

1.1.1 Reviewing Access Standards and Technologies

The analysis of the standards and study of the technologies used for AAA are described in the deliverable "D1.1.2 & D1.2.2 – Analysing standards and technologies for AAA"[2].

During the initial phase of the project, the state-of-play of standards and technologies to support secure data exchange between public administrations was documented.

The evidence gathering is based on:

- assessment of documents and online resources describing AAA implementations and the standards & technologies they are built upon,
- input from experts (also through interviews) active in the field of AAA,
- input from discussions during the workshop on AAA solutions for INSPIRE held in Leuven in March 2014 (organised by ARE3NA),
- input from discussions during a similar workshop organised in Brussels in April 2014 (organised by GÉANT[3]) focusing on the research and academic sector.

[1] https://joinup.ec.europa.eu/asset/are3na-aaa/home

[2] https://joinup.ec.europa.eu/asset/are3na-aaa/document/analysing-standards-and-technologies-authentication-authorization-accounti

[3] http://www.geant.net/

Since the access to spatial datasets and their metadata is organized through a Service Oriented Architecture (SOA), the main focus for the study and the testbed was on the architecture. Although the aim of INSPIRE is to make as much of the existing datasets available for sharing and reuse, there might be some situations where public access to the services needs to be restricted.

Access to discovery services can only be restricted when *"such access would adversely affect international relations, public security or national defence" (Directive 2007/2/EC Art.13)*. Access to the other type of network services and the corresponding spatial data can, in addition to the already mentioned reasons for discovery services, be limited for various other reasons, *e.g.* to protect personal data, for IPR reasons, or to protect rare species/habitats. However such limitations *"shall be interpreted in a restrictive way"* and *"the public interest served by disclosure shall be weighed against the interest served by limiting or conditioning the access" (Directive 2007/2/EC Art.13)*.

The study has revealed that even when public access to services does not need to be restricted, an AAA framework can still provide benefits by controlling and monitoring the use of the service.

Another lesson learned is that INSPIRE developments build further on generic ICT standards and technologies. This is not different for AAA implementations.

ARE3NA aims to identify what components are missing from the functioning of a European SDI and develop reusable mainly open source solutions to support INSPIRE implementation in the EU Member States, as well as encouraging their reuse in other sectors beyond the environment. This project aims to contribute to ARE3NA by providing evidence, practical experience and reusable solutions that support access control to INSPIRE data and services, while drawing on best practices from other sectors.

As we will describe further in this report, the testbed is an implementation based on open standards and open source components available on the market. Only for the spatial extension of the XACML standard (GeoXACML) we did not find an open-source initiative and used a closed source implementation of the open standard.

Terminology is important in this context and the definitions used in the scope of this project are taken from the OGC Geospatial Digital Rights Management Reference Model[4]:

- **Access control** – a combination of authentication and authorisation.
- **Authentication** – verification that a potential partner in a conversation is capable of representing a person or organisation.
- **Authorisation** – determination whether a subject is allowed to have the specified type of access to a particular resource. Usually, authorisation is applied in the context of authentication. Once a subject is authenticated, it may be authorised to perform different types of access.
- **Accounting or rights management** – tracking and controlling the use of content, rights, licences and associated information.

For establishing access control across public authorities in Europe participating in INSPIRE, this work proposes **federated authentication and local authorization**, also referred to as an Access Management Federation (AMF).

[4] GeoDRM RM (http://www.opengeospatial.org/standards/as/geodrmrm)

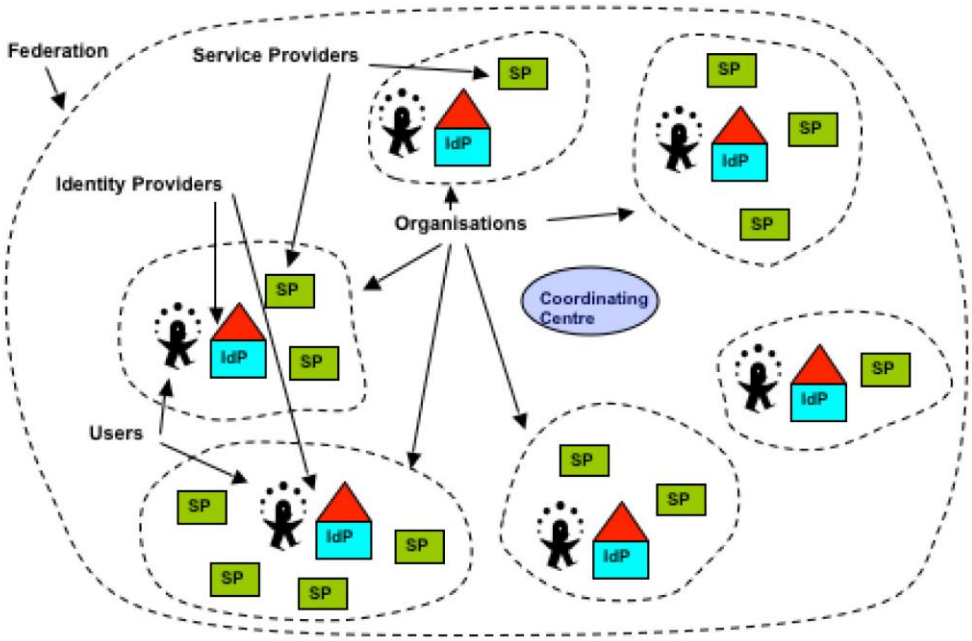

Figure 1: Access Management Federation

All these federations are using the same setup, as illustrated in Figure 1:

- **Service Providers** (SP) host protected resources that can be used by authenticated and authorized users of the federation.
- **Identity Providers** (IdP) provide the login and the authentication of organizational user accounts.
- A **Coordination Centre** (CC) controls the technical compliance with policies and procedures of the federation and thereby establishes the trust between members of the federation.

Member organisations participating in a federation operate IdPs for their users and any number of SPs to expose their protected resources. An organization can join the federation by applying to the coordination centre as a SP, an IdP or both.

The coordination centre evaluates the organisation's application and can accept it as a trusted party by checking technical compliance according to the policies and procedures of the federation. These policies and rules are defined by the federation and, therefore, can vary. Usually, they include some general rules applicable to all members and more specific rules that apply to IdPs and SPs. After being evaluated successfully, the CC will add the organization's credentials to the federation metadata, allowing the organization to interact with services within the federation. This architecture supports also the concept of **Single Sign-On (SSO).**

During the project's analysis phase, several AAA related standards were studied. The most relevant are represented in Figure 2. From this scheme, it becomes clear that several standards exist which can be used for an AAA implementation for INSPIRE. It also shows that the only extension to support geographical data is an extension on XACML – the OGC standard GeoXACML.

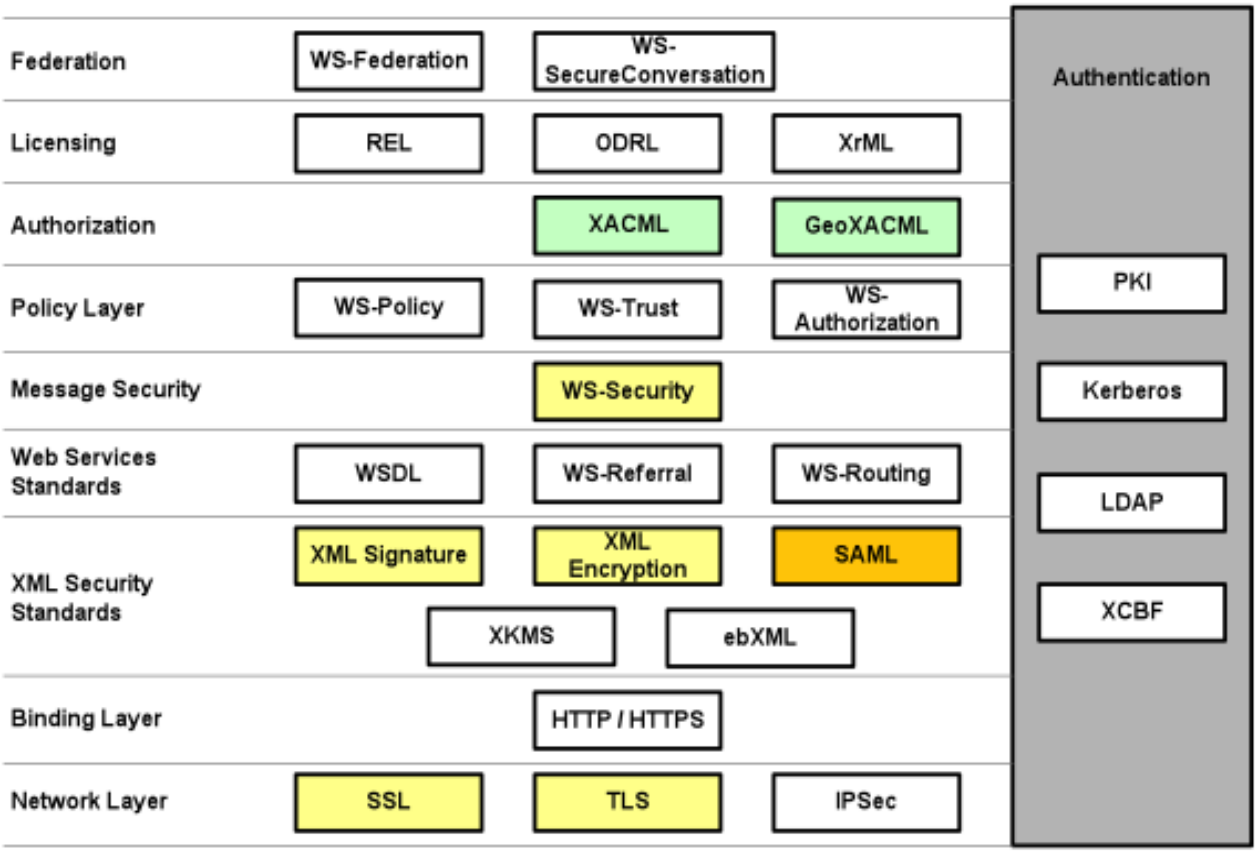

Figure 2: Schematic overview of AAA and related standards

Several tools and technologies exist to implement AAA standards, both open source as well as closed source solutions. A total of 65 products are documented during the analysis of technologies for AAA. The inventory is based on an initial assessment done by the Kantara Initiative[5] and was updated to reflect the current status and enhanced with additional information during this project.

Shibboleth is one of the most popular open source environments to implement and manage federations. Shibboleth creates an architecture and open-source implementation for identity management and federated identity-based access control based on SAML. The consortium chose Shibboleth for the testbed federation because it is an open-source solution that is widely accepted and used. Moreover, several AAA implementations in the context of SDIs and INSPIRE have used Shibboleth before (e.g. Persistent TestBed (PTB) initiative of AGILE-OGC-EuroSDR).

The operational impact of running an AMF with a single Coordination Centre for INSPIRE services is an important aspect that needs to be covered in any AAA setup. The amount of SPs in the federation is estimated at approximately 2000. Compared to other operational federations using Shibboleth, we do not expect major issues in terms of stability or performance.

This project has many potential links with other actions of the ISA programme. From the study, the relation with the ECAS-STORK project, Action 1.4 is clear, as well as with ISA action 1.18, Federated Authorization Across European Public Administrations.

1.1.2 Best practices across public administrations and themes

Key services and data-sharing activities in Europe that can be considered best practices regarding AAA implementations were studied and documented in *"D1.3 – Best Practices of AAA implementations"*[6].

The focus is on secure access to services across Europe, including the relevant technologies and standards being used, as well as the organizational conditions that can facilitate the successful set-up of such access mechanism.

1.1.2.1 Methodology

The selection of Best Practices is based on the experience and knowledge of consortium members in national and European projects and the INSPIRE Maintenance Group (MIG).

The Best Practices were collected based on a template covering following aspects:

- An abstract summarizing the project in which AAA mechanisms were implemented including what has been done, how it was done and who was involved;
- Standards and technologies applied in the project including authentication, authorization and XML security standards, and technologies/tools used. The template included some commonly used standards, but left also room to indicate other standards and technologies.
- Organizational set-up, including a list of participating organisations as SPs or IdPs, involvement of other organisations. Specific organisational or legal measures taken to support the AAA implementation could be listed as well.
- A list of technological and non-technological issues encountered during the project and corrective actions taken to resolve them. Open issues that need particular attention could also be listed.

In total, 8 practices from 7 Member States were selected and analysed. The information was collected in different ways. First, the consortium partners filled the template for the projects in which they were involved themselves, if necessary with the help of the participating organisations. Second, documents and online information was consulted to complete or describe some of the practices centrally. Third, additional information was gathered during the workshop that took place in Leuven from 17 to 18 March 2014. The workshop was also used to validate the Best Practices descriptions.

1.1.2.2 Inventory and analysis

The different best practices were described individually and compared according to key characteristics. This comparison is summarized in the Table 1 below.

[6] *https://joinup.ec.europa.eu/asset/are3na-aaa/document/best-practices-aaa-implementations*

Table 1: Comparison of the Best Practices from the technological point of view

	Standards							Tools		Applications & services		
Bast Practice	**HTTP/HTTPS**	**WS-S**	**LDAP**	**SAML**	**OpenID**	**OAuth**	**GeoXACML**	**Shibboleth**	**Other**	**Clients**	**WMS**	**WFS**
AT - AAA in e-Government	✓	✓		✓	P					Web shop		✓
BE - LNE-ADC Flanders			✓	✓		✓				Several		
DE - GDI-DE	✓	✓	✓	✓			✓	✓		Openlayers, QGIS	✓	✓
DE - GDI-DE INSPIRE testsuite	✓	✓	✓	✓			✓	✓		INSPIRE testsuite	✓	✓
FR - Geoportal IGN	Not standards based											
NL - Province of Limburg	✓	✓							Spring Security	Web client, ArcGIS	✓	✓
PL - Polish Geoportal	✓	✓								Open Layers		
UK - OWS Interoperability Experiments	✓	✓	✓	✓	✓		✓	✓		Several GIS	✓	✓

1.1.2.3 Observations and conclusions

From the table and the description of the best practice cases we can make these main observations and conclusions:

1. The objectives to set-up an AMF are different for some of the projects. Some want to provide secure access to (OGC) web services (Access Control). Other projects want to better understand who is using their data (Accounting).
2. In several of the projects different types of clients were used to access secured services (mobile, web GIS or desktop). Desktop applications will need to be customized (or workarounds need to be found) in order to guarantee successful access. This should be done by the software vendors/providers.
3. The OGC web services covered in the different projects are WMS and WFS.
4. Almost all projects use basic security standards such as HTTPS and WS-S and most use SAML. Shibboleth is used in three cases as the tool to implement SAML based AMF. LDAP is frequently used to store user information.
5. Implementing an AAA layer to guarantee secure access is a complex process and requires dedicated IT security experts to be involved throughout the process.
6. AAA architectures, with many levels of authority, and many partners, require the set-up of a Coordinating Centre to manage the federation. To streamline the cooperation between the different stakeholders it is also recommended to have clear agreements on the roles and tasks in the federation.
7. It is necessary that the geospatial sector players that want to implement an AAA architecture to grant secure access to OGC Web Services (OWS) need to cooperate closely with the specific agencies or bodies that are responsible for ICT (security) and that deal with, for instance, eIDs and STORK implementation.
8. To simplify an AAA implementation and to comply with EU and national privacy rules, it is necessary to minimize the attributes to be exchanged between SP and IdP.

1.2 Analysis and review of the evidence base

Following the initial evidence gathering, an analysis and review of the data was performed. To support this exercise, a SWOT analysis was carried out and a workshop was organised in order to present and discuss the findings.

1.2.1 Analysis of the evidence base

The document *"D2.1 – Analysis of Evidence Base: Relationships and Gaps between Technologies, Standards and Best Practices"*[7] outlines the relationships and (possible) gaps between standards and technologies and the best practices. The analysis is based on the desktop study, and work with and input from AAA experts active in the field of e-Government and INSPIRE.

1.2.1.1 Lessons learned

From the analysis of the evidence base the following main observations and lessons learned were made:

- An Access Management Federation (AMF) seems the most obvious choice for setting up an AAA mechanism for INSPIRE
- Several IT security standards and technologies exist to build upon
- An AAA implementation should be as generic as possible
- Certain standards must be chosen, but this does not prevent combinations with other standards because many of them are interoperable
- The definition of attributes, roles and rules is key to any solution
- The establishment of a Coordination Centre is challenging, yet critical for the success of an EU-wide AAA mechanism for INSPIRE

1.2.1.2 Chosen standards and technology for AAA

The standards and technologies for secure access and exchange of information have been analysed and are described in detail in the documents "*D1.1.2 & D1.2.2 Analysing standards and technologies for AAA*", noted above. From the existing standards and technologies, the consortium proposed the following:

1) Authentication
    a. Standard: SAML
    b. Software: Shibboleth for IdP and SP
    c. Technology: Apache Web Server for SP and Apache/Tomcat for IdP; LDAP for the user repository
2) Authorization
    a. Standard: XACML, GeoXACML
    b. Software: SDInterceptor for realization of the Policy Enforcement Point; SDGeoPDP for realization of the Policy Decision Point
    c. Technology: Apache Web Server for SDInterceptor deployment; Apache/Tomcat for SDGeoPDP
3) Accounting
    a. Standard: n/a

[7] *https://joinup.ec.europa.eu/asset/are3na-aaa/document/analysis-evidence-base-relationships-and-gaps-between-technologies-standar*

b. Software: Web Server logging capabilities → Apache "CustomLog" directive

c. Technology: Apache Web Server

1.2.1.2.1 Standard for Authentication - SAML

To justify the choice for the proposed standard for Authentication a brief SWOT analysis of both SAML and OpenID was carried out (See Table 2 and Table 3).

Table 2: SWOT of the use of OpenID

	Helpful to achieve the objective	Harmful to achieve the objective
Internal factor	**Strengths** • Simple SSO. A user logs in once and gains access to all systems without being prompted to log in again at each of them)	**Weaknesses** • Missing a method to model trust between parties; user attributes should not be trusted • SSO not sufficient for OpenLayers based applications using protected services
External factor	**Opportunities** • Easy to integrate into Web-based offering • Self-organised (open) user registration	**Threats** • Phishing • Spoof of attributes, e.g. email address • Not a standard of an accredited standardisation body

Table 3: SWOT of the use of SAML

	Helpful to achieve the objective	Harmful to achieve the objective
Internal factor	**Strengths** • Model trust between participating parties using SAML metadata • Simple SSO • Scalability	**Weaknesses** • Complexity of the SAML protocol
External factor	**Opportunities** • Flexibility to support solutions in different environments • Many SAML implementations	**Threats** • Single Sign-out: it is not enough to log out from all the services. E.g., a mobile user needs to log out also from the application • Missing user education that SSO is in place and its implications

From the SWOT analysis, comparing the capabilities of OpenID and SAML, it can be concluded that an AMF should be based on SAML. There are three major reasons for this choice.

Firstly, it provides the ability to establish a white listing of trusted partners, the members of the federation. When using Shibboleth, the OSS implementing SAML, this feature is supported "out of the box". In an OpenID-based architecture a similar approach can be realised but will require additional efforts.

Secondly, the assurance of released attributes enables us to separate the authentication (to the IdP) and establish the authorization (to the SP). This important separation of concerns allows only one standard to be mandated to build the AMF: SAML. Which software / standard is selected at each SP must not be mandated – a recommendation, however, may help.

And thirdly, the support of automatic SSO, which is required to build applications such as web-mapping based on OpenLayers, can only be implemented using OpenID with limitations (such as the fact that the "return_to" URL, specified in the authentication request to an OpenID provider, has to be verified as a registered endpoint of the involved OpenID relying party's realm as stated in the OpenID Authentication specification, section 9.2.1.).

Moreover, the analysis of different practices from the geospatial, the e-Government and academic sectors has shown that SAML is increasingly being implemented and forms the backbone of many AAA. In that sense, there is a convergence towards the use of this core standard for secure access.

However, the authentication of users via OpenID is not excluded by choosing SAML as the core standard for authentication in an AMF. As successfully implemented in the COBWEB[8] federation and demonstrated during the GEOSS AIP-6 initiative[9], a so-called trust gateway from SAML to OpenID can be deployed.

[8] FP7 project *http://cobwebproject.eu*

[9] *http://www.ogcnetwork.net/pub/ogcnetwork/GEOSS/AIP6/documents/Summary/AIP-6_ER_summary.docx*

1.2.1.2.2 Standard for Authorisation – XACML and GeoXACML

The separation of concern for authentication and authorization also introduces the relationship between the SP and the IdPs: The SP is relying on the user information (attributes) released by any IdP to undertake authorization. There is no need to mandate a particular standard for the enforcement of access rights at the SP side, but the technology used should be able to support Attribute Based Access Control (ABAC), because the IdP is releasing user attributes. In addition, the use of request and environment information (attributes thereof) is also relevant when enforcing access rights.

The general purpose eXtensible Access Control Markup Language (XACML) from OASIS is recommend as the standard to be used. When access decisions based on geo-specific constraints are required, XACML is not sufficient. However, in this case, the geo-specific extension from OGC named GeoXACML is recommended to be used.

Figures 3 and 4 provide a schematic view for a 'simple' example of how access management would work and how the proposed standards support such implementations. An important principle is that authentication and authorisation are split between the IdPs (Authentication) and SPs (Authorisation). A trusted relationship is built between the asserting (IdP) and relying (SP) partner based on SAML metadata. SAML is also used to assert to the partner relying on the IdP that the persons wanting to access a resource are who they claim to be. The assertion about a user happens through the exchange of attribute information about the user. These attributes will, in turn, determine if the user receives access rights or not, and to which parts of the requested resource. This authorisation is done by using (Geo)XACML.

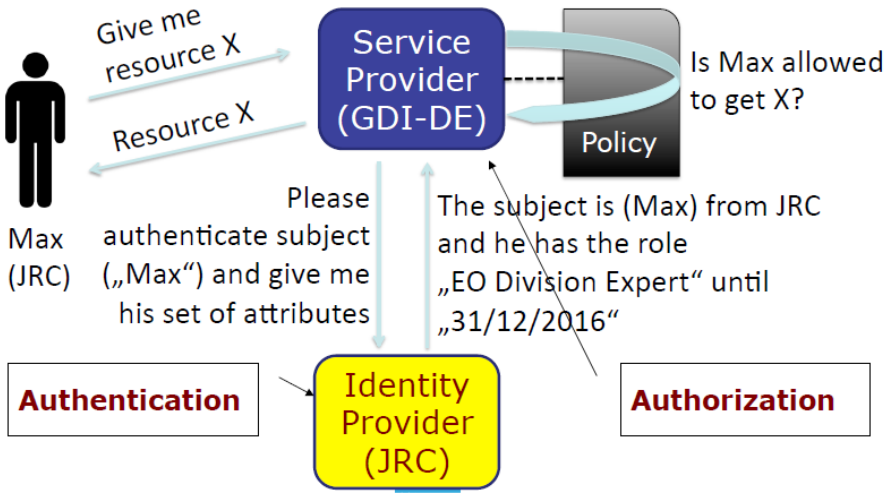

Figure 3: Example of Access Management with distribution of duties

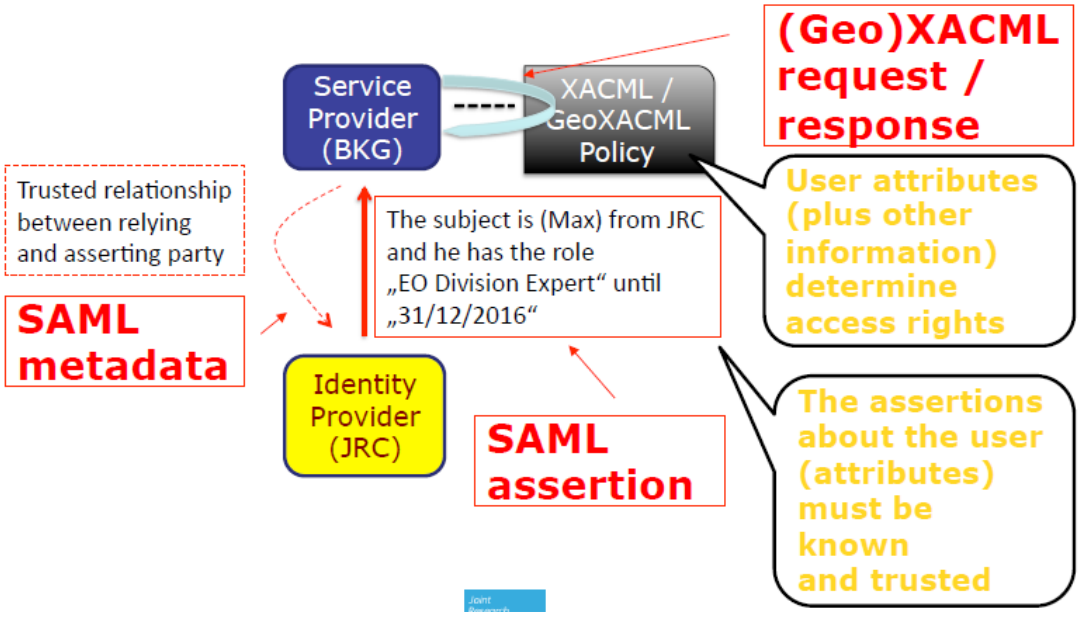

Figure 4: The use of SAML and (Geo)XACML for Access Management

1.2.1.2.3 Standard for Accounting – General Web Server logging capabilities

SAML attributes can be trusted (because we use SAML) and be used for associating a user with a request.

The Apache "CustomLog" can be leveraged to create use/user metrics.

1.2.1.2.4 Software and technology

From the intended software to be used for testbed realization, Apache, Tomcat, LDAP and Shibboleth are open source software, whereas SDInterceptor and SDGeoPDP are closed source solutions (for which no open source alternatives were available at the time of setting-up the testbed).

Figure 5 illustrates the different technologies and software used for the testbed implementation.

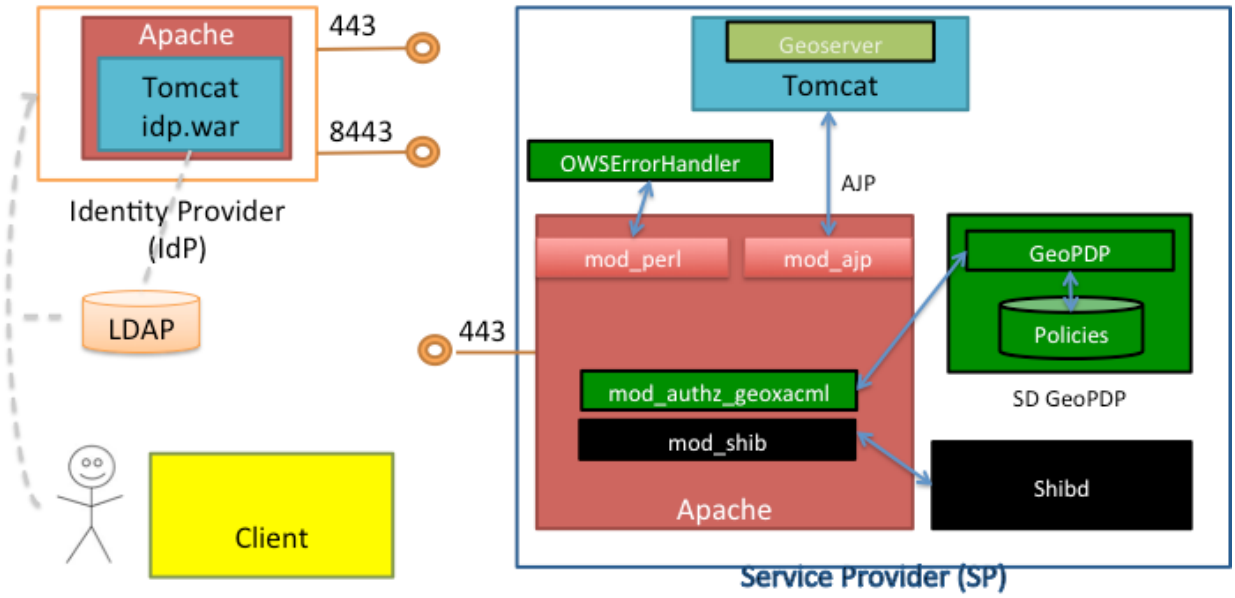

Figure 5: Software proposed to realize the testbed

The user tries to access the OGC service (provided by the Geoserver in the image above) with a Client (browser). The Shibboleth module (mod_shib) intercepts the request. This module checks with the Shibboleth daemon (Shibd) whether there is an authentication session available for this user. If this is not the case, the user is redirected to the Identity Provider (IdP). The user receives an authentication form from the IdP and authenticates. The IdP validates the credentials with the user directory (LDAP) and is redirected back to the SP. Again the Shibboleth module (mod.shib) intercepts and checks with the daemon (Shibd). Now there is a valid authentication session and the request is forwarded to the Policy Enforcement Point (PEP – mod_authz_geoxacml). The PEP accesses the user profile information from the session and sends this, combined with the OGC request information, to the Policy Decision Point (PDP – GeoPDP). The PDP checks the policy and returns a "deny" or "allow" decision. If allowed, the OGC Service is accessed via the Tomcat connector (mod_ajp) and the result is returned to the client. In case of denial, the Apache PERL module (OWSErrorHandler) is called via mod_perl and generates an appropriate response (e.g. Service denied) to the client.

An important consideration is related to a gap in AAA solutions for the geospatial community: the AAA standards and technologies work well with web (and mobile) clients, but for GIS desktop clients certain workarounds are required. This was a topic of analysis and testing during the testbed. Structurally, however, this issue can only be solved in cooperation with GIS desktop software providers.

1.2.2 ARE3NA-AAA Workshop

To support the project's objective to actively involve Member State representatives, a workshop was organised on March 16 and 17 in Leuven, Belgium. The project team decided to organize the workshop early in the project to involve the supporting organisations and subject matter experts as soon as possible and to foresee more time for the actual development of the testbed.

1.2.2.1 Participants

The 19 participants were AAA- and INSPIRE experts and stakeholders coming from a multitude of communities and Member States:

- Representatives from the consortium members: Geosparc, IDgis, Secure Dimensions and KU Leuven University;
- Representatives from organisations that are expected to be involved in the testbed: LNE-ACD, GDI-DE, GDI Bayern;
- Representatives from the Joint Research Centre (INSPIRE) and DG DIGIT (ISA programme);
- People involved in European and national/sub-national AAA implementation projects in the context of INSPIRE and e-Government (from Austria, Poland and France);
- Other stakeholders and interested parties such as the Dutch Cadastre, the Belgian Mapping Agency (NGI-BE) and Deloitte.

1.2.2.2 Objectives

The initial objective of the workshop was to examine, together with the participants, the initial evidence base gathered and analysed in the first phase of the project. In addition it aimed to present and discuss the SWOT analysis of the proposed standards and technologies to be adopted in the testbed phase, as noted above. More specific objectives included:

- To gather additional information from participants about their experience and to detect the potential gaps in the analysis relating to technologies and standards for access to data and services.
- To collect recommendations about what technologies, standards and approaches can best fit a solution for ready adoption for INSPIRE as part of the design of the testbed.

- To gather feedback on the initial proposal of the consortium for the testbed design.
- To discuss any potential barriers to the testbed's successful implementation and to gather recommendations for its development.

1.2.2.3 Preparation

The consortium elaborated an initial set of materials in preparation of the workshop including: (1) a summary of the initial findings on the existing standards and technologies that might be used for an INSPIRE AAA implementation, (2) a brief SWOT analysis of the standards and technologies to be used for the testbed and (3) an outline of the first ideas on the testbed development and implementation phase. As the workshop took place earlier than originally foreseen, the full reports *"D2.1 – Analysing standards & technologies against Best Practices"*[10] and *"D2.2 – SWOT analysis and initial design of the testbed"*[11] were drafted after the workshop. Instead, a series of presentations, as well as a list of questions were prepared in order to guide the discussions at the workshop.

1.2.2.4 Outcome

Overall, the workshop was a success. The proposed agenda was completed and the main objectives were met. Key lessons, recommendations and conclusions from the workshop are covered by a separate report "D2.4 – Results of the Workshop: 'AAA-Architectures for INSPIRE' 16-17 March, Leuven"[12]. The workshop assembly also approved the proposed approach (including scenarios and use cases) and planning for the Testbed development and implementation phase. In this context the following 3 scenarios were agreed:

- Cross-border access to OGC services (WMS or WFS)
- More complex access to (parts of) data sets by users of a thematic community
- Harvesting of INSPIRE catalogues

1.3 Testbed development and implementation

The third project phase to develop and implement a Testbed for AAA was based on (1) the lessons learned in the first two phases of the project, (2) the experience within the consortium and (3) feedback from different Member States and key stakeholders (Workshop).

For the testbed development, it was decided to test the different technical aspects initially among the consortium partners. Following an iterative process (3 iterations of 3 weeks each), the different IdPs and SPs were set up and connected in an AMF. Every two weeks, a technical progress meeting was organised which allowed the consortium technical team members to follow project progress. Interested staff from the Member States and supporting organisations could participate as well to remain informed, to be involved and to contribute where possible. We report this as we feel this has been an important aspect of developing the work. Each consortium partner chose a different technical solution to provide access to his or her respective OGC services:

- Secure Dimensions provided a WFS for testing purposes and a WMS (WorldMap) providing the background layer for the OpenLayers demo client.

---

[10] *https://joinup.ec.europa.eu/asset/are3na-aaa/document/analysis-evidence-base-relationships-and-gaps-between-technologies-standar*

[11] *https://joinup.ec.europa.eu/asset/are3na-aaa/document/discussion-document-swot-analysis-and-initial-testbed-setup*

[12] *https://joinup.ec.europa.eu/asset/are3na-aaa/document/results-workshop-%E2%80%98aaa-architectures-inspire%E2%80%99-16-17-march-leuven*

- IDgis installed a dedicated server, providing OGC services for the Dutch parcel layer.
- Geosparc installed a local proxy to external OGC services, providing the Belgian parcel layer.

IDgis also developed an OpenLayers based test application, used to access the different OGC web services, as well as the authentication services (IdP) in the different countries and the discovery service in the CC. At this point, a working federation was realised with support for SSO, and a test application that was able to show a map using the 3 layers from the 3 secured OGC services. Detailed documentation was produced on how to setup up an IdP and SP, as reference material for the supporting organizations. The initial testbed architecture is described in Figure 6. It should be noted that the "Discovery Service (DS)" in this case should not be confused with INSPIRE Discovery Services for metadata.

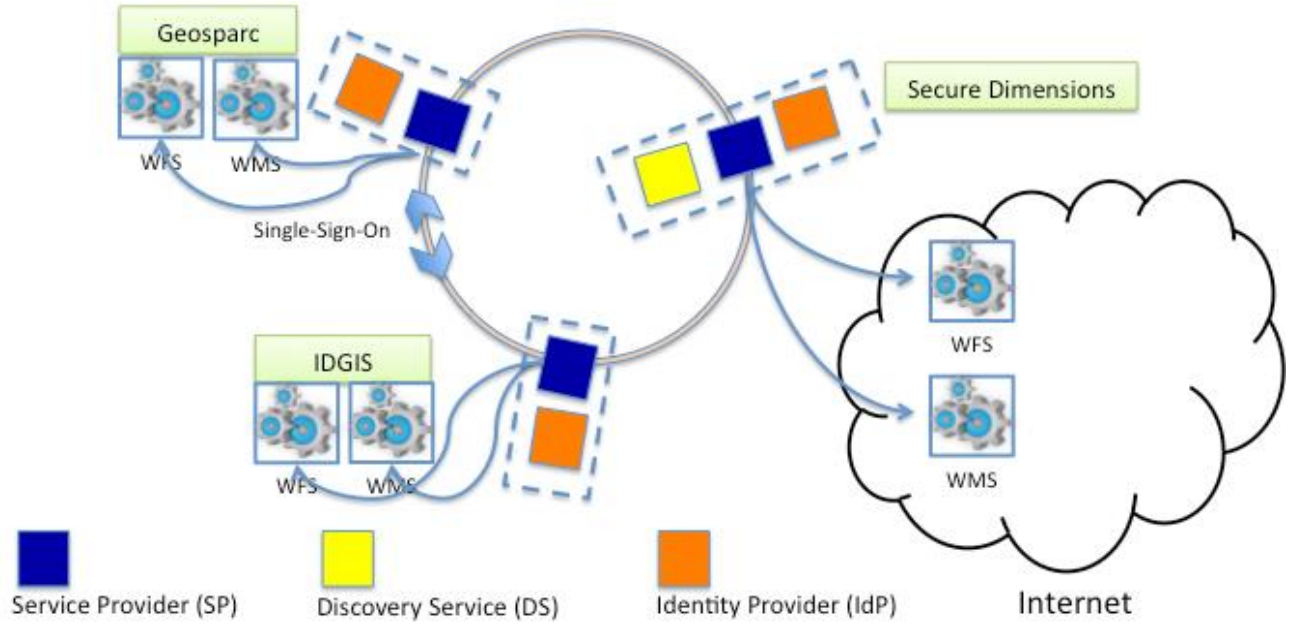

Figure 6: Initial testbed architecture

The next step for the testbed development was to add authorization rules to the OGC services based on a cross-border use case in the test application. As agreed during the workshop, the supporting organizations were involved as soon as possible. In fact, they joined the technical discussions from day one of the testbed development. Following the delivery of the initial federation by the consortium, two operations started in parallel:

- Firstly, the consortium continued the testbed development to prove the proposed solution supports both authentication and authorization, by realizing the cross-border use case.
- Secondly, the technical documentation for setting up an IdP and SP was provided to the supporting organisations and other interested parties, so they could already start their own work in joining the federation.

It should be noted that the consortium opted for the supporting organisations to join the same federation as the consortium was using. The setting up of a second federation would have had less value, as the second federation would not be able to access the test application and services created by the consortium. This point was the official start of the testbed implementation phase. The technical documentation of the set-up of the IdP and SP was also distributed to the JRC. This was done not only for them to assess the documentation, but also to start working on an extra use case as discussed during the workshop: the harvester use case.

The consortium continued the work on the cross-border use case and realized this from the perspective of a Belgian user. There was no need to implement this from a Dutch of German user perspective, as well, since the results would have been similar and would not yield new insights. For testing the cross-border use case, Geosparc provided a second test application based on Geomajas technology. This application also demonstrated the testbed technology stack's correct functioning with an alternative web GIS technology.

During the testbed implementation phase, additional use cases were developed, including the German GDI-DE Testsuite. The GDI-DE Testsuite is a web client, hosted by the German Coordination Office for the German Geospatial Data Infrastructure (GDI), that enables registered users to test GDI-DE services with respect to INSPIRE compliance. For the AAA project, the Testsuite was extended to technically support the SAML profile ECP. This capability allows the compliance testing of services hosted in the AAA federation. The protected services used for verification of the Testsuite capabilities are services from the GDI Bavaria: (i) INSPIRE View Service (WMS) and (ii) Download Service (Atom Feed).

The GDI-DE Testsuite use case also involved constraining access when evaluating INSPIRE compliance based on the attributes of the user: (i) a user can test INSPIRE compliance of the own services with no restrictions, (ii) a user can test the compliance of services to INSPIRE in Germany if they have the NPOC role, (iii) no other users of the federation can use the Testsuite to test compliance to INSPIRE. In order to realise the authorization, the GDI-BY and Secure Dimensions Service provider were configured with XACML policies.

GDI-BY SP functions as a reverse proxy to the production endpoints for INSPIRE compliant View and Download Services of the Bavarian Mapping Agency, currently protected via HTTP Authentication (RFC 2618) using HTTPS. The deployment of the GDI-BY SP is on a Secure Dimensions machine residing outside the Bavarian Mapping Agency's network. GDI-DE IdP provided different user accounts for testing the GDI-DE Use Case "Testsuite". It should be noted that the GDI-DE Testsuite itself is hosted on the GDI-DE Web Server but not as a protected endpoint of the federation. It was not feasible within the scope of this project to adopt the software to support this. Instead, the local login was used as the federation login so that the Testsuite could access protected services of the AAA federation with SSO support.

After completing the testbed implementation, the final testbed architecture was defined (see Figure 7)

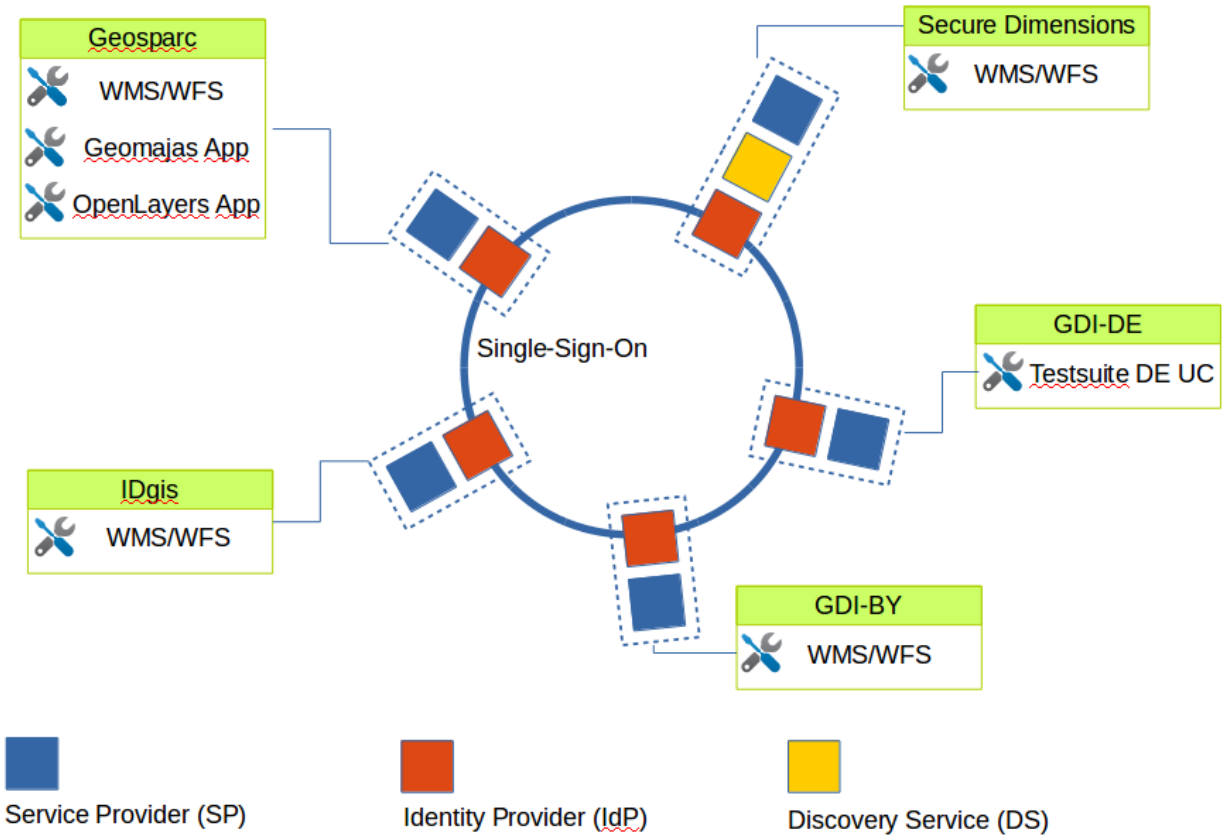

Figure 7: Final testbed architecture

Details regarding the testbed and how the consortium partners set it up can be found in the technical document "ARE3NA-AAA - D3.3a - Testbed Technical Documentation"[13].

2 Main technical achievements and results

2.1 Demonstrator and testbed

In order to provide concrete evidence for a reusable European approach to access control for INSPIRE data and services, the consortium created a testbed. One of the calculated risks in this type of projects is the ability to execute and engage all the parties into the project providing concrete results. Therefore, the decision was made to create the testbed environment in three stages.

In the first stage, the testbed development, a collection of open source technologies was assembled and configured at the premises of the consortium partners in three countries to form a federation with several services and identity providers. This resulted in an environment that the supporting organisations could use to study and get acquainted with the technology. By doing so, the supporting organisations could prepare for joining and testing the testbed with their own infrastructure. Another advantage was that it provided an environment that could be used as a base for the different use cases to test the requirements.

[13] See *https://joinup.ec.europa.eu/asset/are3na-aaa/home* for software and documentation

In a second stage, the testbed implementation, the supporting organisations were involved in the process, providing them with the documentation to set up and configure their own environment. At the same time, the use cases were developed to provide the functional elements as described in the scope.

In a third and last stage, the testbed assessment, action was taken to integrate production use cases into the testbed federation, giving the contributors the opportunity to learn about the standards and technology used as well as challenges and impediments faced.

One of the key observations during the design and implementation of the testbed is that the selected standards and technology are 'open' for re-use. Moreover, from a technical point of view, we found that it is possible to integrate the supporting organisation's existing security infrastructure within the testbed environment.

2.2 Documentation to setup your own testbed

In the previous sections we described what components make up the testbed. This section explains how an organisation can set up its own testbed. In order to set up a testbed, there are basically 3 options:

1. Join the existing federation with an existing or your own SP (and perhaps also your own IdP);
2. Create a new federation and configure a number of SP(s) and IdP(s) in the new federation;
3. Install your own SP and IdP without creating a federation.

The following documents provide all the necessary information to setup a testbed[14]:

- ARE3NA-AAA - D3.3a - Testbed Technical Documentation.docx
- ARE3NA-AAA - D3.3b - Installation Identity Provider.docx
- ARE3NA-AAA - D3.3c - Installation Service Provider.docx
- ARE3NA-AAA - D3.3d - Installation Coordination Centre.docx

2.2.1 Joining the existing testbed federation

This option is only available as long as the CC for the current testbed is available. It is the recommended choice, since it provides the best support in terms of available services and documentation. In this case an organisation can deploy the test applications and actually use the protected WMS layers already configured by the consortium.

In order to join the federation, the following steps should be taken (in this order):

1. Install an IdP;
2. Install an SP;
3. Install the test-application to check whether all layers work in an appropriate way.

Optional steps are:

4. Have the SP cover a WMS server (self-installed or public)
5. Adjust the test-application to make use of the new WMS server (configure the JavaScript code with the correct URL to the OGC layers)

[14] Available from *https://joinup.ec.europa.eu/asset/are3na-aaa/home*

The actual joining of the federation as IdP or SP can be requested by sending an email to the Coordination Centre (in this case via email *support@secure-dimensions.de*) attaching the entity's SAML metadata. After successful testing, the entity will become part of the AAA metadata.

2.2.2 Creating a new federation

This option is more difficult compared to the previous one. The following steps should be performed:

- Install a DS
- Install an IdP
- Install an SP
-

The challenge is that all configuration in the technical documentation (URLs, parameters etc.) might need to be altered in order to accommodate the new DS. It is the organisation's own responsibility to adjust the configuration accordingly. A second issue is that in the new federation, the WMS servers on which the test applications depend are not present. Therefore, the test application will not work correctly out-of-the-box. In this case it is required to ensure the SP covers a WMS server and to adjust the test application to make use of the new WMS.

2.2.3 Using a SP and IdP without a federation

The third option is implicitly accomplished when trying to join the existing federation. Once your own IdP and SP have been set up, there is no obligation to join a federation. Several organizations have SP and/or IdP operational without being part of a larger federation. In many cases the organizations might even have their SP configured to be an IdP as well.

The testbed provided in this project focused heavily on the federation aspect, as it was one of the key challenges to address. In some cases this might not be required. It should be noted that, however, when not joining the existing federation, the example test application will not be granted access to the WMS layers it is trying to show.

2.3 Recommendations of the used software stack

For implementing a federated authentication solution like the proposed access management federation on the basis of SAML 2, it is important not to implement the SAML standard (core, context, profiles, bindings and metadata specifications) independently. This is neither recommended nor feasible given the fact that many different proprietary/Commercial Off-the-Shelf (COTS) and open source solutions exist. It is, indeed, recommended to work closely together in the federation to make the right choices that match the requirements and fit current practices and architectures.

The software solution to implement the authentication part is Shibboleth[15]. The Free and Open Source Software (FOSS) Shibboleth provides production strength implementations to deploy the SP and IdP roles. The Shibboleth Identity Provider is a Java Web Application that can easily be installed on top of the most popular Java Servlet Engines. It is very flexible in terms of support for many different user management systems such as LDAP and Kerberos. The most important aspect, in terms of interoperability with SP installations, is its support for all relevant SAML profiles and bindings, as outlined in the recommendations.

The Shibboleth SP consists of two parts, an Apache module or IIS (Internet Information Service) filter (mod_shib) and a daemon process. Binary installers are available for most of all popular Operating Systems, including Windows. The tight integration with the Apache or IIS Web Server supports a large variety of options to make protected resources available to the federation.

[15] More information on Shibboleth can be found on https://shibboleth.net/

For implementing a single IdP SSO, as outlined earlier, it must be possible to skip the IdP selection for a client with an existing session. To realize this feature, the chosen option is to leverage the SAML Common Domain cookie writing service. For the AAA federation, the IdP Discovery Service developed by the Swiss Academic Federation (SWITCH) was deployed. It has the main feature to combine the IdP Selection and the Common Domain Cookie Writing Service. The SWITCH Discovery Service[16] can be customized to support many technical requirements, including the single IdP SSO. The DS also supports the feature to provide a JavaScript code snippet to integrate a simple IdP selection menu to the home page of the SP. This allows the user to directly select the IdP at the SP and not to visualize a 'stop-over' at the DS for IdP selection. As the IdP select code snippet detects an existing session, it hides itself so that the user only sees the selection if no session exists. As this DS is a single point of failure, it must be operated with the highest availability possible. It is important to note that the DS is a very simple and, therefore, robust and stateless Web Server, which combines different options of providing this web service with high availability. Best practices for the SWITCH federation and how to achieve this have been documented[17]

For implementing the authorization layer with local access rights enforcement at a SP, the XACML and GeoXACML compliant solution from Secure Dimensions has been chosen, even though it is not FOSS. The advantage of using the solution from Secure Dimensions is that the description of access rights and their enforcement are based on the same XML encoded information; the Policy document.

The authorization solution comprises of two parts. Firstly, there is an Apache Web Server module (mod_authz_geoxacml) that is capable of intercepting communication from the client to the protected resource (OGC Web Service for the AAA Federation), as well as the response from the service to the client for rights enforcement. Secondly, there is a Web Service (GeoPDP) for decision-making. As the GeoPDP is a stateless service, it can be deployed in a very flexible manner, e.g. behind a load balancer, to support high performance decision-making.

The accounting layer was implemented by leveraging the custom logging features of the Apache Web Server. As logging of access to protected resources takes place at the SP, and the mod_shib is an Apache Module, all user attributes that were received by the SP are available to the Apache logging feature. It is quite simple to construct a "CustomLog" directive to store access information about the user and the resource in an accountability logfile.

In order to avoid violating user privacy, only the (anonymised) persistent identifier of the user was stored in the logfile.

3 Key lessons

3.1 The choice for an Access Management Federation

The analysis of Best Practices and other initiatives (such as STORK) shows that an AMF is the most obvious choice for establishing an AAA mechanism for INSPIRE. INSPIRE has already federated characteristics, because it is a European SDI built upon the national and sub-national SDIs involving thousands of organisations. Most of the examples analysed (Austria, Belgium, Germany, the UK, STORK, many of the initiatives in the research and education domain) have also established an AMF.

[16] Access the SWITCH discovery service: https://www.switch.ch/aai/support/tools/wayf.html

[17] See *https://www.switch.ch/aai/support/presentations/infoday-2005/AAI-ID05-50-SWITCHwayf.pdf*

The Business Interoperability Working Group (BIWG) of the UK Location Programme has analysed different options with regard to the implementation (or not) of an access control mechanism for geospatial data and services. The AMF solution was compared against a centralised access control approach and concluded AMF would be the preferred solution. Also other studies in other domains such as Grid and Cloud computing communities came to similar conclusions.

AMFs can also 'easily' link to each other, thereby creating a federation of federations or an Inter-federation, enabling users from one federation to access services provided by another federation. This trend can be seen from the examples of eduGAIN and Kalmar initiatives in the education and research domains in the EU. However, the setup and testing of a federation of federations was beyond the scope of this project.

3.2 Many standards and technologies exist to build upon

Several general ICT standards exist from W3C, OASIS and other international standardisation bodies upon which an AAA approach for INSPIRE can be built. Some standards have a very specific function (e.g. X.509 certificates are used to establish HTTPS communication between web browsers and web servers), while others have a broader range of capabilities (e.g. SAML specifies the structure, exchange and processing of assertions about the user's identity). The analysis shows that there are no standards 'missing', but that often specific profiles and bindings need to be developed to match the needs of a particular AAA implementation. SAML seems to be the most popular standard for exchange of information about users. For authorisation, XACML is a widely accepted standard.

At the technology side, many tools exist, both as open source and proprietary solutions. The Kantara initiative documented and tested more than 65 of those tool(kit)s and indicate that most support the implementation of the different AAA standards reviewed in our study.

3.3 AAA solutions should be as generic as possible

Almost all the described standards are generic ICT standards that can serve a multitude of domains. An AAA solution for INSPIRE is not so different from AAA solutions for e-Government, or for the research and education domains. However, the *Study on Authentication and Authorisation Platforms for Scientific Resources in Europe* states that *"authorisation services should be considered to be domain-specific, whereas authentication services should be as generic as possible"*.

The analysis of the standards and technologies reveals there are no special AAA standards for the geospatial domain with the exception of GeoXACML.

Two main questions remain to be addressed:

- How much is in an AAA approach still special or specifically needed for the geospatial world?
- Do we need to implement a special standard for handling the specific geo-parts such as GeoXACML or can parts of the authorisation be done at the application level? In other words, is there a real need for a geospatial extension to an authorisation standard?

Authorisation could be split in a more generic part and an application specific part. The analysis of the Best Practices shows that GeoXACML has been implemented in several cases, although this is limited to the use cases requiring geospatial criteria for authorisation, e.g. where authorisation depends on the location of the user or where the geospatial extent of the spatial data to be accessed varies with user groups. In all other cases this is not needed and often XACML is used.

3.4 Agreement on standards

An important conclusion is the fact that several standards exist for authentication and authorisation. It is equally important to note that, from the analysis of those standards and review of the best practices in different Member States, a consensus appears to exist on which standards need to be used to establish an AAA solution for INSPIRE.

- For **Authentication** the widely accepted standard is **SAML**. Operating a Federation in the context of INSPIRE, requires that participating entities support a specific set of SAML profiles and bindings.
- For **Authorisation** there is consensus on the use of **XACML** as well as GeoXACML for cases where spatial criteria are important.

3.5 Several standards are interoperable

The choice of standards and technologies that can be implemented at the level of the federation does not require all AAA implementations in the Member States to use the same standards. Indeed, while a choice must be made to set up the federation at the European level, it is recommended to leave the existing implementations in the Member States (including at the sub-national level as well as in particular communities) as they are, and build upon them. When/where necessary, supporting tools can be provided to facilitate credential conversion. A similar approach was followed in the European Data Infrastructure (EUDAT[18]) initiative.

In the context of an AAA implementation for INSPIRE, several aspects should be taken into consideration. Firstly, the setup of an AMF for INSPIRE, and in particular the testbed development, requires a clear choice of a standard for authentication and for authorisation. Since SAML is recognised as more secure for the exchange of attribute information, and is also more scalable, it was seen as the logical choice for the authentication part. For authorisation the choice was XACML (together with GeoXACML, when needed). Secondly, as described above, the application of SAML at the European level is not necessarily in contradiction with the use of other standards in the Member States. The Best Practices reveal that SAML is compatible with other standards. In several projects SAML has been implemented along with OpenID (GEOSS AIP-6) or with OAuth (Flanders) without major problems.

3.6 No open source tools available for GeoXACML

The intention of the consortium was to use as much as possible open source tools and components to realise the testbed. The selected tools for the Testbed are all free and open source software, except for the tool to work with the GeoXACML standard, because no FOSS tool was available at during the project timeframe. Instead we used a closed source implementation provided by the consortium partner, Secure Dimensions. If a full FOSS stack is required for an operational AAA suite for INSPIRE, we recommend that an initiative is taken to establish a separate open source project to realise and promote the missing components. In order for such an initiative to succeed, it would be important to find an interested party to lead this open source project and to establish a sustainable ecosystem.

[18] http://www.eudat.eu/

3.7 Support for desktop and web clients

As mentioned earlier, the proposed solution has been successfully tested for both web clients and desktop environments. Although SAML is a web standard for security, with some modifications it is always possible to adjust desktop clients to support it.

Web clients, on the other hand, support the solution by default. In order for a JavaScript client to gain access to the resources behind the SPs within the federation, it is necessary to make sure the user is known at each of those SPs. In the example web applications, this is achieved by first iterating all WMS services and requesting a PNG image (from layer legends). Once that is done, any layer can be added safely from those WMS or WFS. This is a generic way of working that can be applied for any web-mapping client. The consortium tested this using the default version of OpenLayers and Geomajas technologies.

In addition, the consortium modified desktop GIS clients to support the SAML2 ECP protocol. This modification allows the user to point to the federation metadata XML and select its IdP. The consortium was able to access the testbed with a customized QGIS version.

Also, the consortium demonstrated successfully the use of ArcMap 10.2 to connect to protected WMSs from the AAA federation with the support of SSO. It is important to note that this is possible because the AAA Federation provides 'smart' Service and Identity Provider endpoints and not because ESRI's ArcMap has implemented SAML / ECP support. It is further important to understand that connecting to a WFS does not work, as ArcMap connects to a WFS via a third party tool which cannot leverage the smart endpoints properly.

It is up to the providers of desktop GIS applications to apply the necessary modifications in order to support SAML. From the testbed experience, we believe the efforts to add SAML support are very reasonable and limited to implementing the ECP profile.

3.8 The AMF coordination centre is key, but also challenging

A CC plays a pivotal role in any AMF solution. The centre is the organisation or body that should guarantee that activities of the federation conform to the existing legislation at European and national levels. For example, each AMF should respect the rules set out in the European Data Protection Directive (95/46/EC) and the subsequent regulation that has or is being put in place[19]. The CC needs to define rules and to set up agreements (such as SLAs and legal binding contracts) with the participating organisations of the federation. Many AAA initiatives have set up Codes of Conduct to define the rules and to define how the federation will apply legislation. For example, eduGAIN has defined its Codes of Conduct assuring its conformity to Article 7 of the European Data Protection Directive. A CC is necessary but might also be a single point of failure and/or a bottleneck for performance. Consequently, it is of utmost importance to organise it well and to clearly think about who could/should play this role. In the context of INSPIRE this could be, for example, the JRC or another operational entity within the European Institutions.

The organisational mode in which a CC is managing the federation might become complex. The coordination centre orchestrates the cooperation between IdPs and SPs. Several initiatives from the research and educational sectors refer also to the addition of Attribute Providers (AP), focusing on collaboration-specific attribute information for specific communities. Adding this fourth level further complicates the legal and

19 http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM%282012%290011_EN.pdf

technical arrangements. For example, in research it is common to grant access to resources such as computers, experiments and instruments to a particular research project (Virtual Organisation). The project then determines how that access will be allocated among individual project members. This could be applicable for specific INSPIRE thematic communities, too, but access to spatial data objects or geospatial datasets is a different level of granularity compared to a computer or experiment.

3.9 The definition of attributes, roles and rules is important

The analysis of AAA solutions for research and education defines three aspects for a trust model: (1) the SP must trust the IdP to authenticate the users as agreed and to ensure that user information is correct and up-to-date; (2) the IdP must trust the SP to process and protect personal data received from the IdP conform to existing legislation; and (3) the users must trust their IdP and SP to protect their personal data. This is done through the definition of clear rules and roles and by providing a readily trusted mechanism to exchange attribute data about users. EUDAT and other initiatives from the research and education community define this in terms of 'Level of Assurance' (LoA) and 'Level of Trust' (LoT). LoA relates to the SP point of view ("can I trust the means for authentication") and LoT relates to the user point of view ("can I trust the SP"). The potential implications and applicability for INSPIRE and e-government activities should be explored further.

From this context, however, it is useful to consider which attributes we need to exchange; what attributes mean; and to have clear definitions of the attributes (semantics) and their possible values or code lists. This was also confirmed by the EUDAT initiative:

"In order to deal with attributes coming from different sources consistency of semantics is important; names, affiliations, contact details, and so on, need to be interpreted in the same way by every attribute provider, and be published in the same schema. Roles need to be named and interpreted the same way across communities, and/or will have to be named uniquely so as to not clash with the same role in a different community" (European Union, 2012).

The analysis of the AAA solutions for research and education revealed that a full and global harmonisation of attributes, although it has been a priority for a long time, is not feasible. On the other hand, well-defined semantic attributes within a community and mapping mechanisms could be developed. The possible role of ISA core vocabularies, in helping to define role labels, should be explored, such as parts of the Registered Organization Vocabulary.

3.10 Some level of Accounting is needed

The main focus in the ARE3NA-AAA project is on Authentication and Authorisation. However, the examples of Best Practices reveal that also the Accounting part is to some degree required. More precisely, the French and Polish mapping agencies have set up AAA solutions with the aim to better know the use and/or users of their data and services. In addition, some mapping agencies have the ambition to link an AAA solution to e-Commerce services. This is the case in Belgium, France, Poland and Romania, amongst others. An AAA solution for INSPIRE can also be a mechanism to protect the infrastructure against abuse because it will give system administrators the possibility to trace who did what and when on the infrastructure.

Therefore, it is important that the testbed, and in the future an operational AAA solution for INSPIRE, contains a (simple) mechanism for logging users and usage.

3.11 Implementing an AAA framework may improve data and service sharing

Contrary to what is often expected, the implementation of an AAA solution might actually increase the use of INSPIRE datasets and services. The main reason is that several organisations are more eager to provide access to their resources if the access is controlled and managed (by the AAA solution). This can be compared to a market place. If this market place has no proper protection and access control, only few merchants will go there to offer goods. By adding access control, the market place becomes a 'trusted' environment and more and more merchants and consumers will visit it.

As a consequence, this sharing often leads to improved data quality and services. More users with different expectations and needs accessing INSPIRE data and services triggers organisations to meet higher service levels (metadata, availability, performance, interoperability, etc.).

Building on an AMF with Authorization enables different services and data sets to be made available through the same infrastructure. It is not only possible that certain services / datasets are exclusively accessed by other public administrations but also citizens or even commercial companies. Based on trusted attributes of users that, for example, represent affiliations and entitlements, it is possible to manage access according to policies established for INSPIRE or additional activities beyond environmental policy-making.

The collective use of protected and distributed resources is a challenge in each large infrastructure. The problem is mainly around the possibilities to harmonize access rights across resource providers. This gets almost impossible if a user has a separate login at each provider of protected resources.

Single Sign-On (SSO) and the interoperable sharing of user attributes are key to support access to protected resources, such as web services, across several resource providers. The AAA federation supports this. An agreed set of user attributes is released by any IdP of the federation and can be used by any SP to enforce access rights.

Furthermore, the single IdP SSO enables the seamless use of protected resources in one application, regardless of the security domain in which the protected resource resides. In the AAA Federation, one example of a combined consumption of protected OGC Web Services is demonstrated in an OpenLayers web-mapping application. Here, the user must login to be able to load the OpenLayers based application. The underlying JavaScript library then initiates new sessions with other service providers as needed to display a seamless overlay of all protected WMSs, as configured.

In order to provide access to the relevant services of the web-mapping application, it is essential to coordinate (harmonize) the access rights enforced at each SP. This is possible, as a user has a defined set of attributes (and values) upon which access rights can be bound. For example, the OpenLayers application that supported our Cross-Border Use Case leverages the attribute of the country for the user's home organization. In the AAA federation, this involved using country values "B", "DE" and "NL".

For any production use, it is mandatory to agree on the set of user / organizational attributes. Standard, non-personal attributes must have a pre-defined set of values. One example from a production use is inter-federation attributes recommended by GÉANT but others need to be explored, especially from those developed through ISA.

3.12 ISO Metadata and protected services

INSPIRE and other SDIs foresee that users search a data catalogue to find descriptions of data sets and services. In the case of protected services, it is not obvious how to outline this in the ISO metadata for the

services. It is, in particular, two levels of descriptions are possible: (i) outline to the user that this service has access restrictions on it (which should be described in the metadata elements 'Conditions for access and use' and 'Limitations on public access') and (ii) outline to the binding clients the technical options available.

It is important that catalogue server implementations support the use of external codelists to define the semantics of different authentication methods supported by the service. The client must know this in order to bind to the service. Such codelists could form a new register in the INSPIRE registry, which is supported by the Re3gistry software developed by ARE3NA.

3.13 Authorization

The AAA Testbed builds authorization on XACML or GeoXACML policies. This enables a fine-grained authorization model that supports constraint access to, for example, (i) a service endpoint, (ii) a layer of a WMS or Feature Type of a WFS, (iii) an area of interest, (iv) resolution threshold for WMS and (v) the number of features to be returned by a WFS.

Complex rules can be very confusing for users. The more fine-grained the authorization becomes on the server side, the more time and effort should made to explain the user why the system is refusing him to perform a certain (inter)action. For example, in the Cross-Border use case a user (while panning the map) may no longer see the map because the map does no longer contain the country border. Instead a message like "access denied" is shown. This might not be sufficient for handling this case and explaining the user why the map is no longer visible. It would be better to show an error message such as "not allowed to obtain German data outside Germany, unless the German border is visible".

It is, therefore, important to provide a standards-based declaration of the enforced access rights so that the user or the client understands this. It is entirely safe to provide an XACML or GeoXACML policy as a protected resource to users of the federation because we use one source for documentation as well as for enforcement. This way the documentation and the enforcement of the rules will always point to the same logic. This, together with good exception handling should be a guarantee for a user-friendly system, enforcing complex rules.

4 Recommendations

Based on the project results and lessons learnt, we come to the following list of recommendations to establish an AAA solution for INSPIRE. Feedback from participating organisations is reporting in Annex II.

4.1 Access Management Federation (AMF)

For establishing access control across public authorities in Europe participating in INSPIRE, this work recommends federated authentication and local authorization, also referred to as an Access Management Federation (AMF).

For the authentication:

- Use federation metadata (that contains the circle of trust and is maintained by the CC).
- Use standards that support Single Sign-On (SSO), based on the IdPs already in place in the different Member States at the national (and potentially sub-national) level.
- Use SAML as the standard to set up the federation, because of the ability to define an explicit 'trustee list', which is important to avoid security vulnerabilities.

For the authorization:

- Use XACML to describe the authorisation rules.
- Use GeoXACML to describe spatial authorisation criteria.

4.2 Use available and generic ICT standards and tools

Several standards and tools are available. Consensus exists on which standards to be used. To a large extent, the same standards and tools are used in other ongoing developments such as STORK. We, therefore, recommend to use as much as possible these standards and tools and join existing implementations. The only specific standard required to support an AAA solution for INSPIRE is the OGC spatial extension of the XACML standard, GeoXACML.

4.3 IdP to release only non-personal attributes in a federation

To protect privacy of public administration members, citizens or other federation members, the attributes to be used and exchanged in an AAA solution should be limited to non-personal user information.

As a general recommendation, a federation (and in particular the enforcement of access rights) should not rely on personal user attributes. However, the exchange of personal attributes is possible but must be constrained to take place (i) only for a contractual reason and (ii) with the consent (approval) of the user.

As an example, academic federations mandate a core set of attributes that are non-personal. Some SPs, however, may ask the user for additional attributes, and perhaps email addresses or phone numbers. Also, the fulfilment of payment options may require an SP to request additional attributes on top of the basic set. It is possible to support this via the SAML Attribute Query profile.

The AAA federation has implemented the concept of personal attribute release by deploying the uApprove extension[20] to the Shibboleth IdP. The extension can be configured to intercept attribute release based on attribute names and SP domains. So, for example, it is possible to create attribute release policies for an organization's own SPs and other SPs and for personal attributes. A user can acknowledge the attribute release or deny it; in which case, the SP may not function properly and may deny access to the protected resource requested.

4.4 Follow academic AMF best practices

In the academic world, successful AMF implementations exist. An AMF for INSPIRE should be based on the best practices and experience gained.

Academic federations around the world operate on the basis of SAML. The support for crafting a trusted whitelist of participating entities and theirs roles as well as the secure exchange of user attributes are key capabilities. For the provisioning of protected Web Services for geospatial data, we have decided to leverage that academic concept which has proven production strength and scalability. Academic federations operate with as little as 30 entities to as much as 2500 entities.

[20] The uApprove extension is developed by SWITCH. More information is available on *https://www.switch.ch/de/aai/support/tools/uApprove.html*

There are, however, differences between the academic federations and the ARE3NA AAA federation. This is because certain technical requirements introduced by the specifics of client applications, a federation for geospatial data services cannot 'simply' be identical. In particular, academic federations usually support multi-IdP SSO and also use SAML POST Bindings, typically used as the default binding for session initiation with SPs. As outlined in the technical documentation, the AAA federation is configured to have the use of IdPs limited to one, with the default session initiation based on Artefact Binding.

In addition, the automatic SSO requirement, explored and implemented in the AAA testbed, is not required for sharing protected web assets such as HTML pages as it is done by academic federations. Therefore, the AAA federation runs a central DS to support the automatic SSO, leveraged in particular with OpenLayers web-mapping applications.

4.5 The Control Centre should be established

For the implementation of an AAA solution for INSPIRE using an AMF, the CC is critical. Therefore, the control centre responsibility needs to be mandated to an empowered entity. This entity will require the necessary resources to fulfil this responsibility. How much resources are required and how such a CC should be organised will need to be investigated considering existing best practices and INSPIRE's needs.

4.6 Use XCAML for documenting the authorisation rules

It is observed that authorization is often encoded directly in the SP as opposed to defined using an authorisation standard (like (Geo)XACML). We also expect that, in many cases, this practice will continue for some time. Nevertheless, even if the standard is not used to actually define and enforce the authorizations, we recommend its use to at least describe the authorization rules in a common language.

5 Open issues

5.1 Which use cases need Geo-specific standards and tools?

In a follow-up assessment special attention should be given to making a more in-depth inventory of INSPIRE-AAA related use cases. For each of these, the Geo-specific standards and tools should also be analysed.

In the scope of the project, the Cross-Border use case required the enforcement based on geometries. In this use case, the administrative boundaries of The Netherlands and Belgium (as well as their common border geometry) are used to determine if the actual map requested from a Web Map Service is displaying the border. Three basic scenarios are possible: (i) the requested map is outside The Netherlands, outside Belgium, (ii) inside The Netherlands or Belgium, (iii) displaying a cross border map (The Netherlands and Belgium property is displayed on the map).

The GeoXACML Policy consists of exactly three Rules that apply different test functions for geographic relations to the geometries of the administrative border of the Netherlands, Belgium and the common border. Depending on which test functions are true, access is permitted or denied. Clear demand from users of INSPIRE data and services needs to be established and tested.

5.2 Legal and organisational aspects of the coordination centre

The coordination centre plays a key role in the successful implementation of an AMF based AAA solution for INSPIRE. This project revealed the importance of the Coordination Centre, but more detailed analysis

and recommendations on legal aspects, organisational needs and best practices, the necessary resources, etc. are required.

5.3 Discussion on the federation of federations

AMFs have the possibility to be linked to each other to form a 'federation of federations'. The actual needs for this in the context of an AAA mechanism for INSPIRE were not in scope for this study and are still to be explored.

5.4 How to advertise the rules of authentication and authorisation in the service metadata

When a user discovers an INSPIRE service from the catalogue, it is described in ISO compliant metadata. This service metadata description currently provides very little options / limited details to mark a service as "protected". The way this is currently achieved is by using the ISO CodeList as illustrated in the following code snippet:

```
<gmd:resourceConstraints>
            <gmd:MD_LegalConstraints>
              <gmd:accessConstraints>
                <gmd:MD_RestrictionCode codeL-
ist="./resources/Codelist/gmxCodelists.xml#MD_RestrictionCode" codeList-
Value="copyright">copyright</gmd:MD_RestrictionCode>
              </gmd:accessConstraints>
              <gmd:accessConstraints>
                <gmd:MD_RestrictionCode codeL-
ist="./resources/Codelist/gmxCodelists.xml#MD_RestrictionCode" codeList-
Value="license">license</gmd:MD_RestrictionCode>
              </gmd:accessConstraints>
              <gmd:accessConstraints>
                <gmd:MD_RestrictionCode codeL-
ist="./resources/Codelist/gmxCodelists.xml#MD_RestrictionCode" codeListValue="otherRestrictions" />
              </gmd:accessConstraints>
            </gmd:MD_LegalConstraints>
          </gmd:resourceConstraints>
```

It is recommended that the MIG discuss how meaningful it would be to have "access constraints" meaning "otherRestrictions". In order to make a protected service discoverable properly, it requires the metadata to state the accepted authentication methods. For example, as a service is protected via HTTP Authentication (RFC 2617[21]), then the client knows exactly what to support in terms of 'first contact': Either the client sends the HTTP Authorization header immediately or the service will return a HTTP 401 status code. This would signal to the client that a username/password dialog is to be displayed to the user and the input is to be processed according to RFC 2617.

[21] https://www.ietf.org/rfc/rfc2617.txt

Regarding the protection of services in the AAA federation, the metadata would need to state that the authentication methods, accepted by the service, are SAML2 Browser SSO Profile and SAML2 ECP Profile.

In that sense, a proposal from the GDI-Bavaria supporting organization is to use in-line extensions to the ISO metadata, which allows the different authentication methods supported by the service to be expressed. Annex 1 provides a working extension that can be obtained from the GDI-Bavaria Online Catalogue.

5.5 Discuss the full set of exchangeable attributes based on experiments with use cases

During the project an initial set of attributes was defined and used in the Testbed environment. When establishing an operational AAA infrastructure, the set of attributes to be exchanged needs to be analysed and agreed upon between the federation members. The analysis is best organised based on experiments with actual use cases.

The agreement on user attributes to be released by the IdPs of a federation is an important organizational activity that typically is led by the CC. It is important to understand that recommended access decisions, enforced local at any SP, must only be based on non-personal attributes. Also, it is important to note that only non-personal attributes should be declared mandatory. In that light, the AAA project has used the following non-personal user attributes for the different use cases:

Cross-Border Use Case user attributes

Attribute Name	Value / set of possible values
urn:inspire:aaa:country	{BE, DE, NL}

GDI-DE Testsuite Use Case user attributes

Attribute Name	Value / set of possible values
urn:inspire:aaa:role	{N/A, NPOC}
urn:inspire:aaa:domain	{hostname of the SP the user administrates}
urn:SD:subject:organization-name	{GDI-BY, GDI-DE, SD}

However, in order to demonstrate the ability of the deployed technology to support “user approval” for the release of personal attributes, the Secure Dimensions IdP also released personal attributes in addition to the non-personal attributes.

Personal attributes released by the Secure Dimensions IdP

Attribute Name
Surname (urn:oid:2.5.4.4)
givenName (urn:oid:2.5.4.42)

Annex 1 – Code snippet of ISO Metadata extensions supporting different methods of authentication

```
<?xml version="1.0" encoding="UTF-8"?>
<gmd:metadataExtensionInfo>
 <gmd:MD_MetadataExtensionInformation>
  <gmd:extendedElementInformation>
   <gmd:MD_ExtendedElementInformation>
    <gmd:name>
     <gco:CharacterString>urn:oasis:names:tc:SAML:2.0:profiles:SSO:browser</gco:CharacterString>
    </gmd:name>
    <gmd:domainCode>
     <gco:Integer>001</gco:Integer>
    </gmd:domainCode>
    <gmd:definition>
     <gco:CharacterString>In the scenario supported by the web browser SSO profile, a web user either accesses a resource at a service provider, or accesses an identity provider such that the service provider and desired resource are understood or implicit. The web user authenticates (or has already authenticated) to the identity provider, which then produces an authentication assertion (possibly with input from the service provider) and the service provider consumes the assertion to establish a security context for the web user. During this process, a name identifier might also be established between the providers for the principal, subject to the parameters of the interaction and the consent of the parties. To implement this scenario, a profile of the SAML Authentication Request protocol is used, in conjunction with the HTTP Redirect, HTTP POST and HTTP Artifact bindings. It is assumed that the user is using a standard commercial browser and can authenticate to the identity provider by some means outside the scope of SAML.</gco:CharacterString>
    </gmd:definition>
    <gmd:dataType>
     <gmd:MD_DatatypeCode codeL-
ist="./resources/Codelist/ML_gmxCodelists.xml#MD_DatatypeCode" codeList-
Value="codelistElement">codelistElement</gmd:MD_DatatypeCode>
    </gmd:dataType>
    <gmd:parentEntity>
     <gco:CharacterString>MD_RestrictionCode &lt;&lt;CodeList&gt;&gt;</gco:CharacterString>
    </gmd:parentEntity>
    <gmd:rule>
     <gco:CharacterString>additional metadata codelist element</gco:CharacterString>
    </gmd:rule>
    <gmd:source>
     <gmd:CI_ResponsibleParty>
      <gmd:organisationName>
       <gco:CharacterString>Andreas Matheus</gco:CharacterString>
      </gmd:organisationName>
      <gmd:role>
       <gmd:CI_RoleCode codeList="./resources/Codelist/ML_gmxCodelists.xml#CI_RoleCode" codeL-
istValue="author">author</gmd:CI_RoleCode>
      </gmd:role>
```

```
        </gmd:CI_ResponsibleParty>
       </gmd:source>
      </gmd:MD_ExtendedElementInformation>
     </gmd:extendedElementInformation>
    </gmd:MD_MetadataExtensionInformation>
</gmd:metadataExtensionInfo>
<gmd:metadataExtensionInfo>
 <gmd:MD_MetadataExtensionInformation>
  <gmd:extendedElementInformation>
   <gmd:MD_ExtendedElementInformation>
    <gmd:name>
     <gco:CharacterString>urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp</gco:CharacterString>
    </gmd:name>
    <gmd:domainCode>
     <gco:Integer>002</gco:Integer>
    </gmd:domainCode>
    <gmd:definition>
     <gco:CharacterString>An enhanced client or proxy (ECP) is a system entity that knows how to con-
tact an appropriate identity provider, possibly in a context-dependent fashion, and also supports the
Reverse SOAP (PAOS) binding [SAMLBind]. An example scenario enabled by this profile is as follows: A
principal, wielding an ECP, uses it to either access a resource at a service provider, or access an identity
provider such that the service provider and desired resource are understood or implicit. The principal
authenticates (or has already authenticated) with the identity provider, which then produces an authen-
tication assertion (possibly with input from the service provider). The service provider then consumes the
assertion and subsequently establishes a security context for the principal. During this process, a name
identifier might also be established between the providers for the principal, subject to the parameters of
the interaction and the consent of the principal. This profile is based on the SAML Authentication Request
protocol [SAMLCore] in conjunction with the PAOS bindi</gco:CharacterString>
    </gmd:definition>
    <gmd:dataType>
     <gmd:MD_DatatypeCode codeL-
ist="./resources/Codelist/ML_gmxCodelists.xml#MD_DatatypeCode" codeList-
Value="codelistElement">codelistElement</gmd:MD_DatatypeCode>
    </gmd:dataType>
    <gmd:parentEntity>
     <gco:CharacterString>MD_RestrictionCode &lt;&lt;CodeList&gt;&gt;</gco:CharacterString>
    </gmd:parentEntity>
    <gmd:rule>
     <gco:CharacterString>additional metadata codelist element</gco:CharacterString>
    </gmd:rule>
    <gmd:source>
     <gmd:CI_ResponsibleParty>
      <gmd:organisationName>
       <gco:CharacterString>Andreas Matheus</gco:CharacterString>
      </gmd:organisationName>
      <gmd:role>
       <gmd:CI_RoleCode codeList="./resources/Codelist/ML_gmxCodelists.xml#CI_RoleCode" codeL-
istValue="author">author</gmd:CI_RoleCode>
      </gmd:role>
```

```
        </gmd:CI_ResponsibleParty>
      </gmd:source>
    </gmd:MD_ExtendedElementInformation>
  </gmd:extendedElementInformation>
</gmd:MD_MetadataExtensionInformation>
</gmd:metadataExtensionInfo>
```

In addition to the example above, another valid approach is to use external codelists for specific purposes. The following example outlines the use of external code lists to indicate that the service endpoint requires SAML authentication using Web Browser SSO or ECP profile.

```
<gmd:resourceConstraints>
    <gmd:MD_LegalConstraints>
        <gmd:accessConstraints>
            <gmd:MD_RestrictionCode codeList="./resources/Codelist/gmxCodelists.xml#MD_RestrictionCode"
                codeListValue="copyright">copyright</gmd:MD_RestrictionCode>
        </gmd:accessConstraints>
        <gmd:accessConstraints>
            <gmd:MD_RestrictionCode codeList="./resources/Codelist/gmxCodelists.xml#MD_RestrictionCode"
                codeListValue="license">license</gmd:MD_RestrictionCode>
        </gmd:accessConstraints>
        <gmd:accessConstraints>
            <gmd:MD_RestrictionCode codeList="./resources/Codelist/gmxCodelists.xml#MD_RestrictionCode"
                codeListValue="otherRestrictions"/>
        </gmd:accessConstraints>
    </gmd:MD_LegalConstraints>
</gmd:resourceConstraints>
<gmd:resourceConstraints>
    <gmd:MD_SecurityConstraints>
        <gmd:useLimitation>
            <MD_RestrictionCode codeList="http://www.secure-dimensions.eu/inspire/authCodelists.xml#AuthenticationCode"
                codeListValue="urn:oasis:names:tc:SAML:2.0:profiles:SSO:browser"/>
        </gmd:useLimitation>
        <gmd:useLimitation>
            <MD_RestrictionCode codeList="http://www.secure-dimensions.eu/inspire/authCodelists.xml#AuthenticationCode"
                codeListValue="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"/>
        </gmd:useLimitation>
        <gmd:classification>
            <gmd:MD_ClassificationCode codeList="./resources/Codelist/gmxCodelists.xml#MD_ClassificationCode"
                codeListValue="unclassified" />
        </gmd:classification>
    </gmd:MD_SecurityConstraints>
</gmd:resourceConstraints>
```

Annex II Feedback from Supporting Organizations

GDI-BY Feedback

The contribution of GDI-BY to the testbed work package included the following activities:

- provision of one access-protected INSPIRE View Service (OGC Web Map Service) and one access-protected INSPIRE Download Service (Atom Feed)
- provision of the extended metadata sets for the services
- test of the GDI-DE Testsuite's extended version using the protected services

Neither an IdP nor a SP was deployed locally at GDI-BY. From the perspective of a regional spatial data infrastructure (SDI) like the GDI-BY operating in the German state of Bavaria, interoperable authentication

and authorization is currently not a top priority issue. The majority (approx. 80%) of view and download services currently available in the GDI-BY are available without access protection. This reflects Bavaria's open data policy. The only organisation which provides access-protected services uses its own technical solution (HTTPS Authentication with SSL encryption).

As there is currently no cross-organisational authentication / authorisation use case within the GDI-BY, it was not feasible to allocate sufficient resources for the installation and testing of an IdP and an SP in a real production environment. Bavarian public authorities provide their web services through a centrally managed internet gateway using a reverse-proxy configuration. A new application / service can only be made available through this gateway after having undergone a standardised security testing procedure including a penetration test.

However, it is recognized that there are potential use cases for interoperable authentication and authorization on the national or the European level.

The extension of the GDI-DE Testsuite application facilitating the test of access-protected services is deemed beneficial. Apart from minor issues, it ran smoothly during the tests and provided new insights into the INSPIRE compliance of access-protected web services. As the majority of access-protected services within the SDI Germany (GDI-DE) currently use standard HTTPS Authentication with SSL encryption, this alternative technology could also be taken into consideration when further extending the GDI-DE Testsuite.

The extended metadata sets were tested for compliance with INSPIRE and ISO using the GDI-DE Testsuite. They were also tested in practice using different metadata catalogue implementations. In the Testbed, the MD_RestrictionCode code list was extended by adding additional values identifying different authentication methods. This was done by providing a separate schema describing those values. Testing showed some technical issues associated with this approach. Currently available metadata compliance test suites validate metadata against standard ISO schemas and thus mark the extension as an error. Also, currently available metadata catalogue implementations are usually based on standard ISO schemas and / or internal schemas. This can lead to the loss of the elements using the additional code list values when the extended metadata sets are imported into a catalogue. To avoid high costs for the adaption of existing testing and catalogue software, it is therefore suggested, to do the metadata extension according to the rules specified in ISO 19115:2003 Annex F.5 (although it might be argued that the additional code list items would be a logical expansion of the existing standard set of values). However, the resulting in-line extension using the MD_ExtendedElementInformation element would lead to metadata sets that pass existing ISO compliance tests and should work smoothly with most existing catalogue implementations. An example of such an extension (in this case an extended MD_MaintenanceFrequencyCode code list) can be found here:

http://geoportal.bayern.de/csw/gdi?REQUEST=GetRecordById&VERSION=2.0.2&service=CSW&outputschema=csw:IsoRecord&elementsetname=full&ID=6f5a389c-4ef3-4b5a-9916-475fd5c5962b

GDI-DE Feedback

The contribution of Kst. GDI-DE to the use case of testing protected INSPIRE web services included the following activities:

- Provision of GDI-DE Testsuite source code
- Provision of server infrastructure for deployment of GDI-DE Testsuite extension and IdP
- Testing GDI-DE Testsuite extension with protected services

- Implementation of Identity Provider (IdP) in the BKG/GDI-DE production environment

Kst. GDI-DE is aiming for the implementation of a homogeneous access control solution. This promises added value to the SDI by enabling cross-organizational authentication and authorization. In recent years, various prototypes have illustrated how an Access Management Federation (AMF) can meet technical requirements of an SDI. As a result, a WAYF service has been added as a central component in the GDI-DE architectural concept. While use cases of cross-organizational access control within individual German states exist, use cases that make use of cross-border authentication and authorization between different states have been difficult to identify within GDI-DE. As a result, funding for the implementation of a GDI-DE federation still remains an open issue.

Kst. GDI-DE regards the "GDI-DE Testsuite" use case realized within the ARE3NA AAA study as a further proof-of-concept for implementing a harmonized protected access in SDI. From a monitoring perspective, testing protected web services for INSPIRE compliance is an important aspect. Currently, it is not possible to test protected INSPIRE web services for compliance, because data providers have implemented heterogeneous access control mechanisms. The underlying use case illustrates how a standardized access control supports harmonized authentication and authorization between the extended GDI-DE Testsuite and two implemented SPs.

Testing protected web services with the extended GDI-DE Testsuite entails particular requirements regarding user roles: While data providers need to be able to test their own protected services, a national point of contact (NPOC) must be able to test all services for monitoring purposes. The implementation of the underlying use case allows access rules to be defined following XACML standard.

The experimental use of the implemented GDI-DE Testsuite extension showed that the protected web services could be tested for INSPIRE compliance. One INSPIRE View Service (Web Map Service) and one INSPIRE Download Service (Atom Feed) could be accessed at two different SPs each. The different access rules functioned during testing: While a user with the role "NPOC" was able to test all web services at two foreign domains, a user without this role was unable to test any of them.

In future work, it would be interesting for GDI-DE to add the GDI-DE Registry to the illustrated work flow. Starting in 2015 the GDI-DE Registry automates the monitoring use case by executing the GDI-DE Testsuite via its API.

In a final activity within the ARE3NA AAA project, Kst. GDI-DE implemented an IdP within the BKG production environment that hosts the central components of the GDI-DE. Installation and configuration of the Shibboleth IdP were conducted following the documentation provided by ARE3NA AAA. The implementation process showed to be quite complex for personnel not familiar with user management software like Shibboleth or LDAP. While most aspects were covered by the provided documentation, some technical details needed to be clarified via direct support by Secure Dimensions GmbH. Beyond that, the rather passive design of the present server environment entails particular requirements for the IdP. Firstly, the environment exposes one server as a central entry point (load balancer), while the IdP runs on a separate server behind this entry point. This requires a proxy pass redirect via AJP-protocol to the IdP and the handling of two different certificates for ports 443 and 8443 on the load balancer. Secondly, the environment does not allow direct requests outside the internal network. Thus the IdP is unable to request remote metadata from the federation directly, but needs a proxy to do so.

With additional support by Secure Dimensions GmbH, it was possible to overcome these system specific barriers and setup the IdP to function in the BKG production environment that hosts the central components of the GDI-DE. The federation metadata was stored and requested locally in this case to facilitate configuration. The implemented IdP provides identities to the ARE3NA AAA federation for all present use

cases.

JRC Feedback

Description of the use case performed by JRC

The JRC is responsible for providing access to metadata about geospatial data and services within the scope of the INSPIRE directive through its European geoportal. To ensure good operation of this service it is necessary for the geoportal to know if the metadata being provided is available to users in the correct way, including the testing of services. If some of these services are protected then the geoportal harvesters of catalogue information are not able to fully perform this test. The use case, therefore, wanted to show how, in a machine-to-machine setting, the access control testbed could include the geoportal to see if it could access a protected service from a public organisation involved in INSPIRE. The result of this work could mean that this 'super-user' could then be included in a fully operational federation to ensure appropriate checks can be made across the metadata and services of INSPIRE being accessed by the geoportal.

Main findings

- The case was successful and, following appropriate security settings were in place, it was relatively easy (with support) to implement this form of access to the geoportal.
- The result is likely to be scalable, meaning that there would not need to be multiple bilateral agreements between the geoportal and (meta-) data providers to access their protected services, as the geoportal would be recognised as belonging to the federation.
- The specific configuration for security meant more effort was needed in supporting the use case to understand where barriers existed and how solutions could be implemented. It is possible that equally secure settings could face similar issues and, naturally, more preparation time before deployment to raise awareness with all involved could have helped.
- Practical/political considerations for setting up a federation also need to be explored, and this should be discussed in the INSPIRE MIG. This impact on eventual technical choices.
- The JRC was also able to build on previous experiences with Shibboleth from a couple of years ago, and put in place a practical implementation in the context of the geoportal, which was also helped by reusing code.
- The federation definitely would appear to be the best solution for this case's needs (centralised authentication helps greatly) but an opportunity should be taken to explore what other technologies may be adopted. Shibboleth has worked but maybe some e-government tools would be appropriate. This could also apply across the federation and INSPIRE stakeholders maybe should share details about what level of access control they intend to use, what preferred technologies are and if these are, to some extent, readily interoperable with Shibboleth.

DOV Feedback

Description of the use-case: The drillings use-case

Within Flanders, DOV is responsible for the INSPIRE services regarding soil and sub-soil data. One of the most important datasets is that of the drillings. Since DOV is a covenant of multiple agencies within the

Flemish government, they have the concept of a “DOV-partner”. Multiple “partners” work together to gather and maintain the drillings dataset (and others). It usually takes a while for drillings to get published, as they undergo multiple checks. Also, some drillings (i.e. failed ones) never actually get published.

The idea was to extend such “partner” rights to people from the Netherlands or Germany. It would grant them access to drillings that have not yet been published.

Unfortunately, some organisational barriers came up with as a result that this use-case was never fully realized.

Main findings

When discussing the testbed implementation for DOV, it became apparent they already had a very similar architecture in place. They were already configured to be a Service Provider (SP) for the Belgian Identity Provider (IdP), using the SAML2.0 authentication protocol.

The difference is that they chose to use a different technical implementation to set up the SP: OpenAM instead of Shibboleth. On one hand this realization strengthened our case, as they obviously agreed with the proposed testbed solution, seeing they had chosen the same path. On the other hand, it made it difficult to join the testbed federation. This is because their SP is host to a thousand servers and applications, belonging to different organizations. Connecting this system to a testbed federation could possibly compromise the security of all applications within the SP. This was a decision beyond the power of the responsible of the project. As a result, the only way to join the testbed was to create a duplicate of their current setup and connect it to the testbed federation. Creating such a duplicate though, wouldn't yield any new learning.

On top of that, DOV had already done tests with connecting their OpenAM system to other IdPs and Sps, and they have already configured multiple ways of logging in (alternatives to using the Belgian IdP).

In a sense we can conclude that DOV was successful in implementing the testbed, but with alternative, compatible technology and connecting to a different IdP.

This still left the authorization part to be explored. It is the policy within DOV that every Web Service is secured independently. Working with a proxy to add security to another Web Service would be a violation to their security policy. As a result the proposed solution would never be accepted.

Another issue that came to their attention is that the proposed authorization service (the SD Interceptor) was maintained at a central location at Secure Dimensions. This means all authorization checks are done in a central service. This also means it is a black box DOV has no control over.

After this review, the testbed was put on lower priority. One use-case DOV was very much interested in is to build the security (SAML authentication + some authorization) directly into their WMS server (Geoserver). This, however, falls outside the project scope.