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

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

D2.2 – Discussion document: SWOT analysis and initial testbed setup

Danny Vandenbroucke

Dirk Frigne

Pieter De Graef

Andreas Matheus

Reijer Copier

Robin S. Smith

Joint
Research
Centre

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

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

Disclaimer

Copyright notice

Bibliographic Information:
Vandenbroucke D, Frigne D, De Graef P, Matheus A, Copier R, authors Smith RS, editor. Authentication, Authorization and Accounting for Data and Services in EU Public Administrations: D2.2 Discussion document: SWOT analysis and initial testbed setup. European Commission; JRC94627

Table of Contents

List of Tables

List of Figures

1 Introduction

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

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

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

This document *"D2.2 – Discussion document: SWOT analysis and initial testbed setup"* puts together the material used for the discussions during the workshop on 'AAA-architecture for INSPIRE' that took place in Leuven from 16 to 17 March 2014. The material consists of: 1) a series of questions used to help participants to prepare for the workshop and to guide the discussions during it; 2) a brief SWOT analysis on the possible standards and technologies and 3) an initial description of the testbed. All the material was presented and discussed during the 1.5 day workshop[1]. This includes the images in this report that have been taken directly from the workshop slides. A full report with the results of the workshop is presented in a separate report: *"D2.4 – Results of the Workshop: 'AAA-Architectures for INSPIRE' 16-17 March, Leuven"*.

2 Topic List for Guidance during the Workshop

An important part of the workshop will be dedicated to discussions in breakout groups and through panel discussions. Also throughout the presentations a red thread will be followed: *"what are the most appropriate standards and technologies for an AAA approach for INSPIRE taking into account the technological and organisational boundary conditions of the organisations that will participate"*? In order to allow participants to prepare the discussions, a simple questionnaire / topic list has been prepared. The questions aim at providing guidance during the workshop, and the break-out sessions and panel discussion in particular.

[1] The material was not distributed among the workshop participants before the workshop because the workshop was organised at an earlier stage than originally foreseen.

1. What are the technological challenges and issues revealed in previous AAA-projects?
    a. Use of SAML or other standards?
    b. Technological boundary conditions (what can be done, what can't) in place in existing organisations?
2. What are the organisational challenges and issues to implement an Access Management Federation?
    a. How many IdP and SP will be part of the federation?
3. What are the use cases we should cover in the testbed?
    a. What do you think about the proposed use cases?
    b. Which use cases are missing?
4. What do you think about the proposed AAA-architecture and technical solution?

3 SWOT Analysis of Standards and Technologies

The goals of the ARE3NA-AAA project, and the testbed in particular, are defined as follows: 1) to define the standards and technologies to be used to achieve an AAA mechanism across organisations in Europe; 2) to evaluate the proposed concept of an Access Management Federation (AMF) in a testbed; 3) to involve different organisations from different Member States and their INSPIRE compliant services to demonstrate the approach in practice; and 4) to gain better understanding of the advantages and implications of the approach for future operational use.

3.1 SWOT analysis

The standards and technologies for secure access and exchange of information have been analysed and are described in detail in the document "D1.1.1 & D1.2.1 Analysing standards and technologies for AAA". Although several standards and technologies exist, the consortium proposes to implement SAML and (Geo)XACML to setup a testbed following the concepts of AMF. We first provide a brief SWOT analysis of both SAML and OpenID, the reasons for choosing SAML and (Geo)XACML are explained.

	Helpful to achieve the objective	Harmful to achieve the objective
Internal factor	**Strengths** • Simple Single Sign-on (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 1: SWOT of the use of OpenID

	Helpful to achieve the objective	Harmful to achieve the objective
Internal factor	**Strengths** • Model trust between participating parties using SAML metadata • Simple Single Sign-on (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

Table 2: SWOT of the use of SAML

Many operational and pilot implementations of AMF based on SAML exist, especially in academia (see Figure 1).

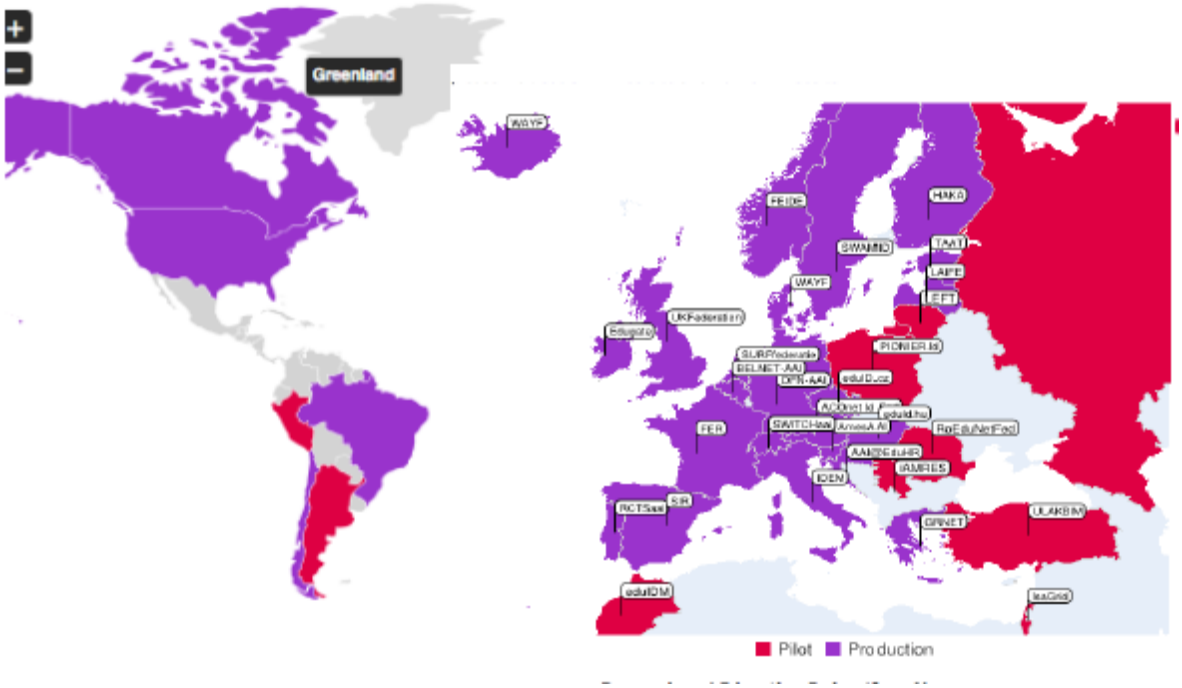

Figure 1: AMF based on SAML in the Academic World

These implementations are often complex and span Europe, the Americas, Asia and Australia. Based on the pros and cons it is proposed to use the following standards:

AAA: SAML (V2)

- ✓ It is a mainstream IT Standard (OASIS) with existing implementations

- ✓ Based on Open Standards and Open Source Software

A**A**A: XACML (V2) or GeoXACML (V1)

- ✓ It is a mainstream IT Standard (OASIS / OGC) with existing implementations
- ✓ Based on Open Standards and Closed Source Software

AA**A**: Web Server logging capabilities

- ✓ SAML attributes can be trusted (because we use SAML) and be used for associating a user with a request
- ✓ Apache "CustomLog" directive can be leveraged to create use metrics

Figure 2 and 3 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.

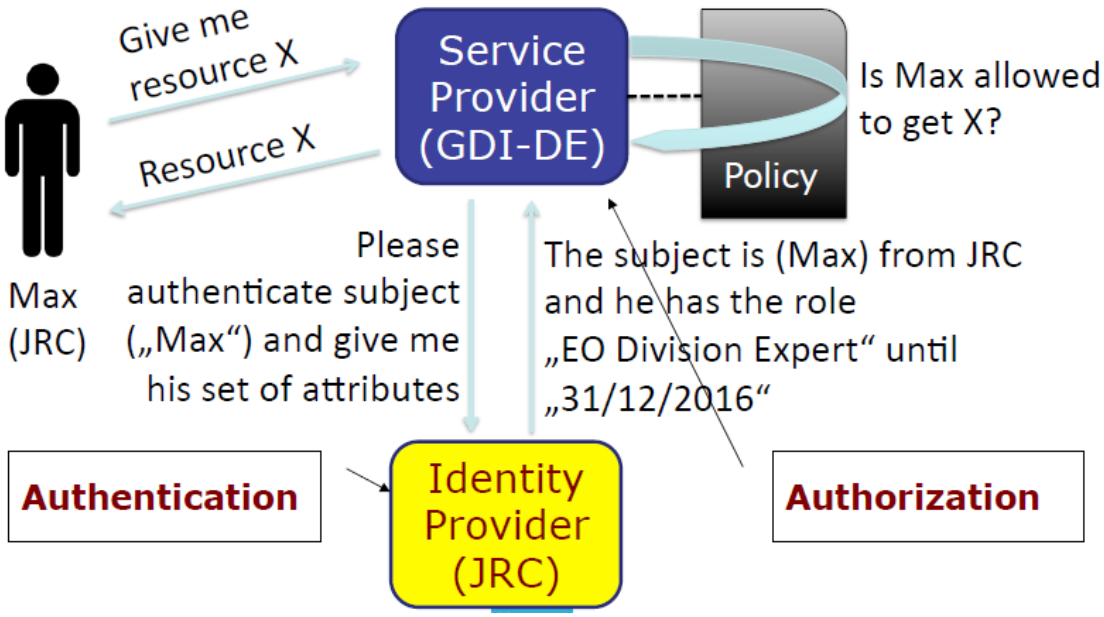

Figure 2: Example of Access Management with distribution of duties

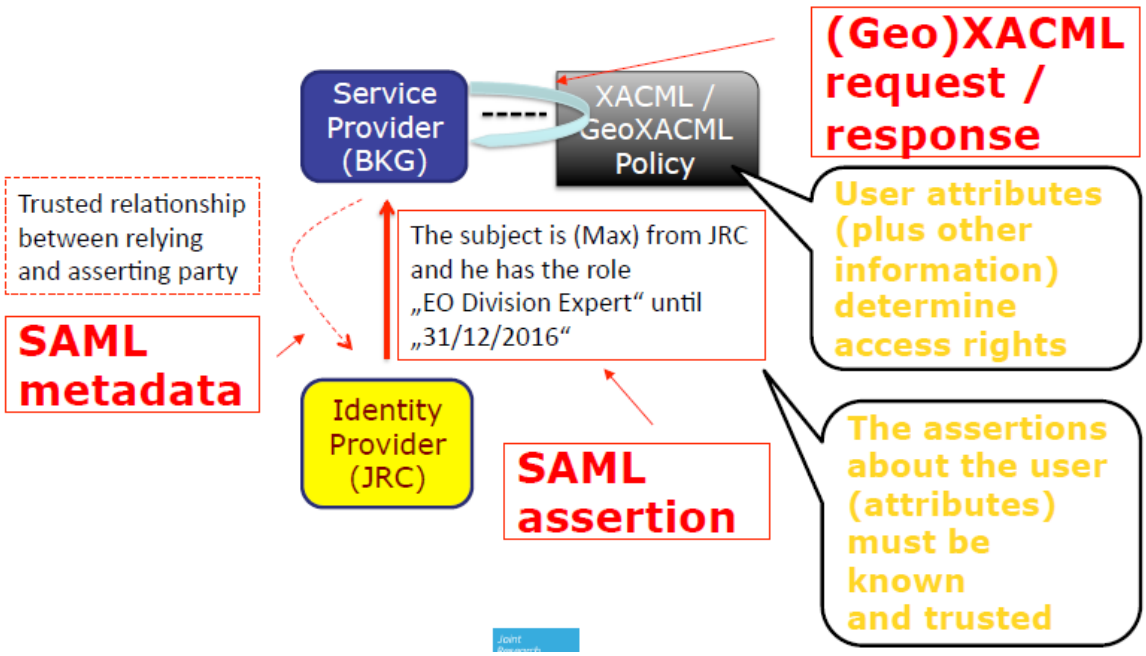

Figure 3: The use of SAML and (Geo)XACML for Access Management

The proposed standards and technology will be discussed throughout the workshop, and especially during the breakout groups.

3.2 Standards and technologies: convergence and gaps

From the SWOT analysis, comparing the capabilities of OpenId and SAML, it can be concluded that it seems to be the appropriate approach to base an AMF on SAML. There are three major reasons for this choice.

Firstly, it provides the ability to establish a white listing of trusted partners, which turn out to be the members of the federation. Of course, this could be added to an architecture based on OpenId, but with the deployment of Shibboleth – the Open Source Software implementing SAML – this feature is supported with an “out of the box” deployment which is more straightforward.

Secondly, the assurance of released attributes enables to separate the authentication (to the IdP) and establish the authorization (to the SP). This important separation of concerns enables that only one standard must 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 Single-Sign-On, which is required to build applications such as web-mapping based on OpenLayers, cannot be implemented using OpenId.

Moreover, the analysis of different practices from the geospatial, the e-Government and academic sectors has shown that SAML is more and more implemented and forms the backbone of many AAA solutions (see Vandenbroucke et al., 2014; European Union, 2012). 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 federation and demonstrated during the GEOSS AIP-6 initiative, a so called trust gateway from SAML to OpenId can be deployed.

In terms of technology, software and standards, the following is anticipated to be used to setup of the testbed:

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: 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
    b. Software: Apache "CustomLog" directive
    c. Technology: Apache Web Server

From the intended software to be used for testbed realization, the following software is Open Source:

1) Apache, Tomcat, LDAP, Shibboleth

From the intended software to be used for testbed realization, the following software is Closed Source:

2) SDInterceptor and SDGeoPDP

The following figure illustrates the different technologies and software intended to be used for the testbed realization.

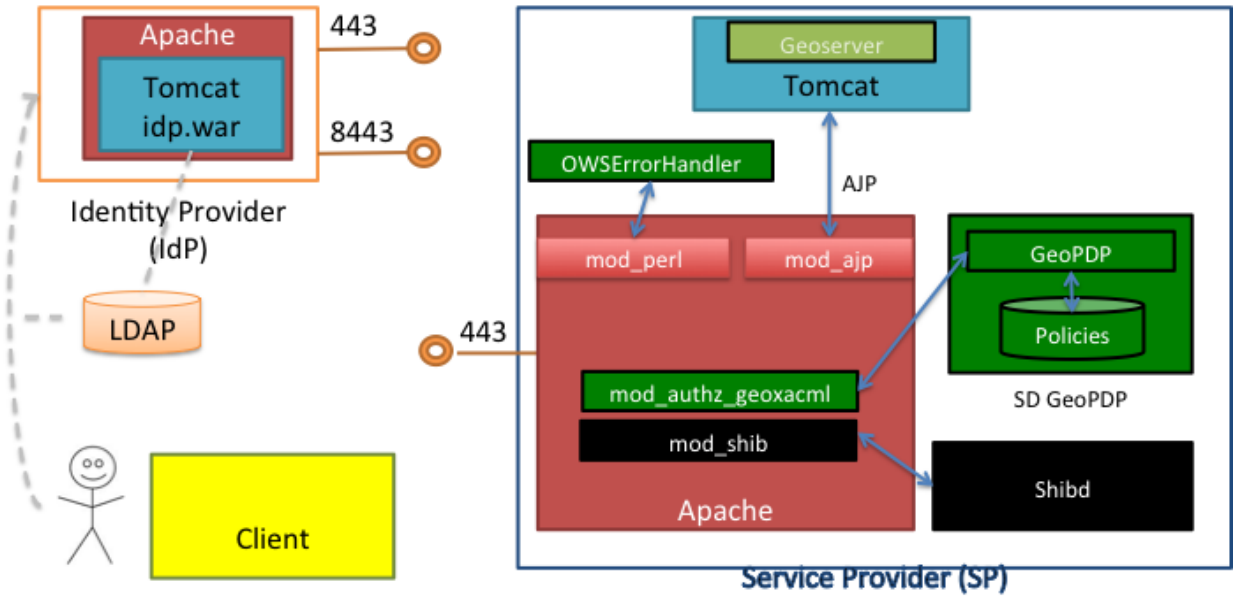

Figure 4: Software proposed to realize the testbed

In order to realize the testbed AMF, the deployment of a so called SAML Discovery Service is required to support the automatic Single-Sign-On capability. According to the SAML standard, this should be compliant to the IdP Discovery Profile, which requires deploying a cookie management service for the common domain of the federation. It is the intention to use the PHP-based Discovery Service available as Open Source from SWITCH. The deployment requires not more than a simple Apache Web Server with PHP support. As this Web Server is the single point of failure, its deployment must take place on a web server with availability as close as possible to 100%. However, the consortium does not foresee any specific hardware setup for ensuring high-availability as we will "just" run a testbed.

Finally, there remains still an important issue – we could consider this a gap in AAA solutions for the geospatial community: the AAA standards and technologies work well with web (and mobile) clients, but GI desktop clients still need workarounds. This will be a topic of analysis and testing during the testbed but is an issues that can only be solved in cooperation with GIS software providers.

4 Initial Setup of the Testbed

The way the standards and technologies for AAA work together to deploy secure access mechanisms to (geospatial) data has been described in detail in *"D1.1.1 & D1.2.1 Analysing standards and technologies for AAA".* It follows the concept of the separation of duty in which the IdP (authentication) is the asserting party and the SP (authorisation) is the relying party. The next question is: where will such a mechanism be deployed? The setup assumes we will have an IdP Proxy (managing the users and user information) and several SP Proxies (providing the services).

4.1 Testbed deployment

The testbed can be deployed in several ways:

1. In the PRODUCTION Network

The IdP, as well as the SPs would be situated in the production network (behind the firewall). The testbed federation would be outside that firewall (see figure 4). There are advantages and disadvantages of this solution:

- It is closest to reality, but most difficult to implement;
- It remains questionable whether it is feasible in the context of the testbed. Probably it is not: it requires agreement from ICT department and higher hierarchy within organisations, which might be hard to be achieved in the lifetime of the project.

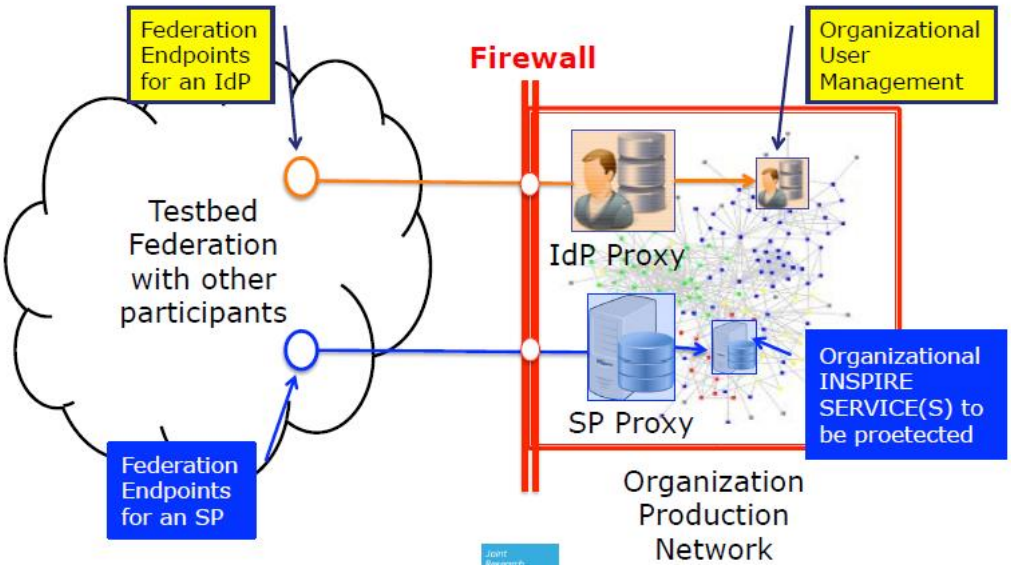

Figure 5: Testbed as part of the production network

2. In the SANDBOX Network

The testbed would be organised as a kind of 'sandbox', with the IdP and SPs outside the firewall of the production environment, but themselves 'protected' behind an external firewall. There are, again, pros and cons:

- A quite realistic scenario;

- ☞ The question remains whether each testbed participant has a sandbox environment. If not, can it easily be set-up?

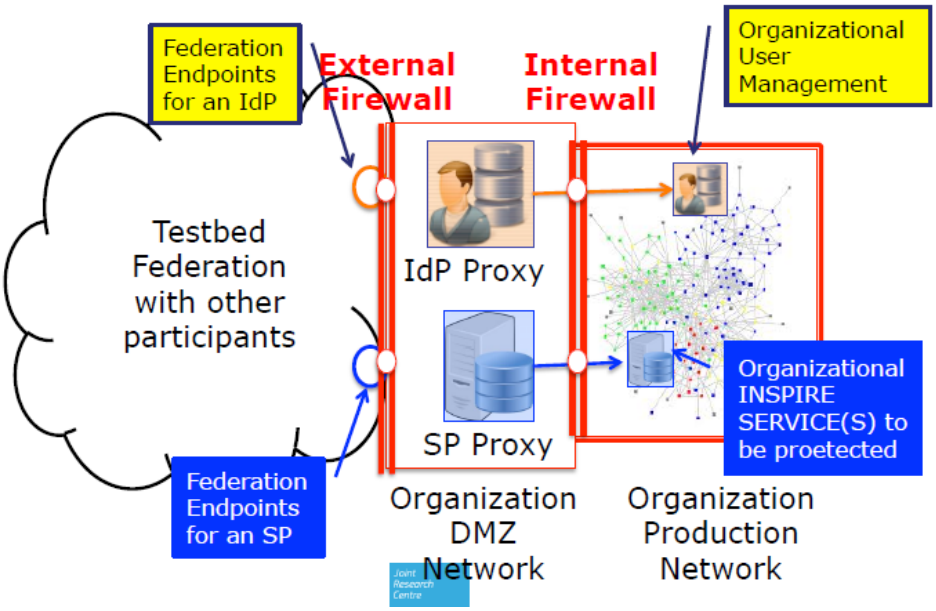

Figure 6: Testbed as sandbox network

3. In another Network

The last option is to setup the testbed outside the firewall that protects the production environment, independent of any private or production network. Pros and cons are:

- ☞ It is the least realistic approach but has minimum impact to production network of participating organization;
- ☞ Conclusions and recommendations are still meaningful.

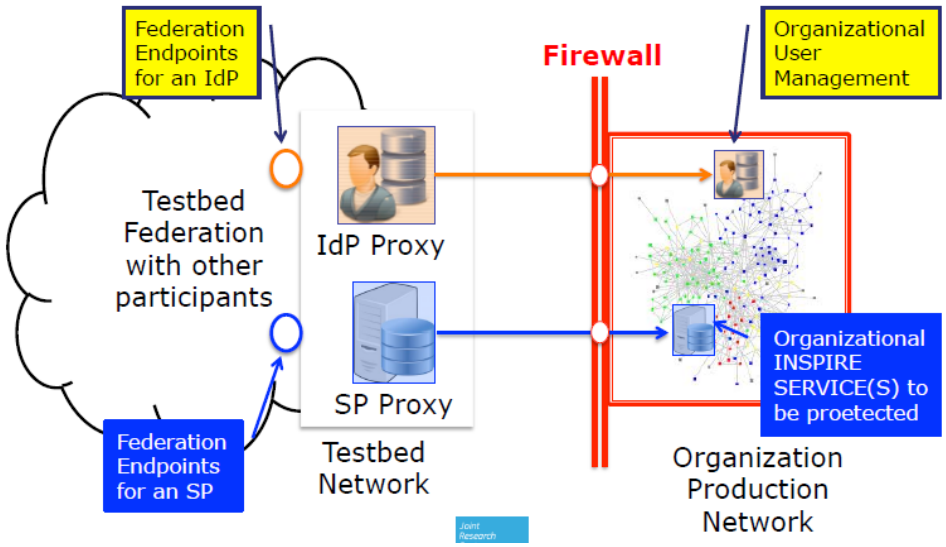

Figure 7: Testbed outside the production network

The sandbox option is probably the most realistic and useful option in the context of the project.

4.2 Example of a use case

As an example of a potential use case, the harvesting of protected services by the JRC is presented and discussed. This use case is based on already existing activities of the JRC in which an application, a harvester, tries to access services from the Member States through their respective catalogues. By helping the harvester to automatically connect to relevant web services with relevant access controls, resources can be appropriately provided through the European INSPIRE geoportal and all relevant content tested. In turn, the harvester testing can provide more complete feedback to the Member States, helping them to understand their progress towards implementation through the system's feedback reports. The workflow of the use case (scenario) is described in Figure 8.

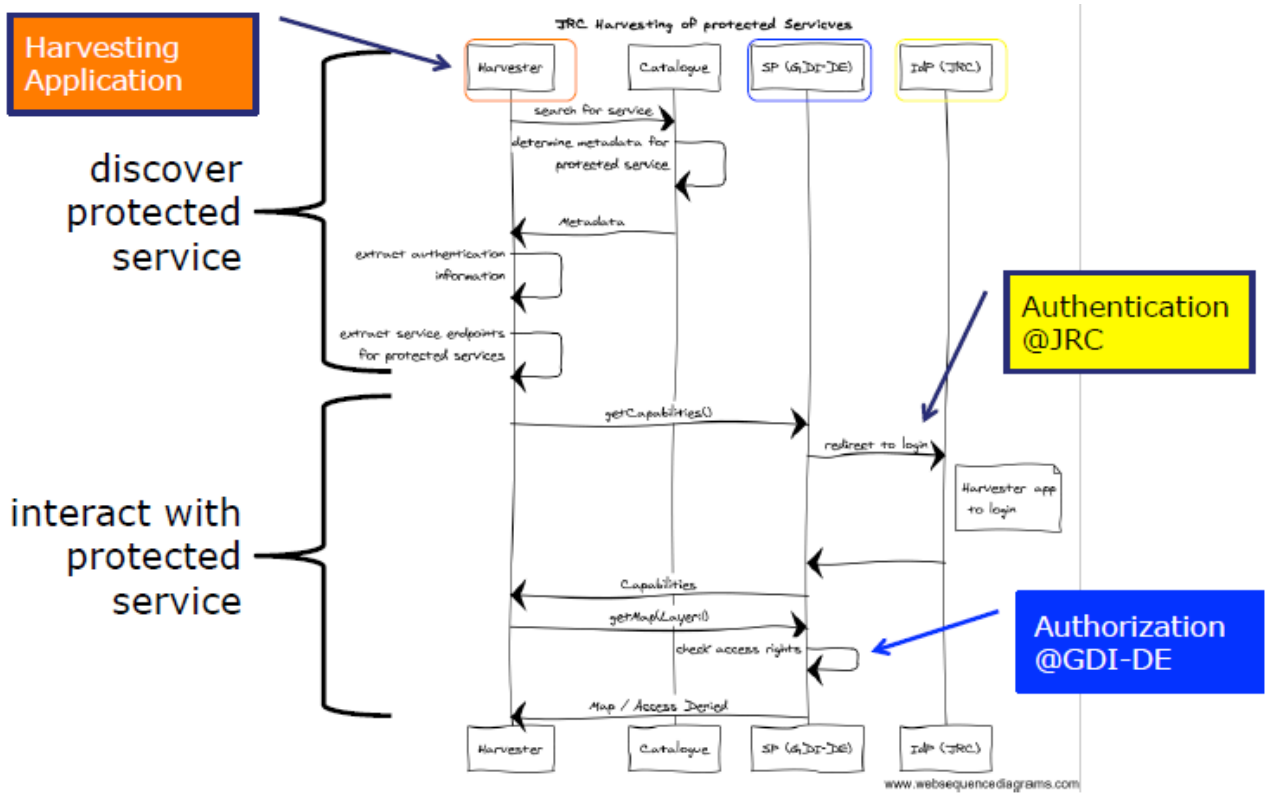

Figure 8: Access flow for the harvesting use case (e.g. for German services)

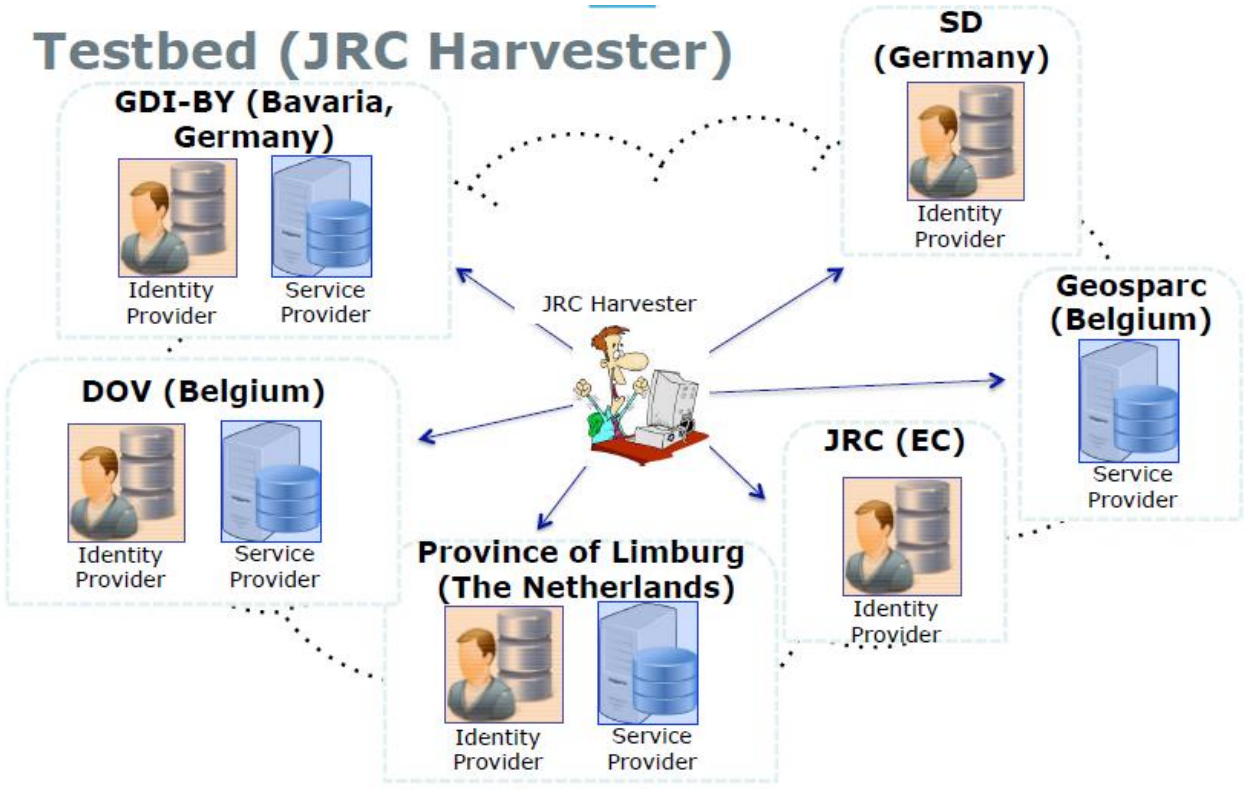

Figure 9: The JRC harvester use case and the testbed

How would an AAA mechanism work in the described use case? The harvesting application looks for services in the catalogues of Member States. It gets back the metadata for a particular protected service (e.g. from GDI-DE). The application needs to extract the authentication information and service endpoint(s) for the protected service(s). The application then starts to interact with the protected service, requesting getCapabilities() and is redirected to a login (authentication @ JRC). The harvester application then logs in and the protected service provides the Capabilities of the service. The harvesting application then asks for getMap(Layers). At that moment, access rights are checked (authorisation provided by GDI-DE) and accepted or not. It is assumed in this case that the JRC plays the role of the IdP. The architecture of the use case in the context of the testbed set-up is illustrated in Figure 9.

A number of topics are covered at the workshop and a set of experts has been identified (see Appendix I). As noted above, more details of the workshop activities following this preparation document are presented in the study's Deliverable about the workshop outcomes (*D2.4 – Results of the Workshop: 'AAA-Architectures for INSPIRE' 16-17 March, Leuven*).

5 References

De Lathouwer, B. (2013). Citizen Observatory Framework with Access Management Federation In GEOSS. ENVIP'2013 Workshop at the International Symposium on Environmental Software Systems (ISESS) 2013, Neusiedl am See, Austria, 10th October 2013. Available from: *http://www.slideshare.net/CobwebFP7/bd-l-envip2013*

European Union (2012). Advancing Technologies and Federating Communities: A Study on Authentication and Authorisation Platforms for Scientific Resources in Europe. Study carried out by a consortium led by TERENA.

Grohmann (2012). Access Management Federation for Spatial Data and Services in Germany, presentation at the OGC Tc, Austin, TX, USA.

Higgins, C., Koutroumpas, M., Matheus, A. and Seales, A. (2012). Shibboleth Access Management Federations as an Organisational Model for SDI. *International Journal of Spatial Data Infrastructures Research*, 2012, Vol.7, 107-124.

OGC (2012). Architecture of an Access Management Federation for Spatial Data and Services in Germany: *http://portal.opengeospatial.org/files/?artifact_id=47848*, an OGC White Paper edited by Andreas Matheus

Tinkl, W. and Pichler, P. (2014). Authentication, Authorisation, Accounting: Experience and Status in Austria, an Overview. Presentation at the ARE3NA Workshop on AAA for INSPIRE, 17-18 March 2014, Leuven, Belgium.

Vandenbroucke, D., Frigne, D., De Graef, P., Matheus, A. and Copier, R. (2014). Authentication, Authorization and Accounting for Data and Services in EU Public Administrations: D1.3 – Best Practices of AAA implementations.

6 Appendix I: agenda and interested stakeholders

Agenda

Monday 17 March 2014		
10:30-11:00	Registration, coffee and welcome	Danny Vandenbroucke (KU Leuven) and Dirk Frigne (geosparc)
11:00-12:00	AAA and the ISA Programme	
11:00-11:20	ISA: Secure solutions for public administrations	Miguel Alvarez Rodriguez (DG DIGIT)
11:20-11:40	STORK 2.0 Project Overview	Miguel Alvarez Rodriguez (DG DIGIT)
11:40-12:00	ARE3NA – Re-usable components for INSPIRE – AAA as a key layer of the INSPIRE architecture	Robin Smith and Michael Lutz (DG JRC)
12:00-12:30	Overview of standards and technologies related to AAA in the context of INSPIRE	Danny Vandenbroucke (KU Leuven) and Dirk Frigne (geosparc)
12:30-13:30	Lunch	
13:30-14:50	Experiences and Best Practices of AAA-implementations in Europe and requirements	
13:30-13:50	Secure access to spatial data for academia, the UK experience	Chris Higgins (EDINA)
13:50-14:10	Implementing secure network services in the Netherlands	Reijer Copier (IDgis)
14:10-14:30	The German experience	Andreas von Dömming (GDI-DE)
14:30-14:50	Secure access to spatial data from the sub-soil	Marleen Vandamme (DOV) / Tom Van Gulck (LNE-ACD)
14:50-15:30	Short interventions (5-10') of representatives from other experiences/projects of AAA implementations - Experience in France - Experience in Poland - Experience in Austria Possible requirements and discussion	Benjamin Cotasson (IGN-FR) Jacek Szczęsny (GUGiK) Peter Pichler (LFRZ)
15:30-15:45	Coffee break	
15:45-16:30	Set-up of the testbed for Authentication and Authorisation: introduction to a federated approach	Andreas Matheus (Secure Dimensions)
16:30-17:00	Open discussion on the proposed set-up for the test-bed	
17:00-17:30	Introduction to the breakout groups: presenting the challenges to be discussed, distributing the role/tasks within each group	Danny Vandenbroucke (KU Leuven)
Tuesday 18 March 2014		
09:30-10:30	2 breakout groups around two challenges of AAA-implementation	

10:30-11:00	Coffee break	
11:00-11:45	2 breakout groups around two challenges of AAA-implementation	
11:45-12:30	Short reports from the breakout groups and discussion	Rapporteurs breakout groups
12:30-13:30	Lunch	
13:30-14:30	Panellist discussing the challenges of a successful AAA implementation	Dirk Frigne (chair, geosparc), Michael Lutz (JRC), Miguel Alvarez Rodriguez (DIGIT), Alice Vasilescu (Deloitte), Andreas von Dömming (GDI-DE), Chris Higgins (EDINA)
14:30-15:15	Presenting the planning for the testbed taking into account the discussions in the breakout groups	Pieter De Graef and Andreas Matheus
15:15-15:30	Closing (with coffee)	Danny Vandenbroucke, Danny

Interested stakeholders

	Name	Affiliation	Attending	Country	e-mail
1	Robin Smith	EC JRC, IES	1	IT	robin.smith@ext.jrc.ec.europa.eu
2	Michael Lutz	EC JRC, IES	1	IT	michael.lutz@jrc.ec.europa.eu
3	Andrea Perego	EC JRC, IES	0	IT	andrea.perego@jrc.ec.europa.eu
4	Miguel Alvarez Rodriguez	EC DG DIGIT	1	BE	Miguel.ALVAREZ-RODRIGUEZ@ec.europa.eu
5	Dirk Frigne	GeoSparc	1	BE	dirk.frigne@geosparc.com
6	Frank Maes	GeoSparc	0	BE	Frank.maes@geosparc.com
7	Danny Vanden-broucke	KU Leuven	1	BE	Danny.vandenbroucke@sadl.kuleuven.be
8	Ann Crabbé	KU Leuven	0	BE	Ann.crabbe@sadl.kuleuven.be
9	Andreas Matheus	Secure Dimensions	1	DE	andreas.matheus@secure-dimensions.de
10	Reijer Copier	IDgis	1	NL	Reijer.Copier@idgis.nl
11	Herman Assink	IDgis	1	NL	herman.assink@idgis.nl

12	Marleen Vandamme	DOV, Flanders	1	BE	marleen.vandamme@lne.vlaanderen.be
13	Lieven Raes	CORVE	0	BE	lieven.raes@bz.vlaanderen.be
14	Tom Van Gulck	LNE-ACD	1	BE	tom.vangulck@lne.vlaanderen.be
15	Andreas von Dömmingen	GDI-DE	1	DE	andreas.doemming@bkg.bund.de
16	Markus Seifert	Bayern	1	DE	Markus.seifert@lvg.bayern.de
17	Machtelt Kusters	Province of Utrecht	0	NL	Not sure she is able to participate
18	Michel Grothe	Geonovum	0	NL	m.grothe@geonovum.nl
19	Alice Vasilescu	Deloitte	1	BE	alvasilescu@DELOITTE.com
20	Chris Higgins	EDINA	1	UK	chris.higgins@ed.ac.uk
21	Clare Hadley	Ordnance Survey	0	UK	Clare.Hadley@ordnancesurvey.co.uk
22	Ana Maria Piñuela Marcos	ATOS-ES	0	ES	*ana.pinuela@atos.net*
23	Damien Van der Eecken	NGI-BE	1	BE	damien.vander.eecken@ngi.be
24	Bart Rosseau	City of Ghent	0	BE	bart.rosseau@gent.be
25	Pieter De Graef	Geosparc	1	BE	*Pieter.degraef@geosparc.be*
26	Markus Jobst	BEV	0	AT	*Markus.jobst@bev.gv.at*
27	Jacek Szczęsny	Head Office of Geodesy and Cartography (GUGiK)	1	PL	*Jacek.Szczesny@codgik.gov.pl*
28	Benjamin Cotasson	IGN (France)	1	FR	*Benjamin.Cotasson@ign.fr*
29	Peter Pichler	Land, forst- und wasserwirtschaftliches Rechenzentrum Gesellschaft mbH (LFRZ)	1	AT	*Peter.Pichler@lfrz.at*
30	Tom Vijlbrief	Kadaster NL	1	NL	*tom.vijlbrief@kadaster.nl*
	TOTAL		20		