ISA Action 1.17: A Reusable INSPIRE Reference Platform

(ARE3NA)

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

D1.3 – Best Practices of AAA implementations

Danny Vandenbroucke

Dirk Frigne

Pieter De Graef

Andreas Matheus

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, 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: D1.3 – Best Practices of AAA implementations. European Commission; 2015. JRC94623

Table of Contents

List of figures

Glossary

AAA	Authentication, Authorization, Accounting
AAAI	Authentication, Authorization, Accounting Infrastructure
ACM	Access Control Management
AMF	Access Management Federation
CUAHSI	Consortium of Universities for the Advancement of Hydrologic Science
DG Connect	EC Directorate General Communications Networks, Content & Technology
EEA	European Environmental Agency
ECP	Enhanced Client or Proxy
EDINA	Edinburgh University Data Library of the University of Edinburgh
eID	Electronic ID
ELF	European Location Framework
ESA	European Space Agency
ESB	Enterprise Service Bus
ESDIN	European Spatial Data Infrastructure Network
EU	European Union
FEDICT	Federal Body for ICT in Belgium
G2B	Government to Citizen
G2C	Government to Business
G2G	Government to Government
GA	Government Agency
GDI	Geodateninfrastructur (DE), Geografische Data Infrastructuur (BE)
GDI-DE	The Spatial Data Infrastructure of Germany
GEOSS	Global Earth Observation System of Systems
GIS	Geographic Information System
GUI	Graphic User Interface

HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICT	Information and Communication Technology
ICT-PSP	ICT Policy Support Programme of the EC
IDM	Identity Management
IGN	Institut Géographic National (France)
IdP	Identity Provider
INSPIRE	Infrastructure for Spatial Information in the European Community
ISA	Interoperability Solutions for European Public Administrations
JRC	Joint Research Centre
KML	Keyhole Markup Language
LDAP	Lightweight Directory Access Protocol
LDBV	Landesamt für Digitalisierung, Breitband und Vermessung
LNE-ACD	Environment, Nature and Energy Department of the Flemish Government, Central Data Management Unit
NASA	National Aeronautics and Space Administration of the USA
NESI^{2}S	Network to enhance a European Environmental Shared and Interoperable Information System
NMCA	National Mapping and Cadastre Agency
NPOC	National Point of Contact (INSPIRE)
OASIS	Organisation for Advancing Standards for the Information Society
OGC	Open Geospatial Consortium
OWS	OGC Web Service
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PVP	PortalVerbund Protocol , a specific Austria protocol for secure access
RFC	Request for Comments mechanism
SAML	Security Assertion Markup Language

SDI	Spatial Data Infrastructure
SEIS	Shared Environmental Information System
SOAP	Simple Object Access Protocol
SP	Service Provider
SSO	Single Sign-on
STORK	Secure idenTity acrOss boRders linked
TLS	Transport Layer Security
WFS	Web Feature Service
WMS	Web Map Service
WMTS	Web Map Tile Service
WS	Web Service
WSS	Web Service Security
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language

1 Introduction

This report 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. 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 a 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 report *"D1.3 – Best Practices of AAA implementations"* covers objective 2 of the project and is one of its key deliverables. As defined in the Terms of Reference, the report examines the state of play of key service and data-sharing activities in Europe that can be considered best practice regarding AAA implementations. 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 mechanisms. Chapter 2 describes briefly the method applied for collecting and analysing best practices in this context. Major examples of AAA mechanisms implemented in the geospatial and e-Government sectors are described in more detail in Chapter 3, covering several European countries. Chapter 4 analyses the different cases by comparing their key characteristics. In chapter 5 we describe some other (ongoing) initiatives at the European and global levels both from GI as well as other sectors, that are deemed to be relevant for defining an AAA approach in the context of INSPIRE. Finally, chapter 6 draws some conclusions.

2 Method

The selection of Best Practice was based on

- Experiences of consortium members in national and European projects;
- Complemented with selected practices from other Member States known through the activities of the INSPIRE Maintenance Group (MIG).

Also information from previous projects such as NESI²S (2008-2010), a Network to enhance a European Environmental Shared and Interoperable Information System in support of SEIS and the INSPIRE technical

evaluation exercise (2014) provided some useful references to activities related to access control in the context of SEIS and INSPIRE respectively (see also section 3.8).

The description of Best Practices was based on a template (see annex of this report) which covered the 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, authorisation and XML security standards, and technologies/tools used. The template included some commonly used standards, but also left room for listing other standards and technologies used.
- **Organizational set-up**, including a list of participating organisations as Service provider (SP) or ID provider (IdP), other organisations involved and a total number of organisations involved (if known). Specific organisational or legal measures seen as supporting the AAA implementation could be listed as well.
- A list of **technological and non-technological issues** encountered during the project and how they were resolved (if appropriate). Open issues that need particular attention could also be listed.

A total of 7 practices from 7 countries were selected, described and analysed. The information was collected in different ways. Firstly, the consortium partners filled the template for the projects in which they were involved themselves, in some cases with the support of participating organisations. Secondly, documents and online information were consulted to complete or describe some of the practices in a comparable way. Thirdly, 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.

3 Best Practices in different European Countries

Based on the template, several practices from different countries were collected and described. Some examples are from the e-Government/ICT sector, while others focus on the geospatial or INSPIRE context. We summarize them in the following sections.

3.1 AAA in e-Government (Austria)

The implementation of AAA in Austria is closely linked with e-Government activities (e-Government Bund-Länder-Gemeinden, 2014; Austrian Trust Federation, 2014). It is based on a series of use cases which in turn are based on a series of assumptions. The following use cases have been defined (Tinkl and Pichler, 2014):

1) Government Agency ***GA-B*** needs to have online access to application (**APP**) provided by agency ***GA-A***. Both agencies are legally independent.

2) GA-B maintains an internal provisioning system containing the identity and attributes of their personnel and their level of security clearance

3) Both GA-A and GA-B signed the trust framework agreement (Portalverbundvereinbarung).

The whole set-up is based on a process to establish trust:

1) GA-A publishes a set of roles that may have access to certain resources (or functions) in APP; e.g. "Query a person in the criminal register" or "Delete an entry of a person in the criminal register"

2) GA-A assigns a set of roles for APP to GA-B based on legal considerations

3) GA-B knows which employees are authorized to use roles on APP and assigns these roles in their system.

The mechanisms to support Government to Government (G2G) interactions are illustrated in Figure 1. Other use cases are defined as well, e.g. access from systems (non-human actors); logging for delegated access (application chaining); transaction accounting for paid transactions and online audit access (to show GA-A which has access in GA-B).

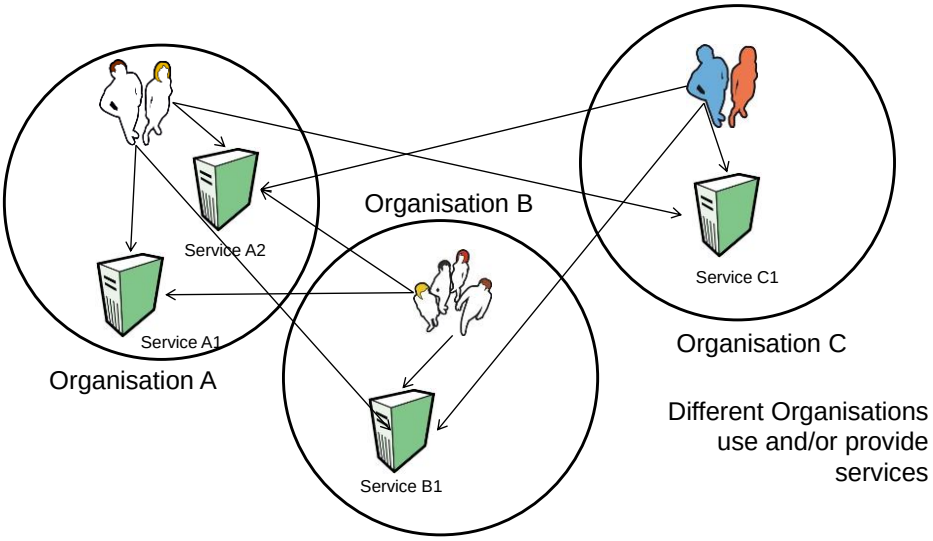

Figure 1: AAA-mechanism to support G2G interactions (Tinkl and Pichler, 2014)

The protocol implemented originally, was specific for secure access tasks in Austria, known as PVP 1.x (PortalVerbund Protocol), also called PVP R Profile based on Reverse Proxy that defined the following core items:

- PVP-Token: the data structure included in each authenticated transaction
- Protocol architecture: using reverse proxies for access control
- Protocol binding:
    - HTTP-binding (using custom HTTP-headers)
    - SOAP-binding (using a custom WS-Security token)
- Certificate Management

An important driver creating an Austrian governmental AAA infrastructure was the launch of the computer based Central Residence Register. In 2002, the first common specification of the technical protocol was

specified (PVP 1.4.1 and 1.5) along with the multilateral contract (PVP 1.0, which is still valid), allowing participants to trust each other and to define rights and obligations of IdPs and SPs. In 2004, many participants decided to develop a common software package for the Austrian Portal Federation. The PVP Standard portal was developed by the Ministry of the Interior and the LFRZ (an ICT company under the control of the Ministry for Agriculture), with the federation established in 2010. All ministries, federal state administrations and local community administrations can access the services of the federation. In addition, many specialised organisations can access the federation and/or provide services. The adoption of common AAA standards has allowed internal applications to be developed. The federated portal technologies have been reused for the organisation of portals for citizens. By 2010, there were more than 130,000 registered G2G users, and more than 600.000 non-G2G users. Millions of transactions are handled every day across the Austrian government, e.g. the Ministry of the Interior alone generating around 2 million transactions/day.

Since 2010, efforts have been under way to migrate the Portalverbund to industry standards, with SAML as the first protocol that has been implemented. The protocol specification is a deployment profile of the Kantara e-Government 2.0 Interoperability Profile based on the Web-Single-Sign-On Profile of SAML 2, called PVP2 S(AML) Profile (Tinkl and Pichler, 2014; Austrian Trust Federation, 2014). At the time of the workshop, i.e. March 2014, PVP2 was on its way to be integrated into production systems and work was done to develop central services required for a SAML Federation (e.g. central SAML metadata services) (Tinkl and Pichler, 2014). As a result, the federation is handling different protocols at the same time (see figure 2). This is possible as portal software converts different protocols and profiles, and as the services need not be updated, e.g. for the introduction of Version 2.0 of SAML.

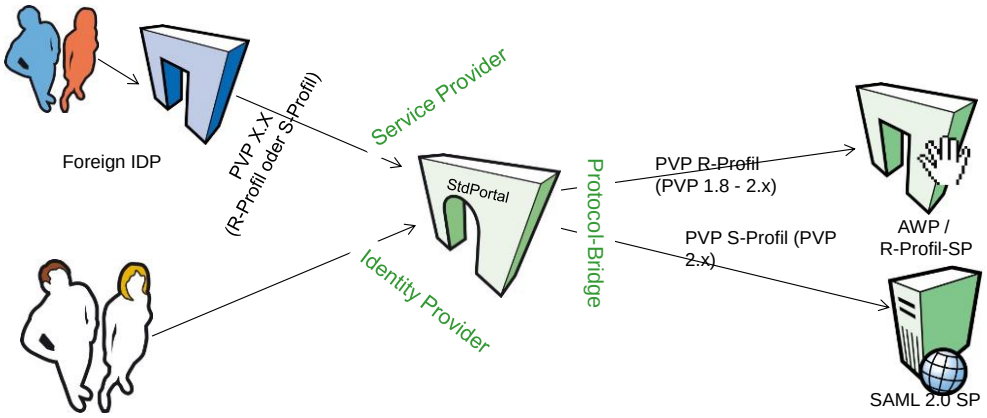

Figure 2: Handling different protocols and profiles (Tinkl and Pichler, 2014)

The federation will be extended to Government to Business (G2B) and Government to Citizen (G2C) types of interaction. The Trust Framework is in its elaboration phase. The goal is to establish Business to Business (B2B) and Business to Citizen (B2C) federations that are interoperable with the e-Government Federation. This will also include the Enterprise Service Portal being implemented by the federal government. The workgroup associated with this activity is operated by Austria Pro, an organization of the Austrian Chamber of Commerce.

The current architecture is used in applications around the INSPIRE services, namely a service and metadata editor, administration GUI and e-Commerce GUIs. The idea is to build up a central e-commerce platform for governmental data that have costs (e.g. not only some geospatial data, but also data from other government services), using PVP as a technical protocol between this payment platform and online services. An

example of a community that already frequently uses the secured INSPIRE services is the surveyors' community: they download spatial data sets by using a secure download service.

Currently 8 federal states are part of the federation (the 9th state has its own solution), along with the National Statistical Institute, the Environmental Agency and other public authorities.

3.2 LNE-Flanders (Belgium)

The Environment, Nature and Energy Department (LNE) of the Flemish Government is responsible for planning and evaluating environmental policy in compliance with economic and social demands and for the coordination of all environmental actors, as well as the implementation and enforcement of environmental legislation in Flanders. The Central Data Management Unit (ACD) is responsible for setting up an information system to manage all environment-related data. In this context, LNE-ACD has set-up an AAA-architecture to provide secure access to all their environmental information holdings, including data being served through several INSPIRE and other services. LNE-ACD plays the role of SP and the Federal ICT Agency (FEDICT) is the IdP. They are also owner and manager of the Access Control Management (ACM) and Identity Management (IDM) services.

LNE-ACD uses OpenAM, an open source access management, entitlements and federation server platform, as a SP for authentication and authorization. This OpenAM uses an OpenDJ Lightweight Directory Access Protocol (LDAP) for storing user information. Authentication on the other hand is provided by the Belgian ACM service (owned and managed by FEDICT), who acts as the IdP. The overall architecture is shown in Figure 3.

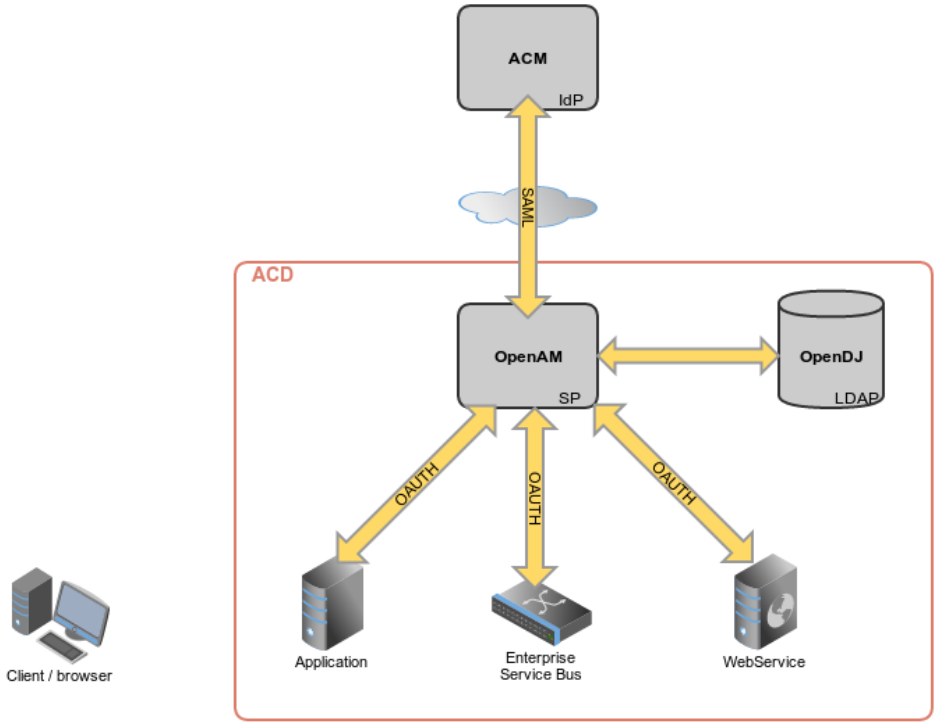

Figure 3: Overview of the AAA architecture of LNE-ACD (Best Practice Sheet LNE-ACD, 2014)

Behind the ACM system, there is an IDM, which is the actual user store[1] of the Belgian government. This IDM will push its content to the OpenDJ within LNE-ACD. When a user logs in, the ACM provides only limited data, as the OpenAM can search its local LDAP (e.g. for user roles, etc.). SAML is used for exchanging information on users between LNE-ACD and FEDICT. All the applications within ACD use the OAuth protocol to communicate with OpenAM. Most applications are also divided into a backend Web Service and a client application (providing a GUI). All Web Services are made available through an Enterprise Service Bus (ESB). If a user wants to log in to an application and access data, a sequence of steps are taken as can be seen from Figure 4.

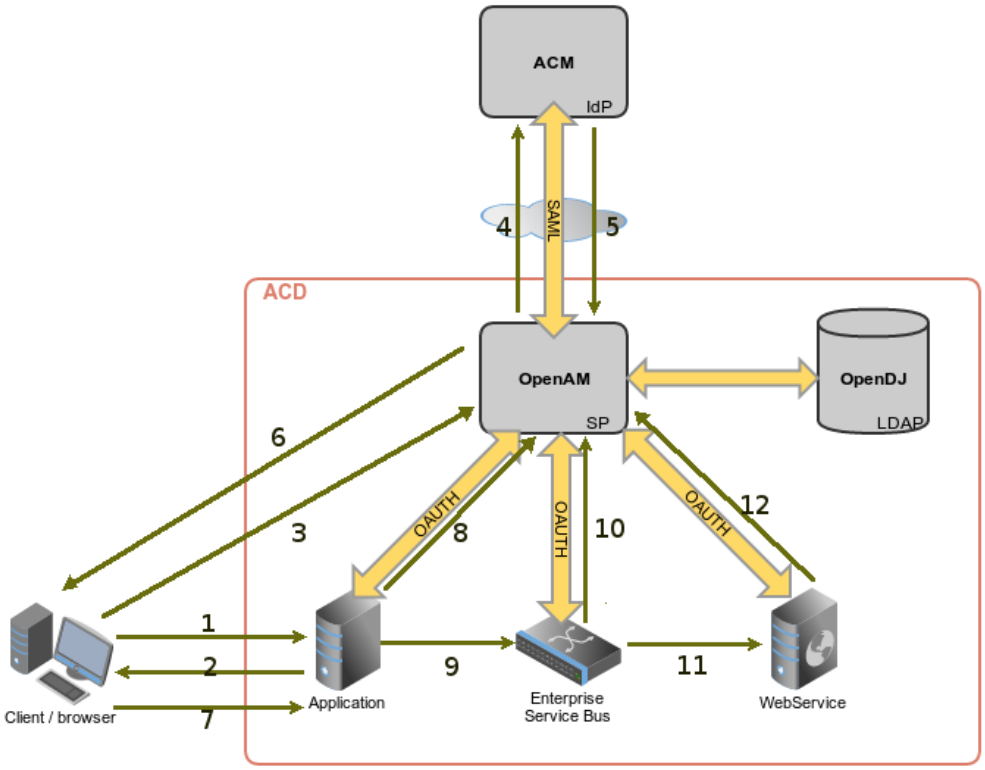

Figure 4: secure access to LNE-ACD data (Best Practice Sheet LNE-ACD, 2014)

Explanation of the arrows:

1. The user accesses the application. At this point he is not logged in.
2. The application will redirect the user to the OpenAM login page.
3. The user will then access the OpenAM login page.
4. OpenAM will, in turn, redirect to the ACM login page, using SAML.
5. Once credentials are provided, the user is logged in. ACM will let OpenAM know. At this point, the user has an active session, identified through a token.
6. OpenAM will let the user know.
7. The user can now access the application.

[1] Storing information about users (also using LDAP)

8. The application will check the token through the OAuth protocol to see if it is valid. If this is the case, then the user may be granted access (depending on the authorization rules in the application). It is assumed that the user has sufficient rights.
9. The application must access a resource from a Web Service (because the client application in ACD will not have DB access). It must go to the ESB, which acts as a proxy to the Web Service.
10. The ESB will, again, check the validity of the session, as it does not perform authorization.
11. The user has a valid session and, as such, is granted access to the Web Service.
12. The Web Service application will check the token through the OAuth protocol to see if it is valid. If so, the user is granted access to the Web Service. It is then up to the Web Service to verify authorization.

During the implementation, some lessons were learned. Firstly, it is recommended to work with experienced ICT/security experts, especially since integration between systems and environments requires customization and troubleshooting. Secondly, it is important to have a clear and common vision between the different SPs and IdPs. At the start of the project there were different visions between the LNE-ACD and FEDICT on the Authentication Attributes (SAML content) which required several discussions before consensus was reached.

3.3 GDI-DE (Germany)

The project "Betriebsmodell" (operating model) covered different aspects of how to operationalize a Spatial Data Infrastructure in Germany (von Dömming, 2014; Grohmann, 2012) as part of the work of the GDI-DE (the German national SDI). This included defining an organizational model which would provide protected services for geospatial data. In the timeframe of the project, an Access Management Federation (AMF) was established that served protected Open Geospatial Consortium (OGC) Web Services, which were, in turn, used by different kinds of applications. Figure 5 provides an overview of the AMF configuration.

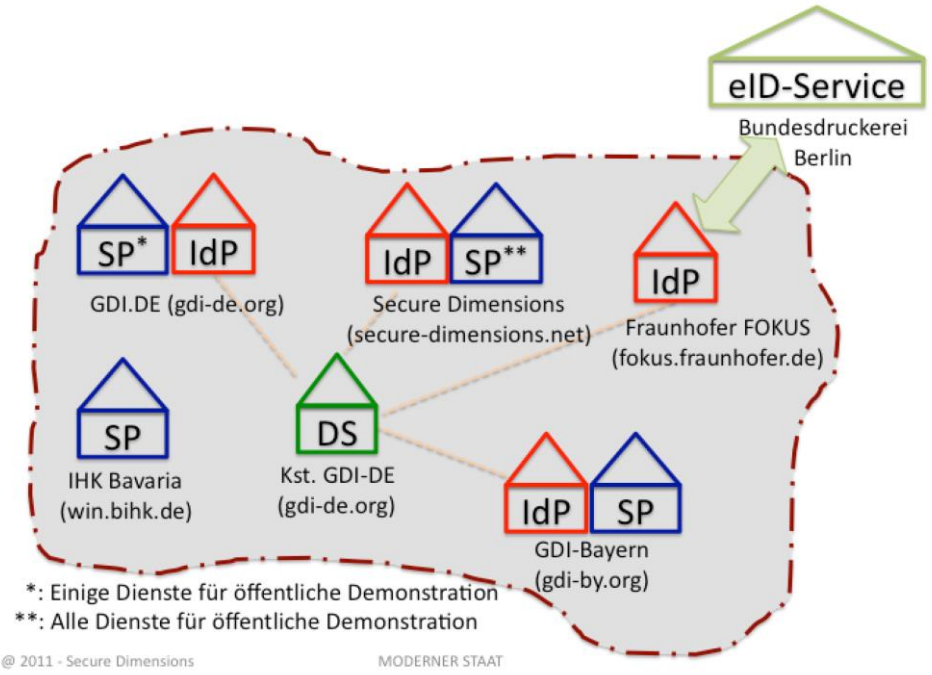

Figure 5: AMF of the project "Betriebsmodell GDI-DE" extended with German ID card authentication [some (*) or all (**) services used for public demonstration] (Grohmann, 2012)

The main government participants in the context of the AMF were the coordination office of the SDI in Germany and the Regional Authority for Digitalisation, Broadband and Survey, or LDBV (Landesamt für

Digitalisierung, Breitband und Vermessung) of Bavaria. The technology provider was Secure Dimensions, an SME active in the field of secure access to data. The authentication and Single-Sign-On was based on SAML and was realized by using Shibboleth technology. The authorization was realized by an implementation of GeoXACML. Basic IETF security standards were also used such as RFC 2818 (HTTPS), RFC 4346 (TLS 1.1), RFC 2617 (HTTP Authentication), RFC 2965 (HTTP State Management Mechanism), as well as standards from W3C such as CORS, XML Digital Signatures, XML Encryption. Other technology and tools used included: a SWITCH Discovery Service; LDAP (OpenLDAP); the set-up of a GeoXACML Policy Enforcement Point (PEP) as an Apache module and a GeoXACML Policy Decision Point (PDP) as a Web Service; and an OpenLayers based Browser mapping client as well as a QGIS based desktop mapping client. Figure 6 provides a detailed overview of the different modules at the SP side (von Dömming, 2014).

For the process of access control, two user attributes were provided by the Identity Providers:

- Organizational affiliation; the home organization of the user
- Role at the organization for participation in the federation

For German ID card users, other attributes were involved

- Organizational affiliation = DE
- Role = CITIZEN
- Surname as stated on the ID card
- First name as stated on the ID card

Figure 6 provides an example of a setup of an Access Control system based on an Apache Web Server. In terms of XACML information flow, the Reverse Proxy module acts as a Policy Enforcement Point (PEP). It is this module that will intercept requests and create GeoXacml compliant authorization decisions which is sent to Geospatial Policy Decision Point (geoPDP) based on a series of rules. When authorization is given, the request is forwarded to the service and the response is sent to the client (OGC, 2012).

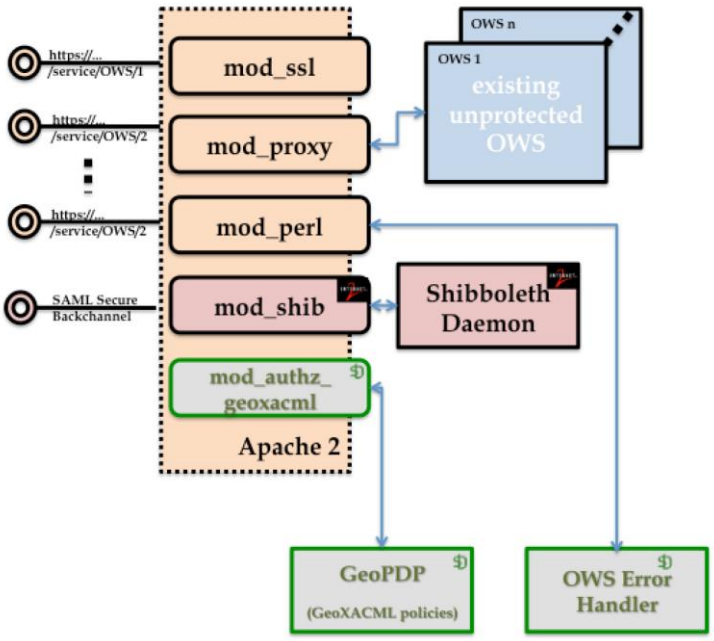

Figure 6: Modules of the Service Provider (WMS & WFS example) in the project "Betriebsmodell GDI-DE" (OGC, 2012)

Following German regulations on privacy, the user is warned that their names will be used by the application, along with the opportunity to deselect the provision of the name attributes. As a consequence, the user might have limited access to services of the federation.

Several organizational and technical issues emerged during the implementation. Firstly, some legal issues had to be solved to establish the Coordination Centre. Recommendations were formulated but not implemented as they were not within the scope of the project. High level tasks to establish the federation and maintain the list of trusted entities remain to be taken care of. In particular, it was found that the coordination centre must be setup in such a way that it enforces the policies and procedures of the federation. The Coordination Centre must also include a technical team to support users that need help. Secondly, some organizational issues emerged to determine the appropriate list of user attributes. In the end, the list of user attributes varies per use case, and a proper list has been agreed upon. Thirdly, there were some technical issues: e.g. it was not obvious that "direct" Single-Sign-On supporting OpenLayers type of clients was required. This was solved by using a Central Discovery Service and SAML Artefact Binding.

Detailed information about the project results are outlined in the OGC White Paper *"Architecture of an Access Management Federation for Spatial Data and Services in Germany"*.[2]

3.4 Geo-portal IGN (France)

IGN France implemented an AAA layer inside the French Geoportal (Cotasson, 2014). The motivation for the layer was based on the premise that IGN-France wants to know who uses the data and how, what data and services are used and how much the data is used (number of hits, amount downloaded). Furthermore, IGN wants to prevent the illegitimate use of its data. IGN has, therefore, developed a protection mechanism for data and services, focusing on the geo-portal and the interaction of the client with IGN. The link between the user (use) and IGN (data/services) is defined through a key. A filter defines the authentication, to control customer use, and authorization, to control what data and services are used. A table links the requested data/services with information on the type of protection (from no protection to high protection requiring a user name and password) and the validity period. A database stores statistics on the use of the data and services (per month, hour and even more detailed). No standards are used. The system is based on IGN's own developments.

[2] *http://portal.opengeospatial.org/files/?artifact_id=47848*

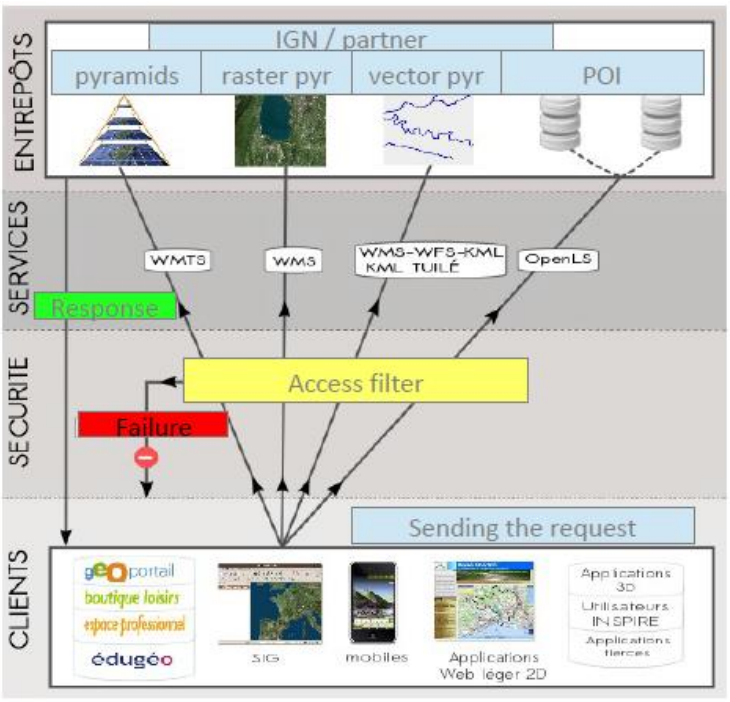

Figure 7: Architecture of the French geo-portal (Cotasson, 2014)

Figure 7 provides an overview of the AAA-layer as part of the geo-portal architecture, while Figure 8 shows the filter and key mechanisms. The Access filter is steering the authentication and authorization. It is situated between the data/service layer and the client (API/portal) layer. A 'keys' database contains information on the context of use, i.e. type of protection for each resource (data/service). The keys are managed through an application and a statistics database contains information on access by the users.

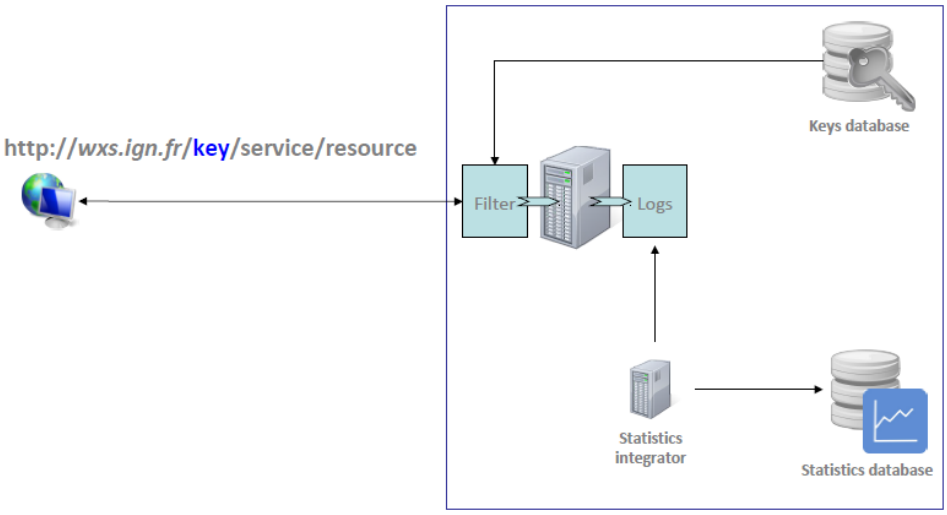

Figure 8: The IGN AAA mechanism is based on the use of a key (Cotasson, 2014)

On the organisational side, one administrative team manages the process. They publish / control the data, and provide rights management to manager teams that provide keys: they propose keys for development / testing sites / apps, for the production environment (e.g. IGN professional shop), for production of specific sensitive data (e.g. spatial orthoimagery: Geosud) and, in the future, for mobile applications (iPhiGéNie).

3.5 Province of Limburg (The Netherlands)

The purpose of the system "Concept Plannen"[3] is to share (still confidential) draft land use plans in a secure manner between various organizations involved in spatial planning within the province of Limburg (Copier, 2014a). The system comprises of three modules: secured OGC WMS/WFS services, a viewer which is complemented by a reporting system and an admin console to upload plans and to configure security constraints. Users can upload their spatial plans and enable other users (e.g. from other organizations) to access these plans. The security constraints are implemented in such a way that authenticated users are never aware of plans that they are not authorized to access. Performing a WMS GetMap or WFS GetFeature request results in a map or a feature collection including only information of spatial plans its owner explicitly granted the authenticated user (or group) access to. The configured security constraints are applied by filtering the data that the services retrieve from the database. All users share a single application instance that contains a single database with user and access constraints information (Copier, 2014a).

The access mechanism was set-up by IDgis BV, a Dutch SME active in the geospatial field. Besides the Province of Limburg, several municipalities took part in the project based on an informal commitment.

Authentication standards were entirely based on HTTP. No authorization standards were used. The authorization system is entirely custom built and complemented by using existing tools such as: PostgreSQL and a custom 'visibility' rule system; the open source tool deegree which was modified to utilize the access constraints implemented in the database and Spring Security. Figure 9 depicts the overall architecture of the AAA set-up.

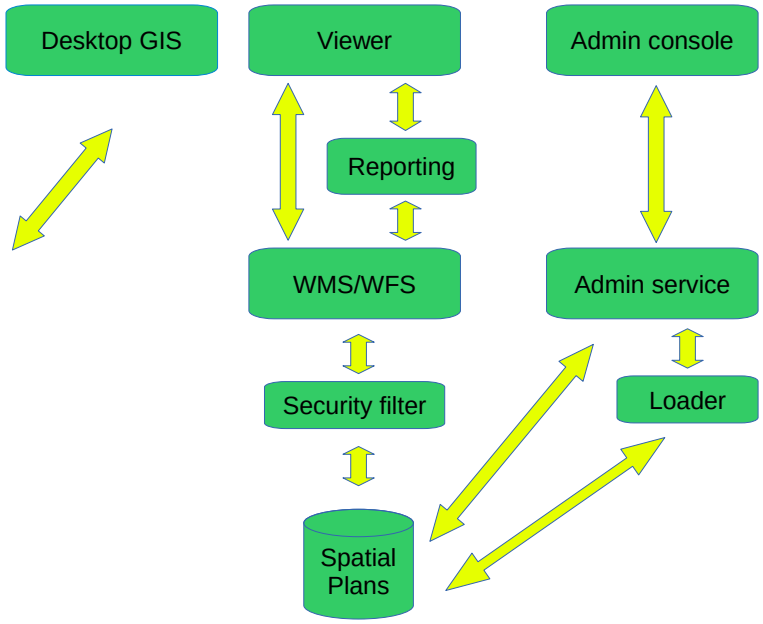

Figure 9: Architecture of the AAA implementation for the Province of Limburg (Copier, 2014b)

Several issues were raised during the project's life time. Firstly, it was found that a reporting system was needed as part of the solution performing requests on the secured services on behalf of an authenticated user in order to enforce the same security constraints. This was solved by placing the reporting system and

[3] These are similar to land zoning plans or land use plans.

the secured services within the same 'realm' and having the reporting system copy the received authorization header into the request sent to the secured service. Secondly, it was not obvious how to integrate a mechanism to instruct deegree to only disclose a subset of the data. This was solved by defining a wrapper around the jdbc driver that was taking care of the security constraints (Copier, 2014a).

3.6 Secure service access via the geo-portal (Poland)

The Polish geo-portal provides access to spatial data sets and services. Some of the services are protected. Several authentication methods are available (Szczęsny, 2014).

- WSS - A WSS activates a web security interface. This is required when users want to use the security gateway or in case of licensed data.
- Httpauth – Activates basic HTTP authentication enabling full support for a secured ArcGIS server within ArcMap.
- SAML – Activating SAML 1.0 tokens via a HTTP header or request parameter (not active anymore).
- Guest – activates the guest account.
- Token – Activates the native Security Token Service Support.
- SSO – Activates the Single Sign-on support.

Three monitoring solutions were also integrated: including a monitoring service (Oracle Service Bus), AWStats[4] and Nagios[5].

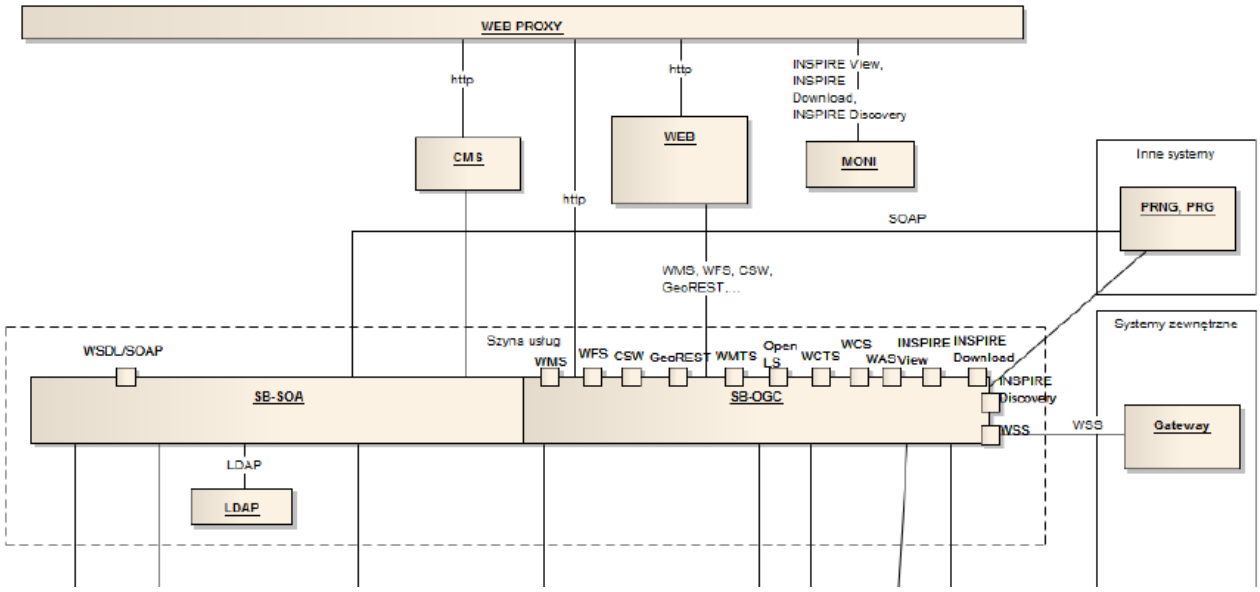

Figure 10: The Polish SDI architecture elements for an AAA layer (Szczęsny, 2014)

The project identified issues, including the replication of the Security Manager configuration; an overflowed alert database (BAM) which only works with outdated versions of Internet Explorer (v7-8); the management of ORACLE applications requiring several people; and a need to optimize the LDAP.

[4] http://www.awstats.org/

[5] http://www.nagios.org/

3.7 ESDIN and OGC OWS IE (Europe, UK)

In the context of the European Spatial Data Infrastructure Network (ESDIN) project and several OGC Web Service (OWS) Interoperability Experiments, an AMF based solution making use of Shibboleth was set-up and tested extensively between 2010 and 2012 (Higgins, 2012). It was found that Shibboleth provides a standard based, open source, interoperable mainstream IT solution implementing AMFs around the OGC Web Services (OWS) that are part of today's SDI's. Furthermore, it has been demonstrated (using a prototype federation of INSPIRE compliant services) that this can be done without modifications to either mainstream Shibboleth or OWS. However, it was found also that non-browser based clients require adaptation.

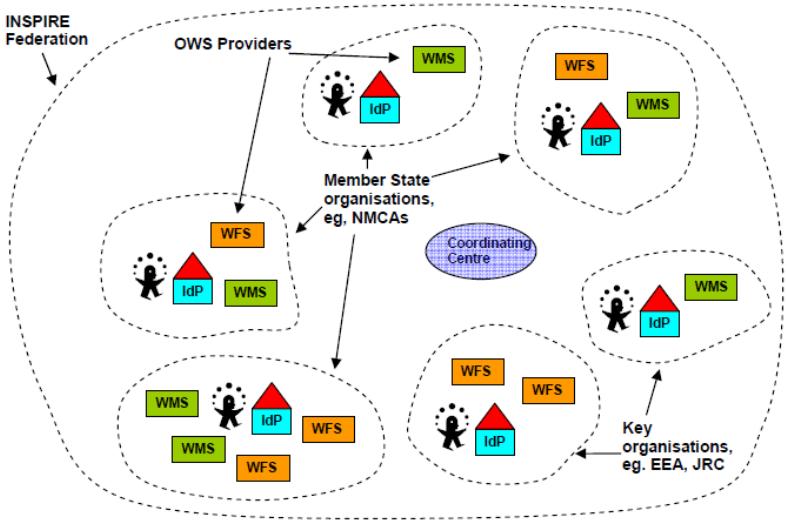

Figure 11: A Possible Evolution for the ESDIN Federation (Higgins, 2012)

Various options exist as to how the main actors within a European SDI/Federation may organise themselves in order to realise the objective of allowing authorised users from key organisations, e.g., EU bodies responsible for environmental policy, seamless access to harmonised protected geospatial information through OWS. In the ESDIN project, a 'simple' pan-European AMF was set-up involving INSPIRE NCPs, who are often National Mapping and Cadastral Agencies (NMCAs), acting as SPs serving WMS or WFS. The role of the coordinating centre was played by one of the partners of the consortium, while several partners played the role of IdP (see Figure 11).

The aim of the Authentication Interoperability Experiments was to test standard ways of transferring authentication information between OGC clients and OGC services by using existing standards and technologies. The following protocols and mechanisms were tested: HTTP Authentication, HTTP Cookies, SSL/X509, SAML, Shibboleth, OpenID and WS-Security. Two SAML profiles were taken into account during the experiments, namely the Web Browser SSO Profile and Enhanced Client or Proxy (ECP) Profile. EDINA, one of the partners in the project, developed and demonstrated two clients: one desktop (based on OpenJump) implementing the SAML Enhanced Client or Proxy (ECP) Profile (OASIS, 2005) and one browser based (OpenLayers) implementing the SAML Web Browser SSO Profile. Several software providers tested their software and made some modifications in order to integrate the SAML/Shibboleth solution: EDINA, Snowflake, Cadcorp, Envitia, con terra and the Joint Research Centre. The software producing participants in the OWS Shibboleth IE modified their clients in weeks, not months, and several are making their modified software commercially available.

Organisational issues that were raised during the projects relate to the way the federation should be organised. Firstly, several options could be chosen, such as one federation with one organisation in each country responsible to implement the federation, i.e. the INSPIRE NCP would join the single pan-European federation and act as the gateway for all the other legally mandated organisations in the country that are standing up INSPIRE services. Secondly, secure access mechanisms are complex to implement and it is difficult to understand important issues without being deeply involved in the internet security community. Thirdly, one of the main challenges relate to privacy issue and how user identity information should be managed.

The project also defined some areas for further research and testing. Further investigation and testing are needed for different types of service chaining. The project only tackled "transparent" chaining (i.e. where the user knows the details of the services being invoked) but "translucent" and "opaque" chaining (where the user invokes a service that in turns invokes a number of other services) are likely to increase in importance. More research in and testing in inter-federation interoperability is needed. Individuals might belong to more than one federation and it is likely that, as federated approaches expand, this will become more common. Finally, the perceived complexity of SAML is one of its strengths as well as one of its weaknesses. It allows for great flexibility enabling a wide variety of use cases and various profiles may be supported with individual SAML components able to be used in isolation. This complexity and the use of different profiles need to be taken into account when setting-up an AMF.

3.8 Other activities related to access control

NESIS[2] (2008-2010), a Network to enhance a European Environmental Shared and Interoperable Information System, was a project under the ICT-PSP Programme that aimed to promote the uptake of ICT solutions by public authorities in order to enhance environmental monitoring and reporting mechanisms. The Network aimed to support the creation of a Shared Environmental Information System (SEIS[6]) by providing a coherent framework to consolidate existing best practices. In the context of the project, ICT developments in the environmental sector were analysed in 12 countries and used as input to define a roadmap for SEIS. The project revealed that although most of the environmental information is shared and made accessible without any restriction, some countries implemented some access control mechanisms, especially to support secure exchange of information between businesses and government (e.g. with regard to waste). In most cases, this was limited to the implementation of simple authentication mechanisms using HTTPS (e.g. Austria, Czech Republic, Italy, Lithuania, Malta and Norway).

The INSPIRE technical evaluation aimed to test the existing INSPIRE components such as metadata records and services reported by the Member States and searchable through the European INSPIRE portal or through national/regional/thematic portals. The analysis, which was carried out in the Spring of 2014, revealed that several Member States are developing access control mechanisms to protect their view and download services (WMS, WFS). Although the evaluation exercise did not collect detailed information on the standards and technologies used, it established which Member States are active in this field, namely Austria, Finland, Czech Republic, Germany (some Länder), Lithuania and Latvia. Although access control mechanisms are mostly developed to protect download services (WFS), also viewing services (WMS and WMTS) also have some forms of access control, in particular for monitoring purposes.

[6] See *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52008DC0046*

4 Analysing Best Practices

It is not possible to provide a full benchmarking or even full comparison of the different Best Practices. The objectives, scope and approaches are too different from each other to do this. However, it is possible to compare some of the characteristics of the different practices, i.e. the application (or not) of standards, the different standards implemented, the technology or environments used, as well as whether secure access mechanisms have been set-up for OWS and, if so, which ones and which specific clients were used for accessing the secured services. Furthermore, we can also compare the best practices from the organisational point of view and analyse the issues that were raised, including those still open or solved.

Table 1 provides an overview of the standards, tools, applications and services involved.

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	✓	✓
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	✓	✓

From the table and the description of the best practice cases examined, we can make several observations:

1. Some of the projects start from the objective to set-up an AMF to be able to have secure access to (OGC) web services, with a focus on having a Single Sign-on mechanism to access the services in a cross-border and cross-organisational context. The focus is, therefore, on the authentication (by the IdP) and, to a certain extent, also on the authorization aspects (by the SP). Other projects, such as the examples of IGN France and of the NMCA of Poland, have different goals. Their objective is to better know who is using their data: *"allows the IGN marketing service to better know which type of customer (Web site mobile or GIS context) uses which data or which service (e.g. WMS / WMTS) on the Geoportal platform"*. In the context of this study, the focus is not on accounting but, rather, on authentication and authorization.

2. Several projects tried to deal with the use of different type of clients to get access to secure services: mobile applications, web mapping applications or desktop applications. While the first two do not pose too complex problems, it can be seen that desktop applications, by their nature, need to take precautions (workarounds need to be found) in order to guarantee security on the local desktop. This development, specific to the application, should be undertaken by software providers to ensure secured encryption of data. As a consequence, the focus of the testbed in this study will not develop desktop applications but could provide specific recommendations for varying software providers. The OGC web services covered in the different projects are WMS and WFS.

3. Almost all projects use basic security standards of HTTPS and WS-S, with many of them also using SAML. LNE-ADC combines SAML to exchange information on attributes with the IdP, with OAuth to exchange information between the applications/service(bus) and the SP. OpenID has been used to grant access to individuals in the OGC Interoperability Experiments, while the Austrian PVP standard will be extended with an OpenID[7] profile. LDAP is used to store information about users. Finally, Shibboleth has been used in three cases to help the implementation of a SAML based approach.

The projects also revealed several organisational issues. The most important ones are:

1. Implementing an AAA layer to guarantee secure access is a complex process. It is recommended that ICT experts that know the security domain very well are involved in this process. It is also recommended that a budget is foreseen to support this, as AAA is not a job to be done in-between other duties, instead requiring dedicated staff and technical resources.
2. Where an AAA-architecture is being implemented in a country that has many levels of authority and/or many partners, it is necessary to set-up only one Coordination Centre for the whole 'INSPIRE-federation' (or reinforce an existing organisation who would play this role) to manage the federation, including the maintenance of the metadata about the SP and IdP. To streamline the cooperation between all the relevant stakeholders, it is also recommended to set-up agreements to fix the roles and tasks in the federation.
3. It is also necessary that when the geospatial wants to implement an AAA-architecture to grant secure access to OWS, it is important that they cooperate with the specific agencies or bodies that are responsible for ICT (security) (potentially at organisational, regional or national levels), including those that deal with ISA-related AAA tools such as eIDs and STORK implementation.
4. In order to simplify an AAA implementation (and in some cases to be conformant with EU and national legislation regarding privacy), it is necessary to minimize the attributes to be transferred between SP and IdP.

[7] In the description of the standard PVP Version 2 (general part) it is stated that besides the PVP R Profile, the PVP S Profile, two other profiles will be developed: PVP X Profile and PVP O Profile. The latter is a profile based on the OpenID protocol. Arguments to do so are 1) the OpenID protocol is implemented in many existing products and 2) SaaS services often offer the protocol as well.

5 European and Global initiatives

There are several ongoing initiatives at the European level that are studying or implementing AAA solutions. We describe a study and its findings performed in the context of the broad research communities aiming at providing a distributed virtual environment to store, access and share scientific resources. We also examined the European Location Framework, which will deliver a pan European cloud platform and a series of web services to enable access to harmonised data in cross-border applications based on INSPIRE components developed by the Member States.

5.1 Authentication and Authorisation for Scientific Resources

Scientific research has become, over the years, extremely data intensive and increasingly multi- and interdisciplinary, international and real-time (European Union, 2012). Data produced by the research community are heterogeneous, as is the demand to store, access and preserve them. Today, scientific and other users have access to an unprecedented amount of scientific (big) data. However, this raises questions regarding data quality, persistency, preservation, authenticity, privacy and copyright. To answer these challenges, scientific data infrastructures[8] require new types of access control and security, just like other sectors of society.

In 2011, the DG Communications Networks, Content & Technology (DG Connect) initiated a study to evaluate the feasibility of an integrated Authentication, Authorisation and Accounting Infrastructure to support the development of a robust platform to preserve, access and share scientific information at the European level. The study analysed the user access requirements of the different scientific communities, assessed the state of play of existing AAA infrastructures based on a series of use cases, and carried out a gap analysis between the requirements and the infrastructures in place.

The requirements analysis showed the need for an AAA infrastructure that facilitates collaboration and at the same time preserves ownership and authenticity of data. The analysis also showed that scientific users would like to use their institutional credentials to access data and services from their peers. Moreover, more and more scientists also use social media to share and access information. The work uncovered several requirements (European Union, 2012), such as:

- AAA infrastructures should enable Single Sign-On across services;
- Enhance authorisation to support attributes should be provided not only by users' home organisations but also by research communities;
- Allow the utilisation of the shared facilities of large datacentres for trusted data depositing and processing, with guaranteed data and information security;
- Support different types of credentials and provide ways to translate them to access different systems;
- Support simplified and seamless access to both licensed information resources and Open Access.

The second part of the study focused on the assessment of existing AAA infrastructures such as eduGAIN, eduroam and several examples of Grid and Cloud infrastructures. This included the underlying technologies

[8] Sometimes scientific data infrastructures are abbreviated as SDI. We will not do this in this report because of the use of SDI as an acronym for Spatial Data Infrastructures.

and standards, and the use-cases they support. The assessment resulted in some important conclusions (European Union, 2012) that might be relevant for an AAA-approach for INSPIRE:

- All infrastructures evaluated provide Single Sign-On for the users, although the technology used varies: SAML for Identity Federations, 802.1X + RADIUS for eduroam, X.509 certificates for EGI, PRACE and most of the e-Science infrastructures.
- No single AAA technology can be adopted universally, but there should be mechanisms in place to allow for the integration of different technologies. The current trend in the research network environment is to converge Grid identity infrastructures (based on X.509 certificates) and NREN-operated identity infrastructures based on RADIUS and SAML and to explore the application of technologies based on secure tokens, such as OAuth and Security Token Services (STSs).
- Authorization requires mechanisms for the aggregation of identity data (attributes) for authorisation decisions. This is particularly challenging in a heterogeneous environment and it is often implemented via complex systems. There is consensus that current AAA Infrastructures should evolve to support external attribute authorities that will be in charge of providing the information about the users, rather than relying solely on Identity Providers.
- Accounting remains one the weakest aspects of most of the considered AAA Infrastructures (with the probable exception of some Grid AAAIs). There seems to be consensus that service-oriented architectures can hide complexity while offering rich mechanisms, including better support for accounting.

The study ends by providing some recommendations, for example:

1) Promote the widespread use of existing standards for federated access control;
2) Enhance existing AAA Infrastructures to address the needs of research communities for accessing different types of services in a secure way (e.g. mobile access, use of guest IdPs);
3) Enhance authorisation in inter-federation scenarios through distributed attribute management;
4) Phase-out IP-based authentication;
5) Harmonise attributes.

The study provided legal and organisational conclusions and recommendations, which could be useful inputs for the analysis phase of the AAA approach for INSPIRE.

5.2 European Location Framework (ELF)

The European Location Framework is a project under the ICT-PSP Programme running for three years from 2013-2015. The objective is to provide up-to-date, authoritative, interoperable, cross-border, reference geographic information for use by the European public and private sectors. The project brings together 30 participating partners into a collaborative consortium including national and regional mapping and cadastral agencies, software developers, application providers, research and academia.

In order to provide secure access to the services developed in the context of the ELF, an AAA approach has been set-up based on previous experiences of some of the participating organisations, as well as an analysis of existing practices. The work is part of broader discussions, including for data policies and Digital Rights Management in the context of the ELF. Indeed, in SDIs and even in INSPIRE, not all web services are necessarily 'open' in the sense of either 'open access' or 'free of charge'. There are a number of reasons

why a service might be 'protected' - data security, data sensitivity, IPR licensing, charging, performance management and marketing. Eurogeographics (2014) see such issues related to licensing and access resting in how to address them in an interoperable way.

From that perspective, the ELF is also looking into standards and technologies for AAA mechanisms. ELF is starting from the experience of the Finnish-led Oskari platform which follows a centralised user management approach: the user names and passwords are stored in the Oskari backend, managed by the Finnish Mapping Agency (NLS FI). In a next step, a federated system (in a first stage with some countries) will be setup, although the service provision will remain centralised. HTTP and SAML will be used for authentication, XACML and geoXACML for authorisation (see Figures 12 and 13).

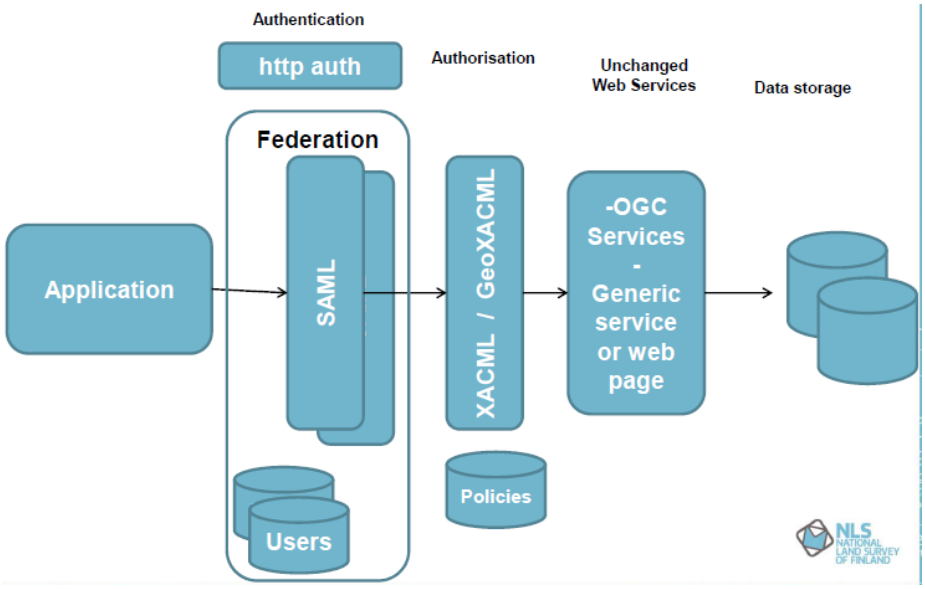

Figure 12: AAA Architecture for ELF (Reini, 2013)

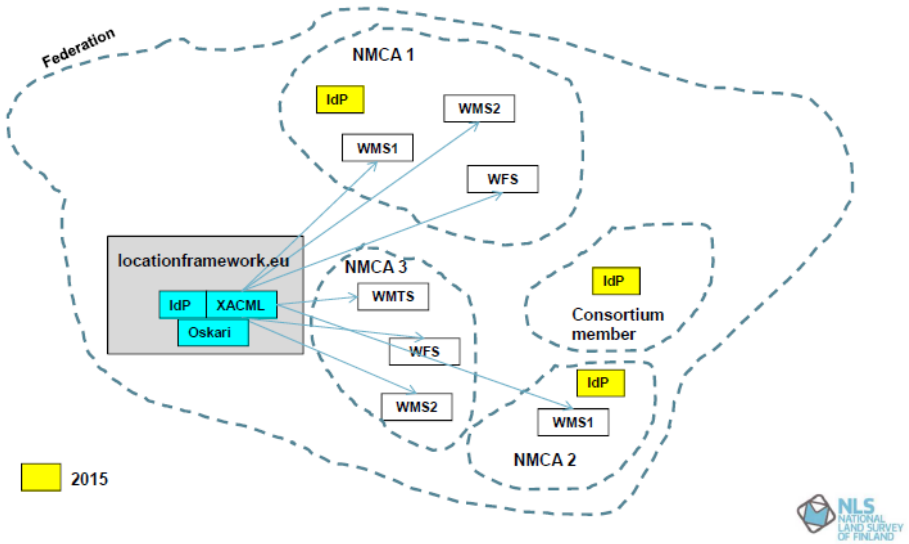

Figure 13: The ELF Federation with authorisation via XACML and spatial, layer and feature based restrictions

Several roles have been defined such as guest, user and administrator. Once the role is granted, certain access rights are granted as well. Access policies take into account, for example, the user, their role, the resources requiring access control (e.g. layers), the conditions (e.g. timeframe), the possible actions (e.g. GetMap), etc.

5.3 Activities in the context of GEOSS

The OGC is an active partner and contributor to the Global Earth Observation System of Systems (GEOSS) programme[9]. In that context, the Group on Earth Observations organises regularly GEOSS Architecture Implementation Pilots (AIPs). In the last pilots (AIP-5 and AIP-6) much attention has been paid to the implementation of AAA solutions. The work in this area is done as part of the European COBWEB project, a 7th FP project dealing with the creation of a Citizen Observatory Framework supported by an Access Management Federation solution (De Lathouwer, 2013). Several organisations are involved in the experiments, including:

- National Aeronautics and Space Administration of the USA(NASA)
- Consortium of Universities for the Advancement of Hydrologic Science (CUAHSI)
- GDI-DE
- European Space Agency (ESA)
- Secure Dimensions
- University of Edinburgh

SAML 2.0 is used a key standard for the IdPs and SPs, but also a trust OpenID gateway has been setup by the University of Edinburgh to test how the two standards can be jointly used. The use of OpenID in the GEOSS AIP project was based on specific requirements from the GEOSS head office that deemed OpenID was the only 'simple' and 'feasible' solution for many developing countries.

[9] https://www.earthobservations.org/geoss.shtml

6 Conclusions

In this report we analysed a selection of Best Practices with regard to AAA implementations, both in the context of INSPIRE and e-Government. The Best Practices were selected based on the knowledge of the consortium members, but also on the work done in previous projects such as NESIS and the INSPIRE technical evaluation which uncovered which Member States were most active in this field.

From the different practices, we can learn that some initiatives are focussing more on monitoring the users of the data and services, and what users are doing with the data (e.g. IGN France). However, in most projects, the focus is on access control. These initiatives usually setup an Access Management Federation (AMF) using SAML and (Geo)-XACML for authentication and authorisation, respectively. Examples such as the setup in Flanders (LNE-ACD) show that standards such as SAML can easily be combined with other open standards such as OAuth. This is also the case for the use of OpenID. Although we came to the conclusion in our analysis of existing AAA standards and technologies that OpenID has certain drawbacks (see Crabbé et al., 2014) they are not mutually excluding each other.

That is also one of the important findings of the study on AAA solutions for the research sector, as well as other initiatives that were briefly described in this report (e.g. the GEOSS Architecture Interoperability Pilots). No single AAA technology can be adopted universally, but there should be mechanisms in place to allow for the integration of different technologies. This confirms one of the assumptions made from the beginning of the ARE3NA project, i.e. to setup an AMF for INSPIRE that does not require existing access control mechanisms in Member States to change their architecture and the standards and technologies they use.

In the analysis documents we will come back to these conclusions in order to take them into account for the testbed and when formulating recommendations and guidelines for INSPIRE.

References

Austrian Trust Federation: *http://www.portalverbund.at/de/node/6* [Accessed on 2 May 2014].

Copier, R. (2014). Best Practice factsheet describing the implementation of an AAA-Architecture for Concept Plans for the Province of Limburg, The Netherlands.

Copier, R. (2014). Secured services in the province of Limburg (NL): How to share working drafts between spatial planners of different organisations, Presentation at the ARE3NA Workshop on AAA for INSPIRE, 17-18 March 2014, Leuven, Belgium.

Cotasson, B. (2014). AAA Layer inside French geoportal. Presentation at the ARE3NA Workshop on AAA for INSPIRE, 17-18 March 2014, Leuven, Belgium.

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*

e-Government Bund-Länder-Gemeinden: *http://www.ref.gv.at/Portalverbund.577.0.html*, Austria [Accessed on 2 May 2014].

De Graef, P. (2014). Best Practice factsheet describing the implementation of an AAA-Architecture in LNE-ACD, Flanders, Belgium.

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 Mattheus

Pflänging, P. and Hörbe, R. (2011). Portalverbundprotokoll Version 2: Algemeiner Teil.

Reini, J. (2014). Inspire KEN Service protection / AAA ELF.

http://www.eurogeographics.org/sites/default/files/INSPIRE-KEN-ServiceProtection-ELF.pdf

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.

von Dömming, A. (2014). Best Practice factsheet describing the implementation of an AAA-Architecture in GDI-DE, Germany.

Annex: template to describe Best Practices

<table>
<tr><td colspan="3">Abstract

Describe in not more than 10 lines what the implementation provided (focus should be on solutions for Authentication and Authorization). The text should stand on its own and provide a good overview of what has been done, how it was done and who was involved. Details about other aspects of the project (if it was part of a bigger project) should not be given …

(might be complemented with illustrations, e.g. architecture diagrams)</td></tr>
<tr><td colspan="3">Standards and technologies</td></tr>
<tr><td colspan="2">Standards applied</td><td rowspan="2">Technologies applied

Provide here in the form of a bullet list which technologies and tools were applied and/or developed (e.g. Shibboleth)</td></tr>
<tr><td>Authentication standards
❑ LDAP
❑ Kerberos
❑ Other
……
Authorization standards
❑ XACML
❑ geoXACML
❑ Other
……</td><td>XML Security standards
❑ SAML
❑ Other
Other standards</td></tr>
<tr><td colspan="3">Organizational aspects</td></tr>
<tr><td colspan="2">Stakeholders involved

Provide here in bullet form the organizations involved (data providers, service providers, ID providers, …), as well as the overall number of participating organizations</td><td>Organizational and legal measures

Describe here briefly if and which specific organizational/legal measures were taken</td></tr>
<tr><td colspan="3">Issues encountered</td></tr>
<tr><td colspan="2">Problems/issues encountered

Provide here in bullet form the problems and issues encountered. This might be specific problems related to the implementation of the standards, the technologies, as well as legal/organizational problems.</td><td>Solutions found

Provide for each of the problems/issues mentioned in the left column if and how they were resolved; indicate if it has not been resolved and remains an open issue</td></tr>
</table>