ISA Action 1.17: A Reusable INSPIRE Reference Platform

(ARE3NA)

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

D2.4 – Results of the Workshop: 'AAA-Architectures for INSPIRE' 16-17 March, Leuven

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 D2.4 – Results of the Workshop: 'AAA-Architectures for INSPIRE' 16-17 March, Leuven . European Commission; 2015. JRC94731

Table of Contents

Glossary

AAA	Authentication, Authorization, Accounting
ACM	Access Control Management
ADMS	Assets Description Metadata Schema
AIP	Architecture for Interoperability Pilots
AMF	Access Management Federation
ARE3NA	A Reusable INSPIRE Reference Platform (ISA Action 1.17)
ATOM Feed	IETF RFC 4287 The Atom Syndication Format
BAM	Business Activity Monitoring from Oracle
CIRCABC	Communication and Information Resource Centre for Administrations, Businesses and Citizens
COBWEB	Citizen Observatory Web
CORDIS	Community Research and Development Information Service
CSW	Catalogue Service for the Web
DCAT	Data Catalogue Vocabulary
DG DIGIT	Directorate General for Informatics
DSS	Digital Signature Software
EC	European Commission
ECAS	European Citizen Action Service
ECP	Enhanced Client or Proxy
EDINA	Edinburgh University Data Library of the University of Edinburgh
ELF	European Location Framework
eID	Electronic ID
ESDIN	European Spatial Data Infrastructure Network
eTrustEx	Document exchange platform of the EC
EU	European Union
G2B	Government to Citizen

G2C	Government to Business
G2G	Government to Government
GDI	Geodateninfrastructur (DE), Geografische Data Infrastructuur (BE)
GDI-DE	The Spatial Data Infrastructure of Germany
GEOSS	Global Earth Observation System of Systems
GI	Geographic Information
GIS	Geographic Information System
GUGiK	Head Office of Geodesy and Cartography, Poland
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICT	Information and Communication Technology
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IDM	Identity Management
IGN-BE IGN-FR	Institut Géographic National (France and Belgium)
IdP	Identity Provider
INSPIRE	Infrastructure for Spatial Information in the European Community
ISA	Interoperability Solutions for European Public Administrations
JRC	Joint Research Centre of the European Commission
LDAP	Lightweight Directory Access Protocol
LFRZ	Land-, forst- und wasserwirtschaftliches Rechenzentrum GmbH
LNE-ACD	Environment, Nature and Energy Department of the Flemish Government, Central Data Management Unit
MOA	Modules for Online Applications
NGO	Non-Governmental Organisation
OGC	Open Geospatial Consortium
OSI	OGC Web Services Shibboleth Interoperability Experiment

OWS	OGC Web Service
PID	Persistent Identifiers
PVP	Is a specific Austria protocol for secure access
RDF	Resource Descriptor Framework
SAGA	Standards and Architectures for E-Government-Applications
SAML	Security Assertion Markup Language
SDI	Spatial Data Infrastructure
SME	Small and Medium Enterprise
SOS	Sensor Observation Service
SP	Service Provider
SSO	Single Sign-on
sTESTA	Secure Trans European Services for Telematics between Administrations
STORK	Secure idenTity acrOss boRders linked
SWOT	Strengths, Weaknesses, Opportunities and Threats
UC	Use Case
UKAMF	UK Access Management Federation
VGI	Volunteered Geographic Information
WFS	Web Feature Service
WMS	Web Map Service
WMTS	Web Map Tile Service
XACML	eXtensible Access Control 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, 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 report *"D2.4 – Results of the workshop 'AAA architectures for INSPIRE', 16-17 March, Leuven"* covers the results of the discussions during a workshop in Leuven, Belgium, to present initial findings of the project and gather feedback on the approach for the testbed from participating organisations and other experts. In particular, the report summarises the experiences from 7 implementations in 7 Member States with regard to the application of standards and technologies for AAA. The report draws also some general and more specific conclusions in regard to the deployment of the testbed (Task 3 of the project).

The report consists of the following sections: section 2 defines the objectives of the workshop, the targeted participants and the agenda; section 3 provides a summary of the presentations, while section 4 summarises the discussions in the breakout groups and of the panel. Section 5 outlines the testbed planning and section 6 draws some general conclusions of the workshop.

2 Objectives, Participants and Agenda of the Workshop

As part of the analysis phase of the project, a workshop was organised to gather together consortium partners, testbed participants, AAA experts and Member State stakeholders to discuss the findings of the study phase of the project (see deliverables *"D1.1.1 & D1.2.1 Analysing standards and technologies for AAA"* and *"D1.3 – Best Practices of AAA implementations"*), to learn from experiences of AAA implementations in Europe and to gather recommendations from participants for the development and implementation of the testbed (Phase 3 of the project).

The workshop *"Authentication, Authorization and Accounting for Data and Services in EU Public Administrations: Developing an AAA-Architecture for INSPIRE"* involved 19 participants discussing existing practices

regarding AAA implementation in Europe in the context of e-Government and INSPIRE and provided input to prepare and conduct the testbed. Discussions took place in two breakout groups on the potential scenarios and use cases, as well as the technological challenges and issues to be addressed in the testbed.

In the next sections we briefly describe the objectives of the workshop, the participating stakeholders and the agenda.

2.1 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 (Task 1), and to present and discuss a SWOT analysis of the proposed standards and technologies to be adopted in the testbed phase. 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.

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. Because the workshop took place earlier than originally foreseen the full reports *"D2.1 – Analysing standards & technologies against Best Practices"* and *"D2.2 – SWOT analysis and initial design of the testbed"* were drafted after the workshop. Instead, a series of presentations (see annex), as well as a list of questions (see section 4) were prepared in order to guide the discussions at the workshop.

2.2 Participants

The 19 participants were experts and stakeholders coming from a multitude of communities:

- 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/ARE3NA) and DG DIGIT (ISA programme);
- People involved in European and national/sub-national AAA implementation projects in the context of INSPIRE and e-Government;
- Other stakeholders and interested parties such as the Dutch Cadastre, the Belgian Mapping Agency (NGI-BE) and Deloitte.

The list of participants is included in the annex.

2.3 Agenda

The workshop consisted of a series of introductory presentations: 1) to explain the importance of an AAA approach for INSPIRE and the link with the ISA programme; 2) to summarise the first findings of the consortium on AAA standards and technologies and 3) to present examples of AAA implementations and the standards and technologies used in different projects throughout Europe (AT, BE, DE, FR, NL, PL and UK). Moreover, enough time was foreseen to have discussions in breakout groups and through a panel with different AAA experts to gather information and recommendations to set-up the testbed.

Monday 17 March 2014		
10:30-11:00	Registration, coffee and welcome	Danny Vandenbroucke (KU Leuven) and Dirk Frigne (geo-sparc)
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 S. 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 (geo-sparc)
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 Authorisa-	Andreas Matheus (Secure

	tion: introduction to a federated approach	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 (Technical and Policy)	
10:30-11:00	Coffee break	
11:00-11:45	2 breakout groups around two challenges of AAA-implementation (Technical and Policy)	
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

3 Summary of and Lessons Learned from the presentations

This section provides a summary of the presentations given during the workshop with the most important/relevant lessons learned in view of the ARE3NA-AAA project and the testbed, in particular. The details of the examples of Best Practices were integrated in the report *"D1.3 – Best Practices of AAA implementations"* and will not be repeated here. The presentations themselves are available as annex to this report.

3.1 AAA solutions as key part of the ISA programme

3.1.1 The ISA programme and initiatives for secure access - Miguel Alvarez Rodriguez (DG DIGIT)

The 'Interoperability Solutions for European Public Administrations (ISA)' programme is the follow-up of the programme 'Interoperable Delivery of European eGovernment Services to public Administrations', Business and Citizens (IDABC) programme. The objectives of ISA are 1) to develop cross-border and cross-sector solutions for efficient and effective interactions between public authorities and their citizens and businesses, 2) to promote, share and reuse existing interoperable solutions and 3) to support ICT systems that allow smooth implementation of Community policies and activities.

ISA supports several actions related to secure access to and exchange of data by/between public authorities: Key enablers for secure eGovernment services, a cluster of eID-related actions and tools for e-Signature (e.g. STORK, DSS-tool); the set-up of a secure telecommunication network (sTESTA) and the secure exchange of DOCs (eTrustEx).

3.1.2 The STORK project - Miguel Alvarez Rodriguez (DG DIGIT)

STORK stands for 'Secure idenTity acrOss boRders'. It is one of the key projects of the ISA programme. The objective is to create a system for the recognition of eIDs (electronic Identity Card) and authentication of citizens from any Member State, allowing them access to eGovernment applications in cross-border set-ups. For example, a student with Belgian eID can have access or not (depending of the type and the year of studies, the teacher, etc.) to some documents in a university of another Member State in Europe (Cotasson, 2014).

The advantages of STORK are multi-fold:

- Easy-to-deploy solution for the provision and consumption of secure identity services of national and foreign citizens;
- Access to a Reference interoperability technical solution for the mutual recognition of eID at the European level;
- It is a flexible interoperable solution that can handle any type of electronic identity and assurance levels; It can be used as a service or as tool
- It is a solution maintained and supported by the EC and many Member States.

A first proof of concept demonstrating the integration of ECAS within the STORK project was funded by IDABC programme and executed in 2011. In the context of STORK 1.0, a SAML profile was developed. As a result, ECAS linked to STORK enables a citizen from a Member State to use a national eID to have the authentication needed to access electronic services delivered by the European Commission (e.g. CIRCABC, CORDIS).

However, several problems remained after the initial phase: 1) Member State officials and civil servants from all over Europe need to access EC applications and 2) European Commission Authentication System (ECAS) credentials are used since national eIDs are not (yet) recognised by the EC applications.

STORK provides four levels of authentication and has been implemented in 29 portals. STORK 2.0 is also being deployed and further tested in eHealth, Internet banking, eLearning and public services for business pilots in the ISA programme. STORK 2.0 is following an Access Management Federation (AMF) approach based on circles of trust in Member States.

Lessons learned:

1. STORK uses a federated system based on different circles of trust provided by the Member States. This is also the model to be applied (and foreseen) in the context of an AAA-approach for INSPIRE.
2. STORK is applied in several thematic areas. An AAA-approach for INSPIRE could contribute to the testing of the AMF that will be set-up and in particular the use of specific SAML profiles/bindings.

3. The use of eIDs for secure access by citizens could become part of the testbed in order to test secure access to INSPIRE services by citizens (G2C use case).

3.2 An AAA solution for INSPIRE based on existing standards and technologies

3.2.1 ARE3NA: AAA as a key layer of the INSPIRE architecture – Robin Smith (JRC)

ARE3NA is an ISA action (1.17) focussing on the sharing of reusable components for INSPIRE implementation and on interoperability in cross-border/cross-sector contexts, with its 'watch-words' being: collaboration, reuse, openness and interoperability. Its main activities include: 1) the establishment of a collaborative platform to support sharing of best practices (using JoinUp and the INSPIRE Forum); 2) maintaining an INSPIRE implementation software inventory, including Open Source tools; 3) identifying other policies & platforms dealing with spatial data exchange; 4) identifying 'missing items' in INSPIRE and between INSPIRE & other sectors; and 5) developing Open Source solutions and guidelines.

ARE3NA builds further on the existing INSPIRE assets (e.g. semantic assets such as INSPIRE GML Application Schema) and extends them with software and service assets from the Open Source world (e.g. the GeoMajas SDI Open Source suite) and from ongoing and recently completed European and national projects (e.g. ELF). Efforts are linked to other ISA actions where appropriate, e.g. the Core Vocabularies (Location, Person, Business and Public Service), and the Assets Description Metadata Schema (ADMS). Several projects are ongoing in ARE3NA to support and extend INSPIRE such as: the exploration of cross sector mobile applications, the Resource Description Framework and Persistent Identifiers (RDF & PIDs), Registry software, INSPIRE metadata and mappings to the open data portal DCAT Application Profile, Volunteered Geographic Information (VGI) and reusable tools, a candidate download service (including open source tools a demonstrator and guidelines) using the Open Geospatial Consortium's (OGC) Sensor Observation Service and the AAA study which is the topic of this workshop.

Questions ARE3NA would like to be answered are: "What will help AAA adoption in different organisations: "What are the challenges", "Would specific GI vocabularies/roles help" and "What tools/approaches could help".

3.2.2 AAA-architecture for INSPIRE: Standards & technologies – Danny Vandenbroucke (KU Leuven)

The INSPIRE Directive foresees public access to spatial data through services (discovery, view, download)[1]. The goal is to have as few access barriers as possible, i.e. to provide direct and free access. However, the Directive also foresees that public access can be limited for particular reasons. For example, access to a view service can be limited for IPR or privacy issues, or even to protect the environment (e.g. particular habitats or species). As a consequence, Member States might set-up access control mechanisms to protect some of their INSPIRE services.

It is important to define the key concepts of such an access control (or AAA) mechanism as clear as possible, for example with AAA as part of an AMF. These and other concepts have been defined in *"D1.1.1 & D1.2.1 Analysing standards and technologies for AAA"* together with the standards and technologies to

[1] Discovery services are usually CSW services, view services are usually WMS or WMTS, while download services can be in the form of WFS or ATOM Feed.

implement them as part of an AMF. An overview of the most common standards and technologies was given during the workshop, as well as a description of how they fit together and how they make the AMF work.

Lessons learned:

1. An AAA approach is an important layer of the INSPIRE architecture. As the project is an ISA action it is important to look into the experiences of other actions dealing with secure data exchange, such as STORK.
2. It is important to have clear definitions, not only with regard to the basic concepts of an AAA mechanism, but also to specific aspects such as 'attributes' exchanged between IdPs and SPs, the 'roles' and 'rules' applied in the AMF, etc.

3.3 Experiences from several countries

In total 7 experiences of AAA implementations were given during the workshop from 7 countries: UK, Belgium, The Netherlands, Germany, Austria, Poland and France. The experiences are documented in more detail in *"D1.3 – Best Practices of AAA implementations".* We only summarise the main highlights of the presentations and the lessons learned in this report.

3.3.1 Secure access to spatial data for academia: the UK experience – Chris Higgins (EDINA)

EDINA has a long lasting experience in the delivery of secure services for the academic sector (research and education), part of which is geospatial web services based on OGC standards. The UK has setup an AMF (UKAMF) with currently more than 8 million users and approximately 400 entities involved as IdPs or SPs. The SPs are entirely responsible for the management of access rights to its services. Most organisations involved use SAML and Shibboleth, but other implementations exist as well.

Implementations have been setup and tested in the context of many (European) projects such as ESDIN (*http://www.esdin.eu/*) and more recently COBWEB (*http://cobwebproject.eu/*). In many of those projects the work was done in cooperation with the OGC and integrated with Interoperability Experiments of OGC and Global Earth Observation System of Systems (GEOSS). One of those experiments, the OGC Web Services Shibboleth Interoperability Experiment (OSI), delivered an open source reference implementation of a modified desktop client conformant with the SAML ECP Profile (*http://esdin.fgi.fi/wiki/index.php/Esdin:AuthIE:Client*). Other examples, such as the COBWEB project that is performed in cooperation with GEOSS, are explained in more detail in *"D1.3 – Best Practices of AAA implementations"* (see also Higgins et al., 2012).

3.3.2 Secured services in the province of Limburg (NL) – Reijer Copier (IDgis)

IDgis is a SME active in the field of GI and INSPIRE. The company developed an approach to secure the exchange of working drafts of spatial zoning plans between spatial planners of different organisations in the Province of Limburg, the Netherlands. Several requirements were defined: 1) only people involved in the planning process should be authorised to access the (draft) plans and 2) it should be easy to add plans, to define users (and user groups) and to configure security constraints.

The architecture consisted of three components: OGC web services (OWS), a Mapviewer and an administrator console. The Mapviewer had to allow, besides the viewing of the (draft) spatial zoning plans, a detailed location report to be provided, as well as feedback to the planner. The administrator console had to make it possible to upload plans and to define users, user groups and security constraints.

3.3.3 Access Management Federation for Spatial Data and Services in Germany – Andreas von Dömming (GDI-DE)

The AAA implementation in Germany is part of the establishment, development and operation of the German national Spatial Data Infrastructure, the GDI-DE, through a specific work package on using protected data and services. GDI-DE defined several requirements for an AAA approach in Germany: 1) consideration for existing infrastructures, 2) security as an add-on; 3) no central storage of user accounts; 4) must be based on distributed data and services and 5) follow the "Standards and Architectures for E-Government-Applications (SAGA 4.0)", a national German standardisation approach.

SAGA 4.0 provides more detailed requirements: roles for access control are clearly defined, core attributes for identities are defined as well, services are stateless; and the composition of services. SAML 2.0 is also recommended. Most eGovernment applications are using a web browser as a frontend. The presentation also covered some organisational issues, such as: "Who accepts users"; "Who grants access rights for data and services"; "Who coordinates access rights, including between different domains" and "Who supervises the working process". GDI-DE followed a role based access control approach. User attributes (organisation and role) are provided to service providers for the purpose of access control.

3.3.4 Secure access to spatial data from the sub-soil - Tom Van Gulck (LNE-ACD)

The AAA implementation in the Flemish Ministry of Environment, Nature and Energy (LNE) is a good example of the cooperation between a Region (corresponding to the Länder in Germany) and the federal level. While FEDICT at the federal level plays the role of IdP (Access Control Management and Identity Management), LNE is the SP and has setup a mechanism to receive attribute information from the federal level about individuals that want to access services delivered by entities at the Regional level. LNE organises the access to applications and services from different SPs of the Flemish Community.

A mixture of open standards is used for communication with the applications and services (e.g. OpenAM, OpenDJ and OAuth) and for getting the attribute information from the federal level (e.g. SAML).

3.3.5 An AAA layer inside the French Geoportal – Benjamin Cotasson (IGN-FR)

IGN France, the French mapping agency, has implemented a specific solution in order to better understand who is using their data and how (e.g. through a web browser or other application). They also want to track which data and services are used the most, the intensity of use and the amount of data downloaded. An AAA solution, therefore, has been setup as part of the IGN geoportal, with a focus on the third 'A', Accounting. IGN sees the protection of their data and services as part of the relationship with their customers defined through the use of keys. Based on information in a key, a customer can get access (or not) to certain data sets and/or services.

The mechanism is intended to be used for access to data via web interfaces, mobile devices and desktop applications. The AAA implementation does not currently make use of any standard, as it is an in-house solution. It is a basic authentication mechanism that should prevent most of the potentially illegal use of

data and services. It should be noted that, currently, France does not provide citizens with eID cards that would provide other forms of authentication, as noted above.

3.3.6 Developing an AAA-Architecture for INSPIRE - Jacek Szczęsny (Head Office of Geodesy and Cartography, Poland)

The AAA implementation of the Polish mapping agency, the Head Office of Geodesy and Cartography (GUGiK), also focuses on the monitoring of the data and services being used, including statistics on the users and usage. Several technologies are being used, with some basic authentication mechanism. The Polish geoportal has now 5000 registered users. The solution developed is based on several AAA components: Java and Python scripts have been developed to support the administration of the national Geoportal, including an LDAP database for managing user identities; securing of spatial data services using the SecurityManager of Conterra; and basic monitoring of (non-)spatial geoportal services using Oracle's Business Activity Monitoring (BAM).

3.3.7 AAA Experience and Status in Austria, an Overview – Peter Pichler (LFRZ)

Austria has a long tradition of AAA implementations, mainly in the context of e-Government. AA(A) mechanisms support different types of interactions in e-Government processes: Citizen to Government (G2C), in which citizens are using the Austrian Citizen Card (eID) and MOA (Modules for Online Applications); Business to Government (G2B), in which businesses are using the portal for business company services (Unternehmesseriveportal); and Government to Government (G2G), based on the Austrian Portal Federation (Portalverbund). The latter mechanism also includes Accounting, while the others only focus on Authentication and Authorisation. The efforts related to G2C authentication have been integrated with STORK. Citizens can make use of an e-card (Austrian Citizen Card) or of a Mobile device to access government services. More and more citizens are making use of these means of authentication. Companies can access the portal for business services through the use of the e-card of an employee of the company. The main challenges in the approach were to set-up a register of companies and the processes for the authorisation management within the companies.

The main focus of AAA implementations has been on the G2G type of interactions. The main challenge in this case was to have a mechanism that supports the federal structure of Austria. Many organisations are involved: Ministries, Federal State Governments, Courts; Special Topic Agencies (such as statistics, environmental protection, financial auditing, food safety, drug studies, calibration and measurement, water protection and IT Services); Governmental Insurance Agencies; and compulsory interest groups for business cooperation, employees, farmers and advocates. Moreover, for Authorisation Management, there are important boundary conditions. No one person has the right to use a G2G service. Instead it is the organisation that he/she is working for that is accessing the services. The agency delegates this right to staff needing the service, according to the scope of their duties. If responsibilities within the organisation change, then the authorisation conditions will also need to change.

The Austria federation is based on following principles:

1. Organisations that want to access services from other organisations use an IdP. They can use their own or a shared infrastructure.
2. Access rights for all governmental applications are managed by the home organisation of the user.
3. Organisations providing services are SPs and have the infrastructure to provide the services.

4. A multilateral contract between all participants allows SPs to trust the AAA information passed to them from the federation's IdPs through the "Portal Federation Agreement".

In 2010, the federation was established. All ministries, federal state administrations, local community administrations can access services of the federation. Many special topic organisations have also access to the federation and/or provide services to it. Internal applications are developed using the common AAA approach based on the PVP standard (see for more information on the use of this protocol *"D1.3 – Best Practices of AAA implementations")*. The federated portal technologies are used for the organisations internal portals to support C2G interactions. Already in 2010, there were more than 130,000 registered G2G users and more than 600,000 non-G2G users, with millions of transactions handled every day.

Lessons learned:

1. Using SAML and Shibboleth to protect OGC Web Services (OWS) is feasible and may not be difficult to implement on the server side or with browser based clients. This, however, needs more efforts when desktop-based clients are involved, which may potentially include the use of some workarounds.
2. The testbed approach that was applied in the context of the OGC Interoperability Experiments is a good way to setup, test and learn about different technical solutions.
3. AMF for spatial data and services can be established in ways similar to existing AMFs, as found in the academic sector, because everything is based on general ICT security standards with only a geo-extension for authorisation (such as geoXACML).
4. The definition of attributes should be kept simple (e.g. organisation, role), while the role and rules should be clearly defined in relation to the access policy of the SP (which can be very different).
5. The mixed use of open standards is possible: specific organisations or regions can deploy e.g. OAuth, while the exchange of authentication information (the attributes) can be done using SAML.
6. There is an interest from INSPIRE stakeholders, mainly the mapping agencies, in Accounting so that usage of data and services can be logged/monitored as part of their service delivery to customers.

4 Summary of the Major discussions

An important part of the workshop was dedicated to discussions in breakout groups and through panel discussions. In order to allow participants to prepare the discussions, a simple questionnaire was prepared to guide the group and panel discussions.

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 cannot) 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?

In the following sections, the results of the discussions are summarised.

4.1 Scenarios and use cases

In the first breakout group possible scenarios and the related use cases for the testbed were discussed.

In more general terms, the INSPIRE Directive foresees public access to services. Restrictions to discovery services are only allowed based very specific reasons which are listed in the Directive (e.g. national defence). Restricted access to other types of INSPIRE services (e.g. view and download) might be invoked for a series of cases also described in the Directive (e.g. IPR, personal data, sensitive data about species in danger). Moreover, in some cases, conditions might apply for data usage. Access to (parts of) the data might also be different based on differing roles in an organisation. Moreover, users may not only be someone representing an organisation but also citizens, not-for-profit organisations and businesses. In all cases, access control is needed.

The scenarios and use cases should cover user-to-machine and machine-to-machine interactions. They must include access to different type of INSPIRE services: CSW, WMS and WFS. In addition, testing should include different types of clients: browser, desktop and server based applications (including for citizens, staff from NGOs or businesses). The testbed should also reflect different user-types: civil servants of public authorities and individual citizens. At least one cross-border scenario (i.e. access by users from outside a particular country) should be taken into account.

Three different scenarios were discussed in more detail during the breakout group:

Scenario 1 – harvesting catalogues

The JRC is running the European INSPIRE geoportal. It contains a catalogue and catalogue service that is harvesting all the catalogues of the Member States that have been defined as endpoints for this geoportal. These national (or regional) catalogues might, in turn, harvest metadata from other catalogues (e.g. in Germany, the federal catalogue is harvesting 32 catalogues from the Länder and thematic communities). The JRC is also testing the conformity of metadata records and services against the INSPIRE Implementing Rules and guidelines, as well as the services' performance. The JRC, therefore, requires access to all these services, even if there are access control mechanisms in place, and, more specifically, the JRC's server to have the appropriate access rights. This scenario provides a clear machine-to-machine use case, involving access to different type of INSPIRE services for any type of access control mechanism that may be in place.

Organisations involved: JRC, 3 test organisations (SPs), central IdP (Secure Dimensions)

Scenario 2 – cross-border viewing and downloading of data sets

INSPIRE is supporting cross-border applications using geospatial information. A common scenario is where a user (person from a public administration) needs spatial data sets from different countries related to one or more INSPIRE themes. In such cases, the user should be able to access/reach the required data sets using their own login credentials (e.g. after a search through the European INSPIRE portal), view (map) the data and its metadata to check their fitness for purpose and be authorised to download the data sets of interest through a WFS or ATOM feed. This is a user-to-machine interaction but the result will depend on the access policies from different SPs in different countries. The scenario could be extended with users that do not belong to a public authority, but act on behalf of a not-for-profit organisation, or even as individual citizens.

Scenario 3 – access to (parts of) spatial data sets / services by users of a thematic community

A more complex scenario might involve different types of user that require full access to complete data sets, while other users may need to have access to basic information where certain parts of the same spatial data sets and/or their attributes are not accessible. Such a case can be found in the context of data related to environmental policies related to protected sites. People working for public authorities from other policy areas (other than environmental policy) and the general public (e.g. farmers, individual citizens) might need/want to know general information about where protected sites are located and the general environmental characteristics of those sites. On the other hand, they are not likely to have access to sensitive information, such as details about the particular species present (attribute information) or to sites that have been delineated but are not yet designated (i.e. sites at the planning stage). There may also be instances where staff members from more than one public authority are involved in the designation of the sites, along with staff from not-for-profit organisations and certain individual experts who could require access rights to all the information present as part of the designation process. Authentication in this case would involve, for example, access for staff members of public authorities based on their role in the organisation and for individual citizens potentially using their eID. This scenario involves a more complex form of authorisation to take account of what can be seen, downloaded, etc.

These three scenarios were discussed during the breakout groups. From the discussion, it was concluded that the first scenario is feasible and useful as part of the testbed, while scenario three might be too complex in view of the available resources and timing of the project. A more detailed description of the scenarios and related use cases will be provided as part of the testbed set-up (see D3.3 - Technical documentation of the finalised testbed).

4.2 Technical challenges and choices

The second breakout group discussed the technological challenges and choices to be made in view of the testbed. The most important general conclusions can be summarised as follows:

1. There was an agreement among the consortium members, the stakeholders of the participating countries and the JRC to use SAML as a base standard. However, it will also be necessary to investigate and test several profiles and bindings, such as the Enhanced Client and Proxy Profile (ECP) for desktop clients and the Web Browser Single Sign-On Profile for web browser based applications.

2. The testbed should be developed in different iterations. The consortium will start with an internal testbed with a “mini-federation” with three consortium partners. At the same time, the testbed will

be explained to the involved stakeholders and other interested parties, e.g. IGN France (see also section 5).

3. The testbed is not foreseen to be open to other interested parties. However, a copy of the production services could be set-up for those interested in order to experiment with the testbed environment.

Regarding authentication, the following recommendations were put forward:

1. The testbed should put in place the same configuration as in the COBWEB project and the GEOSS Architecture for Interoperability Pilots (AIP) 6. This means a Single Sign-On (SSO) profile for browser applications and an ECP for desktop and server applications. This can offer a solution for testing in an INSPIRE context that is being implemented in similar infrastructures.

2. The testbed must chose an HTTP Artefact binding because the POST binding is not supported by clients, such as OpenLayers. A choice will be needed between two options:

    a. An additional port in the firewall (e.g. 8443[2]) is used to establish the secure backchannel independent from the client facing certificate used on port 443. This requires that the firewall accepts inbound requests on port 8443. As an alternative, the secure backchannel could be established on port 443[3];

    b. an additional IP in the same domain with port 443 is used. This allows an independent set-up of the secure back channel and prevents the firewall issue as the standard port for HTTPS is used.

3. The Coordination Centre should apply the following principles to support the testbed. An organisation that wants to join the federation must be checked: i.e. the metadata of the AMF must be validated. The Coordination Centre must also handle / manage the federation metadata and set-up contracts with SPs and IdPs. Rules must be defined that work for all data products in the federation and (ideally open source) tools should be used to verifying metadata compliance etc.

4. There is a need to automate metadata refreshment at the IdPs and SPs to reflect organisational changes of the AMF. This can be done automatically by using Shibboleth, whereas OpenAM would require some development for automated updates.

Regarding authorisation, the following recommendations were put forward:

1. It is necessary to agree on a standard for authorisation in to inform partners in the federation about the policies of SPs and to exchange the attributes and values of the authorised user and use. This is not necessary for the actual authorisation itself, i.e. for enforcing the policy (although (Geo)XACML, or other means, could do this).

---

[2] The use of port 8443 on the IdP has an implication to all firewall configurations at the SP domains: As part of the SAML Artefact Binding, the SP is requesting message exchange with the IdP via HTTPS on port 8443. As port 8443 is not the standard HTTPS port, the outbound firewall must allow this type of communication.

[3] But that setup loses the certificate independence between browser facing and secure backchannel endpoints. This would therefore imply that all secure backchannel messages are signed with the browser facing certificate and requires refreshing of the SAML federation metadata when the browser facing certificate expires.

2. XACML and (Geo)XACML in case of geo-specific conditions are proposed as the only possible candidates for authorisation.

3. The exchange of attributes and values need to be considered carefully. It is recommended to 'borrow' attributes from existing AAA implementations: e.g. STORK has defined some key attributes that can be reused, also eduGAIN has defined 5 core attributes and some possible extensions[4]. There is also a clear need to make a distinction between natural persons and persons representing an organisation (in which they have a certain role).[5]

STORK – examples of attributes[6]		
eIdentifier	Date of birth	Text Residence Address
Given Name	Country of birth	Canonical Residence Address
Surname	Nationality	Email address
Gender	Marital status	Fiscal number

EduGAIN: attributes (recommended)	
Display name	Person Affiliation
Common name	Home organisation
Mail	Home organisation type

4. There are two architectural approaches for enforcing authorisation: i) by developing a separate module to perform enforcement in combination with standard OGC web services; or ii) by integrating the authorisation directly in the OGC web service. The first solution is recommended for 'simple' policies and where it is impossible to change the actual implementation of services, as well as where the setup is by proxy. The latter is for 'complex' policies where it is not feasible in terms of performance or where it cannot be fulfilled by re-writing the query or filtering of results.

4.3 Results from the panel discussion

During the workshop, a panel discussion was organised to explore in more detail some of the Best Practices presented and to provide more feedback from participants during the workshop.

General recommendations given by the panellists:

[4] Also other experiences exist, e.g. in Flanders the SSO domains are based on target groups. In Austria, attribute profiles have been defined which might be useful for applications-specific roles.

[5] During the workshop it was suggested to have a fixed set of attributes but with flexibility in the policies and a fixed set of rules linked to attributes (e.g. a rule based on the role in the organisation). Roles are defined as a group of functions.

[6] For a full list see "Towards pan-European recognition of electronic IDs (eIDs): D5.8.3b Interface Specification

- Remain realistic and do not re-invent the wheel. Build on top of existing solutions and keep the testbed 'simple' (in order to save costs to implementers);
- Keep the approach flexible and scalable;
- Define clearly what should be tested and document this thoroughly in a technical guidance document (including items such as the definition of roles);

During the testbed it is important to collect information about the process itself:	
✓ What is the organisational context? ✓ What are the barriers encountered? ✓ What are the organisational bottlenecks?	✓ What are the criteria for success? ✓ What is the pre-test status of the organisation? ✓ What have we learned?

- Include conformity and interoperability testing; what will be your acceptance tests;
- Use cases should be based on interviews with different users, technical and non-technical people;
- Define clear attributes and roles for G2G, G2B and G2C cases; define a clear process for managing the attributes;
- Convince stakeholders to participate; awareness-raising is crucial and the work needs to take into account that joining a federation is not 'free' but will require some investment;
- Requirements for training but gaining expertise are important issues;
- Involve additional stakeholders to make sure all authorisation aspects are covered; test the impact of involving more stakeholders;
- Make the testbed sustainable / persistent: who will maintain the test infrastructure; what should be the next steps when the testbed has been initiated;

Panellists also suggested that several other points be taken into account during the testbed (and include findings in the final report):

- Which SAML profiles / bindings are recommended and why?
- How would a Coordination Centre of an AMF for INSPIRE work?
- What is the final recommended list of attributes (names and values; registry of services)?

In more general terms, the participants showed a great interest in the AAA-implementations and in participating in the testbed:

- LNE-ACD (Flanders) has different internal services they want to expose and they want to set-up one SP to proxy the services and organise access based on different identities. Currently, there is duplication of data sets because organisations do not have access to each other services.
- Also the Dutch Cadastre provides services (WMS and WFS) and is interested in using e-ID solutions. The Dutch Cadastre would also like to contribute by providing access to protected services for the harvesting case by the JRC.

- GDI-DE is aiming to have a follow-up of the access control project they already conducted and wants to extend it with some new use cases.
- Also IGN-FR is interested to join and/or contribute to the testbed, while Austria wants to follow-up the testbed as well.

5 Testbed (T3)

The workshop was an important initial step in defining the testbed, with planned activities presented in this report. Based on the input and discussions during the workshop, a revised plan has been elaborated for the testbed (De Graef, 2014). The testbed activities correspond to Task 3 (T3) of the project which has been split up into three subtasks to be addressed in three consecutive iterations:

1. Task 3.1: Testbed development;
2. Task 3.2: Testbed implementation;
3. Task 3.3: Testbed assessment and refinement.

For the testbed development the initial proposal was to work with three iterations of three weeks each to develop the entire testbed. Although during the workshop, the supporting organizations indicated that they were willing to be involved as soon as possible, the consortium proposed to not divert too much from the original project plan.

The main reason is that before the supporting organizations can get started in the testbed implementation, they should be given clear documentation on how to actually implement it. To write this documentation, the testbed should be developed first, so that practical experience can be taken into account in its drafting.

Before the testbed development begins, Secure Dimensions will write a more detailed technical analysis document outlining the different use-cases of the testbed. Using this document, the consortium will develop the testbed on its own servers. During the development phase, Geosparc will write extensive documentation describing each use-case.

During the testbed development, useful indicators will be collected and measured: e.g. how long does it take a senior analyst to set up the system without experience of the proposed software stack.

5.1 Task 3.1: Testbed development

This task will result in the development of the actual software stack and the documentation that will be used in the testbed. A working demonstrator will be deployed involving the local testbed on the infrastructure of the contractors. This local testbed will run on 3 servers, provided by Geosparc, IDGis and Secure Dimensions, respectively. The local testbed has the advantage that the supporting organizations will be offered a functional and tested system that can act as a reference when deploying the testbed on top of their own respective environments. It is likely that some changes to the testbed settings will have to be made in order to adapt to the particular situation of the supporting organizations. They may, however, already have similar technology in place as the technologies suggested by the consortium.

The following technical use-cases will be addressed. They are needed for any of the scenarios described in section 4:

- UC1 – Requesting certificates
- UC2 – Setting up a Service Provider
- UC3 – Setting up an Identity Provider
- UC4 – Configuring basic users in the IDP
- UC5 – Setting up a WMS service under the SP
- UC6 – Ensuring authorization through geoXACML
- UC7 – Setting up the Discovery Service
- UC8 – Setting up a Federation through the Discovery Service
- UC9 – Creating a client application that connects to all WMS services
- UC10 – Creating a QGIS add-on to support SSO through SAML

Once all these use-cases are finished, the testbed on the local servers of the consortium members will correspond to a working federation. Within this federation, different users will exist with different access rights.

This task has been split up into three sprints lasting three weeks each, starting on Monday the 7th of April. This phase ends on Friday the 6th of June.

5.2 Task 3.2: Testbed implementation

The scope of this task is to assist the supporting organizations in setting up the testbed on their own infrastructure, using the documentation provided in Task 3.1. Activities include:

1. Installation and configuration of the testbed on the infrastructure of the supporting organization;
2. Adaptation of the test scenarios to connect to INSPIRE services used by the supporting organizations;
3. Configuration of a web GIS client to access protected INSPIRE services (using the AAA stack developed in Task 3.1).

All findings of the testbed implementation will be added to the existing testbed documentation and reported periodically.

This task will run from the 9th of June until the 29th of August. The first week is reserved for communicating the documentation from Task 3.1 to the JRC and the supporting organizations, and making updates if needed. From the second week onwards, it is up to the supporting organizations to start implementing the testbed on their own infrastructure.

5.3 Task 3.3: Testbed assessment and refinement

This will be done through frequent interactions of the consortium partners with the supporting organizations. This is feasible because the different partners are either active in ongoing projects and services within the supporting organizations or have worked together recently on projects and systems. In both cases, consortium members are located in close proximity to the supporting organizations, offering onsite and hands-on support, if needed.

The supporting organizations will start the tests. On a frequent basis, the contractors will follow progress, address potential issues and make improvements. Where necessary, the contractors will make adaptations and remove impediments as they would arise.

For the activities of Task 3.3, sufficient time has been foreseen because the consortium partners are depending upon the resources available within the supporting organizations, as well as upon the timeframe in which these resources can be made available. Also, this time should allow the consortium to make the necessary changes to the AAA software stack and redeploy it on the organization's environments.

An additional use-case for this phase is to adjust the JRC harvester to actually be able to harvest secured INSPIRE services (this task will be undertaken by Secure Dimensions):

- UC11 – Harvesting Member States secured services

Although this phase begins a bit later than Task 3.2, all findings will be reported at the same time as those for Task 3.2.

6 General Conclusions

The AAA-Architectures for INSPIRE workshop allowed work undertaken by the consortium working on the AAA study and testbed to be presented to a wider and knowledgeable audience. It brought together experiences from different domains, including the academic community, ISA programme actions, the JRC and several Member States working on access control for geospatial data and services and e-government. In total, 19 experts contributed their technical expertise and experience to the proposed approach for the design of the testbed and discussed organisational and technological issues alongside potential access control scenarios / use cases.

A number of important issues were identified for the topic as a whole, as well as specific considerations for the testbed development towards federated access for EC and cross-border policy/service needs. These included understanding that there are some important differences in terminology within the access control domain and that the semantics of the technical approach are not yet well defined, impacting on the ready adoption and potential reuse of technical solutions/approaches.

Importantly, the workshop has allowed knowledge to be shared about the standards involved. It became clear that selecting SAML will not be enough to support interoperability, as SAML is a framework with particular profiles that need to be selected based on the use cases being defined in the study. The selected profiles will, in turn, also determine some of the geospatial technologies involved due to dependency/binding issues. Technology was, however, not the only focus and participants indicated the importance of awareness-raising and education, including new issues that will need to be addressed in a fully functioning context of an AMF. These included managing contracts for trusted partners, and the fact that AMFs

require resources (including several full-time staff) for their set-up and maintenance, which would apply to all relevant INSPIRE stakeholders.

An important conclusion from the workshop was the observed interest of the testbed partner organisations asking to be involved in the development as soon as possible in the development phase. At the same time it is clear that good documentation is needed in order to involve them at an early stage. Early involvement could lead to a co-creation process following an approach with several iterative steps in the development phase and additional lessons learnt for both the developers and the public sector organisations involved, helping the initial experimental implementation foreseen under ARE3NA. Early development of the testbed within the consortium with a live example will aid the creation of clear documentation and evidence for the participating organisations to follow. In addition, the workshop has allowed stakeholders to know the sorts of topics that the assessment of the testbed is likely to address.

The workshop has also raised interest from the other countries, namely Austria (mainly e-government), France and Poland (mainly geoportals/geospatial). This possible involvement will further be explored by the consortium, potentially aiding the reuse of the tools developed beyond the three testbed organisations.

Good links have also been made with the ISA Actions involved in this topic and details from their pilot activities (such as user attribute management in STORK) could potentially be adopted or reused in the testbed. As relevant ISA actions evolve, and depending on the interests of INSPIRE stakeholders, more of the ISA technologies and methodologies could aid access to INSPIRE data, as many elements are common to access control within a European e-government context, thus offering potential savings through common approaches.

References

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). Report of the AAA workshop, version 1.1. IGN France, Saint-Mandé, France.

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

Crabbé, A., Vandenbroucke, D., Matheus, A., Frigne, D., Maes, F. and Copier, R. (2014). D1.1.2 & D1.2.2 – Analysing Standards and Technologies for AAA.

De Graef, P. (2014). General Planning Testbed.

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

Federal Ministry of Interior (2008). SAGA: Standards and Architectures for E-Government-Applications (4.0).

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). D1.3 – Best Practices of AAA Implementations.

Annex

	Name	Affiliation	Country	e-mail
1	Robin Smith	EC JRC, IES	IT	robin.smith@jrc.ec.europa.eu
2	Michael Lutz	EC JRC, IES	IT	michael.lutz@jrc.ec.europa.eu
3	Miguel Alvarez Rodriguez	EC DG DIGIT	BE	Miguel.ALVAREZ-RODRIGUEZ@ec.europa.eu
4	Dirk Frigne	GeoSparc	BE	dirk.frigne@geosparc.com
5	Danny Vandenbroucke	KU Leuven	BE	Danny.vandenbroucke@sadl.kuleuven.be
6	Andreas Matheus	Secure Dimensions	DE	andreas.matheus@secure-dimensions.de
7	Reijer Copier	IDgis	NL	Reijer.Copier@idgis.nl
8	Herman Assink	IDgis	NL	herman.assink@idgis.nl
9	Tom Van Gulck	LNE-ACD	BE	tom.vangulck@lne.vlaanderen.be
10	Andreas von Dömming	GDI-DE	DE	andreas.doemming@bkg.bund.de
11	Markus Seifert	GDI Bayern	DE	Markus.seifert@lvg.bayern.de
12	Alice Vasilescu	Deloitte	BE	alvasilescu@DELOITTE.com
13	Chris Higgins	EDINA	UK	chris.higgins@ed.ac.uk
14	Damien Van der Eecken	NGI-BE	BE	damien.vander.eecken@ngi.be
15	Pieter De Graef	Geosparc	BE	Pieter.degraef@geosparc.be
16	Jacek Szczęsny	Head Office of Geodesy and Cartography (GUGiK)	PL	Jacek.Szczesny@codgik.gov.pl
17	Benjamin Cotasson	IGN (France)	FR	Benjamin.Cotasson@ign.fr
18	Peter Pichler	Land, forst- und wasserwirtschaftliches Rechenzentrum Gesellschaft mbH (LFRZ)	AT	Peter.Pichler@lfrz.at
19	Tom Vijlbrief	Kadaster NL	NL	tom.vijlbrief@kadaster.nl