Open Geospatial Consortium

Approval Date: 2012-03-23

Publication Date: 2012-04-18

External identifier of this OGC® document: http://www.opengis.net/doc/WP/architecture-access-management

Reference number of this document: OGC 12-026

Category: OpenGIS® White Paper

Editor: Andreas Matheus

Architecture of an Access Management Federation for Spatial Data and Services in Germany

Warning

This document is not an OGC Standard. This document is an OGC White Paper and is therefore not an official position of the OGC membership. This paper is distributed for review and comment. It is subject to change without notice and may not be referred to as an OGC Standard. Further, an OGC Discussion Paper should not be referenced as required or mandatory technology in procurements.

Document type:	OpenGIS® White Paper
Document subtype:	White Paper
Document stage:	Approved for public release
Document language:	English

License Agreement

Table of Contents

ACCESS MANAGEMENT FEDERATION FOR SPATIAL DATA AND SERVICES

Any questions regarding this document should be directed to the editor or any the following contributors:

CONTACT	COMPANY	E-Mail ADDRESS
Andreas Matheus	Secure Dimensions	andreas.matheus AT secure-dimensions.de
Jan Grohmann	Federal Agency for Cartography and Geodesy (BKG)	jan.grohmann AT bkg.bund.de
Christian Kiehle	Christian Kiehle	Christian AT kiehle.org

FORWARD

This document describes the results of a project that evaluated the feasibility on how to deal with protected data and services in a distributed environment. The solution to this problem was to establish a federation of trusted organizations for the purpose of exchanging protected geospatial information within Germany, leveraging OGC Web Services.

The architecture for the Access Management Federation for Spatial Data and Services (GeoAMF) is based on open standards from OASIS, OGC, IETF and W3C. The project has shown that the used security solution is capable and flexible to realize different use cases with operational relevance.

The concept of a Access Management Federation for Spatial Data and Services as illustrated in this document can be the enabler of sharing protected information such as regular web resources but also spatial data and services to marry the organizational and the governmental use for citizens based on one identical infrastructure.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The Open Geospatial Consortium shall not be held responsible for identifying any or all such patent rights.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the standard set forth in this document, and to provide supporting documentation.

MOTIVTION AND REQUIREMENTS

The coordination office for the German Spatial Data Infrastructure (Kst. GDI-DE[1]) has finished a project that was funded by the German Ministry of Internal Affairs (BMI). This project focused on the challenging question of how to establish and run a Spatial Data Infrastructure within Germany. One work package addresses on the using of protected data and services. This work package of the project "Betriebsmodell GDI-DE"[2] evaluated technical options and operational requirements to establish an Access Management Federation for spatial data and services within Germany.

For the project setup and the evaluation of the security infrastructure, three use cases have been taken forward to be evaluated:

1) Planning of extending high-speed internet infrastructure (Breitbandausbau)
2) Qualification of German ensembles (Nachqualifizierung von Denkmalen)
3) Information next to your home (Bauvorlage)

Use Case 1)

> One of many tasks of an Engineering Office is to plan digging activities for cable and empty tube rollout enabling high-speed Internet all over Germany. In order to coordinate the activities e.g. with other constructions and to ensure cost efficiency, the Engineering Offices require access to many different types of geospatial information. This information includes for example the maps and the technical description of empty tubes that are in the ground alongside major roads. Another important source of information is to know where the German Telekom Hotspots are to get connected to. Finally, the access to planning information of completed, active and future cable rollout is necessary. In addition, the official topographic maps and digital satellite photos are also planning basis. These different types of geospatial information and facts are provided by different providers such as the Bavarian Mapping Agency, the German Telekom and the Chamber of Industry and Commerce. All of them make the information available by Web Map Services deployed in their own security domain.

Use Case 2)

> One of many tasks of a State Office for the Preservation of Historical Monuments is to qualify identified historical monuments. The identified sites are represented by a location and a brief description, where a qualified site includes a geographic extend matching the actual ground shape of the historical monument. In order to qualify an identified historical monument, the building shape information must be obtained from another department of the government.

Use Case 3)

> For a German Citizen that wants to purchase a house or attempts to build one, it is very useful to obtain as many relevant pieces of information as possible to get a complete view of the new neighborhood. Some of the geospatial information that help to get an understanding of the quality of the neighborhood are noise emission caused by major roads at day or during the night, emission of power plants including the location of atomic plants, the loca-

[1] http://www.gdi-de.org

[2] http://inspire.jrc.ec.europa.eu/events/conferences/inspire_2011/abstracts/194.doc

tion of dump areas and the location of GSM antennas. In addition, the information about the direct neighbors helps to address them in the process of building construction planning.

A survey of suppliers for the required geospatial information showed that providers exist and that the information is available via OGC Web Services. Unfortunately, the different providers have deployed the services in their (security) domain and different protection mechanisms established such that a combined use of the information is extremely difficult and not user friendly.

Therefore, one key motivation was to establish an Access Management Federation that enables the seamless use of the information provided by different suppliers using different protection schemes. For ensuring a user friendly consumption of the information in a combined fashion, e.g. using an OpenLayers client or a desktop GIS, it was an important requirement to support Single-Sign-On.

Towards the managed access to the information, the vision was to authenticate each user with his home institution (remotely) and use some attributes of the user to undertake access control locally. It was important to ensure that policies for accessing the protected information of the service providers are met but that also the rights across the federation allow certain users to work on the use cases above.

INTRODUCTION

An Access Management Federation (AMF) is a network of organizations that trust each other for the means of sharing protected resources among each other. Worldwide, many academic AMFs are available for the purpose of sharing information and services between academic institutions such as Universities and Research Organizations. In the academia, some of the well known AMFs are UK Access Management Federation (United Kingdom http://www.ukfederation.org.uk/), In Common (USA http://www.incommon.org/) and DFN-AAI (Germany https://www.aai.dfn.de).

All these federations are using the same setup, as illustrated the figure below:

(i) A service provider (SP) that hosts protected resources which can be used by authenticated and authorized users of the federation;

(ii) An identity provider (IdP) which provides the login and the authentication of organizational user accounts;

(iii) A coordination center (CC) that controls the compliance with policies and procedures of the federation and thereby establishes the trust between members of the federation.

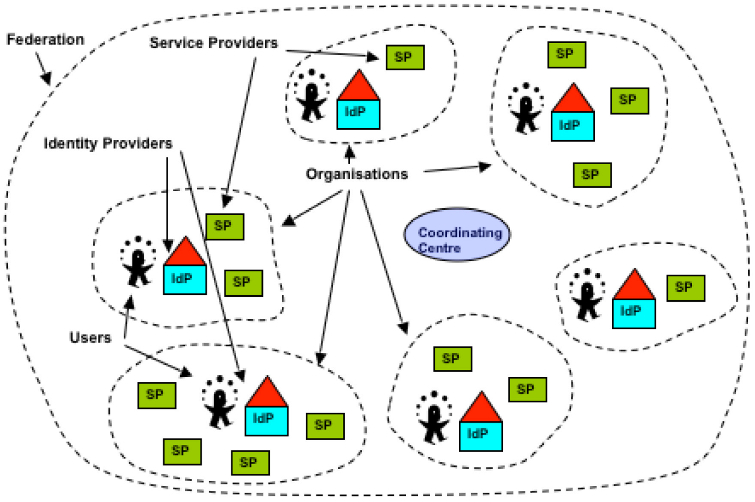
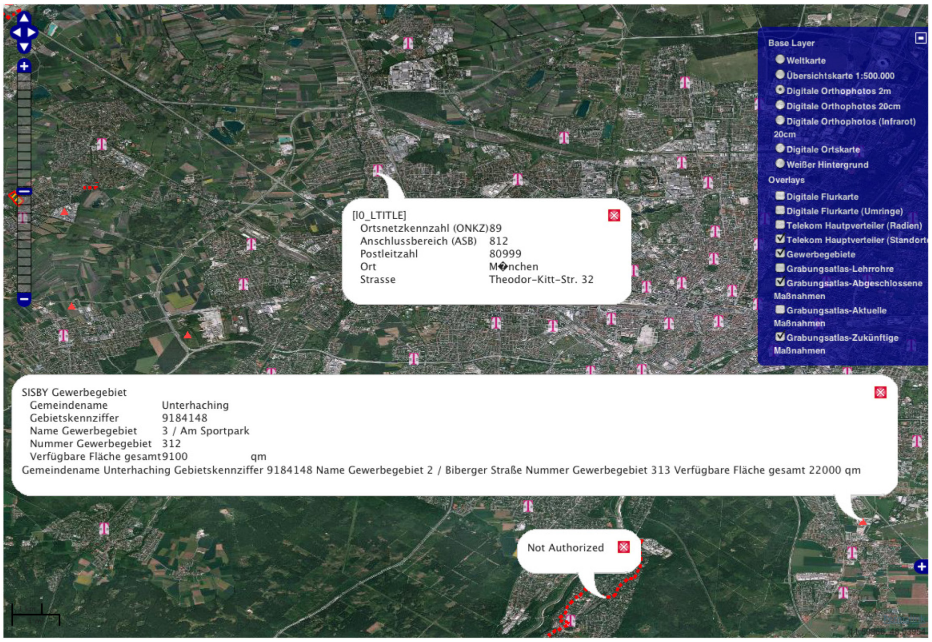


Figure: High-level view of a federation [source: http://www.swith.ch]

According to these role definitions, an organization can join the federation by applying to the Coordination Center (CC) as a Service Provider, an Identity Provider or both. For the legal act of accepting the organization, the CC checks technical compliance according to the policies and procedures of the federation. After being evaluated successfully, the CC will add the organization’s credentials to the federation metadata. Technically, the federation metadata is an XML file hosted online by the CC that includes an expiration date and is digitally signed by the CC to avoid tampering. The federation metadata of this GeoAMF can be obtained here: http://ds.gdi-de.org/federation-metadata.xml

Operational use of the federation requires that the user authenticates with his organization and not with each service provider. Once authenticated, Single-Sign-On ensures that the user gets a session established with all service providers of the federation when required and that a core set of user attributes are exchanged with the Service Provider. Based on the submitted user attributes, the Service Provider can establish security measures such as access control or audit.

An Access Management Federation for spatial data and services (GeoAMF) – as described in this document – can be established leveraging the same architecture, roles and organizational principles. The main differences are, that a Service Provider does host OGC Web Services and not regular Web resources such as HTML pages and that the client is a desktop GIS or a Web Browser based geo application such as an OpenLayers based client, as illustrated in the next figure.



Base Layer

○ Weltkarte
○ Übersichtskarte 1:500.000
● Digitale Orthophotos 2m
○ Digitale Orthophotos 20cm
○ Digitale Orthophotos (Infrarot) 20cm
○ Digitale Ortskarte
○ Weißer Hintergrund

Overlays

□ Digitale Flurkarte
□ Digitale Flurkarte (Umringe)
□ Telekom Hautpverteiler (Radien)
☑ Telekom Hauptverteiler (Standort
☑ Gewerbegebiete
□ Grabungsatlas-Lehrrohre
☑ Grabungsatlas-Abgeschlossene Maßnahmen
□ Grabungsatlas-Aktuelle Maßnahmen
☑ Grabungsatlas-Zukünftige Maßnahmen

```
[I0_LTITLE]
  Ortsnetzkennzahl (ONKZ)89
  Anschlussbereich (ASB)   812
  Postleitzahl             80999
  Ort                      M�nchen
  Strasse                  Theodor-Kitt-Str. 32
```

```
SISBY Gewerbegebiet
  Gemeindename             Unterhaching
  Gebietskennziffer        9184148
  Name Gewerbegebiet       3 / Am Sportpark
  Nummer Gewerbegebiet     312
  Verfügbare Fläche gesamt9100          qm
Gemeindename Unterhaching Gebietskennziffer 9184148 Name Gewerbegebiet 2 / Biberger Straße Nummer Gewerbegebiet 313 Verfügbare Fläche gesamt 22000 qm
```

Not Authorized

Figure: Screenshot of an OpenLayers client for UC1 showing a map comprised of protected OGC WMS provided by different organizations of the federation

As illustrated on the figure above, the current user can load the OpenLayers based client and see certain map layers of different WMS (using the GetMap operation), according to the need-to-know principle. Requesting detailed (textual) information via the GetFeatureInfo operation, the access is not granted if the point of interest is outside the authorized area.

The above example application leverages the Single-Sign-On quite heavily because the OpenLayers client is hosted at the Secure Dimensions Web Server, the WMS for the base layer (satellite image) is hosted at the Bavarian Mapping Agency and the Telekom overlays are served by the Chamber of Industry and Commerce.

THE USE OF STANDARDS

In order to build an Access Management Federation for spatial data and services based on OGC Web Services, existing open security standards and their implementations can be leveraged. An Access Management Federation that shall support Single-Sign-On can be established based on the OASIS standard Security Assertion Markup Language (SAML). This standard defines different Profiles and Bindings that ensure the use of the protected services via Web Browser and desktop clients by defining interoperable means of sharing user assertions. The aspect of access management, based on fine grained and spatial access rights can be implemented based on the OGC standard GeoXACML.

Security Assertion Markup Language

The Security Assertion Markup Language by OASIS defines in its version 2 the ability to express assertions about the identity of entities. In its core, it defines the XML dialect to encode the assertions. Different profiles exist that support the encoding of other assertions, e.g. for stating authorizations. In different profiles, SAML defines the means for exchaning assertions between the relying and asserting party. Different bindings are defined that support the actual exchange of the assertions via HTTP. SAML supports the use of W3C's XML Digital Signatures and XML Encryption to ensure integrity and confidentiality of the assertions exchanged, independent from a network layer communication protection, such as SSL or TLS.

In particular, the following SAML 2 Profiles and Bindings are in use:

Web Browser SSO Profile [SAML 2.0, Profiles, section 4.1]

The Web Browser SSO Profile describes the means to establish a new session with a Service Provider using an Identity Provider. It is important to emphasize that for this profile, the Service Provider initiates a user challenge to determine the home institution and thereby the Identity Provider to be used for login. This typically involves a Discovery Service, provided within this project by the Coordination Center.

This profile does not specify by which means the user actually logins in. This is up to the Identity Provider selected by the user.

This profile is only suitable for Desktop Clients if they implemented required features of a Web Browser. These features include processing of HTML, support for JavaScript and handling of HTTP redirects and Cookies. Therefore, technically this profile should be used for Web Browser applications only.

Enhanced Client or Proxy (ECP) Profile [SAML 2.0, Profiles, section 4.2]

The Enhanced Client or Proxy Profile supports to establish a new session with a Service Provider without the means of HTTP redirects (HTTP status code 302). Instead, the client is used as a relay for SOAP messages to be exchanged between the Service and the Identity Provider. This profile is kicked-off by the Service Provider if the client indicates the capabilities of supporting this profile, as defined by this profile. The associated HTTP Header elements and values have already been defined by the Liberty Alliance project. It is important to understand that it is not the duty of the Service Provider to initiate the user interaction for selecting the home institution. Instead, it is the duty of the client itself. This ensures that an appropriate, perhaps environment specific implementation inside the desktop client is possible.

This profile mandates HTTP Basic or Digest authentication as a login scheme provided by the Identity Provider.

In the context of a GeoAMF, this profile is suitable for desktop clients because it does not require html processing, nor does it require JavaScript support. However, it requires that the client implements support for IETF RFC 2818 (HTTPS) and IETF RFC 2965 (Cookies) and IETF RFC 2617 (HTTP Authentication).

Whereas the Web Browser SSO Profile provides the means for Single-Sign-On as a "build-in" feature, the ECP does not! It is up to the desktop client implementation to support Single-Sign-On.

HTTP POST Binding [SAML 2.0, Bindings, section 3.5]

The HTTP Post Binding is typically used with the Web Browser SSO Profile to securely exchange assertions between the Identity and Service Provider. Because we have experienced problems with application firewalls, this binding is not used in the federation directly. However, it is used to authenticate users as German citizens via an external eID Service.

HTTP Artifact [SAML 2.0, Bindings, section 3.6]

The HTTP Artifact binding describes a communication protocol between the client, Service and Identity Provider such that it avoids the direct exchange of assertions via the client. Different from the HTTP POST binding, where the user assertion is communicated from the Identity Provider to the Service Provider via the user's client, this binding only releases artifacts to the client and the actual assertion is exchanged between the Identity Provider and the Service Provider via a so called secure backchannel.

This binding was used for the project to securely exchange user assertions because of application firewall issues identified with the HTTP POST binding.

SAML SOAP Binding [SAML 2.0, Bindings, section 3.2]

The SAML SOAP Binding is used with the secure backchannel between an Identity and Service Provider to exchange user assertions. In the project setup, the communication is based on HTTPS with mutual authentication and the SOAP messages itself are encrypted and digitally signed as described by the W3C standards XML Encryption and XML Digital Signatures.

SAML Reverse SOAP (PAOS) Binding [SAML 2.0, Bindings, section 3.3]

The PAOS Binding is used with the Enhanced Client or Proxy (ECP) Profile, where the Service and Identity Provide sent SOAP encoded messages to the client that are to be relayed.

Geospatial eXtensible Access Control Markup Language

For establishing access control to enforce the rights of authenticated users, the OGC standard GeoXACML 1.0 is used.

Geospatial Access Control Markup Language

GeoXACML is an extension of the OASIS standard eXtensible Access Control Markup Language (XACML) 2.0. It defines the data type Geometry and functions according to the ISO Simple Features Specification (ISO 19125). It is thereby possible to perform geospatial processing in a GeoXACML policy to enforce access rights where geometries are involved.

Geographic access restrictions within this project exit in Use Case 1 where the Engineering Offices can only obtain planning information within their authorized area. For Use Case 3 geographic rights ensure that a citizen can only request detailed geographic information in the near vicinity around his property.

THE ACCESS MANAGEMENT FEDERATION FOR SPATIAL DATA AND SERVICES

The provision of protected spatial data and services is handled different within the federal states of Germany. Some of them have their own security gateway in a whole e-government solution. Others protect their data and services simply via https and username/password, however they often building up extra identity management systems to check authentication of users that do not belong to their own organization.

The challenge is to get protected data and services of different data and service providers into use because of their different application and system environments. For interoperability reasons the use of open standards is necessary and therefore in the context of security the use of SAML 2.0, XACML 2.0 and GeoXACML 1.0 is recommended in the architecture[3] of a SDI in Germany.

[3] http://www.gdi-de.org/download/AK/A-Konzept_v2_100909.pdf (only in German)

To show the technical feasibility of this open standards and considering a distributed identity and authorization management we set up an access management federation based on shibboleth.

Further information on this topic is figured out in the OGC Shibboleth IE Report[4] and in an article about Shibboleth Access Management Federations as an Organizational Model for SDI[5].

The entry point of this federation can be found at https://sp.gdi-de.org.

Architecture and Deployment

The architecture for the Access Management Federation for spatial data and services, realized during the project, leverages the exact same architecture as described for IT main stream Access Management Federations based on SAML.

However, the architecture of the realized GeoAMF extends the AMF concepts by (i) introducing GeoXACML based access control and (ii) the protected resources are OGC Web Services.

As illustrated in the figure below, the realized federation consists of different Service Providers (illustrated in blue) and different Identity Providers (illustrated in red). The Coordination Center that operates the Discovery Service and hosts the digitally signed federation metadata is located within the GDI-DE domain.

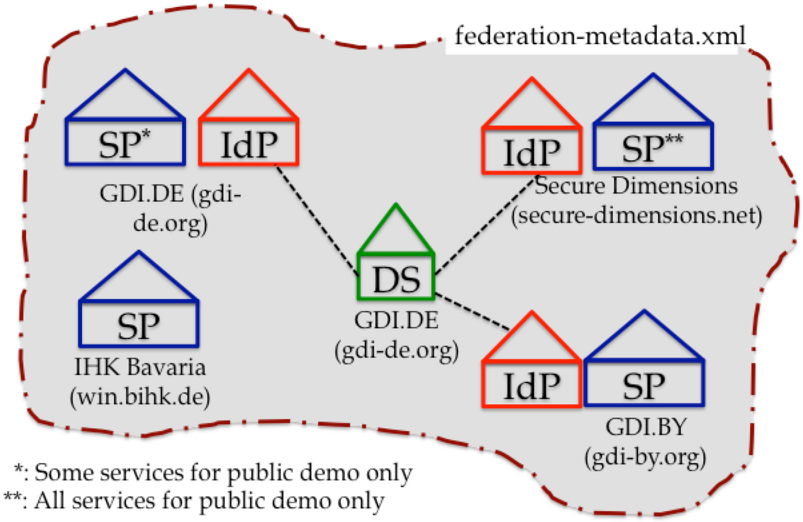

federation-metadata.xml
SP*
IdP
GDI.DE (gdi-de.org)
IdP
SP**
Secure Dimensions (secure-dimensions.net)
DS
GDI.DE (gdi-de.org)
SP
IHK Bavaria (win.bihk.de)
IdP
SP
GDI.BY (gdi-by.org)
*: Some services for public demo only
**: All services for public demo only

Figure: GeoAMF of the project "Betriebsmodell GDI-DE"

Even though this is a fairly small federation, it was large enough in terms of distribution and diversity of OGC Web Services to evaluate the given concept. In particular, the variation in domains (gdi-by.org, secure-dimensions.net, bihk.de and gdi-de.org) ensured to evaluate the Single-Sign-On requirement and the exchange of XML information cross domain.

[4] See OGC 11-019r2

[5] http://ijsdir.jrc.ec.europa.eu/index.php/ijsdir/article/view/245/295

Identity Management

Each organizational Identity Provider of the federation operates its own user management system. For this project, the user management system gets connected via LDAP and the user attributes are fetched from LDAP.

For the process of access control, the following two user attributes are released by the organizational Identity Providers

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

For a user that uses the new German ID card, the following attributes are used

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

In order to be compliant with the German regulations for privacy, the user is appointed that the first and given name will be used by the application and the user has the opportunity to deselect the dissemination of the name attributes. As a consequence, the user may have limited access to services of the federation.

Authentication via new German ID card

For the realized federation, the model that only organizational users can participate in the federation was extended. One specific IdP was deployed that supports the login via the new German ID card. In order to achieve this, a one-to-one trust relationship between the specific IdP and the so called eID-Service of the German "Bundesdruckerei", situated in Berlin was established. The Bundesdruckerei is the German Government agency that releases the new German ID card.

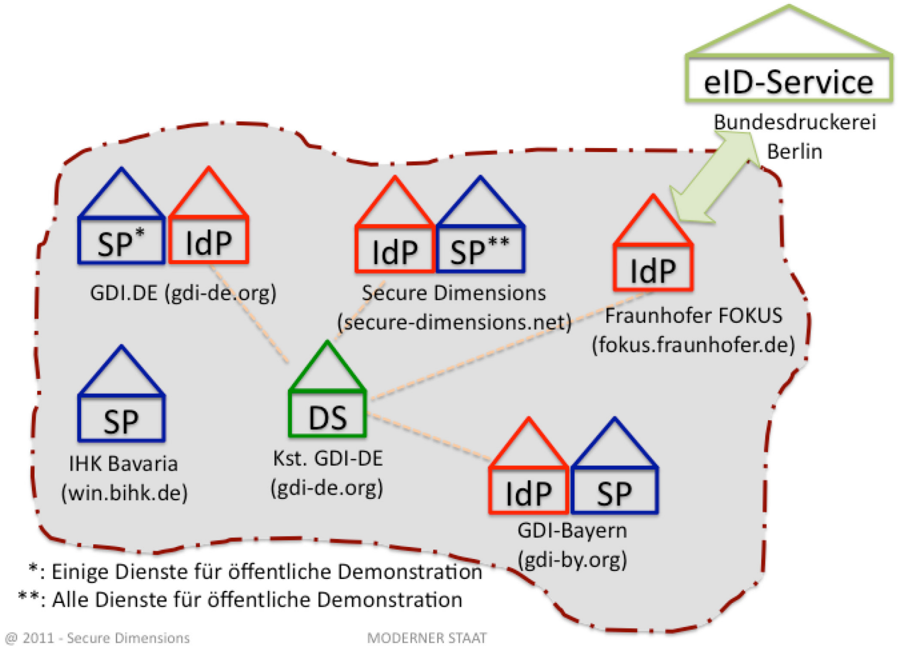


Figure: Extending the AMF for German ID card authentication

The trust relationship to the external eID-Service was established by asymmetric encryption with X.509 certificates, certifying each other party's identity. Furthermore, additional keys are involved that support to read certain attributes of the user.

In order to prevent unwanted information disclosure concerning personal information using the new German ID card authentication, encryption of SAML requests and responses takes place, when communicating with the eID Service.

The Identity Provider, provided by Fraunhofer FOKUS is based on the Shibboleth main stream IdP that was extended with a specific Login Handler. More information about the Login Handler for the new German ID Card is available at the Shibboleth IdP Contributions Page: https://wiki.shibboleth.net/confluence/display/SHIB2/Contributions

Data and Services

Each of the Service Provider makes the different types of geospatial information available via OGC Web Services. Mostly Web Map Services provide maps and additional feature information, but also Web Feature Services (Transactional) are available serving ensemble information and supports the update of the features as required by Use case 2.

Data Type	Service Type	Service URL
Raster data	WMS	https://sp.gdi-by.org/service/WMS/DFK
Vector data	WFS	https://sp.gdi-by.org/service/WFS/DFK
Raster data	WMS	https://sp.gdi-by.org/service/WMS/DTK25
Raster data	WMS	https://sp.gdi-by.org/service/WMS/LVG
Raster data	WMS	https://sp.gdi-by.org/service/WMS/LVG
Raster data	WMS	https://sp.gdi-by.org/service/WMS/LVG
Raster data	WMS	https://sp.gdi-by.org/service/WMS/DOK
Raster data	WMS	https://sp.gdi-by.org/service/WMS/DOP20
Raster data	WMS	https://sp.gdi-by.org/service/WMS/DOP20CIR
Raster data	WMS	https://sp.gdi-by.org/service/WMS/GA
Raster data	WMS	https://sp.gdi-by.org/service/WMS/PS
Vector data	WFS	https://sp.gdi-de.org/cgi-bin/securewfs
Raster data	WMS	https://win.bihk.de/service/WMS/TKHV
Raster data	WMS	https://win.bihk.de/service/WMS/GWG

Table: Data and Services (subset) of the Access Management Federation

It is important to note that all service URLS are using the HTTP*S* scheme.

Establishing a session with a Service Provider

The session establishment is identical as described in the SAML specification and therefore it is required to use HTTPS based connumication only! Any unknown user, requesting a secured service or application from a Service Provider must authenticate by the means described for a Web Browser or a Desktop Client.

For a Web Browser based client, such as an OpenLayers based client, the Browser gets redirected to the IdP, selected by the user. As each Service Provider supports decentralized IdP discovery, there is no visible stopover for the user when getting redirected to the Discovery Service. After the user has logged in with the means provided by the IdP, the Browser gets – after successful login – redirected back to the Service Provider and the response for the request is returned to the Browser if the user has the appropriate access rights.

For a Desktop Client, the decentralized IdP discovery support from the Service Provider cannot be used. Instead, the Desktop Client must provide a list of available IdPs to the user. After the user has selected an IdP, the Desktop Client will prompt the user for the login credentials via HTTP Basic or Digest Authentication.

After the user has successfully established a session with the first service provider, additional sessions with other Service Providers for the federation get established without bothering the user to login again. Single-Sign-On is guaranteed by any Web Browser client as long as JavaScript and Cookies are enabled. For a desktop application, the availability of the Single-Sign-On feature depends on the session management actually implemented in the desktop application.

Access Control

Each Service Provider enforces access rights on their services, hosted applications and geospatial information. For this project, two different deployment variations appeared:

1) A participating organization already has the OGC Web Service in operation and it is to be connected to the federation without modification.
2) A participating organization deploys an OGC Web Service to be used in the federation.

Situation 1) gets handled by setting up a Reverse Proxy using the Apache 2 web server. In order to enforce access rights, each communication to a service URL known within the federation is intercepted as described in the XACML information flow control. The Reverse Proxy, acting as a Policy Enforcement Point, uses the intercepted request to create a GeoXACML compliant Authorization Decision, sent to a Geospatial Policy Decision Point (GeoPDP). Based on the returned decision, the Reverse Proxy returns a service compliant exception or the intercepted request gets forwarded to the actual service. The response from the actual service is returned to the client and all URL information is modified to identify the proxy address and not the own address. For example, the response of the GetCapabilities request to a WMS will contain URLs to identify the network endpoint for the mandatory GetMap, the optional GetFeatureInfo and GetLegendGraphics request. However, the result of a GetMap request is not modified because it will not reveal internal information; it is just an image.

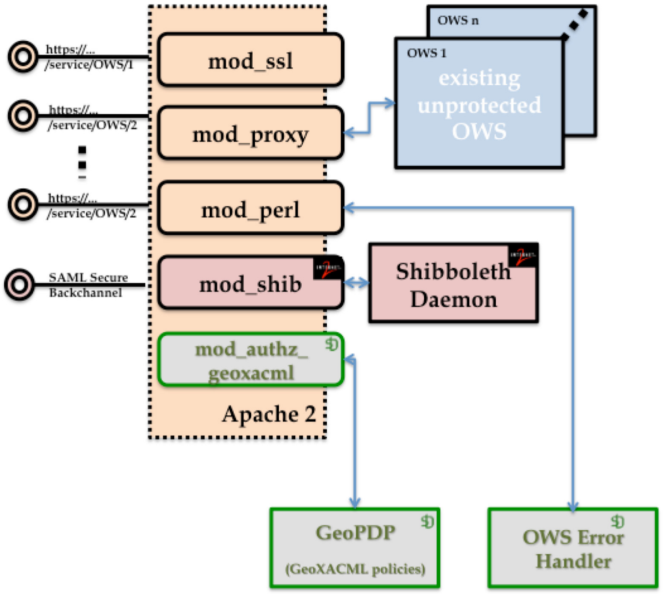


Figure: Modules of the Service Provider (WMS & WFS example)

The figure above illustrates an example setup of the Access Control system integrated with the Apache 2 Web Server. In terms of XACML information flow, the reverse proxy (see figure above) acts as Policy Enforcement Point. It is based on standard Apache 2 webserver modules. On the other hand, the Context Handler of XACML specification is implemented by the following Apache 2 webserver modules: mod_authz_geoxacml. This module accepts (in this setup) WMS and WFS-T (all versions) requests supporting HTTP GET and POST and separates the request parameters as well as the XML (through POST)to create a GeoXACML-standards based Authorization Decision Request. This module also implements the GeoXACML obligation handling to ensure that required adjustments of a OWS request or response can happen based on the access rights of the requesting user. For example, a WFS request can be modified to add geospatial conditions or the map image of a WMS can be modified to erase information for unauthorized areas.

The module can be loaded and configured from the Apache configuration file (httpd.conf). The important information that the modules need is the GeoPDP URL, because the GeoPDP will accept the Authorization Decision Request and return a decision.

In the case that access has to be rejected, the Error Handler ends the processing. The OWS Error Handler is implemented in Perl to ensure best flexibility to meet project specific needs, such as internationalization. It highly depends on the overall context how much information is to be released to the user in the case access rights are missing. This can vary from a simple “Not Authorized” to a “Please have your credit card ready and call 1-800-pay-good. In any case the Error Handler ensures that an OWS standards compliant exception is returned to the client. For example, the WMSErrorHandler returns an image according to the WMS GetMap request parameters if the exception parameter is “IN_IMAGE”. The text on the image may vary for the illustrated reason.

GeoXACML Policy

For the introduced Access Management Federation for spatial dats and services, access rights are bound to three different types of information:

1) The user’s home organization
2) The user’s role acting in the federation for the organization
3) The user’s first and given name (German ID card only)
4) The area of responsibility assigned to the organization

Applying this scheme to the users from the Engineering Offices as described in Use Case 1), the following matrix reflects the rights:

Engineering Office \ Role	ING-History	ING-Current	ING-Future
München (ING-Munich)	Rob	Joe	Amy
Nürnberg (ING-Nurenberg)	Clara	Steve	Marie
Bayern (ING-Bavaria)	Jane	Claris	Dave

Table: Users of Engineering Offices

The rights concerning roles (ING-History, ING-Current and ING-Future) are modeled according to the RBAC Profile of XACML 2.

The geographic restrictions in place for expressing the areas of responsibility for each Engineering Oficce are:

Engineering Office Munich / Nuremberg: Authorized area is 50 km radius around Munich / Nuremberg city centre

Engineering Office Bavaria: Authorized area is the state of Bavaria represented by a GML geometry.

Enforcing the geographic conditions involves the testing of topological relations and distances between geometries. As the restriction applies to the GetFeatureInfo operation of a WMS, the Authorization Decision Request will contain the point geometry that is identified by the request. The following figure illustrates a GeoXACML condition that implement the Munich restriction.

```
<VariableDefinition VariableId="Munich">
  <AttributeValue DataType="urn:ogc:def:dataType:geoxacml:1.0:geometry">
    <gml:Point gid="Munich" srsName="EPSG:4326" xmlns:gml="http://www.opengis.net/gml">
      <gml:coordinates cs=" " ts=",">11.575278 48.136944</gml:coordinates>
    </gml:Point>
  </AttributeValue>
</VariableDefinition>

<Condition>
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
    <Apply FunctionId="urn:ogc:def:function:geoxacml:1.0:geometry-is-within-distance">
      <Apply FunctionId="urn:ogc:def:function:geoxacml:1.0:geometry-one-and-only">
        <ResourceAttributeDesignator AttributeId="urn:ogc:def:profile:xacml:2.0:infopoint"
DataType="urn:ogc:def:dataType:geoxacml:1.0:geometry"/>
      </Apply>
      <VariableReference VariableId="Munich"/>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#double">50000</AttributeValue>
    </Apply>
  </Apply>
</Condition>
```

Listing: Condition matching 50km radius around Munich city centre

```
<VariableDefinition VariableId="Nuremberg">
  <AttributeValue DataType="urn:ogc:def:dataType:geoxacml:1.0:geometry">
    <gml:Point gid="Nuremberg" srsName="EPSG:4326" xmlns:gml="http://www.opengis.net/gml">
      <gml:coordinates cs=" " ts=",">11.077778 49.452778</gml:coordinates>
    </gml:Point>
  </AttributeValue>
</VariableDefinition>

<Condition>
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
    <Apply FunctionId="urn:ogc:def:function:geoxacml:1.0:geometry-is-within-distance">
      <Apply FunctionId="urn:ogc:def:function:geoxacml:1.0:geometry-one-and-only">
        <ResourceAttributeDesignator AttributeId="urn:ogc:def:profile:xacml:2.0:infopoint"
DataType="urn:ogc:def:dataType:geoxacml:1.0:geometry"/>
      </Apply>
      <VariableReference VariableId="Munich"/>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#double">50000</AttributeValue>
    </Apply>
  </Apply>
</Condition>
```

Listing: Condition matching 50km radius around Nuremberg city centre

As seen in the figure above, the condition is identical to the one for Munich, but the defined geometry is different. It represents the city center for Nuremberg and not – as before – for Munich.

The GeoXACML condition for the Bavarian Engineering Office requires to use the Bavarian state border as a GML geometry. For this project, an export of the state border from the productive system of the Bavarian Mapping Authority was used. Because of the high precision used, the extracted polygon consists of 120,000 points.

```
<VariableDefinition VariableId="Bavaria">
  <AttributeValue DataType="urn:ogc:def:dataType:geoxacml:1.0:geometry">
    <gml:Polygon gid="Bavaria" srsName="EPSG:4326" xmlns:gml="http://www.opengis.net/gml">
      <gml:outerBoundaryIs>
        <gml:LinearRing>
          <gml:coordinates>120,000 points from the production system ...</gml:coordinates>
        </gml:LinearRing>
      </gml:outerBoundaryIs>
    </gml:Polygon>
  </AttributeValue>
</VariableDefinition>

<Condition>
<Apply FunctionId="urn:ogc:def:function:geoxacml:1.0:geometry-within">
  <Apply FunctionId="urn:ogc:def:function:geoxacml:1.0:geometry-one-and-only">
    <ResourceAttributeDesignator AttributeId="urn:ogc:def:profile:xacml:2.0:infopoint"
DataType="urn:ogc:def:dataType:geoxacml:1.0:geometry"/>
  </Apply>
    <VariableReference VariableId="Bavaria"/>
  </Apply>
</Condition>
```

Listing: Condition matching within Bavarian State Border

Operational Readiness

Based on the undertaken evaluation within the project “GDI-DE Betriebsmodell” there is a strong indication that the technical setup is ready for operational use to build an Access Management Federation for spatial data and services. As for the operation of Access Management Federations around the globe, this project has also shown that high level tasks to establish the federation and maintain the list of trusted entities must be taken care of. In other words, there are also operational and not only technical requirements that must be taken care off. In particular, a coordination center must be setup that at least enforces the policies and procedures of the federation.

As one example, the role of the Coordination Center involves the verification of requests for joining the federation as an Identity or Service Provider. Among various tasks it is required to verify network endpoints, check availability and the compliance of certificates in place. The Coordination Center was also identified within the project to be responsible for maintaining the digital signature of the federation metadata, and hosting the federation metadata on a high available web server.

In order to get a better insight into the related requirements how to run an operational federation, during the project, the DFN (Deutsche Forschungsnetz e.V.) located in Berlin, who runs the Academic Federation in Germany (DFN-AAI), was consulted and asked for their experience and advice. Their strong recommendation was that the Coordination Center must also include a trouble support team to support users that need help.

One of the technical requirements, identified during the project was, that it is required to operate a 24/7 available web server that hosts the Discovery Service and potentially the federation metadata. Even though there is no great functional burden and performance on that web server, its safe guarding is one key aspect to be watched by the Coordination Center.