The EUMETSAT EO Portal and Clearinghouse Project

PV 2009 Conference

European Space Astronomy Centre (ESAC)
ESA, Villafranca del Castillo, Madrid, Spain
1-3 December 2009

Uwe Voges (con terra)
Michael Schick (EUMETSAT)
Marko Reiprecht (con terra)
Rafael Zarza (EUMETSAT)
Agenda

Introduction

Project History / Project Status

Information Models

System Overview

Product Navigator

Clearinghouse

IdentityProvider (IdP)- and UserManagement-Concept

Conclusion
EO Portal provides a single point of online access to EUMETSAT data and dissemination services

- Past: several applications with self contained user management
- Users had to register with every application and to memorise different user ids and passwords

EO Portal encapsulates the legacy applications and offers a harmonised user interface to discover, search, order / subscribe to data and services

Clearinghouse:

- allows users to access data and services of partner agencies (e.g. CNES Altimetry products, NOAA, WMO, ESA)
- vice versa: allows partner agencies to discover, search, order and subscribe to EUMETSAT data and services via a set of programmatic, interoperable services

- Services are based on OGC/HMA and INSPIRE EU specifications
Introduction

Some Services used programmatically (e.g. ordering) require user details passed using security concepts.

In order to implement this between different organizations:

>> A harmonized and standards based security concept is required

>> This involves the operation of a federated Identity Management System, including IdentityProvider (IdP)
2008:

- Started with architectural design phase accomplished by con terra
  - accompanied by comparison and selection of COTS/ Open Source SW
  - documented in a trade-off analysis
- Next step: Implementation of Collection Catalogue (called “Product Navigator”)
  - based on con terra’s terraCatalog SW
- Development of sophisticated security concept including IdentityProvider (IdP)-
  and UserManagement
  - based on SUNs OpenSSO

2009:

- first release of the Clearinghouse was launched:
  - integrating legacy systems for orchestrated user administration service calls
- Successful Experiment: to check interoperability with ESA/HMA UserManagement
- OGC/HMA based EO Product Search realized and integrated into Clearinghouse
- Presently:
  - Realization of the Order Service providing OGC/HMA Order Service Interface
  - WMS/WCS Prototype underway
Information Models

Different types of information are involved:

- especially (meta-)data for EO Product discovery and ordering

EO Metadata is provided and managed at Collection and Product level

Collection Metadata

- based on ISO19115-2 (conceptual model) and ISO19139 (encoding model)
- specific EUMETSAT requirements (e.g. channels of distribution) are described in ISO conformant extensions to ISO19115-2 and ISO19139-2

Product Metadata

- based on HMA´s “OGC GML Application Schema for EO Products”

Ordering / Subscription Information

- based on information model of OGC/HMA Order Services
- As the legacy systems use different information models for ordering / subscription, mappings between OGC/HMA Order and legacy models was important
System Overview

- **EO WebPortal**: main web-interface
- **Product Navigator UI**: web-interface for Metadata Discovery / Management
- **EO Product Search/Order/Subscription**: web-interface for discovery and ordering/subscription and Order-Follow-Up
- **UserManagement/IdP**
- **Clearinghouse**: provides OGC, INSPIRE and EUMETSAT-interfaces. Communicates with legacy systems and external partner agencies
- **MapServer**: provides WMS for definition of spatial filters and visualization of spatial extends of items
- **Data Centre/EAT/UNS**: EUM legacy systems for Product Discovery, Order/Subscription
- **Partner Agency Services**: provide their functionality via OGC/HMA web services
- **EO Portal Datastore**: Database Components (RDBMS, LDAP, files)
Product Navigator (navigator.eumetsat.int)

Matthew Schick et al.
PV2009 Conference
ESAC, Madrid, Spain, 1.-3 Dec 2009

responsible for Management and Discovery of Collection Metadata. Consists of:

- Web-UI for browse/search/discovery of Collection Metadata
- Components for Metadata Management
- Service component (Collection Catalogue Server): provides discovery and management of Collections via service interfaces

Web Search UI

- Search by combinations of spatial extent, content type, data format, keyword etc.
- Spatial extent is defined using selections within an OGC WMS based-interactive map
- Metadata details: URL can lead user to various applications or servers such as the EO Product Order for offline product search/order or online registration
For the metadata management different components are available:

- Web User-Interface (Metadata Editor) for insertion/editing of metadata entries
- Batch-import of XML encoded metadata files
- Periodical automatic harvesting of single XML encoded metadata files from known locations (also possible to automatic harvest metadata from other Catalogues)
- Export of metadata

provides different OGC CSW- and INSPIRE-service interfaces

Implementation based on con terra's sdi.Suite terraCatalog version 2.3.
Main goals

- Integration of legacy-systems and partner agencies via web-service interfaces
- Provision of programmatic interfaces to discover, search and order EO Data from EUMETSAT and partner external agencies
- Interfaces based on OGC/ESA/HMA- and INSPIRE-specifications:
  - OGC/HMA EO Product Discovery Interface (finished)
  - EO Product Ordering (work in progress)
  - User-Management (finished)
- Interfaces implemented as so called “Adaptors”:
  - …translate requests sent to interface, route it through Legacy Abstraction Layer to legacy system and their response back via the interface to requestor
2010 the OGC/HMA interface for EO Collection discovery (CIM EP) will be provided

- **Connector** will be integrated sitting on top of INSPIRE interface of Product Navigator
- Provides mapping between

  INSPIRE DS and CIM as defined in HMA-T

Start 2010 integrating partners based on the OGC/HMA interfaces

- processing is done by brokers
- broker handles requests from Adaptor by delegating sub-requests to Connectors
- **Connector** interacts with service (in specific format and interaction model)
- **Connector results** are integrated by broker and returned by the Adaptor in expected format of Clearinghouse interface

broker concept is already tested in the implementation of the UserAdminBroker

- This allows for retrieval and management of user-information within legacy systems

- Some Legacy systems already enhanced to support UserManagement concepts
Brokers in final version:

- **EO Collection Broker**: proceeds searches Collection-metadata in ProductNavigator and in partner agency collection catalogues
- **EO Products Broker**: proceeds searches for EO Product metadata on Data Centre and on external EO product catalogues
- **EO Order Broker**: supports ordering (subscription) of EO products from EUMETSAT or from partner agency order services

Clearinghouse is fully integrated with UserManagement concept

- protected services are secured by WS-Security and expect SAML2 tokens
- for interaction with protected services in other domains (e.g. partner companies), Clearinghouse must request SAML token from EO-Portal Security Token Service

Implementation is done with Java 6, XML/XSLT, Apache CXF and Mule 2

- **Mule 2**:
  - lightweight Java-based messaging framework
  - based on ideas from Enterprise Service Bus (ESB) architectures.
- For the integration with the UserManagement libraries had been developed.
UserManagement/IdP-Concept

builds up on OASIS SAML 2

centralized authentication, while user has different credentials at different providers

- Advantage: business entities maintain own user accounts, no global unique ID required

Concept differentiates between

- SSO at web applications
- the way how web services are secured

For SSO between web service consumer (WSC) and secured web service no global security token is required:

- because WSC is able to request new token for business entity at STS
- to be done via SAML2 AuthnRequest protocol and private/public key mechanisms

Trust in requesting entity at web service requires two things:

- First: valid and trusted signature of the whole request
- Second: valid and trusted security token from an IdP
IdentityProvider (IdP) components:

- **central login**: user authenticated via username/password
- user can only consume services within circle of trust, if authenticated at IdP

- **SingleSignOnService**: SSO between web applications. Interface specified in SAML2

- **User Registry** user profiles, mapping of local user ids to pseudonyms to provide user privacy during communications with services

- **IdP WebService** is secured by the WS-Security.
  - For calling: WSC needs to put security token in soap header
UserManagement/IdP-Concept

Service-Provider (SP):

- business web service; secured equally to IdP WebService
- SP User Registry manages local user profiles
- AssertionConsumerService endpoint of SSO between web applications at SP: interface specified in SAML2

Supports HMA UserManagement

- IdPs AuthenticationService validates user credentials and creates HMA security token (SAML1) on authenticate request
- token can be used by HMA federating entity to consume web services provided by EO-Portal.
Conclusion

Provision of interoperable access to data of GS is important

Effort for becoming familiar with those standards and migrating legacy systems towards those goals is quite high

Introduction of components towards an interoperable infrastructure is advisable to be taken with little steps

- Prototyping of components and concepts are essential prior introducing those into operations

With the complexity of standards expertise from external consultants is required, if it is not possible to have staff completely allocated to such domains

The approach taken by EUMETSAT towards a harmonized/interoperable infrastructure will be continued in 2010

For this it is:

- important that standards remain stable
- partner organizations invest into an interoperable infrastructure so that an exchange of data is possible and beneficial to the end users