Open Geospatial Consortium, Inc.

Date: 2009-09-11

Reference number of this document: OGC 09-063

Version: 0.3.0

Category: Public Engineering Report

Editor: Lewis Leinenweber

OGC® OWS-6 GeoProcessing Workflow (GPW) Thread Summary Engineering Report

Warning

This document is not an OGC Standard. This document is an OGC Public Engineering Report created as a deliverable in an OGC Interoperability Initiative and is not an official position of the OGC membership. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an OGC Standard. Further, any OGC Engineering Report should not be referenced as required or mandatory technology in procurements.

Document type:	OpenGIS® Public Engineering Report
Document subtype:	NA
Document stage:	Approved for Public Release
Document Language:	English

Preface

This document summarizes the work accomplished in the GeoProcessing Workflow (GPW) thread of the OWS-6 Testbed and provides an outlook for potential areas for work to be done in future testbeds.

Forward

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 Inc. 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.

OWS-6 Testbed

OWS testbeds are part of OGC's Interoperability Program, a global, hands-on and collaborative prototyping program designed to rapidly develop, test and deliver Engineering Reports and Change Requests into the OGC Specification Program, where they are formalized for public release. In OGC's Interoperability Initiatives, international teams of technology providers work together to solve specific geoprocessing interoperability problems posed by the Initiative's sponsoring organizations. OGC Interoperability Initiatives include test beds, pilot projects, interoperability experiments and interoperability support services - all designed to encourage rapid development, testing, validation and adoption of OGC standards.

In April 2008, the OGC issued a call for sponsors for an OGC Web Services, Phase 6 (OWS-6) Testbed activity. The activity completed in June 2009. There is a series of on-line demonstrations available here: http://www.opengeospatial.org/pub/www/ows6/index.html The OWS-6 sponsors are organizations seeking open standards for their interoperability requirements. After analyzing their requirements, the OGC Interoperability Team recommended to the sponsors that the content of the OWS-6 initiative be organized around the following threads:

1. Sensor Web Enablement (SWE)
2. Geo Processing Workflow (GPW)
3. Aeronautical Information Management (AIM)
4. Decision Support Services (DSS)
5. Compliance Testing (CITE)

The OWS-6 sponsoring organizations were:

- U.S. National Geospatial-Intelligence Agency (NGA)
- Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD)
- GeoConnections - Natural Resources Canada
- U.S. Federal Aviation Agency (FAA)
- EUROCONTROL
- EADS Defence and Communications Systems
- US Geological Survey
- Lockheed Martin

- BAE Systems
- ERDAS, Inc.

The OWS-6 participating organizations were:
52North, AM Consult, Carbon Project, Charles Roswell, Compusult, con terra, CubeWerx, ESRI, FedEx, Galdos, Geomatys, GIS.FCU, Taiwan, GMU CSISS, Hitachi Ltd., Hitachi Advanced Systems Corp, Hitachi Software Engineering Co., Ltd., iGSI, GmbH, interactive instruments, lat/lon, GmbH, LISAsoft, Luciad, Lufthansa, NOAA MDL, Northrop Grumman TASC, OSS Nokalva, PCAvionics, Snowflake, Spot Image/ESA/Spacebel, STFC, UK, UAB CREAF, Univ Bonn Karto, Univ Bonn IGG, Univ Bunderswehr, Univ Muenster IfGI, Vightel, Yumetech.

Contents

Page

Tables

Page

OGC® OWS-6 GeoProcessing Workflow (GPW) Thread Summary Engineering Report

1 Introduction

1.1 Scope

This OGC® document summarizes work completed in the GeoProcessing Workflow thread of the OWS-6 Testbed.

This OGC® document is applicable to the OGC Interoperability Program testbed.

1.2 Document contributor contact points

All questions regarding this document should be directed to the editor or the contributors:

Name	Organization
Lewis Leinenweber	BAE Systems, Inc

1.3 Revision history

Date	Release	Editor	Primary clauses modified	Description
2009-05-15	0.0.1	Lewis Leinenweber	All	Initial document
2009-05-22	0.1.0	Lewis Leinenweber	Clause. 7	Added recommendations for future testbed work
2009-06-04	1.0	Lewis Leinenweber	Clause 7, and various	Updates and edits for Future Work; and other minor edits
2009-08-03	0.3.0	Carl Reed	Various	Prepare for publication as PER

1.4 Future work

Improvements in this document are desirable to completely and accurately document the work completed in the OWS-6 GeoProcessing Workflow thread.

Additionally, ideas for work to be considered for future testbeds can be found in Clause 7 at the end of this document.

2 References

The following documents are referenced in this document. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. For undated references, the latest edition of the normative document referred to applies.

RFQ/CFP for Web Services Initiative - Phase 6 (OWS-6), Annex B - OWS-6 Architecture, issued 21 July 2008

OGC 06-121r3, *OpenGIS® Web Services Common Specification*

OGC 09-035, *OWS-6 Security Engineering Report (draft)*

OGC 09-036r1, *OWS-6 GeoXACML Engineering Report*

OGC 09-037, *OWS-6 UTDS-CityGML Implementation Profile*

OGC 09-038, *OWS-6 GML Profile Validation Tool Guidelines Engineering Report*

OGC 09-041r1, *OWS-6 WPS Grid Processing Profile Engineering Report*

OGC 09-053r3, *OWS-6 GeoProcessing Workflow Architecture Engineering Report*

3 Terms and definitions

For the purposes of this report, the definitions specified in Clause 4 of the OWS Common Implementation Specification [OGC 06-121r3] shall apply. In addition, the following terms and definitions apply.

3.1
Security domain
An environment or context that is defined by security policies, security models, and a security architecture, including a set of system resources and set of system entities that are authorized to access the resources. An administrative domain may contain one or more security domains. The traits defining a given security domain typically evolve over time.

3.2
Authentication
Verification that a potential partner in a conversation is capable of representing a person or organization

3.3
Authorization
Determination whether a subject is allowed to have the specified types of access to particular resource

Grid
A system that coordinates resources that are not subject to centralized control using standard, open, general-purpose protocols and interfaces to deliver nontrivial qualities of service

3.4
Non-repudiation
Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information.

3.5
Proxy
An agent that acts on behalf of a requester to relay a message between a requester agent and a provider agent. The proxy appears to the provider agent Web service to be the requester. (W3C)

3.6
Trust
The characteristic that one entity is willing to rely upon a second entity to execute a set of actions and/or to make set of assertions about a set of subjects and/or scopes

4 Conventions

4.1 Abbreviated terms

BPEL	Business Process Execution Language
DDMS	DoD Discovery Metadata Standard
GeoPDP	Geospatially-enabled Policy Decision Point
GeoXACML	Geospatial eXtensible Access Control Markup Language
GPW	GeoProcessing Workflow
HPC	High Performance Computing
IC-ISM	Intelligence Community Metadata Standard for Information Security Marking
JSDL	Job Submission Description Language
NSG	National System for Geospatial Intelligence
OGF	Open Grid Forum
PAP	Policy Administration Point

PDP	Policy Decision Point
PEP	Policy Enforcement Point
RPC	Remote Procedure Call
SAGA	Simple API for Grid Applications
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
STS	Security Token Service
TPS	Token Processing Service
WfMC	Workflow Management Coalition
WfXML	Workflow XML
WPS	Web Processing Service
WS-DAI	Web Service Data Access and Integration
WSDL	Web Services Description Language
WSRF	Web Services Resource Framework
XACML	eXtensible Access Control Markup Language
XPDL	XML Processing Definition Language

5 GeoProcessing Workflow (GPW) Overview

The Geo-Processing Workflow (GPW) thread in OWS-6 aimed to develop and demonstrate interoperability among geo-processes through service chaining, workflow and web services, with emphasis on implementing security capabilities for OGC web services, including SWE services. Work in this thread built on the results from previous testbeds, which includes authentication/authorization from OWS-4 and SOAP/WSDL recommendations from OWS-5. The workflow and security tasks exercised OGC and other web service across three operational security environments: 1) internal to a single trusted domain; 2) between two trusted domains; and 3) between a trusted and non-trusted (or temporarily-trusted) domain. The foundation of this work used already approved existing workflow and security standards from OGC and others such as W3C, OASIS, etc when applicable.

The results in the GPW thread were realized through a workflow scenario to demonstrate interoperability in a service-oriented architecture and RESTful architecture. Outcomes of the tasks and associated demonstrations were documented in Engineering Reports.

The main topics for investigation and experimentation in the OWS-6 GPW thread were as follows:

- Security for OGC Web Services
- Asynchronous Workflows & Security
- Grid-Enabled Web Processing Service (WPS) profiles
- GML Application Schema Development, Validation & ShapeChange Enhancements

5.1 GPW Engineering Reports and Documents

Engineering Reports and other related documents developed and delivered as outcome of the GPW thread are shown in Table 1.

Table 1, GPW Engineering Reports (ERs) and Documents

OGC Doc #	Document Title	Editor
09-035	OWS-6 OGC Web Services Security ER	con terra / IP Team
09-036r1	OWS-6 GeoXACML ER and associated XACML documents	UniBW
09-037	OWS-6 Urban TDS Implementation Profile ER	interactive instruments
09-037 (xsd)	OWS-6 CityGML application schema Urban TDS	interactive instruments
09-038	OWS-6 GML Profile Validation Tool Guidelines ER	interactive instruments
09-039	OWS-6 CityGML CR	interactive instruments
09-041	OWS-6 WPS – Grid Processing Profile ER	Univ of Muenster (IfGI)
09-053r3	OWS-6 GeoProcessing Workflow ER	Univ of Muenster (IfGI)

5.2 GPW Implemented Web Services and Components

The following services and components were developed and deployed to demonstrate and test capabilities being investigated in this thread:

Table 2, GPW Implemented Services and Components

Service/Component	Participant
PEP (WFS – Airport features) (fine-grained access using obligations)	con terra
PEP (WFS – City features)	con terra
PEP (JPIP/WCS-T)	con terra
PEP (W3DS)	con terra
PEP (WFS) (course-grained access)	con terra
PEP (AA-FL Gateway to WCS-T)	con terra
Airport-Federal Gateway to WCS-T	con terra
PDP (WCS-T in Federal Domain)	con terra
PDP (WPS for workflow)	con terra
PDP (W3DS)	con terra
Security Token Service (STS) (Airport domain)	con terra
Security Token Service (STS) (Federal domain)	con terra
Security Token Service (STS) (Regional domain)	con terra
PEP Proxy (configurable for multiple PEPs)	con terra
GeoPDP (WFS – Airport features)	AM Consult
GeoPDP (WFS – City features)	AM Consult
PEP (WMTS – UAB) (REST and SOAP)	Geomatys
PEP Proxies (2) (WMTS – UAB (REST and SOAP)	Geomatys
PEP (2) (WMTS – LISASoft) (REST and SOAP)	Geomatys
PEP Proxies (2) (WMTS – LISASoft)(REST and SOAP)	Geomatys
PEP (WFS - Airport Features)	Geomatys
PEP Proxy (WFS - Airport Features)	Geomatys
PEP (WFS - City features - UTDS)	Geomatys
PEP Proxy for WFS (City Features)	Geomatys
RESTful Workflow API/engine	Vightel
BPEL Workflow engine	GMU
WPS – Grid Processing (TrajectoryService)	STFC
WPS - Grid Processing (Plume Service)	Univ of Muenster (IfGI)
WPS - Grid Processing (Debris Flow)	GIS.FCU
GML Profile Validation Tool	LISASoft
Enhanced UGAS ShapeChange Tool	interactive instruments
WFS - CityGML Urban TDS (Airport)	interactive instruments

Service/Component	Participant
WFS - CityGML Urban TDS (City)	interactive instruments
CityGML instance (datasets) for Urban TDS (Airport & City)	interactive instruments
CS/W ebRIM profile with associated metadata	Galdos
Client for CityGML / Urban TDS	Univ of Bonn – Karto
GIS Desktop Client (ArcEditor)	ESRI

6 Security for OGC Web Services

In this thread, a work environment was deployed to address security architecture and implementations within and across three different security domains. The services and components were implemented to analyze security requirements, evaluate solutions and make recommendations to address web security issues in these three operational environments.

The security services work in this testbed built on the results of OWS-4 (authentication/authorization) and OWS-5 (SOAP/WSDL) as part of a solution.

Relevant specifications, standards and other OGC documents used in this thread are listed in Table 3

Table 3, Relevant Security Specifications, Standards and OGC Documents

Relevant Security Specifications, Standards and OGC Documents
WS-Security v1.1
WS-Trust v1.3
WS-Policy
WS-ReliableMessaging
WS-Federation
XML Digital Signature
XML Encryption
Security Access Markup Language (SAML) v 1.1, v2.0
XML Access Control Markup Language (XACML) v1.0, v1.1, v2.0
Geospatial eXtensible Access Control Markup Language (GeoXACML) (OGC 07-026r2)
OWS-4 Trusted GeoServices (OGC 06-107r1)
OWS-4 GeoDRM Engineering Viewpoint and supporting Architecture (OGC 06-184r2)
Geospatial Digital Rights Management Reference Model (GeoDRM RM) (OGC 06-004r3)
ISO 15000, 15408, 15443, 10181

6.1.1 Security Domain Environments

Three security domain environments were deployed for this thread:

- Internal – web services entirely defined within a single domain (i.e. private network).
- External (trusted) – web services accessed, exercised, and called between domains which are trusted.
- External (non-trusted) – web services accessed, exercised, and called between trusted and non-trusted or temporarily trusted domains.

6.1.2 Web Services Security Environments and Solutions

GPW requirements defined in the OWS-6 RFQ were realized by development and deployment of the following type of components to enable an operational security environment. Instances of these components were deployed for test along with implementations of web services and workflows within and across three security operational domains:

- Policy Enforcement Point (PEP) or Gatekeeper.[1]
- Policy Decision Point (PDP)
- Secure Token Service (STS)
- Token Processing Service (TPS)
- Policy Administration Point (PAP)*

* The PAP was not implemented as a separate entity exposed as a service; rather it was provided as a manual interface to maintain policies in the PDP by direct edit and administration.

A variety of OGC web services were deployed and exercised in an operational scenario to test the security capabilities within and across the three security domains. Web services that supported different binding patterns, such as SOAP and REST, were deployed to investigate functionality, interoperability and possible version-related differences in function.

Two different integrated clients were used to exercise components in the deployed service and security architecture:

- XNavigator provided by University of Bonn – Karto - a thin-based client also having 3D capabilities;
- ArcEditor provided by ESRI – a GIS Desktop application (thick) client.

These clients were used to authenticate/authorize users and allow for selection of the appropriate target resource via a Security Proxy software component.

[1] Para. 7.1, Architecture in OGC 06-184r2, GeoDRM Engineering Viewpoint and supporting Architecture

The working environment exercised non-repudiation mechanisms and experimented with both network layer and message layer security to identify the different options provided by the different approaches.

The optional Web single sign on (SSO) system described in the RFQ was not implemented as part of the GPW working environment.

The outcomes of tasks performed by Participants in the GPW thread relative to the security aspects for service implementations and integration as described in the RFQ are shown in Table 4.

Table 4, Goals in GPW Thread to Address Security in Real World Scenarios

Goals and Recommendations to Address Security aspects in the context of a real-world scenario	Thread outcome
Asynchronous workflows exercised internal to a single trusted domain and with other trusted and non-trusted domains	Achieved
Security for OGC web services exercised to include REST, SOAP and OGC services that don't deploy SOAP	Achieved
Interoperability of OGC web services exercised which implement different versions of security standards such as SAML 1.1 and SAML 2.0; and SOAP 1.1 and SOAP 1.2.	Partially achieved
Data access restrictions exercised using attribute level restrictions based on U.S. Department of Defense IC-ISM security markings and geographic area restrictions using GeoXACML.	Achieved
Audit trail reporting exercised; for example for data - who accessed, when it was accessed, what data was accessed.	Not achieved
Non-repudiation mechanisms exercised.	Achieved
Message layer and network layer security aspects analyzed and evaluated.	Achieved

6.2 Asynchronous Workflows & Security

Participants in the GPW thread performed tasks to investigate, evaluate and deploy asynchronous workflows that required access to services and resources involving three separate security domains.

Workflow implementations in this testbed focused on two approaches:

1. Workflow engine-independent solutions for workflow management that build on work completed in OWS-5 using standards defined by the Workflow Management Coalition (WfMC) such as WfXML, WfXML-R and XPDL;

2. Continue work to develop and employ asynchronous workflow capabilities using BPEL workflow language and associated workflow engine.

6.3 Grid-Enabled Web Processing Service (WPS) Profiles

The goal of WPS Grid Processing tasks in OWS-6 was to investigate, define and implement a WPS Grid Processing Profile, which is integrated with a grid computing infrastructure using relevant specifications. As an outcome, findings and recommendations resulting from efforts to implement the WPS Grid Processing Profile service were documented. The WPS Grid Processing Profile Engineering Report provides guidelines for users and developers to implement a WPS with access to distributed resources in a Grid Computing infrastructure.

Results from this testbed demonstrated that the WPS specification is mostly sufficient for accessing distributed Grid resources. Thus, instead of developing several candidate profiles for the WPS, several Grid Computing WPS processes were developed and demonstrated in the context of different real-world scenarios. One instance was developed that defined conventions for including JSDL-related parameters in a WPS request.

The Open Grid Forum (OGF) has a family of specifications that can be applied to accessing distributed computing and data resources. Relevant specifications include, but are not limited to, the HPC-Basic Profile, the Simple API for Grid Applications (SAGA), Grid-RPC, the Data Access and Integration set of specifications (WS-DAI-*), and the Web Services Resource Framework (WSRF).

For the OWS-6 Interoperability testbed, two ways to make use of OGF and related specifications, concepts and their implementations were identified. First, WPS can interact with distributed computing resource in the backend (encapsulating other resources). Secondly, the WPS can become a fully embedded resource accessed by middleware (integration alongside other services).

In the GPW thread, four geospatial services for performing distributed processes in a Grid Computing environment were implemented as WPS processes (encapsulation of distributed resources).

Two services where developed for the OWS-6 GPW Airport Demonstration Scenario:

- WPS Trajectory Service process
- WPS Plume Service process

Two other services where developed for the OWS-6 GPW Debris Flow Demonstration Scenario:

- WPS Rainfall Interpolation process
- WPS Geophone Analysis process

6.4 GML Application Schema Development, Validation and ShapeChange Enhancements

The work in this task area for a number of testbeds has been focused on evaluating emerging formats for the exchange of geospatial information across the U.S. National System for Geospatial Intelligence (NSG) enterprise, to include transfer of information through Coalition networks. In OWS-6 testbed work was undertaken to test the feasibility to create GML application schema based on OGC's Geography Markup Language Version 3.2.1 and OGC's CityGML to encode NSG data and serve as a transfer format among NSG participants. As a result, the CityGML profile for Urban Topographic Dataset (UTDS) requirements was developed based CityGML v.1.0 and the DGIWG Profile(s) of ISO 19107 that support three-dimensional geometry/topology.

Enhancements were developed for the current ShapeChange tool to incorporate incremental changes to address issues discussed with the Sponsor.

A GML Profile Validation tool was developed based on the DuckHawk testing framework. This tool is hosted and available at the Codehaus open source repository. Links to the repository are:

- Source code is available here: http://svn.codehaus.org/duckhawk/trunk/

- OWS6 specific things are in the module OWS6 here: http://svn.codehaus.org/duckhawk/trunk/ows6/

7 Recommendations for Future Testbed Work

7.1 GeoProcessing Workflow

- Investigate how to use hybrid workflow with SOA and ROA workflow concepts and participants.
- Define and demonstrate how to map security aspects from SOA to ROA and vice versa.
- Continue to advance security concepts to include licensing in workflows
- Investigate how to automatically assemble workflows based on semantic ontology concepts.
- Investigate techniques and approaches to improve Human Interaction in a workflow.
- Investigate how cloud computing relates to GeoProcessing and Workflow.
- Define and demonstrate how to implement semantics in standard service descriptions.
- Define and demonstrate how to use semantics in standard discovery and in data retrieval.
- Define and demonstrate semantic validation in an operational environment; what support infrastructure is required?

7.2 OGC Web Service Security

- Investigate, define and demonstrate use of additional metadata, such as access constraints, in service metadata can be made available for discovery and binding to secured web services. Investigate further the use of WS-MetadataExchange as a possible solution in conjunction with WS-Policy.
- Investigate and demonstrate how a catalog service can support content metadata for secured services that would allow appropriate level of information to be published without violating access constraints or adversely affecting performance.
- Investigate and recommend approaches and metadata content to use for harvesting/registering secured web services (e.g., that use a PEP as gatekeeper to control access to the underlying resource).
- Investigate and recommend alternative approaches to allow separation of concerns when requesting service capabilities metadata; such as, separation of binding, content and security policy information.
- Investigate and recommend possible additional Error messages when an exception occurs for secured services. Need to consider a balance between preventing inadvertent information leakage and providing useful information to the requestor to assist with correcting such error conditions.
- Evaluate issues with regard to ‘blocking’ and ‘filtering’ data in a service response as it relates to secure service requests. Develop recommendations and guidance for approaches to provide adequate information in the response, while addressing the issue of potential information leakage.
- Investigate and make recommendations for standardized use of service-specific obligations. Evaluate, compare and recommend approaches to define access control policies using GeoXACML and Obligations in XACML. Compare and contrast relative merits and prepare recommendations for best practices using OGC web services.
- Evaluate performance factors associated with various architectures and approaches to applying security mechanisms for use with OGC web services. Such approaches would include use of GeoXACML, XACML and obligations and potentially others. Perform selected tests of OGC web service types (WMS, WFS, WCS, etc.) to compare and contrast performance of each approach using common criteria leading to form recommendations for suitability by service type, architecture or other application criteria. Identify critical factors that influence performance measures.

7.3 Grid Processing

7.3.1 Service Level Agreements

- Investigate and assess and demonstrate use of standards and standard approaches to establish and use Service Level Agreement (SLA). The SLA formalizes a business relationship and enables contractual parties to measure, manage and enforce certain Quality of Service (QoS) guarantees. Therefore, attaching SLA functionality to OWS will pose a great advancement for future business models.

Grid Computing is a promising technology for actively enforcing the promised service quality goals from within the SLAs.

7.3.2 Cloud Computing

- Investigate and assess standards, methods and implementation approaches for use of OGC web services, most probably WPS Grid profile, with cloud computing infrastructures. The emerging term Cloud Computing is one of the latest trends in the mainstream IT and overlaps with some concepts of distributed and Grid Computing. Cloud Computing collects a family of well-known methods and technologies like Software as a Service (SaaS), Virtualization and Grid Computing and describes a paradigm of outsourcing specific tasks to a scalable infrastructure and consequently enabling new business models. There are a number of open issues for cloud computing; for examples see the "Open Cloud Manifesto[2]”. Nevertheless, the Cloud Computing paradigm is promising for geospatial applications to enable new and promising business models.

7.3.3 Refactoring OGC Service(s) model to support Grid

- Investigate and recommend approaches and test specific implementations where limitations of the OGC specifications that would benefit from a refactoring under Web Service Resource Framework (WSRF), especially as it relates to WPS grid profiles and grid computing. Some factors that may be considered are as follows:
    - **Service tied to data.** OGC data services such as WMS, WFS, and WCS make no distinction between the service instance and the data source – the data must be ‘known’ to the service. Typically, a data provider must also provide the OGC service. This can lead to ‘brittle’ architectures, and prohibits resource-sharing. Grid technology, on the other hand, encourages architectures that leverage multiple (separate) data and compute resources – a data provider need not also provide services.
    - **Latency.** OGC data services such as WMS, WFS, and WCS operate in a synchronous request-response mode. There is no mechanism for handling latency associated with very large requests. Again, this leads to brittle architectures – especially where workflow requires data outputs to be chained to processing service inputs. The WSRF suites of specifications for Grid services provide standard notification mechanisms for dealing with latency.
    - **Service coherence model.** There is no formal model integrating data resources behind OGC service instances – that is, there is no mechanism for asserting that the same data is exposed as visualization (WMS), gridded coverage (WCS) or feature instances (WFS). The implied resource pattern of WSRF, however, provides a mechanism for identifying unambiguously the data resource behind a service.

[2] http://opencloudmanifesto.org/

  - **Workflow abstraction.** Since OGC specifications bind data and services, there is no mechanism to abstract workflows in terms only of data and operations.
  - **OGC service consistency.** OGC Web Processing Service (WPS) uses a different model for identifying data than data services such as WMS, WFS, and WCS – an external data resource may be identified by URL. Again, the use of WS-Addressing in WSRF offers an opportunity to unify the mechanism for identifying data across all the OGC services.

7.3.4 Security and the Grid

- Investigate, demonstrate and recommend how OGC web service security approaches that can be integrated with Grid security mechanisms

7.4 GML Application Schema Processing and ShapeChange

- Develop enhancements to ShapeChange tool to address existing and emerging application schema modeling and mapping issues.
  - Investigate further use of constraints/validation in ShapeChange, which includes modeling in UML/OCL, converting to Schematron and publishing so that the can be accessed via http, and possibly adding support for geometrical/topological constraint checking.
  - Investigate interaction with dictionaries at run-time in ShapeChange, which includes code list dictionaries, constraint dictionaries, CRS/UOM dictionaries, schema repositories, etc.
- Refine capabilities and usability aspects for newly developed GML Profile Validation tool. Demonstrate applicability and use for additional profiles.