Remote Sens. **2011**, *3*, 1234-1250; doi:10.3390/rs3061234

OPEN ACCESS

Remote Sensing

ISSN 2072-4292

www.mdpi.com/journal/remotesensing

Article

Post-Disaster Image Processing for Damage Analysis Using GENESI-DR, WPS and Grid Computing

Conrad Bielski [1,⋆], Simone Gentilini [2] and Marco Pappalardo [3]

[1] Institute for the Protection and Security of the Citizen, Joint Research Centre of the European Commission, via Enrico Fermi 2749, I-21027 Ispra, Italy

[2] Institute for Environment and Sustainability, Joint Research Centre of the European Commission, via Enrico Fermi 2749, I-21027 Ispra, Italy; E-Mail: simone.gentilini@gmail.com

[3] Telespazio S.p.A., via Tiburtina 965, I-00156 Rome, Italy; E-Mail: marco.pappalardo@telespazio.com

⋆ Author to whom correspondence should be addressed; E-Mail: Conrad.Bielski@jrc.ec.europa.eu; Tel.: +39-332-789-233; Fax: +39-332-785-154.

Received: 11 April 2011; in revised form: 2 May 2011 / Accepted: 3 June 2011 / Published: 14 June 2011

Abstract: The goal of the two year Ground European Network for Earth Science Interoperations-Digital Repositories (GENESI-DR) project was to build an open and seamless access service to Earth science digital repositories for European and world-wide science users. In order to showcase GENESI-DR, one of the developed technology demonstrators focused on fast search, discovery, and access to remotely sensed imagery in the context of post-disaster building damage assessment. This paper describes the scenario and implementation details of the technology demonstrator, which was developed to support post-disaster damage assessment analyst activities. Once a disaster alert has been issued, response time is critical to providing relevant damage information to analysts and/or stakeholders. The presented technology demonstrator validates the GENESI-DR project data search, discovery and security infrastructure and integrates the rapid urban area mapping and the near real-time orthorectification web processing services to support a post-disaster damage needs assessment analysis scenario. It also demonstrates how the GENESI-DR SOA can be linked to web processing services that access grid computing resources for fast image processing and use secure communication to ensure confidentiality of information.

Keywords: post-disaster; building damage assessment; web processing service; security; image processing

1. Introduction

When disaster strikes over a populated area, geospatial information about the state of the afflicted region is paramount. Remotely sensed imagery acquired by satellites are usually among the first types of image data made available to analysts to produce maps. Since disasters can occur at any moment, an automated process can be conceived to do the following: image discovery, access, processing, and dissemination. This paper presents one of the Ground European Network for Earth Science Interoperations-Digital Repositories (GENESI-DR) [1,2] project technology demonstrators developed in the context of an operational post-disaster damage needs assessment scenario.

The Joint Research Centre of the European Commission (JRC) is involved in post-disaster damage assessment analysis both inside and outside the European Union. Primary analysis is based on remotely sensed imagery using both pre- and post-disaster images whereby analysts identify damage extent and severity. Soon after the team has been alerted to a disaster, the following scenario is generally played out as quickly as humanly possible:

1. Disaster alert identifying location and disaster type is received (via online alerting system or government representative);
2. Search and download pre-disaster imagery if available;
3. Order/Acquire and download post-disaster imagery as soon as possible;
4. Analyse pre- and post-disaster imagery to identify affected populated areas;
5. Produce and disseminate maps and reports to stakeholders based on the most current available information.

Technically, items 1 to 4 of the above described scenario can be automated. The developed technology demonstration presented in this paper was specifically focused on automating these aspects of the scenario by using currently available web and computing technologies as well as technologies developed within the context of the GENESI-DR project.

In this paper the technical details of the implementation of a working solution to the scenario described above are presented. The next section provides an overview of similar works and state-of-the-art solutions followed by a detailed description of the implemented solution and methodology. Finally, the results are shared with a discussion and final conclusions.

1.1. GENESI-DR

The need for open access to online Earth Science repositories is at the heart of the GENESI-DR project. Among the many objectives of this project, the authors of this paper were most interested in the distributed image search, discovery and access capabilities to operational repositories of remotely sensed imagery and geographical web processing chaining. One such operational repository is maintained by the Community Image Data (CID) portal action [3] of the JRC that also provides orthorectified imagery resulting from a semiautomatic orthorectification application based on area matching algorithms [4].

1.2. Web Processing Service

A Web Processing Service (WPS) is a standard developed by the Open Geospatial Consortium (OGC) [5] that provides rules for geospatial processing service requests and responses. Specifically, its aim is to provide access to GIS functionality over the internet and was chosen for this project because of its extensibility and wide use for geospatial web services.

1.3. Computing Power

Automated image analysis in many cases requires significant computing resources which may not be available at the location where the image is stored, either because the repository does not offer such a service or the algorithm and/or methodology to be applied is not available. The demo required that the images be processed by a specialised methodology [6] in a secure setting because of the sensitive nature of the information to be analysed. Today, both cloud and grid computing [7,8] provide solutions to the requirements described above. Based on a recent interview with Ian Foster of Argonne National Laboratory (http://youtu.be/hQW33I6PAUg), cloud = hosted whereas grid = federated. Public cloud solutions such as Amazon EC2 and Microsoft Azure were not chosen due to security and licensing concerns (which were not thoroughly investigated by specialist in this area) and because these services do not guarantee confidentiality. While a private cloud (*i.e.*, hosted services platform within your organisation such as Eucalyptus) could solve these concerns, none of our project partners had such a computing infrastructure in place at the time. A grid computing solution was chosen because it provided a solution to our security and licensing concerns and was made available by one of our project partners, the European Space Agency (ESA). The advantages of using cloud or grid computing in a post-disaster image processing scenario are scalability and parallelisation. Depending on the image processing requirements, the number of jobs submitted can easily be scaled (*i.e.*, the infrastructure can handle a single processing job or a thousand jobs) and depending on the resources available within the computing infrastructure, the number of jobs running in parallel can also be increased. Both these advantages ensure that the required computing power is available to the disaster analysts on-demand.

1.4. Trust

Post-disaster damage information needs are a sensitive matter and the demonstration had to provide an end-to-end level of security to keep out parties that should not have access to the data and information.

Such a level of trust was achieved through the use of security certificates (X.509), certificate proxies (VOMS proxies) and the adoption of Virtual Organisations (VOs).

The security infrastructure of the demonstration was based on X.509 certificates, a standard for a Public Key Infrastructure (PKI) (http://en.wikipedia.org/wiki/Public_key_infrastructure). The X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm. In X.509, authentication and authorization processes take place. In the authentication phase, the need to interact with a trusted relaying party is addressed through the interaction with globally trusted third parties, *i.e.*, Certification Authorities (CAs). A certificate authority or certification authority (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named entity of the certificate. This allows others (*i.e.*, entities who depend on this trust) to be confident that the signatures or assertions made by the private key correspond to the certified public key. With such a trust model, a CA is a trusted third party that is trusted by both the owner of the certificate and the entity relying on the certificate. CAs are characteristic of many PKI schemes.

The user is identified with identity certificates signed by CAs allowing the system to delegate their identity temporarily to other users and/or systems. This process generates proxy certificates allowing the WPS service to run with the identified user's privileges.

Authorization requires the involvement of resource providers such as computer centers, storage providers, *etc.*, and VO's because authorization cannot be granted based on local access rights alone. Instead, authorization must reflect the service level agreements negotiated between the VO's and the resource providers. This mechanism designates VO's as the administrators of entity membership (*i.e.*, groups, roles, *etc.*) and resource providers evaluate the attributes granted by VO's to their users and map them to local credentials used to access the resources.

2. A Review of the State-of-the-Art

This technology demonstrator could not be developed within the project timeframe without access to key technologies already available, the use of web and security standards, and the GENESI-DR infrastructure. Before delving into the details of our implementation, a short review of projects and solutions being tested and implemented is provided. Note that this is a very dynamic research area at the moment as suggested by Brauner *et al.* [9] which continues to push the implementations of geospatial standards [10] that can lag behind the state-of-the-art by several years in certain situations. This review presents related attempts and highlights the different technologies used for their solutions.

2.1. WPS and Service Chaining

Since the introduction of the OGC WPS standard in 2007, the ability to provide geospatial services has greatly improved. An early example (even before the standard was fully accepted) is Gehlot and Verbree [11] that use WPS for combining and chaining geospatial data and services. Today, many different solutions are available to the consumer of geographic information [12]. There are also examples of distributing WPS processes such as Granell *et al.* [13].

Schaeffer [14] introduced a Transactional WPS (WPS-T) approach that provides a highly flexible means to dynamically deploy and undeploy WPS processes or workflow chains. This approach is not limited to any schema or deployment information and therefore fosters reusability and flexibility while maintaining interoperability by means of the introduced schema inheritance. In the experiment, the uploaded workflows are presented as a WPS service that internally calls the Business Process Execution Language (BPEL) engine to do the work.

The disaster theme is also quite widespread within the context of WPS and service chaining. Stollberg and Zipf [15] presented a means to help simplify the creation of a processing chain by describing the workflow structure with an XML schema. This schema acts as a layer between the WPS and BPEL using the Web Service Description Language (WSDL) [16] and the Orchestration Engine (OE). In the context of Spatial Data Infrastructures (SDI), Walenciak *et al.* [17] describe their solution for the visualisation of evacuation route simulations based on distributed geographic information for disaster management. Other approaches to orchestrating WPS include centralised service chaining where a single service invokes all other services in sequence and controls the work flow and cascading chaining where data is directly exchanged with individual services that communicate with each other [18].

Lanig *et al.* [19] proposed a solution to access powerful distributed computing infrastructures via WPSs based on WSDL and Simple Object Access Protocol (SOAP) [20]. However, it is difficult to tell what level of security and trust was provided in their solution because few details of their implementation were provided. Another proposed solution to accessing distributed computing resources for geospatial WPS was based on BPEL [21]. Finally, Baranski [22] presents a proof of concept and implements a grid-enabled WPS to increase calculation performance and improve service availability in the context of an SDI.

Friis-Christensen *et al.* [23] provide a thorough review of the state of geographic information services and Service Oriented Architecture (SOA) (http://en.wikipedia.org/wiki/Service-oriented_architecture) and propose that data transfer between client and server should be limited. The solution presented in this paper takes into account some of their suggestions when possible, specifically using asynchronous client-server communication and the ability of sending processing code.

There are currently several different WPS implementations available. While the solution described in this article uses PyWPS [24], other open source possibilities include 52°N (http://52north.org/communites/geoprocessing/wps/index.html), which is a full Java$^{\text{TM}}$based open source implementation, and ZOO (http://www.zoo-project.org/), which is based on a C language kernel.

2.2. *Trust and Security*

When dealing with remotely sensed imagery, there are many reasons why data owners and/or end-users do not want to share their data and keep prying eyes from accessing it. When security is an issue, many organisations want to be certain that the person accessing the data is who they are (*i.e.*, trust), and nobody else can get access (*i.e.*, security).

Liu *et al.* [25] needed a solution to provide different levels of access to different parts of sensitive images. Their solution makes secure transmission of imagery possible and decryption keys grant users the ability to decrypt sections of the image depending on their access level for viewing. While this solution was not meant for remotely sensed imagery, it certainly could be applied for the distribution of such imagery. However, when it comes to processing the imagery the encryption/decryption requirements could be cumbersome.

Lanig and Zipf [26] use a similar method to the one described in this paper for trust. The Globus Toolkit [27], an open source software toolkit for building computing grids, provides the grid security and delegation infrastructure based on the concept of Virtual Organisation (VO) where users can share resources based on their level of trust given by the service providers. Furthermore, security is provided by the Grid Security Infrastructure (GSI) which is part of the Globus Toolkit. This security infrastructure implements transport-level and message-level security as well as certificates based authentication (CA) via X.509.

Trust and security is an issue that is not only specific to the geospatial community and thus many of the implemented solutions are derived from the state-of-the-art in that domain. Currently, the two most common trust models are the hierarchy and bridge models, which are based on three different public-key authorities and the trust mechanisms developed between them. The PKI consists of a community of principals, a community of verifiers and an authentication authority that is recognized by both. The purpose of the infrastructure is to allow a verifier to authenticate attributes (commonly the identity) of a principal when they communicate over an unsecured network.

Choosing the hierarchical trust model requires every key to be the subject of no more than one certificate or certificate request message. On the other hand, the bridge trust model uses a subordinate CA that can be certified by more than one root. The result is not a hierarchical model because the subordinate CA could/would have more than one superior. A good overview of PKI's in general and the hierarchical and bridge trust models is provided by Moses [28] if one would like to delve deeper into this complex subject. Due to the considerable size of the Earth Science and geospatial communities in general, the bridge trust model makes the greatest sense because it can adapt better to the growth in users and organisations providing both data and services. This choice is not mandatory and, as the system demonstrates, can be easily changed because every security policy to be adopted can be seen as a high level service to be integrated into the general architecture.

This overview of state-of-the-art solutions in the context of web based geospatial processing shows that the topic is still maturing and technologies are constantly evolving. The solution described in this article is considered state-of-the-art for the following reasons: (1) it is based on current standardised technologies, (2) the GENESI-DR SOA continues to develop following the demanding requirements of the services end-users, (3) it is compliant with standards including and not limited to INSPIRE [29], and (4) it provided a solution to a delicate image processing scenario which was previously not available.

3. Automating the Post-Disaster Image Processing Scenario

GENESI-DR adopts a service oriented architecture and the demo wanted to take advantage of this because web services located all over the globe can communicate through common "languages" (*i.e.*, open standards such as OpenSearch, X.509, and WPS) to achieve the experimental goal to automate the post-disaster image processing scenario described in the introduction. The Test Driven Development (TDD) [30] process was applied to this project in order to deliver an automatically testable working prototype. The methodology is described in the next sections.

3.1. Scenario

Many agencies today monitor natural disasters around the world providing automated alerting mechanisms via the web. For example, the Federal Emergency Management Agency (FEMA) (http://www.fema.gov/about/programs/disastermanagement/) coordinates US agencies disaster reporting and information dissemination while the Global Disaster Alert and Coordination System (GDACS) provides near real-time alerts about natural disasters occurring around the globe and helping to coordinate the European Commission's civil protection and humanitarian aid mechanisms (http://www.gdacs.org/). Both provide RSS feeds (http://en.wikipedia.org/wiki/Rss) and access to the Common Alerting Protocol (CAP) (http://en.wikipedia.org/wiki/Common_Alerting_Protocol), making it possible to automatically monitor disasters around the globe. Such automated disaster alerting systems trigger the post-disaster damage assessment scenario providing the geographic location, time and type of disaster. The disaster location and the time it occurred are necessary to begin the post-disaster damage assessment image processing workflow.

Based on the alert information, the service will discover relevant data sets within the GENESI-DR. Remotely sensed image based damage assessment requires very fine spatial resolution imagery, *i.e.*, <10 m spatial resolution, because coarser imagery is not suitable for detecting damage to buildings [31]. Image search and discovery parameters could also be tuned in order to provide the most recent archived imagery with respect to the date the disaster occurred. Ideally, the triggered service could also send a request to acquire post-disaster imagery through such a mechanism as the disaster charter (http://www.disasterscharter.org) but such a service request was not implemented into the demo presented in this article.

Once suitable imagery has been discovered, the service requires access to the image files themselves in order to send the imagery for processing. In the context of this scenario, the two processing methods are image orthorectification (if required) and an automated information extraction procedure to delineate regions in the imagery where people live and work. The two procedures from herein will be referred to as Near-Realtime Orthorectification (NOR) and as Urban Area Mapping (UAM). Where the processing takes place does not matter as long as the resources required to process the images are available immediately.

Finally, everything must be achieved in a secure and trusted environment due to the sensitive nature of the information, making sure that unidentified individuals and/or organisations do not have access to any resources without prior consent. The resulting processed imagery and related information is then placed back to a repository where stakeholders and analysts can access it for further examination.

3.2. Methodology

The above scenario was implemented using already available technologies and infrastructures. The following needed to be implemented:

1. The NOR and UAM applications were already regularly applied at the JRC but needed to be served via a WPS turning them into services;

2. Trusted communication between the various clients and servers needed to be provided;

3. The UAM application is computationally heavy and therefore access to a computing cluster was necessary and;
4. An image upload/submission tool for GENESI-DR was developed to permit trusted dissemination of results.

The team decided to serve the two applications via a WPS in order to ensure interoperability because the applications were routinely applied at the JRC but installed on different machines, on separate networks running in customised environments, and built with different technologies. Serving them via WPS turned the applications into services. It is hoped that this decision could also encourage future upgrading of the proposed processing workflow by easily adding other services if required.

4. Results

Figure 1 provides a simplified sequence diagram showing only the main components. A Unified Modeling Language (UML) sequence diagram is shown in Figure 2 and in media 1 (see supplementary media file) explaining in detail what goes on during the service process. The following describes the elements of the UML diagram (Figure 2).

Figure 1. Simplified sequence diagram (see media 1 for full explanation and Figure 2 for details). This figure presents the activities of the UAM-WPS in the processing chain. The boxes on the right identify the process whereas the arrows distinguish the type of connection to each service element: white is an open connection whereas black is a secure connection.

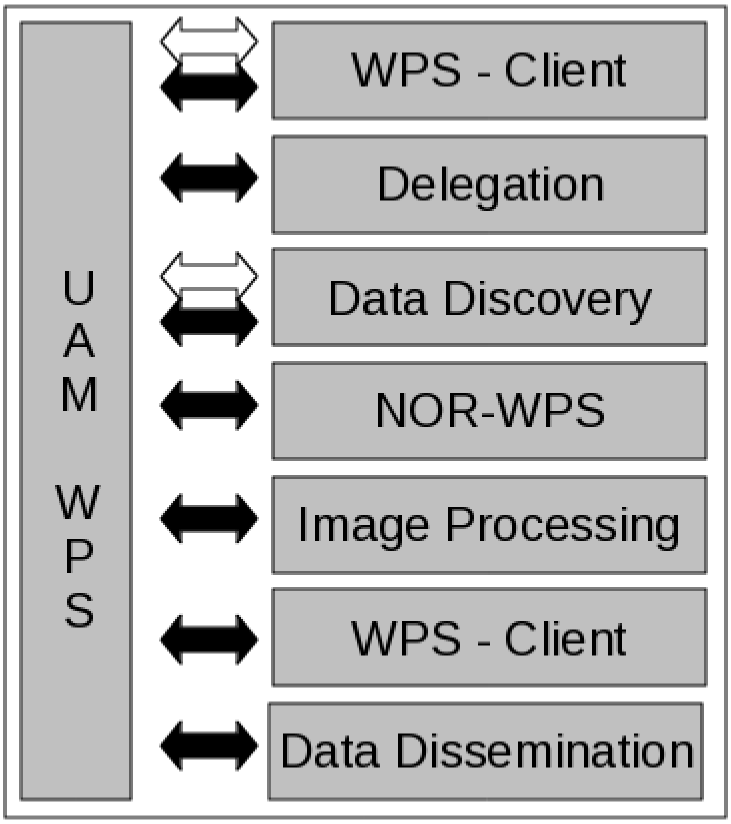
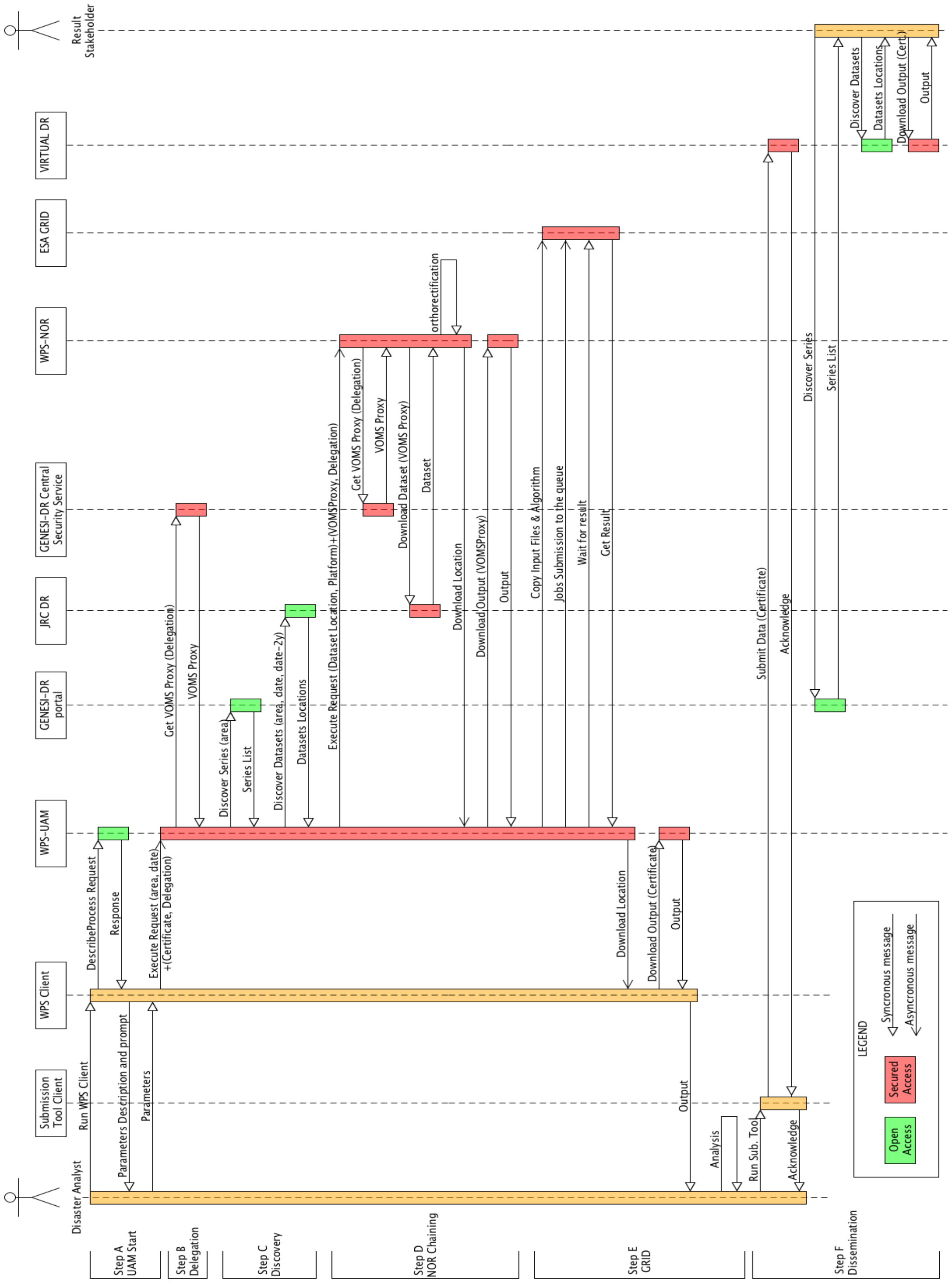


Figure 2. *Sequence Diagram* of the GENESI-DR technology demonstration for the described post-disaster damage needs assessment scenario using WPS. The media file that accompanies this article provides additional explanations.



4.1. Scenario Description

The two human actors driving the development of this demo are the disaster analyst and the result stakeholder. The main components of the demo are the following:

- **The WPS Client**. An ad-hoc simplified WPS client customized to perform GENESI-DR data discovery via the OpenSearch technologies (http://en.wikipedia.org/wiki/OpenSearch) and supporting the use of X.509 certificates for authentication was developed in Python (http://www.python.org/) applying the TDD technique.

- **The JRC WPS Server**. UAM and NOR were exposed as geospatial web services via the same server. The server machine was running the Debian Linux distribution with Apache as the web server. Two Apache modules were also required: mod-gridsite for X.509 certificates support and mod-Python for accessing HTTP(S) protocol objects via Python. PyWPS [24] provided the WPS v1.0.0 interface but the software layer between PyWPS and the underlying in-house developed applications needed to be developed and TDD was also applied.

- **GENESI-DR (Discovery Service / Central Security Service)**. The GENESI-DR provided catalog discovery functionality via OpenSearch web syndication. OpenSearch, with the Geo and Time extensions developed within GENESI-DR, will be part of OGC CSW3.0 (currently being discussed in draft documents 09-084 and 10-032). The GENESI-DR Central Security Service is a server that provides VOMS proxies for authorisation delegation as well as stores information linking users to Virtual Organisations.

- **Digital Repositories (JRC DR, Virtual DR)**. The Digital Repositories in GENESI-DR provide secure access to geospatial datasets and include the GENESI catalogue generator, discovery agent, data catalogue, and catalogue access service. The JRC CID DR is GENESI-DR compliant and serves a subset of the data available from the CID Portal (http://cidportal.jrc.ec.europa.eu/imagearchive/main/). The Virtual Digital Repository was set up specifically for this demo and is a standard GENESI-DR Digital Repository used to show the possibilities of secured and remote dissemination.

- **On Demand Grid Processing**. ESA provided access to their computing grid which is also part of the European Grid Infrastructure (http://www.egi.eu/). Processing jobs were submitted using the GridWay (http://www.gridway.org) metascheduler providing access to machines running Scientific Linux. The UAM binaries and input imagery were submitted in this manner based on a bash script prepared by the WPS.

4.2. Test Driven Development

The TDD technique was applied during the development of all the software written in Python. TDD is a software development practice [30] characterised by short development iterations that provide constant feedback on the state of the running code. Each iteration comprises three steps:

1. A test for new functionality is written and making sure the test fails;

2. The production code to pass the test is written making the test succeed;

3. The code is refactored, removing duplication and making it more readable. The updated version is re-tested to be sure that nothing was broken during refactoring.

This technique helps to produce flexible and automatically testable software that reduces maintenance needs and the cost of adding new features. Furthermore, the tests themselves are also used as *living* code documentation.

4.3. Service Activity

As a general GENESI-DR project policy, the search and discovery of geospatial metadata resources is open whereas access permission to data and/or processing resources is restricted. For this demonstration, resource access permission was given to those belonging to the UAM-WPS VO where the VO is like a working group. Grid middleware such as the Globus Toolkit enables the sharing of heterogeneous resources, such as hardware and software, among VO's. It is installed and integrated into the existing infrastructure of the companies involved and provides a special layer placed between the heterogeneous infrastructures and the specific user applications. In grid computing, a VO is a group who shares the same computing resources (http://en.wikipedia.org/wiki/Virtual_organization). The use of the GENESI-DR security infrastructure guarantees authenticated resources access in both directions (client and server). In fact, when a client connects to a server via HTTPS, both provide their identities via the certificates to each other. The client and the server verify each other's identity (thanks to a trusted Certificate Authority) and furthermore, the server crosschecks the identity of the client against local access control lists.

The following account is a description of the completed demo (Figure 2 and media 1). The scenario begins with the disaster analyst receiving an alert. The alert provides the location, time and type of disaster. At this time, all the relevant information is known to begin the service which is accessed via the WPS client installed on the disaster analysts' computer. When the custom WPS client starts, it performs a describeProcess request, known *a priori*, to the UAM-WPS. The UAM-WPS responds synchronously (*i.e.*, a response must be received before continuing) telling the WPS client that the UAM-WPS requires two parameters to continue: the geographic area to search for imagery and the date of the event. The decision to let the WPS client start with a known describeProcess request was to ensure the custom client could easily adapt dynamically to potential adjustments in the input parameters of the service. This WPS request/response functionality is open and therefore there is no need for the WPS client to identify itself.

Part of the response to the getCapabilities request contains an abstract for each service available, detailing how and in which form the user must supply authentication and delegation. If the client attempts an execute request, without a proper certificate, Apache (http://httpd.apache.org/) will return a "forbidden access page" whereas if the client does not provide the required delegation credentials, the service will terminate and return a WPS response describing the error.

Authentication is not defined in the WPS standard and furthermore the OGC has not approved a standard that binds authentication with geospatial services. However, the OGC will start an Authentication Interoperability Experiment to test standard ways of transferring authentication (http://www.opengeospatial.org/projects/initiatives/authie) that in turn will lead to an OGC Approved Best Practices document aimed at service implementers and organizations accessing the services.

It is worth stressing that the use of certificates and basic authentication, which are below the application layer, do not affect the compliancy of the services to the WPS standard.

Today, developers wanting to use both authentication and geospatial services must provide a customized solution. In the case of the post-disaster damage scenario demo, the solution was to adopt the GENESI-DR standards. Consequently, the end-user of the presented processing chain is tied to the use of the customised WPS client which works well within the framework of GENESI-DR because the security requirements are a part of this framework. A possible solution to reduce the complexity of the client and increase interoperability would be to move the username and password used for delegation as input parameters to the service into the execute request.

Now the WPS client can continue with the execute request that actually starts the service processing chain of events. Execution however requires identification and therefore the WPS client must be authenticated (via Apache and HTTPS) and authorized (via Apache and GridSite) to run the service through a valid X.509 certificate and provide the necessary information to the UAM-WPS for delegation (*i.e.*, to act on the user's behalf with the same rights as the user). The delegation requires a username and password provided through base authentication over HTTPS. Consequently, throughout the running life of the UAM-WPS instance, the UAM-WPS execution is secure.

The second stage of the UAM-WPS involves requesting and obtaining the actual delegation based on the credentials provided by the user. The username and password are provided to the central security service to obtain a VOMS proxy. The VOMS proxy is a special X.509 certificate that expires quickly and in the context of the UAM-WPS, the VOMS proxy had a 12 hour lifespan. This short lifespan prevents replay attacks but not man-in-the-middle attacks. Man-in-the-middle attacks are prevented by encryption and the handshake mechanisms of SSL including trust in the presented certificates. A normal X.509 certificate on the other hand is usually valid for one year. Furthermore, the VOMS proxy also contains virtual organisation related information. All connections during the second stage are secure.

The third stage is data discovery. The UAM-WPS needs to search and discover the wanted imagery and uses the GENESI-DR open search/discovery capabilities to find the wanted data holdings. Data discovery is based on geographic region of interest and date via OpenSearch. The UAM-WPS requests a temporal range from the event date to two years back in time. Data discovery in GENESI-DR is in two parts. First, the UAM-WPS asks the GENESI-DR portal for the list of data series corresponding to the search criteria and receives the resulting data series list containing information on the location of digital repositories holding these series. Second, the UAM-WPS redefines the discovery connecting directly to the digital repository of interest obtaining image specific metadata including the actual URL of the resources. The UAM-WPS demo, for illustration purposes, connected only to the JRC DR. Data discovery in GENESI-DR is open.

The next stage is orthorectification of the discovered imagery using the NOR-WPS. Orthorectification was included in the demo to prove service chaining including identity delegation between WPS processes which can be hosted anywhere on the internet. Note that the two services, UAM and NOR, were on the same server for the demonstration but are completely independent and could be located anywhere in the world. The NOR-WPS requires the input image location (URL), the sensor type (taken from the image metadata), a valid X.509 certificate and the delegation to proceed. The VOMS proxy provided by the UAM-WPS is used by the NOR-WPS for secure execution of the orthorectification. Furthermore, the

NOR-WPS gets its own VOMS proxy to securely download the discovered imagery from the JRC DR. Once the image has been orthorectified, the NOR-WPS provides the location (URL) of the result back to the UAM-WPS. Finally, the UAM-WPS with its VOMS proxy can securely download the NOR-WPS output. Note that a new secured process is instantiated on the NOR-WPS server.

The penultimate stage is the remote execution of the UAM image processing workflow on a computing grid. Having the NOR-WPS results available, the UAM-WPS securely connects to the ESA computing grid and copies all necessary data and programs for job queuing. Once the transfer is complete, the grid infrastructure submits the jobs to the computing queue. Job management was controlled using the GridWay interface that connects to the PBS (http://www.pbsworks.com) job scheduler. The scheduler decides how the job will be queued and can be configured for emergency cases if necessary. Once the results are ready, the UAM-WPS downloads the results from the grid infrastructure. Finally, the location (URL) of the processed imagery is given to the WPS client via the UAM-WPS.

While the disaster analyst that submitted the UAM-WPS request has access to the results, other analysts and/or stakeholders may also require access to the results. For this reason, a data submission tool that was developed during the GENESI-DR project was included in the demo. The data submission tool sends to a virtual DR the geospatial data that the disaster analyst would like to disseminate. The virtual DR upon receiving the data with the accompanying metadata sends back an acknowledgment once the upload is complete. The virtual DR is federated to the GENESI-DR infrastructure and therefore the newly submitted imagery can be discovered by anyone from anywhere in the world. However, only those with the proper credentials will have access to it.

5. Conclusions and Discussion

The successful demonstration of a WPS for the described post-disaster damage assessment scenario demonstrates the power and maturity of the applied technologies:

- The GENESI-DR infrastructure provided the image discovery functionality and secure authorized access to imagery from a variety of data owners as well as dissemination to authorized partners.
- The WPS standard provided a controlled "self service" to users and stakeholders which presented the required credentials and possessed the needed permissions. This service means that people anywhere can have access to the services whenever they are required and tailor them to their particular needs.
- Grid computing infrastructures both in Europe and across the globe provide on-demand access to high performance computing clusters.
- Web security and authorization provided a secure way of communicating and authorizing services.

The results also demonstrate that a WPS can be used successfully in the context of a post-disaster damage assessment scenario as used by analysts at the JRC.

Part of the success of this WPS demo is the digital repository search and discovery ability of GENESI-DR. However, very fine spatial resolution imagery is needed for the disaster analysis scenario and many of the project digital repositories did not have such image holdings. Consequently, the

UAM-WPS would benefit from a wider variety of remotely sensed image providers giving access to their data sets. The authors would like to see commercial image providers give GENESI-DR like access to their image archives, making image discovery and potentially acquisition services more accessible to WPS users.

The custom WPS client works well within the framework of GENESI-DR because the security requirements are a part of this framework. However, such a custom WPS solution does limit interoperability. A possible solution to reduce the complexity would be to move the username and password for delegation as input parameters to the service via the execute.

The demonstration targeted a specific image processing scenario, however other scenarios can easily be conceived that use a similar processing chain. Adapting the demo to other needs would be quite straightforward.

Customizing the algorithms and methods used to process the remotely sensed images is also possible. Such services are already available both from public agencies and private companies. However, they do not all support the security framework used in the demo, which was a requirement for the disaster damage scenario, nor are they connected to such a large database of searchable digital repositories.

Service triggering at the moment was a human user, however the mechanism can easily be replaced by an alert monitor waiting for certain information to be made available from a variety of alerting sites. Triggers can also be envisaged depending on other types of triggers such as data availability that cater to the requirements of the end-user.

The time it took the service to process the imagery was quite similar to the computing times experienced in-house which are in the order of under an hour. The differences would be most notable, however, where human operators have been replaced specifically in the search and discovery of the needed imagery and the posting of the results for dissemination. With a triggering mechanism in place, overall processing time would also depend on whether an operator is present when an alert has been signaled.

With remotely sensed imagery, data ownership and licensing are another issue that could potentially derail the adoption of such services within an organisation. The secure communication within the WPS demonstration makes sure that only the data owner and/or authorized user has access. However, some licensing terms require that the data be always kept on the owners' premises, which means that farming out processing tasks on computers outside the organisation could be in breach of the licensing agreement. Solutions to these obstacles are being developed in the form of new specifications for geospatial digital rights management (GeoDRM) (http://www.opengeospatial.org/standards/as/geodrmrm) in order to more easily share data without losing control of one's intellectual properties.

Acknowledgements

The authors would like to thank ESA for providing access to their grid computing resources for testing. Funding for this project came from the European Commission DG INFRASTRUCTURES FP7 Capacity Programme.

References

1. Ground European Network for Earth Science Interoperations-Digital Repositories (GENESI-DR); 2010. Available online: http://www.genesi-dec.eu/ (accessed on 28 April 2011).
2. European Commission FP7 Project Page for GENESI-DR; Available online: http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&ACTION=D&DOC=1&CAT=PROJ&RCN=86424 (accessed on 27 April 2011).
3. Burger, A.; Hasenohr, P.; Åstrand, P.J. Providing Access to Terabytes of Earth Observation Data—Infrastructure, Services, and Licensing. In *Proceedings of 14th MARS Annual Conference "Geomatics in support of the CAP"*, Ljubljana, Slovenia, 3–5 December 2008.
4. Westin, T.; Edgardh, L.A. *Automatic Model Adjustment to Reference Data Sets*; 2006. Available online: http://www.spacemetric.com (accessed on 27 April 2011).
5. Schut, P. *OpenGIS Web Processing Service (WPS) 1.0.0*; 05-007r7; Open Geospatial Consortium Inc.: Wayland, MA, USA, 2007. Available online: http://www.opengeospatial.org/standards/wps (accessed on 28 April 2011).
6. Pesaresi, M.; Gerhardinger, A.; Kayitakire, F. A robust built-up area presence index by anisotropic rotation-invariant textural measure. *IEEE J. Sel. Topics Appl. Earth Obs. Remote Sens.* **2008**, *1*, 180-192.
7. Stokes, J. Amazon goes from cloud to grid with new cluster product. *Ars Technica* 2010. Available online: http://arstechnica.com/business/news/2010/07/amazon-goes-grid-with-cluster-compute-instances-for-ec2.ars (accessed on 27 April 2011).
8. Stokes, J.; The cloud: A short introduction. *Ars Technica* 2009. Available online: http://arstechnica.com/business/news/2009/11/the-cloud-a-short-introduction.ars (accessed on 27 April 2011).
9. Brauner, J.; Foerster, T.; Schaeffer, B.; Baranski, B. Towards a Research Agenda for Geoprocessing Services. In *Proceedings of 12th AGILE International Conference on Geographic Information Science*, Hannover, Germany, 2–5 June 2009.
10. Khalsa, S.J.; Percivall, G. Geoscience depends on geospatial information standards. *IEEE Geosci. Remote Sens. Soc. Newslett.* **2010**, *12*, 18-22.
11. Gehlot, S.; Verbree, E. Web-Based Sharing of a Geo-Processing Chain: Combination and Dissemination of Data and Services. In *Proceedings of The International Symposium on Geospatial Databases for Sustainable Development/ISPRS TC Commitee IV Geo-Databases and Digital Mapping*, Goa, India, 25–30 September 2006.
12. Foerster, T.; Schaeffer, B.; Brauner, J.; Jirka, S. Integrating OGC Web Processing Services into Geospatial Mass-Market Applications. In *Proceedings of The International Conference on Advanced Geographic Information Systems & Web Services*, Cancun, Mexico, 1–6 February 2009.
13. Granell, C.; Diaz, L.; Gould, M. Managing Earth Observation Data with Distributed Geoprocessing Services. In *Proceedings of The International Geoscience and Remote Sensing Symposium (IGARSS 2007)*, Barcelona, Spain, 23–27 July 2007; pp. 4777-4780.

14. Schaeffer, B. Towards a Transactional Web Processing Service (WPS-T). In *Proceedings of GI-Days 2008: The 6th Geographic Information Days*, Muenster, Germany, 16–18 June 2008; Volume 32.
15. Stöllberg, B.; Zipf, A. Development of a WPS Process Chaining Tool and Application in a Disaster Management Use Case for Urban Areas. In *Proceedings of 27th Urban Data Management Symposium (UDMS 2009)*, Ljubljana, Slovenija, 24–26 June 2009.
16. Christensen, E.; Curbera, F.; Meredith, G.; Weerawarana, S. *Web Services Description Language (WSDL) 1.1*; W3C Note; The World Wide Web Consortium (W3C), 15 March 2001. Available online: http://www.w3.org/TR/wsdl (accessed on 28 April 2011).
17. Walenciak, G.; Stöllberg, B.; Neubauer, S.; Zipf, A. Extending Spatial Data Infrastructures 3D by Geoprocessing Functionality—3D Simulations in Disaster Management and environmental Research. In *Proceedings of The International Conference on Advanced Geographic Information Systems & Web Services*, Cancun, Mexico, 1–6 February 2009.
18. Stöllberg, B.; Zipf, A. OGC Web Processing Service Interface for Web Service Orchestration Aggregating Geo-processing Services in a Bomb Threat Scenario. *Lecture Notes Comput. Sci.* **2007**, *4857*, 239-251.
19. Lanig, S.; Schiling, A.; Stöllberg, B.; Zipf, A. Towards Standards-based Processing of Digital Elevation Models for Grid Computing through Web Processing Service (WPS). In *Proceedings of The 2008 International Conference on Computational Science and its Applications (ICCSA2008)*, Hong Kong, 19–21 March 2008.
20. Box, D.; Ehnebuske, D.; Kakivaya, G; Layman, A.; Mendelsohn, N.; Nielsen, H.F.; Thatte, S.; Winer, D. *Simple Object Access Protocol (SOAP) 1.1*; W3C Note; The World Wide Web Consortium (W3C): 8 May 2000. Available online: http://www.w3.org/TR/2000/NOTESOAP20000508/ (accessed on 28 April 2011).
21. Hobona, G.E.; Fairbairn, D.; James, P.M. Workflow Enactment of Grid-Enabled Geospatial Web Services. In *Proceedings of the UK e-Science All Hands Meeting*, Nottingham, UK, 10–13 September 2007.
22. Baranski, B. Grid Computing Enabled Web Processing Service. In *Proceedings of GI-Days 2008: The 6th Geographic Information Days*, Muenster, Germany, 16–18 June 2008; Volume 32.
23. Friis-Christensen, A.; Ostländer, N.; Lutz, M.; Bernard, L. Designing service architectures for distributed geoprocessing: Challenges and future directions. *Trans. GIS* **2007**, *11*, 799-818.
24. Cepicky, J.; Becchi, L. Geospatial Processing via Internet on Remote Servers PyWPS. *OSGeo J.* **2007**, *1*, 39-42. Available online: http://www.osgeo.org/ojs/index.php/journal/issue/view/17 (accessed on 27 April 2011).
25. Liu, J.; Sun, J.; Xu, Z.Q. Secure distribution for high resolution remote sensing images. *J. Appl. Remote Sens.* **2010**, *4*, 1-12.
26. Lanig, S.; Zipf, A. Interoperable processing of digital elevation models in grid infrastructures. *Earth Sci. Inf.* **2009**, *2*, 107-116.
27. Foster, I. Globus Toolkit Version 4: Software for service-oriented systems. In *IFIP International Conference on Network and Parallel Computing*; LNCS 2779; Springer-Verlag: Berlin/Heidelberg, Germany, 2005; pp. 2-13.

28. Moses, T. PKI trust models. In *IT-University of Copenhagen Course Material*; IT-University of Copenhagen: Copenhagen, Denmark, 2003. Available online: http://www.itu.dk/courses/DSK/E2003/DOCS/PKI_Trust_models.pdf (accessed on 1 May 2011).
29. Infrastructure for Spatial Information in the European Community (INSPIRE). *Official J. Europ. Union* 14 March 2007. Available online: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:108:0001:0014:EN:PDF (accessed on 28 April 2011).
30. Beck, K. *Test Driven Development: By Example*; Addison-Wesley Professional: Boston, MA, USA, 2002.
31. Kerle, M. Satellite-based damage mapping following the 2006 Indonesia earthquake—How accurate was it? *Int. J. Appl. Earth Obs. Geoinf.* **2010**, *6*, 466-476.