Geophysical Research Abstracts
Vol. 12, EGU2010-12315, 2010
EGU General Assembly 2010

A Security Architecture for Grid-enabling OGC Web Services

Valerio Angelini (1) and Luca Petronzio (2)

(1) Italian National Research Council (CNR), Institute of Methodologies for Environmental Analysis (IMAA), Prato (PO), Italy (angelini@imaa.cnr.it), (2) Elsag Datamat, Rome, Italy (luca.petronzio@elsagdatamat.com)

In the proposed presentation we describe an architectural solution for enabling a secure access to Grids and possibly other large scale on-demand processing infrastructures through OGC (Open Geospatial Consortium) Web Services (OWS). This work has been carried out in the context of the security thread of the G-OWS Working Group.

G-OWS (gLite enablement of OGC Web Services) is an international open initiative started in 2008 by the European CYCLOPS , GENESI-DR, and DORII Project Consortia in order to collect/coordinate experiences in the enablement of OWS's on top of the gLite Grid middleware. G-OWS investigates the problem of the development of Spatial Data and Information Infrastructures (SDI and SII) based on the Grid/Cloud capacity in order to enable Earth Science applications and tools. Concerning security issues, the integration of OWS compliant infrastructures and gLite Grids needs to address relevant challenges, due to their respective design principles. In fact OWS's are part of a Web based architecture that demands security aspects to other specifications, whereas the gLite middleware implements the Grid paradigm with a strong security model (the gLite Grid Security Infrastructure: GSI).

In our work we propose a Security Architectural Framework allowing the seamless use of Grid-enabled OGC Web Services through the federation of existing security systems (mostly web based) with the gLite GSI. This is made possible mediating between different security realms, whose mutual trust is established in advance during the deployment of the system itself.

Our architecture is composed of three different security tiers: the user's security system, a specific G-OWS security system, and the gLite Grid Security Infrastructure. Applying the separation-of-concerns principle, each of these tiers is responsible for controlling the access to a well-defined resource set, respectively: the user's organization resources, the geospatial resources and services, and the Grid resources.

While the gLite middleware is tied to a consolidated security approach based on X.509 certificates, our system is able to support different kinds of user's security infrastructures. Our central component, the G-OWS Security Framework, is based on the OASIS WS-Trust specifications and on the OGC GeoRM architectural framework. This allows to satisfy advanced requirements such as the enforcement of specific geospatial policies and complex secure web service chained requests.

The typical use case is represented by a scientist belonging to a given organization who issues a request to a G-OWS Grid-enabled Web Service. The system initially asks the user to authenticate to his/her organization's security system and, after verification of the user's security credentials, it translates the user's digital identity into a G-OWS identity.
This identity is linked to a set of attributes describing the user's access rights to the G-OWS services and resources. Inside the G-OWS Security system, access restrictions are applied making use of the enhanced Geospatial capabilities specified by the OGC GeoXACML.
If the required action needs to make use of the Grid environment the system checks if the user is entitled to access a Grid infrastructure. In that case his/her identity is translated to a temporary Grid security token using the Short Lived Credential Services (IGTF Standard).
In our case, for the specific gLite Grid infrastructure, some information (VOMS Attributes) is plugged into the

Grid Security Token to grant the access to the user's Virtual Organization Grid resources. The resulting token is used to submit the request to the Grid and also by the various gLite middleware elements to verify the user's grants.

Basing on the presented framework, the G-OWS Security Working Group developed a prototype, enabling the execution of OGC Web Services on the EGEE Production Grid through the federation with a Shibboleth based security infrastructure. Future plans aim to integrate other Web authentication services such as OpenID, Kerberos and WS-Federation.