Geophysical Research Abstracts
Vol. 15, EGU2013-10841-1, 2013
EGU General Assembly 2013

Exploiting OAuth 2.0: from User Delegation for OGC Services to a Generic Federation-as-a-Service Solution for Federated Identity Management

Philip Kershaw (1), Jens Jensen (3), Ag Stephens (2), and Willem van Engen (4)

(1) STFC Rutherford Appleton Laboratory, NCEO/Centre for Environmental Data Archival, Didcot, United Kingdom (philip.kershaw@stfc.ac.uk), (3) STFC Rutherford Appleton Laboratory, Department of Scientific Computing, Didcot, United Kingdom (jens.jensen@stfc.ac.uk), (2) STFC Rutherford Appleton Laboratory, NCAS/Centre for Environmental Data Archival, Didcot, United Kingdom (ag.stephens@stfc.ac.uk), (4) Nikhef, PO Box 41882, NL 1009 DB Amsterdam, The Netherlands

We explore an application of OAuth to enable user delegation for OGC-based services and the evolution of this solution to form part of a wider Federation-as-a-Service offering for federated identity management.

OAuth has established itself in the commercial sector as a means for users to delegate access to secured resources under their control to third parties. It has also found its way into the academic and research domains as a solution for user delegation. Notable examples including the CILogon project for Teragrid in the US, and also, closer to the Earth Sciences, as part of the OGC Web Services, Phase 6 Testbed. Both are examples of OAuth 1.0 implementations. Version 2.0 has seen significant changes to this original specification which have not been without controversy but it has arguably provided a greater degree of flexibility in how it can be applied and the use cases that it can address.

At CEDA (Centre for Environmental Data Archival, STFC), a Python implementation of OAuth 2.0 was made to explore these capabilities with a focus on providing a solution for user delegation for data access, processing and visualisation services for the Earth Observation and Climate sciences domains. The initial goal was to provide a means of delegating short-lived user credentials to trusted services along the same lines as the established approach of Proxy certificates widely used in Grid computing. For the OGC and other HTTP-based services employed by CEDA, OAuth makes a natural fit for this role, integrating with minimal impact on existing interfaces. Working implementations have been made for CEDA's COWS Web Processing Service and Web Map Service.

Packaging the software and making it available in Open Source repositories together with the generic nature of the solution have made it readily exploitable in other application domains. At the Max Planck Institute for Psycholinguistics (Nijmegen, The Netherlands), the software will be used to integrate some tools in the CLARIN infrastructure*. Enhancements have been fedback to the package through this activity. Collaboration with STFC's Scientific Computing department has also seen this solution expand and evolve to support a more demanding set of use cases required to meet the needs for Contrail, an EU Framework 7 project. The goal of Contrail is to develop an Open Source solution for federating resources from multiple Cloud providers. Bringing the solution developed with OAuth together with technologies such as SAML and OpenID it has been possible to develop a generic suite of services to support federated access and identity management, a Federation-as-a-Service package. This is showing promise with trials with the EUDAT project. A deployment of the Contrail software is also planned for CEMS (the facility for Climate and Environmental Monitoring from Space), a new joint academic-industry led facility based at the STFC Harwell site providing access to large-volume Earth Observation and Climate datasets through a Cloud-based service model.

* This work is part of the programme of BiG Grid, the Dutch e-Science Grid, which is financially supported by the Netherlands Organisation for Scientific Research, NWO.