Contribution ID: **112** Type: **not specified**

Linking Authenticating and Authorising Infrastructures in the UK NGI (SARoNGS)

Friday, 30 March 2012 11:25 (25 minutes)

Description of the Work

The SARoNGS service currently sits between two infrastructures that make use of separate authentication authorisation mechanisms. It issues pseudo-anonymous grid credentials to members of institutes subscribed to the UK access management federation. The credential is made available through MyProxy in the form of a GSI-proxy certificate and may optionally contain VOMS assertions. The X509 certificate is never released by the service.

SARoNGS was designed to allow individuals from all research community backgrounds to access grid resources without needing to understand the complexities peculiar to the identity management technologies chosen by the grid development community. It made the following assumptions:
1, individuals accessing grid resources would be registered at an institute which was part of the UK access management federation;
2, individuals use browsers;
3, the research communities provide grid portals.
i.e. With the say-so of each individual logging into a portal, SARoNGS provides that portal with a grid (and VO) credential specific to that individual.

Due to the complex nature of data release, the policies laid down by the UK access management federation, the registration requirements of the VOs and the operational requirements of the resource providers (consequently also the grid federation [IGTF] policies), the SARoNGS approach has had to overcome a number of technical and political obstacles. We will present those obstacles and how we have solved them.

Conclusions

The UK houses two separate authentication authorisation infrastructures for academic research, one relatively easy-to-use system based on the relationship between individuals and their Universities; the other more complex, based upon the individual's personal credentials under their own management and the out of band subscription to Virtual Organisations.

In reality these are complex systems which don't align themselves very well. We have bridged the gap and where necessary plugged holes to produce a production service which presents the simpler Shibboleth authentication environment and uses this to issue the more complex grid credentials supplying them to the portals to use on behalf and at the request of the user.

We have learned much in the process have solved many issues allowing researchers in the UK access to UK based grid resources. On a larger scale we have identified sociopolitical barriers to uptake, which we hope to solve through EGI, federation and standards activities.

Impact

We understand that each digital asset will have associated with it an access policy and that this is driven by a broad range of requirements on e.g. provenance of data, stability of service, licensing of tools, ownership, copyright, law, etc. We also understand that each individual who wishes to make use of those assets has two main requirements, that the access be as simple as possible and that their personal and research data is not abused. We understand that universities and other agencies called in to identify or otherwise vouch for those individuals often err on the side of conservative attribute release policies or do not have the relevant authority to assert what resource providers are asking them to release.

In this presentation we hope to demonstrate what we have learned in the process of bridging the gap between institutional, community and infrastructure lead Identity Management environments. There are gaps; there are flaws; and there are misconceptions.

Through our experiences we describe short term solutions to the larger problem. By bringing the discrepancies between grid and other communities to light we hope that all communities can work towards a common understanding of identity and authority.

URL

https://cts.ngs.ac.uk/

Overview (For the conference guide)

We aim to provide simple trusted access to digital services for the UK's research community including Grid and Cloud provision. To achieve this we have to satisfy conditions laid down by three types of entity:
1, Individuals
2, Resources
3, Identification & Attribute Authorities
Each of these is governed by policies and legal requirements placed upon them as well as human rights legislation, making it difficult if not impossible to fit one access mechanism to all stakeholders.

SARoNGS was a JISC funded technical project that was developed in the UK to apply a federated access model (The Shibboleth based UK access management federation) to the grid environment. It resulted in a production service supported by the UK NGI to issue grid credentials, obtain VO assertions and place them within reach of the user so to provide access these online service.

We will present the details of this service, the ways we joined the loose ends together, the remaining issues and future directions.

Primary author: JONES, Mike (MANCHESTER)

Presenter: JONES, Mike (MANCHESTER)

Session Classification: Security