EUGridPMA

P.O. Box 41882
NL 1009 DB Amsterdam
The Netherlands

Our Reference: EGP/091013/EIRG-01 *Date: Tue, 13 October 2009 Pages: 2*

It has come to our attention that the e-IRG is considering issues related to authentication and authorization, in particular in the context of the access for new, large scientific communities to e-Infrastructures such as those provided by EGEE and EGI. In this context, we would like to clarify some of these issues, and point out recent and ongoing activities that address the difficulties that are common perceived as being challenges for access to such e-Infrastructures.

It is commonly recognised that users are neither inclined nor equipped to deal with certificates, and with the way they are bound to physical systems. This is a long-standing issue and, following the e-IRG Recommendations in 2004 and 2005, the community has been working on solutions to this issue along various avenues that we want to outline below.

Facilitating the procurement of certificates for users, such that these can be acquired as and when needed based on a login commonly known to the user (her or his home organisation, university or institute). These are only short-lived and can be used for the job at hand. These do not need to be managed or maintained. These "SLCS" services (and the longer-lived but equally accessible 'MICS' services) have been introduced in the International Grid Trust Federation IGTF following early use cases and the e-IRG recommendation. In Europe, these services are based on national educational and research federations that are now maturing rapidly.

Technologically, they use a wide variety of software, of which 'Shibboleth' is the best known but certainly not the most widely used in Europe. Others include *PAPI* (Spain), *SimpleSAMLPHP* (Norway and others), *PingID* (Netherlands), and others – most of which today use a common 'SAML2' protocol. Several of these have been linked to the above-mentioned SLCS and MICS services, starting with the Swiss AAI federation in 2007, and the German DFN AAI in 2008. TERENA, the association of NRENs in Europe, is now in the final stages of a multi-national service that will grant access to certificates for users from Norway, Sweden, Finland, Denmark, the Netherlands and the Czech Republic, with the potential to expand to more countries.

In all these cases, however, the national federation has to be sufficiently mature to satisfy the basic security requirements of a large-scale valuable e-Infrastructure – their primary use case traditionally has been access to journal papers, and the assurance requirements on federations for the e-Infrastructure access are most certainly higher than those. The IGTF continues to work with and support the integration of national federation in the e-Infrastructure

and the Grid, bringing concrete use cases anchored in the needs by sites and resource centres to meet the expectancy of the federations. The TERENA sponsored Research and Educational FEDerationS group “REFEDS”, where also the IGTF is represented, aids the international coordination of these federations, in line with the community requirements and the e-IRG recommendations. Projects such as GEANT also support this via eduGAIN.
The major obstacle may remain at the national and institutional level, since not all universities and research centres are equally well prepared to join their national federations with an appropriate assurance quality today.

However, in many cases it may be entirely unnecessary to burden end-users with certificates or even with technological details of grid. Over the years, and in many national grids, community portals have been established that hide grid complexity, and all of the user authentication technology, behind application-oriented portals or science gateways. Internationally the most well-known are those from TeraGrid and DEISA, but also EGEE and most national grids have established and fostered such portals.
Recently, a specific policy to enable and promote science portals was adopted by the EGEE project, based on a recommendation from the Joint Security Policy Group. Inspired by work in several NGIs, this policy explicitly allowed for anonymous and pseudonymous users, and federated access to these portals allowed also complex work to be done from these.

Lastly, work on Portals and the ‘SLCS’ and ‘MICS’ services is being combined to provide an even more transparent user experience on the short term., allowing users to view the e-Infrastructure as a transparent extension to their research.

Not leveraging the past and current efforts with respect to national federations, the SLCS and MICS services based on these, their integration in portals and the role of the IGTF in matching the requirements from resource centres in the e-Infrastructure and identity providers would likely lead to duplication of effort if projects were to establish a parallel infrastructure for authentication and authorization.

In summary, the previous e-IRG recommendations have enabled and fostered an extensive programme to facilitate access to academic and research communities to the e-Infrastructure. It is now timely and appropriate to accelerate the process of improving identity management assurance levels nationally, to support the continued integration of federated ID in the International Grid Trust Federation – the IGTF being the established forum where resource centres and NGIs can coordinate their requirements with the identity providers and user communities, and to promote the use of compliant and secure science gateways and portals in the e-Infrastructure of EGEE and EGI.