EUGridPMA

With the same online resources in demand from researchers across the world, how are security requirements met and top secret research kept safe from prying eyes? **David Groep**, Chair of EUGridPMA explains how the organisation coordinates a highly distributed group of identity providers to deliver solutions

Can you outline the overall remit of the EUGridPMA? What primary issues does it work to address and what does your role encompass?

E-Infrastructure depends on collaboration and allows researchers from all over Europe to leverage ICT in order to work together and achieve better results faster. In the real world, such collaborations depend on personal contact, but science, faced with ever larger data volumes, is relying on virtual collaborations to bring people together. In this electronic world we need to find ways of establishing who we are without this face-to-face contact. The more valuable the resource, for instance, the greater the need for a comprehensive electronic identity. It can be annoying when someone enters an online forum under your name and quite serious when attackers read your personal emails. It is however disastrous if someone attains access to your bank account. Both users and resource operators therefore have an interest in ensuring good quality credentials, and confirming that all users at least meet some minimum requirements.

Today's research is a global exercise, and scientists use resources from all over the world, so we realised early on that a scalable system was needed to issue trustworthy credentials, in a way that obviates the need for registration at each and every site of a database. The EUGridPMA itself does not issue credentials, but coordinates a highly distributed group of national and regional identity providers, who are intimately familiar with the local environment, know their user base, and can work with national resource centres to collect requirements. Being local, they can actually ensure face-to-face meetings when issuing credentials for a user, and in doing so via a documented and standard process inspire the trust required by resource providers.

Making sure that these electronic identities in the grid infrastructure meet the minimum requirements set by resource providers and user communities is the task of the EUGridPMA, the European Policy Management Authority for grid authentication in e-Science.

A key aspect of your remit is to coordinate the 'global trust fabric' of grid infrastructures. Can you explain what this entails in layman's terms?

The 'trust fabric' is like a passport to the grid infrastructure. It provides every grid user and every computer system with a unique identity. When you give someone access to your computer systems, you want to be sure that it's the same person over time. And when tomorrow someone shows up with the same name, it should be the same registered person.

The trust fabric built by the EUGridPMA is based on a set of requirements and procedures jointly agreed by the resource providers in collaboration with the identity provider experts in the grid.

It is important to emphasise that the EUGridPMA focuses on what I would call technical trust. The basic premise of the PMA is to ensure that electronic identities are firmly bound to physical persons (or things), and that you can rely on the electronic name for granting or denying access to your services. It is not the role of the PMA to say that you have to grant access to anyone or deny it. Nor can we guarantee that nothing untoward shall ever happen to you – we can't – and nobody can, unless you cast your computer in concrete. What we give you is a unique way to identify every participant in the grid.

How integral is collaboration for today's IT industry? Can you discuss the range of players with whom you share relations? What are the benefits of this approach?

EUGridPMA serves the research community. Science has always been a global endeavour, and to some extent we are speeding up the forging of collaborations by bringing ICT into the mix. Open Access policies and responsible sharing of data not only helps others to validate research results, but it enables people to look at existing data in new ways, and take the next step.

For the EUGridPMA, our 'relying party' members are very important since they represent the interest of the resource centres and large multinational user communities that are at the forefront of e-Science. Major communities such as the European Grid Infrastructure (EGI) and the Partnership for Advanced Computing in Europe (PRACE) in Europe also play a key role in making risk assessments and reconciling security and availability. The national and regional identity providers at the same time bring in their local user base and ensure their requirements are discussed.

Having concrete requirements to work from, and a user base that requires solutions helps us to maintain focus. It is always tempting to follow the latest and greatest in technology, but when it does not solve

an actual problem at hand, you will only succeed in scaring your users away. The mixture of representatives in the EUGridPMA ensures a good combination of innovation and consolidation.

What targets do you have for the EUGridPMA, both in the short and long term?

EUGridPMA's infrastructure stands at a critical point: we have to make the jump from serving tens of thousands of ICT-savvy scientists to serving millions of researchers from a wide range of disciplines. The research infrastructures identified in the European Strategy Forum on Research Infrastructures (ESFRI) roadmap will determine the focus in the coming years, and there are a lot of new and exciting user cases to be addressed by the e-Infrastructure. Serving potentially millions of researchers from social sciences and humanities, life sciences, etc. means expansion to new technologies and a wider spectrum of resources. The security risks for these scenarios are more diverse, so we will also need to support different identity assurance levels.

We have gained significant experience in operating a trusted identity management fabric. Much of this technical knowledge is equally applicable to securing the collaboration infrastructure for virtual research communities as well. Here we will not be accrediting operators according to specific standards, but we will rather gather and document best practices and make these available as guidelines for the community.

In the end the participation of resources providers, users, and other parties in general will determine the success of the EUGridPMA. I believe that by supporting more security scenarios via differentiated assurance levels, and by promoting best practices, we can aid interoperability and support the development of ICT infrastructures for the European Research Area.

Safety and privacy remain of paramount concern within grid structures and the worldwide web more generally. What steps are you taking to safeguard users as far as possible?

Making an IT system safe is an end-to-end enterprise, with some conflicting requirements. Every user has a right to privacy, and identity providers have a special role to play in protecting personal data. The threat of identity theft is quite real, and the International Grid Trust Federation (IGTF) requirements demand each provider has a privacy and data release policy that complies with national laws and best practices.

On the other hand, incident response teams need to be able to identify, track and correlate suspicious behaviour across the entire grid. The people they chase in cyber-crime are seldom the legitimately identified users, but imposters and criminal organisations that have stolen electronic IDs or stolen passwords via malware and Trojans. It is important to correlate both grid and traditional information in catching the culprit, and as result electronic grid identities have to be sufficiently rich in data.

It is difficult to strike a balance, and for the time being the name of the person is in his electronic ID, but nothing else. Additional information, such as email addresses and phone numbers, are collected only when someone is actually granted access to a resource, or is enrolled as part of a research group.

Still, I expect this will change in the future. Some research for example is so sensitive that scientists will want to use pseudonyms to protect themselves or be fully anonymous. Good compensatory controls will allow resource owners access to pseudonymous users. Balancing the right to anonymity and the demands of good incident response will however require more time.

Can you offer an insight into the range of challenges associated with managing research efforts across the globe?

For me there are a couple of key elements that have made this international collaboration in identity management a success: a clear and strong use case for global interworking in science – the infrastructure has to work, and identity management is a precondition for everything else; a clear focus on solving technical policy coordination and steering clear of politics – thus making sure that all participants retain their own autonomy; and as a basic modus operandi recognising the national and regional initiatives as key elements of a global structure.

The PMA has also been fortunate in the support it has received from the European Commission and the e-Infrastructure Reflection Group, as well as EU projects such as Enabling Grids for E-Science (EGEE), Distributed European Infrastructure for Supercontinuity Applications (DEISA), PRACE and EGI-InSPIRE. Also a whole range of specific support actions, such as EUMedGrid, the E-Infrastructure shared between Europe and Latin America (EELA), and EUAsiaGrid, have helped expand the geographic region where the EUGridPMA and IGTF are active. The EUGridPMA needs this support to ensure the PMA stays on track and remains relevant to the community.

In the end, it all boils down to people appreciating what we share as well as our cultural traditions and differences, and learning and benefiting from them. For me it has been one of the most rewarding aspects of engaging with the IGTF; the spirit of camaraderie and the thrill of getting things done together and seeing developments applied.

www.eugridpma.org