# A Certification Authority for Grid *t*-Infrastructure

## An Online CA Case Study

Daniel Kouřil, Michal Procházka
CESNET z. s. p. o., Zikova 4, 160 00 Praha 6, and
Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic
e-mail: {kouril,michalp}@ics.muni.cz

## 1 Introduction

Current Grids provide great potential for complex problems solving but they are often too complex for unexperienced users. It is necessary to establish an effective training infrastructure—*t*-Infrastructure—that allows users to get quickly familiar with the environment. A secure and flexible user identity management is crucial for such a training infrastructure to be effective.

We propose a design of a solution introducing a controlled mechanism for the identity management suitable for training courses organization. A pilot implementation of the solution is being prepared in the EU EGEE project[1].

## 2 Grid Identity Management

Authentication in the Grids is usually based on the use of independent identity providers—certification authorities—that issue digital certificates asserting identity of their bearers. In order to provide an adequate level of trust, the Grid CAs implement a rigorous certification procedure, including strict rules that each requestor must fulfill before a certificate is issued to her. The certification policy usually involves a process of proper identification of the person, requiring the user to visit personally the CA office and present her official ID card and prove her affiliation with her home organization. Such a procedure makes it possible to build a trusted infrastructure where the certificates provide sufficient level of trust about identity of their owners. At the same time, however, the certification process is quite heavyweight for the users.

While this certification process is necessary for users aiming at a regular production use of the Grid, the standard certification procedure makes severe obstacles in situations where it is necessary to provide a lot of users with certificates in a fast way, for instance during training courses. It is not feasible to ask all the trainees to obtain proper certificates before the course starts, so the organizers must have a mechanism at hand that allows to provide the course attendees with certificates. Such certificates cannot replace that ones issued by the standard Grid CAs but they allow the users to get familiar with the Grid environment. In order for the resource owners to accept such certificates, they must minimize the risk of being misused.

The demand is evident for a well-established and formalized CA providing a service for organizing training events—*t*-CA. In this article we present a design of such a service based on an online CA solution that provides a good trade-off between level of trust and ease to use.

## 3 A *t*-CA Solution

The concept of an online CA is an emerging alternative to the classical model of a CA, where the signing machine is not kept disconnected from the network and allows to issue certificates on the fly. The online CAs are also often used as a "convertor" from other authentication methods, such as Kerberos. In this section we demonstrate how an online CA can be used to address the certification requirement of the *t*-Infrastructure.

### 3.1 *t*-Infrastructure Requirements

In order to be able to ensure smooth run of the training events, the organizers must be able to equip the attendees with certificates quickly and with minimal administrative overhead. The certificates issued this way must be trusted enough to be accepted by the end resources, which is the most challenging part of the design. The primary concern of the resource providers is to secure their facilities so the certificates must be traceable and their usage must be limited for a very short time.

### 3.2 Using an Online CA

We propose to use the online CA solution based on MyProxy [1] to fulfill the requirements. As it operates online and no operator is needed to handle the CA signing key, the certificates can be issued very efficiently on demand. In order to limit their usage all the certificates issued by the CA will be only short-lived (valid for 8 hours). Due to this limited lifetime, the model need not to deal with revocations and propagation of revocation information, which is one of the crucial problems in deployment of classic PKI.

[1] http://www.eu-egee.org/

Subject name of each issued certificate will be unique, formed using a generic name and the certificate serial number (e. g. "Grid Trainee 12345"). Such a naming will make it possible to base access control on subject names, which is a common technique in the Grids.

We follow the classical model of CA management and suppose to have multiple Registration Authorities that register new users with the online CA. These RAs must be familiar with the CA principles and policy and they also must be trained how to access the CA facilities in a secure manner. Usually, the course organizers will be trained this way.

In our model each user is registered by the RA as part of the on site registration. Each user is provided with a username/password pair. This combination is used by the user to generate a certificate from the online CA. The lifetime of the user record is limited to the duration of the training course, lifetime of each certificate generated by the user is limited to 8 hours. If the event spans multiple days than the user is required to retrieve a new certificate at the beginning of each day.

All operations of the CA are logged to allow further audit. This information allows to trace the person and the event where the certificate was issued, which may be useful in case an inproper behavior using this certificate is detected.

### 3.3 *t*-CA Operation

In order to allow easy access for the RAs we will provide a set of administrative tools that can be used to manage the users registered with the online CA. We will offer both command-line oriented tools and web-based interface to access the CA. Protecting this RA – CA channel is crucial for secure CA operation so we propose to use sophisticated methods for authentication, such as two-factor authentication based on the smart card technology.

As all interactions must be easy for the users we propose that all passwords generated by the system are random, yet easy to remember. We also suppose the password management will be tied with the rest of the *t*-Infrastructure so the same username/password combination could be used to access all the services (e. g. Grid portals and User Interface machine). Such an arrangement minimizes the risk of passwords being forgotten, lost, or shared.

### 3.4 CA Acceptance

In previous section a technical solution was described that fulfills the requirements for an *t*-CA. However, in order for such a CA to be acceptable by the resource providers, a formal accreditation of the CA should be possible. Such a process involves a scrutiny of the policy that describes in details the way how the CA works. We will write a document specifying such a policy that will be published and available for the trusted parties. Whenever possible, the document will follow the minimal requirements for Grid CAs as defined by the IGTF body[2], which is in charge of CAs accreditation. We also plan to specify the policy to be compliant with previously established recommendations for similar services, such as the "Accreditation Requirements for Short-Lived Credential Generation Services" profile defined by the IGTF.

[2] `http://www.gridpma.org/`

## 4 Security Considerations

The *t*-CA solution does not have any ambition to replace the model of current Grid CAs and their accreditation. Certificates issued by the *t*-CA service does not provide the same level of trust as the users cannot be identified properly by design. Even if precautions were defined that minimize the risk of misuse such certificates, the trusted parties should get familiar with the principle of the *t*-CA solution before they accept it on their resources.

## 5 Future work

Having a *t*-CA is not enough for a training course organization. A connection to the user management system is necessary as well, which ensures that users registered with the CA will also be allowed to access the end services. We plan to move from the current gridmap-file mechanism to the VOMS server, which is the basic authorization block of the EGEE infrastructure.

The *t*-CA solution will be installed in the production environment of the Virtual Organization for Central Europe (VOCE) of the EGEE project. The VOCE provides Grid facilities and training for users from the Central Europe region.

## 6 Conclusion

We presented a design of a CA that offers a controlled way for issuing certificates for training courses. We demonstrated how the proposed solution improve the training process and makes the training infrastructure more secure. We not only described the technical solution but also stressed the need for a formal policy, which allows everyone to check the details of the certificate process.

## References

[1] J. Novotny, S. Tuecke, V. Welch. "An Online Credential Repository for the Grid: MyProxy". *Proceedings of the Tenth IEEE Symposium on High Performance Distributed Computing (HPDC10)*. August 2001.