

## **TERENA eScience PKI**

**Milan SOVA**

CESNET, CZ

Currently, many grid projects and middleware rely on X.509 PKI to provide proper authentication. Besides its indisputable advantages, the PKI has some non-negligible costs. On one hand, they are represented by operating Certificate Authorities complying with strict requirements specified by IGTF PMAs. On the other hand, users very often find the management and especially obtaining certificates too cumbersome. The complexity of PKI has been repeatedly pointed out as one of the obstacles to wide-spread adoption of grid technology.

Several National Research and Education Networks associated in TERENA have joined their efforts to build a shared PKI able to serve potentially millions of users from their constituency. The TCS eScience Personal CA takes advantage of national identity federations to facilitate user identity vetting and enrolment procedures. The system uses identity management systems (IdMS) at participating institutions to perform the functions of registration authorities. The certificate enrolment application acts as a SAML Service Provider relying on information provided by IdMS performing as SAML Identity Providers (IdP). When applying for a personal certificate, users authenticate at their home IdP using credentials they normally use to access local services. The IdP controls the certificate issuance process by releasing SAML attributes specifying the user's eligibility for the service and the information to be included in the certificate such as the user's name and email address.

The TCS eScience Personal CA is part of the TERENA Certificate Services that uses a commercial PKI provider. Outsourcing the actual CA machinery to a specialized company results in professional-level services such as CRL and OCSP management.

The paper describes the legal, organizational and technical aspects of the TCS eScience PKI.