Valentin Pocotilenco, Veaceslav Sidorenco,
Technical University of Moldova, Stefan-cel-Mare av., 168,
Alexei Altuhov, Petru Bogatencov ,
RENAM Association Str. Academiei, 5, of 331

MD-GRID CERTIFICATION AUTHORITY

Certificate Authority is a trusted network entity, responsible for managing X509 digital certificates and is a trusted entity that validates the identity of the holder of a digital certificate. Paper describes the particularities of MD-Grid CA established for grid users and scientific communities of Moldova.

I. Introduction

A Certification Authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption and decryption. The CA computer, where the signing of the certificates will take place, needs to be a dedicated machine, running no other services than those needed for the CA operations. The CA computer must be located in a secure environment where access is controlled, limited to specific trained personnel.

Software-based private keys of the CA must be protected with a pass phrase of at least 15 elements and that is known only by designated personnel of the CA. On-line CA's using Host Security Module (HSM) must adopt a similar or better level of security. Copies of the encrypted private key must be kept on off-line media in secure places where access is controlled.

II. RENAM services

RENAM Association implements and run a range of services that require authorization or authentication [1,2]:

- CERT – since May 2007 RENAM association start own CERT center.

- GRID – in September 2007 RENAM association deployed first GRID site in Moldova and 4 new nodes are under construction under SEE-GRID range of EU-cofunded projects.
- Video conferences – RENAM can organize videoconferences using specific communication equipment and technologies.
- LMS – RENAM association can propose LMS to all their network users.
- Access to scientific publications.

III. GRID authentication and main actions for MD Grid CA deployment

European Grid computing authentication is based on services provided by the European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA)[3]. EUGridPMA is a body that was created to establish requirements and best practices for grid identity providers to enable a common trust domain applicable to authentication of end-entities in inter-organizational access to distributed resources. As its main activity the EUGridPMA coordinates a Public Key Infrastructure for use with Grid authentication middleware.

General structure of a RENAM CA in cooperation with EUGridPMA as root is represented at fig. 1. In process of development of CA, with EUGridPMA as root, following information must be conveyed to the PMA Chair:

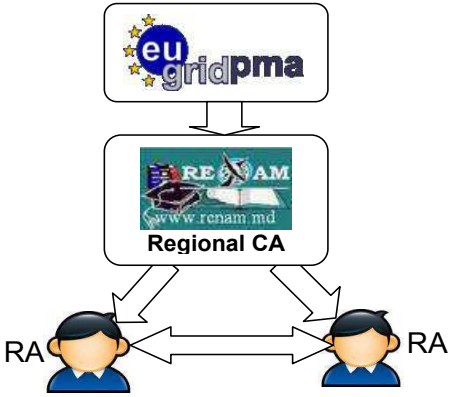

***Figure 1*. General structure of a RENAM CA in cooperation with EUGridPMA**

- Name of the person representing the Authority in the PMA and possibly an alternate. In this section will be provided complete information about responsible person, and their abilities to work in dedicated domains (data encryption, secured network's, and other).
- Contact information. In this section will be presented detailed contact information of CA geographical placement, phone or fax number's, email addresses.

- geographical and community scope of the Authority;
- CP and CPS document(s) and a link to where the CP/CPS will be made available to interested parties. In this section will be described a specific document, which is named Certificate policy/ Certification Practice Statement (CP/CPS). The document also can be retrieved through web site where CP/CPS is accessible.

CP is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

CPS is a statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

- fingerprint(s) of the source of trust or root certificate.

Each authority must publish for their subscribers:

- the CA root certificate or the set of CA certificates up to a self-signed root;
- a http or https URL of the PEM-formatted CA certificate;
- a http URL of the PEM or DER formatted CRL;
- a http or https URL of the web page of the CA for general information;
- the CP and/or CPS documents;
- an official contact email address for inquiries and fault reporting
- a physical or postal contact address

IV. Conclusions

At present RENAM is ready to put in production the CA, which will serve as a local CA and RA for Moldavian research and educational community for specific purposes like support of grid sites operation, MD-CERT, LMS, data transfer between applications, services with authentication and for the purpose of securing RENAM users data transfer.

References:

1. E. Peplow, P. Bogatencov, G. Secrieru, B. Varzari, V. Sidorenco, I.Fedeashin. RENAM: National Research and Educational Networking Association of Moldova. Acta Academica 2001. International Informatization Academy, Branch of R. Moldova, Chisinau, "Evrica", 2001, pp. 57-65.
2. Research and Educational Networking Association of Moldova. http://www.renam.md/
3. European Policy Management Authority for Grid Authentication. http://eugridpma.org/