IISAS Certification Authority

Jan Astalos
Department of Parallel and Distributed Computing
Institute of Informatics
Slovak Academy of Sciences
http://www.ui.sav.sk

IISAS and CrossGrid

- Grid application development
  - simulations related to prediction of flood events
- Collaborative problem solving environment
- Virtual organization for flood forecasting
- CrossGrid testbed participation
- IISAS Certification Authority

Need for certificates

- Virtual organization for flood forecasting
- Scientists from Slovakia participate in HEP experiments (ATLAS, ALICE)
- Scientists from other application areas, not related to any of current virtual organizations. (we expect new VOs to emerge)

IISAS Certification Authority

- Managed by IISAS, Bratislava, Slovakia
- Based on openssl
- Certificate issuing machine:
  - Located in a room with restricted access, in locked case
  - Not connected to network
  - Managed by CA operator

IISAS CA certificate

- Private key is 2048 bits long
- Encrypted by passphrase >15 characters
- CA certificate lifetime is 5 years
- Backup copy of the key and sealed envelope with the passphrase are locked in a safe

Certificates

- IISAS CA issues certificates for subjects:
  - Related to organizations from Slovakia
  - Involved in research or deployment of Grids
- Types of certificates:
  - Server, personal and services
- Applicability
  - Authentication and communication encryption

Certificates

- Private keys are at least 1024 bits long
- Generated by applicants
- Certificate maximum lifetime is one year
- Naming conventions:
  - C=SK, O=*organizationName*, OU=*organizationUnit*, CN=*commonName*

Certificate issuing procedure

- IISAS CA accepts authenticated certificate requests from IISAS registration authorities
- Other certificate requests are forwarded to appropriate RAs for authentication and validity checks
- Certificates are issued for authenticated requests
- Issued certificates are sent to the applicant

Authentication checks

- Applicant should contact RA personally
- Authentication is performed by:
  - Valid official ID document (Passport, ID card)
  - Firm personal acquaintance with RA
- RA also checks relation of applicant to organization specified in certificate request
- Requests for server or service certificate must be signed by valid certificate of system administrator

Certificate revocation procedure

- IISAS CA accepts revocation requests from RAs or certificate subscriber sent by e-mail signed by a valid IISAS certificate
- Other revocation requests are forwarded to appropriate RA for authentication and validity checks
- Certificates are revocated for authenticated requests
- Certificate subscriber is notified

Circumstances for revocation

- Information in certificate becomes wrong or inaccurate
- Private key was lost or compromised
- Certificate is no longer required
- Subject has failed to comply with rules in CP/CPS document
- The server for which the certificate was issued has been retired

CRLs

- CRLs are issued whenever certificate is revocated
- Reissued at least 7 days before CRL expiration
- CRL lifetime is 30 days
- CRLs are published as soon as issued

CP/CPS document

- Draft version 0.4 (September 2, 2002)
- OID: 1.3.6.1.4.1.13496.1.2.1.0.4
- Follows structure suggested by the RFC 2527
- CA, RA's and certificate owners are obliged to follow procedures specified in CP/CPS document
- Certificate subscribers are notified about changes
- Relation of certificate and version of CPS document is based on the date the version was released

Information publishing

- IISAS CA online repository contains:
  - IISAS CA certificate
  - Latest CRL
  - Copy of CPS/CP document
  - Other relevant information (list of RAs)
  - LDAP repository (to be created)
- URL: http://ups.savba.sk/ca/

Event logs

- Boots of CA signing machine
- Interactive logins and logouts
- Certification requests
- Revocation requests
- Issued certificates
- Issued CRLs

Registration Authorities

- RAs will be created for organization and VO
  - trusted by members of VO
- CA - RA communication will be secured
- List of RAs will be maintained at:
  - http://ups.savba.sk/ca/ra-list.html
- RAs will log
  - Certificate requests
  - Revocation requests

Thank you.