6th EUGridPMA meeting in Vienna,
January 25-27 2006

pkIRISGrid

a PKI for e-science activities provided by the Spanish NREN RedIRIS

Javi Masa, RedIRIS
javi.masa@rediris.es

RedIRIS

red.es

pkIRISGrid - Overview

- General information
- PKI structure
- CA
  - Certificate and private key
- End-entity
  - Certificate and private key
- Computer security controls
- Certificates
- Revocations and CRLs
- Record archival
- Repository

pkIRISGrid - General information

- pkIRISGrid CA is the PKI used in IRISGrid
  - IRISGrid is the infrastructure to support e-science activities provided by the Spanish NREN RedIRIS
- pkIRISGrid CA was established in April, 2005
- CP/CPS document follows RFC 3647
- Current CP/CPS OID:
  - 1.3.6.1.4.1.7547.2.2.4.**1.1.0** (Version 1.1.0)

pkIRISGrid - General Architecture

- Single Certification Authority
  - Issue certificates
  - Issue CRLs
  - Revoke certificates
- A group of Registration Authorities
  - Validate the identity of the end entities
  - Authenticate and approve their requests
  - Forward validated requests to the CA

pkIRISGrid - CA certificate

- Self signed
- Certificate lifetime 10 years
- Name form:
  - DC=es, DC=irisgrid, CN=IRISGridCA
- Accessible from:
  - http://www.irisgrid.es/pki/cacert/
- Basic Constraints: CA: TRUE
- Extensions Key Usage and Basic Constrainst marked as critical

pkIRISGrid - CA Private Key

- Private key length is 2048 bits
- Protected by a pass phrase
  - Pass phrase length is greater than 16 characters
  - Instances of the private key encrypted with operators pass phrase
- Private key backup
  - Extra instance of the private key encrypted with a randomly generated pass phrase are stored on removable media
  - Pass phrase kept in paper form placed in a sealed envelope
  - All backup copies (operators and extra) are kept as secure as the one used for signing

pkIRISGrid - End-entity Certificates

- End-entities
  - Natural persons, Network entities (host, service)
- Certificate lifetime: 1 year
- Name form
  - DC=es, DC=irisgrid, O=organization_string, CN=**name.surname**
  - DC=es, DC=irisgrid, O=organization_string, CN=FQDN
  - DC=es, DC=irisgrid, O=organization_string, CN=**service**/FQDN
- Accessible from
  - http://www.irisgrid.es/pki/valid_cert.phtml
- **Basic Constraints**: CA: FALSE
- Extensions **Key Usage** and **Basic Constraints** marked as critical

pkIRISGrid - End-entity private key

- Subscriber generates its own key pair
  - Web interface
- CA and RAs
  - Do not generate end-entities private key
  - Have no access to the user's private key
- Key length: 1024 or 2048 bits
- Protected by a pass phrase

- CA security controls
  - Dedicated offline machine
  - Without network adapter
  - It is switched off between signing operations
  - Laptop stored in a non-flammable vault when not in use
  - Certificates and keys stored in USB sticks in vault
  - Physical access is restricted to pkIRISGrid CA operators
- RA security controls
  - Hosted by RedIRIS servers (TLS)
  - User interface
    - `https://RAn.irisgrid.es`
  - Administrator interface (PAPI protected)
    - `https://RAn.irisgrid.es/admin/`

pkIRISGrid
Certificate enrollment process (person) - I

- User
  - generate key pair with form provided at the pkIRISGrid web site
- Entry/CSR is stored in LDAP
- RA operator
  - Uses admin module to show all pending CSRs
  - Meet user to validate data and identity
- User
  - Shows ID card (with photo), CSR number, and introduces the PIN set when certificate was requested
- RA operator
  - Approves CSR
  - Uses admin module to export approved CSRs to CA

- CA operator
  - Receives a mail with information to download new CSRs/CRRs
    - Download CSRs and CRRs (in XML format)
  - Copy the file to an USB stick (aux1)
  - Starts CA laptop and attaches CA key USB stick
  - Execute CA software (ca, crr, crl, ...)
    - Software detects unauthorized data modifications
    - Signs, denies, revokes, generates CRL
    - and produces LDIF files
  - Copy LDIF files to the USB stick (aux1)
  - Extracts USB sticks
  - Power off and stores laptop and CA key USB stick in vault

pkIRISGrid
Certificate enrollment process (person) - III

- CA operator
  - Carries USB stick (aux1) to a network access computer
  - Upload LDIF files to pkIRISGrid LDAP server
    - Update certificates, traces, revocations, CRLs, ...
    - Using ldapmodify command or another secure program
- Cron process
  - Finds entries modified today and
  - Sends mails with instruction to download certificates, ...

pkIRISGrid - Revocation circumstances

- Certificate will be revoked
  - CA is informed that the subscribed has ceased to be a member of or associated with a pkIRISGrid program or activity
  - Private key is lost, compromised or suspected to be compromised
  - It is not needed any more
  - Incorrect information is noticed in the certificate
  - The private key of the pkIRISGrid CA have been compromised or lost

pkIRISGrid - Revocation request

- Who can request revocation
  - The owner of the certified key
  - pkIRISGrid CA or any RA that has proof of a compromise
  - The RA which authenticated the owner of the certificate
  - The holder of the private key (not always the owner ;)
  - Any person presenting proof of knowledge that the subscriber's private key has been compromised or some data changed
- Procedure for revocation request
  - By the owner of certificate using the online revocation facilities
    - In case of emergency going to the RA as soon as possible and ask the appropriate RA to request revocation
  - By the RA administrator using a secure web interface
  - By the CA administrator

pkIRISGrid - CRL

- CRL v2
- Valid 30 days
- Includes all revoked certificates
- Issued immediately after every certificate revocation process
- Issued at least 7 days before expiration
- CRL public repository:
  - http://www.irisgrid.es/pki/crl/
  - ldap://ldap.rediris.es:1380/cn=IRISGridCA,dc=irisgrid,dc=es

pkIRISGrid - Records Archival
(minimum retention period: 3 years)

- RA (web/LDAP server) will record and archive
  - Certificate signing requests
  - Certificate revocation request
  - Validation of certificate signing requests from RA
  - Export of CSRs from RA
  - Issue and import of certificate to LDAP
  - Revocation of certificate (admin/user)
  - Issued CRLs
- CA will record and archive
  - Login, logout, reboot of the CA computer
  - CSRs and CRRs
  - Issued certificates
  - Issued CRLs

pkIRISGrid - Repository

- Public repository
  - `http://www.irisgrid.es/pki/`
  - Policy document
  - pkIRISGrid CA certificate
  - Valid certificate list
  - Certificate revocation list
  - Link to EUGridPMA home page (*when we obtain accreditation*)
  - Contact information
- RA
  - Certificate request link
  - Certificate revocation link
  - Download certificates
  - Help

pkIRISGrid - Thank you

- Thanks to Tony Genovese (our main reviewer)
- And you all for your patience

pkIRISGrid - Contact Information

- Contact information
  - Name: Javi Masa
  - Email: javi.masa @ rediris.es
  - Phone: +34 955056623
  - Address: RedIRIS. Edificio CICA.
    Avenida Reina Mercedes s/n.
    41012. Seville.
    Spain
- This presentation can be downloaded from:
  - http://www.irisgrid.es/coord/eugridpma/
    pkirisgrid-20060125-eugridpma-vienna.pdf