Grid-Ireland CA Update

David O'Callaghan

8th May 2012

25th EU Grid PMA Meeting

SCC, KIT, Karlsruhe, Germany

Overview

- Practice updates
- Policy updates
- Plans and Issues
- Robots

Practice updates

- Updated process for adding an RA (i.e. agent)
  - Letter from RA's superior signed by superior and RA-to-be agreeing to comply with procedures and policy
- RA-CA communication mechanism
  - RA can access web interface via X11 over SSH
- New RA: RA-ICHEC-Galway
  - For Ireland's national HPC centre / PRACE partner
- Signing CRLs with SHA1

Policy Updates

- Draft in progress that
  - moves from 2527 to 3647 template
  - with minimal required changes from current version for compliance.
- Re-writing needed to make it readable and properly use 3647 template
  - Empty sections
  - Information in incorrect sections
- Robots (later…)

Plans & Issues

- Federated-Identity—assisted Classic CA Prototype
  - fill user registration through Shib-protected form
- SLCS Prototype
  - Based on MyProxy CA / GridShib CA
- SHA-2 support to be checked…
- Remote identity vetting (e.g. via videoconf)

Robot Certificates

- Would like to introduce these for automation, etc. for grid and HPC
- Will follow “Guidelines on IGTF Approved Robots”
  - Assume software tokens (i.e. file-based storage)

Robot Certificate Policy Text

3.2.3 Authentication of individual identity

1. The certificate must be requested from the Grid-Ireland RA in person, or be authenticated with a valid personal Grid-Ireland CA certificate;
2. The certificate request must be preceded by a secure online submission to the Grid-Ireland CA Public Server;
3. The identity of the Robot certificate owner must be authenticated as for a personal certificate;
4. The RA must retain a record to allow a Robot certificate to be traced to its owner.

Robot Certificate DN

C=IE, O=Grid-Ireland,
OU=*example.ie*, L=*RA-TCD*,
CN=Robot: *robot name* managed by *owner*

- Robot name expresses some intended purpose, e.g. “CMIP5 iRODS LFC client”
- Owner is email address of persistent group or natural person responsible for robot, e.g. “help@grid.ie” or “david.ocallaghan@cs.tcd.ie”
- May replace : with -

Robot Certificate Profile

Basic Constraints (Critical) CA:FALSE
Key Usage (Critical) Digital Signature, Key Encipherment
Subject Key Identifier <subject's key identifier>
Authority Key Identifier <auth key id>

Subject Alternative Name email:<owner's e-mail address>
Issuer Alternative Name email:grid-ireland-ca@cs.tcd.ie
Extended Key Usage clientAuth
Certificate Policies
(Robots) 1.2.840.113612.5.2.3.3.1
(PKP Soft) 1.2.840.113612.5.2.3.1.2.1