Security Update

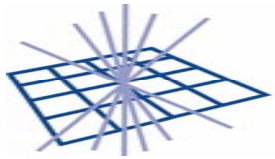
LCG GDB

CERN, 6 Dec 2006

David Kelsey

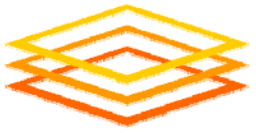
CCLRC/RAL

d.p.kelsey@rl.ac.uk



GridPP

UK Computing for Particle Physics



Open Science Grid

Overview

- News
- IGTF issues
- New top-level Policy document
- Site Operational Procedures Policy

News

- Oxana Smirnova joined JSPG
  - To represent NDGF
- Ian Neilson (LCG Security Officer)
  - Moving to other tasks in Grid Deployment
- Romain Wartel
  - New EGEE Security Officer
  - Leads OSCT
- WLCG Security (not an operational role)
  - DPK - Security Coordinator
- *Big thanks to Ian for his major contributions*

IGTF issues

- International Grid Trust Federation
  - Coordinates Grid Authentication (CAs)
  - 3 regional PMAs
- DPK represents LCG as “Relying Party” on EUGridPMA
- Recently requested to join TAGPMA (Americas)
  - LCG has many users and resources in Americas
  - TAGPMA is dealing with online CA profiles
- I attended TAGPMA meeting last week
  - Membership approved
- JSPG drafting our “requirements” on IGTF

Requirements for IGTF

From: The LCG/EGEE Joint Security Policy Group (JSPG)
Draft Dated: 28 November 2006
Subject: (Draft) Relying Party Requirements for IGTF from LCG/EGEE
(not yet approved by the projects management bodies)

- LCG and EGEE endorse the requirements expressed by Open Science Grid (dated 11 March 2005) as presented and discussed at the Tallinn EU Grid PMA meeting in May 2005. (see http://www.eugridpma.org/agenda/fullAgenda.php?ida=a052
  - Thursday agenda item at 09:15)

- LCG and EGEE, as relying parties, agree with all of the statements and proposals included in the OSG document and asks the IGTF and regional PMA's to treat this OSG document as also describing the requirements of LCG/EGEE.

IGTF requirements (2)

In addition to the OSG requirements, LCG/EGEE asks IGTF to meet the following requirements:

1) Naming

- For an end-entity certificate issued to a natural person, a commonName attribute MUST be used as part of the subject DN, and it MUST contain a reasonable presentation of the actual name of the end-entity, as this is used as one item of confirmation during the user registration process with the VO.

2) Identity vetting

- The CP/CPS MUST describe:
  - How the identity (DN) assigned in the certificate is unique within the namespace of the issuing CA
  - How the identity (DN) assigned in the certificate will never be re-issued to another end entity during the lifetime of the CA
  - How the CA attests to the validity of the identity

IGTF requirements (3)

- In order for a registration authority (RA) to validate the identity of a person, the subject SHOULD contact the RA face-to-face and present valid government or employer issued photo-id and/or official documents.

- If face-to-face is not possible then the CP/CPS MUST describe:
  - How the CA provides accountability, showing that they have verified enough identity information to get back to the physical person any time during the lifetime of the certificate

IGTF (4)

- Lots of ongoing discussion
  - How to do identity proofing if not face to face?
    - What info needs to be presented/recorded?
  - How to check that person requesting a service certificate is allowed to do so?
- Long term solution
  - Levels of Assurance – and technology to use them
  - Sites and VOs can then decide what level they need
- Short term
  - We have to agree a common worldwide solution

Top-level Security Policy

- New, revised document
- Structure and approach presented to GDB in Oct 06
- Current draft (V5.3)
  - Discussed at JSPG face to face meeting (17 Nov)
- V5.4 almost ready
  - But not for presentation today
- Will be distributed by e-mail soon
- For discussion in Jan GDB

Site Operational Procedures Policy

- **https://edms.cern.ch/document/726129**
  - **Draft V0.8, 20 Sep 2006**
- **Presented at Oct GDB**
- **Questions raised then**
  - **Have any lawyers seen it?**
  - **Who is the authorised signatory at the site?**
- **Since then**
  - **Had very useful meeting with CERN legal experts on 16 Nov (JSPG)**
  - **Updated version produced at JSPG (5 Dec)**

Site Policy (2)

- General feedback from CERN legal
  - Happy with overall approach
  - Lots of useful suggestions on wording
    - Consistent wording with Grid AUP and main policy
  - Do not specify who is the authorised signatory
    - Sites to decide (same as for contracts)
  - Suggest adding a disclaimer clause (not there yet)
- Version attached to today's agenda
  - Draft coming out of yesterday's JSPG
  - Needs one more round with CERN lawyers and JSPG
- Will be distributed as soon as we can
  - Needs to go back to EGEE ROC managers again

Requests to GDB

- Please comment on the
  Site Operational Procedures Policy
  - For approval in Jan GDB
- Comment on new top level policy (when sent)
  - First discussion at Jan GDB
  - Approval at Feb GDB

JSPG Meetings, Web etc

- Meetings - Agenda, presentations, minutes etc

http://agenda.cern.ch/displayLevel.php?fid=68

- JSPG Web site

http://proj-lcg-security.web.cern.ch/

- Membership of the JSPG mail list is closed, BUT
  - Requests to join stating reasons to D Kelsey
  - Volunteers to work with us are always welcome!
- Policy documents at

http://cern.ch/proj-lcg-security/documents.html