Logistics of Large Scale CA - Deployment & Operations

Matthew Viljoen

Grid Operations Support Centre

Grid Operations Support Centre
http://www.grid-support.ac.uk/

GOSC

Run by the Grid Operations Support Centre, a distributed "virtual centre" providing deployment and operations support for the UK e-Science programme.

Matthew Viljoen

R.A.L.

CA

- De facto CA for UK e-Science community
- Medium Assurance Level CA for the Grid.
- Issues User and Server certificates
- One of the largest Grid CA in the world

Matthew Viljoen
R.A.L.

CA Infrastructure

- Manage 97 Registration Authorities (RAs) at ~42 institutions - a total of ~120 people

- Bath University - BBSRC - Birmingham University - Bristol University - Brunel University - Cambridge University - Cardiff University - Cranfield University - Culham Science Centre - Daresbury Laboratory - Diamond Light Source Ltd. - Durham University - NeSC, Edinburgh - Glasgow University - Imperial College, London - Lancaster University - Leeds University - Leicester University - Liverpool University - Manchester University - NERC - Newcastle University - Nottingham University - Oxford University - Plymouth Marine Laboratory - Portsmouth University - Queens University, Belfast - Queen Mary University of London - Reading University - Royal Holloway University of London - Rutherford Appleton Laboratory - Sheffield University - Southampton University - Stirling University - Swansea University - Surrey University - University College London - University of East Anglia - University of Wales, Aberystwyth - University of Wales, Bangor - Warwick University - Westminster University - York University

- Regular RA training courses

- Certificate validity: root = 5 years; user = 1 year

Matthew Viljoen
R.A.L.

Overview

Since 2002:

- Over 6700 certificates issued to date
- ~15% revocation rate
- ~3200 live certificates currently
- Upgrade from OpenCA 0.6.22 to 0.9 in 2005 - many usability issues addressed

Matthew Viljoen
R.A.L.

Architecture

- Centrally administered, Portal based
- RBAC for RA login

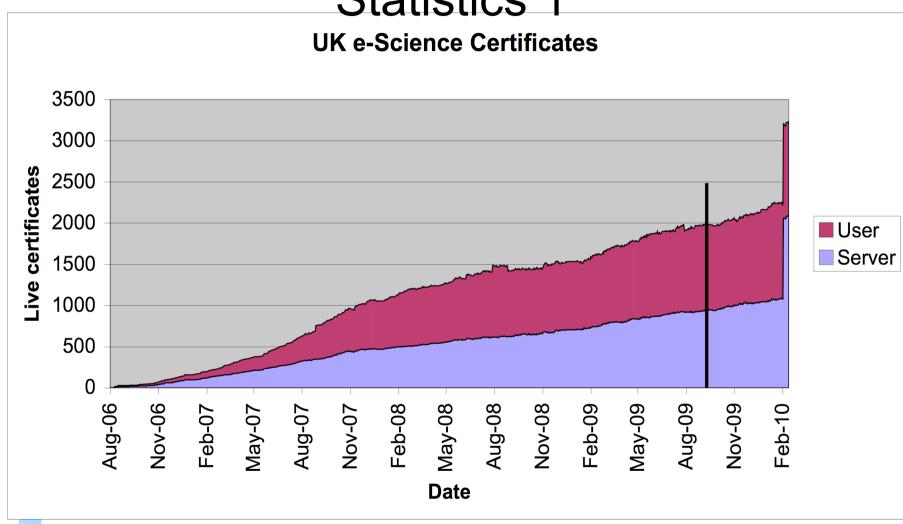| *Interface*	
public	no certificate required *(new certificate request)*
admin	any valid certificate required *(renewals, revocations)*
ra	RA operator certificate required
node	CA operator certificate required

ra and **node** interfaces also authenticate via Apache
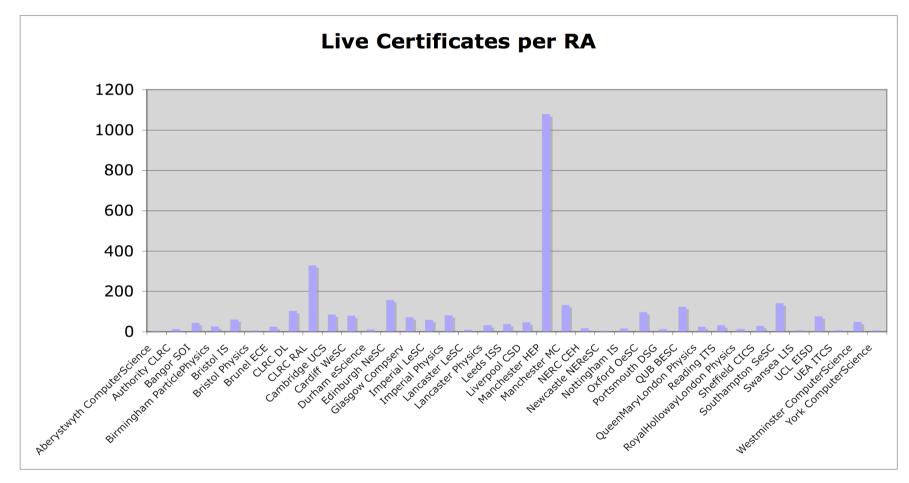
Matthew Viljoen
R.A.L.

Statistics 1

UK e-Science Certificates

Matthew Viljoen
R.A.L.

Statistics 2

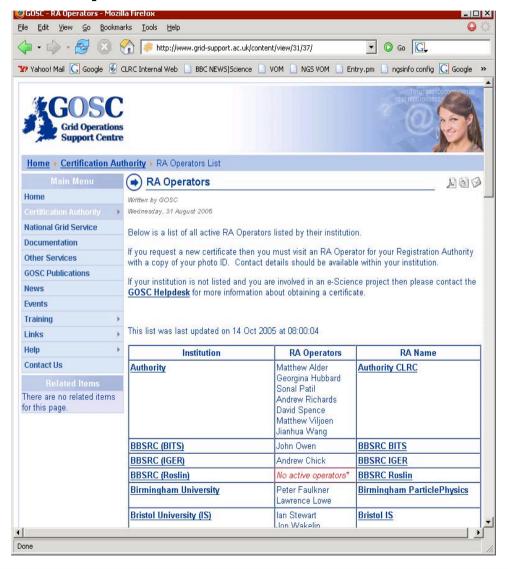**Live Certificates per RA**

Matthew Viljoen

R.A.L.

Logistic Challenges

- Comprehensive helpdesk system
- Guide users through enrollment procedure
  - Arrange meeting between users/RAs
  - automatic customized emails:
    1. ->RA informing of new request
       ->User to meet RA
    2. ->User to download signed certificate
    3. ->Reminders of pending certificate expiry
- Scalability concerns (middleware & hardware)

Problem of Lapsed RAs

- **Dynamic RA operator list which is database driven**

Other operational issues

- User feedback
  - Indirectly through RA audit to uncover usability-related problems (end user & RA operator) Also CP/CPS compliance
- Offer alternative interfaces
  - > Alternative interfaces with CA (Applet, Bash/Python)
- Comprehensive online help

Matthew Viljoen

R.A.L.

Future plans

- Purchase of HSM

- Hierarchical CA structure to cater for other certificate usages

  – training/low assurance CA, object signing, encryption?

Matthew Viljoen
R.A.L.

Thank you

Matthew Viljoen

m.j.viljoen@rl.ac.uk

Grid Operations Support Centre

http://www.grid-support.ac.uk