CCLRC
Rutherford Appleton Laboratory

GOSC

UK e-Science CA - Status and Upgrade

Matthew Viljoen

Grid Operations Support Centre

support@grid-support.ac.uk

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

Matthew Viljoen
R.A.L.

GOSC

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

CCLRC

MANCHESTER 1824
The University of Manchester

UNIVERSITY OF OXFORD

THE UNIVERSITY OF EDINBURGH

CA

- De facto CA for UK e-Science community
- Medium Assurance Level CA for the Grid.
- Issues User and Server certificates
- Internationally accepted. First (and so far only) non-US CA to be accepted by TeraGrid. EUGridPMA member
- One of the largest Grid CA in the world

CA Infrastructure

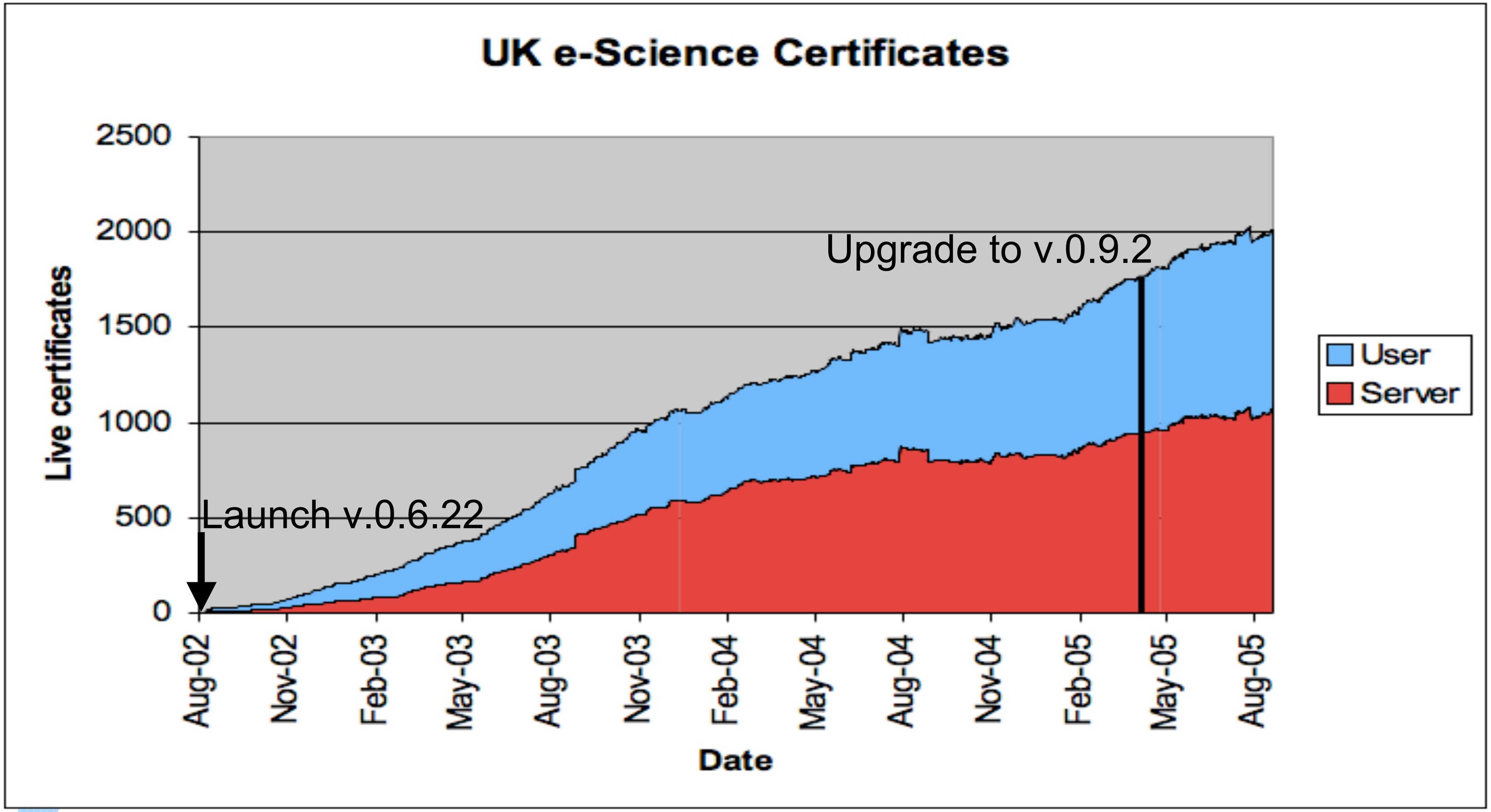
- Manage 97 Registration Authorities (RAs) at ~42 institutions - a total of ~120 people
- Bath University - BBSRC - Birmingham University - Bristol University - Brunel University - Cambridge University - Cardiff University - Cranfield University - Culham Science Centre - Daresbury Laboratory - Diamond 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

Statistics

Since 2002:

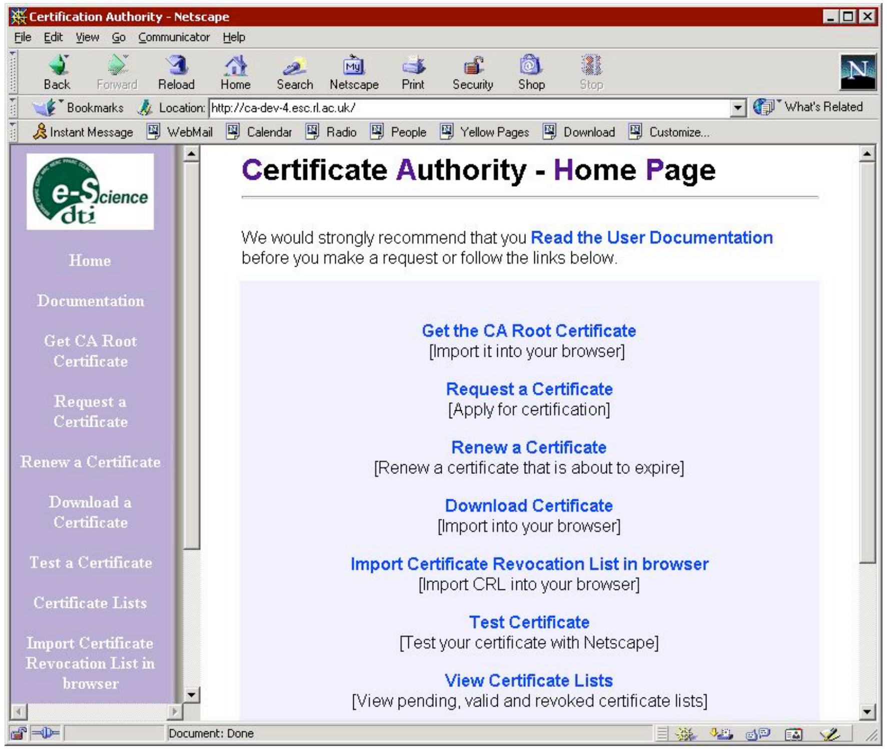
- Over 4900 certificates issued to date
- 15% revocation rate
- ~2100 live certificates currently

Statistics 2



Original Production CA

- Launched in July 2002 as replacement for UKHEP Testbed CA
- -> Production e-Science CA
- Based on OpenCA v.0.6.22



Certificate Authority - Home Page

We would strongly recommend that you Read the User Documentation before you make a request or follow the links below.

Get the CA Root Certificate
[Import it into your browser]

Request a Certificate
[Apply for certification]

Renew a Certificate
[Renew a certificate that is about to expire]

Download Certificate
[Import into your browser]

Import Certificate Revocation List in browser
[Import CRL into your browser]

Test Certificate
[Test your certificate with Netscape]

View Certificate Lists
[View pending, valid and revoked certificate lists]

Requirements #1

- Reliability
- Ease of use
- Security (inc. offline signing)
- Scalability
- Cost effectiveness
- Ease of fine tuning -> access to source

We chose OpenCA Research & Development Labs

Requirements #2 (Grid/UK-specific)

Not provided by OpenCA:

- Easy way of renewing certificates keeping **SAME** distinguished name
- Server certificate CNs need to be one of two forms:
  - *Without* service:

    `grid-data.rl.ac.uk`
  - *With* service type:

    `gsiftp/grid-data.rl.ac.uk`
- DN namespace reflecting issuing RA:

  `C=UK/O=eScience/OU=Authority/L=CLRC/CN=matthew viljoen`

Requirements #3 (User)

- Automatic notifications
  - informing RA of new request/renewal/revocation*
  - informing user of imminent expiry of certificate

**Not* provided by OpenCA

2002-2005 Problems

- Reluctance to update -> Divulgence from OpenCA project
- Incompatibility with newer browsers (only NS4.79 and IE were supported for enrollment; NS4.79 for RAs) -> Instability
- Scalability issues (Berkeley DB?)

2005 Upgrade

- Evaluated OpenCA 0.9.2

  Increased security ✓

  Cleaner architecture ✓

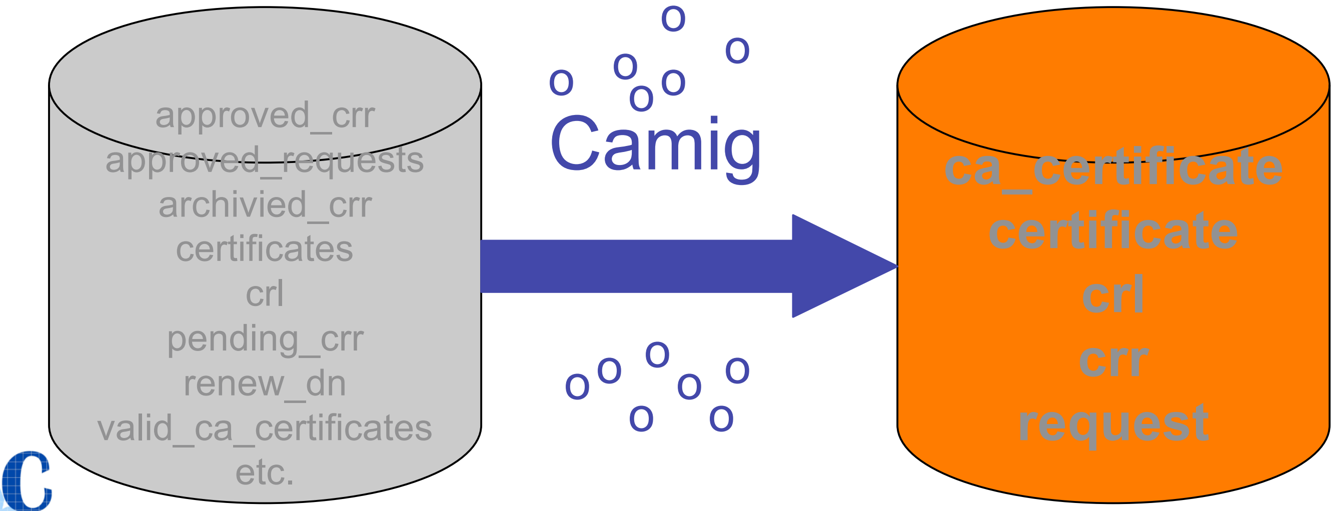
  Improved scalability ✓

  Enhanced browser support ✓

  Look and feel ✓

CA Database Migration

- 1800 Live certificates
- Scalability problems with BDB -> migrate to RDBMS (PostgreSQL)
- Wrote migration program in Java



approved_crr
approved_requests
archivied_crr
certificates
crl
pending_crr
renew_dn
valid_ca_certificates
etc.

Camig

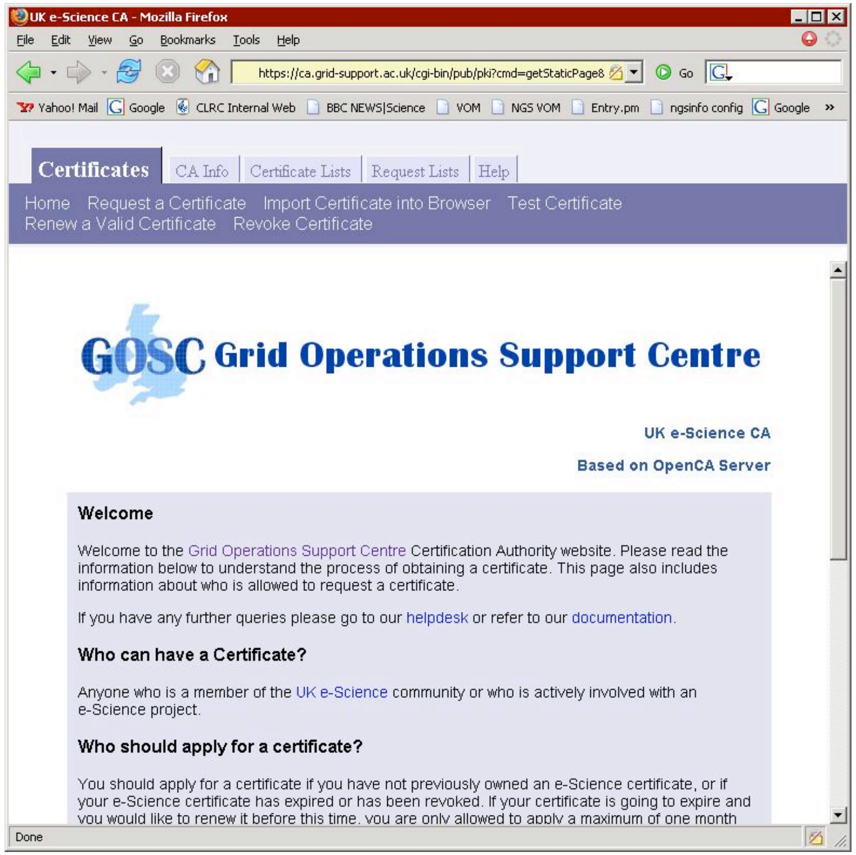
ca_certificate
certificate
crl
crr
request

April 2005 - Upgrade complete!

After modifying OpenCA 0.9.2 to include Grid CA/UK specific requirements:

- same DN renewal
- renewals/revocations requiring certificate to be presented
- RA in DN
- RA notifications
- extra checks of requests
- check for temporal DN uniqueness
- removed login+approval signing
- …

Minimal DB changes


UK e-Science CA - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ca.grid-support.ac.uk/cgi-bin/pub/pki?cmd=getStaticPage8
Go
Yahoo! Mail
Google
CLRC Internal Web
BBC NEWS|Science
VOM
NGS VOM
Entry.pm
ngsinfo config
Google
Certificates
CA Info
Certificate Lists
Request Lists
Help
Home
Request a Certificate
Import Certificate into Browser
Test Certificate
Renew a Valid Certificate
Revoke Certificate
GOSC Grid Operations Support Centre
Done

UK e-Science CA

Based on OpenCA Server

Welcome

Welcome to the Grid Operations Support Centre Certification Authority website. Please read the information below to understand the process of obtaining a certificate. This page also includes information about who is allowed to request a certificate.

If you have any further queries please go to our helpdesk or refer to our documentation.

Who can have a Certificate?

Anyone who is a member of the UK e-Science community or who is actively involved with an e-Science project.

Who should apply for a certificate?

You should apply for a certificate if you have not previously owned an e-Science certificate, or if your e-Science certificate has expired or has been revoked. If your certificate is going to expire and you would like to renew it before this time, you are only allowed to apply a maximum of one month

Authentication Mechanisms

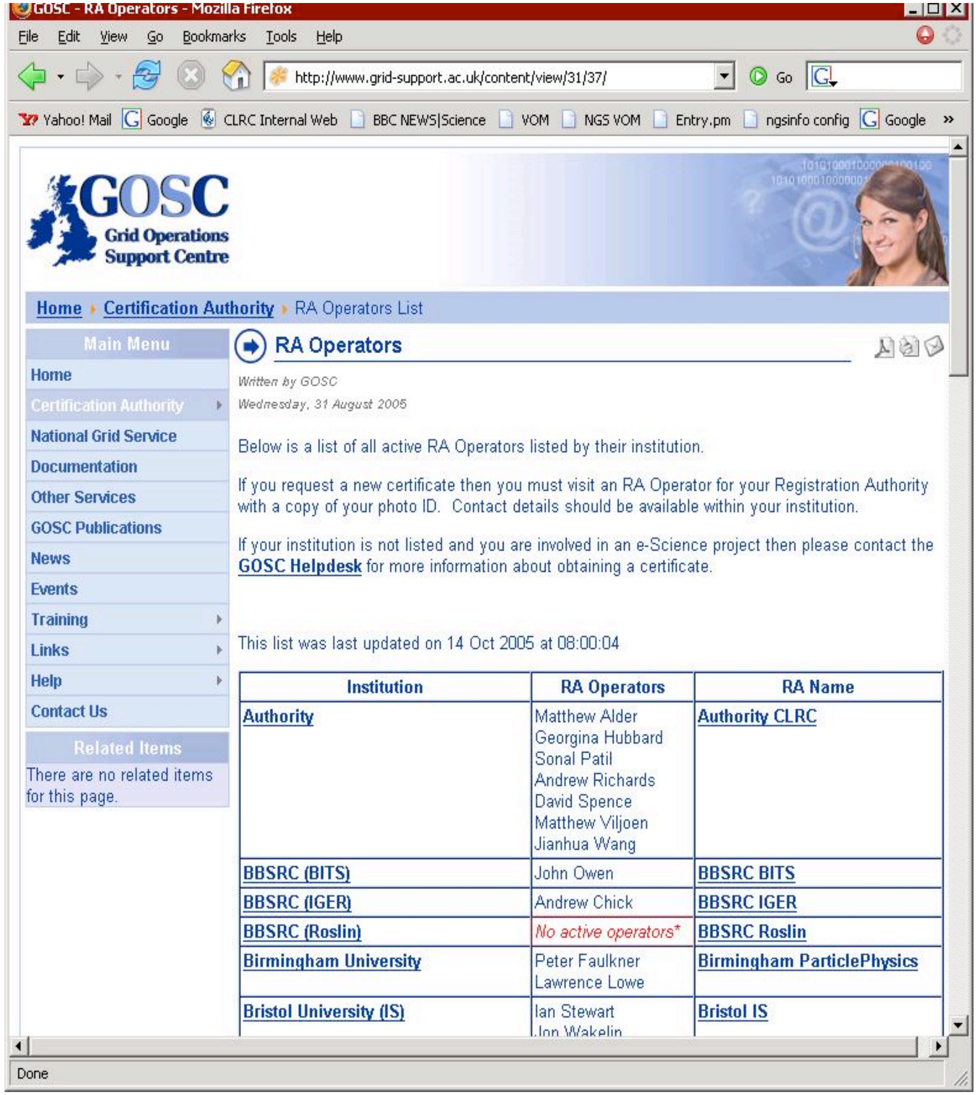
Interface

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

ra and **node** interfaces also authenticate via apache

Other work

- Dynamic RA operator list which is database driven
- Monitoring


GOSC - RA Operators - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.grid-support.ac.uk/content/view/31/37/
Go
Yahoo! Mail Google CLRC Internal Web BBC NEWS|Science VOM NGS VOM Entry.pm ngsinfo config Google »
GOSC
Grid Operations Support Centre
Home › Certification Authority › RA Operators List
Main Menu
Home
Certification Authority
National Grid Service
Documentation
Other Services
GOSC Publications
News
Events
Training
Links
Help
Contact Us
Related Items
There are no related items for this page.
Done

RA Operators

Written by GOSC
Wednesday, 31 August 2005

Below is a list of all active RA Operators listed by their institution.

If you request a new certificate then you must visit an RA Operator for your Registration Authority with a copy of your photo ID. Contact details should be available within your institution.

If your institution is not listed and you are involved in an e-Science project then please contact the GOSC Helpdesk for more information about obtaining a certificate.

This list was last updated on 14 Oct 2005 at 08:00:04

Institution	RA Operators	RA Name
Authority	Matthew Alder Georgina Hubbard Sonal Patil Andrew Richards David Spence Matthew Viljoen Jianhua Wang	Authority CLRC
BBSRC (BITS)	John Owen	BBSRC BITS
BBSRC (IGER)	Andrew Chick	BBSRC IGER
BBSRC (Roslin)	*No active operators**	BBSRC Roslin
Birmingham University	Peter Faulkner Lawrence Lowe	Birmingham ParticlePhysics
Bristol University (IS)	Ian Stewart Jon Wakelin	Bristol IS

Usability issues

- RA audit to uncover usability-related problems (end user & RA operator)
- Complex workflow
- Simplify PKI for the non-specialist (browser-dependant issues)

  OR: *Why do I need to use the same browser to download my certificate that I used to request my certificate?*

  – > Alternative interfaces with CA (Applet, Bash/Python)
- Streamline and integrate online help

Future work

- Keep track of latest OpenCA versions & version history
- Support for handling bulk requests
- Incorporation of HSM
- RA notification of “forgotten” requests
- Consolidate our Grid/UK CA changes
- Perhaps launch separate Grid/OpenCA distribution?

Thank you

Matthew Viljoen

m.j.viljoen@rl.ac.uk

Grid Operations Support Centre

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