CA Stuff

Jens Jensen

Dave Meredith

John Kewley

GridPP31, Imperial, London

Sept. 2013

Current Stuff

- Rather more shoestring without NGS
  - Implications for DR/BC and innovations
- Still pretty large, still alive, still running

People

- Jens Jensen – CA manager
- Dave Kelsey – ambassador extraordinary
- John Kewley – Support
- Suleman Tariq – admin
- Dave Meredith – CW code
- + 2-3 people doing day-to-day signing
- + the TAG

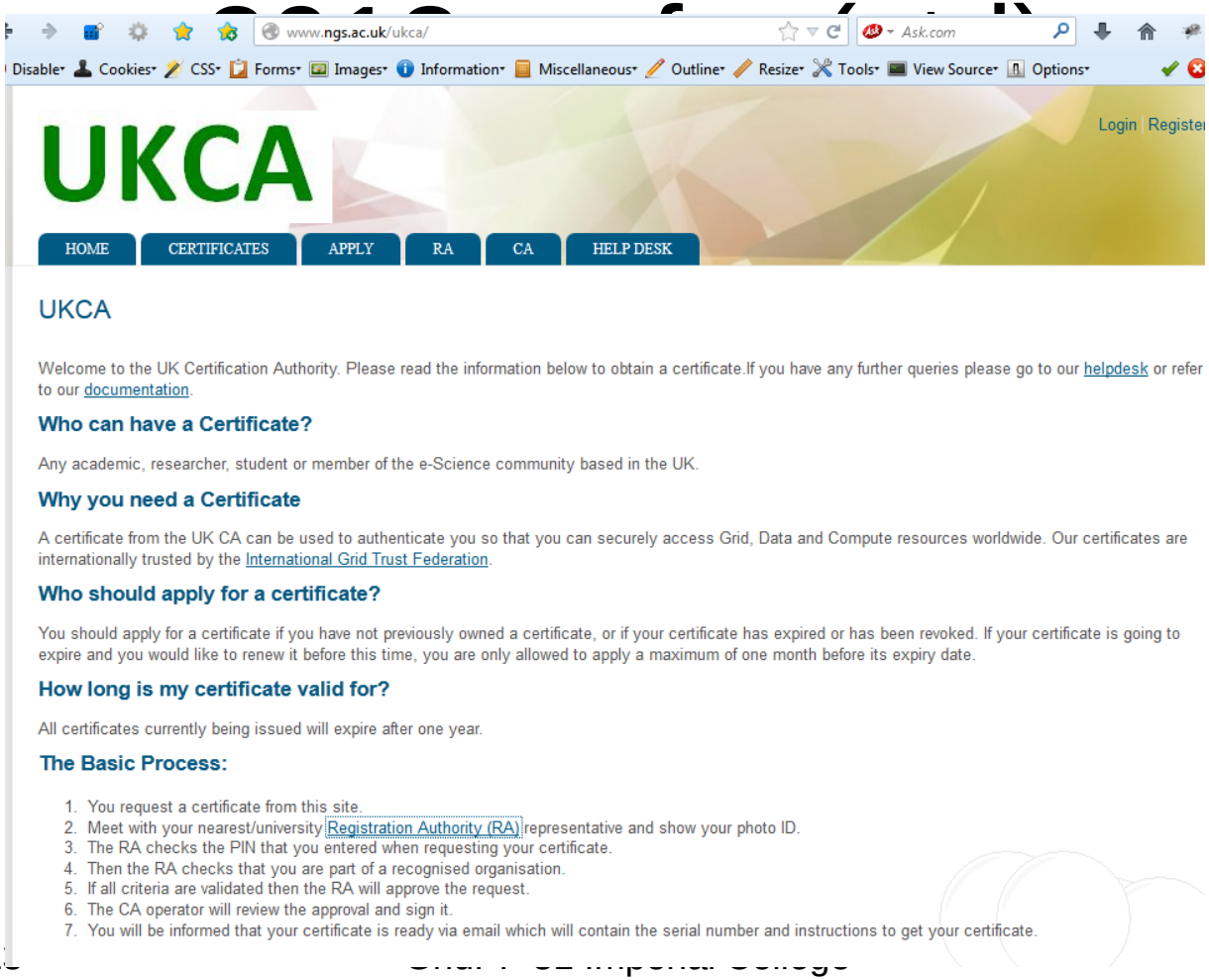
CertWizard Stuff

- Dave Meredith (code)
- Aims to replace browsers
  - Browsers are fickle in their X.509 support
  - Latest HTML5 might help, eventually
  - Needs Java. Macs not good at Java?
- Implementing bulk requests, RA ops

2013 so far

- Retired the old (2007) CA Certificate
  - Surprisingly complicated process…
- Perl scripts to CW
  - update by Robert Frank - full release soon
  - Imperial (Adam)
- Shib-2 compatible release of SARoNGS

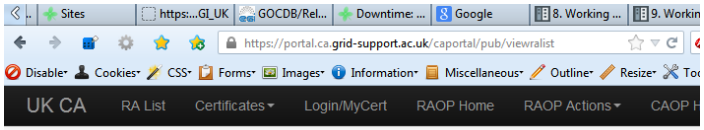
- New CA website: http://www.ngs.ac.uk/ukca



Science & Technology Facilities Council

2013 so far (ctd)

- New CA Portal with new RA interface, currently in use by many of our RAs



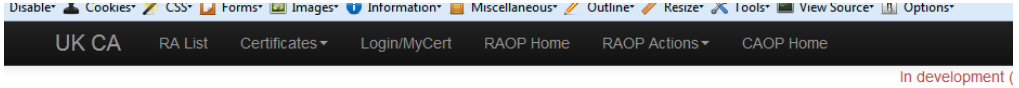
RA List (82)

RAs for your institution are listed below

RA List last refreshed: (Tue Sep 24 16:21:09 BST 2013)

Click links to see local RA Operators/contacts

#	L (Location)	OU (Org Unit)
1	Aberdeen	DIT
2	Aberystwyth	ComputerScience
3	Aberystwyth	IBERS
4	AstonUniversity	ISA
5	Bath	Chemistry
6	Bath	BUCS
7	BBSRC	BITS
8	BBSRC	IGER
9	BBSRC	NBI
10	BBSRC	Roslin
11	Bangor	SOI
12	Birmingham	ParticlePhysics



Search Signing Requests (CSRs)

Search Submitted/Refreshed OK

_ matches any single char
% matches a string

For RA all

Type NEW_or_RENEW

Common Name Like (CN) A Name

Distinguished Name Like (DN) CN=some body,L=DL,OU=CLRC,O=eScience,C

Data Like (shown if own ROLE_CAOP) CWIZPIN

Email Address Like someone@world.com

Email Address is Null (if checked, this will override email search string above)

Serial (if given, all other search criteria are ignored) 1234

Results per page: 20 Search

CSR Results (total = 171 , Tue Sep 24 16:25:06 BST 2013)

#	Type	Serial	Submitted On	Email	CN	DN
1	NEW	4765472	08-Nov-2009	a.giannakoudis@cranfield.ac.uk	garyfallos giannakoudis	DN
2	NEW	4769568	10-Nov-2009	ol8@leicester.ac.uk	owen lancaster	DN
3	RENEW	4778528	16-Nov-2009	pc229@kent.ac.uk	pieremanuele canepa	DN
4	NEW	4800032	24-Nov-2009	ja176@le.ac.uk	jawad ashraf	DN
5	NEW	4816160	03-Dec-2009	zhi.shang@stfc.ac.uk	zhi shang	DN

https://portal.ca.grid-support.ac.uk/caportal

2013/14 TODO

- Update client tools for SHA-2 (jglobus2)
  - MyProxyUploader part of CertWizard
  - GSI-SSHTERM
- Bulk requests (perl CLI script / CA REST server)
- Sign all certificates (user and host) with SHA2 from 1 Dec
- New CA Portal updates: certificate requests and renewals from browser

Roadmap Stuff

- Finalise “new” policy (unified)
- Multi-LoA: IOTA profile (< Classic) for SARoNGS and InCommon
- SHA2
- Moonshot integration (pos via MyProxy)
  - Initially non-prod
- Redo DR/BC, cheaper

Roadmap Stuff – LoA

- Federated identities and other ext'l
- Background is JSPG portal policy
- Federation policies and VO agreements "strengthen" user's credential
  - Towards a "cloud" login (on-demand)

Roadmap Stuff (potential)

- Key management service (a la MyProxy)
- Online signing?
- Moonshot: production service (expected)
  - More credential-with-LoA+AuZ than X.509+VOMS
  - Offer X.509 via conversion
  - Vision: may not need User CA
  - And at least not RAs, and paperwork
- Still need to support host certs (gateway?)

Roadmap Stuff (potential)

- Renewal of recently expired certificates
  - Protocol goes to great lengths to allow this
- If intermediate CA certs need SHA2:
  - Re-sign intermediate CA certificates (2A and 2B) – same DNs, same keys, different serials
  - No changes to EE certs
  - No change to Root cert