Grid-Ireland CA Update

David O’Callaghan

May 2009, Zürich

Grid-Ireland CA

Update Part A

David O'Callaghan — 31st May 2007 — Istanbul

CA Upgrade

From the minutes:

"Soon to upgrade to new OpenCA software"
— Brussels, Sept 2004

"Plans to upgrade CA software"
— Abingdon, Jan 2007

This summer we will really do it!

Part B

Grid-Ireland CA Update4

David O'Callaghan

May 2009, Zürich

e-INIS

The Irish National e-Infrastructure

European Grid Initiative

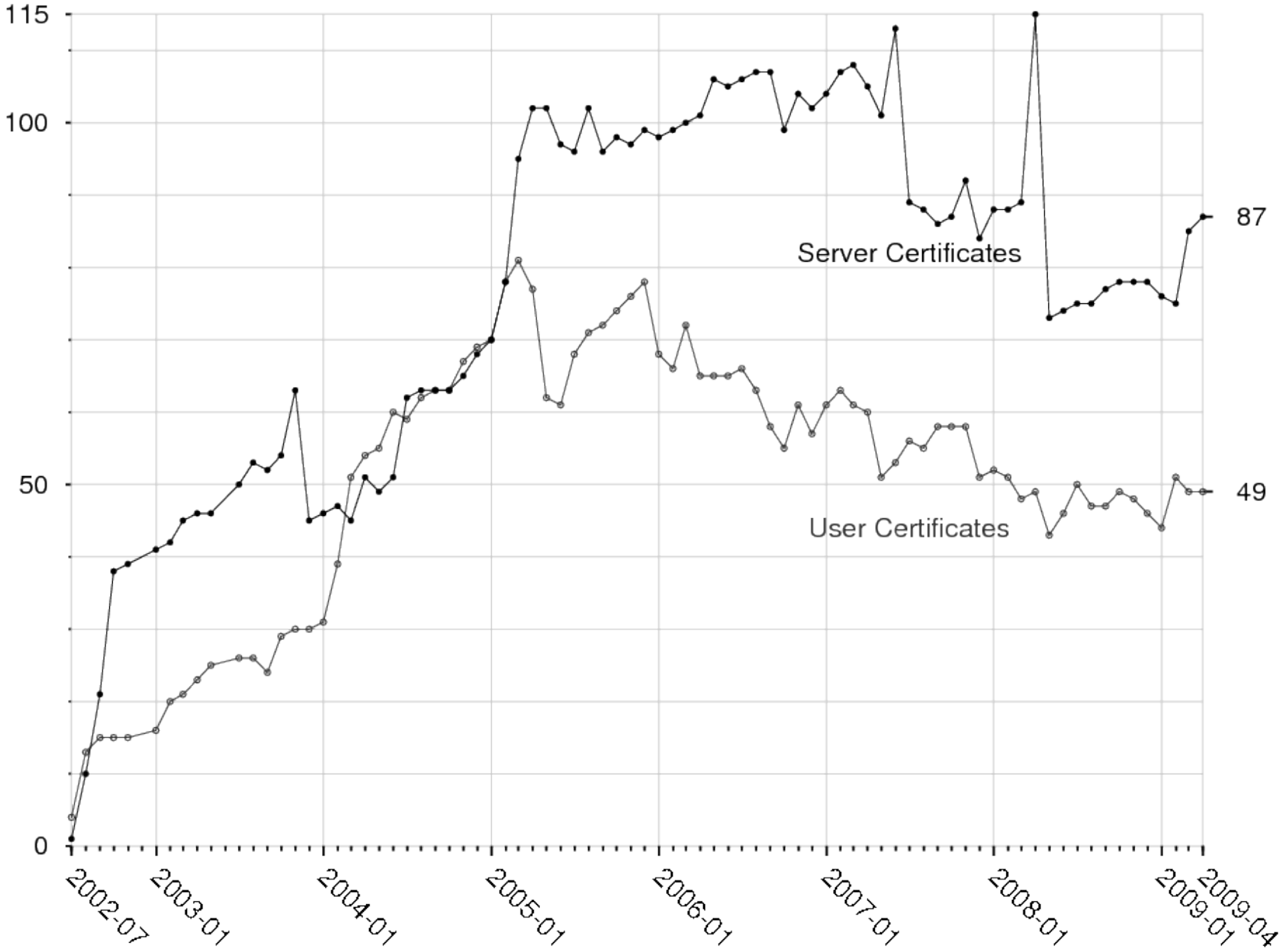
At the end of April 2009

- 881 certificates have been issued
- 136 are valid
- 606 have expired
- 139 were revoked

Of 136 valid certificates

87 are for servers

49 are for people


115
100
50
0
Server Certificates
87
User Certificates
49
2002-07
2003-01
2004-01
2005-01
2006-01
2007-01
2008-01
2009-01
2009-04

Self-Audit Results

17 “must change” items (*D*)

7 major change recommendations (*C*)

41 minor change recommendations (*B*)

49 good items (*A*)

Must Change

CP/CPS did not specify

- Message digest ✓
- Lifetime of certificates ✓
- RFC ~~3280~~ 5280 compliance ✓
- Subject DN linked to single end-entity ✓
- CA archives requests and confirmations ✓
- how RA and CA should communicate ✗

Must Change

- Compromise & disaster recovery plan
  - Not documented ✗
- Certificates & CRL profiles
  - *policyIdentifier* not in certificates ✓
  - MD5 used in CRLs ✓
- Entity identification
  - Host ownership verified by personal RA knowledge only ✗

Major Changes

- CP/CPS does not specify
  - procedure for changes to document ✗
  - how changes to CA key data are managed ✗
- CP/CPS in RFC 2527 format
  - Change to RFC 3647 ✓
- Audits
  - CA does not carry out operational audits ✓

Physical Security

Hardware

Certificate Profile

- RFC 5280 + GFD 125
- Include certificate policy identifiers
- Key sizes
  - CA: 2048 bits (big enough?)
  - End-entities: min 1024 bits, default 2048 bits
- SHA-1 + RSA
  - Will support SHA-2 when supported/required
  - Should we issue a SHA-2 CA cert now?

Distinguished Names

DC=ie, DC=grid, O=*Grid-Ireland*,
CN=*Grid-Ireland Certification Authority (Test 2009)*

DC=ie, DC=grid, O=*Grid-Ireland University*,
OU=*Users*, CN=*Aoife Greille*

DC=ie, DC=grid, O=*National University of Grid-Ireland*,
OU=*Hosts*, CN=*www.nugi.ie*

DC=ie, DC=grid, O=N*ational University of Grid-Ireland*,
OU=*Hosts*, CN=*host/gridgate.nugi.ie*

DC=ie, DC=grid, O=*Grid-Ireland University*,
OU=*Robots*, CN=Robot:*Grid Monitoring - Aoife Greille*

1.0.2

Done

+ Applied various patches from mailing list
+ Created a profile for Robots
+ Set Subject Alt. Name to hostname for Hosts
+ Configured cert-based authentication for ops
+ Configured list of RAs and organizations
+ Configured Levels Of Assurance
+ Improvements to UI (CSS, JavaScript)

Outstanding Issues

+ Random 64-bit serial numbers
+ Tie each RA Operator to their organization
+ Enable revocation requests
+ Implement sanity checks of certs + requests
+ New CRL URL

Outstanding Issues

- Robots only on hardware tokens?
- Configure UI to clearly seperate requests for Users, Robots and Hosts.
- Configure certificate authentication for Robots and Hosts requests

- Server certificate request only via OpenSSL

Timeline

Summer of code (and policy) work

By September 2009 (Berlin)

- New system and policy ready
- Apply for (re-)accreditation or audit

By January 2010 (Dublin)

- New CA in production use

checkcerts.pl

- Updated Crypt::OpenSSL::X509 is on **github**
  - http://github.com/dsully/perl-crypt-openssl-x509
  - Should make it into future release to distros
- No real progress on GFD-125 test suites
  - Proposed it as a job for a summer student...