

# Grid-Ireland CA Self-Audit

David O'Callaghan

September 2010, Zagreb



# Grid-Ireland CA

## *Update Part A*

David O'Callaghan — 31<sup>st</sup> 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!

David O’Callaghan — 31<sup>st</sup> May 2007 — Istanbul

*Part B*

# Grid-Ireland CA Update /

David O'Callaghan

May 2009, Zürich

# 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

# Grid-Ireland CA Self-Audit

David O'Callaghan

September 2010, Zagreb



# e-INIS

The Irish National e-Infrastructure

**Grid-Ireland**



# The Plan

EduGate

+

TCS e-Science CA

=

Happy Grid-Ireland Users



# The Reality

EduGate Pilot

-

Unwilling Institutions

(+ TCS e-Science CA)

=

Less happy Grid-Ireland Users

# New Plans

**Get current Grid-Ireland CA properly compliant**

as part of self-audit review process/time-scale  
without major software or document changes  
(no improvement in UX for RAs or users...)

**Plan for next generation of Grid-Ireland AAI**

Tentatively,

Develop experience with national federation

Fed-based SLCS CA for national users

Possible later accreditation

**Overhauled “federally-assisted” Grid-Ireland CA**

for “international” users, hosts, robots, etc.

# Self-Audit Results

2	D	Must change
12	C	Major changes
20	B	Minor changes
33	A	Good
3	X	Could not evaluate



# Self-Audit Results 2007

17 “must change” items (*D*)

7 major change recommendations (*C*)

41 minor change recommendations (*B*)

49 good items (*A*)

# Self-Audit

Used to GFD.169 v1.0 from April 19, 2010

Many items are complex / multi-value

Some errors / unclear terminology

“An RA must validate the association of the CSR.”

and Auditing Spreadsheet for Classic AP

Section numbers for GFD.169 don't all correspond

Used two copies to capture where practice differs  
from policy



# Must Change

Certificates & CRL profiles

Annual Internal Operational Audits

# Major Changes

CRL to RFC 5280 requirements

*policyIdentifier* not in certificates

MD5 used in CRLs

Entity identification

Host ownership verified by  
personal RA knowledge

# Major Changes

CP/CPS does not specify

- procedure for changes to document

- how changes to CA key data are managed

- physical set-up

CP/CPS in RFC 2527 format

Records / logs

- Difficult to make available for auditing

# Major Changes

## Publication

Some items were missing or difficult to find on web site

Compromise & disaster recovery plan

Privacy & Confidentiality

Not documented

# Hardware







# Physical Security