

**7th TAGPMA
Face-to-Face
Meeting**



TAGPMA Updates
Doug Olson,
(for Vinod Rebello, chair)

APGridPMA Mtg, Taipei
April 8, 2008

-
- 7th Face-to-Face TAGPMA meeting last week
 - CAs Status
 - Charter Updated (V2.4)
 - SLCS Profile updated (V2.1)
 - DOEGrids CA Audit

7th TAGPMA F2F Meeting

- April 2-4, 2008, Oakland, CA, USA
- <http://indico.na-df.rnp.br/indico/conferenceDisplay.py?confId=37>
- CA updates for
 - TACC, NERSC, ULAGrid, NCSA, Venezuela
- HSM vendor presentations
- Some TAGPMA process discussions
- DOEGrids Audit update (later slides)
- SLCS updates (later slide)
- 8th TAGPMA F2F in Merida, Venezuela
 - 21st to 23rd July 2008
- 9th TAGPMA F2F in La Plata Argentina
 - around November/December 2008

- Accredited
 - Argentina, Brazil, Canarie, Chile, DOEGrids, LA Catch All, Mexica, NCSA (SLCS, MICS)
- In Process
 - Fermilab KCA, TACC (Classic, MICS), Venezuela

-
- Version 2.4 of the Charter has been approved
 - Better reflection of how the TAGPMA operates
 - 2 year Membership: Letter of introduction/renewal
 - Ties the representative (POC) to the soliciting Institution
 - Affirmed commitment by Institution to TAGPMA participation (F2F meetings, document development and reviewing)
 - Inactivity implies resignation

SLCS Profile Status

- SLCS Profile (Original Version 1.1, 15/11/2005)
- Proposed a two stage revision
 - Language update has already been **approved** (Version 2.0)
 - Lowered HSM operating mode to FIPS Level 2 (V2.0.1)
 - Want role-based operators
 - Removed export of plaintext keys from HSM (V2.1)
 - Policy update
 - Require CRLs for ALL SLCS CAs, with 1 day response time
 - SLCS with short enough certificates need only publish and empty CRL

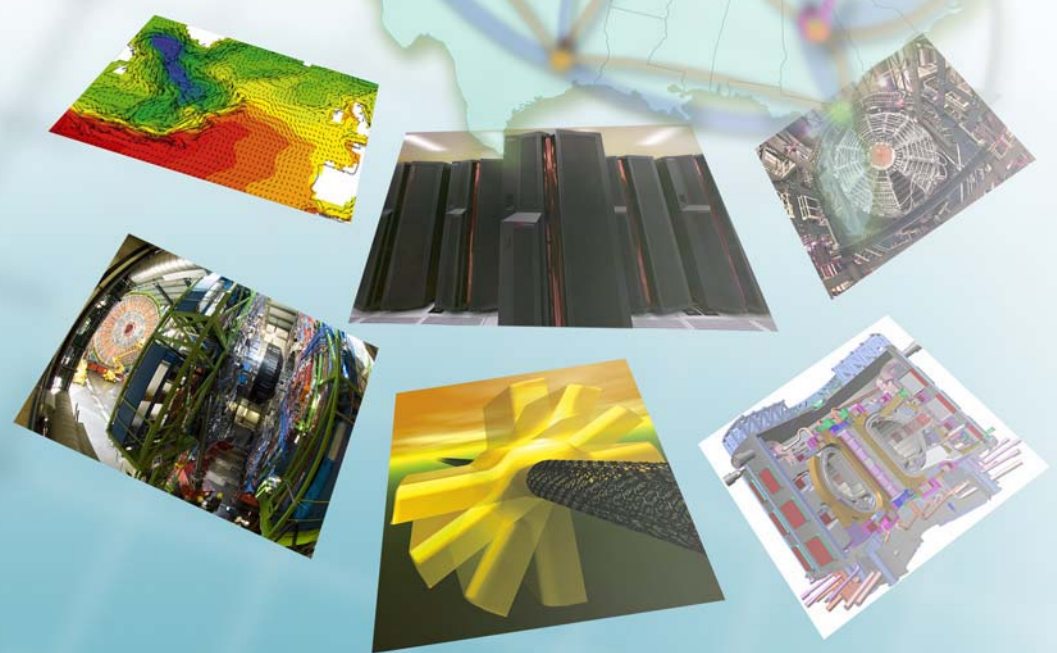


Excerpt from DOE Grids Audit Report

Doug Olson,
for Michael Helm
and the ESnet ATF team

See original version in
EUGridPMA Jan 08
And TAGPMA Summary
Apr 08

APGridPMA - April 2008

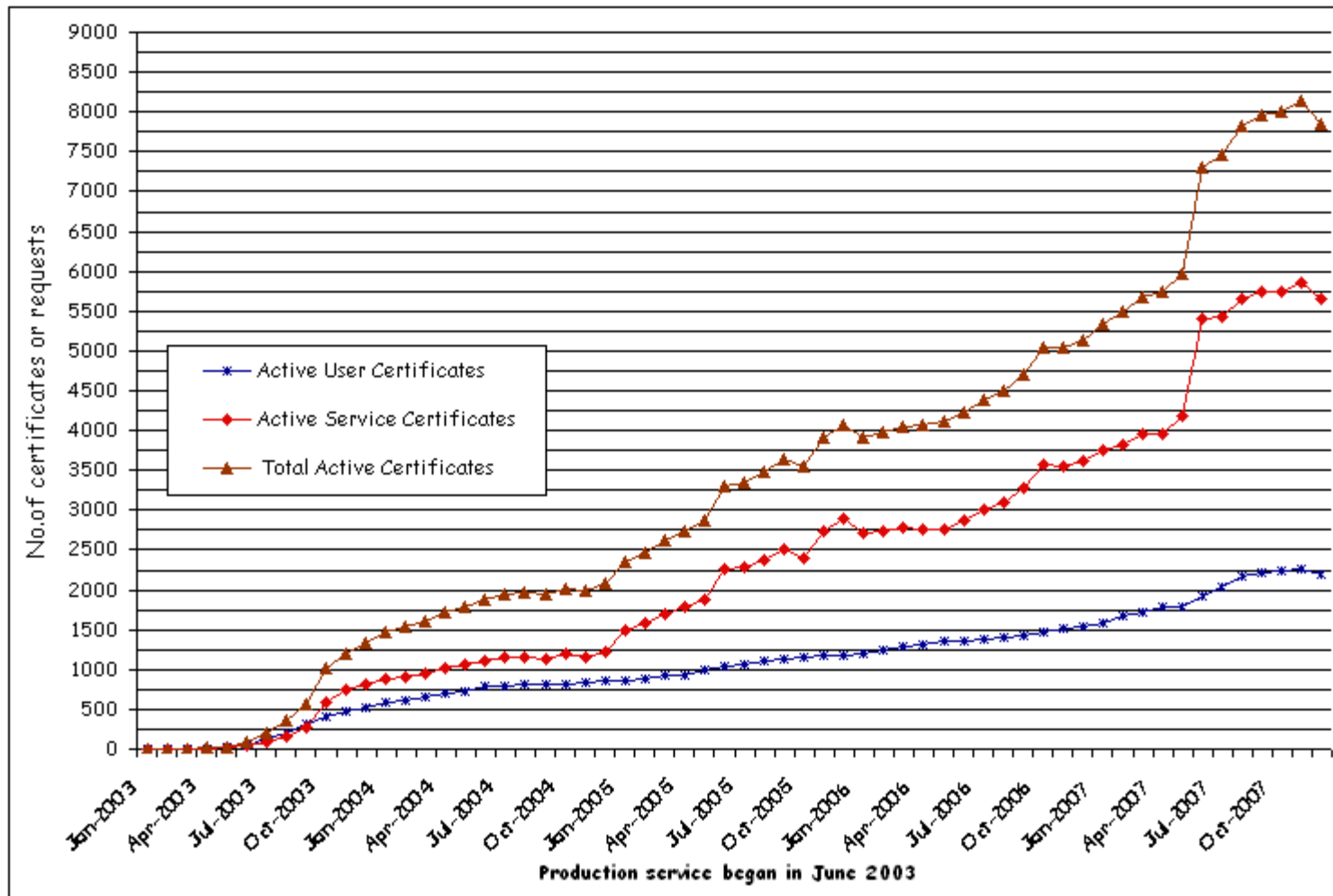


Networking for the Future of Science



www.doeagrids.org

Serves Open Science Grid and U.S. science community



DOEGrids CA Audits

- We did an extensive internal audit, which functioned partly as a tutorial
 - The intent was preparation for ...
- We did a one-day “community” audit
 - “Community” = “inside DOEGrids”, with one exception
- We tried to look both broadly, and deeply, at our DOEGrids service

DOEGrids Audit Day

11 Dec 2008

- Introduction
 - Charge
 - DOEGrids Intro
 - DOEGrids CA and HSM
 - DOEGrids System and Security
 - DOEGrids RA and certification process
 - ESnet 800-53 process

DOEGrids Audit Day (2)

- Audit
 - IGTF Audit framework (partial)
 - “Operational Review”
 - NIST 800-53
 - DOEGrids PMA
 - Inspection
 - Audit review
- 12 Dec (Wed)
 - Draft comments due

Who Are the Auditors? (1)

“Internal” Audit

- Dan Peterson (ESnet)
 - ESnet security officer; 800-53 coordination
- Michael Helm
 - ATF team lead
- Dhivakaran Muruganantham
- Doug Olson
- John Webster
 - ATF and ESnet staff
 - In some cases had limited time

Who Are the Auditors? (2)

Community

- Robert Cowles (SLAC – DOEGrids PMA chair)
 - Numerous community roles; active in DOEGrids since the beginning
- Dan Peterson (ESnet)
 - ESnet security officer; 800-53 coordination
- Scott Rea (Dartmouth/HEBCA) (observer)
 - TAGPMA; cross-signing and US Higher Ed
- Mary Thompson (LBL – retired)
 - DOEGrids “founder”; extensive Grid experience
- John Volmer (ANL – DOEGrids RA)
 - Policy experience, FBCA liaison

Audit Process

Oct 2007 – Dec 2007

- Discussion about foundation and scope (Sep-Oct 2007)
- Support Doug Olson's auditing efforts in PMA and OSG RA (Oct 2007)
- 3 – day (+) internal audit (Nov 2007)
 - 2 days focused on NIST 800-53
 - 1 day focused on OGF Audit Framework
- Create a “Reviews” site as on-going ESnet effort
- Organize (semi-)external auditors
- Conduct “Audit Day” (11 Dec 2007)
- Collect reports from auditors
- Write report
- Come to Amsterdam
- ?
- Profit!

Internal Audit

3 Days in November

- 2 Days devoted to NIST 800-53
- 1 Day devoted to OGF Audit Framework

Intentions:

- Tutor team members on components
- Do a self-audit where possible – anticipate issues, identify obvious problems, particularly those an outsider might not see
- Provide input and structure for “community” auditors
 - Primarily for 800-53 because of size & scope

NIST 800-53

Internal Audit

- Dan Peterson tutors Mike Helm (1st) and then Dhiva and other team members on
 - The structure of 800-53
 - How LBL (our institution) managed its process, and composed its responses
 - Where ESnet and the PKI project fit into the LBL product
- Mapped LBL product onto R Cowles framework (see previous PMA minutes :^)

DOEGrids Audit Day

11 Dec 2007

- “Community” audit
- Ambitious agenda – only got thru OGF Framework and some PMA
- Functioned more like a program review – our community is more attuned to this method of work
 - Half day of presentations and discussions, much like takes place at IGTF PMA
 - Half day of
 - Review of “internal” audit material
 - Discussion of points and issues in framework
 - Not even enough time to do framework step by step ; we covered points of interest
 - “Site” visits where appropriate

DOEGrids Audit Day (2)

Format

- 2 Remote attendees (1 video, 1 audio only)
 - John Volmer (ANL)
 - Scott Rea (Dartmouth)
 - Obviously were unable to complete site inspection components
- 2 Guests (on site)
 - Robert Cowles – SLAC
 - Mary Thompson – LBL
- ESnet Security officer (on site)
 - Dan Peterson

DOEGrids Internal Audit

Let's go back to the "internal audit" the ATF team & Dan Peterson conducted in Nov 2007 – Day #3 – the OGF Audit Framework (NB: **1.0-b4** 17 Oct 07)

Mike Helm recorded this audit, and it was used as the basis for the Audit Day community audit

DOEGrids Internal Audit (2)

Significant deviations: 5a (RFC 3647), 15a & seq (CA transition), 45a (Control of renewal), 47 (This resulted in a major recollection of log files), 60a (ID verification), 68a-b (policy on record maintenance)

Audit error: 4a (recorded as broken, but actually working)

Minor: 21, 26a, 35a, 36, 40a, 41 (Grid Cert Profile), 43a, 44a, 54, 57, 58a (we probably exceed existing requirements, but not our own), 63a, 64a (policy), 66a,

Problems with audit framework: 5a (3647), 8b (FIPS 140 level 3?), 11a-b (not suff for HSM), 31a (CRL profile), 34a, 37a, 45b (dropped “not”?), 50a (What is the intent of this?)

Community Auditors' Reports

- We haven't completed processing this material
- A report should have been completed by now, but ...
- [For the summaries – see the EUGridPMA version of this talk]

Attempt at Summary

- Documentation (eg CPS) errors should be fixed
- People wish we had a different CA & PKI than the one we have (“Show me the money!”)
- The DOEGrids PMA needs revitalization
- There are other issues that people want to talk about/audit (the framework is too rigid?)
- The documentation needs to get right with RFC 3647

Amsterdam Discussion

- Agreement to “accept” the American-style time-shifted identity verification
 - Documentation and formalization needed
- RFC 2527 format is not a significant problem
 - Many older CAs have this format, not likely to change
- Renewal/notification and certificate auditing needs work
- The numerous documentation errors / omissions need to be addressed

DOEGrids Operations Status

- Final report STILL not done (target: May 1)
 - Owed to ESnet management
 - Owed to DOE program manager
 - Owed to ... everybody
 - Lost principal writer
 - Lost Technical Writer
- We will address the minor errors in the course of the year
- We will “upgrade” to Grid CP now that it is published
- We will develop a 3/5 year renewal process
 - Fixing our internal notification system to RAs will be a big step in this direction, but not complete
- We will upgrade the CPS document to RFC 3647
 - Loss of tech writer makes it less clear which will happen first
 - Documentation and formalization needed
- We will focus on NIST SP 800-53 as the framework to support this work
- We will try to adopt a continuous, low level audit strategy
 - Difficult to force on collaborators
- Probably have to provide a hardware token client profile