PRAGMA-UCSD CA

Mason Katz - UCSD
APGrid PMA Meeting
Beijing
29.11.2005
Overview of San Diego Supercomputer Center

- Founded in 1985
  - Non-military access to supercomputers
- Over 400 employees
- Mission: Innovate, develop, and deploy technology to advance science
- Recognized as an international leader in:
  - Data Management
  - High Performance Computing
  - Grid and Cluster Computing
  - Networking
  - Visualization
- Primarily funded by NSF
- SDSC is part of TAG PMA
PRAGMA Grid

- Approximately 20 institutions.
- Not Production level CA trust
  - Simple CA is widely used
  - Some sites have no CA
  - Cross-issuing of certificates is common
- SDSC CA system is not usable for us
  - Policy restrictions
  - Manageability
  - DN naming issues (not de facto standard format)
  - Strictly for NSF Accounted users
  - We need to issue certificates for foreign collaborators (both host and user)
- PRAGMA needs a Grid wide CA for sites without their own production level systems (catch all system)
Bottom-up Grid

- **Bottom-up Grid**
  - Globus 2.4 (soon GT4) is the only requirement
  - Too many institutions to mandate complete software stack (very different from grid like TeraGrid)

- **Applications create their own sub-grids**
  - Each with unique application requirements
  - Application drivers enforce these requirements
  - Common application requirement may become common middleware requirements (e.g. ninf-g, gfarm)

- **CA Policy**
  - None, we trust everyone within PRAGMA (even the old Globus CA)
  - Right method to get started
  - Wrong method to continue
Grid Account Management Architecture (GAMA)

- GSI credential management solution.
- For web/grid portals and web service clients.
- Automatically install and configure components using Rocks.
  - CA System (CACL)
  - MyProxy (Credential Repository)
  - Globus (GSI libraries)
  - Axis web services wrappers
  - Tomcat containers hosting Axis services.
GAMA Roll and Rocks

- Rocks is a leading open source clustering distribution
  - Top-to-bottom software stack
- Rolls are optional components
  - Grid (GT4)
  - Gama (CA)
  - Dozens of others
- Goal is to build turnkey systems
  - Insert CDs
  - Answer a few questions
  - Done
  - Systems can be
    - Computational Clusters
    - Visualization Clusters
    - Web Servers
    - CA Systems (GAMA)

- www.rocksclusters.org
GAMA and NAREGI CA

- GAMA has made the CA system an optional component
  - CACL (for SDSC)
  - Simple CA
  - NAREGI CA
- Required changes to both GAMA and NAREGI CA
- Software release is planned for January 2006
CA Plans

◆ Usage
  ✐ All UCSD related PRAGMA projects
    • PRAGMA
    • OptIPuter
    • NBCR
  ✐ Any institution within PRAGMA without a regional PMA accredited CA system

◆ Timeline
  ✐ 01-06 GAMA / NAREGI CA integration complete
  ✐ 02-06 CA deployment
  ✐ 03-06 PRAGMA meeting (Australia) to discuss CA usage policies
  ✐ 04-06 Procedures/Policy documented and application for APGrid PMA accreditation
  ✐ 12-06 All PRAGMA user/host certificates to be issued by an accredited regional PMA. Removal of all non-accredited CA from PRAGMA
Issues / Questions

- System to be online
  - For MyProxy access
  - For requesting certificates
- Security
  - Nothing but GAMA access allowed
  - No user logins
  - Root access restricted using RSA dongles
- Physical machine access
  - How to restrict?
  - NAREGI system is in a locked cage
- User identity confirmation
  - Only issue certificates at PRAGMA (or other face-to-face) meetings?
  - Can a existing user verify another unknown user (RAOs)
- I’m here to learn from you.
Credits

- **GAMA Developers**
  - Sandeep Chandra (SDSC)
  - Kurt Mueller (SDSC)

- **NAREGI CA Developers**
  - Shinichi Mineo (NEC)
  - Takuto Okuno (NEC)

- **PRAGMA**
  - Cindy Zheng (SDSC)
  - Bill Link - CACL support (SDSC)