Open Science Grid

Berkeley Lab

Identity Vetting Practices in U.S. for Scientific Computing + OSG RA details

Doug Olson

LBNL, OSG RA, …

EUGridPMA Meeting, Amsterdam, 14 January 2008
Updated for TAGPMA, 4 April 2008 - Oakland

Contents

- General Overview
- Examples
  - –NERSC
  - –BNL/RACF
  - –FNAL
- Applicability for Open Science Grid
- Discussion of id vetting process

Overview

- Why this talk
  - I think there are some differences in implicit assumptions about between the U.S. and European participants in the IGTF that sometimes lead to surprises, misunderstandings (even conflicts?).
  - The views expressed are my own and are not any official view of DOEGrids, OSG, USA but do help explain things about how the OSG RA operates.
- The scope is unclassified “open” science projects, primarily particle and nuclear physics.
  - No important secrets are being protected
  - No hazards to people or property are being secured
  - The primary goal of the infrastructure is to facilitate efficient use of resources for the science programs
    - So the cost of an incident is measured primarily by the Denial of Service affect

Overview (cont.)

- ID in the U.S.
  - Identity, like most matters of birth, life, death are documented by authority of the States and not the Federal government
    - Documentation varies from state to state, some states still don't have photo ID
    - Little or no inter-state comparison of identity records
    - Driver's license is the most common form of ID, and is historically rather easily forged so young people can buy alcohol
    - Only small percentage of US citizens have a passport
  - A federal law passed in 2005 is supposed to result in a national identity card system under the label REAL ID.
    - Sets standards for state issued driver's license and DMV issued ID cards
    - Will integrate state ID databases so ID verification can be checked across state boundaries
    - Dept. Homeland Security just released specifications for the program
      - All newly issued ID should comply by 2011
      - Previously issued ID should comply by 2017
    - Still plenty of time for complaints, changes, delays

Overview (more cont.)

- General considerations of ID vetting for access to scientific facilities
  - On-site access for employees and long-term guests
    - Typically involved face-to-face visit to badge office with photo ID, photo taken and paperwork signed by user and some authority
  - Off-site access for guests
    - Typically user provides contact info and justification via unauthenticated web form
    - May include printing, signing, FAXing a policy form
    - Requests are approved by some previously known authority, often via plain insecure email
- Typical Resource Policies
  - Privacy – normally no privacy is assured
  - Integrity – no guarantees for integrity of data or software
  - Availability – no guarantee of resource availability to user
  - Obligations – users are expected to comply with the normal security features

Overview (yet more cont.)

- Difficulties with Face to Face

  - Distance, $$$ for extensive F2F network
  - Lack of standard ID
    - Who can tell if ID is forged?

U.S. and Europe from 4000 km altitude in Google Earth

Overview (still yet more cont.)

- Sponsorship/membership model for ID vetting
  - Drivers and motivation
    - Supported for U.S. science
    - U.S. science is funded nationally, not by state
  - Registration effort is provided by science projects
  - Identity Federations (like InCommon) are a long way from providing ID for most scientists
  - ID vetting is coupled to membership/participation in a science project.
    - Some ID vetting is performed when joining a project
    - Some lifecycle membership management exists so a collaboration knows when members leave
  - Results is a hierarchical model of project PI and local PIs who are the authorities to define membership
  - The consequence for PKI is that initial ID vetting does not need to be stronger than happens already for VO membership, but renewal/re-issuance of DN is more important

Example - NERSC

- First time PI
  - –Fill out https web form with contact info, nationality
  - –Sign & FAX AUP to NERSC
  - –NIM account created, pw received via phone call
- All PI's
  - –Write ERCAP proposal in NIM using https forms
  - –Allocation is granted by NERSC/DOE
  - –PI can add additional users to NIM
    - Users sign & FAX AUP to NERSC
    - Users call NERSC for password
  - –PI & users can login to machines and use resources up to the allocation

Example - BNL/RACF

- New User
  - –Sign & FAX AUP to BNL
  - –Register as a BNL Guest
    - https registration form, state experiment affiliation
    - Local sponsor endorses guest
  - –Take cyber security training (web-based)
  - –Request login account on https form, include guest ID number, and a previously known sponsor
  - –Call for password?

Example - FNAL

- Offsite visitor computer user
  - –Read and agree to policies
  - –Fill out https form (incl. client cert)
    - State affiliation to group/division, etc. at FNAL
      - Someone at FNAL endorses request
    - https form provides initial password
  - –Email sent to user when account is ready

Applicability to OSG

- DOEGrids PKI is a collaborative effort to provide X509 ID tokens for science with direct funding for CA operations and leveraging RA effort from the science community.
- OSG registration process is modeled on user facility remote access process
- Registration Agents have a scope of one or more VOs and zero or one user facilities
- Agents maintain lists of Sponsors who can provide attestation for subscriber requests
- The OSG process has many similarities to the MICS profile

At/Following Amsterdam Meeting

- Agreed that "PI/distributed/TTP/delegated/sponsorship…" process should be described as one of the valid procedures.
- So, how to describe it?
- Look at http://tagpma.es.net/wiki/bin/view/Sandbox/NSF
- Discussion

- → Trusted agent
  - RA documents id vetting by trusted agent (ta = sponsor)

Summary Statement

- A person (a human end-entity (EE)) requests identity certification. An attestation by a trusted agent (TA) about the identity of this person to a *registration authority* (RA) is sufficient evidence to permit the RA to accept the certification request.
  - RA should document how the TA communicated the ID vetting attestation to the RA
  - How TA is identified
  - show integrity of id vetting to CSR submission
  - RA responsible for attestation