Proposal for Namespace Assignment Policy in the IGTF

David Groep, Apr 20nd, 2009

The IGTF Charter

- Name uniqueness throughout the IGTF is anchored in the Charter

- Current Charter assigns a namespace to an Authority, implying that the basic managed entity is a one single CA

  "On accreditation, a specific subject name space or set of subject name spaces is allocated to each authority. This name space must not overlap with any existing name space already assigned to an existing authority for any AP, assigned by any of the regional PMAs within the International Grid Trust Federation."

Is this a problem or an asset?

- The answer is probably: both
- Always need to preserve binding to a single entity (changing that is obviously *not* to be changed)
- Pros of having it assigned to a single CA
  - A DN in the logs would maps directly to a single CA.
  - If a DN is associated with abuse, otherwise multiple certificates may need to be revoked across multiple CAs.
  - If one of the CAs is compromised the suspicion is limited to that one CA.
  - Can easily differentiate between Cas based on just names (e.g. in simplified VOMS, or when OIDs are not checked but LoA matters)

Pro for a change

- Pros of assigning namespaces to PMA members
  - Simpler for users. They have a single DN from the Classic/MICS/SLCS. One entry in VOMS and grid-mapfiles rather than multiple.
  - Allows users to "upgrade" from SLCS to MICS/Classic (for example), depending on their authN factors.
  - Allows users to "downgrade" from MICS/Classic to SLCS (for example, if they're away from their computer and need a short-lived certificate).
  - Simpler for system administrators.
  - Allows CA roll-overs (already used here!)

Assigning to PMA members is Good

- Propose to change text in the Federation Doc to:

3.1 Management and communication of identifiers

On accreditation, a specific subject name space or set of subject name spaces is allocated to each PMA member for its accredited authorities. This name space must not overlap with any existing name space already assigned to an existing PMA member for any AP, assigned by any of the regional PMAs within the International Grid Trust Federation.
The assignment of a name space to a PMA member will be according to current best practices, and the name space shall have a reasonable relationship to the scope of the PMA member. Any proposal for name space assignment shall be circulated amongst all PMAs within the International Grid Trust Federation, and the assignment will not be effective unless positive confirmation of uniqueness has been received from all PMA chairs.
Each PMA will distribute widely the list of assigned subject name spaces.

Deleted: authority.

Deleted: authority

Deleted: an authority

Deleted: authority.

Deleted: permanent

Time line

- EUGridPMA proposes this change and approved it in their January 2009 meeting
  (minutes and proposal circulated to the IGTF)
- Presenting now to the IGTF
- Discussion proposed at APGridPMA and TAGPMA F2F meetings (April 2009)
- On acceptance: Agree in May at the IGTF meeting in Chapel Hill


eu
gridpma