Setting the scene: SRM

• SRM
  – Protocol for controlling storage

• Delegation
  – Allows an SRM server to act “on behalf of” end-user.
  – Creating X.509 certificate & private key on server, signed by end-user.

• GSI
  – V. similar to SSLv3 but incompatible.
  – Allows clients to trigger delegation
Why delegate?

- Protocol-independent 3rd-party copy
  srmCopy

- Reserving network bandwidth
  srmPrepareTo(Get|Put), srm(Get|Put)Done, srmCopy

- X.509-aware tertiary storage
  SrmBringOnline, srmPrepareTo(Get|Put), srm(Get|Put)Done, srmCopy

- Federated SRM
  Everything except srmPing.
Why switch from GSI to SSL?

• GSI is **not a standard** (SSLv3 is)
• Coupling delegation with transport negotiation is **inflexible**.
• It's **not widely used** outside of Grid
• Only libraries are coming from a **single vendor**: Globus
• Hard to add advanced features; e.g., no hardware acceleration.
What to do about delegation?

- If delegation isn't needed then SSLv3 should work fine.
- When delegation is needed then client requires some extra functionality.
- Soln: a service that allows delegation. (NB. we're **not** talking about a single, per-site shared service; rather, each service has a common extra API)
# Delegation Services

<table>
<thead>
<tr>
<th>Name</th>
<th>Tech.</th>
<th>C / Native</th>
<th>Java / JVM</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Client</td>
<td>Server</td>
<td>Client</td>
</tr>
<tr>
<td>Globus Credential Delegation Service</td>
<td>SOAP</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>GridSite Delegation Service</td>
<td>SOAP</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Globus New Delegation Service</td>
<td>REST</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>IVOA Delegation Service</td>
<td>REST</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>
Introducing the winner

• GDS is a **de facto standard**.
  – Developed ~2005 by Andrew McNab for web management software.
  – Adopted by gLite, after going through a review process

• Current version is v2.0.0
  – In production (FTS, GridSite, ...)

• **Two** independently developed libraries (Java and C), both provide **client** and **server**.
GDS: an EMI standard

- Other services in EMI also need to delegate
  - EMI ES (execution service), FTS, ...
- Agreement to use GDS within EMI.
- Current API docs need tidying up:
  - Conflates documenting software with documenting the standard,
  - Leaves some things too vague.
- Some work underway in this area
Taking it further

• GDS is a “standard” only within EMI.
  – Not endorsed by any standards body.
• No obviously applicable standard
• Should we start an OGF WG?
  – Suggest writing up GDS as an experience report
Talked to David Chadwick

• Sadly, he couldn't make it today.
• I've tried to summaries his comments in the following two slides
  – He makes good points
  – To me, the questions/points seem very reasonable, but I don't completely agree with his “answers” :-}
Comments from D. Chadwick

- Delegation should be:
  - accountable, revokable, fine-grained, recursive/re-entrant

- He described an existing system:
  - Uses federated identity
  - Delegation uses a trusted 3rd party: an Attribute Authority (AA).
  - Result is an authz attribute:
    - Either a SAML attribute assertion
    - or X509 AC, signed by AA
Comments from D. Chadwick 2

• GDS isn't “delegation”, but “masquerading”
  – The 3\textsuperscript{rd} party doesn't know the identity of the delegatee.

• Masquerading may be implemented as special case of “real” Delegation.
Comments from D. Chadwick 3

- Doesn't wire-protocol already exist?
  - CMP (RFC 4210) or CMC (RFC 5273)
  - Somewhat “inverted” roles:
    - The delegator is CA, delegatee is EE,
  - Would need a “kick-off” message
    - Equivalent to a message from CA → EE, saying “you want to request a cert. now”
    - Believes such a message may exist, but it might not.
My thoughts ..

• Properties of delegation:
  – Accountability: not with GDS
  – Revokable: not with GDS (do we need it for short-lived credentials?)
  – Fine-grain: not with GDS
  – Recursive/re-entrant: yes.

• Believe CMP lacks features from GDS:
  – ability to associate certificate with an ID.
    • Might not be a problem: use Alt. Name ext.
  – session management.
My thoughts ..

• Fine-grain authz requires defn of operation semantics
  – User A delegates either
    • ability to do operation X to B: what does 'X' mean?
    • Or a role / attribute (equiv. What does the role mean? Already agreement with VOMS)

• GDS doesn't require trusted 3rd party.
My thoughts ..

• Attribute certificates?
  • A signs B's cert with an attribute stating B can do operation X (or role) on her behalf.

• Believe it's hard to allow revocation without trusted 3\textsuperscript{rd} party.
Possible way forward

• Form (research/working/..) group within OGF to look into delegation.

• Document the current status:
  – Provide a formal description of GDS as an experience document
  – David Chadwick says he can write an equivalent document for his system.

• Look to see if there's interest in establishing a common standard here.
Thank you!

EMI is partially funded by the European Commission under Grant Agreement RI-261611