Transition to DOEGrids CA

- Technical issues
- CA Support files distribution
- Testing
- Transition Model plan
- GSI handling of certificates
- Strategies for dealing with errors
Technical Issues

- Old CA will expire in Jan 2004 –
  - **NO RENEWAL**
- Name Space (domain components)
- More required fields (VO identification)
- Better support for renewals
  - IE
  - Password based for service – type certs
- Outstanding issues
  - Need to triage, perhaps?
CA Support files distribution

- EDG
- ALL COMPUTERS!
  - Clients: more important to update
  - Management/maintenance issues
- Possible future work
  - Installation solutions (GPT?)
Testing

- Bugs found in signing_policy files
- Change to root CA cert
  - SubjectAltName – email name
- Capitalization
  - Legacy GT
- **GSI error handling**
  - Looking for signatures
Transition Model Plan

- Update your clients
- Update your servers
- Then get your certs
- Agents: get new certs ASAP
- Recommend some in-house testing
- But let’s shut down new certs on DOESG by August
GSI Certificate handling (1)

- [http://www.globus.org/security/config.html](http://www.globus.org/security/config.html)
  - Not very well known?
- Search path for CA information
  - CA signing pk cert, signing_policy file
  - Uses opaque “hash” names
- Search path for EE certificates
- Directory search:
  - First directory wins, even if it’s useless
- EE certificate search:
  - First EE cert with correct name form wins….
GSI Certificate handling (2)

- Opaque error messages (see next slides)
- No signature
- Need alternative strategies
Some Cert – related error messages

- **No-1**
  - GRAM Job submission failed because authentication failed:
  - GSS Major Status: Authentication Failed
  - GSS Minor Status Error Chain:
  - init.c:499: globus_gss_assist_init_sec_context_async: Error during context initialization
  - init_sec_context.c:206: gss_init_sec_context: SSLv3 handshake problems
  - globus_i_gsi_gss_utils.c:866: globus_i_gsi_gss_handshake: Unable to verify remote side's credentials: Couldn't verify the remote certificate
  - OpenSSL Error: s3_pkt.c:1031: in library: SSL routines, function SSL3_READ_BYTES: sslv3 alert bad certificate (error code 7)
Some Cert – related error messages

- **No-2**
  - GRAM Job submission failed because the job manager failed to open stderr (error code 74)
  - [hangs]

- [A particularly nice one, since it doesn’t look like a certificate or authentication error]
Some Cert – related error messages

- **No-3**
  - GRAM Job submission failed because authentication failed:
  - GSS Major Status: Authentication Failed
  - GSS Minor Status Error Chain:
    - init.c:499: globus_gss_assist_init_sec_context_async: Error during context initialization
    - init_sec_context.c:189: gss_init_sec_context: Unable to verify remote side's credentials
    - globus_i_gsi_gss_utils.c:873: globus_i_gsi_gss_handshake: SSLv3 handshake problems: Couldn't do ssl handshake
    - OpenSSL Error: s3_clnt.c:836: in library: SSL routines, function SSL3_GET_SERVER_CERTIFICATE: certificate verify failed
    - globus_gsi_callback.c:351: globus_i_gsi_callback_handshake_callback: Could not verify credential
    - globus_gsi_callback.c:438: globus_i_gsi_callback_cred_verify: Could not verify credential: self signed certificate in certificate chain (error code 7)
Some Cert – related error messages

- **No-5**
  - GRAM Job submission failed because authentication failed:
  - GSS Major Status: Authentication Failed
  - GSS Minor Status Error Chain:

  - init.c:499: globus_gss_assist_init_sec_context_async: Error during context initialization
  - init_sec_context.c:189: gss_init_sec_context: Unable to verify remote side's credentials
  - globus_i_gsi_gss_utils.c:873: globus_i_gsi_gss_handshake: SSLv3 handshake problems: Couldn't do ssl handshake
  - OpenSSL Error: s3_clnt.c:836: in library: SSL routines, function SSL3_GET_SERVER_CERTIFICATE: certificate verify failed
  - globus_gsi_callback.c:351: globus_i_gsi_callback_handshake_callback: Could not verify credential
  - globus_gsi_callback.c:424: globus_i_gsi_callback_cred_verify: Can't get the local trusted CA certificate: Cannot find issuer certificate for local credential (error code 7)
Some Cert – related error messages

Other errors that could/should be identified:
- Bad signing policy file
- Missing signing policy file
- Missing CA cert
- Bad CA cert
- Revoked CA cert
- &c....
Error message problems

- Verbiage
- Overlap (See next slide for test chart)
  - no-1:
    - incompatible or misconfigured client or misconfigured server
  - no-2:
    - misconfigured client, or ~/.globus/certificates directory, or some kind of dhcp error
  - no-3:
    - incompatible or misconfigured client
  - no-5:
    - misconfigured client or misconfigured server
## Compatibility matrix

Key: “of” = old CA support files; “nf”=new  
“oc” = EE cert from old CA; “nc” = new

<table>
<thead>
<tr>
<th>Number</th>
<th>Client</th>
<th>Server</th>
<th>Result</th>
<th>Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>of-oc</td>
<td>of-oc</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>of-nc</td>
<td>of-oc</td>
<td>no-1</td>
<td>grid-proxy-init -verify</td>
</tr>
<tr>
<td>3</td>
<td>of-oc</td>
<td>of-nc</td>
<td>no-5</td>
<td>misconfigured server</td>
</tr>
<tr>
<td>4</td>
<td>of-nc</td>
<td>of-nc</td>
<td>no-5</td>
<td>grid-proxy-init -verify</td>
</tr>
<tr>
<td>5</td>
<td>nf-oc</td>
<td>of-oc</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>nf-nc</td>
<td>of-oc</td>
<td>no-1</td>
<td>incompatible</td>
</tr>
<tr>
<td>7</td>
<td>nf-oc</td>
<td>of-nc</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>nf-nc</td>
<td>of-nc</td>
<td>no-1</td>
<td>none found</td>
</tr>
<tr>
<td>9</td>
<td>of-oc</td>
<td>nf-oc</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>of-nc</td>
<td>nf-oc</td>
<td>no-2 (err 74)</td>
<td>misconfigured client</td>
</tr>
<tr>
<td>11</td>
<td>of-oc</td>
<td>nf-nc</td>
<td>no-3</td>
<td>incompatible</td>
</tr>
<tr>
<td>12</td>
<td>of-nc</td>
<td>nf-nc</td>
<td>no-3</td>
<td>grid-proxy-init -verify</td>
</tr>
<tr>
<td>13</td>
<td>nf-oc</td>
<td>nf-oc</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>nf-nc</td>
<td>nf-oc</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>nf-oc</td>
<td>nf-nc</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>nf-nc</td>
<td>nf-nc</td>
<td>ok</td>
<td></td>
</tr>
</tbody>
</table>
Notes on the tests

- Starting point is case #1
- Desired end point is case #16
- Clear lines are cases where globus job ran
- Case #7 is bizarre but unimportant
  - Shouldn’t work, don’t allow
- Cases #5 & #9 are intermediate steps
- Solaris 8 – binary GT 2.2.4 distro unpatched
  – no data on other platforms
Error message problems

- There are 4 distinct error fingerprints
- "Misconfigured client" can be the cause of any one of the 4.
- Nor are ANY of the errors unique to any particular configuration problem.
- Plus there are other errors to take into account
Strategies for dealing with errors

- Update all machines involved
- Run grid-proxy-init --verify at all times
  - Why isn’t this mandatory? What use is the other form?
  - Catches all client misconfiguration cases
- ALWAYS store CA support files in /etc/grid-security/certificates
- Eliminate any other element of TRUSTED_CA
Strategies for dealing with errors (2)

- **doegrids-hash-check**
  - Script to check machine CA cert installation
  - Deal with errors it identifies before calling
  - This could catch all incompatibilities

- May provide verify –type scripts
  - What would be useful?
  - openssl verify + Globus security info

- Scripts are front line
Strategies for dealing with errors (3)

- GPT – install kits for CA support files
  - Is this worth doing?
  - Takes some tinkering/time
- Still need to collect and annotate errors