Proposed ACL's on Space Tokens
as part of the WLCG SRM 2.2 MoU addendum number 1.

Patrick Fuhrmann
Tigran Mkrtchyan
ACL's can only be applied to space tokens, not to space token descriptions, which can lead to unexpected behavior if ACL-I and ACL-II differ.
Talks to VOMS server

**voms-proxy-init**

\[ DN=DC=de/CN=Patrick \]
\[ Lifetime=1 \text{ Year} \]

**CERTIFICATE**

**grid-proxy-init**

\[ DN=DC=de/CN=Patrick \]
\[ Lifetime=24 \text{ HOURS} \]

**PROXY**

\[ DN=DC=de/CN=Patrick \]
\[ /atlas \]
\[ /atlas/Role=production \]

**Server**

You need to trust the VOMS server.

\[ DN=DC=de/CN=Patrick \]
\[ /atlas \]
\[ /atlas/Role=production \]

**MAPPING**

Similar to Kerberos

**CERTIFICATE MAPPING**

You need to trust the VOMS server.

\[ DN=DC=de/CN=Patrick \]
\[ /atlas \]
ACL operations on Spaces

- Write-to-space
- Replicate-from-space
- Stage-to-space
- Read-from-space
- Query-space
- Update-space
- Modify-space-acl
- Purge-from-space
- Release-space
# ACL operations on Spaces

<table>
<thead>
<tr>
<th>SRMOp</th>
<th>Acl Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepare to Put</strong></td>
<td>Write-to-space</td>
</tr>
<tr>
<td><strong>Prepare to Get</strong></td>
<td>Read-from-space</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Write-to-space</td>
</tr>
<tr>
<td></td>
<td>Stage-to-space</td>
</tr>
<tr>
<td><strong>Bring Online</strong></td>
<td>Stage-to-space</td>
</tr>
<tr>
<td></td>
<td>Write-to-space</td>
</tr>
<tr>
<td><strong>Purge From Space</strong></td>
<td>purge-from-space</td>
</tr>
<tr>
<td><strong>Release Space</strong></td>
<td>release-space</td>
</tr>
<tr>
<td><strong>Query Space</strong></td>
<td>query-space</td>
</tr>
<tr>
<td><strong>Change Space</strong></td>
<td>change-space</td>
</tr>
</tbody>
</table>

**Remark:** Replicate-from-space is weaker than read-from-space because no pin is created on the source file. Therefore we need two different ACL operations.
Access Control List Composition

- The Access Control “Subject” is either the DN or the Fully Qualified Attribute Name (FQAN)
- Only primary FQAN's should be considered when matching ACL's

**DN=/DC=de/CN=Patrick**

- /atlas/Role=production
- /atlas
- /atlas/MC

**Primary FQAN**
Access Control List Composition (cont)

Space

Space ACL
(Sorted List Of ACE's)

Space ACE

- Subject type
- DN/FQAN
- Operation Mask
- ALLOW/DENY

Type is fqan
fqan:/atlas/Role=super
stage;read;write
ALLOWED

Sorted List Of ACE's
Access Control List Composition (cont)

➢ Only those ACE's of an ACL are considered for comparision, where the requester DN/FQAN matches the ACE DN/FQAN
➢ A single request may ask for more than one bit of the operation bit mask (e.g. read and stage).
➢ As soon as a negative ACE for one of the operation bits is hit, the complete request is denied.
➢ As soon as a positive ACE is found for an operation bit, this particular bit is no longer processed.
➢ In order to get the complete request through, all operation bit must at some point find a ACCEPT.
➢ If the request reaches the end of the sorted ACE list, and not all operation bits have been ACCEPTED, the request is denied.
Access Control List Composition (cont)

e.g.: regular atlas user needs to read a file which is on tape.

Request:

<table>
<thead>
<tr>
<th>fqan:/atlas</th>
<th>stage</th>
<th>read</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqan:/atlas</td>
<td>stage</td>
<td>read</td>
</tr>
<tr>
<td>fqan:/atlas/Role=production</td>
<td>stage</td>
<td>read</td>
</tr>
<tr>
<td>dn:/DC=de/CN=Patrick</td>
<td>stage</td>
<td>read</td>
</tr>
<tr>
<td>dn:/DC=de/CN=Patrick</td>
<td>stage</td>
<td>read</td>
</tr>
<tr>
<td>dn:/DC=de/CN=Patrick</td>
<td>stage</td>
<td>read</td>
</tr>
</tbody>
</table>

- ACCEPT
- DENY
Access Control List Composition (cont)

e.g. :DN='Patrick' needs to read a file which is on tape.

Request:

\[
\begin{align*}
\text{dn:/DC=de/CN=Patrick} & \quad \text{stage read} \\
\text{fqan:/atlas} & \quad \text{stage} \\
\text{fqan:/atlas/Role=production} & \quad \text{stage read} \\
\text{dn:/DC=de/CN=Patrick} & \quad \text{stage} \\
\text{dn:/DC=de/CN=Patrick} & \quad \text{read} \\
\text{dn:/DC=de/CN=Patrick} & \quad \text{stage read} \\
\text{dn:/DC=de/CN=Patrick} & \quad \text{read} \\
\text{dn:/DC=de/CN=Patrick} & \quad \text{stage read}
\end{align*}
\]

\[
\begin{align*}
\text{ACCEPT} & \\
\text{ACCEPT} & \\
\text{ACCEPT} & \\
\text{DENY} & \\
\text{ACCEPT} & \\
\text{ACCEPT} & \\
\end{align*}
\]