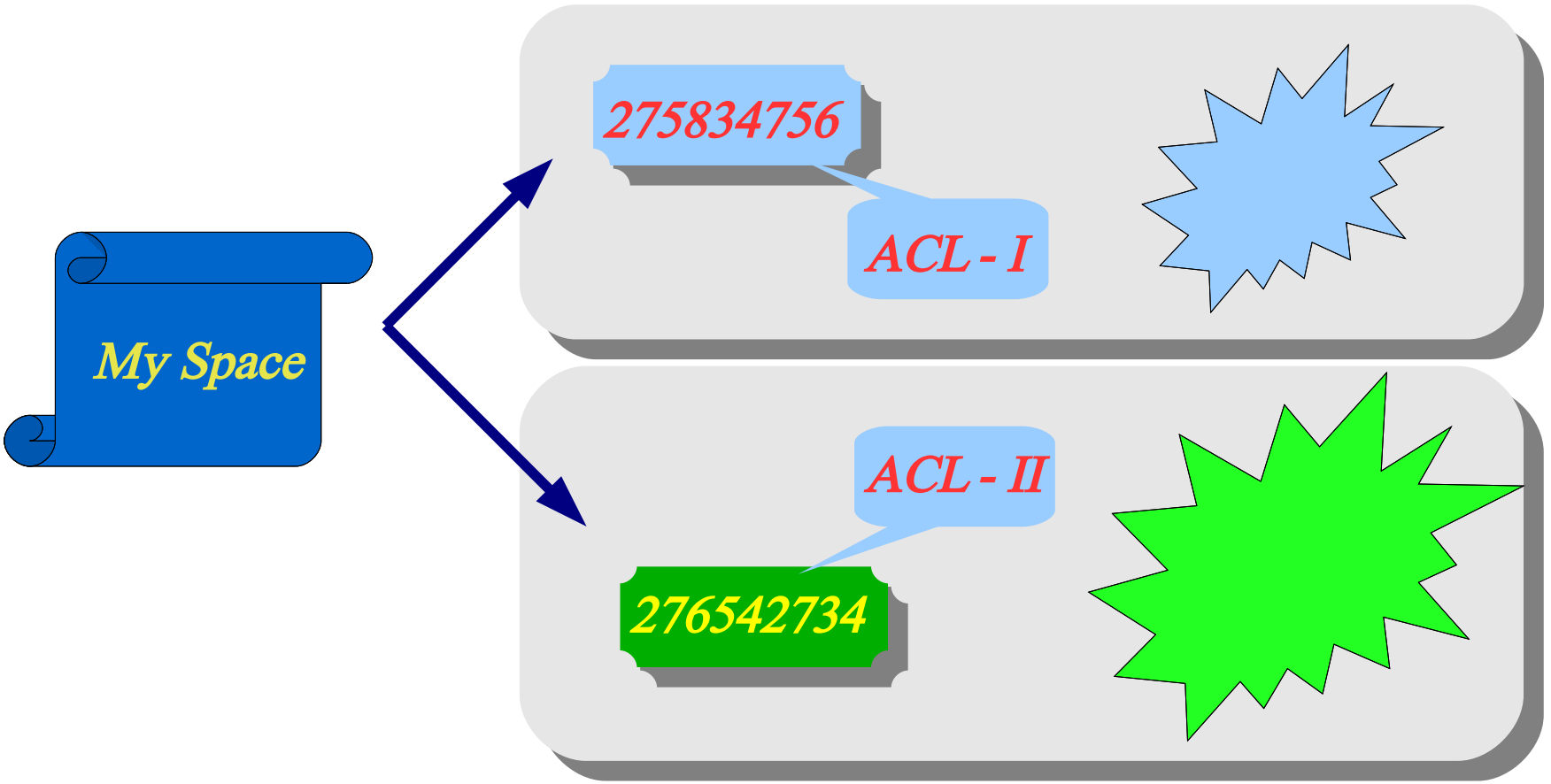
dCache.ORG

Proposed ACL's on Space Tokens

as part of the WLCG SRM2.2 MoU addendum number 1.

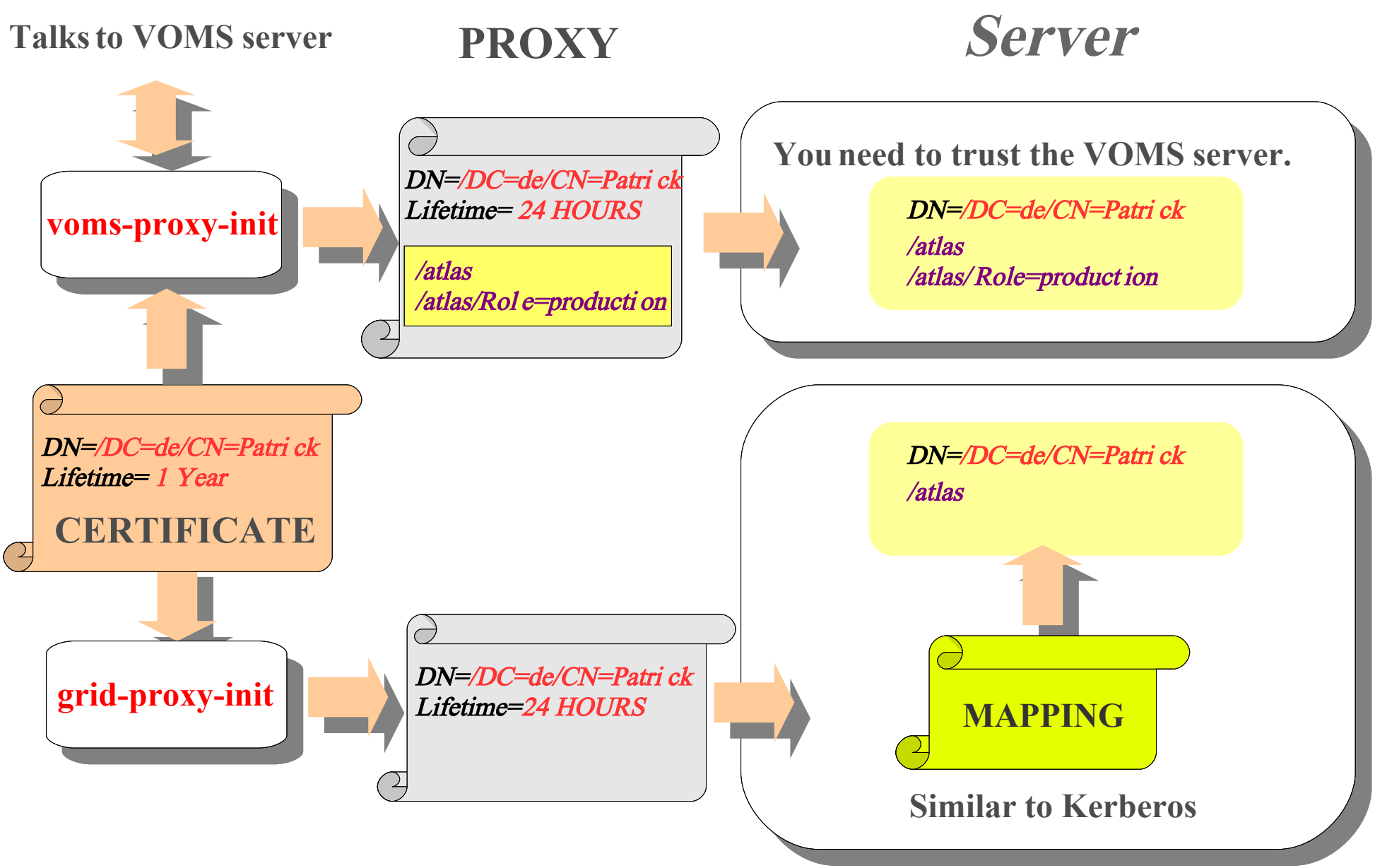
Patrick Fuhrmann
Tigran Mkrtchyan

dCache.ORG



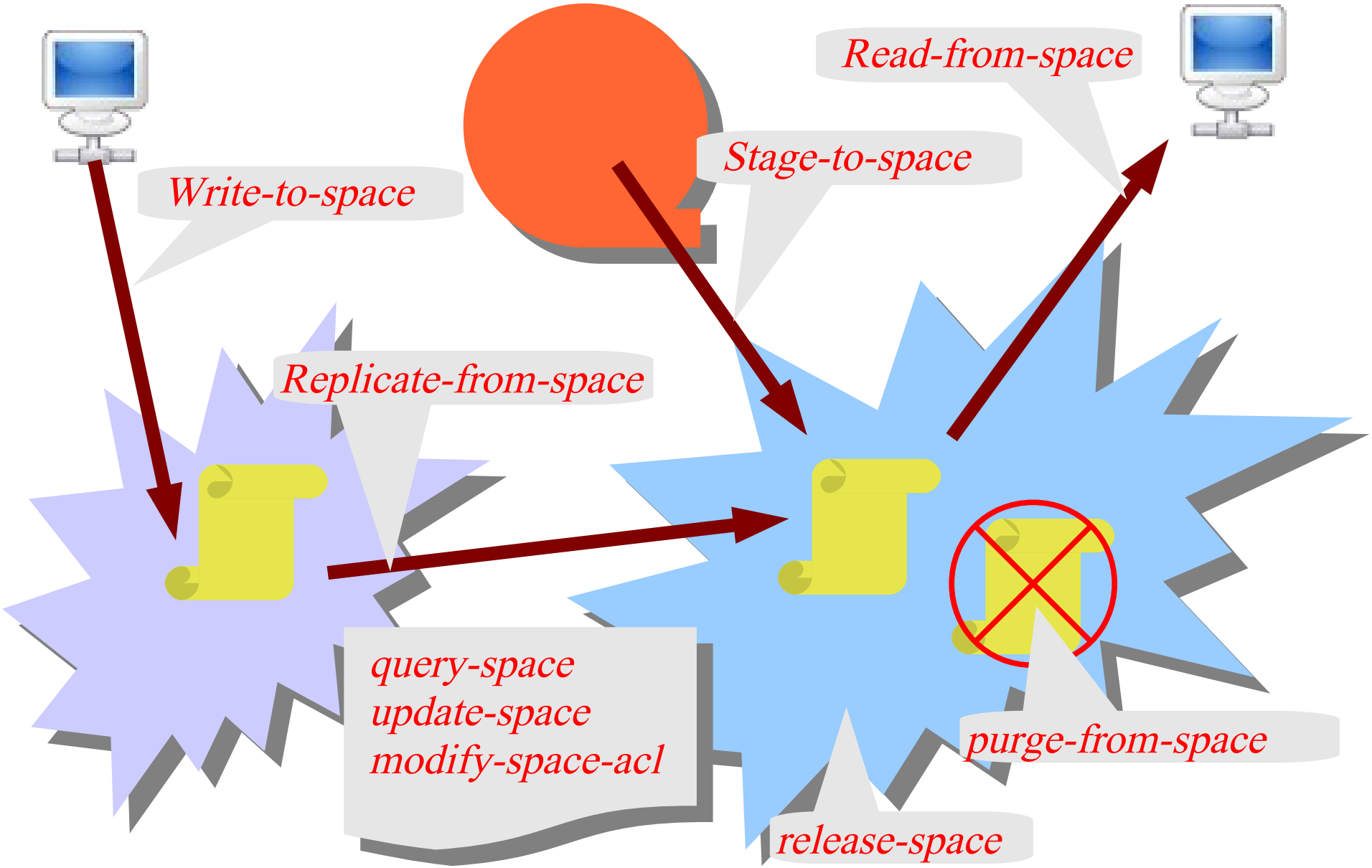
! ACL's can only be applied to space tokens, not to space token descriptions, which can lead to unexpected behavior if ACL-I and ACL-II differ. !

dCache.ORG



dCache.ORG

ACL operations on Spaces



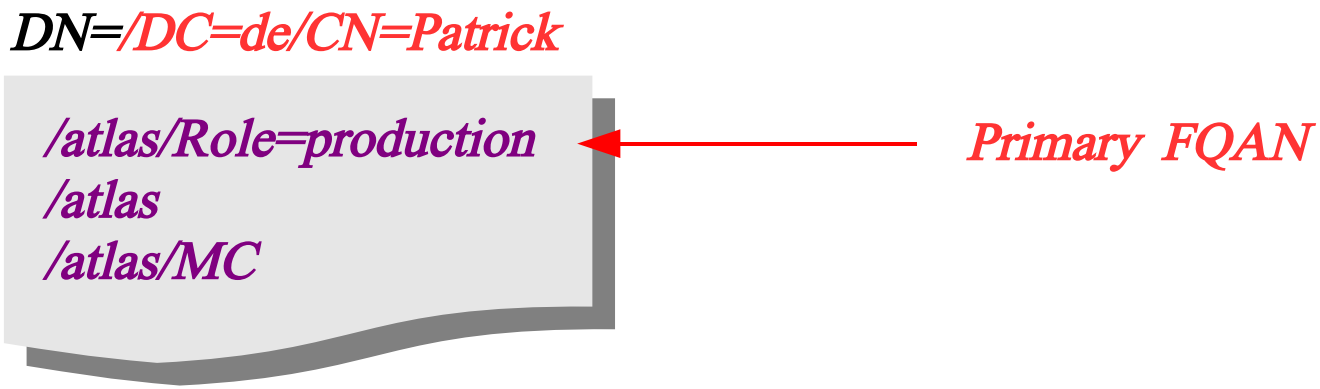
ACL operations on Spaces

SRM Op	Acl Operation	
Prepare to Put	Write-to-space	
Prepare to Get Copy	Read-from-space Write-to-space Stage-to-space	Replicate-from-space Write-to-space
Bring Online	Stage-to-space Write-to-space	Replicate-from-space
Purge From Space	purge-from-space	
Release Space	release-space	
Query Space	query-space	
Change Space	change-space	

Remark :
Replicate-from-space is weaker than read-from-space because no pin is created on the source file. Therefor 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



dCache.ORG

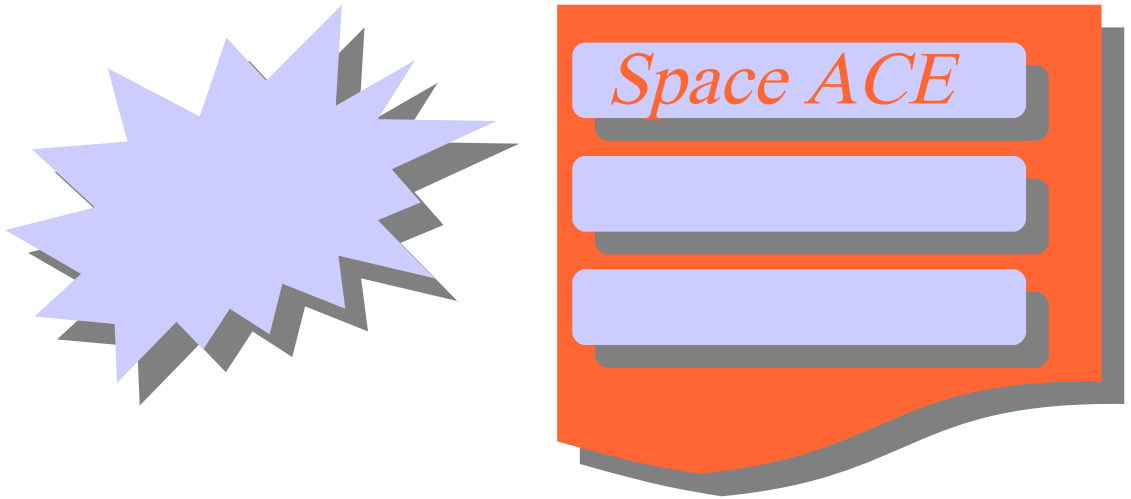
Access Control List Composition (cont)

dCache.ORG

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

Access Control List Composition (cont)

dCache.ORG

- 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.

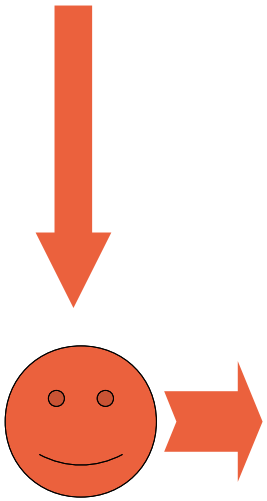
Access Control List Composition (cont)

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

Request :

fqan:/atlas *stage read*

fqan:/atlas	stage	ACCEPT
fqan:/atlas/Role=production	stage read	ACCEPT
dn:/DC=de/CN=Patrick	stage	ACCEPT
dn:/DC=de/CN=Patrick	read	DENY
fqan:/atlas	read	ACCEPT
dn:/DC=de/CN=Patrick	stage read	ACCEPT



dCache.ORG

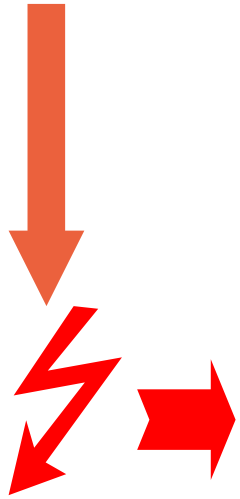
Access Control List Composition (cont)

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

Request :

dn:/DC=de/CN=Patrick *stage read*

fqan:/atlas	*stage*		*ACCEPT*
fqan:/atlas/Role=production	*stage*	*read*	*ACCEPT*
dn:/DC=de/CN=Patrick	*stage*		*ACCEPT*
dn:/DC=de/CN=Patrick		*read*	*DENY*
fqan:/atlas		*read*	*ACCEPT*
dn:/DC=de/CN=Patrick	*stage*	*read*	*ACCEPT*



dCache.ORG