# Security Group

D7.5 Document and Open Issues

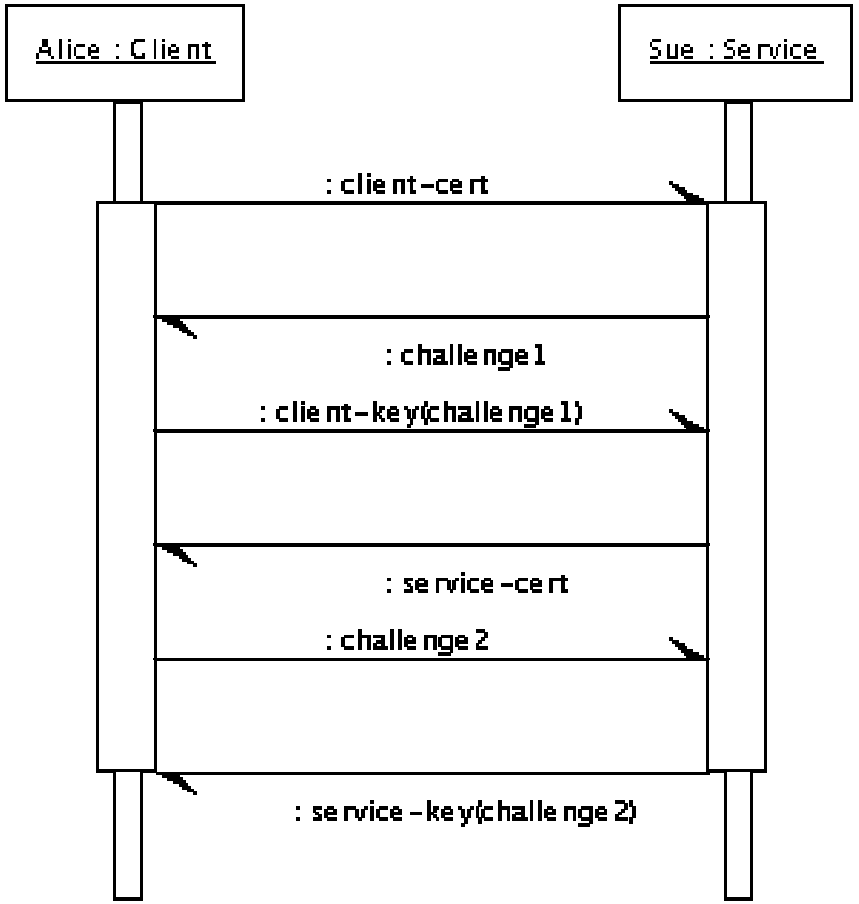
E-mail Akos.Frohner@cern.ch

# D7.5: Overview

- What is Security? (Chapter 3): general description
- Assumptions (Section 3.7): what will we not do
- 3 ∩ 3.7 = 4: Security Requirements
- Achieved goals (Chapter 5): what is done
- Plans (Chapter 6): not a consistent design yet!
- Checklists (Chapter 7): summary of 4 & 5 & 6

| | | | | | |
|---|---|---|---|---|---|
| AUT | Authentication | CNF | Confidentiality | USR | Usability |
| AUZ | Authorization | INT | Integrity | IOP | Interoperability |
| AUD | Auditing | NET | Network | SCA | Scalability |
| NRP | Non-Repudiation | ADD | Additional | PER | Performance |
| DLG | Delegation | MNG | Manageability | | |

# Mutual Authentication



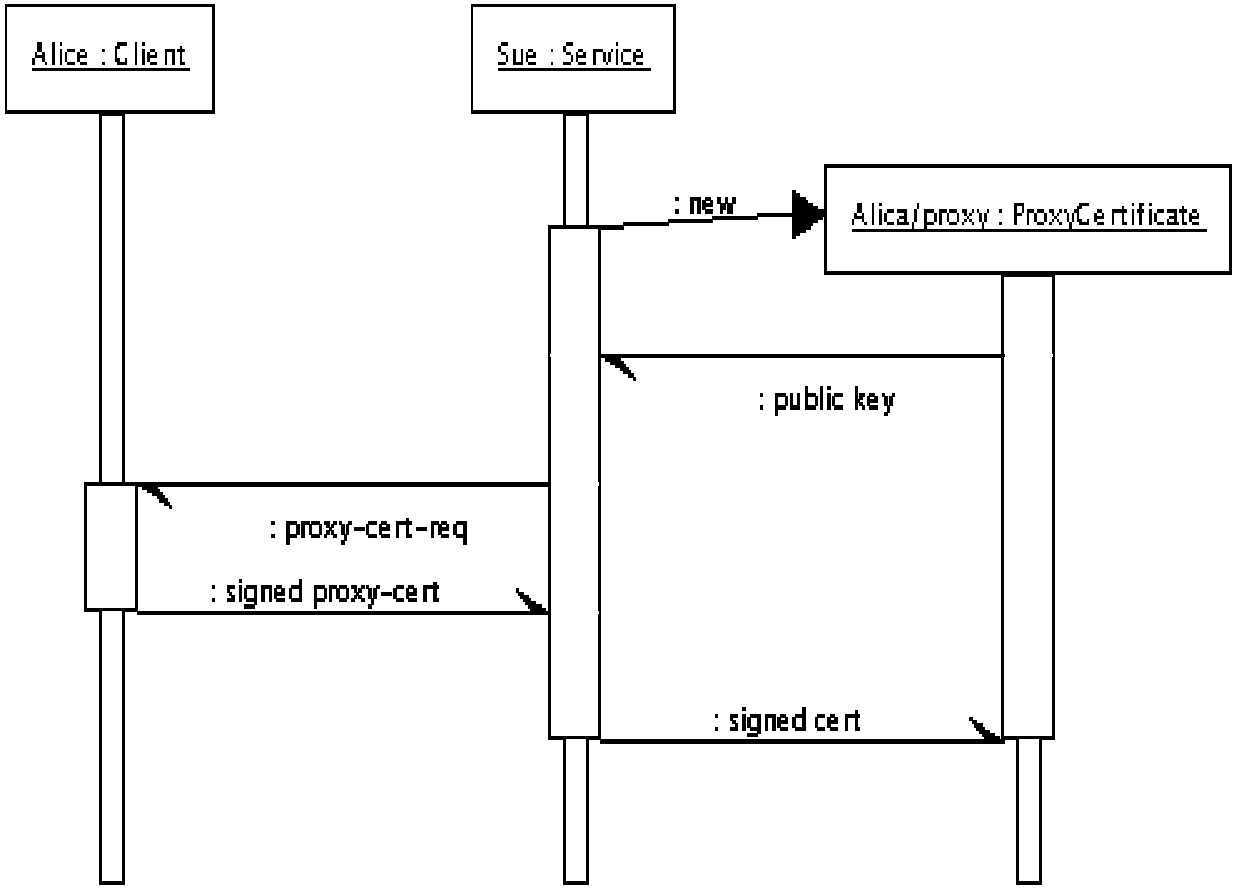

GSI – certificate based authentication

- AUT-02 symmetric
- AUT-05 lives beside existing authentication systems
- AUT-14 no associated VO or other authz information in a cert

- challenge = random data
- key(data) = encoding with key
- validation: decode(public key, encode(private key, data)) = data

Short-time certificates! -> no CRL

# Delegation




- proxy certificate is generated on the server side
- private key not crosses the net
- rights of the proxy are subset of the original rights

# Testbed1: CA/RA

- 11 CA
- well defined practices
- focus on only one VO: DataGrid

- CA = RA ?
- membership info in VO/LDAP

goal: „production deployment"

Certificate Management:

- scaleable revocation list handling
- user cert storage (central?)
- roaming access: web portals
- long term/renewable proxy certificates for long jobs

# Requirements: Authorization

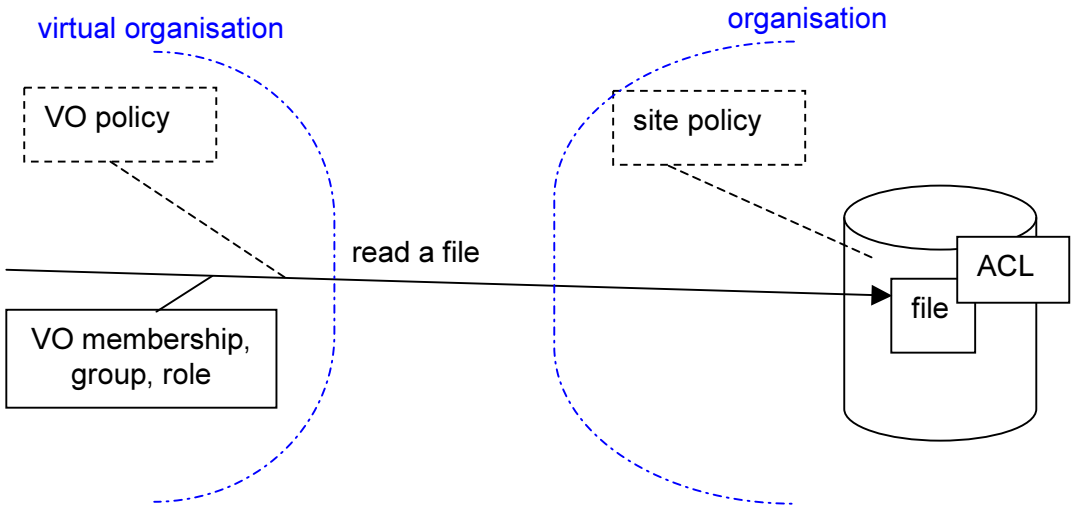
- AUZ-05 based on various info (id, CRL, role, group, lightweight ...)
- AUZ-16 disconnected operation
- AUZ-17... central access control – immediate disable?
- AUZ-21 user attributes: VO, groups, role (default)
- AUZ-23,24 authorize the resource, not the user – whom to trust?
- AUZ-25... granularity: controlled operations and objects

Questions:

- listing accessible resources vs. checking permission case-by-case
- central control (policy?) vs. disconnected operation
- group membership information – data source?

# Authorization: Membership (dataflow)

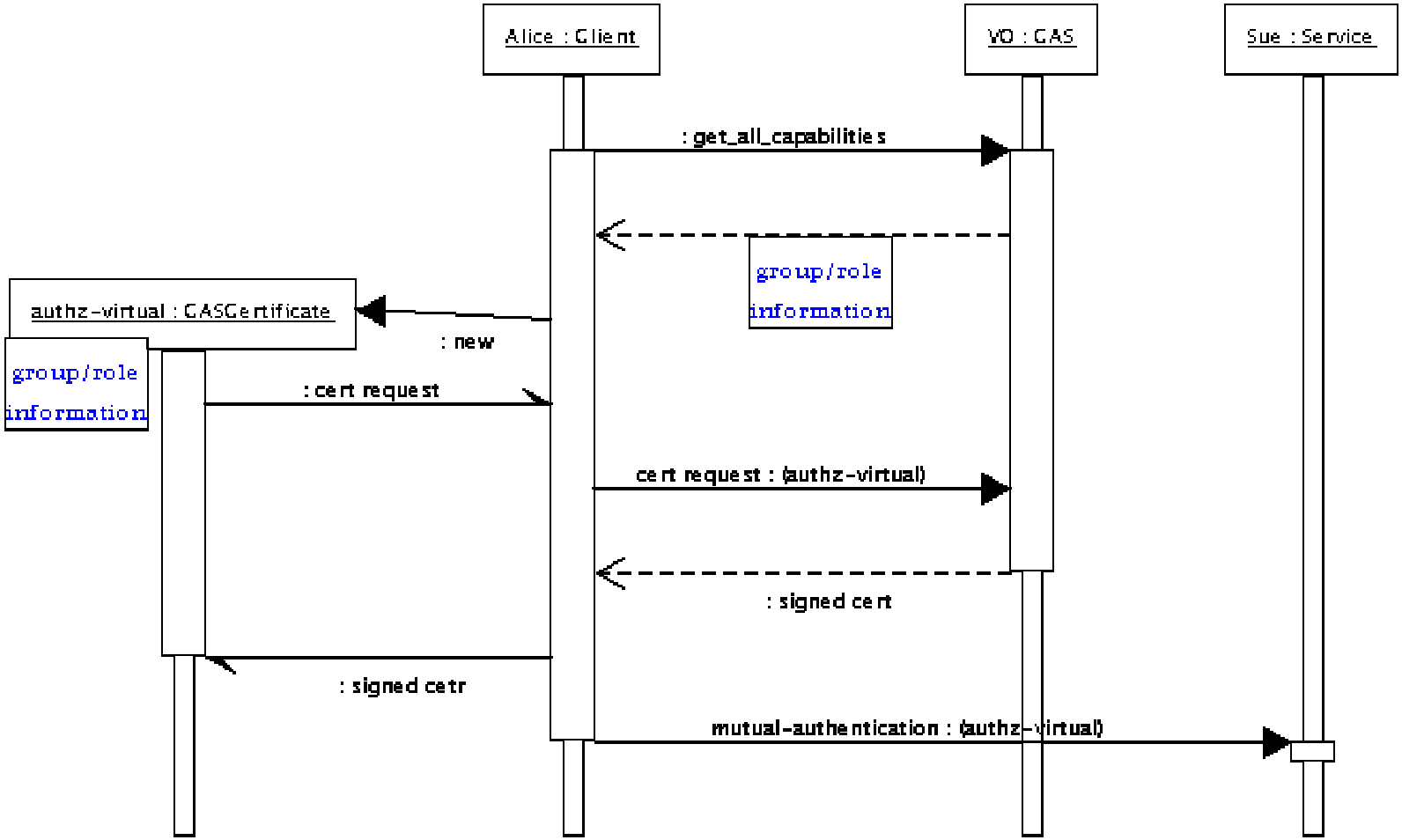
Not D7.5!




- Authenticate a user at a service
- Gather additional information associated to the user or the actual session (e.g. group membership, role, time)
- Gather additional information associated to the protected service or object (e.g. file permissions)
- Get local policy applicable to the situation (e.g. temporarily disabled user)
- Make an authorization information based on the identity and the additional information

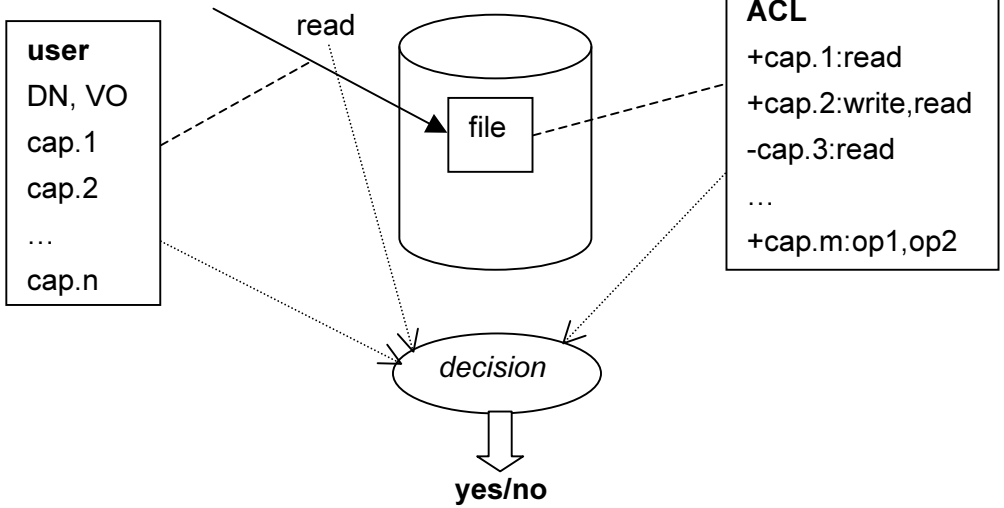
# Authorization: Membership (sequence)

Not D7.5!



# Authorization: Access Control List

Not D7.5!




- user – list of capabilities
- operation
- protected object – access control list

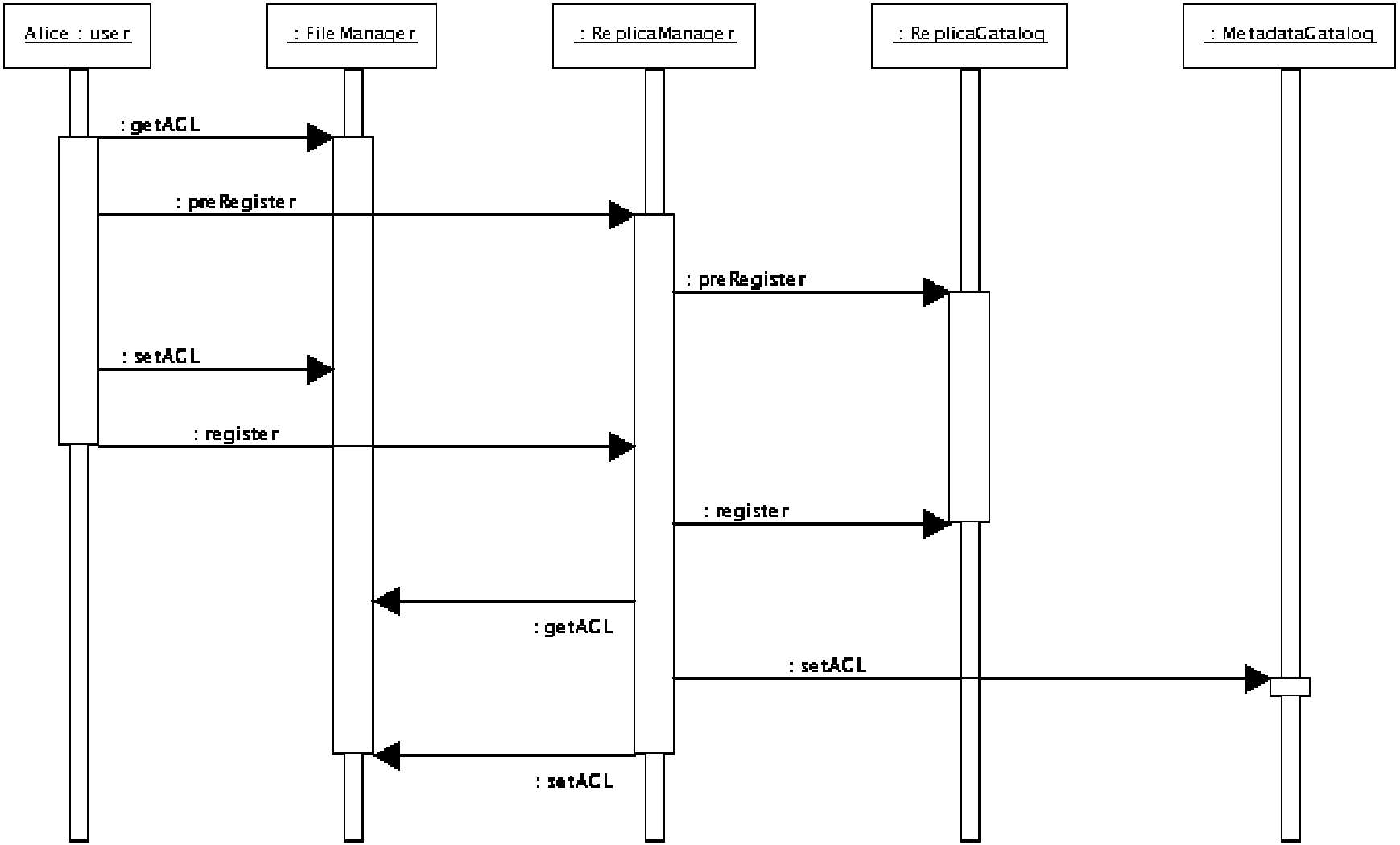
-> yes/no decision

capability:

- DN
- VO DN
- group/role/...

# Authorization: File Replication (WP2,5)

Not D7.5!



# Testbed1: WP2, WP5

in Tomcat configuration files:

- certificate checking
- certificate -> identity
- identity -> role

Goals:

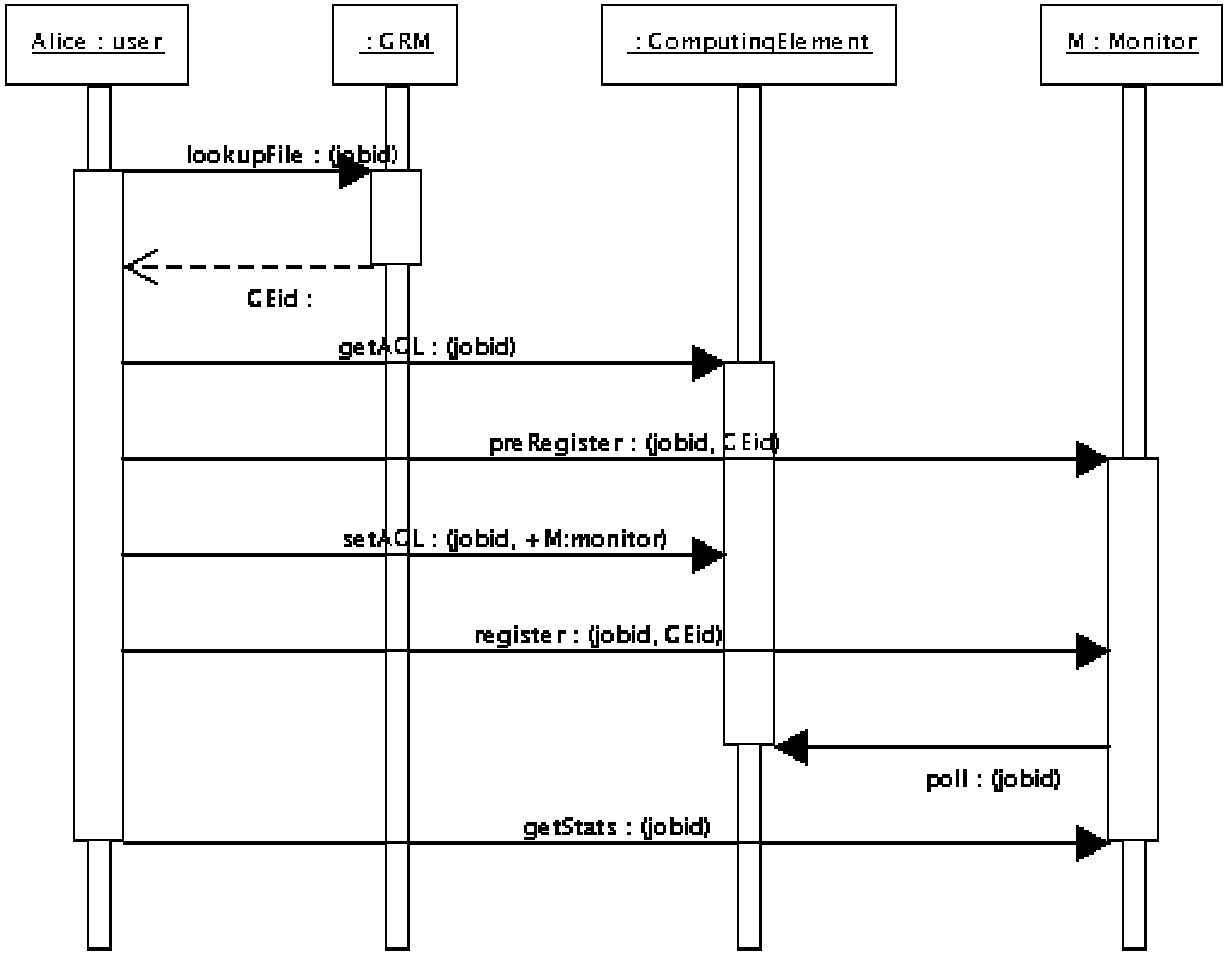
- Short term: local authorization DB
- Long term: general solutions for other services as well

Testbed-1: only local filesystem with gridftp for remote access

- pool of local userids
- VO = groupid
  group-level access permissions

# Authorization: Job Monitoring (WP1,3,4)

Not D7.5!



# Other Requirements

- Auditing+Non-repudiation: „trustable log"
- Delegation: traceable delegation – original identity preserved
- Confidentiality: protecting the data from unwanted access (before)
- Integrity: check for possible manipulations and errors (after)
- Network: firewalls (NAT, dynamic firewall config in plans)
- Management/Usability: make it simple
- Interoperability: with other „grids"
- Scaleable/Robust (user/machine/institute/country):
  1000/200/10/5 -> 10.000/1.000/100/10 -> 100.000/10.000/100/10

# Open Issues

gridmap file: authentication & authorization & map to local userid

- authentication: configurable trust (trusted CAs from VO?) -> CAS
- authorization: central vs. local service -> both
- mapping:
  - single userid: grid service does everything (SE)
  - pool of userids: local enforcement system (CE)
  - 1-1: local authorization system (maybe as an extra step)