Security Co-ordination Group (WP7 SCG)

EDG Heidelberg
30 September 2003

David Kelsey
CCLRC/RAL, UK
d.p.kelsey@rl.ac.uk

Overview

- Security in EDG 2.1
- SCG/Applications joint session (Saturday)
- VO naming, ACL syntax (input to GGF)
- D7.7 plans
- Summary

Comments

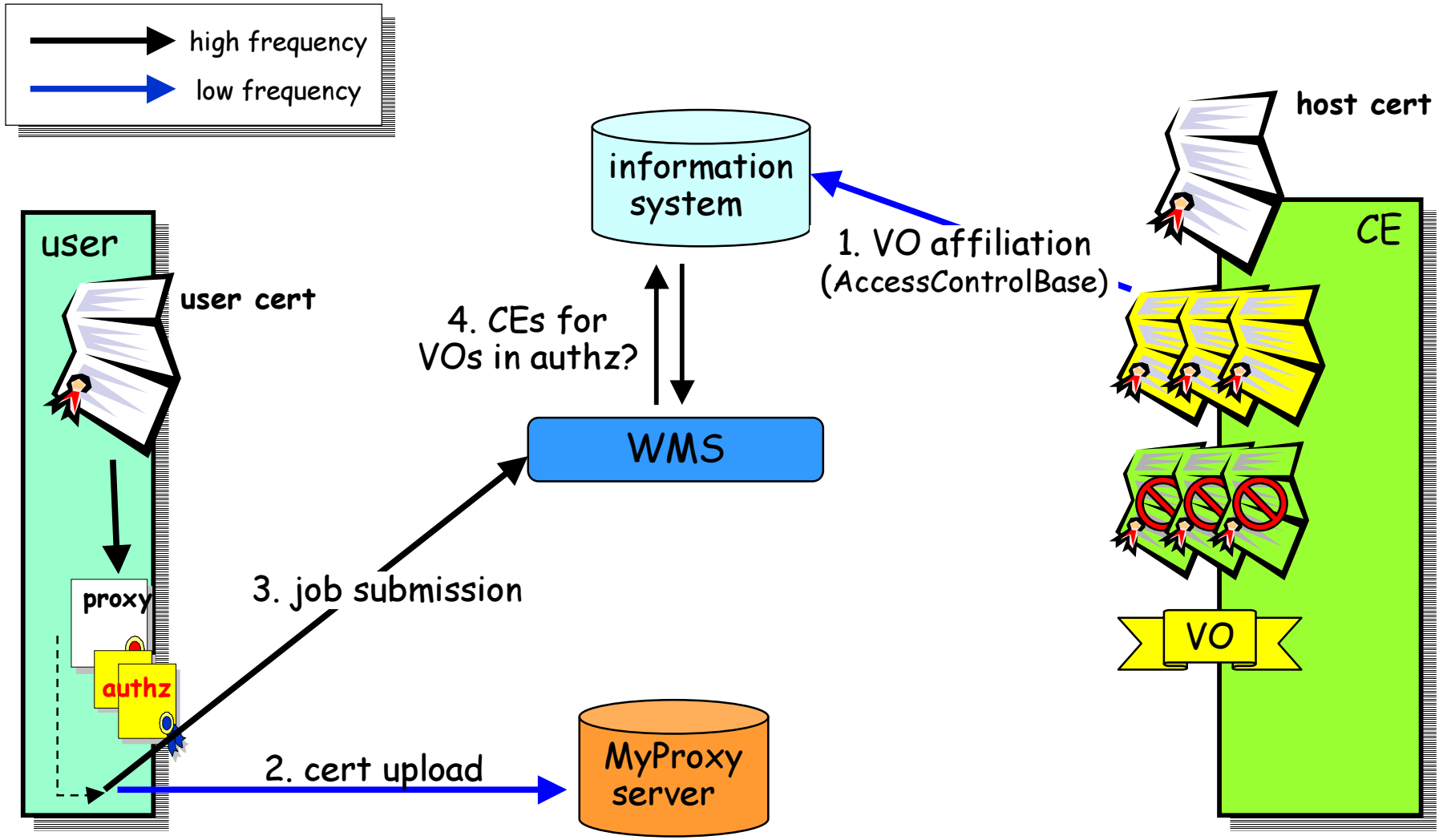
- This is the **first** time I have not had to request a slot in the summary plenary (at final project conference!)
- SCG has come of age
- Quote:
  - *EDG realised it had forgotten security (1st conference)*
    - Fabrizio Gagliardi (26 Sep 2003)
- So….no security requirements
- All requirements fully satisfied!

Security in EDG 2.1

VOMS

- VOMS is deployed
- Big improvement in Authorization (AuthZ) functionality
  - Fine-grained access control
  - Groups, sub-groups, roles, capabilities
  - Support for multiple VO's
- Unfortunately little time for services to use the VOMS attributes
- EDG PTB (26 August) decided that job submission integrated with VOMS together with LCAS/LCMAPS was the highest priority for the EDG 2.1 Application TB
  - WP1/WP4/SCG efforts

Job Submission

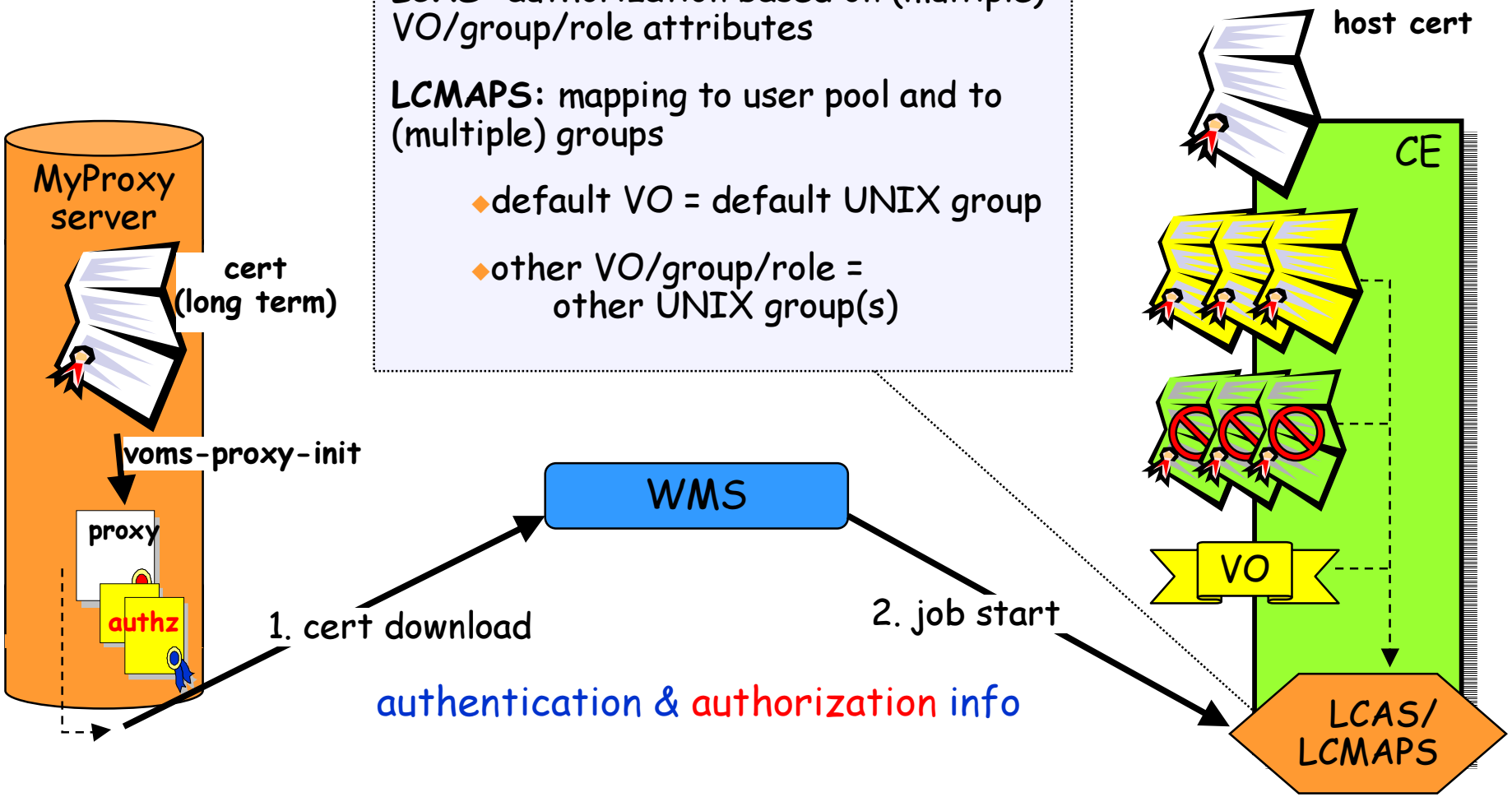


Running a Job

LCAS: authorization based on (multiple) VO/group/role attributes

LCMAPS: mapping to user pool and to (multiple) groups

- default VO = default UNIX group
- other VO/group/role = other UNIX group(s)



VOMS status

- VOMS server deployed (19th Sep)
  - INFN, RAL and CERN running servers
  - ITeam and WP6 VO's tested
- VOMS client
  - Included in UI
  - Configured at CERN on dev testbed
- Need to run VOMS servers for other VO's
  - NIKHEF offer to do this (WP6)
- VO managers need training

WP1 Security

- WP1
  - Proxy renewal service (26 Sep)
    - Support for VOMS
    - Renew proxy with same VOMS info as in old proxy
  - Logging and Bookkeeping service (26 Sep)
    - Access control implemented
      - Job-owners can specify an ACL to allow others access
      - Uses GACL library
      - ACLs stored in LB database
      - New LB API (and command line) to add/remove ACL entries
    - VOMS support (AuthZ info extracted for use in ACL)
  - WMS
    - Uses VO info from CE Info provider for job matchmaking
      - If job comes with VOMS proxy (VO name only)

WP2 and WP3 security

- WP2
  - edg-java-security deployed (24th Sep)
  - Authentication works
  - Authorization not enabled
  - C++ client now working but not deployed
- WP3
  - Authentication in R-GMA deployed
    - Well tested, but currently turned off
  - No delegation
  - No Authorization
  - C++ client as well
    - will be turned on with Java security
  - R-GMA browser (requires host certificates as in WP2)

WP4 Security

- WP4
  - LCAS, LCMAPS deployed (12th Sep)
    - Full fine-grained VOMS support
    - Sys admins have to enable this on clusters
      - Only for central LDAP-based user database
    - If not then coarse-grained VO-based AuthZ
      - Or local group-based AuthZ – defined by sys admin
  - GACL-based access control: LCAS plug-in
  - Translation tool for local credentials to GACL
  - CE Info Provider can give static list of VO's
    - For use in WP1 WMS

WP5 Security

- WP5
  - Secure mode (edg-java-security) deployed
  - Insecure mode supported in parallel
    - always mapped to WP6 VO
  - Plan to switch off insecure mode
    - Needs testing
    - Needs WP2 to call secure mode
  - ACLs supported (GACL) but not deployed
    - Therefore no fine-grained access control
  - Testing restricted write access (from VOMS)
    - May be possible on EDG 2.1
  - No delegation (web services)

SCG/Applications

Joint SCG/WP8-9-10 session

- To consider use cases for VOMS and priorities
  - Groups
  - Roles
  - Access Control etc
- Papers written by each WP during the summer
- Useful discussions
- Also highlighted many other missing or incomplete features
  - Accounting, monitoring, quotas, …

Cartoonist View of the World

Actually it's 2 years and 10 months…

Conclusion

- For deployment beyond EDG 2.1
  - If resources available and bug-fixing allows…
- Implement fine-grained access control to files (WP2/5)
  - Using WP9/GOMES as an example
  - Possible demo for EU Review (Feb 2004)
- Really would have liked to tackle Bio-medical encryption
  - Very doubtful that we will find time

VO naming, ACL syntax

Names and syntax

- Offering EDG AuthZ as input examples to GGF
  - VOMS, LCAS/LCMAPS, Java Security, GACL, GridSite, etc
- GGF OGSA-AuthZ working group
  - Co-chaired by EDG member (Andrew McNab)
  - AuthZ/Access Control with SAML and XACML
- We need globally unique names for VO's
  - Also need to establish the root of trust
  - Propose using registered DNS names
    - e.g. *vo-atlas.cern.ch*
    - Or even *lhcb.org*
- Strings in ACL entries – defined format
  - /VO[/Group/[Sub-group(s)]][/Role=r][/Capability=c]

Deliverable D7.7

Plans for D7.7

- D7.7 (PM36)
  - Final Report on Security
- Discussed at SCG meeting on Monday
- Linda Cornwall (RAL) – editor
- Will concentrate on
  - Successful deployment of new AuthZ technology
    - Design described in D7.6
  - Show the requirements that have now been met
    - As specified in D7.5
  - Describe areas for work in future projects
- Security evaluations also in other deliverables (e.g. D6.8)

Summary

- Much progress has been made
  - Delays in EDG 2.0 delayed the security implementation
- Nevertheless
  - We will demonstrate AuthZ in WMS
    - On application testbed (EDG 2.1)
  - Some simple access control may be possible on files
    - Even on EDG 2.1
  - Working on full demo for EU review
- A big thank you to all my colleagues in SCG
  - The architects, designers and developers