Security

WP7: Security Coordination Group (SCG)

David Kelsey (CCLRC-RAL, UK)
d.p.kelsey@rl.ac.uk

DataGrid is a project funded by the European Commission
under contract IST-2000-25182

Outline

- SCG Objectives
- SCG Achievements
  - *Overview*
  - *Authentication*
  - *Authorization*
  - *Requirements analysis*
- Lessons learned
- Future & Exploitation
- Questions

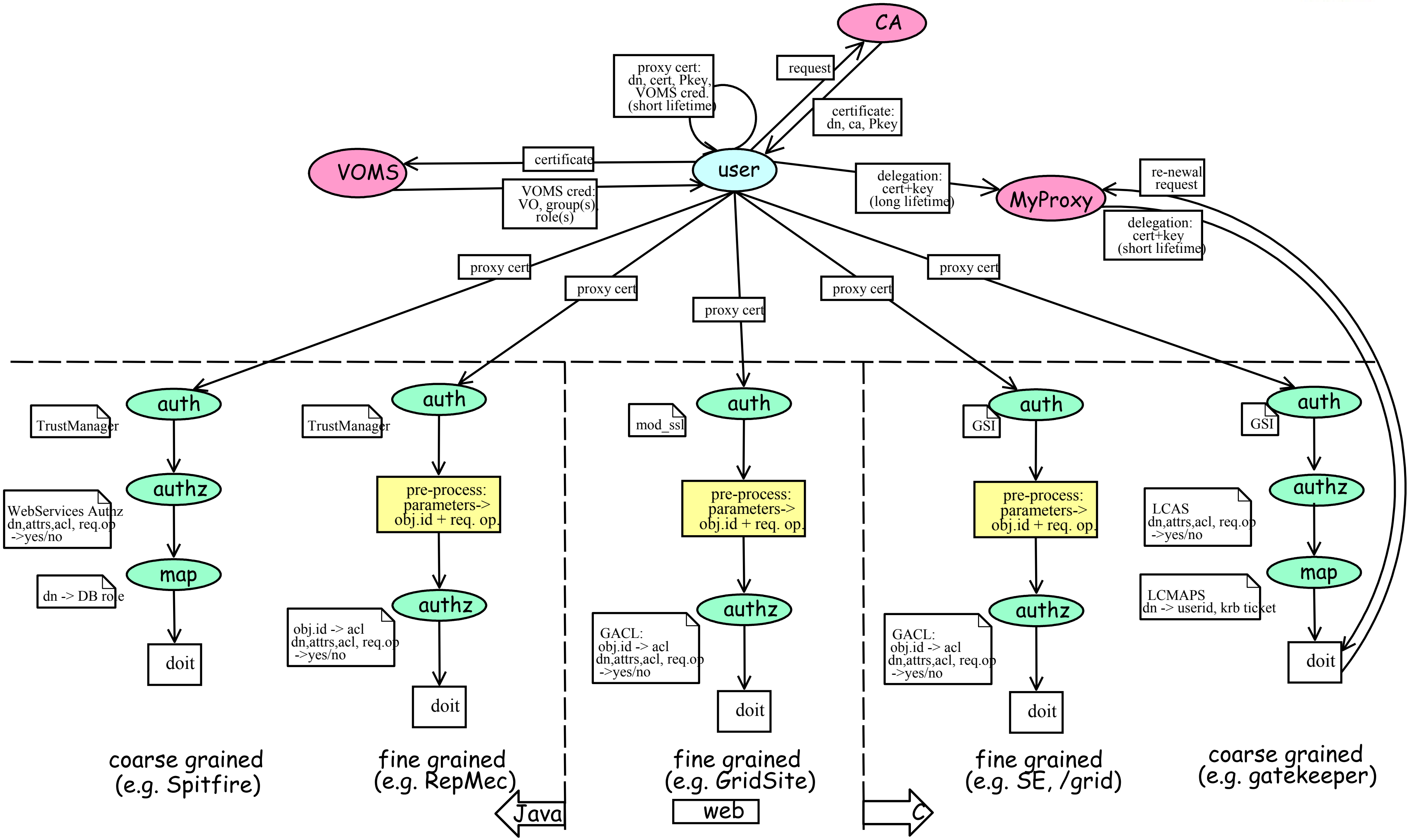
SCG Objectives

- No single work-package to tackle Grid security
  - n.b. WP2 has a security task and team
- Security Coordination Group (SCG) was formed in late 2001
  - Task 7.4 (TA) in WP7 started in month 13
- Mandate of SCG (sub-group of WP7)
  - To produce the Deliverables of WP7 on Security (task 7.4)
  - To help coordinate security activities in WPs 1 to 7
  - To liaise with WP6 CA/Authorization groups (and others)
  - To contribute to the Architecture of the EU DataGrid (ATF)
- n.b. most of the effort was unfunded
  - At least one representative per middleware WP
  - Collaboration with DataTAG and national Grid projects

SCG Achievements

- Authentication: Certification Authorities for EDG and others
  - WP6 Certificate Authorities Coordination Group
- DataGrid Security Requirements (D7.5, May 2002)
  - 112 requirements in many areas…
  - Authentication, Authorization, Auditing, Non-repudiation, Delegation, Confidentiality, Integrity, Network, Manageability, Usability, Interoperability, Scalability, Performance, Robustness
- Several useful joint meetings with WP8, 9 and 10 for VO use cases
- Security Design (D7.6, March 2003)
- Implementation, Integration and Deployment of many security components, some in collaboration with other projects
- Final Security Report (D7.7, January 2004)
  - includes comparison with initial requirements

Overview of the EDG Security Components


CA
request
certificate: dn, ca, Pkey
proxy cert: dn, cert, Pkey, VOMS cred. (short lifetime)
VOMS
certificate
VOMS cred: VO, group(s), role(s)
user
delegation: cert+key (long lifetime)
MyProxy
re-newal request
delegation: cert+key (short lifetime)
proxy cert
proxy cert
proxy cert
proxy cert
proxy cert
auth
TrustManager
authz
WebServices Authz dn,attrs,acl, req.op ->yes/no
map
dn -> DB role
doit
coarse grained (e.g. Spitfire)
auth
TrustManager
pre-process: parameters-> obj.id + req. op.
authz
obj.id -> acl dn,attrs,acl, req.op ->yes/no
doit
fine grained (e.g. RepMec)
Java
auth
mod_ssl
pre-process: parameters-> obj.id + req. op.
authz
GACL: obj.id -> acl dn,attrs,acl, req.op ->yes/no
doit
fine grained (e.g. GridSite)
web
auth
GSI
pre-process: parameters-> obj.id + req. op.
authz
GACL: obj.id -> acl dn,attrs,acl, req.op ->yes/no
doit
fine grained (e.g. SE, /grid)
C
auth
GSI
authz
LCAS dn,attrs,acl, req.op ->yes/no
map
LCMAPS dn -> userid, krb ticket
doit
coarse grained (e.g. gatekeeper)

Authentication

Certification Authorities (CAs) for

- EU DataGrid
- EU DataTAG
- EU CrossGrid
- LHC Computing Grid project (LCG)
  - Global service for particle physics
  - Includes North America and Asia
- The same CA's also used by many national projects
  - France, Italy, Netherlands, Nordic countries, Spain, UK, …
- This PKI is used for cross-authentication by applications spanning several Grids

DataGrid PKI History

- Started planning the PKI in Autumn 2000
  - First meeting of WP6 CA group in December 2000
- Requirements
  - Use Globus Toolkit and GSI (X.509 PKI)
  - Users – require **single sign-on**
  - **One** identity certificate for use in many different Grids
  - Only support Grid Authentication
    - No long-term encryption, digital signing, …
- Pre-existing Certification Authorities in some countries
  - For other purposes and/or larger communities
  - Czech Republic, France, Italy, Portugal, UK,…

Early PKI Decisions

- **Keep Authorization and Authentication separate**
  - Authorization not stable enough and too VO-specific
- **One Grid electronic identity**
  - For use in all Grid projects (EU and national)
  - For user convenience
- **Would one CA be enough?** NO
- **Hierarchy or cross-signing?** NO
- **What is the most appropriate scale?**
  - **One** CA per country
- **Define "minimum requirements" for EDG-approved CA's**

CA Approval process

- "Minimum requirements" document
  http://marianne.in2p3.fr/datagrid/ca/
- Evaluation of CP/CPS and presentation to WP6 CA meeting
  - no physical audit
- Concentrate on
  - Registration Authority procedures
  - Operational procedures of the CA
  - Unique Distinguished Names within the whole PKI

Approved CAs

- Certification Authorities
  - 21 CAs span:
    - Europe
    - North America
    - Asia
  - Independent administration
  - Backbone of present & future global grid projects
- “Catch-all” operated by CNRS
- Under consideration
  - Belgium
  - Hungary
  - Israel
  - Japan
  - Pakistan

ArmeSFo	Armenia	HellasGrid	Greece
ASGCCA	Taiwan	INFN	Italy
CERN	Switzerland	LIP	Portugal
CESNET	Czech Rep.	NIKHEF	Netherlands
CNRS	France	NorduGrid	Nordic Countries
CyGrid	Cyprus	PolishGrid	Poland
DOE	USA	Russia	Russia
FNAL	USA	SlovakGrid	Slovakia
GermanGrid	Germany	Spain	Spain
GridCanada	Canada	UKeScience	UK
Grid-Ireland	Ireland		

Authorization (AuthZ)

- GSI based (or compatible) authentication
- grid-mapfile or VOMS based authorization (can be both)
- policy or ACL based access control
  - coarse and fine grained solutions
  - access control description's syntax is not yet standard
- implemented alternatives:
  - edg-java-security for Java web services
  - GSI/LCAS/LCMAPS for native C/C++ services
  - mod_ssl/GACL for Apache based web services
  - Slashgrid for transparent filesystem ACLs and GridSite
- Modified MyProxy service for credential renewal (incl AuthZ)

Virtual Organization Management Service (VOMS)

- Joint development with DataTAG
- Issues credentials to prove group/role/VO membership
  - standard RFC 3281 Attribute Certificate format
  - single string attributes – FQAN
- Core service: standalone daemon for the “login”
  - single purpose – high performance
- Administrative service: web service with API, command line and web user interface
  - for administration and registration
- Migration tools for gridmap-files and VO-LDAP servers

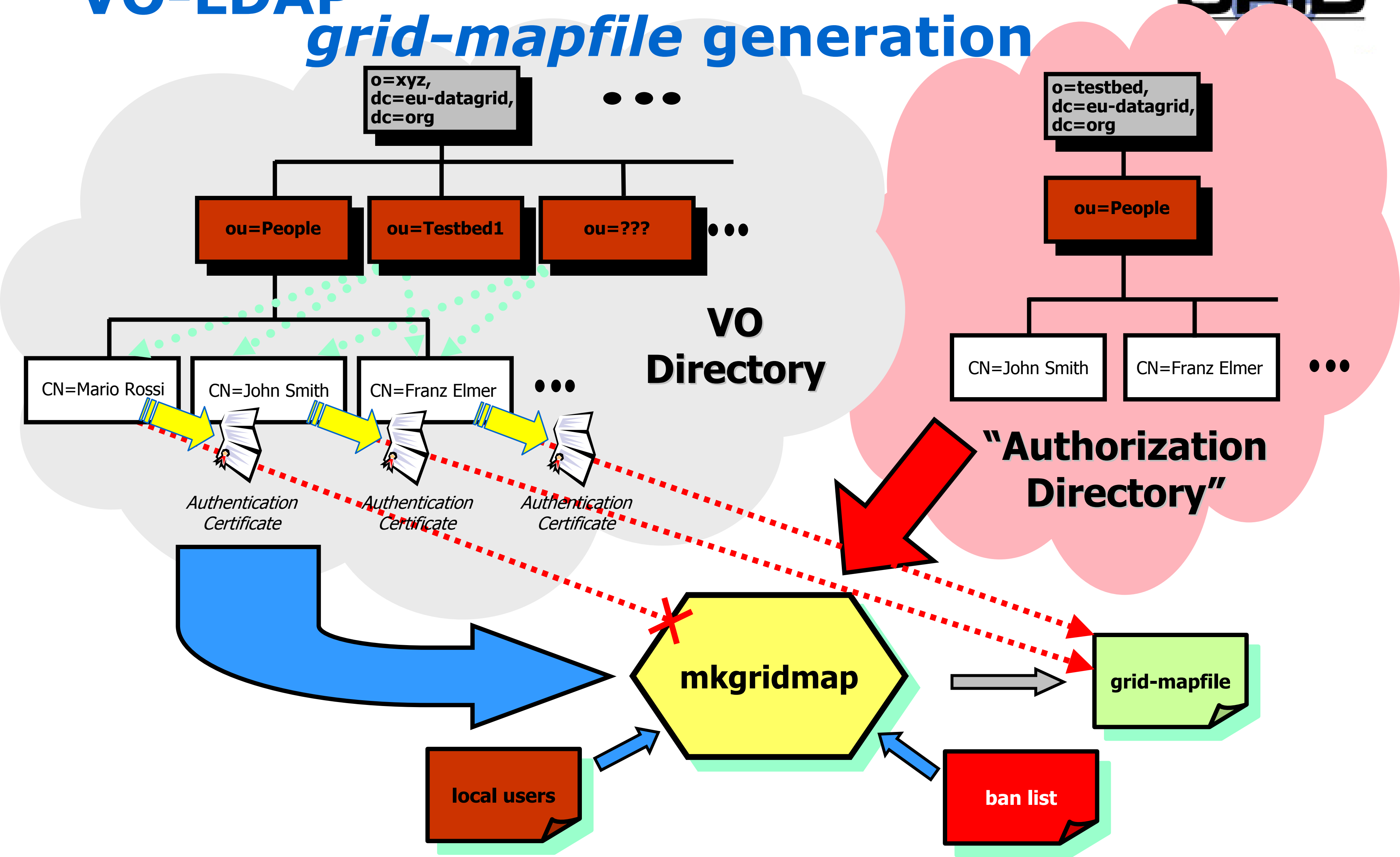
Local Site Authorization (WP4)

- Local Centre Authorization Service (**LCAS**)
  - Handles authorization requests to local fabric
    - decisions based on proxy user certificate and job specification;
    - supports *grid-mapfile* mechanism.
  - Plug-in framework (hooks for external authorization plugins)
    - allowed users, banned users, available timeslots, GACL
    - plugin for VOMS (to process authorization data)
- Local Credential Mapping Service (**LCMAPS**)
  - provides local credentials needed for jobs in fabric
  - mapping based on user identity, VO affiliation, local site policy
  - plug-ins for local systems (Kerberos/AFS, LDAP nss)

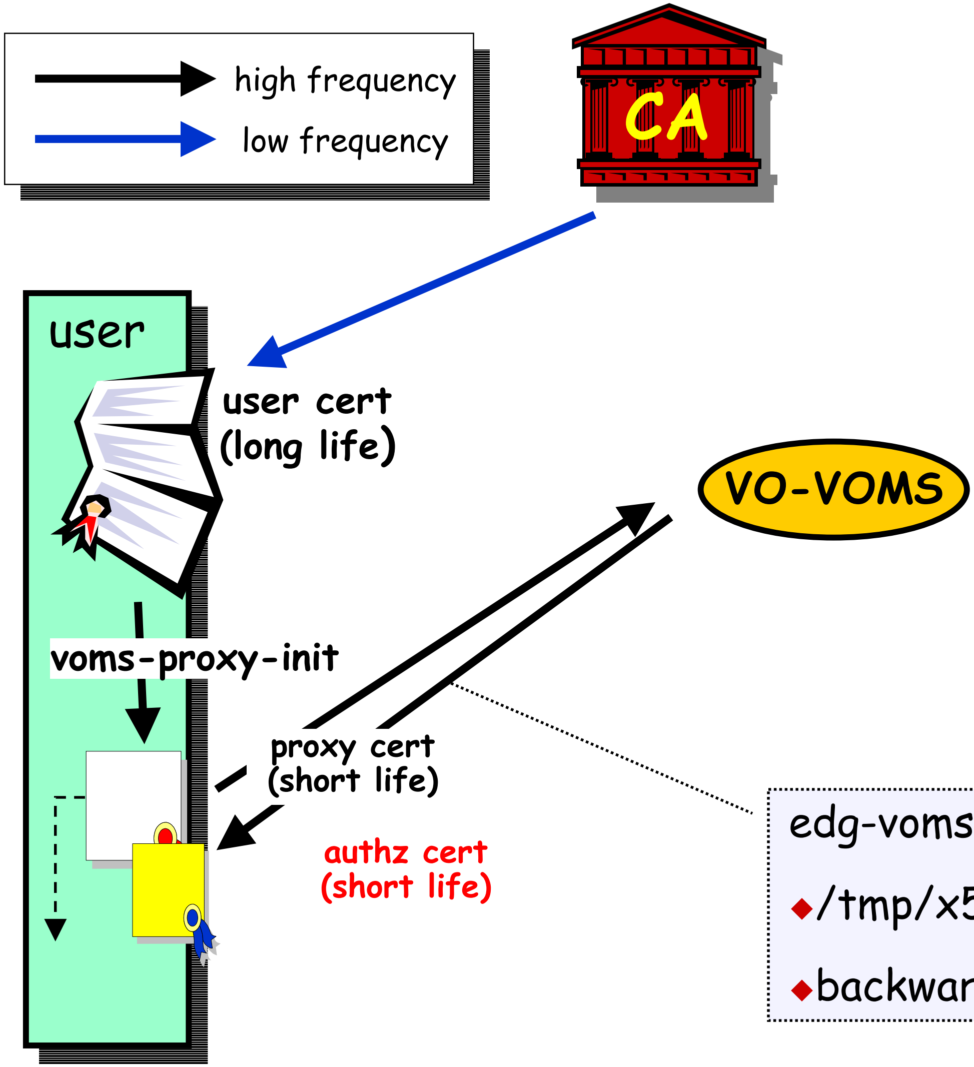
edg-java-security (WP2)

- Trust manager
  - GSI compatible authentication (supporting proxy chain)
  - Adapters to HTTP and SOAP
  - Currently deployed for Tomcat4
  - VOMS credential verification
- Authorization Manager
  - Authorization and mapping for Java services
  - Plug-in framework for maps: database, XML file and for backward compatibility: gridmap-file
  - Handles VOMS attributes

VO-LDAP *grid-mapfile* generation



VOMS “Login”

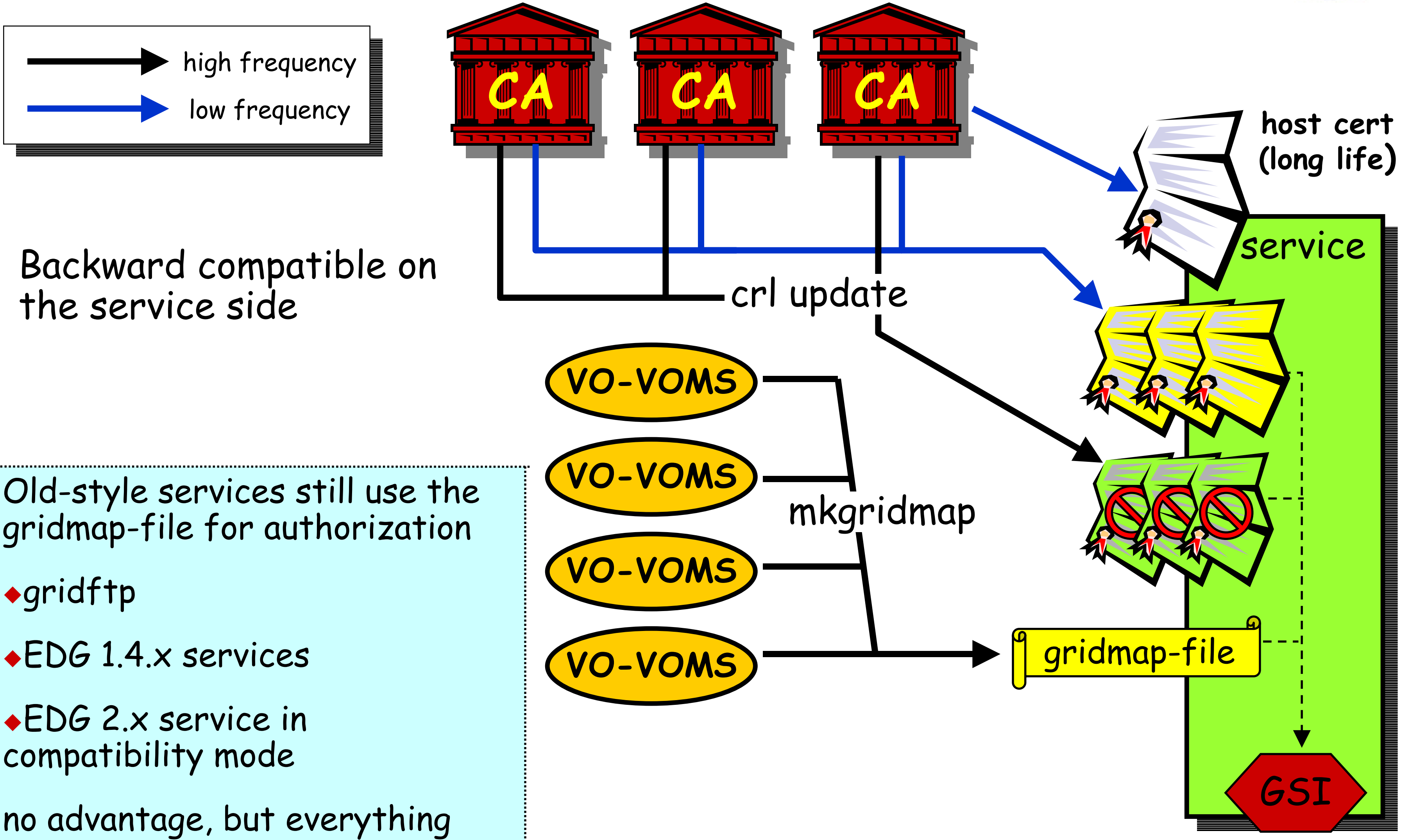


The VOMS credential is backward compatible with GSI

edg-voms-proxy-init -voms iteam

- /tmp/x509_up<UID> (normal proxy location)
- backward compatible proxy format

Old-style GSI Service



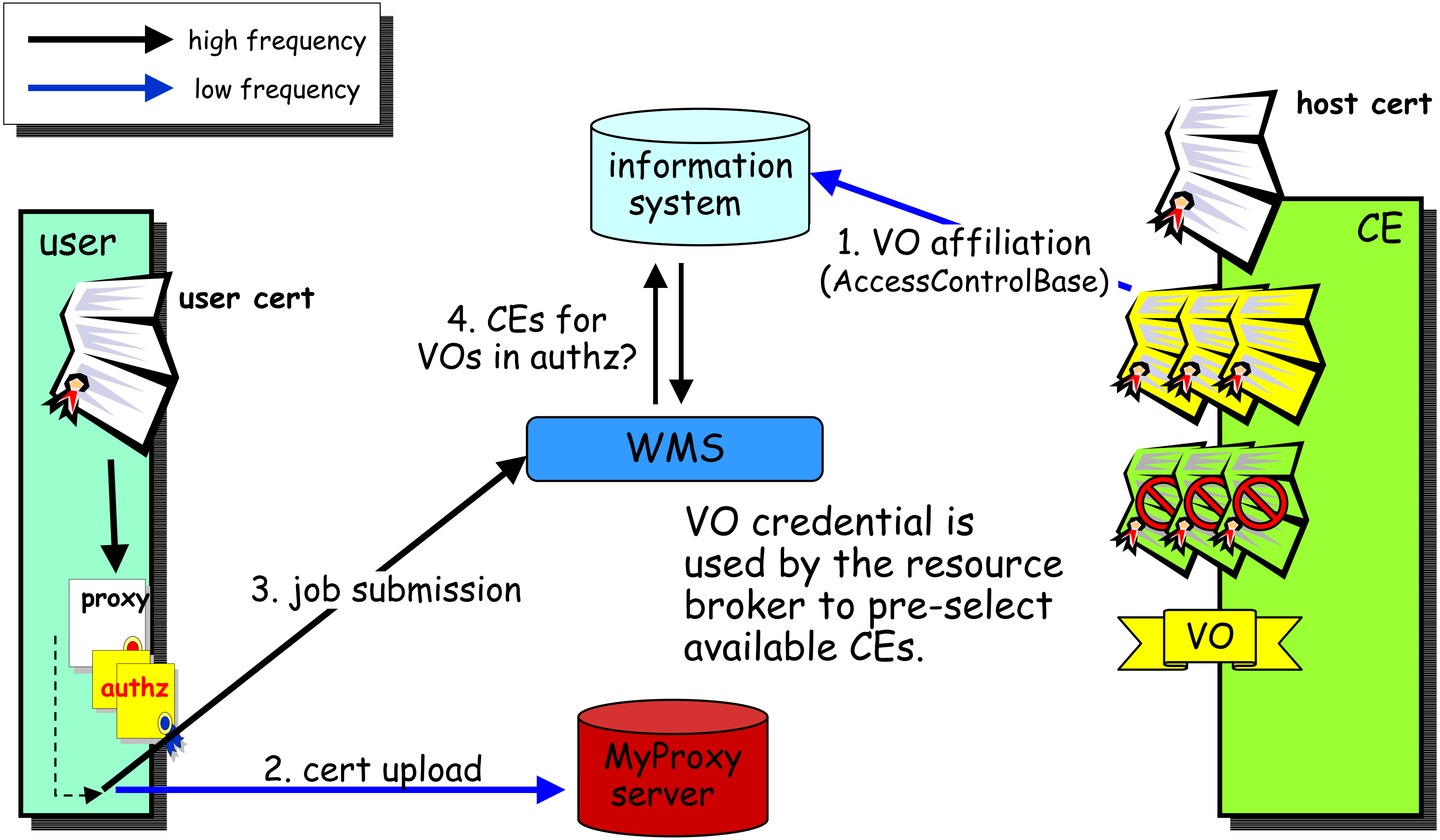
Backward compatible on the service side

Old-style services still use the gridmap-file for authorization

- gridftp
- EDG 1.4.x services
- EDG 2.x service in compatibility mode

no advantage, but everything works as before...

Job Submission



VO credential is used by the resource broker to pre-select available CEs.

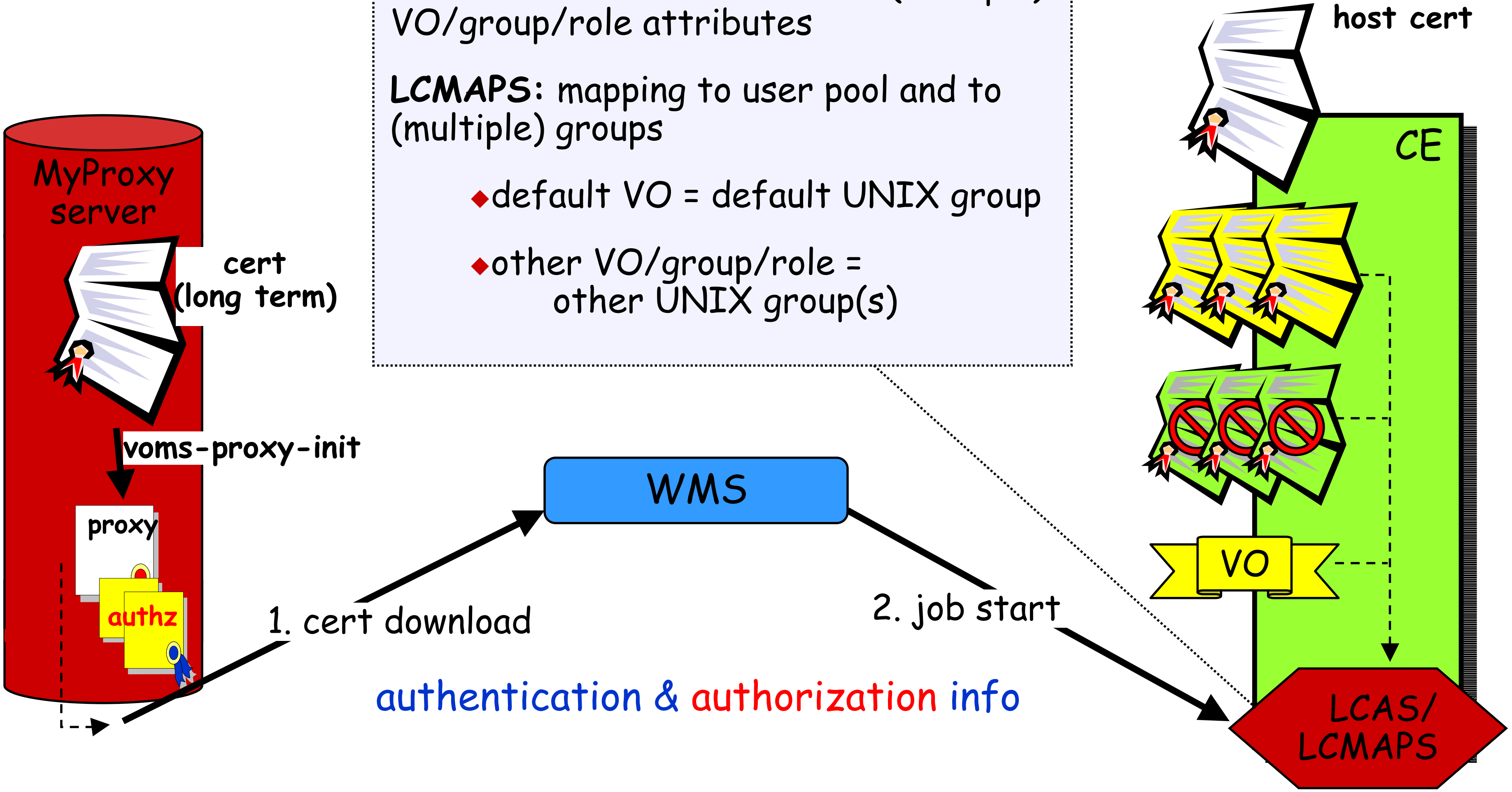
Running a Job

VO credential for authorization and mapping on the CE.

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)



authentication & authorization info

Requirements analysis (EDG 2.1)

- Only consider EDG requirements here (longer term aims: see D7.7)

- Success ←
- Mostly satisfied ←
- Not satisfied ←

	Number	FS	PS	NS
Authentication	13	11	1	1
Authorization	23	8	9	6
Confidentiality	14	1	3	10
Non-Repudiation	3			3
Usability	3	3		
Interoperability	3	2	1	
Other areas	15	3	8	4
Total	74	28	22	24

FS= fully, PS=partially, NS=not… satisfied

“Partially” means not all WPs and/or not all languages

Requirements - comments

- Authentication
  - The EDG PKI is a major success
    - Except for 1 “NS”, i.e. revocation in < 10 minutes
- Authorization
  - Another major success of the project
    - But not all components are fully deployed and/or configured
  - “NS” requirements are related to
    - Assigning job priorities and pre-checking fine-grained access (WP1)
    - Authorization of resources rather than users (WP10)
- Confidentiality
  - “NS” requirements are related to
    - Encryption/decryption and fine-grained access control to files/keys
    - Concealing information about users and audit data

Bio-medical confidentiality

- Requires fine-grained AuthZ on files and encryption keys (in RMC)
  - A solution is described in D7.6 design document
- Many components implemented and deployed
  - Shown to work independently
  - Sufficient to fulfil some application requirements
- Only partial integration into EDG release 2.1 was possible
  - Difficult to integrate security into existing systems
  - Difficult priority decisions were taken by the project management
  - Stability more important than functionality
- We *have* successfully integrated fine-grained AuthZ in Job submission
  - fine-grained AuthZ on SE and RM not yet deployed/configured
- Medium-grained AuthZ (group level) on files is achievable
- But fine-grained AuthZ requires more development and integration

Lessons learned

- In hindsight, the D7.5 requirements were rather ambitious
  - The expectations of the applications were documented but there was not sufficient analysis of the difficulty of integration
- SCG started late (as defined in the TA)
  - Most done by unfunded effort
  - And/or collaboration with other projects
- Integration of security into existing systems is complex
- Security **must** be an integral part of all development
  - From the start!
- In future projects, there must be a WP dealing with security
- EGEE has benefited from our experience

Future & Exploitation

- Authentication
  - The CA infrastructure will continue – a general service for EU Grid
  - EGEE will manage the EDG PKI in a new EU PMA
  - LCG driving the requirements for global physics authentication
  - Grid CAs to be registered in new TERENA CA repository (TACAR)
  - eInfrastructure and eIRG meetings (Ireland) to consider this topic
  - DataGrid people will continue in EGEE and GGF CAops group and gridpma.org
- Security Policy issues
  - DataGrid people already active in defining LCG policy and procedures
  - Useful input to EGEE and eIRG

Future & Exploitation (2)

- Authorization
  - Components and people will continue in EGEE, LCG and other projects
  - VOMS is part of LCG-2
    - The HEP applications need roles and groups
  - Work in GGF security area groups will continue
    - EDG providing reference implementations
  - Web services, VOMS, LCAS, GridSite, SlashGrid etc in GGF OGSA-AUTHZ
    - XML policy, XACML specs for AuthZ, VOMS Attribute Certificates, …
    - Will drive and track standards
- Two papers will be submitted for publication in Grid journal

Concluding comments

Is a summary needed?

- Thanks to all members of SCG (names them?)
- Thanks to all CA colleagues (US, Asia,…)
- Thanks to DataTAG, GridPP etc.

Thanks to the EU and our national funding agencies for their support of this work