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 work
- Exploitation
- Summary

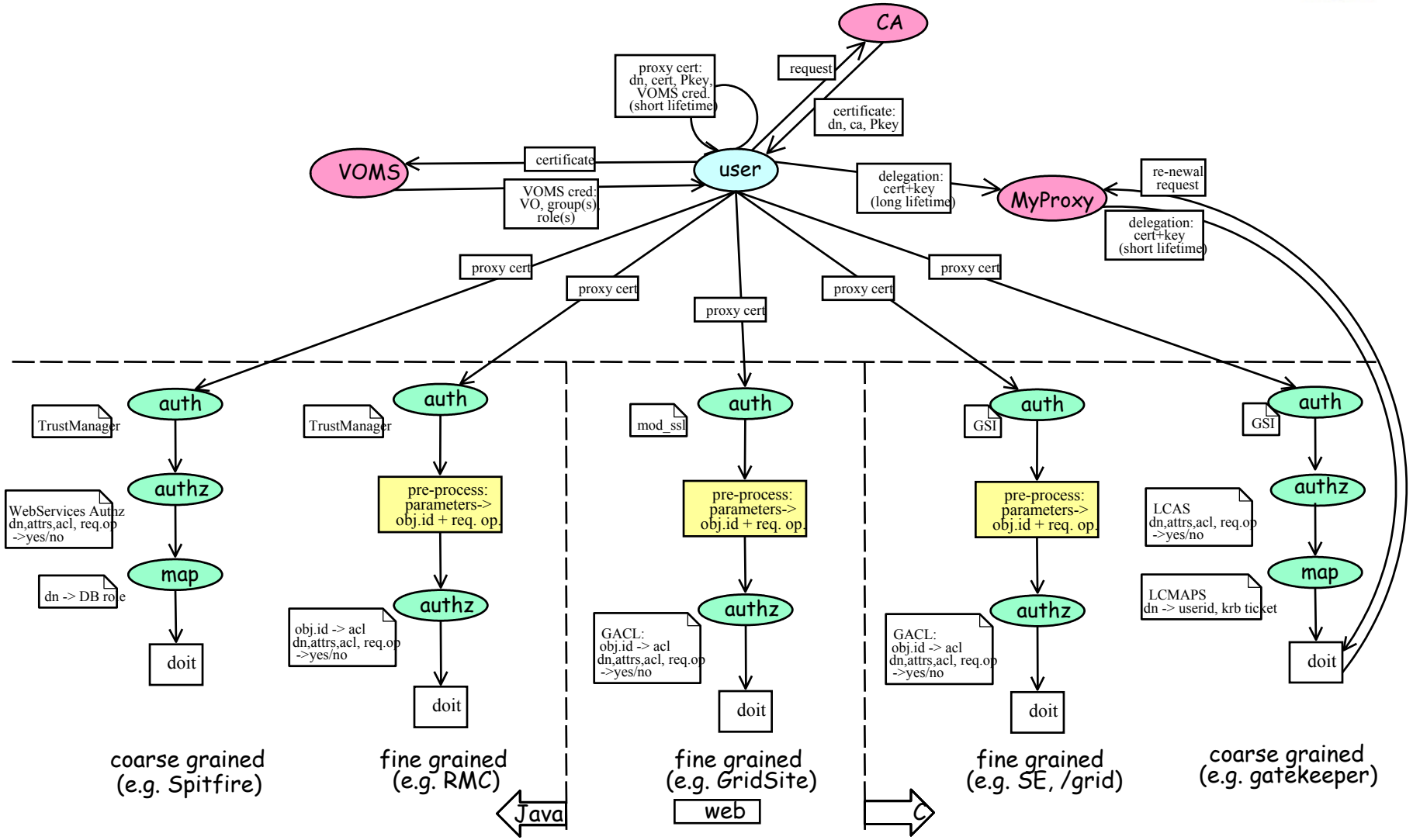
SCG Objectives

- No single work-package to tackle Grid security
  - But 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)
- SCG has larger scope than foreseen in TA task 7.4
  - At least one representative per middleware WP
  - Collaboration with DataTAG and national Grid projects

SCG Achievements - overview

- Authentication: Certification Authorities (CAs) 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 joint meetings with WP8, 9 and 10 for VO use cases
- Security Design (D7.6, March 2003)
- Successful implementation, integration and deployment of many security components
- Final Security Report (D7.7, January 2004)
  - includes comparison with initial requirements

Overview of the EDG Security Components (D7.6)



Authentication

A PKI with 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 many 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 policy and procedures (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
- Concerns about scalability
  - Regional Policy Management Authorities (PMA)
  - CAs could be run by NRENs

Approved CAs

- Certification Authorities
  - 21 CAs span:
    - Europe
    - North America
    - Asia
  - ~ 3000 certificates issued
- "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) overview

- The Authorization model
  - Build on the GSI-based authentication
  - *Global* AuthZ by one or more VOs
  - *Local* site/resource-based AuthZ
- Early DataGrid VO management system: "VO-LDAP"
  - System for easy management of grid-mapfiles
- New DataGrid AuthZ system: VOMS
- policy or ACL based local access control
  - coarse and fine grained solutions
- DataGrid security components:
  - GSI/LCAS/LCMAPS for C/C++ services
  - edg-java-security for Java web services
  - mod_ssl/GACL for Apache based web services
- Services can either use the grid-mapfile or use VOMS credentials
- Modified MyProxy service for credential renewal (incl AuthZ)

Virtual Organization Membership Service (VOMS)

- Joint development with DataTAG
- Issues signed credentials to prove group/role/VO membership
  - Moved to standard RFC 3281 Attribute Certificate format
- The AC is included as a non-critical extension of the user's proxy certificate
  - Backwards compatible
- Core service: standalone daemon for the "login"
  - Administered by the VO manager
- Administrative service: web service with API, command line and web user interface
  - for administration and registration
- VOMS migration tools for grid-mapfiles and VO-LDAP servers

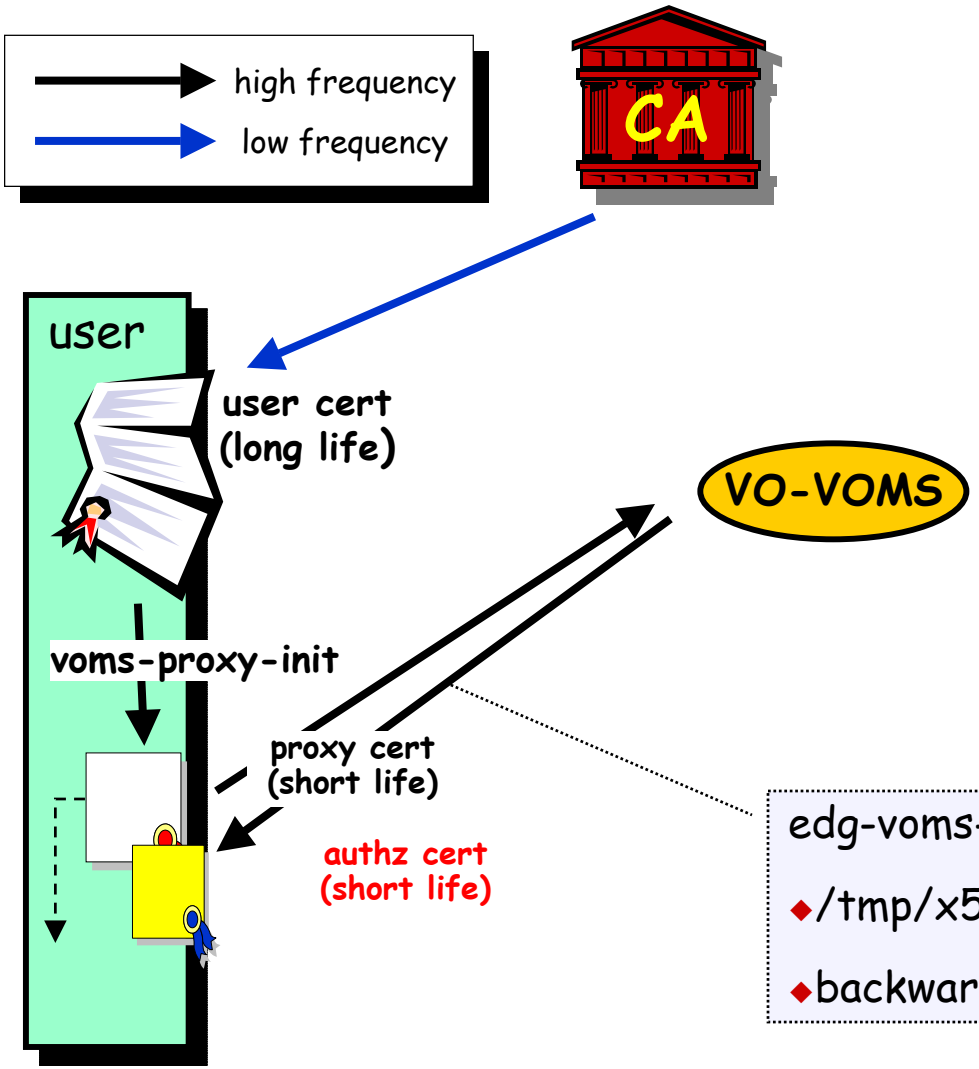
Local Site Authorization (WP4)

- Local Centre Authorization Service (**LCAS**)
  - Handles authorization requests to local fabric
    - decisions based on user proxy 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
- Authorization Manager
  - Authorization and mapping for Java services
  - Plug-in framework for maps: database, XML file and for backward compatibility: grid-mapfile
  - Handles VOMS AuthZ attributes

VOMS "Login"

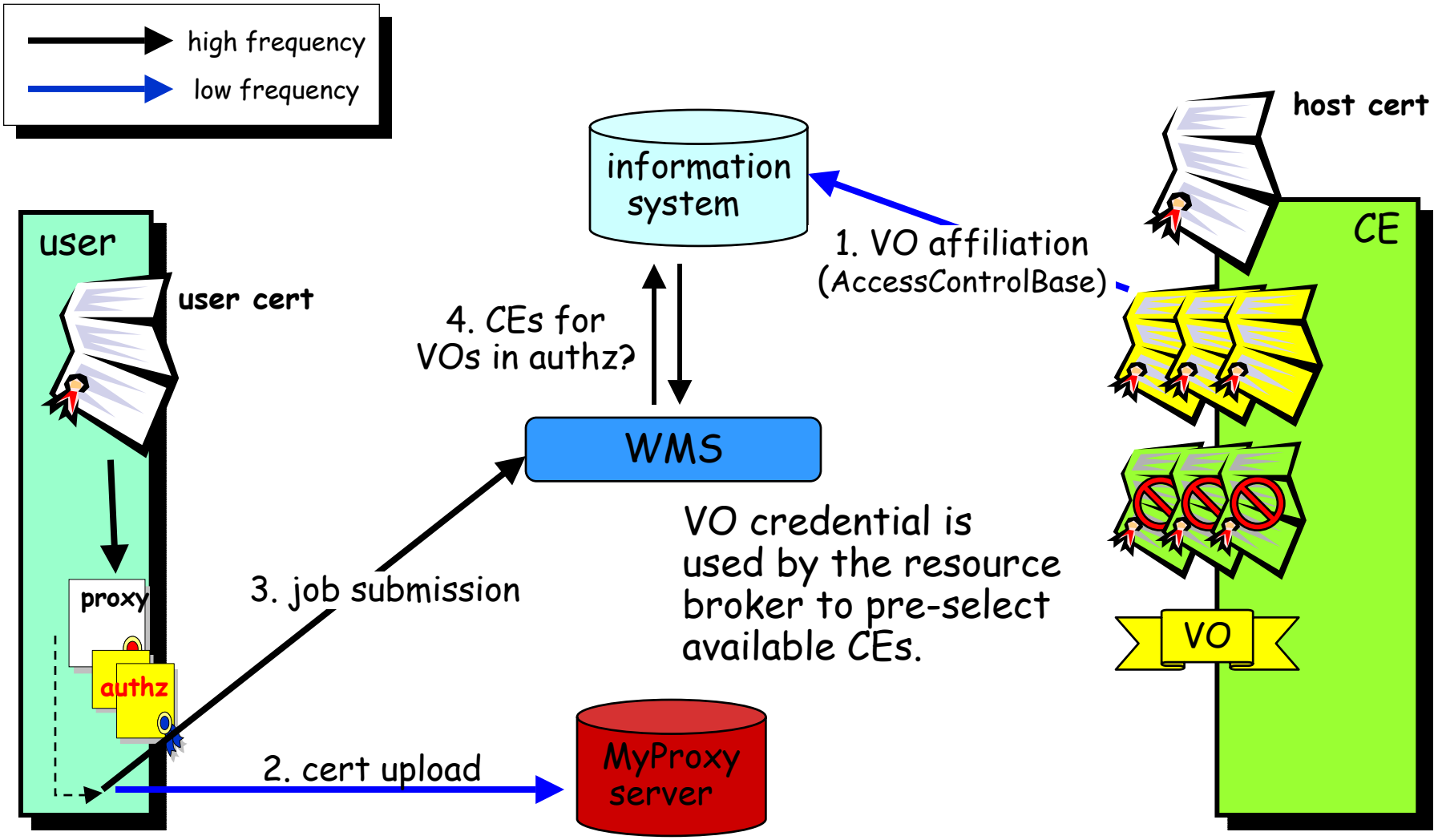


The VOMS credential is backward compatible with GSI

edg-voms-proxy-init -voms iteam

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

Job Submission



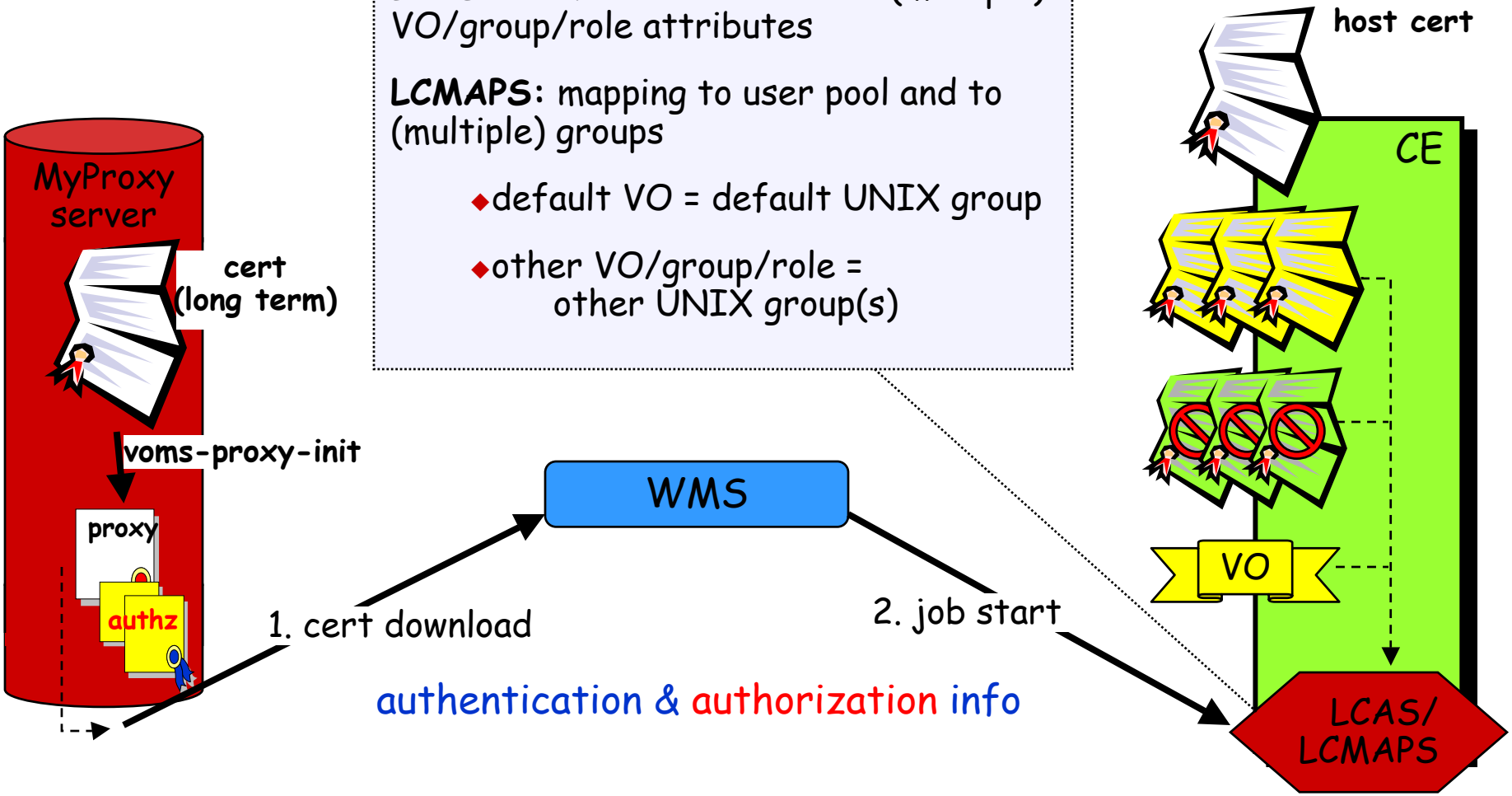
Running a Job

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)



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" (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 (mainly WP10)
    - Encryption/decryption and fine-grained access control to files/keys
    - Concealing information about users and audit data
- The DataGrid design and implementation is aimed at meeting all requirements and prototyping secure services
  - towards industrial strength

Bio-medical confidentiality

- Requires
  - encryption of the anonymized medical image (when outside the hospital)
  - fine-grained AuthZ on files and encryption keys (in LRC)
- See D7.6 for more details of the design
- Many of these components are implemented and deployed
  - Shown to work independently and meet the requirements
- But 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
  - But fine-grained AuthZ on SE files not yet configured
- Fine-grained access control to the encryption key and patient data in the metadata catalogue requires more work

Lessons learned

- Be careful collecting requirements
  - 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
- Security must be an integral part of all development
  - from the start
  - Larger scope SCG started late (but as defined in the TA)
- Building and maintaining "trust" between projects and continents takes time
- Integration of security into existing systems is complex
- There must be a dedicated activity dealing with security
- EGEE planning has already benefited from our experience

Future work

- Authentication
  - Continue and expand the EDG PKI
  - Secure credential management: online services, SmartCards
  - Faster and more robust certificate revocation, e.g. OCSP
- Authorization
  - Fuller use of VOMS AuthZ credentials
  - Mutual AuthZ: VOs should approve resources and services
  - Convergence with GGF standards (XACML, SAML, …)
- Restricted delegation
- Confidentiality
  - Integrate and deploy the proposed solution for WP10
- Build on DataGrid design and components for industrial strength
  - PKI/SSL authentication, standards-based authorization, ws-security,…

Exploitation

- Authentication
  - The CA infrastructure will continue
    - Discussions started with DEISA and SEEGRID
  - 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
    - A general EU Grid PKI infrastructure?
  - DataGrid people will continue in EGEE and GGF
- Security Policy issues
  - DataGrid people already active in defining LCG policy and procedures
  - Important input to EGEE and eIRG

Exploitation (2)

- Authorization
  - EDG components and people will continue in EGEE, LCG and other projects
  - VOMS is part of LCG-2
    - The HEP applications need roles and groups
  - Integration with SlashGrid, ACLs (GACL) and GridSite
    - Joint work with UK GridPP, using VOMS and working with PERMIS team
  - Work in GGF security area groups will continue
    - EDG providing reference implementations in OGSA-AuthZ
    - WS-security, VOMS, LCAS, GridSite, SlashGrid etc
    - XML policy, XACML, VOMS Attribute Certificates, SAML
    - Will continue to drive and track standards
- Publication of the work is ongoing

Summary

- Authentication
  - We have built a large Grid PKI used by many EU projects
  - strong links to North America and Asia
  - support for global applications
- Authorization
  - DataGrid has made major contributions in this area
  - Established the VO as an important security domain
- Future work & exploitation
  - Much still to be done in Grid security
  - The people will continue in EGEE and elsewhere
  - DataGrid security architecture, design and components will be used