Managing Dynamic User Communities in a Grid of Autonomous Resources

Vincenzo Ciaschini
Vincenzo.Ciaschini@cnaf.infn.it

http://grid-auth.infn.it/docs/chep2003.pdf

Talk Outline

- Introduction
- Authorization requirements
- VO Membership Service
- Local site enforcement mechanisms (LCAS, LCMAPS)
- Spitfire TrustManager
- Conclusions

Authors

A. Frohner – CERN
D. Kouril - CESNET
F. Bonnassieux - CNRS
R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Gianoli , F. Spataro - INFN
O. Mulmo – KDC
D. Groep – NIKHEF
L. Cornwall, D. Kelsey, J. Jensen – RAL
A. McNab – University of Manchester
P. Broadfoot, G. Lowe – University of Oxford

Introduction (1)

- **EDG security infrastructure based on X.509 certificates (PKI)**
- **Authentication**
  - 16 national certification authorities
  - Policies and procedures → mutual thrust
  - Users identified by certificates signed by their national CA
- **Authorization**
  - Cannot decide Authorization for grid users only on local site basis
  - At least 2 entities involved
    - Resource Providers (e.g. Tiers in LCG framework)
    - Virtual Organizations (e.g. LHC experiments collaborations)

Introduction (2)

Authorization (cont.)

- Resource granting established by agreements VO’s - RP’s.
  - VO’s administer user membership, roles and capabilities
  - RP’s evaluate authorization granted by VO to a user and map into local credentials to access resources
    - Trust/Authorization Manager for Java (e.g. Spitfire)
    - LCAS/LCMAPS for farms
    - SlashGrid for storage (Andrew’s talk)
- Need tool to manage membership for large VO’s (10000 users)
  - Globus mechanism (grid-mapfile) not scalable
- VO membership service (VOMS)
  - Extends existing grid security infrastructure architecture with embedded VO affiliation assertions
  - Permits authorization control on grid services for job submission, file and database access.

Authorization requirements

- **Architecture**
  - centralized and scalable (for an Auth policy VO based)
- **Attributes support**
  - group membership (subgroup, *multiple inheritance*, ..)
  - Roles (admin, student, ..), capabilities (free form string), ..
  - Temporal bounds
- **Resource Provider**
  - keep full control on access rights
  - traceability user level (not VO level)
- **Security issues**
  - Auth Server must not be a Single point of failure
  - Auth communications must be trusted, secured and reserved

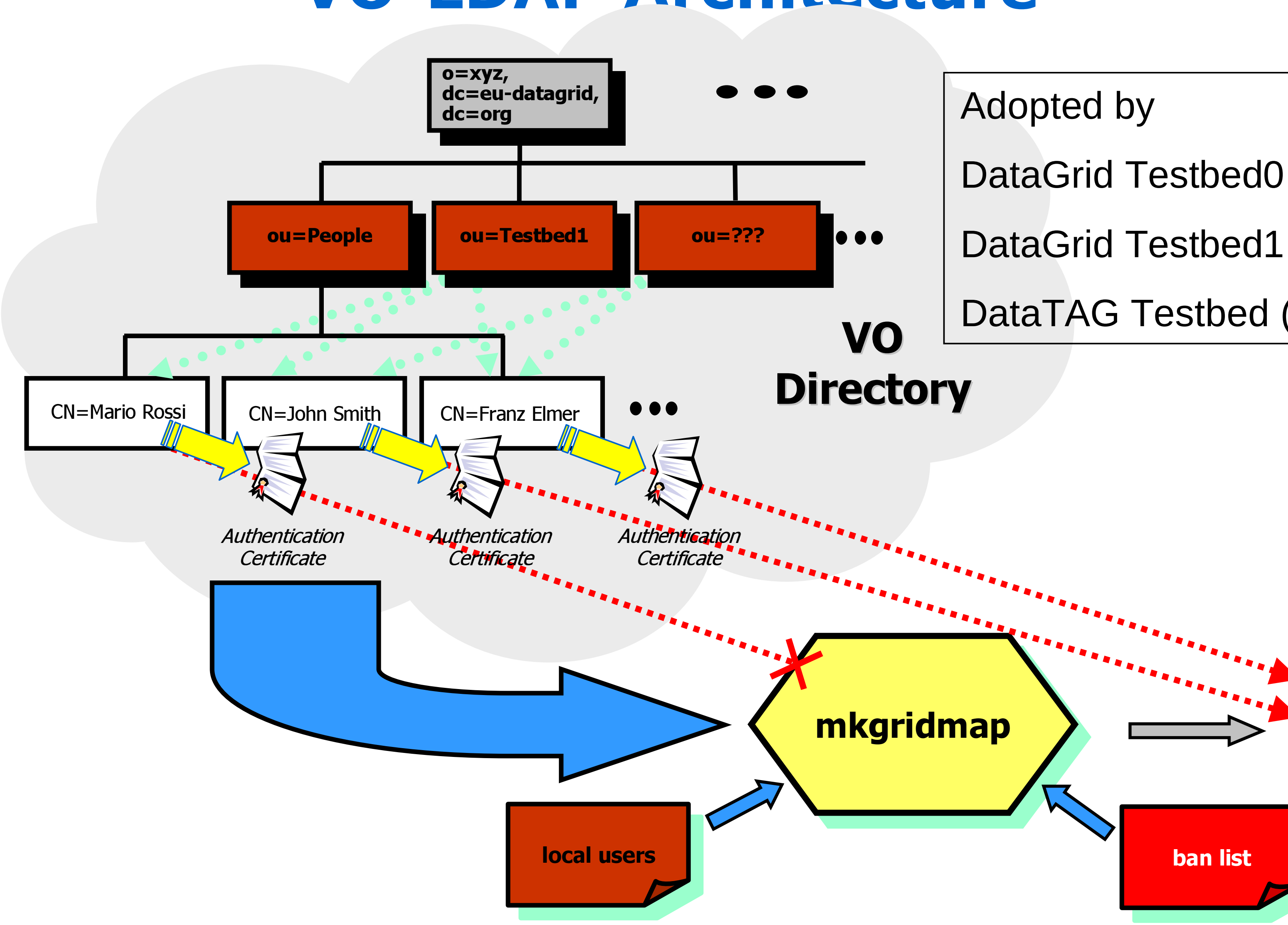
Globus Authorization Mechanism

- **grid-mapfile**
  - Grid credentials (user’s Certificate) to local credentials (unix account) mapping
  - “Boolean” authorization
  - Information provided via VO-LDAP servers
  - Managed “manually” by the resource admin (via mkgridmap)

```
"/C=IT/O=INFN/L=Parma/CN=Roberto Alfieri/Email=roberto.alfieri@pr.infn.it" alfieri
"/C=IT/O=INFN/L=Parma/CN=Fabio Spataro/Email=fabio.spataro@pr.infn.it" spataro
```

- **No centralization**
- **No scalability**
- **Lack of flexibility**

VO-LDAP Architecture



Adopted by

DataGrid Testbed0 (2001/02)

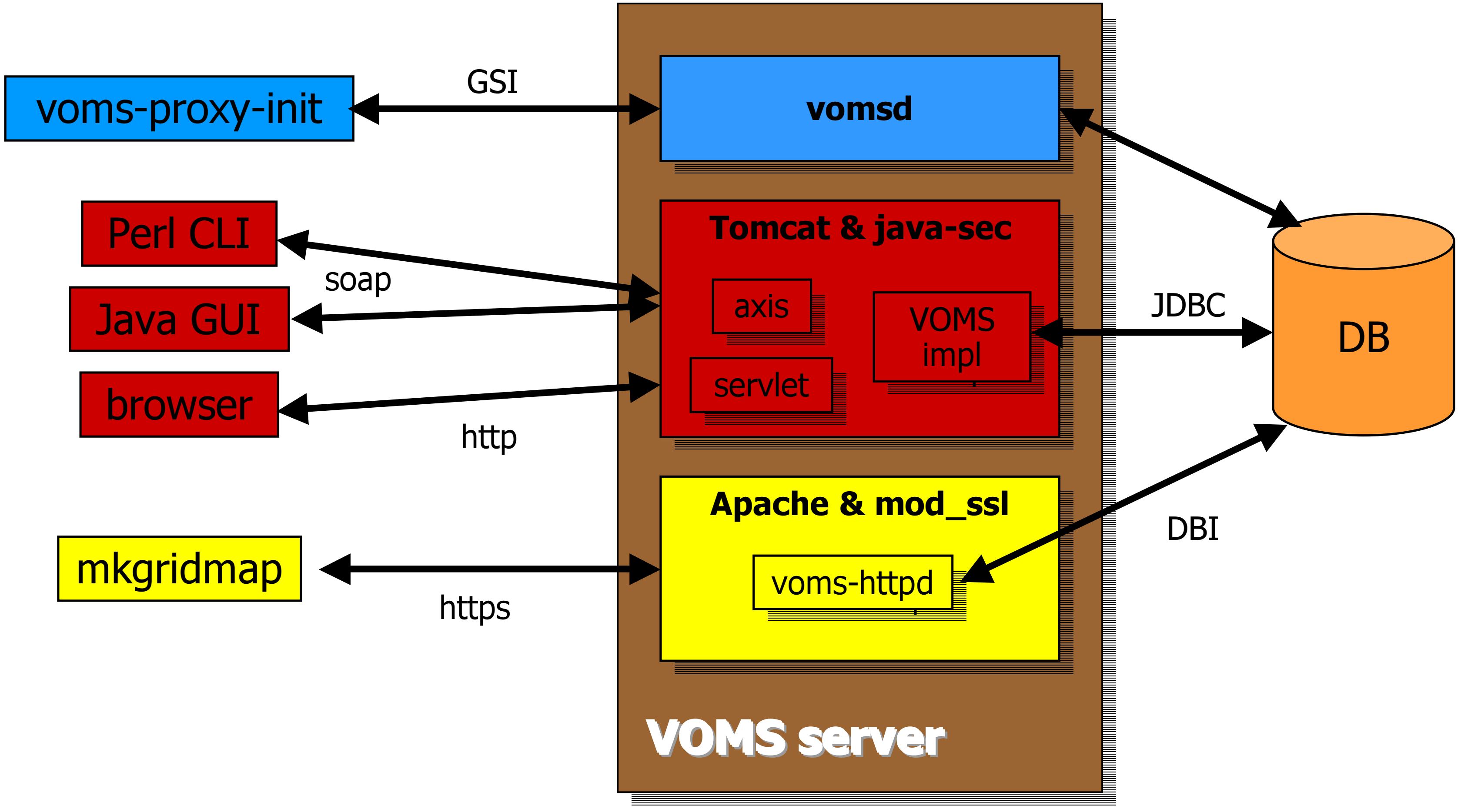
DataGrid Testbed1 (2003)

DataTAG Testbed (2003)

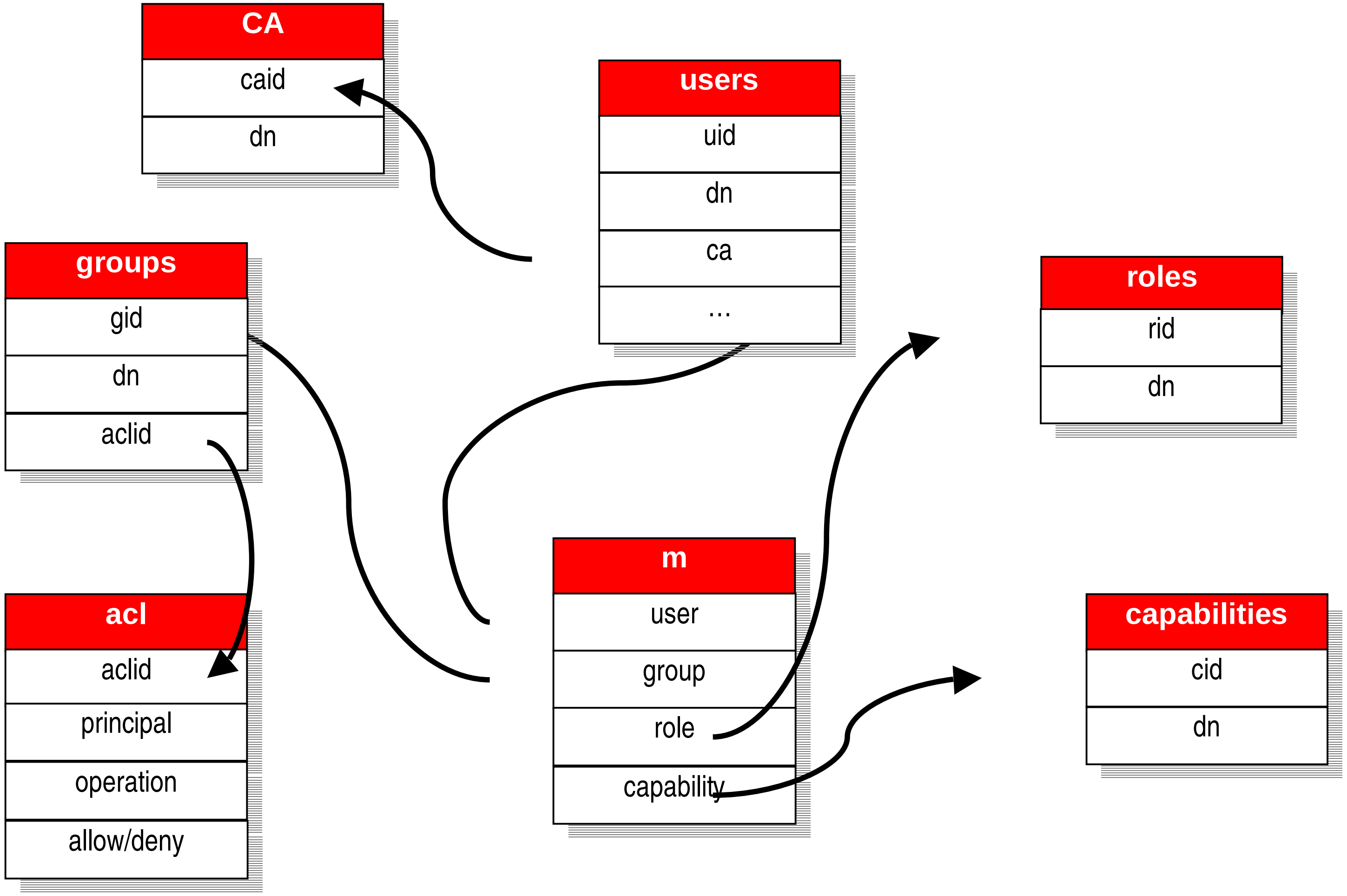
The Virtual Organization Membership Service

- **The Virtual Organization Membership Service (VOMS)**
  - Developed by European Datagrid and Datatag collaborations to solve current LDAP VO servers limitations
  - Grants authorization data to users at VO level
    - Each VO has its own VOMS
    - Support for group membership (subgroup, *multiple inheritance*, ..), "forced" groups (i.e. for negative permissions), roles (admin, student, ..) and capabilities (free form string)
  - Essentially a front-end to an RDBMS
    - User client – queries the server for authorization info
    - User server – returns authorization info to the client
    - administration client – used by VO administrators for management
    - administration server – executes client update operations on db
    - transition tool – interface to mkgridmap++ (see below)
  - All client-server communications are secured and authenticated
  - Authorization info is processed by the gatekeeper
    - full functionality of VOMS achieved via LCAS/LCMAPS plug-ins (see below)

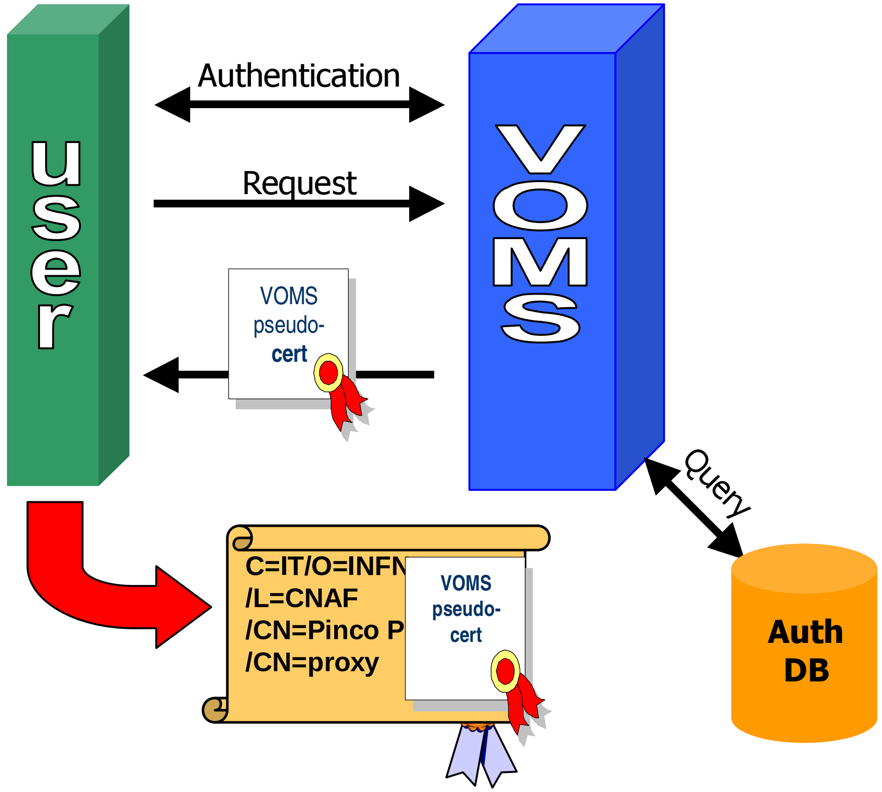
VOMS overview



DB Structure (simplified)



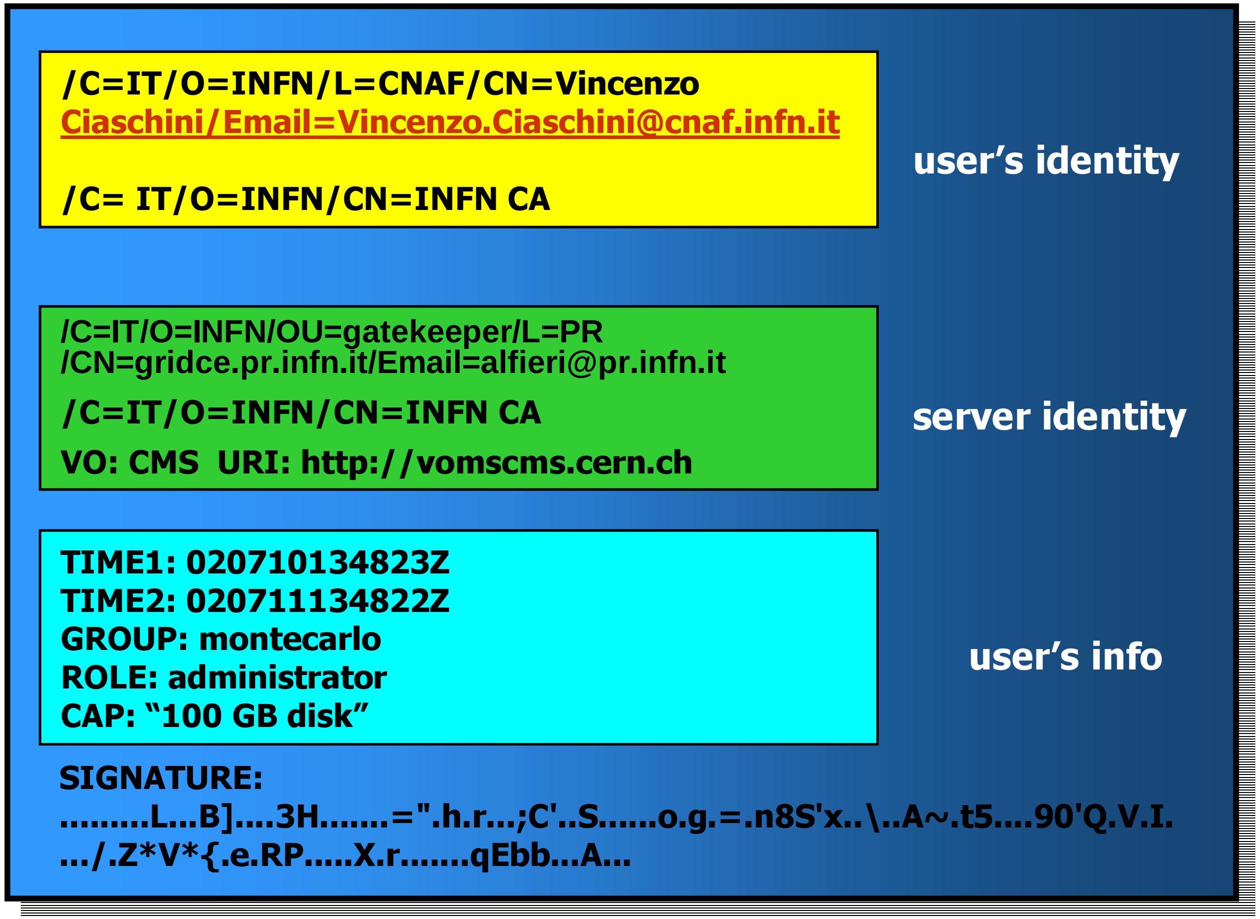
VOMS Operations



1. Mutual authentication Client-Server
   - Secure communication channel via standard Globus API
2. Client sends request to Server
3. Server checks correctness of request
4. Server sends back the required info (signed by itself) in a “Pseudo-Certificate”
5. Client checks the validity of the info received
6. Client repeats process for other VOMS’s
7. Client creates proxy certificates containing all the info received into a (non critical) extension
8. Client may add user-supplied auth. info (kerberos tickets, etc…)

Pseudo-Certificate Format

- The pseudo-cert is inserted in a non-critical extension of the user's proxy
  - 1.3.6.1.4.1.8005.100.100.1
- It will become an Attribute Certificate
- One for each VOMS Server contacted



/C=IT/O=INFN/L=CNAF/CN=Vincenzo Ciaschini/Email=Vincenzo.Ciaschini@cnaf.infn.it

/C= IT/O=INFN/CN=INFN CA

user's identity

/C=IT/O=INFN/OU=gatekeeper/L=PR /CN=gridce.pr.infn.it/Email=alfieri@pr.infn.it

/C=IT/O=INFN/CN=INFN CA

VO: CMS URI: http://vomscms.cern.ch

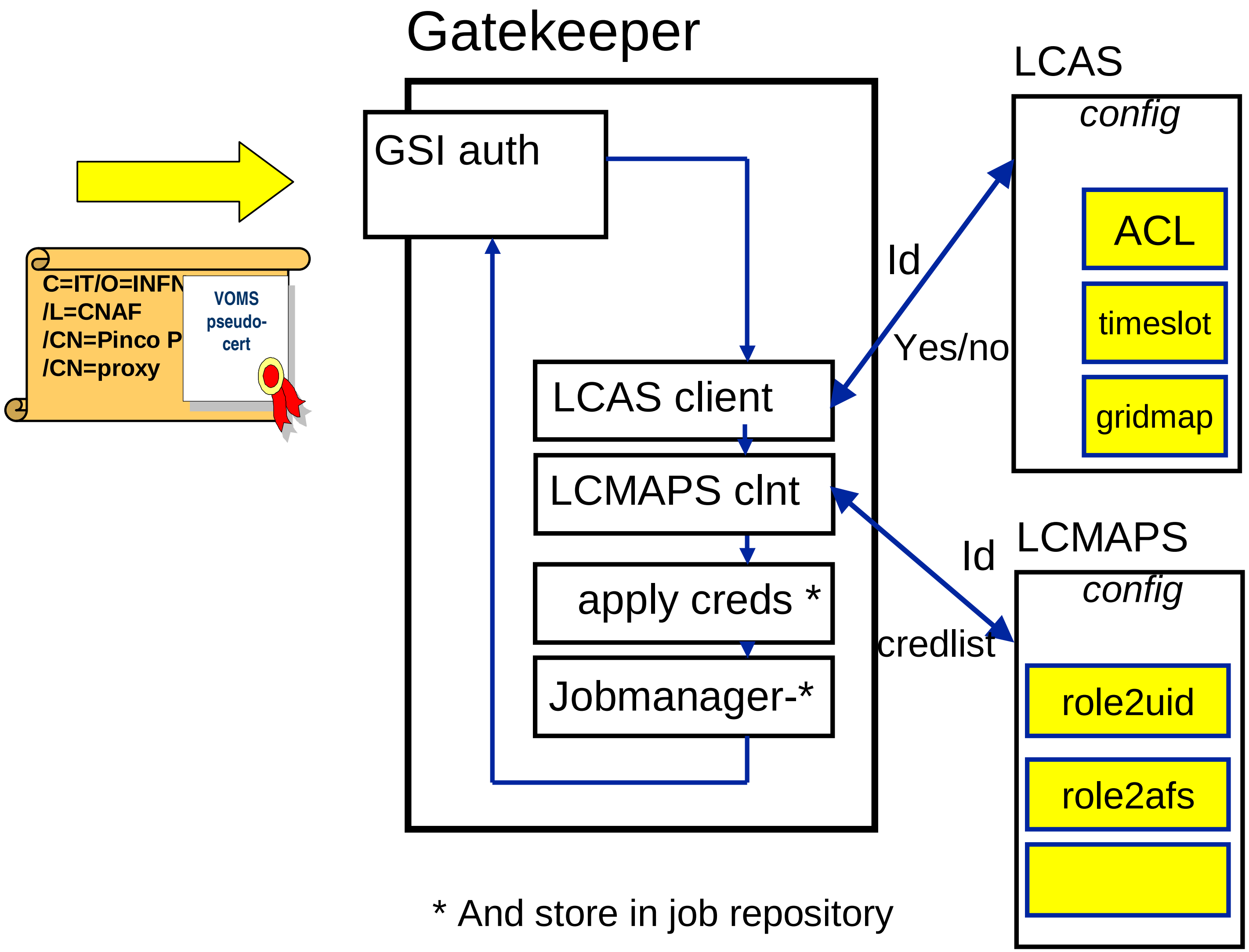
server identity

TIME1: 020710134823Z
TIME2: 020711134822Z
GROUP: montecarlo
ROLE: administrator
CAP: "100 GB disk"

user's info

SIGNATURE:
.........L...B]....3H.......=".h.r...;C'..S......o.g.=.n8S'x..\..A~.t5....90'Q.V.I.
.../.Z*V*{.e.RP.....X.r.......qEbb...A...

EDG gatekeeper



* And store in job repository

Local Site Authorization Services

Local Centre Authorization Service (LCAS)

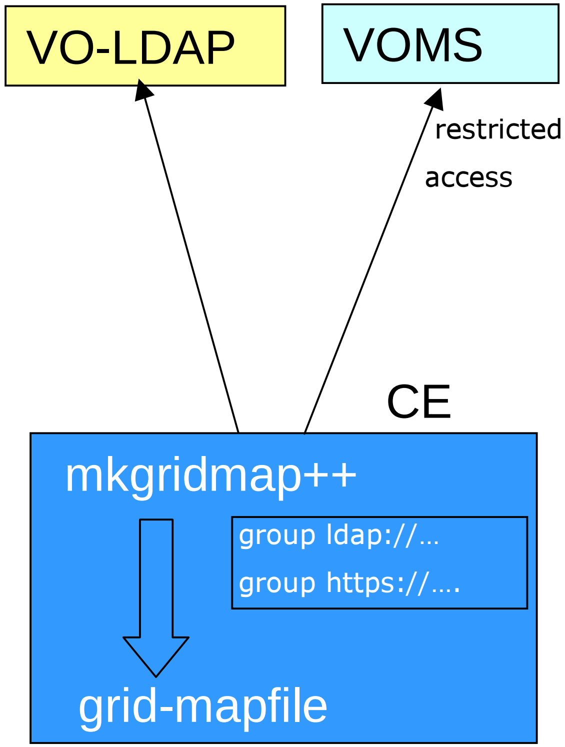
- Handles authorization requests to local fabric
  - Authorization decisions based on proxy user certificate and job specification
  - Supports grid-mapfile mechanism
- Plug-in framework (hooks for external authorization plug-ins)
  - Allowed users (grid-mapfile or allowed_users.db)
  - Banned users (ban_users.db)
  - Available timeslots (timeslots.db)
  - Plugin for VOMS (to process Authorization data)

Local Credential Mapping Service (LCMAPS)

- Provides local credentials needed for jobs in fabric
- Plug-in framework
- Mapping based on user identity, VO affiliation, site-local policy
- Replace Gridmapdir, but keep functionality
- Supports standard UNIX credentials, pool accounts (Gridmapdir)

mkgridmap++

- **Need for a tool for the transition to LCAS/LCMAPS mechanism**
- **VOMS and VO-LDAP can and MUST coexist**
  - VOMS can also be used for grid-mapfile generation.
  - New directive in the config file
- **New feature**
  - Authenticated access to VOMS (*not LDAP*) servers based on https protocol to restrict the clients allowed to download the list of the VO members



Spitfire

- **Provides uniform access to various implementations of database back ends via a grid-enabled front end**
  - SOAP interface
  - JDBC interface to RDBMS
- **TrustManager: certificate validator for Java services**
  - Permits (mutual) secure client-server authentication
  - Supports X509 certificates and CRL's
- **Support for connections via HTTP(S) using GSI certificate for authentication**
- **Role-based authorization**
  - Support for Authorization info provided by VOMS

Status and Future Works

First production **VOMS version** (Client/server, Admin, mkgridmap++) released Feb. ‘03

VOMS Demo at First Datatag EU Review (CERN, March 19. 2003)

Work in progress

- **VOMS**
  - Certificates will be substituted by Attribute Certificates (RFC3281)
  - Support for time cyclic/bound permissions and roles
  - Database Replication
- **LCAS/LCMAPS**
  - Plug-in framework
  - Plug-in for VOMS

More Informations

VOMS

Web site http://grid-auth.infn.it/

CVS site http://cvs.infn.it/cgi-bin/cvsweb.cgi/Auth/

Developers' mailing list sec-grid@infn.it

LCAS-LCMAPS

Web site http://www.dutchgrid.nl/DataGrid/wp4/

CVS site http://datagrid.in2p3.fr/cgi-bin/cvsweb.cgi/fabric_mgt/gridification/lcas/

http://datagrid.in2p3.fr/cgi-bin/cvsweb.cgi/fabric_mgt/gridification/lcmaps/

Spitfire

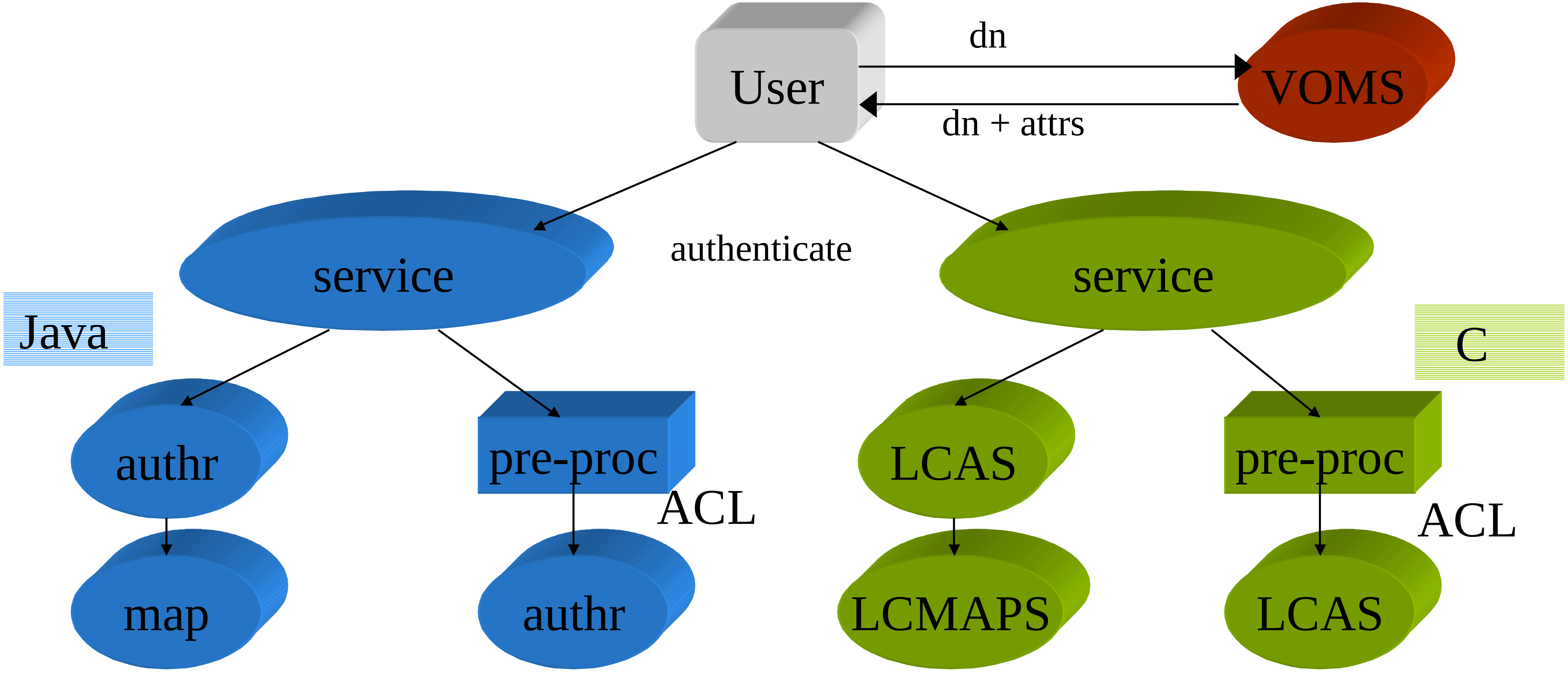
Web site http://spitfire.web.cern.ch/Spitfire/

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

Related Works

- **CAS (Globus Team)**
  - Proxy generated by CAS server, not by user (difficult traceability)
  - Proxy not backward compatible
  - Attributes are permissions (resources access controlled by VO)
- **Permis (Salford Univ., England)**
  - AC’s stored in a repository at the local site
  - Good policy engine
  - VOMS complementary (flexible VOMS AC + PERMIS pol. engine)
- **Akenti (US Gov.)**
  - Target Web sites, not easy migration in a VO environment

Authorization



Coarse-grained
e.g. Spitfire

Fine-grained
e.g. RepMeC

Coarse-grained
e.g. CE, Gatekeeper

Fine-grained
e.g. SE, /grid