# Installing a gLite VOMS server

*Joachim Flammer*

*Integration Team, CERN*

*EMBRACE Tutorial,*
*Clermont-Ferrand*
*July 2005*

www.eu-egee.org

Information Society

# Overview

- **Introduction to VOMS**
  - Features
  - Registration
  - Groups & Roles
- **Installing VOMS**
  - Reminder of gLite installation
  - Installation via apt
- **Configuring VOMS**
  - Key aspects
  - Verifying installation
- **Registering VOMS admin**
- **VOMS server web interface**
  - Groups
  - Roles
- **VOMS command line interface**
- **Known bugs**
- **Summary**

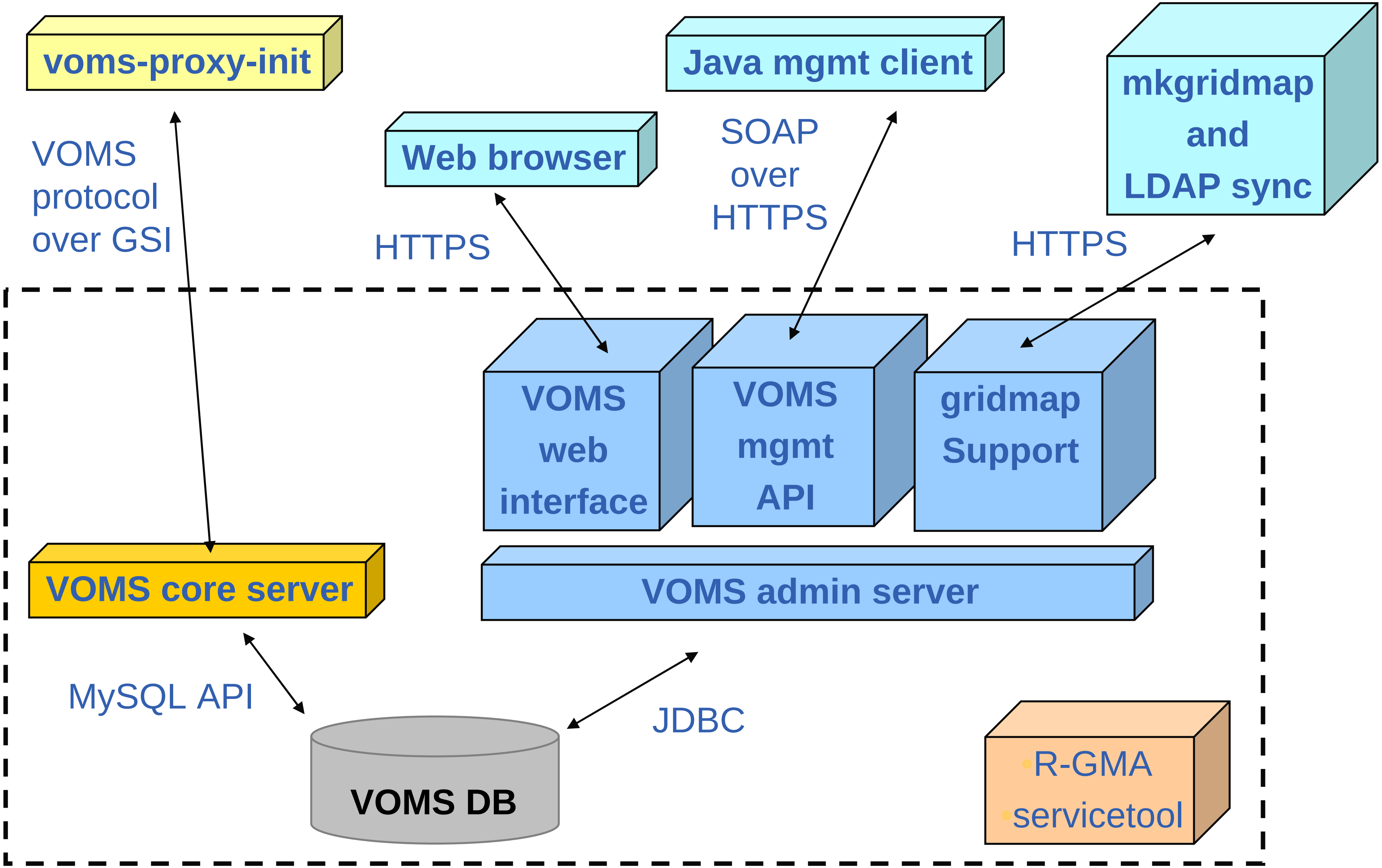
# Introduction to VOMS

- **Virtual Organization Membership Service (VOMS)**
  - Account Database
    - Serving information in a special format (VOMS credentials)
    - Can be administered via command line & via web interface
  - Provides information on the user’s relationship with his/her Virtual Organization (VO)
    - Membership
    - Group membership
    - Roles of user

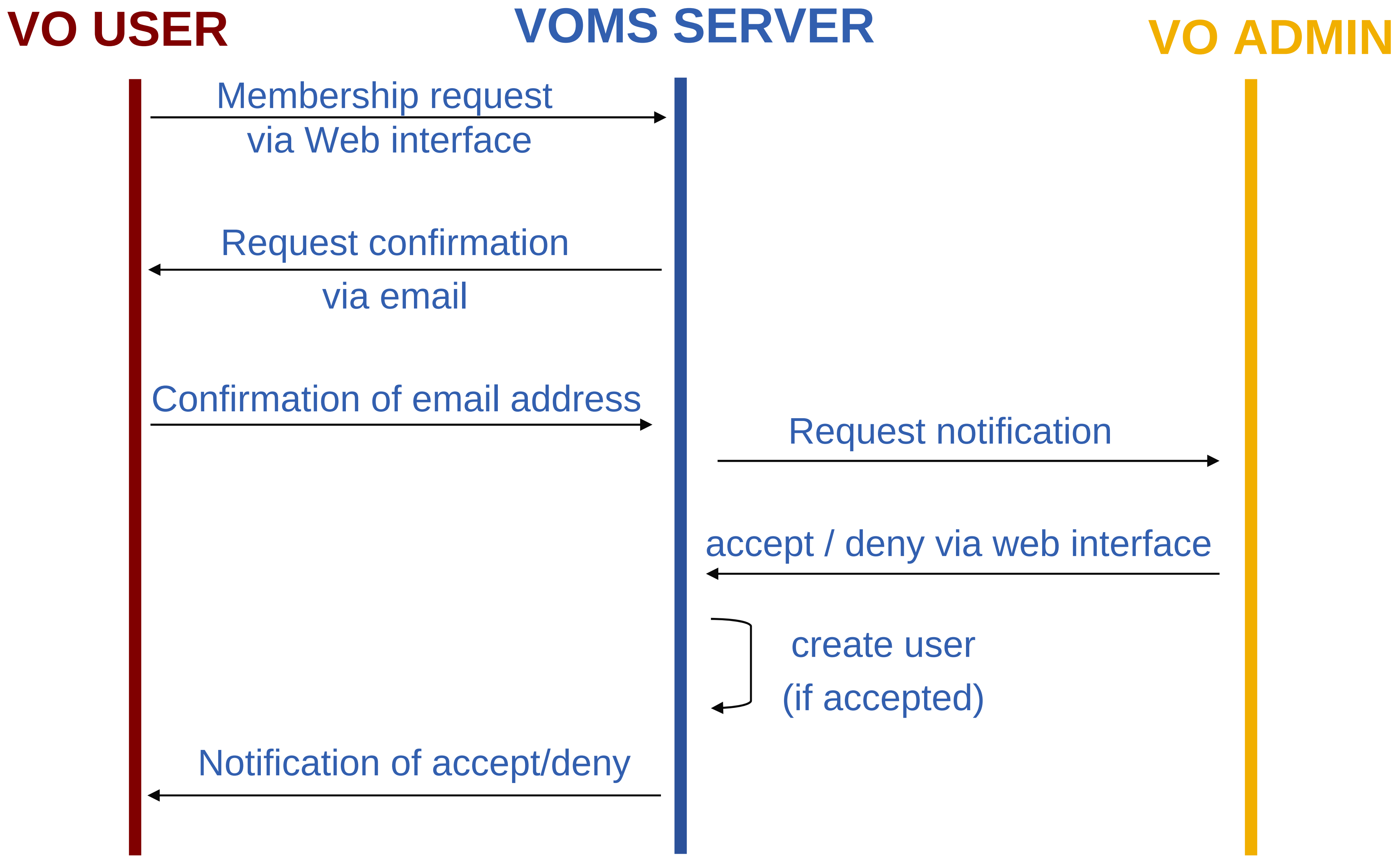
# Introduction to VOMS

- **VOMS Features**
  - Single login using (proxy-init) only at the beginning of a session
    - Attaches VOMS certificate to user proxy
  - Expiration time
    - The authorization information is only valid for a limited period of the time as the proxy certificate itself
  - Multiple VO
    - User may log-in into multiple VOs and create an aggregate proxy certificate, which enables him/her to access resources in any one of them
  - Backward compatibility
    - The extra VO related information is in the user’s proxy certificate
    - User’s proxy certificate can be still used with non VOMS-aware service
  - Security
    - All client-server communications are secured and authenticated

# VOMS architecture



# Registration process


VO USER
VOMS SERVER
VO ADMIN
Membership request via Web interface
Request confirmation via email
Confirmation of email address
Request notification
accept / deny via web interface
create user (if accepted)
Notification of accept/deny

# Groups

- **The number of users of a VO can be very high:**
  - E.g. the experiment ATLAS has 2000 member
- **Make VO manageable by organizing users in groups:**

  Examples:
  - VO BIOMED-FRANCE
    - Group Paris
      - *Sorbonne University*
        - Group Prof. de Gaulle
      - *Central University*
    - Group Lyon
    - Group Marseille
  - VO BIOMED-FRANCE
    - BIOMED-FRANCE/STAFF can write to normal storage
    - BIOMED-FRANCE/STUDENT can only to volatile space
- **Groups can have a hierarchical structure**
- **Group membership is added automatically to your proxy when doing a *voms-proxy-init***

# Groups rights

- **Assign rights to certain members of the groups**
  - using Access Control Lists (ACL) like in a file system
    - Allow / Deny
      - create/delete – controls subgroup operations
      - add/remove – controls membership operations
      - setACL/getACL – controls ACL operations
      - setDefault/getDefault – controls default membership operations
      - ALL – special permission for all operations
  - Specifying unit for entry:
    - The local database administrator
    - A specific user (not necessarily a member of this VO)
    - Anyone who has a specific VOMS attribute FQAN
    - Anyone who presents a certificate issued by a known CA (Including host and service certificates)
    - Absolutely anyone, even unauthenticated clients

# Roles

- **Roles are specific roles a user has and that distinguishes him from others in his group:**
  - Software manager
  - Administrator
  - Manager

- **Difference between roles and groups:**
  - Roles have no hierarchical structure – there is no sub-role
  - Roles are not used in 'normal operation'
    - They are not added to the proxy by default when running *voms-proxy-init*
    - But they can be added to the proxy for special purposes when running *voms-proxy-init*

- **Example:**
  - User Yannick has the following membership
    - VO=BIOMED-FRANCE, Group=Paris, Role=SoftwareManager
  - During normal operation the role is not taken into account, e.g. Yannick can work as a normal user
  - For special things he can obtain the role "Software Manager"

# gLite general installation – short reminder

- **VOMS server can be installed via a gLite deployment package**
  - Download: http://glite.web.cern.ch/glite/packages
- **Installation via**
  - Installer script
  - APT
- **Installation will install all dependencies, including**
  - other necessary gLite modules
  - external dependencies (e.g. TOMCAT)
- **You will need to install non-freely available packages yourself (e.g. Java)**

# Installing VOMS via apt

1. **Verify if apt is present:**
   - rpm -qa | grep apt
   - Install apt if necessary:
     - rpm -ivh http://linuxsoft.cern.ch/cern/slc30X/i386/SL/RPMS/apt-0.5.15cnc6-8.SL.cern.i386.rpm
2. **Add gLite apt repository:**
   - Put one of the following lines in a file (e.g. glite.list) inside the /etc/apt/sources.list.d directory
   - rpm http://glitesoft.cern.ch/EGEE/gLite/APT/R1.2/ rhel30 externals Release1.2 updates
3. **Update apt repository:**
   - apt-get update
   - apt-get upgrade
4. **Install VOMS server:**
   - apt-get install glite-voms-server-config

Extra packages needed (non freely distributable) :

- **Exception: J2SE v 1.4.2_08 JRE: http://java.sun.com/j2se/1.4.2/download.html**

**See http://glite.web.cern.ch/glite/packages/APT.asp**

# gLite configuration – short reminder

- **Configuration files**
  - XML format
  - templates provided in /opt/glite/etc/config/templates
- **Hierarchy of configuration file**
  - Global configuration file
  - service specific configuration files
- **Parameter groups**
  - User parameters (‘changeme’)
  - Advanced parameters
  - System parameters

# VOMS Server key configuration aspects

- Virtual organization description (one instance per VO)
  - **name** of the VO
  - VOMS (core) service TCP **port** number on which the server will listen for one VO
    - must be a valid, unique port number – typically from 15000 upwards
  - **e-mail** address used to send emails on behalf of the VOMS server

- MySQL database configuration
  - Administrator **password** of used MySQL database

- Servicetool configuration
  - To publish the existence and status of the VOMS server to the information system (R-GMA)

# Configure & start the VOMS server

1. **Go to configuration directory and copy templates**
   – cd /opt/glite/etc/config
   – cp templates/* .
2. **Customize configuration files by replacing all ‘changeme’ values with the proper values**
3. **Go to the scripts directory and execute the VOMS Server configuration script**
   – cd scripts
   – ./glite-voms-server-config.py –configure
4. **Start the VOMS server**
   – ./glite-voms-server-config.py --start

# Verify installation

- **Using gLite configuration script**
  - ./glite-voms-server-config.py –status
- **Connecting to the VOMS server via browser**
  - https://<hostname>:8443/voms/<your-vo-name>
- **Checking if VOMS server shows up in R-GMA**
  - https://<rgma-server-machine>:8443/R-GMA

# Register VOMS administrator

The first VOMS administrator has to be added manually using the command line tools:

- **Copy your public grid certificate to your VOMS server**
- **Run voms-admin command to add yourself as admin**

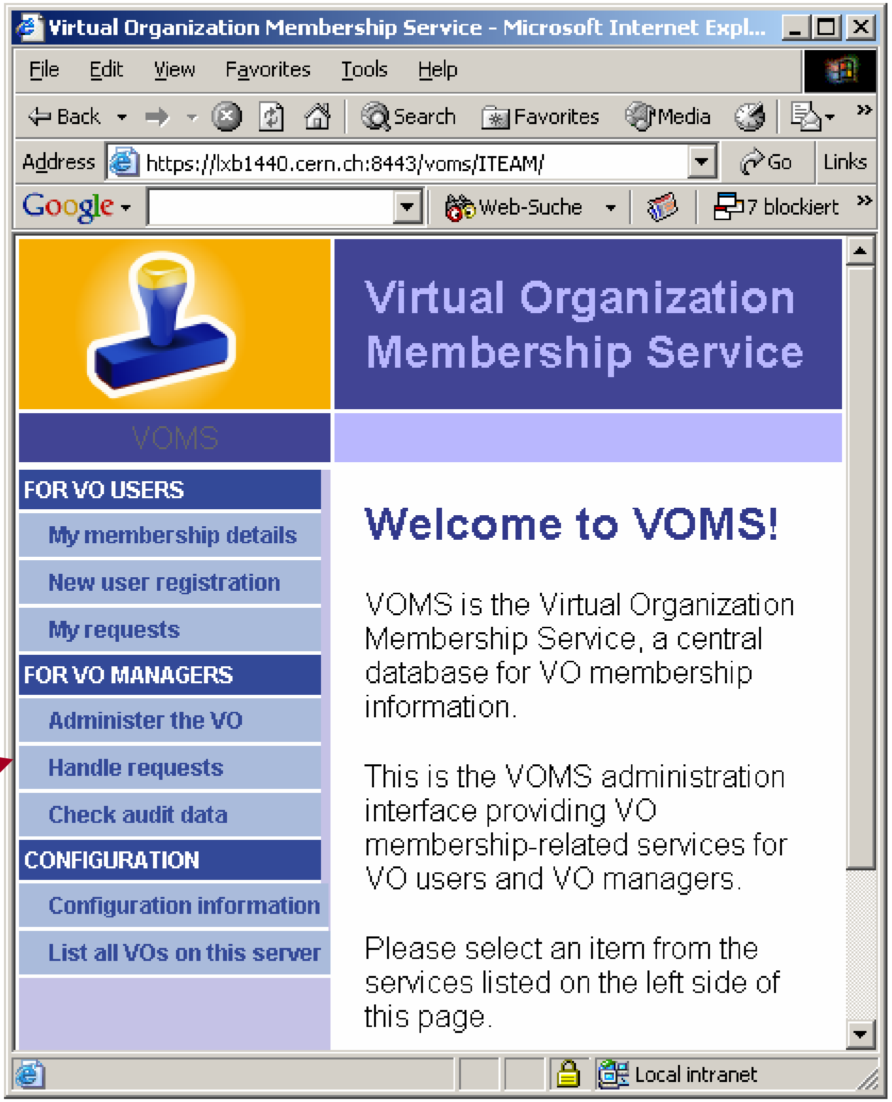
```
$GLITE_LOCATION/bin/voms-admin --vo <VO name> \
                    create-user <certificate.pem> \
                    assign-role VO VO-Admin <certificate.pem>
```

***Then you can start to work using the web interface …***

# VOMS Web interface

- **VO user can**
  - Query membership details
  - Register himself in the VO
    - You will need a valid certificate
  - Track his requests

- **VO manager can**
  - Handle request from users
  - Administer the VO


Virtual Organization Membership Service - Microsoft Internet Expl...
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://lxb1440.cern.ch:8443/voms/ITEAM/
Go Links
Google Web-Suche 7 blockiert
Virtual Organization Membership Service
VOMS
FOR VO USERS
My membership details
New user registration
My requests
FOR VO MANAGERS
Administer the VO
Handle requests
Check audit data
CONFIGURATION
Configuration information
List all VOs on this server
Local intranet

Welcome to VOMS!

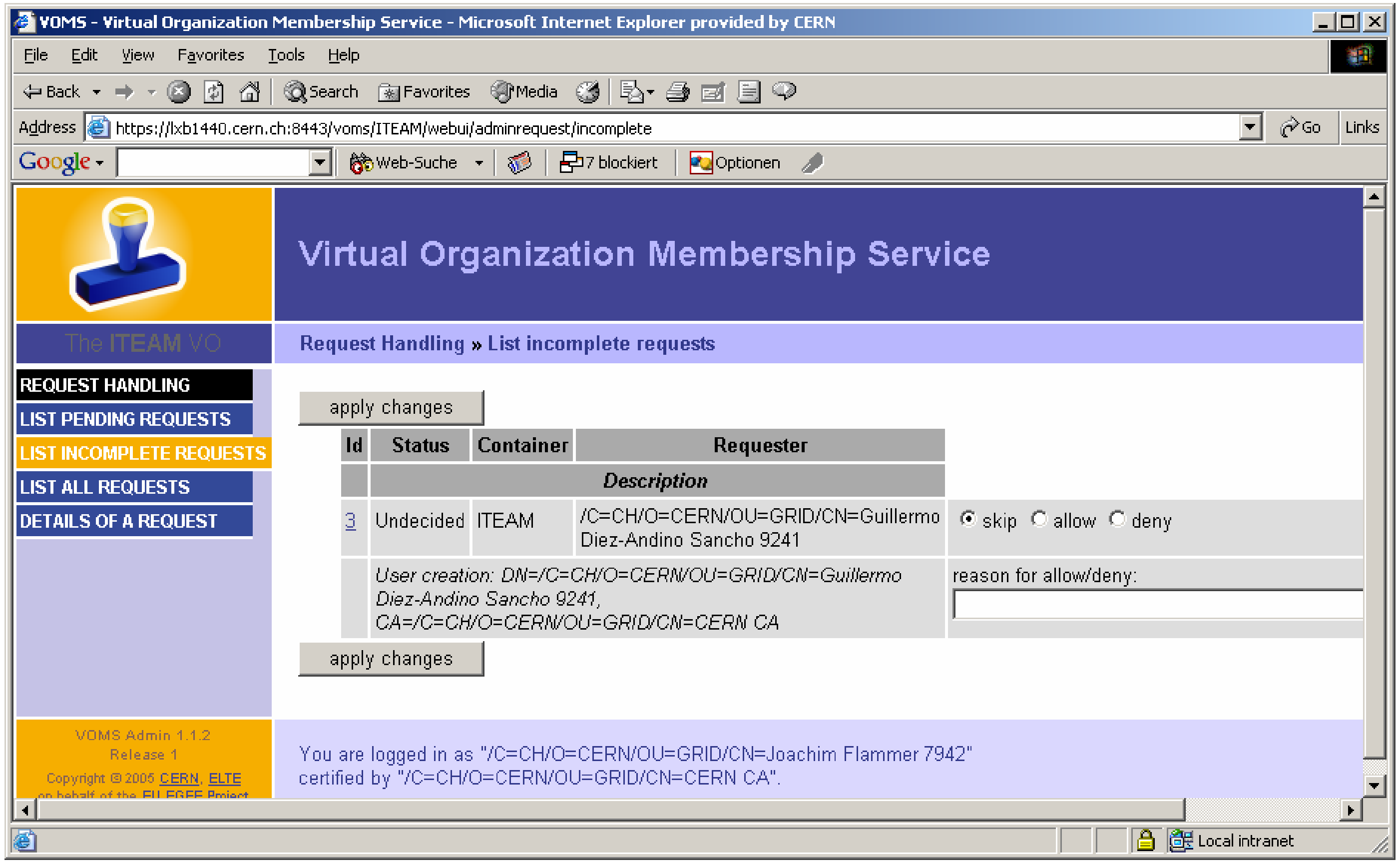
VOMS is the Virtual Organization Membership Service, a central database for VO membership information.

This is the VOMS administration interface providing VO membership-related services for VO users and VO managers.

Please select an item from the services listed on the left side of this page.

# VO Managers - Handling requests

- **VO manager will be informed of new requests via mail**
  - Query requests
  - Accept / Deny requests


VOMS - Virtual Organization Membership Service - Microsoft Internet Explorer provided by CERN
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google Web-Suche 7 blockiert Optionen
Local intranet

https://lxb1440.cern.ch:8443/voms/ITEAM/webui/adminrequest/incomplete

Virtual Organization Membership Service

The ITEAM VO

Request Handling » List incomplete requests

REQUEST HANDLING
LIST PENDING REQUESTS
LIST INCOMPLETE REQUESTS
LIST ALL REQUESTS
DETAILS OF A REQUEST

apply changes

| Id | Status | Container | Requester | |
|---|---|---|---|---|
| | **Description** | | | |
| 3 | Undecided | ITEAM | /C=CH/O=CERN/OU=GRID/CN=Guillermo Diez-Andino Sancho 9241 | ● skip ○ allow ○ deny |
| | *User creation: DN=/C=CH/O=CERN/OU=GRID/CN=Guillermo Diez-Andino Sancho 9241, CA=/C=CH/O=CERN/OU=GRID/CN=CERN CA* | | | reason for allow/deny: |

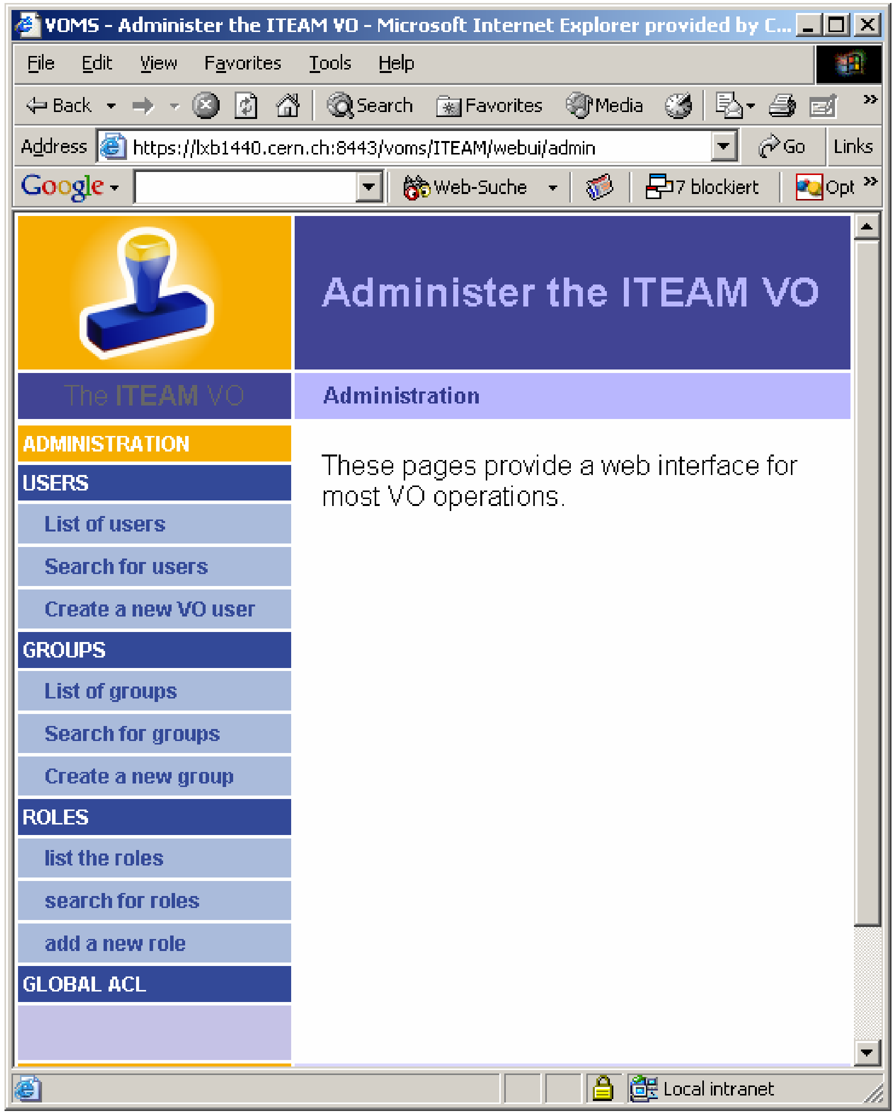
apply changes

VOMS Admin 1.1.2
Release 1
Copyright © 2005 CERN, ELTE
on behalf of the EU EGEE Project

You are logged in as "/C=CH/O=CERN/OU=GRID/CN=Joachim Flammer 7942" certified by "/C=CH/O=CERN/OU=GRID/CN=CERN CA".

# VO Managers - Administer a VO

- **The administrator interface allows you to**
  - **Manage users**
    - List users
    - Search for users
    - Create users
  - **Manage groups**
    - List groups
    - Search for groups
    - Create groups
  - **Manage roles**
    - List roles
    - Search for roles
    - Create roles


VOMS - Administer the ITEAM VO - Microsoft Internet Explorer provided by C...
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://lxb1440.cern.ch:8443/voms/ITEAM/webui/admin
Go Links
Google Web-Suche 7 blockiert Opt
Local intranet

Administer the ITEAM VO

The ITEAM VO

Administration

ADMINISTRATION

USERS
- List of users
- Search for users
- Create a new VO user

GROUPS
- List of groups
- Search for groups
- Create a new group

ROLES
- list the roles
- search for roles
- add a new role

GLOBAL ACL

These pages provide a web interface for most VO operations.

# Command-line interface

## Creating a VO

```
voms-admin-configure install --vo <VO-name>
                             --port <core-service-port>
                             --dbapwd <mysql-password>
                             --smtp-host <smtp-relay-host>
                             --mail-from <Sender-address-for-service-generated
                                        mails>
```

## Deleting a VO

```
voms-admin-configure remove --vo <VO-name>
                            --dbapwd <mysql-password>
```

## Adding VO administrator

```
voms-admin --vo <VO-name> create-user <cert.pem>
           assign-role VO VO-Admin <cert.pem>
```

# Command line interface (cont.)

- **General commands**

```
voms-admin [OPTIONS] --vo=NAME [-h HOST] [-p PORT] COMMAND PARAM
voms-admin [OPTIONS] --url=URL COMMAND PARAM
```

**COMMAND:**

| | |
|---|---|
| – get-vo-name | |
| – list-users | list all users of VO |
| – create-user <CERTIFICATE.PEM> | |
| – delete-user USER | |
| – list-cas | list certificate auth. accepted by VO |
| – list-roles | |
| – …. | |

**See VOMS admin user guide for entire list and details**

# Thank you very much for your attention!

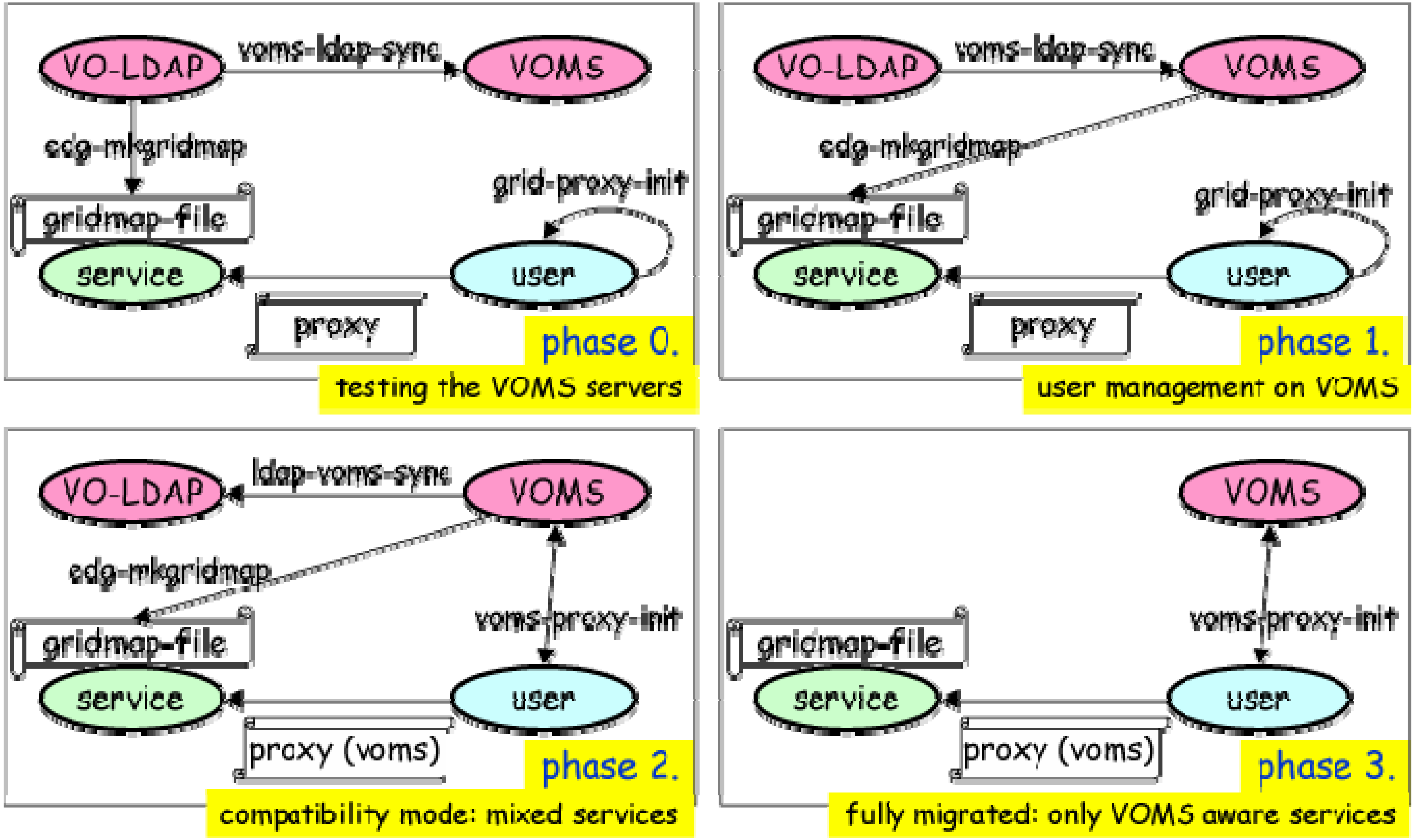
# Backup slides

# Known bugs

- **Parameters of a VO cannot be changed for the moment**
  - E.g. changing the VOMS port
  - Only possibility is to
    - Remove VO
    - Create VO again via command line interface
  - Pay attention: data will not be backuped!

- **Please refer to release notes for further details**

# VOMS migration plan



phase 0.
testing the VOMS servers

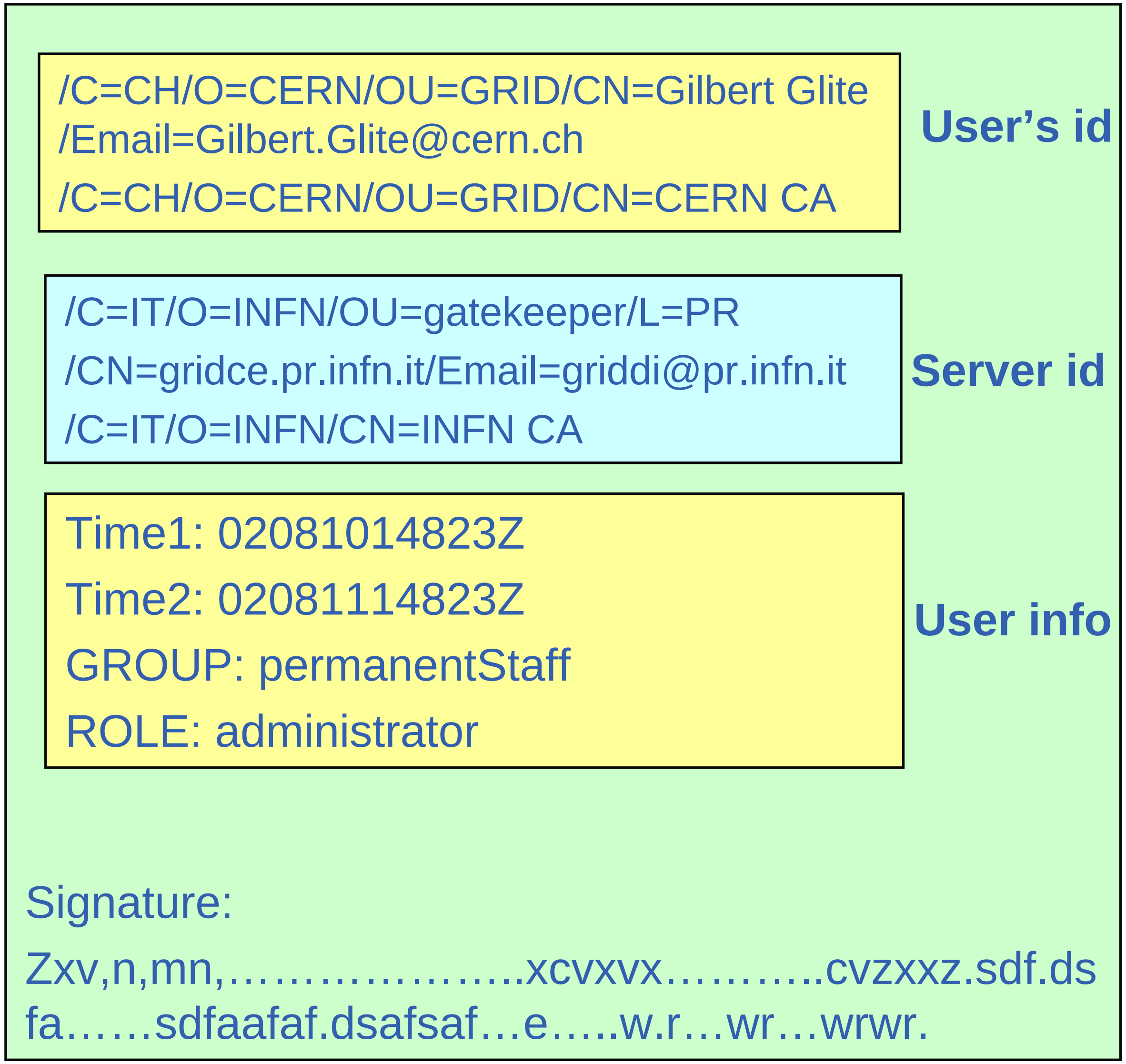
phase 1.
user management on VOMS

phase 2.
compatibility mode: mixed services

phase 3.
fully migrated: only VOMS aware services

# VOMS Attribute certificates

- **The pseudo-cert is inserted to a non-critical extension of the user's proxy**
- **One for each VOMS server contacted**



/C=CH/O=CERN/OU=GRID/CN=Gilbert Glite /Email=Gilbert.Glite@cern.ch

/C=CH/O=CERN/OU=GRID/CN=CERN CA

**User's id**

/C=IT/O=INFN/OU=gatekeeper/L=PR

/CN=gridce.pr.infn.it/Email=griddi@pr.infn.it

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

**Server id**

Time1: 020810148232Z

Time2: 020811148232Z

GROUP: permanentStaff

ROLE: administrator

**User info**

Signature:

Zxv,n,mn,…………………xcvxvx……….cvzxxz.sdf.dsfa……sdfaafaf.dsafsaf…e…..w.r…wr…wrwr.