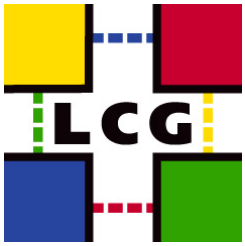

LCG Security Group

Proposal for meeting the LCG User Registration and VO Membership Management Requirements

Date:	**2nd July 2004**
EDMS Reference:	**https://edms.cern.ch/file/481701/0.1/GDB_Proposal_20040713.doc**
Internal Version:	**0.1**
Status:	**Draft**
Author:	**Maria Dimou (editor of the relevant Task Force)**

Document Log			
Issue	**Date**	**Author**	**Comment**
0.1	30 June 2004	Maria Dimou	Draft for GDB meeting on 13th July 2004 With comments by the Task Force members.
0.2	2 July 2004	Maria Dimou	Comments from B.Cowles, D.Kelsey, T.Levshina, I.Neilson, D.Skow following the Security Group meeting of 1 July 2004.

1 Preamble

A Task Force[1] (TF) was mandated after the March 8th 2004 GDB with the following basic goals:

1. Meet the robust registration process as now proposed in the Registration Requirements document[2].
2. Investigate the use of existing sources of membership information. Given the existence of an ORGanisational DataBase (ORGDB) in most organisations and, for the LCG Grid specifically, due to the rule that LHC collaborators have to register in the CERN HR database, this will be the only ORGDB considered by the TF.
3. Achieve all possible compatibility between the requirements and existing proposed solutions, namely, investigate the technicalities of VOMS and VOX/VOMRS interfacing to ORGDB.

This proposal concerns LHC experiment Virtual Organisations (VOs) only. It covers the above-described Goals 1 and 2. Technical investigation for the fulfilment of Goal 3 still continues.

2 Introduction

Following information gathering from the ORGDB administrators, the LHC experiments' secretariats and the CERN Users Office the TF concluded that:

- The ORGDB is usable but not always of sufficient quality or managed.
- There is a need to harden some of the ORGDB registration procedures.
- Each VO has to provide its management process, based on a template of required information that the TF will prepare.
- The aimed user registration flow diagram is included in https://edms.cern.ch/file/481701/0.1/UserReg_flow.pdf.

3 Definitions

Relevant to this proposal taken from the Registration Requirements document:

- **Personal user data:**
  - Family Name,
  - Given Name,
  - Institute name, i.e. the user's employing institute,
  - Contact Phone number.
- **Registration Data:** Authentication (AuthN) related information:
  - Personal user data,
  - Email address,
  - DistinguishedName (DN) extracted from a valid personal digital certificate issued by his/her Certification Authority (CA).
- **Site:**[3] An institute which is providing one or more Services to the Grid.
- **VO Database:** Authorisation (AuthZ) related information, i.e. the user's role(s) in the VO. His/her access rights to a resource and on data stored at it will depend on this information.
- **VO manager:** The responsible person recording in the VO Database, after appropriate checks, the status of a member of the VO, i.e. performing user entries, assignment of roles, information updates and user removals. The VO management function can be performed by a group of persons delegated by the VO manager.

---

[1] The Members:
Maria Dimou (LCG Registrar and DTeam VO manager, Editor), Joni Hahkala (VOMS admin. development Leader), David Kelsey (LCG Security Group Leader), Tanya Levshina (VOX Project leader), Ian Neilson (TF coordinator, LCG Security Officer).

[2] https://edms.cern.ch/file/428034/2/LCG_User_Registration.pdf.

[3] Site, Resources and Resource Administrator definitions taken from https://edms.cern.ch/file/431463/1/Resource_Administrators_Guide.doc

- **Usage Rules:** The rules (sometimes mentioned as Guidelines) governing the use of Grid resources.
- **Institute Representative (IR):** The person at the user's employing institute, who can check the validity of his/her data and confirm the identity of the user and his/her right to become or remain a member of a VO.

4 The proposal:

The LCG Requirements document explains: "*The main objective of the registration process is to collect the user's Registration Data. Duplication of Personal user data and the procedures of validation and authentication should be avoided so that Grid users register only once and their Registration data are checked only in a single place.*

Robust documented verification procedures must be used to establish the link between a person, his/her Registration data and the associated AuthZ data."

The TF, trying to satisfy the requirement on non-duplication of information and procedures proposes:

1. The following databases will be involved in the Registration process:
    a. The ORGDB, containing the user's Authentication (AuthN) information in terms of *Personal user data* and email address.
    b. The AuthN part of VODB, containing at least:
        i. the user's DN,
        ii. the VODB_Expiry_Date, i.e. the possible end of VO membership for the user, as defined in the Requirements Document. This will have an initial value, not exceeding one year, assigned to it at user registration time, provided the user's contract with the institute is of a longer duration.
        iii. VODB_Registration_Date, automatically taken from the system 'date' the moment that the VO manager accepts the user in the VODB.
    c. The Authorisation (AuthZ) part of VODB, containing at least:
        i. The flag showing whether he/she is in "Suspended Status". The VO manager will be the only person authorised to change this flag.
        ii. The user's access rights on resources and data , as defined in the Registration Requirements Document.
2. All VODB candidates must register in ORGDB before applying to the VO. Users, attempting a VODB registration, who are absent from ORGDB, will have to be prompted to register there first[4].
3. *Personal user data* will only reside in ORGDB. Private user information, e.g. salary, children etc, will not be accessible at all.
4. The VO manager will have to take action in order to enable the candidate entries.
5. The user will fill a web form requesting to join a given VO, where he/she will have to enter sufficient information to establish the link to his/her entry in ORGDB, namely:
    a. Family Name and Given Name,
    b. The CERN_ID appearing on the CERN badge[5], if he/she knows it. Alternatively the birthdate.
    c. Email address. This must be identical to the one in ORGDB. Users will be required to be reachable via this address.

[4] ORGDB Registration procedures in http://ph-dep.web.cern.ch/ph-dep/UsersOffice/Registration/Welcome.html
[5] Examples of CERN access cards in http://test-div-st.webtest.cern.ch/test-div-st/groups/ma/in/Cards.htm. The CERN_ID appears under the CERN logo.

In addition, via this form:

d. The user will confirm his/her acceptance of the Usage Rules,
e. The user's DN as well as the DN of his/her Certification Authority (CA) will be captured by the fact that his/her personal digital certificate must be loaded onto the browser before filling this form.

6. DN verification is still the responsibility of the VO manager. He/she will use out of bound procedures to verify that the DN matches the user's identity as derived from the *Registration data.* Personal certificate renewal should be transparent for ORGDB and VODB, provided the user DN remains unchanged. Acceptable CAs' root certificates will be delivered by the deployment group of the project.
7. Authorised secure access to *Registration Data* will be possible for site administrators via queries to the VODB. The mechanism for this must be defined. No direct access to ORGDB will be allowed.
8. When the VODB_Expiry_Date is reached, users will be unable to run their Grid jobs because they will be suspended automatically from VODB, unless they take, in time, the required actions to renew their VODB registration.
9. The VO manager may need to put the users in "Suspended Status" due to other reasons, mainly related to security, as described in the Registration Requirements Document.

5 Concerns:

- The user's DN(s) is not captured at ORGDB registration time. It is part of the *Registration Data*, as defined in the Registration Requirements Document, but is only present in the VODB. The TF's proposal is to include, in the long-term, this information in ORGDB.
- Users, remain in ORGDB with out-of-date information. The update procedures have to be reviewed in order to cope with the security requirements of the Grid environment.
- ORGDB registration for External users (ORGDB Status code: EXTN) undergoes very little validation from the experiment secretariats e.g. the Team Leader (ORGDB terminology) doesn't have to sign to authorise an EXTN user entry and the Users' Office doesn't get involved. The TF's proposal is to establish a robust ORGDB registration process for EXTN users, involving the Team Leader (*Institute Representative (IR)* in the terminology of the Registration Requirements document). It is the recommendation of the TF to foresee a CERN_ID for EXTN users, in the long-term (it doesn't exist today).
- Users who want to be part of a VO even if their Institute doesn't participate in it. The TF's proposal is for these users to register in ORGDB first as EXTN users and involve their VO manager for approval.
- The ORGDB *Participation_End_Date*, is not managed today, i.e. users are not deleted when this date is reached, especially if they continue their participation in an experiment different to the one for which the *Participation_End_Date* is reached. The TF's proposal is to foresee, in the long-term, more than one *Participation_End_Date,* e.g. *Primary_ Participation_End_Date* and *Secondary_ Participation_End_Date,* i.e. one such date per experiment affiliation. It is the recommendation of the TF to keep these dates scrupulously up-to-date and allow them, when reached, to trigger a user renewal/removal from the VODB according to the Registration Requirements Document.