Joint Security Policy Group

Virtual Organisation Membership Management Policy

Date:	**15 July 2009**
EDMS Reference:	https://edms.cern.ch/document/428034/
Version:	**3.7a**
Status:	**Released**
Author:	**JSPG**

Document Log			
Issue	**Date**	**Author**	**Comment**
1.0	30 June 2003	David Kelsey	Draft in preparation for GDB meeting on 8th July 2003
1.1	2 July 2003	David Kelsey	Mods addressing comments from Ian Neilson
1.2	3 July 2003	David Kelsey	Address more comments from LCG Security group and VO managers. Sent to GDB.
2.0	3 February 2004	Maria Dimou, David Kelsey	Change of registration policy following the 15-17 December 2003 workshop at CERN on "Registration, VO mgnt, Authz". Incorporated comments from Ian Neilson. Replacing document https://edms.cern.ch/file/428034/1/LCG_User_Registration.pdf.
2.1	26 February 2004	Maria Dimou	Added comments by David Kelsey and Ian Neilson
2.2	9 March 2004	Maria Dimou	Clarified that a user can register using a *personal* certificate, to avoid misunderstandings with host certificates.
2.3	25 March 2004	Maria Dimou	Added comments by D.Barberis, F.Carminati, J.Closier, A.Frohner, M.Mazzucato, O.Smirnova and the Security Group members of the 22 March 2004 meeting.
2.4	7 May 2004	Maria Dimou	Added comments by I.Bird, A.Frohner, I.Neilson.
2.5	12 May 2004	Maria Dimou	Added comments by J.Hahkala, D.Heagerty, D.Kelsey, T.Levshina, I.Neilson, D.Skow.
2.6	13 May 2004	Maria Dimou	Added comments by D.Kelsey, T.Levshina, I.Neilson.
2.7	1 June 2004	Maria Dimou	Added comments by M.Delfino, T.Levshina, A.Sciaba. **Released version**.
3.0	29 May 2008	David Kelsey	Changed title from Requirements for LCG User Registration and VO Membership Management to Virtual Organisation Management Policy. Removed many of the definitions and all footnotes. Removed references to LCG. Removed section on Site responsibilities and requirements. This should be covered elsewhere. For discussion at the May 2008 JSPG meeting.
3.1	27 Aug 2008	David Kelsey	For discussion at August JSPG meeting.

3.4	22 Jan 2009	David Kelsey	Includes changes agreed at JSPG Jan 09 meeting. Ready for wide consultation.
3.6	18 May 2009	David Kelsey	Includes changes agreed at May 09 JSPG meeting. “Final call”.
3.7	29 Jun 2009	David Kelsey	Includes changes agreed at Jun 09 JSPG meeting. Addresses all issues raised during final call. Ready for formal approval and adoption.
3.7a	15 Jul 2009	David Kelsey	No changes to text. Status changed to “**Released**” after formal approval by WLCG MB (7 July 2009) and EGEE TMB (10 July 2009).

Virtual Organisation Membership Management Policy

1 Introduction

This policy defines the minimum requirements on Virtual Organisation (VO) Managers for managing the members of their VOs.

2 Scope and Audience

This document is aimed primarily at VO Managers. It defines the checks VO Managers must make to verify the eligibility of their members to join and to remain in the VO. These are independent of the implementation of the underlying technology. It does not address the security requirements for running the actual VO Membership service.

The VO Manager does not necessarily have to be a member of the VO or to have signed and agreed to the VO AUP. This function may be performed by a member of a Grid or Site operations team as a service for the VO.

3 Definitions

Data supplied by the user:

- **Personal user data:**
  - Family Name,
  - Given Name,
  - Institute name, i.e. the user's employing institute (this is required if the user's membership eligibility derives from his/her institutional affiliation)
  - Contact Phone number (this is optional, but the VO Manager may need to contact the user promptly during investigation of security incidents)
- **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).

Other relevant terms:

- **VO Database:** Authorisation (AuthZ) related information, i.e. the user's role(s) in the VO, is stored in this database. 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. The VO Manager does not necessarily have to be a member of the VO or to have signed and agreed to the VO AUP. This function may be performed by a member of a Grid or Site operations team as a service for the VO. All VO Managers must comply with the requirements of this policy.

- **Institute Representative (IR):** If appointed, this person at the user's employing institute is able to 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.
- **VO Registration Information:** Data stored by the Grid describing information about the VO.

4 Membership Management Requirements

The VO must appoint a VO manager and at least one deputy who are responsible for implementing procedures meeting the requirements of this policy. These are important roles which carry operational responsibilities; non-responsiveness of the VO manager or deputies may lead to the suspension of the VO from the Grid.

The VO membership management procedures must ensure that:

- only individuals who have agreed to abide by the VO AUP are registered as members of the VO,
- accurate Registration Data is maintained for all VO members.

Membership of a VO is not necessarily restricted to real persons. Hosts, Services and/or Robots (unattended automated processes acting on behalf of the VO) may also be registered in the VO. In the case of these non-personal registrations, the Registration Data must include the personal details of the real person requesting registration and assuming ongoing responsibility for the entity.

The VO Manager must publish a description of the methods used to verify user data at registration time and periodically review users' affiliation with the VO according to the requirements in the following sub-sections.

4.1 Appointment of the VO manager

The VO should determine how it appoints and replaces its VO manager and deputies.

4.2 Membership Registration

Membership Registration is the process by which people first join the VO. An important objective of this process is to collect the user's Registration Data. Accurate Registration Data must be maintained for all VO members.

VO Managers must check the validity of the user Registration Data and check the user's eligibility for special authorisation (Groups/Roles).

Replication of Personal user data and multiple validation and authentication should be avoided so that Grid users register only once with each VO and their Registration Data are checked only in a single place.

The procedures must unambiguously assign the individuals who take responsibility for the validity of the Registration Data provided, and those with the authority to exercise control over the rights of the user to use Grid resources. This may include an Institute Representative, as defined above, and/or Site Managers.

4.3 Acceptable Use Policy

An important purpose of the registration process is to record the explicit acceptance by the user of the Grid AUP and the VO AUP as well as the acceptance, by the user, that part of his/her information including Personal user data may be made available to the Sites and Grid Operations.

4.4 Membership Renewal

The membership renewal process must include:

- Confirmation, by the VO Manager, that continued membership of VO is still allowed,
- Confirmation or update of all data provided during registration and all special authorisations,
- Reaffirmed acceptance by the user of the Grid AUP and the VO AUP.

Membership of the VO must be renewed at least every 12 months. Additionally all members of the VO should renew following a major change to the Grid Acceptable Use Policy.

4.5 Membership Removal

The following conditions should trigger a timely re-evaluation of the user's right to remain a member of a given VO:

- User or IR request. Ideally, the user should be able to remove themselves from the VO without involvement of the VO Manager,
- Renewal failed to complete in allotted time,
- End of collaboration between the user's institute and the VO, if applicable,
- End of collaboration between the user and the VO,
- End of collaboration between the user and his/her institute, if applicable.

Note that some VOs may not maintain relationships with institutes. The fact that the VO does not maintain relationships with institutes should be recorded on the VO Registration Information.

4.6 Membership Suspension

The suspension of VO membership is the temporary removal of the user from the VO.

The VO Manager must cooperate fully with Grid Security Operations in the investigation of Grid security incidents. A member should be suspended when the VO Manager is presented with reasonable evidence that the member's grid identity has been used, with or without the user's consent, in breach of relevant Grid and/or VO policies (security or otherwise).

The request for suspension may be made by the Grid Security Officer and/or by Grid Operations. Requests from Sites should be routed through and confirmed by the Grid Security Officer and/or Grid Operations. In emergency situations this confirmation may be provided after the actual suspension if the VO Manager decides this is appropriate.

All reasonable efforts must be made by the VO Manager to contact the member when he/she is suspended.

Prior to reinstating a suspended user the VO Manager must notify those who requested suspension.

There should be an agreed dispute resolution procedures which the VO and/or Grid can follow if the user wishes to challenge his/her suspension.

4.7 Audit requirements

The VO Membership Management system(s) must record and maintain an audit log of all VO membership transactions.

This audit log must be kept for a minimum period consistent with the Traceability and Logging Policy (*https://edms.cern.ch/document/428037/*). Audit logs containing personal registration data must not be retained for longer than one year.

The audit logs must include:

- every request for membership,
- every request for assignment of or change to VO authorisation attributes (groups, roles etc.),
- every membership renewal request,
- every membership suspension request,
- every membership removal.

Each of these requests should record the date and time of the request, the originator of the request, the details of the request and whether or not it was approved or successful. The identity of the person granting or refusing the request should be recorded including any verification steps involved and other people consulted, e.g. IR.

4.8 Data privacy

It is recommended that the VO should document its VO Membership data privacy policy. This should include statements on:

- which data, if any, is collected from a VO member in addition to the Registration Data and explain why this data is required,
- how and where the data is stored,
- for how long the data is kept and how expired data is deleted,
- explain who within the VO has access to the data and why,
- how the user can view their own data and request corrections,
- what happens to the VO membership data when the VO ceases to exist,
- describe any third parties to whom VO membership data is disclosed and why. The VO may decide, for example, to grant read access to the data by Grid and Security Operations.