



## **Deliverable 3.9**

# **Analysis of security issues brought about by the user community and by industrial stakeholders**

### **SEVENTH FRAMEWORK PROGRAMME Research Infrastructures**

INFRA-2007-1.2.2 - Deployment of eInfrastructures for scientific  
communities

**Grant agreement for: Combination of Collaborative projects &  
Coordination and support actions**

Proposal/Contract no.: 213010 – **e-nmr**

Project full title: Deploying and unifying the NMR e-Infrastructure in System Biology

Project coordinator: Prof. Dr. Harald Schwalbe

Project website: <http://www.enmr.eu/>

Period covered: from **01-11-2007 to 31-10-2009**

# Table of contents

<b>1. INTRODUCTION .....</b>	<b>3</b>
1.1 PURPOSE .....	3
1.2 DOCUMENT ORGANISATION .....	3
1.3 REFERENCES.....	3
1.4 TERMINOLOGY .....	3
<b>2. EXECUTIVE SUMMARY.....</b>	<b>5</b>
<b>3. SECURITY POLICY OF THE E-NMR PLATFORM.....</b>	<b>6</b>
3.1 OVERVIEW OF GLITE SECURITY.....	6
3.2 E-NMR PORTAL SECURITY.....	9
3.3 DATA SECURITY .....	12
<b>4. THE SECOND ROUND SECURITY SURVEY .....</b>	<b>16</b>
<b>5. ANALYSIS.....</b>	<b>18</b>
<b>6. CONCLUSIONS .....</b>	<b>20</b>

# 1. Introduction

## 1.1 Purpose

This document is the project deliverable D3.9 due by Month 24. It aims at analysing the user community and especially the industry needs in term of security issues. In fact, in order to promote the rapid and successful uptake of NMR Grid technology, we will strive to collaborate closely with the industry as the NMR technology provider.

## 1.2 Document organisation

The document is organised as follows:

Section 1 contains the purpose of the document, its references and a glossary of terms and acronyms;

Section 2 summarizes the content of the document;

Section 3 describes the e-NMR Security Policy published on the project web site in order to collect feedback and ask for approval by e-NMR users and stakeholders;

Section 4 describes the second round of the e-NMR Security Policy survey;

Section 5 analyses the results of the survey;

Section 6 tracks the conclusions.

## 1.3 References

<a href="http://glite.web.cern.ch">glite.web.cern.ch</a>	gLite middleware web page
<a href="http://www.e-nmr.eu">www.e-nmr.eu</a>	e-NMR Project web page
<a href="http://www.jspg.org/wiki/JSPG_Docs">http://www.jspg.org/wiki/JSPG_Docs</a>	JSPG Security Policy documents

## 1.4 Terminology

This subsection provides the definitions of terms, acronyms, and abbreviations required to properly interpret this document.

<b>Term</b>	<b>Definition</b>
AA	Attribute Authority
AC	Attribute Certificate
ACL	Access Control List
BCBR	Bijvoet Centre for Molecular Research, University of Utrecht, The Netherlands
BMRZ	Centre for Biomolecular Magnetic Resonance, Goethe University, Frankfurt, Germany
CA	Certification Authority
CE	Computing Element
CIRMMMP	Interuniversity Consortium for Magnetic Resonance on Metalloproteins, Florence, Italy
EGEE	Enabling Grids for e-Science
EDS	Encrypted Data Storage
FQAN	Fully Qualified Attribute Name
gLite	Codename of the middleware software suite developed by EGEE
GFAL	Grid File Access Library
GUID	Globally Unique Identifier
Hydra	Keystore server for encrypted file storage solution
IGTF	International Grid Trust Federation
INFN	National Institute of Nuclear Physics, Italy
JSPG	Joint Security Policy Group
LCG	LHC Computing Grid
LFC	LCG File Catalogue
LFN	Logical File Name
NGI	National Grid Initiative
NMR	Nuclear Magnetic Resonance
PKI	Public Key Infrastructure
SLCS	Short Lived Credential Service
SE	Storage Element
SRM	Storage Resource Manager
SURL	Storage URL
TURL	Transport URL
UI	User Interface
VO	Virtual Organization
VOMS	Virtual Organisation Membership Service
WMS	Workload Management System
WP	Work Package

## 2. Executive summary

The project deliverable D3.3 (Request for Enhancement of gLite to support bio-NMR applications) issued at Month 18 contained the result of an on-line survey about the requirements related to data security coming from bio-NMR community.

The anonymous on-line survey was proposed to the registered HADDOCK user community (~900 users counting both the registered groups and haddock portal users). These cover a wide range of techniques within the structural biology community. In addition, the survey announcement was posted to the NMR mailing list ([nmr@listes.sc.univ-paris-diderot.fr](mailto:nmr@listes.sc.univ-paris-diderot.fr)) which counts more than 1430 registered members to date. The survey was also sent to a number of biotech and pharmaceutical companies, e.g. GlaxoSmithKline, Sanofi-Aventis GmbH, AstraZeneca GmbH, Bruker GmbH and Merck Pharma GmbH

The survey consisted of 7 questions about security needs of NMR applications, and was made available at the project web portal. Two weeks after the advertising of the target community, a total of 55 answers were collected.

As a status snapshot of the [still accessible survey](#) about the data security issues, 96% of the answers came from Academia and others no-profit organizations, while 4% responded from the private industrial sector.

Referring to the small minority of respondents who indicated security as an issue,

- *One third* came from organizations **having policies preventing to send sensitive data** over internet to be used as input for NMR calculations by the applications web servers.
- *Two-thirds* indicated that the **confidentiality of data handling is expected to be achieved via encryption and ACL-based access.**

However, among the lessons learned, there was that most of users had limited knowledge of grids and in particular of their security aspects. Following the suggestions coming from the project interim review held in June 2009, it was decided to adopt a different approach.

A e-NMR security policy document was prepared, describing in detail the security model recently enhanced as a consequence of the survey results, namely through the deployment of the gLite Encrypted Data Storage System on the e-NMR grid infrastructure. The document was then published on the e-NMR web portal, together with a second round of the security survey designed in a different manner. It consists now in a FAQ format survey, where typical security related questions are simply posed and answered by our team. The user can approve or reject the answer, or leave his comment.

At the end of the survey, the user is asked to have a look at the more detailed e-NMR Security Policy Document available on the project web site, and provide his feedback optionally.

The results of this new survey have shown that the large majority of the users (> 88%) are satisfied by the proposed e-NMR security policy. In addition, more than 70% of the users left us feedback, with different levels of detail, expressing comments about the e-NMR Security Policy document on the final free format text box.

### 3. Security policy of the e-NMR platform

This section describes the security model adopted by e-NMR grid and enhanced after the first survey carried out at Month 18. This description has been published on the project web portal for evaluation by the users.

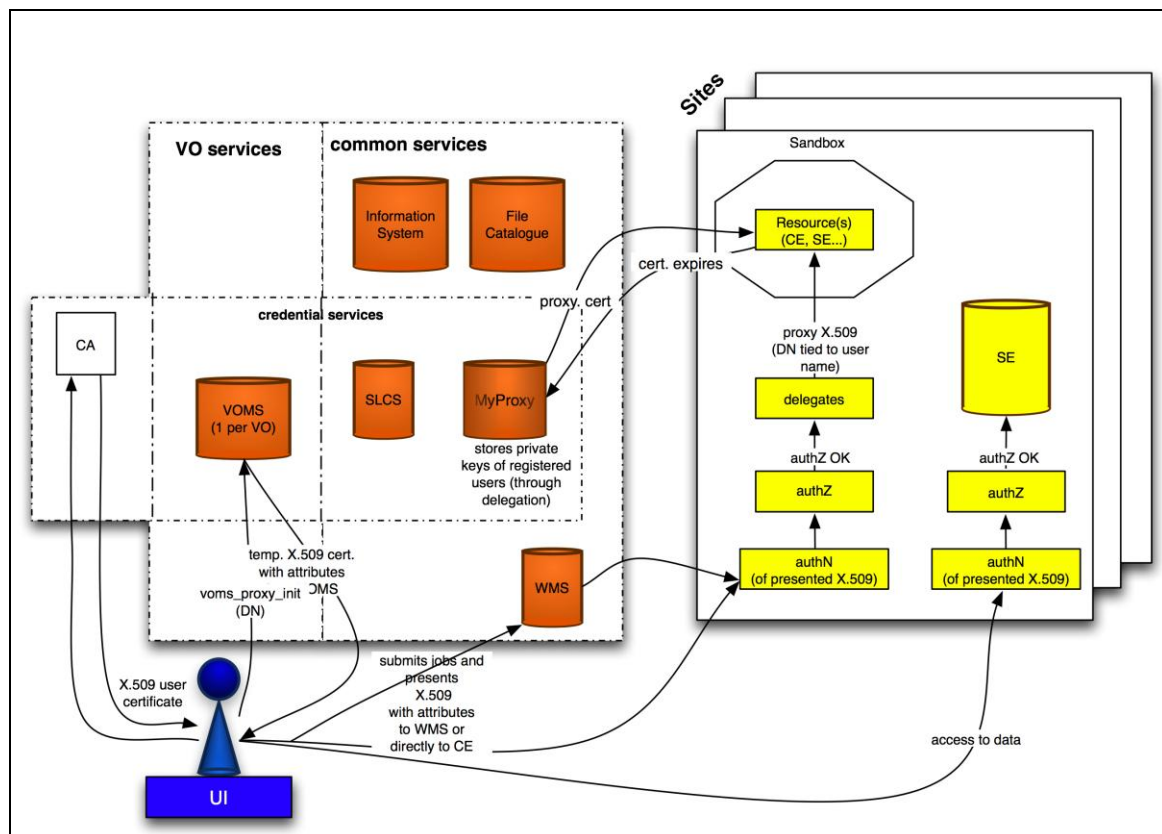
#### 3.1 Overview of gLite security

In grid environments users are organized in so called Virtual Organizations (VO). They allow the management of users across different institutions without the need to observe intra-institutional management structures and policies.

Sites on the other hand correspond to local installations of computing resources (clusters, storage, etc). Agreements are made between the individual sites and VOs that give the members of a VO access to the resources of the sites. In order to do so, sites must install the services of the chosen middleware. It is important to note that the support of VOs by sites does not mean that the site hands over some of its autonomy, particularly in security issues, to VOs. On the contrary, the local site autonomy must be preserved and respected by the VO and its members at all times.

Besides VO and sites, there are also a set of common services that act as a glue between VOs and sites. They can be considered as a part of the underlying grid infrastructure and are typically operated by some of the larger sites on behalf of the infrastructure. Examples are information services, credential stores, management services for VOs etc.

Figure 3-1 shows the high level picture of the gLite components divided into the elements of VOs, sites and common services.



**Figure 3-1:** gLite security overview

The gLite middleware consists of the following software components:

- User Interface (UI): the component through which the user interacts with the grid (submitting of jobs, querying component status, access to data stored on the grid, etc). The user needs to possess a X.509 certificate in order to interact with the grid services, because the gLite security model is currently entirely PKI-based.
- CA: a Certificate Authority provides the X.509 credential to the user. The CAs are coordinated through the International Grid Trust Federation (IGTF). CAs also issue host or service certificates to identify hosts and services.
- VO services: users are permitted to access the grid due to their VO membership. Currently, there is only one supported VO service, the Virtual Organization Management Service (VOMS).
- Common services: these are services that span the grid and may serve one or more VOs at the same time. Examples are the information system, file catalogues and resource brokers.
- Site-specific services: these are services hosted at local sites, like Computing Element (CE), Storage Element (SE)
- Credential services: this is a special class of services, which act either
  - as an Attribute Authority (AA) ,
  - as proxy certificate store and renewal service (MyProxy)
  - as a short-lived credential service (SLCS ).

In gLite a VO is administered through an instance of the Virtual Organization Membership Service, which is hosted on a dedicated server. In the VOMS system VO members are registered and uniquely identified by the combination of the DN of their X.509 certificates and the issuing CA of the certificate. Admission to the service is controlled and granted by access control lists (ACL) and the Grid Security Infrastructure (GSI) mechanisms. This implies that every user that accesses the VOMS service needs to present a valid X.509 certificate (or proxy certificate), such that he can be authenticated and authorized by VOMS.

VOMS classifies users into groups and roles. Members of a VO are organized in groups. In addition, they may be granted roles – a qualifier expressing (administrative) privileges, which may be presented to grid services during authorization decisions

As an example, the user “John Doe” is a member of the VO “enmr.eu”, where he belongs to the groups “cyana”, “haddock”, and “xplornih”. In addition, he has the privilege to act in the role of “VO-Admin” for the “xplornih” group, and “SoftwareManager” for the “haddock” group. When accessing a grid resource, for example he may choose to do this as

- I. A user of the “haddock” group in the role “SoftwareManager” or
- II. A user of the “haddock” group or
- III. A user of the “xplornih” group in the role “VO-Admin” and so on.

The name of the VO, the group membership and optionally a role with which a user chooses to access the grid thus form the smallest unit/context that describes a user. This minimal unit is referred to as Fully Qualified Attribute Name (FQAN). A FQAN simply expresses the membership of the user in a group, possibly added with a role qualifier. The “Name” of the individual FQAN components (i.e. the VO, group and role) is implicitly given by the syntax of the FQAN, which is a string written as: /<vo\_name>/<group>/<subgroup>/Role=<role>. For the above-mentioned three examples the FQANs are

- I. /enmr.eu/haddock/Role=SoftwareManager
- II. /enmr.eu/haddock
- III. /enmr.eu/xplornih/Role=VO-Admin

Note that the role and the group of a user are fully decoupled. From the VO information about a user any group – role combinations can therefore be created. This results in a potentially large number of FQAN combinations.

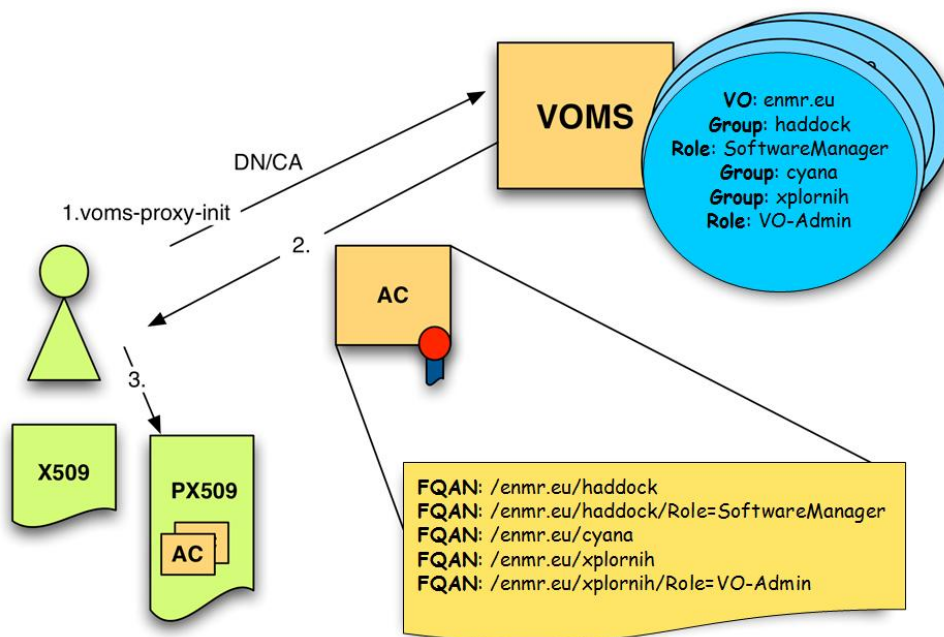
There is also a duality of the use of the role: Firstly, a role can be used to grant privileges to a user for administering the VO in VOMS, e.g. to manage users of a group (e.g. VO-Admin may have management permissions for the group xplornih in VO enmr.eu). Secondly, the role information may be also used during the authorization of the user by a grid resource, if the user presents a FQAN as a credential.

Besides the above-mentioned FQANs one can also envisage attributes consisting of an arbitrary attribute name and an associated value, i.e. a key-value pair. Such attributes are also supported by VOMS. They are called Generic Attributes (GA) and permit the storage of additional information about a user. A GA can, for example, contain entitlement information for a user, or a user's affiliation; in short, information permitting for more granular authorization than just groups and roles. There is currently no consensus on how GAs shall be used and interpreted in gLite. Therefore at the time being they are meaningful only within the VO scope.

When interacting with gLite grid resources a user must not only present his X.509 certificate, but also information describing his membership in a VO. This is achieved through the generation of a proxy certificate, which contains the VO information about the user as stored in VOMS (called VO credentials). This proxy certificate is signed using the user's private key.

The user creates the proxy by executing the command `voms-proxy-init` (see Figure 3-2). During the execution of this command the VOMS service is requested to issue the VO information about the user (FQANs and GAs) in the form of an Attribute Certificate (AC). The AC is signed by VOMS using the private key of the server host certificate. The AC is then embedded inside the user's proxy in the extension field of the certificate. Thus, in the terminology of RFC3820 the VOMS server acts as an Attribute Authority (AA). The term "attribute" refers here to any credentials retrieved from the VOMS server, hence FQANs as well as GAs.

Note that the AC normally contains a list of FQANs, one for each group that the user belongs to. The role is only added to the FQAN, if the user requests it by explicitly adding a command line argument to the command `voms-proxy-init`.



**Figure 3-2:** voms-proxy-init command allows the user to create his proxy with the desired VO AC

A user has the possibility to collect ACs from different VOs and embed them all into a single proxy certificate. Of course he cannot modify the content of the ACs, nor reorder the FQANs in the AC once it has been issued. This is relevant, since the order in which the FQANs appear in the AC may affect the authorization decision. In addition, all group memberships will be listed as FQANs in the AC, i.e. the user cannot hide a membership in a group from grid services.

However, the `voms-proxy-init` command allows a user to specify

- The ordering of the FQANs in the AC, in particular which FQAN will be the first one
- Whether the role qualifier should be added to the FQAN (provided VOMS grants this role to the user).

This approach necessitates (i) that a user precisely knows his VO profile (what groups he belongs to and which roles he may request) and (ii) that he is aware how this information will be used in subsequent authorization decisions.

This procedure is not very user-friendly: Getting to know the VO profile requires the knowledge of the URL to access the VOMS server and more important, understanding the authorization mechanisms can only be expected from an expert user.

### 3.2 e-NMR Portal security

The first service developed by the project aimed at providing GSI secured access to the existing e-NMR portals initially developed to run the application on the local computing resources. In case of no use of grid resources, the user access was guaranteed via registration to each portal providing username and password. In case of use of grid resources, the access rights to the portals were instead guaranteed by requiring:

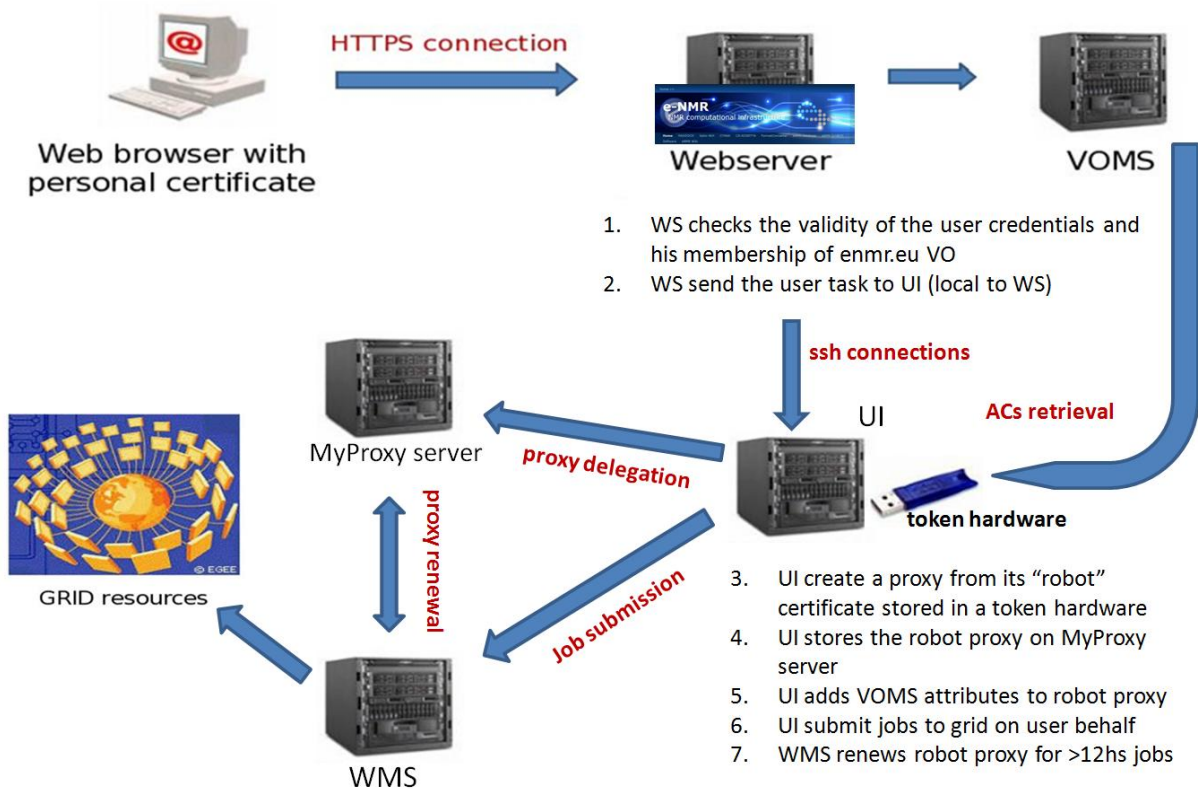
- 1) a X509 personal certificate issued by a IGTF accredited CA loaded into the users' browser

2) the personal certificate DN had to be registered with the enmr.eu VO

Behind the portal a business logic software component performed the needed operations to allow job submission over the e-NMR grid. The first grid-enabled version of the HADDOCK, CS-Rosetta and Xplor-NIH portals implemented job submission making use of X509 robot certificate issued per application by NIKHEF and INFN CAs, according with the VO Portal Policy draft documented by the Joint Security Policy Group (JSPG) of EGEE. In particular, the large number of jobs to be submitted and monitored by the HADDOCK and CS-Rosetta portals calls for automation. The current implementation of these two portals makes use of a robot certificate, qualifying them as a “parametric portal” according to the [Joint Security Policy Group \(JSPG\)](#). The portal also obeys to the BigGRID (Dutch e-Science GRID) policies (see <http://www.biggrid.nl/infra/BiGGrid-VO-Portal-Policy-v1.pdf> ).

A schema of the architecture is shown in Figure 3-3.

A custom User Tracking System was implemented by portal developers in order to keep track of applications usage by each user, associating the DN of the users’ certificate read at portal access time with the identifiers of grid jobs submitted with the robot on behalf of the user. Of course the usual grid accounting tools will see only the aggregate application usage, while the portal administrator will be always able to see the usage records of each user.



**Figure 3-3:** portal security based on personal certificate for access and on robot certificate for job submission on user behalf

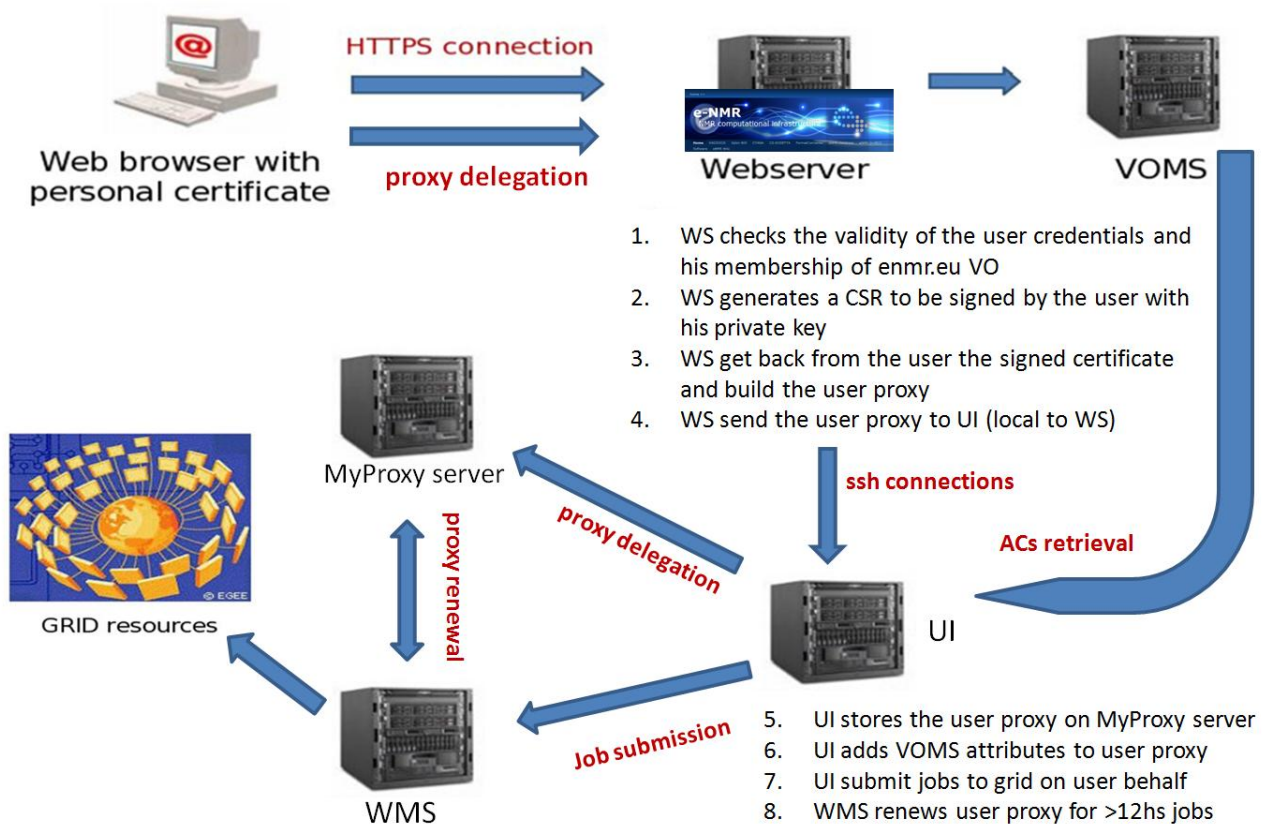
A more advanced version of the portal was developed with the goal of replacing robot-based job management with one based on user credentials via the so-called proxy delegation mechanism.

In this version, the user accessing the portal delegates his credential to both the MyProxy server and the portal web server. The latter will generate a proxy certificate to be used for job

submission on user behalf. The interaction between the user and the delegation service is managed by a java applet.

The new architecture is shown in Figure 3-4. The generation of a proxy certificate is as follows. The user does contact the delegation service running on the web server. The service creates a public-private key pair and uses it to generate a Certificate Sign Request (CSR). This is a certificate that has to be signed by the user with his private key. The signed certificate is then sent back to the service. This procedure is similar to the generation of a valid certificate by a CA and, in fact, in this context the user acts like a CA. The certificate generated so far is then combined with the user certificate, thus forming a chain of certificates. The service that examines the proxy certificate can then verify the identity of the user that delegated its credentials by unfolding this chain of certificates. Once the proxy has been created and associated to the user ID in the web server database, it is transferred on the UI local to the web server LAN and behind a firewall. Decoupling the web server hosting the portal from the UI performing the job submission adds a further level of security. In fact, user proxies created in the web server are immediately destroyed after their transfer to UI. On the other hand, the UI is carefully protected inside the private network, with the minimum set of communication ports left open in order to interact with the e-NMR grid services (VOMS, WMS and MyProxy).

Jobs are submitted to gLite WMS using the short-lived proxy (12 hours of lifetime). Jobs lasting more than 12 hours will have the short-lived proxy automatically renewed before its expiration via the gLite proxy renewal mechanism acting at WMS level using the long-lived credentials (with maximum lifetime of two weeks) stored in the MyProxy server.



**Figure 3-4:** advanced web portal security architecture

The security risks associated with the model described above are not higher than the ones normally accepted by users willing to run their applications on the EGEE grid. These risks are actually lower in our case, if we consider that in other communities most of the grid users keep their personal X509 certificate and private key permanently on the \$HOME/.globus area of shared UIs provided by their institutes. In our model the private key is used only to sign via applet the CSR generated by the web server, so it can be kept secure in the owner's laptop, in a USB key or in a smart card. Short-lived proxy certificates can of course be stolen by external attackers managing to get fraudulent access to UI, WMS, MyProxy server as well as the distributed Worker Nodes where jobs are running, other than by internal administrators of these services, but this is a general issue of the EGEE production grid. It is under the responsibility of the grid site managers to enforce strict policy on the network use to avoid the chance of their site being liable for playing a role in any malicious use such as attacks on other connected systems on the Internet.

### **3.3 Data security**

In the grid, a file is stored in a Storage Element (SE). Files cannot be modified once written, only deleted. One logical file may have several identical replicas in different SEs. Files are identified by a Logical File Name (LFN), and a file catalogue stores the connection between the LFN and pointers to any replicas. Such a pointer is known as a Site URL (SURL). The SURL may be partly specified by the user, but it can be generated automatically so for simple cases there is no need to worry about it. The gLite supported SEs expose the Storage Resource Manager (SRM) interface. SRM allows for getting the Transport URL (TURL) from the SURL. The TURL contains the information about the I/O protocol(s) which can be used for accessing or copying the files stored on the SE.

Files are also identified by a Globally Unique Identifier (GUID), which is a fixed-format string generated by the middleware and guaranteed to be absolutely unique. However, this is not very human-friendly, and for most purposes you can ignore it and just use the LFN.

The file catalogue technology currently used in the EGEE Grid is called the LCG File Catalogue (LFC). It offers a hierarchical view of files to users, with a UNIX-like client interface.

The GFAL (Grid File Access Library) library that offers to the user a POSIX-like interface to access data on various flavours of SEs.

A number of SEs and a VO level LFC have been used so far in the e-NMR grid for unencrypted data storage.

In the case of applications regarding biomedical research and clinical practice, the communities involved need to satisfy severe privacy requirements because they manage confidential data (as, for example, patient's medical history). Then, to allow a model where confidential data are saved on SEs managed by an external organization, a mechanism to prevent the administrator of the machine accessing/modifying the sensible data is required.

At the present time the gLite middleware provides the same security infrastructure for all grid services. The authentication is performed using a X.509-based PKI infrastructure and the VOMS attributes are used to authorize users according to their roles. Moreover, an authorization method based on Access Control Lists (ACL) ensures data access only by their owners. However, data are stored in a clear format. The Storage Element administrator can

access them bypassing the grid security infrastructure. This is known as the insider abuse problem.

Several solutions are available to ensure confidentiality on user data stored in the grid, e.g.:

- Secure Storage (<http://securestorage.sourceforge.net/index.html>)
- GS3 (<http://grid.ct.infn.it/twiki/bin/view/Main/GridSecureStorageSystem>)
- Encrypted Data Storage (EDS, <https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS>)

The latest one has been developed by the EGEE project, and has been widely used by the Biomedical user community in the context of Digital Imaging and Communications in Medicine (DICOM), where ensuring a high data protection level to respect patients privacy is strongly required. The Encrypted Data Storage is an encrypted data service solution which provides a system that encrypts/decrypts files and stores/retrieves them from GFAL library-compliant storage systems. It provides a client-side C library to encrypt and decrypt block level data on the fly. It uses the OpenSSL cryptographic library for the symmetric cryptography routines, thus it can utilize any of the available cipher algorithms, such as the AES cipher. For additional security and redundancy, the encryption keys used to encrypt the files are split and stored in separate keystores (Hydra servers).

Hydra is the central element in the encrypted file storage solution. The Hydra service comprises at least one Hydra server and a set of command-line interfaces to perform the basic commands. The Hydra server consists of a MySQL database and a Tomcat server that acts to contain the actual Hydra software, written in Java.

The encrypted data service solution uses the Hydra servers to store the pieces of the encryption key and their associated ACL information. Therefore the key pieces are only accessible by their respective owners. These encryption keys are split using a particular scheme, Shamir Secret-Sharing Scheme (SSSS) that provides another layer of protection. The encryption key may be split into "M" fragments and may be recovered with possession of "N" fragments, where  $N < M$ . These parameters "M" and "N" are configurable by the number of Hydra servers deployed and the SSSS algorithm respectively. In this case, the security and reliability of the overall service has been increased: an attacker would have to gain access to at least "N" Hydra keystores to recover and encryption key; a legitimate user can tolerate the loss of M-N keystores and still recover their key.

In addition, a legitimate administrator of a Hydra keystore would not have access to the full encryption key.

Encryption keys are generated in the Hydra system based upon the LFN or GUID of the file in question to be encrypted. This LFN or GUID can be retrieved from sources such as an LFC catalogue that contains the logical names and GUIDs for files inside a Storage Element. The LFN or GUID is necessary for retrieval and decryption of files.

A view of the basic operations performed with EDS is shown in figure 3-5.

Figure 3-6 shows an example use case where user encrypted data are processed on the grid by jobs submitted with the user credentials.

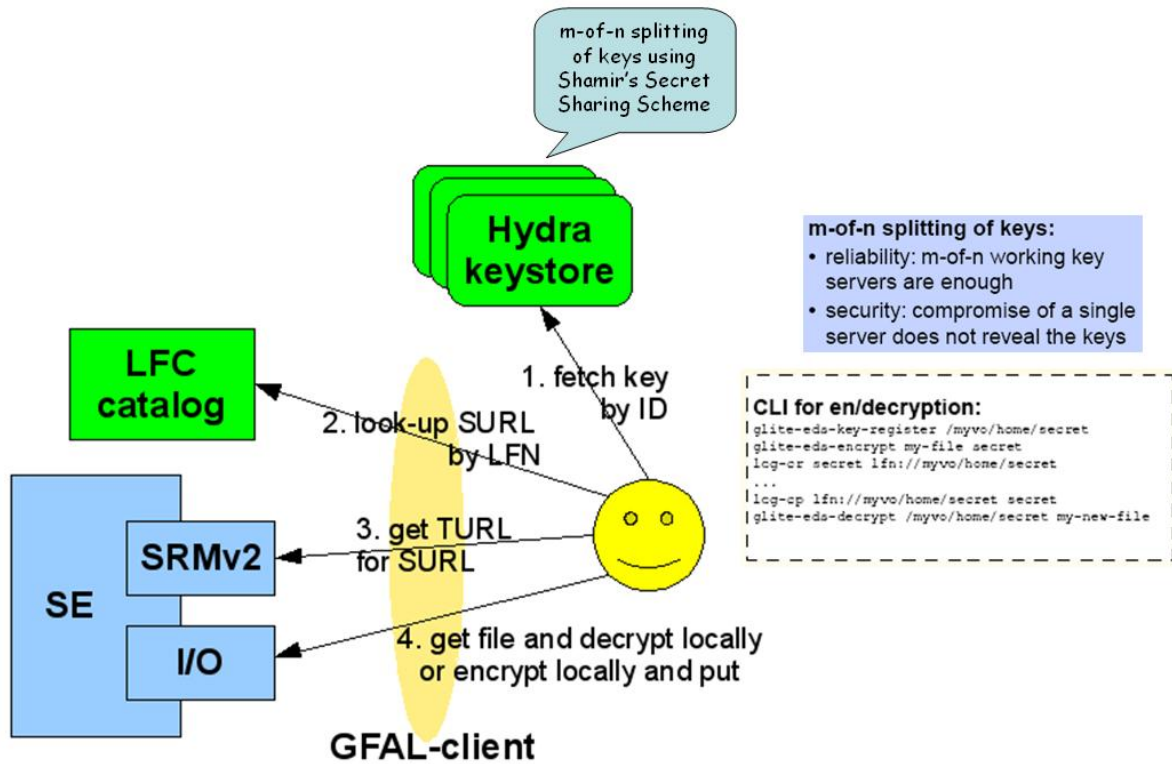


Figure 3-5: Encrypted Data Storage in gLite

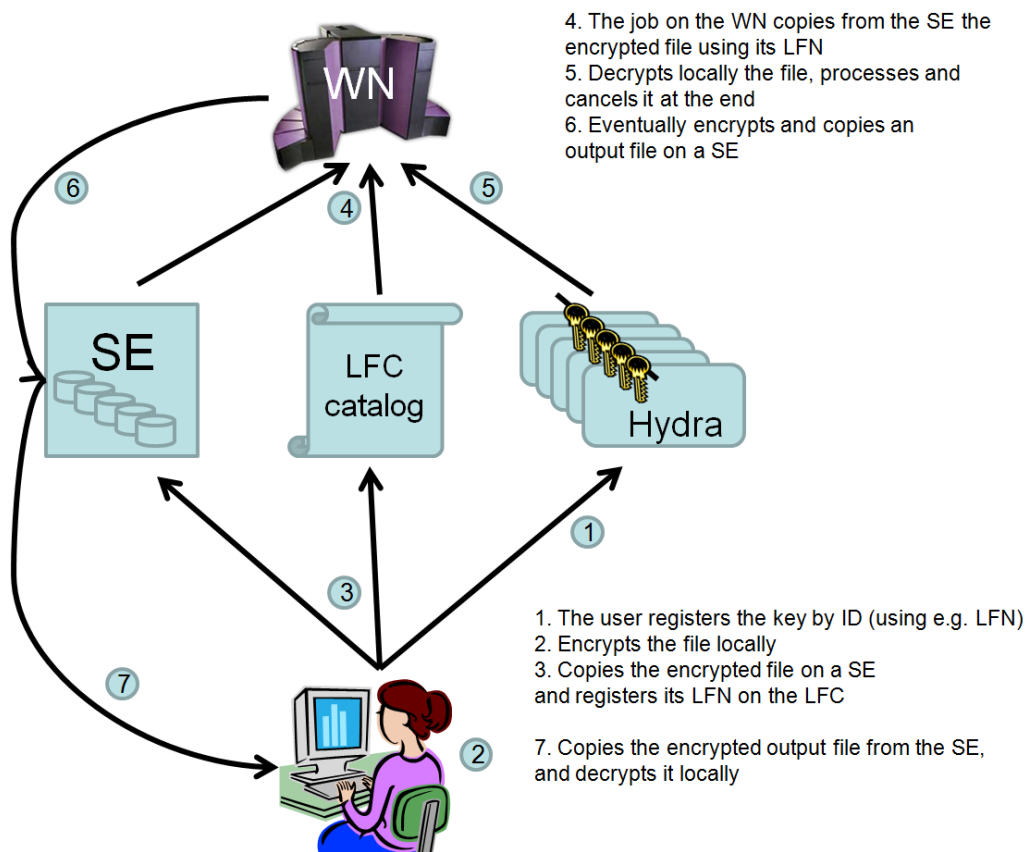


Figure 3-6: Example of Encrypted Data Storage system use case

The first release of the gLite Hydra service has been made available in December 2008, and Hydra clients are already included into gLite UI and WN profiles. It is therefore very natural to implement the EDS solution into e-NMR grid.

Five Hydra servers at the premises of the e-NMR project partners computing centres have been deployed in order to made available the EDS system to e-NMR users. The full list is given in table 3-1.

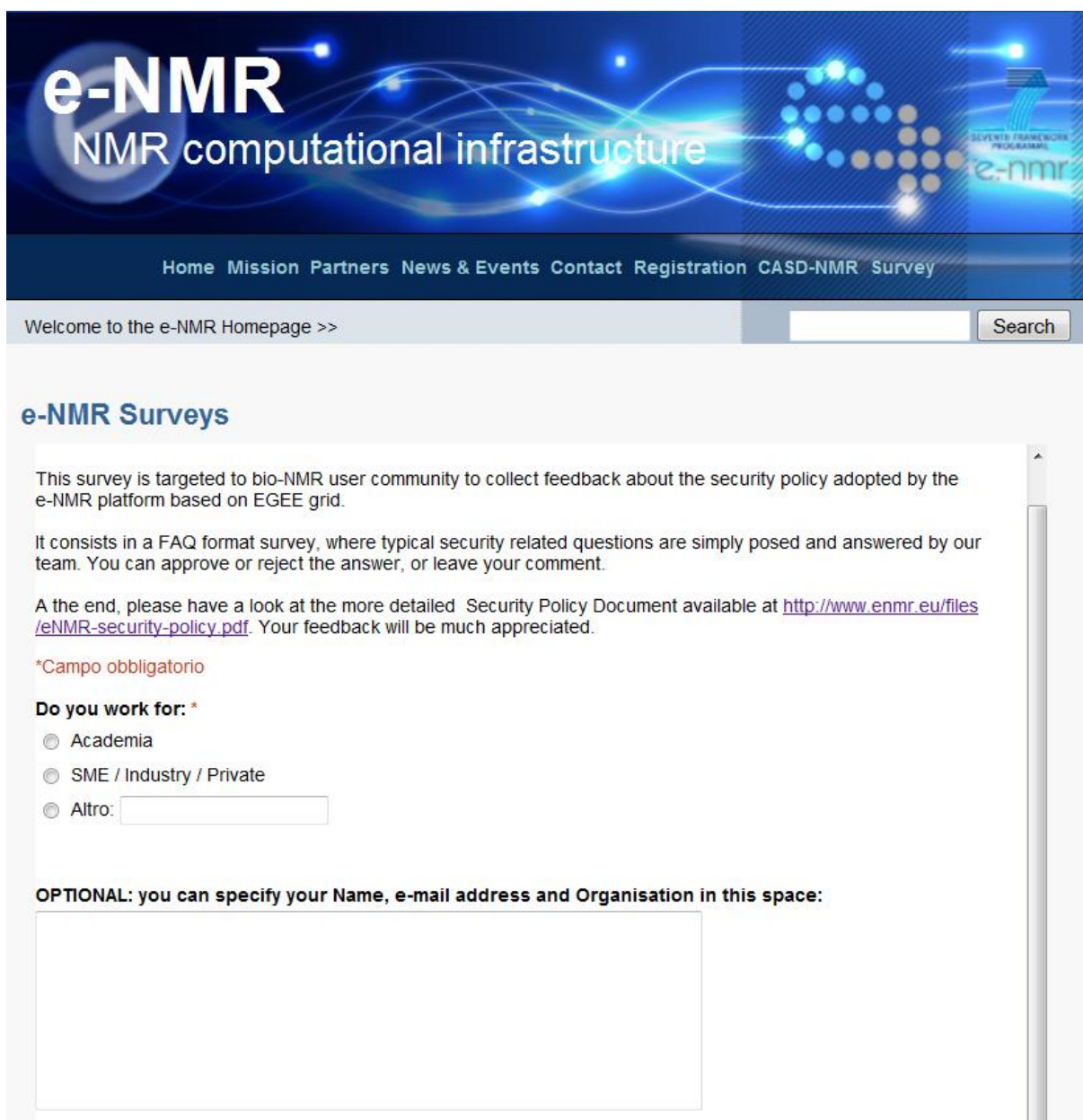
	<b>VOMS</b>	<b>LFC</b>	<b>Hydra</b>
<b>BCBR</b>	-	-	<i>hydra-enmr.chem.uu.nl</i>
<b>BMRZ</b>	-	-	<i>hy-enmr.chemie.uni-frankfurt.de</i>
<b>CIRMMP</b>	-	-	<i>hydra-enmr.cerm.unifi.it</i>
<b>INFN</b>	voms02.cnaf.infn.it, voms-02.pd.infn.it	lfcserver.cnaf.infn.it	<i>amga.pd.infn.it, egee-bdii.lnl.infn.it</i>

**Table 3.1:** List of VO specific central services for security, file cataloguing and data encryption. In *italics* the services added in the second year of the project.

## 4. The second round security survey

The second anonymous on-line survey has been proposed in October 2009 with the goal of obtaining feedback on the security policy implemented by the e-NMR project as described in the previous section. It consists in a FAQ format survey, where typical security related questions are simply posed and answered by our team. The user can approve or reject the answer, or leave his comment. At the end of the survey, the user is asked to have a look at the more detailed e-NMR Security Policy Document available on the project web site, and provide his feedback optionally.

The survey has been published on the e-NMR project web site [www.enmr.eu](http://www.enmr.eu), under the Survey menu item, and can be filled online. It has also been advertised on the BELIEF project portal ([www.beliefproject.org](http://www.beliefproject.org)), and presented at the e-NMR event held in Cambridge at the premises of the EMBL-EBI Genoma Campus in early November 2009. Here below are shown the general layout and all the questions.



**e-NMR**  
NMR computational infrastructure

Home Mission Partners News & Events Contact Registration CASD-NMR Survey

Welcome to the e-NMR Homepage >>  Search

### e-NMR Surveys

This survey is targeted to bio-NMR user community to collect feedback about the security policy adopted by the e-NMR platform based on EGEE grid.

It consists in a FAQ format survey, where typical security related questions are simply posed and answered by our team. You can approve or reject the answer, or leave your comment.

At the end, please have a look at the more detailed Security Policy Document available at <http://www.enmr.eu/files/eNMR-security-policy.pdf>. Your feedback will be much appreciated.

**\*Campo obbligatorio**

**Do you work for: \***

Academia

SME / Industry / Private

Altro:

**OPTIONAL: you can specify your Name, e-mail address and Organisation in this space:**

**If I submit my data to an e-NMR portal for a calculation, where is the data stored and is this information accessible to anyone but myself? \***

The data can be stored encrypted in specially designated machines. Even though that data could be, in principle, accessed by other people, it will be unintelligible unless one of the following happen: a) The encryption algorithm is broken b) The encryption key is compromised

- Yes, this satisfies my security requirements
- No, this does not satisfy my security requirements
- Altro:

**Is my calculation accessible to anyone but myself? \***

The result of your calculation can be encrypted in the grid computing node after the job has been executed.

- Yes, this satisfies my security requirements
- No, this does not satisfy my security requirements
- Altro:

**Are the results of the calculation deleted when I get the results back? \***

The tools the project provides to the user also delete the original data when a copy of it has been received by the user.

- Yes, this satisfies my security requirements
- No, this does not satisfy my security requirements
- Altro:

**Can anyone capture the data while being transferred? \***

Anyone can capture the data in its encrypted form. To be able to decrypt it requires breaking the encryption algorithm used.

- Yes, this satisfies my security requirements
- No, this does not satisfy my security requirements
- Altro:

**Can I allow accessing to my data by other than myself, e.g. the rest of my team or organisation? \***

Sure, you can authorize single persons, or groups, to retrieve your data and its key to decrypt it.

- Yes, this satisfies my security requirements
- No, this does not satisfy my security requirements
- Altro:

## 5. Analysis

At the time of writing (16 November 2009), the security survey was answered by 25 users, 4 of them from SME/ industry/private.

12 filled the optional field with Organisation name and/or e-mail address, with 2 SMEs among them.

The results show that the large majority of the users are satisfied by the proposed e-NMR security policy.

In fact, we got a positive answers to the above 5 questions, in particular, 88%, 92%, 96%, 92% and 96% approval to the e-NMR security measurements outlined.

A few of them including one respondent from a SME found the document too complex for non-IT security experts, and someone from Academia complained about the complexity of the registration process.

To support our analysis, some of the comments are reported here:

### **Example 1 (from Academia)**

“Security of information is a non-issue for me, and to be honest, the ridiculous and drawn out procedure which involved the acquisition of my key (during which we have to endure endless certificates flagged as 'suspicious' by our browsers) has prevented me from recommending the process to anyone else. Also, the policy linked above is neither accessible nor understandable to non-IT professionals due to the language used.”

### **Example 2 (from Academia)**

“1) I am a developer and unlikely to ever use the e-NMR grid for non-test data. I have no experience with confidential data. 2) The registration process and the underlying system are highly complex. To entrust it with confidential data I would have to be sure I understood how everything worked, whether there were potential holes, and whether the e-NMR organisation was sufficiently security-conscious. Would my data really be secure from e-NMR application developers? It would take an IT professional in my organisation to evaluate these things. Protection against casual curiosity is one thing, but for data of economic value I suspect it would be easier to run calculations in-house. 3) I have not read the document. 1) and 2) should explain why.”

### **Example 3 (from SME/Industry)**

“Looks complicated”

The majority of the users gave positive feedback, ranging from a simply OK, good, satisfied, etc. to more detailed and motivated comments. Here below we report the most significant ones.

**Example 4 (from Academia)**

“Our laboratory does not have any commercial computational tasks, which could be performed on the e-NMR grid, so, the level of security, implemented at the moment is completely sufficient for all our needs.”

**Example 5 (from SME/Industry)**

“I'd be very interested in being able to access the platform on a pay-per-job basis, analogous to paying for time at a synchrotron facility.”

**Example 6 (from SME/Industry)**

“Based on my experiences in industry, I would say that in general one is extremely careful in sending any confidential information to computers outside of the companies own network. Therefore, despite that I personally think the security measures in place seem to be more than sufficient, I would still guess that industry in general will refrain from using grid based services and will rather invest in computational resources in-house, to minimize any potential security risks. I do expect that any industrial partners that decide to participate in the e-NMR grid would be interested in paying for training (depending on the fee paid for accessing the grid). Probably best to negotiate access and training in one fee.”

## 6. Conclusions

The first round of the survey about security issues published on D3.3 had shown that the large majority of our sample surveyed was not limited by local policies in sending around their data over internet to be used as input for calculations via web servers. For the rest of the sample however a form of protection of data on grid storage elements via data encryption would have been appreciated.

Thus, it was decided to deploy at the e-NMR grid the Encrypted Data Storage system released by gLite at the end of 2008.

A detailed document describing the e-NMR security policy was created and published on the project web portal. At the same time, a second round of the survey was launched in a more simplified manner: a set of pre-defined security questions already answered by our team. The user was asked to approve or reject the answer. At the end he also had the opportunity to leave a comment about the security policy document or his thoughts about the e-NMR platform and more in general the security on the grid.

The security measures were judged as satisfactory by both academic users and industry. Some respondents from industry indicated that even if the security measures in place seem to be more than sufficient, industry in general will refrain from using grid based services and will rather invest in computational resources in-house, to minimize any potential security risks. We can conclude from this survey that our current implementation of security including the new measures described in this document is thus satisfactory.

The survey will be kept online in order to allow us for continuous feedback and monitoring of the users needs concerning security issues.