Bridging Secure WebCom and European DataGrid Security for Multiple VOs over Multiple Grids

David W. O'Callaghan and Brian A. Coghlan
Department of Computer Science,
Trinity College Dublin, Ireland.
{david.ocallaghan, coghlan}@cs.tcd.ie

***Abstract*— Secure job submission across multiple virtual organisations becomes more important as Grids proliferate. WebCom-G will bring together the condensed graph model of computing and existing Grid software from the European DataGrid (EDG) project to allow users to execute complex tasks involving multiple Grids. In this paper we discuss the security aspects of a system to allow users of existing Grids to securely execute condensed graphs containing Grid jobs. We outline the process that bridges the EDG security architecture and Secure WebCom to make this possible.**

***Index Terms*— Authentication; Authorisation; Grid; Interoperability; Security.**

I. Introduction

Grids [1] allow sharing of resources across multiple domains of administration and security. A collection of people and institutions who agree on resources sharing rules, together with associated computing, storage and network resources form a *virtual organisation* (VO) [2]. For a VO to operate successfully participants must have control over resource sharing policies through a secure infrastructure. Common Grid security requirements include the following:

Single sign on: A user must be able to authenticate once and then have access to multiple Grid resources.

Delegation: A user must be able to pass on his authority to services running on his behalf.

Integration with local security policies: Grid security must interoperate with local security infrastructure and respect local policies.

Multiple VOs

A single Grid typically supports multiple virtual organisations [2], and it is quite possible that an individual might be a member of several VOs within that Grid. Although VOs are intended to be dynamic and flexible organisations there is still necessarily some administrative overhead in setting up such collaborations. In a case where a user wants to do some action in the domain of multiple VOs it may be more convenient to use the existing VOs than to try to form a new collaboration.

Example 1: A scientist is a member of an oceanography VO and a meteorology VO. She can feed data between experiments in the two VOs to produce new and interesting results. △

Complex tasks with multiple VOs running on the same Grid can be coordinated manually, or using a work-flow system [3].

Multiple Grids

Although a single 'Great Global Grid', by analogy to the World Wide Web, is conceivable, currently multiple wide-area, independent (that is, each with an independent set of Grid services) Grids exist. A user wishing to perform inter-VO operations across multiple Grids makes coordination more difficult. The Grids might use common, interoperable software configured differently for each Grid (for example, LCG [4], CrossGrid [5] and Grid-Ireland [6]), or they might use quite different software (for example, DEISA [7]).

Example 2: A scientist combines data and software from the international ATLAS and CMS particle physics VO with compute resources on both his national Grid which does not support those VOs, and LCG, which does. △

Currently, cross-VO operations across multiple Grids must be done manually, i.e. a user must direct operations so that datasets are fed to experiment software, partial results collected, transformed and passed on to other experiment software and so on. This is tedious for any complex interactions, and may require the user to log into multiple sites using multiple credentials.

The WebCom-G [8] project proposes that inter-VO (including inter-Grid) operations can be flexibly controlled using the condensed graph model of computation [9]. This allows complex data and control dependencies to be specified, and leaves scheduling to the condensed graph policies. This article describes a framework to allow these cross-VO operations to be performed securely using the Secure WebCom trust management architecture [10] to work with Grid security services, especially those of the European DataGrid [11], as used by Grid-Ireland, CrossGrid, LCG, EGEE [12], and SEEGRID [13].

In order to do this, we first outline the security architecture of the European DataGrid project and of Secure WebCom in Sections II and III respectively. In Section IV we describe an approach for secure Grid job submission within WebCom. Finally, Section V contains discussion and conclusions.

II. DataGrid Security Architecture

The Globus toolkit [14] acts as the fundamental infrastructure used by many working Grids, providing important basic services such as data transfer and computing resource access. The Globus Grid Security Infrastructure [15] provides identity based security and simple delegation with X.509 [16] and proxy certificates.

The European DataGrid project (EDG) significantly extended the Globus middleware to provide support for workload management [17] and a relational information system [18]. The European DataGrid software is used and updated by international and European Grid projects such as CrossGrid, LCG, EGEE and SEEGRID. It also provides the basis for GridIreland, the Irish national Grid infrastructure for e-science.

Security was an important consideration for the European DataGrid project, and the Globus security architecture was significantly enhanced with Virtual Organisation membership, local authorisation and credential mapping services [19], [20]. The Security Coordination Group of the European DataGrid project collected and documented the project's security requirements [21]. EDG decided to keep a distinction between authentication and authorisation due to the more dynamic nature of authorisation information.

A. Authentication

The EDG security requirements included 17 requirements for authentication of which three important items were:

- the need of a user to authenticate just once per session;
- for interoperable authentication between many Grids and applications; and
- for the ability of authentication to be revoked in the event of loss or compromise of an identity credential.

These requirements resulted in the use of an authentication infrastructure based on the Globus Grid Security Infrastructure (GSI). GSI uses a modified form of X.509 Public Key Infrastructure (PKI) [22]. The identity of a Grid user or server is checked by a Registration Authority (RA) and certified by a Certification Authority (CA). Users and services perform mutual authentication for all interactions.

The EDG Certification Authority Coordination Group had the task of creating an actual authentication PKI, which was unique in its successful use of the technology with a large number of independently operated CAs [23]. The infrastructure was to be used for grid authentication only, and then only in the context of distributed resource access through Globus GSI. It specifically did not support long-term encryption of data or digital signatures.

A single certification authority for the whole project would not be sufficient due to concerns about scaling, trust and a single point of failure or attack. It was also considered important to achieve strong relationships between the CA and associated RAs. To meet these requirements it was decided that an appropriate scale was one CA for each participating country where possible. Hierarchical or cross-signed arrangements of multiple CAs are not compatible with Globus GSI, so a coordinated group of peer CAs appeared to be the most suitable choice.

The European Grid Authentication Policy Management Authority (EUGridPMA) for e-Science (formerly the EDG Certification Authority Coordination Group) sets minimum requirements for operating a Grid CA [24]. CAs that meet the standards can be accredited and trusted by European and international projects after an assessment of the CA's certification policies and practices. The EUGridPMA minimum requirements cover areas of CA physical security; signing namespace; uniqueness of distinguished names; and key lengths and expiration periods.

Each relying party wants to evaluate all the CAs, either that they meet the relying party's required standard, or that they meet an agreed common standard. The members of the PMA (CAs and representatives of relying parties) perform peer review of each CA to establish the common standard. This allows the construction of *Trust Matrices*, the result of which is a CA *Acceptance Matrix*. Currently the inputs used to devise these matrices are created manually, and acceptance results are used indirectly. In future we plan to make evaluation automatic and link acceptance results into the authentication process.

B. Sign-on and Delegation

With Globus GSI the 'sign-on' takes place in a distributed fashion, without a central service. A Grid user generates a proxy credential, that is, a new key-pair signed with the user's private key. This credential is used to delegate the user's authority to Grid services running on his behalf. The proxy certificate has a short lifetime (typically 12 or 24 hours) to limit the negative effects in case it is compromised.

In the validation of this proxy certificate, the basicConstraints attribute of the user's certificate (which states that it is not a CA certificate) is deliberately ignored, going against normal validation procedures. GSI proxy certificates are currently being standardised in the IETF (Internet Engineering Task Force) PKIX standards group [25].

C. Virtual Organisation Membership

In a Grid environment it is natural to grant access to resources according to a user's membership of the appropriate virtual organisation. With the standard Globus GSI approach, access depends on a user having a corresponding entry in a Grid mapfile on the target resource. This requires the site administrators to setup user accounts for all authorised users. Synchronisation of these mappings across all the sites involved in a VO is a serious administration overhead, similar to synchronising Unix passwd files manually.

An improvement within EDG was to create virtual organisation membership LDAP server which allowed VO information to be stored centrally [26]. In this way an administrator for a virtual organisation could add users as members, and manage groups within a VO. To remove the need to create individual accounts for all VO members at each site, a system was devised to lease accounts from a pool [27]. A Grid mapfile can be generated automatically from the information stored on the VO LDAP server and updated at regular intervals.

There were still a number of problems with this system. When the VO information is only updated daily, a new user has to wait up to 24 hours for all sites to update. The same problem exists if a VO manager wishes to make changes to group membership. In response to these issues, and also to provide more fine-grained authorisation, EDG, in conjunction with DataTAG [28], developed a new VO service, the Virtual Organisation Membership Service (VOMS) [29].

VOMS allows the user contact the server to acquire a credential that contains virtual organisation information. This means that a user can acquire a VO credential as soon as she has been added to the virtual organisation. When the VO administrator modifies her group membership, allowed rôles or capabilities, she can acquire an updated credential as soon as the change is made. A user can contact multiple VOMS servers to accumulate credentials for several VOs.

VOMS provides a relatively convenient administrative interface. An authenticated and authorised virtual organisation manager can add users, define group membership, and assign rôles and capabilities. Any authenticated user can request virtual organisation or group membership, rôles and capabilities and the administrator can grant these as appropriate.

To perform a Grid operation, a user requests a short-lived credential from the VOMS server for the virtual organisation in question, specifying which groups, rôles and capabilities he wants to use. If the user is authorised, the service generates and signs a short-term attribute certificate [30] containing the VO information as an optional extension to the GSI proxy certificate. The VOMS-extended credential may be used in a backwards-compatible fashion with standard GSI services.

D. Authorisation and Credential Mapping

The EDG Local Centre Authorisation Service (LCAS) [31] is an authorisation decision engine that can add access control to underlying Grid services such as the Globus gatekeeper or GridFTP server. LCAS provides a plugin framework to allow flexible authorisation setup. The authorisation plugins work together to reach a collective decision based on the resources requested, the identity of the requester from the delegated proxy certificate, and any further credentials the requester may have, such as VOMS virtual organisations, groups, rôles and capabilities. Plugins exist which support

- banned and allowed user lists;
- access control lists based on VOMS attributes; and
- 'opening hours' access based on the time and date when a request is received.

The EDG Local Credential Mapping Services (LCMAPS) [31] provides a flexible system to map Grid users to local credentials on Grid sites. LCMAPS supports plugin modules to support a variety of mappings:

- static mapping from a Distinguished Name onto a local Unix account and group;
- mapping to leased account from a pool of accounts;
- mapping VOMS groups, roles and capabilities onto Unix groups, possibly from a pool of groups, analogous to the pool of accounts; and
- mapping from a Distinguished Name onto local AFS tokens.

The credential mappings that are in effect for the execution of a Grid job are recorded in a job repository, which allows some level of auditing.

To support Java services, the Java Trust Manager and Java Authorisation Manager were developed [32]. The Trust Manager provides Java support for GSI proxy credentials, and the Authorisation Manager handles authorisation for services running in a Java servlet environment such as Tomcat. These services are used in the EDG Spitfire database server and in the R-GMA Grid information system.

III. Secure WebCom Security Architecture

Secure WebCom provides a KeyNote-based trust management system for the WebCom distributed computing architecture [10]. Here we outline condensed graphs, trust management and the combination of these in Secure WebCom.

A. Condensed Graphs and WebCom

WebCom [33] implements the condensed graph model of computation [9]. Programs are defined as graphs of nodes which have operator, operand and destination edges. Nodes can represent atomic tasks or can be 'condensed' nodes containing a further sub-graph of nodes. Evaluation can be made according to eager, lazy or imperative models, and the evaluation models can be mixed within a single graph. Nodes need not concern themselves with synchronisation or concurrency, as these issues are implicit in the condensed graph structure.

WebCom distributes evaluation of a graph over a network of computers. It has a modular structure allowing support for different load balancing, fault tolerance, connection, security and execution methods. The system is architecture neutral in that load balancing and other features are independent of how a task is executed by a node. WebCom masters can schedule tasks to WebCom clients. In turn, WebCom clients can be promoted to client-masters who can schedule sub-graph tasks to other clients [34].

B. Trust Management and KeyNote

Trust management [35], [36] is an approach to security which unifies the specification of security policies, trust relationships and credentials. A credential directly represents the subject's authorisation as delegated by some authority, and it will be respected if that authority is recognized by local policy. This is in contrast to a traditional identity-based access-control approach where access is granted based on who is making a request, and the local access control policy for that request. In such cases it is often necessary to know in advance about all possible users. In a trust management system cryptographic keys are used to identify authorisers and licensees. An authoriser creates a credential containing the licensee's public key and the appropriate authorisation attributes, and signs it with his private key.

KeyNote [37], [38] is an implementation of a trust management system. It provides a compliance checker which is used to verify credentials against the local security policy, and a simple application programming interface. The KeyNote compliance checker provides a standard mechanism for verifying credentials against policy, taking this task away from the application programmer. Credentials and policies (collectively assertions) have a simple, expressive format. The only difference between a credential and a policy assertion is that a local policy is unconditionally trusted. Assertions are created and managed independent to the application, separating the security policy from the application functionality.

C. Secure WebCom

Secure WebCom uses KeyNote to provide a trust management architecture for condensed graph execution. The Secure WebCom environment interacts with KeyNote through its API, meaning that each WebCom node does not need to make any security decisions internally. Synchronisation, concurrency and trust management are all handled transparently by the Secure WebCom environment.

When a task is to be scheduled to a Secure WebCom client by a master, the pair perform mutual authentication with X.509 certificates over an SSL connection. Once authenticated, the pair exchange KeyNote credentials. The client determines if the master is authorised to schedule tasks to it and, similarly, the master checks that the client is authorised to execute that task. Authorisation policy for scheduling and execution is specified independently of the node software. This further increases the separation between policy and functionality.

IV. Towards Secure WebCom–Grid Security Interoperation

The WebCom-G project proposes that inter-VO (including inter-Grid) operations can be flexibly programmed using the condensed graph model of computation. As with other WebCom nodes, Grid jobs may be executed on eager, lazy or imperative schedules. There are a family of possible solutions for authorisation.

A. Credential Creation

Both EDG and Secure WebCom currently use cryptographic keys to identify users and services. The existing Grid projects have strong requirements on the operation of certification authorities they trust, reflected in the policies of the European Grid Authentication Policy Management Authority. Secure WebCom does not yet have such requirements, but to interoperate with existing Grids the roots of trust must be accepted and, most particularly, users must have an existing Grid certificate signed by one of the trusted CAs. The binding of an identity to a public key is outside the domain of KeyNote. However, for a KeyNote authority to know to whom it is issuing credentials, a X.509-type public key infrastructure is desirable. This eliminates the need for out-of-band verification of identity by the KeyNote credential issuer, as in the PGP model [39].

We propose an online Credential Creation Authority (CCA) which generates KeyNote credentials to authenticated users on demand. Figure 1 shows a number of possible interactions with this service. The various arcs and sequences of arcs are referred to below.

The CCA must have a X.509 service certificate, and requests must be made over a mutually authenticated SSL channel, possibly with GSI and VOMS extensions. Mutual authentication will succeed if either:

- the request comes on arc 1_a from a user with a certificate from a trusted certification authority, and the certificate is not on the certificate revocation list; or
- the request comes on arc 1_b or 1_c from a user with a valid proxy certificate, signed by a certificate from a trusted certification authority, and the certificate is not on the certificate revocation list. See the discussion of proxies below.

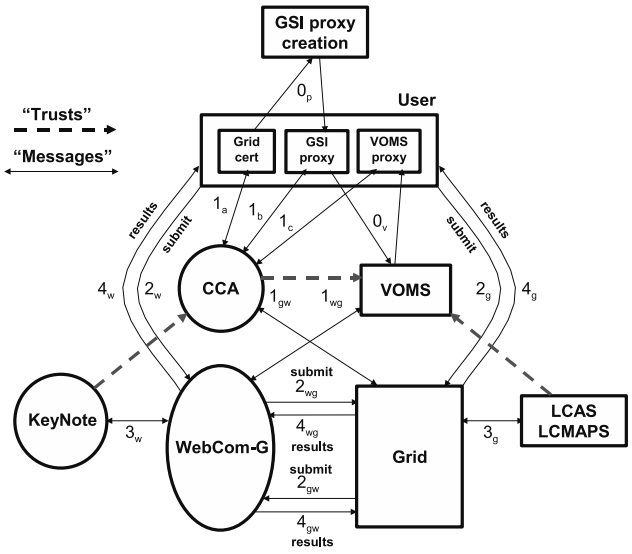

Fig. 1. Credential Creation and Job Submission

If mutual authentication succeeds a credential is generated, signed and issued for the user. Figure 2 shows the KeyNote assertion representing the root of trust in the Credential Creation Authority.

```
Authorizer: "POLICY"
licensees: Key_CCA
Conditions: App_Domain == "WebCom-G" &&
Operation == "GridSubmit"
```

Fig. 2. Credential Creation Authority policy.

The KeyNote credential should be short-lived (e.g. 12 or 24 hours) to respond to changes in the certificate revocation lists or the set of trusted CAs. It may desirable that the credential should prevent further delegation, as each credential needs to be related directly to a Grid certificate. However, in some cases there is a valid reason for allowing the user to associate another Grid credential with their KeyNote credential, and this should not be precluded by design.

There are a number of alternatives for the authorisation that the CCA delegates to users. The first possibility is that the CCA could delegate the same coarse-grained authorisation to all authenticated users, authorising a generic 'Grid submit' operation and only limiting the time of validity, thereby effectively shifting the authorisation policy decision to the underlying Grid mechanisms. An example credential based on this proposal is shown in Figure 3.

At the other extreme, the CCA could create credentials specific to each user. However, this would require an access control database which would effectively replicate the Grid authorisation policy.

In each case the original credential request to the CCA could

```
Authorizer: Key_CCA
licensees: Key_DavidOC
Conditions: App_Domain == "WebCom-G" &&
Operation == "GridSubmit" &&
NotAfter == "2004-02-03 22:25:58" &&
_ACTION_AUTHORIZER==Key_DavidOC
Signature: <signed by CCA>
```

Fig. 3. Example credential issued by Credential Creation Authority authorising DavidOC to perform the GridSubmit operation, with an expiration date, and preventing further delegation.

already contain some authorisation attributes. This would be the case if a proxy certificate with VOMS extensions was used to authenticate on arc 1_c. In this case, if the CCA trusts the attribute authority, the authorisation attributes could be encoded in the KeyNote credential. An example credential based on this proposal is shown in Figure 4.

```
Authorizer: Key_CCA
licensees: Key_DavidOC
Conditions: App_Domain == "WebCom-G" &&
Operation == "GridSubmit" &&
NotAfter == "2004-04-26 22:25:58" &&
VO == "ScienceGrid" &&
VOGroups == "Users" &&
VORoles == "Scientist"
Signature: <signed by CCA>
```

Fig. 4. Example credential issued by Credential Creation Authority authorising DavidOC to perform the GridSubmit operation, with an expiration date, and containing VOMS VO, group and rôle attributes.

B. Proxy Credentials

To use Grid resources a user needs at a minimum a valid GSI proxy certificate. The proxy can be placed under the control of the Secure WebCom environment so that it can perform Grid operations on behalf of the user. This proxy certificate cannot be generated directly by WebCom as this would require that the WebCom client in question has access to the user's private key. Instead the proxy certificate must be generated under the user's control via arc 0_p for a GSI proxy, or arcs 0_p–0_v for a VOMS proxy.

The proxy certificate can be obtained before the KeyNote credential, or later. If the proxy is obtained first, it can be used to authenticate with the Credential Creation Authority on arcs 1_b or 1_c. Allowing proxy authentication here has several benefits: the proxy credential can be bundled with the KeyNote credential and, perhaps more importantly, a Grid job holding the user's proxy can sign-on and invoke WebCom graphs on the user's behalf. This corresponds to the arcs 1_{gw}–2_{gw}–3_w–4_{gw} in Figure 1.

For the user's convenience, the generation of the Grid proxy certificate (if required) and of the KeyNote credential can be wrapped in a single command initiated from a web portal or command-line interface. If the proxy is not created in advance, and the user authenticates with his Grid certificate, then the proxy does not need to be created until it is required for Grid job submission, but control will have to return to the user for this step.

In a traditional GSI environment, a user's Grid proxy certificate is held on the user's personal workstation or on trusted Grid services. In the proposed system, the Secure WebCom environment will have access to the proxy certificate in order to operate on the user's behalf. It is important that the user's proxy certificate is handled securely by WebCom and is not exposed to WebCom clients which are not authorised to schedule Grid jobs. Access to a user's proxy should be controlled by a Grid-specific extension to the existing authorisation between Secure WebCom masters and clients.

With respect to the alternatives proposed for authentication with the Credential Creation Authority, delegation of authority, and the use of proxy certificates, we recommend that:

- proxy certificates are created in advance and used for authenticating with the CCA; and
- authorisation is given for a generic 'Grid submit' operation.

This allows a Grid job holding the user's proxy certificate to invoke a WebCom graph, and it makes the job of the CCA easier than if per-user credentials were to be issued, without precluding these. It further allows propagation of VO authorisations from graphs that submit Grid jobs that themselves spawn child graphs which need these authorisations, whether the parent Grids support these VOs or not. This is a key concept for modularisation of Grid software.

C. Job Submission

To facilitate Grid job submission via Secure WebCom it is necessary to define a WebCom node to represent a Grid job. With respect to security, the representation must have attributes for the Grid to be submitted to, the virtual organisation involved, and group membership, rôle and capability information that the user deems necessary and sufficient. It is important to note that a user may not want to, and probably should not, use all available group, rôle and capability privileges for every Grid action.

When the WebCom environment determines that a Grid job node is to be executed it checks via arc 3_w if the user's KeyNote credential permits Grid execution. This decision is made using KeyNote and without contacting the Grid security services. If the action is permitted the security attributes are used. If required VO attributes are not already held, WebCom contacts the appropriate virtual organisation membership services via arc 1_{wg}, with the parameters specified by the user, authenticating with the user's proxy certificate. If the requests are successful, WebCom will hold suitable credentials to submit the Grid job and retrieve the results when they are available.

In the general 'lazy' case, for each Grid job in a graph WebCom will fetch the appropriate VO credentials 'just in time'. It may be desirable that all credentials needed for a graph are acquired as early as possible. This would avoid the inconvenience of a graph failing after a long period of execution because a request for a credential for the next

grid job was rejected (for whatever reason). If the credential fetching operation is itself specified as a WebCom node, it can be scheduled according to an eager evaluation policy to achieve this behaviour, or according to an imperative policy for the more general case. It would also be possible to reuse credentials if two or more Grid job nodes specify the same VO information. This could be encoded explicitly in the graph or determined automatically by the environment.

Logically, for a user to submit a WebCom job that has no Grid interactions the sequence of events would be:

- The user acquires appropriate Grid credentials via arcs 0_p–0_v.
- The user signs on to WebCom with Grid credentials via arcs 1_a, 1_b or 1_c to create KeyNote credentials.
- The user submits the WebCom job via arc 2_w.
- WebCom checks via arc 3_w that the user is authorized.
- The WebCom job completes execution and the results are returned via arc 4_w.

For a user to submit a Grid job that has no WebCom interactions the sequence would be:

- The user acquires appropriate Grid credentials via arcs 0_p–0_v.
- The user submits the Grid job via arc 2_g.
- The Grid checks via arc 3_g that the user is authorized.
- The Grid job completes execution and the results are returned via arc 4_g.

It is clear that the interactions are so nearly symmetric that except for the first step the same sequence is obeyed, but with 'WebCom' changed to 'Grid' and subscript w changed to g.

For a WebCom job to submit a job to the Grid the sequence of events would be:

- WebCom gets the necessary Grid credentials via arc 1_{wg}.
- WebCom submits the Grid job via arc 2_{wg}.
- The Grid checks via arc 3_g that the user is authorized.
- The Grid job completes execution and the results are returned via arc 4_{wg}.

In this case the interactions are fully symmetric so for a Grid job to submit a job to WebCom the very same sequence is obeyed but with 'WebCom' exchanged with 'Grid' and subscripts w exchanged with g.

Each WebCom node that represents a Grid job could be represented as a subgraph with nodes for each step:

- Acquire the VO credential
- Stage input data appropriately
- Submit the Grid job
- Wait for the job status to indicate completion
- Collect the results

By separating the process into stages we can have WebCom schedule these stages according to different evaluation policies. For example, WebCom could submit a job to the Grid eagerly but collect the results lazily, as shown in Figure 5.

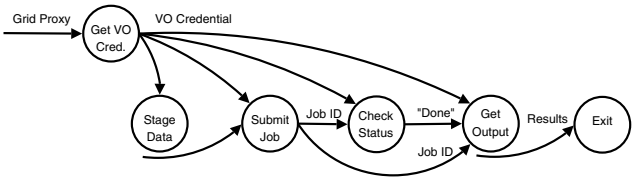

Fig. 5. Condensed Graph for Grid Job Submission

V. Conclusion

In this paper we have described the security aspects of using the Secure WebCom environment to coordinate operations across multiple virtual organisations and multiple Grids.

We have proposed in some detail a method for authorising Grid jobs from within the Secure WebCom environment. We have focused on existing Grids based on the European DataGrid software, such as LCG and Grid-Ireland, but this proposal applies more generally to Grids based on the Globus Grid Security Infrastructure with extensions for virtual organisation membership. A useful side-effect is to allow a single sign-on facility for Secure WebCom and GSI-based Grids, by generating Secure WebCom credentials from Grid certificates, and also to allow WebCom graphs be invoked by Grid jobs.

A major goal of the WebCom-G project is deep integration between WebCom and Grid services such as resource brokerage; logging and bookkeeping; and the relational Grid information service, as provided in the European DataGrid project. Deeper integration between the Secure WebCom and EDG security models is also planned. A framework for Secure WebCom interoperability with middleware rôle-based access control (RBAC) policies has been proposed by Foley *et al.* [40] that allows translation between middleware-specific RBAC policies and a generic KeyNote policy format, but this does not yet support the new VO mechanisms implemented on existing Grids. Implementing an interface for VOMS, LCAS and LCMAPS in this framework would be a major step in providing the necessary integration. The result would be a system that would, for the first time, enable the use of multiple VOs over multiple Grids simultaneously.

References

[1] I. Foster and C. Kesselman, Eds., *The Grid: Blueprint for a Future Computing Infrastructure*, 1999.

[2] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the grid: Enabling scalable virtual organizations," *International Journal of SuperComputer Applications*, vol. 15, no. 3, 2001.

[3] E. Deelman, J. Blythe, Y. Gil, C. Kesselman, G. Mehta, K. Vahi, K. Blackburn, A. Lazzarini, A. Arbree, R. Cavanaugh, and S. Koranda, "Mapping abstract complex workflows onto grid environments," *Journal of Grid Computing*, vol. 1, no. 1, pp. 25–39, 2003.

[4] LHC Computing Grid. [Online]. Available: http://lcg.web.cern.ch/

[5] CrossGrid. [Online]. Available: http://www.crossgrid.org/

[6] Grid-Ireland. [Online]. Available: http://www.grid-ireland.org/

[7] Distributed european infrastructure for supercomputing applications. [Online]. Available: http://www.deisa.org/

[8] J. P. Morrison, B. A. Coghlan, A. Shearer, and R. Perrott. WebCom-G: Grid middleware to hide the grid.

[9] J. Morrison, "Condensed graphs: Unifying availability-driven, coercion-driven and control-driven computing," Ph.D. dissertation, Eindhoven, 1996.

[10] S. Foley, T. Quillinan, J. Morrison, D. Power, and J. Kennedy, "Exploiting KeyNote in WebCom: Architecture neutral glue for trust management," in *Proc. Fifth Nordic Workshop on Secure IT Systems*, October 2000, pp. 101–119.

[11] European DataGrid. [Online]. Available: http://www.edg.org/

[12] Enabling Grids for E-science in Europe. [Online]. Available: http://public.eu-egee.org/

[13] South Eastern European Grid-enabled eInfrastructure Development. [Online]. Available: http://www.see-grid.org/

[14] I. Foster and C. Kesselman, "Globus: A metacomputing infrastructure toolkit," *International Journal of Supercomputer Applications*, vol. 11, no. 2, pp. 115–128, 1997.

[15] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke, "A security architecture for computational grids," in *ACM Conference on Computers and Security*. ACM Press, 1998, pp. 83–91.

[16] R. Housley, W. Polk, W. Ford, and D. Solo, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Apr. 2002, RFC 3280. [Online]. Available: ftp://ftp.isi.edu/in-notes/rfc3280.txt

[17] G. Avellino, S. Beco, B. Cantalupo, A. Maraschini, F. Pacini, M. Sottilaro, A. Terracina, D. Colling, F. Giacomini, E. Ronchieri, A. Gianelle, R. Peluso, M. Sgaravatto, A. Guarise, R. Piro, A. Werbrouck, D. Kouřil, A. Křenek, L. Matyska, M. Mulač, J. Pospíšil, M. Ruda, Z. Salvet, J. Sitera, J. Škrabal, M. Voců, M. Mezzadri, F. Prelz, S. Monforte, and M. Pappalardo, "The DataGrid workload management system: Challenges and results," *Journal of Grid Computing*, Submitted for review.

[18] A. Cooke, A.Gray, L. Ma, W. Nutt, J. Magowan, P. Taylor, R. Byrom, L. Field, S. Hicks, J. Leake, *et al.*, "R-GMA: An information integration system for grid monitoring," in *Proc. Eleventh International Conference on Cooperative Information Systems*, 2003.

[19] *Security Design*, DataGrid Security Coordination Group, March 2003, https://edms.cern.ch/document/344562.

[20] *Final Security Report*, DataGrid Security Coordination Group, January 2004, https://edms.cern.ch/document/414762.

[21] *Security Requirements Testbed 1 Security Implementation*, DataGrid Security Coordination Group, May 2002, https://edms.cern.ch/document/340234.

[22] PKIX Charter. IETF. [Online]. Available: http://www.ietf.org/html.charters/pkix-charter.html

[23] J. Astalos, R. Cecchini, B. A. Coghlan, R. D. Cowles, U. Epting, T. Genovese, J. Gomes, D. Groep, M. Gug, A. B. Hanushevsky, M. Helm, J. Jensen, C. Kanellopoulos, D. P. Kelsey, R. Marco, I. Neilson, S. Nicoud, D. W. O'Callaghan, D. Quesnel, I. Schaeffner, L. Shamardin, D. Skow, M. Sova, A. Wäänänen, P. Wolniewicz, and W. Xing, "International grid CA interworking, peer review and policy management through the european datagrid certifi cation authority coordination group," *Journal of Grid Computing*, Submitted for review.

[24] European grid policy management authority for e-science. [Online]. Available: http://www.eugridpma.org/

[25] S. Tuecke, V. Welch, D. Engert, L. Pearlman, and M. Thompson, *Internet X.509 Public Key Infrastructure Proxy Certificate Profile*, December 2003, http://www.ietf.org/internet-drafts/draft-ietf-pkix-proxy-10.txt.

[26] J. A. Templon and D. A. Groep. (2001) VO server information. [Online]. Available: http://marianne.in2p3.fr/datagrid/documentation/ldap-doc.pdf

[27] Pool accounts patch for Globus. [Online]. Available: http://www.gridpp.ac.uk/gridsite/gridmapdir/

[28] DataTAG. [Online]. Available: http://datatag.web.cern.ch/datatag/

[29] R. Alfi eri, R. Cecchini, V. Ciaschini, L. dell Agnello, A. Frohner, A. Gianoli, K. Lőrentey, and F. Spataro, "VOMS, an authorization system for virtual organizations," in *1st European Across Grids Conference, Santiago de Compostela, 13–14 February*, 2003.

[30] S. Farrell and R. Housley, *An Internet Attribute Certificate Profile for Authorization*, Apr. 2002, RFC 3281. [Online]. Available: ftp://ftp.isi.edu/in-notes/rfc3281.txt

[31] LCAS, LCMAPS and job repository documentation. DataGrid Work Package 4. [Online]. Available: http://www.dutchgrid.nl/ DataGrid/wp4/

[32] EDG Java security. [Online]. Available: http://edg-wp2.web.cern.ch/edg-wp2/security/edg-java-security.html

[33] J. Morrison, D. Power, and J. Kennedy, "A condensed graphs engine to drive metacomputing," in *Proc. international conference on parallel and distributed processing techniques and applications (PDPTA 1999)*, Las Vegas, Nevada, June 28 – July 1, 1999.

[34] J. Morrison and D. Power, "Master promotion and client redirection in the webcom system," in *Proc. international conference on parallel and distributed processing techniques and applications (PDPTA 2000)*, Las Vegas, Nevada, June 26–30, 2000.

[35] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "The role of trust management in distributed systems security," in *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, Vitek and Jensen, Eds. Springer-Verlag, 1999.

[36] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Proc. IEEE Symposium on Security and Privacy*, 1996.

[37] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, *The KeyNote Trust-Management System Version 2*, Sept. 1999, RFC 2704. [Online]. Available: ftp://ftp.isi.edu/in-notes/rfc2704.txt

[38] M. Blaze. (2001, March) Using the KeyNote trust management system. [Online]. Available: http://www.crypto.com/trustmgt/

[39] P. R. Zimmermann, *The official PGP user's guide*. MIT Press, 1995.

[40] S. Foley, T. Quillinan, M. O'Connor, B. Mulcahy, and J. Morrison, "A framework for heterogeneous middleware security," in *Proc. 13th International Heterogeneous Computing Workshop*. NM, USA: IEEE Press, April 2004.