# Domain Account Model

Giulio Galiero, Paolo Roccetti, and Andrea Turli

Engineering Ingegneria Informatica SpA, Roma RM 00185, Italy
{giulio.galiero,paolo.roccetti,andrea.turli}@eng.it

**Abstract.** The use of gateways as a user-friendly way to access the Grid is increasing, as evidenced, for example, by the popularity of TeraGrid Science Gateways. Such gateways, however, imply additional layers of software abstraction, which in turn implies more levels of trust delegation - thus compounding security problems of enforcing trust at different layers.

In this paper we present the Domain Account Model (DAM), extending the Shibboleth and GridShib ones to enable interoperability between identity-based (i.e. GSI) and attribute-based (i.e. SAML) Grid authorization mechanisms, to ease the administration of user attributes by allowing domain separation between Real and Virtual Organizations (VO), and to improve the trust management by means of the OAuth protocol.

## 1 Introduction

Identity fragmentation over different administrative domains has recently been recognised as one of the main usability issues of multidomain systems [1]. The lack of consistent identity management in Grids denies users a seamless experience in the access and usage of resources belonging to different administrative domains. This problem has been addressed in grid systems [2] by leveraging Public Key Infrastructures (PKI) to provide each user with credentials that can be shared among different domains. A limitation of this solution, however, is the lack of privacy that comes from the need to expose the entire user certificate to other parties.

In addition, users must manage their own credentials, which limits the wide usage of grids. A common solution, for example, is to store credentials in an online repository (e.g. MyProxy [3]) and delegate them to portals and services. The underlying security mechanisms in such systems, however, are not transparent to end users, and often require significant user effort to operate.

This paper first enlarges upon existing approaches to these problems (section 2), highlighting additional open issues, and then proposes the Domain Account Model (DAM) as a potential solution (section 3).

## 2 Existing Models

In recent years various models have been put forward to handle Identity Management issues. In Shibboleth [4] and OpenID [5], Identity Providers (IdP) are responsible for authenticating users within their home domain and releasing signed

I. Lovrek, R.J. Howlett, and L.C. Jain (Eds.): KES 2008, Part II, LNAI 5178, pp. 363–370, 2008.

SAML assertions of authenticity (Security Assertions Markup Language [6]). These assertions can be used by federated resources, namely Service Providers (SP), to enforce authorization at resource domains. Shibboleth also allows users to control which attributes can be released to each SP, thus preventing unneeded disclosure of user information.

The Community Account Model (CAM) [7] (developed as part of the TeraGrid project) employs the notion of a web gateway as a usable and scalable solution to access grid resources. Usability is achieved by authenticating users into the TeraGrid 'Science Gateway' with traditional methods (e.g. username/password) - so that users no longer need to possess and manage an X.509 certificate as an explicit authentication/autorization token ("X.509 unawareness"). Scalability is obtained through attribute-based authorization. On the down side, CAM only allows coarse grained authorization to be enforced on grid services, as all community users access protected resources using the identity of the Gateway (whose credentials are located at the gateway itself).

The limitations of CAM are addressed in the GridShib project [8] which integrates the gateway approach with the IdP paradigm provided by the Shibboleth architecture [4]. SAML assertions released by the IdP are pushed to the Shib-enabled Gateway for authorization. Once assertions are verified by the SP, the GridShib SAML tool (GS-ST) enables the Gateway to bind them to new proxy credentials. These credentials can then be used to authenticate to a Shib-enabled Resource running in a Globus Toolkit (GT) container. When a request is received by the container, credentials are parsed by the GridShib For Globus Toolkit (GS4GT) plugin to extract IdP assertions. This allows resource providers to enforce authorization on a user-attribute basis [9]. The user can also create SAML attributed proxy credentials on-demand using the Shib-enabled GridShib Certification Authority (GS-CA). This component authorizes users according to SAML assertions released by the IdP, and embeds these assertions in short-lived proxy credentials. The user can then contact resources directly, i.e. bypassing the Science Gateway.

### 2.1 Open Issues

The identity management mechanisms described in the previous section protect user privacy and increase the usability of grid resources. Nevertheless, our own experience with these models has revealed some open issues.

First of all the model depicted by GridShib only refers to containers capable of handling user attributes as SAML assertions; therefore it cannot be considered as a global comprehensive solution. Typically, resources accessible through a Gateway are deployed in containers belonging to different administrative domains. Each domain can apply local policies for managing and upgrading its own containers. Thus, it is likely that some of these resources will still be protected using identity-based authorization (e.g. gridmap-files), which is not well supported by GridShib. In fact, within the GridShib model resources can be accessed in two ways: either (1) through the Gateway, using proxy credentials of the Gateway itself, or (2) directly, using proxy credentials released by the GS-CA. As such, there is an inconsistency in accessing gridmap-protected resources.

A second limitation of the Shibboleth and Gridshib models is the poor support for Virtual Organizations (VOs). VOs are a foundational concept in grid computing: they are made up of different Real Organizations (ROs) members, entitled to access and share resources. VO-specific attributes are usually assigned to VO members (e.g. roles, as in the RBAC model [10]) to enable a scalable VO administration. In existing models, VO-specific attributes need to be maintained and released by the IdPs of ROs. However this solution faces scalability problems as the number of VOs and of ROs involved in the VO increases - since each SP needs to trust every IdP of every RO involved in the VO. The presence of multiple, distributed IdPs likewise compounds the problem of VO administration.

Finally, existing models do not offer a solution to limit the actions performed by entities delegated by the users. Access to the basic Grid services is typically achieved by stacking up software layers in increasing levels of abstraction. This enhances usability by hiding the innermost complexities of the infrastructure, but also increases the levels of trust delegation: a multi-layered architecture needs to implement security mechanisms to enforce trust at each level. In certain scenarios, user's consent must be requested when a delegated entity acts on her behalf in order to prevent malicious behaviour and increase trustworthiness.

## 3 The Domain Account Model

In this section we introduce the Domain Account Model (DAM) - which builds upon existing models to address the open issues described in 2.1.

The main innovation in the DAM is the adoption of Virtual Organizations as contexts of resource sharing. VO resources can be accessed by means of VOs easy-to-use graphical interface, known as gateways. Usability can greatly benefit from gateways, but this comes at a cost to security - since the gateway is enabled to act on the user's behalf, once she has logged into the gateway. In DAM, however, the Gateway has less autonomy and acts more as an intermediary, enabling users to access resources in the context of a VO. It is worth noting that a single Gateway can be bound to a number of VOs. The adoption of VOs in this way, has three main consequences.

Firstly, there is the need to support interoperability between identity-based and attribute-based authorization. In DAM, user proxy credentials released by a VO-specific Certification Authority (VO-CA) are required to access resources (either directly by users, or by the gateway on the users behalf).

Secondly, there is the need to separate user attributes into two sets: RO-specific attributes and VO-specific ones. RO-specific attributes are maintained and released by the IdP of the RO the user belongs to, while VO-specific attributes are released by an Authorization Authority managed in the context of the VO (VO AA). To access VO resources the Gateway needs to include VO-specific attributes in the users proxy credentials.

Thirdly, as the Gateway is just an intermediary between users and resources, there is a need to support advanced trust scenarios between the user and the Gateway itself. The approach taken in DAM entails controlling the gateway

access both to the VO CA and to the VO AA. Two main scenarios have been identified, depending on the level of trust the user places on the gateway. In the first scenario (*user-gateway full trust*) users would completely trust the gateway once logged in - that is; the mere act of logging into the portal is an explicit delegation of complete trust to the gateway. If total trust is enforced, the gateway can retrieve any user VO-specific attribute from the VO AA, without asking for user approval. In the second scenario (*user-gateway partial trust*) users would not entirely trust the gateway. The user is able to control the activities the gateway is performing on her behalf. In order to approve, restrict or deny the gateway request, however, the user must be informed of which attributes the gateway is aking to retrieve. This raises issues of privacy relating to the user attributes stored in the VO AA. As described shortly, OAuth [11] specifications offer one solution to this - in brief; third-parties, acting on behalf of the user, can retrieve sensitive data given explicit approval from the user.

A general diagram of the DAM is shown in Figure 1. Subsequent sections describe in more detail how DAM works.

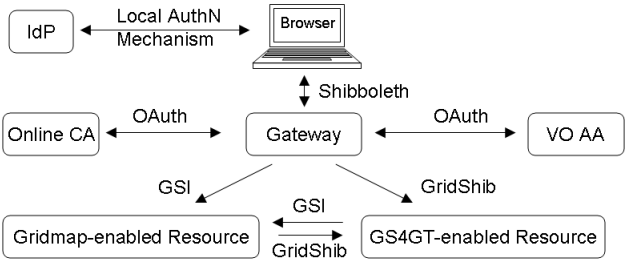


**Fig. 1.** DAM Overview

### 3.1 Identity- and Attribute-Based Authorization Interoperability

A key advantage of the DAM proposal is that, by delegating user credentials to the Gateway, the Gateway is able to access resources protected with identity-based mechanisms. Thus DAM supports interoperability by obviating any need for the Gateway to use its own identity to access resources. The delegation process is shown in Figure 2.

The user authenticates herself to the IdP and obtains SAML assertions she can send to the Gateway for authorization (Steps 1 and 2). After authorization, the Gateway asks the Online CA (could be a GridShib-CA instance) to issue new user proxy credentials. This request to the Online CA also includes SAML assertions received from the user in Step 2. The Online CA replies with new proxy credentials containing (1) the user's Distinguished Name (DN) as subject, and (2) SAML assertions received from the Gateway as extensions (Step 3). The Gateway uses these proxy credentials for resource access authentication. If the resource is protected with an attribute-based mechanism (e.g. GridShib GS4GT handler), then authorization is based on user attributes contained in

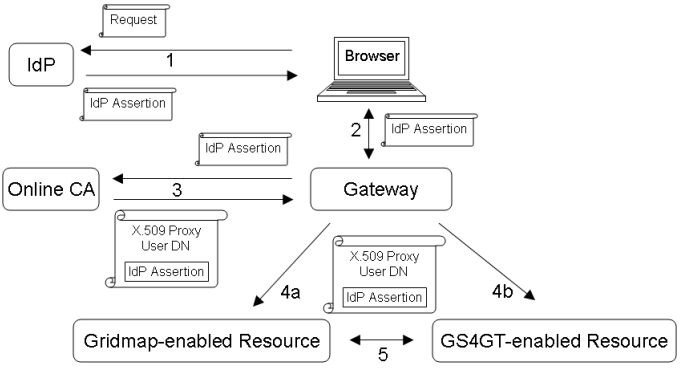


**Fig. 2.** Identity- and Attribute-based Authorization Interoperability

a certificate extension (Step 4a). If the resource is instead protected with an identity-based mechanism, (e.g. GSI GridMap file) then authorization is based on the certificate subject (Step 4b). The Gateway can also delegate credentials to resources (e.g. by using GSI delegation), thus enabling interoperability between resources protected with identity-based and attribute-based mechanisms (Step 5).

In Figure 2 the *user-gateway full trust* scenario is assumed in the interaction between the Gateway and the VO CA. If the gateway is not fully trusted by the user, as in the *user-gateway partial trust* scenario, then the interaction between the Gateway and the VO CA can be subject to user's consent, as will be explained shortly (section 3.3).

### 3.2 Real and Virtual Organization Domains

Separation of administrative domains is a desirable feature in order to achieve flexibility and efficiency in attributes administration. DAM extends the federation model by adding an extra layer supporting management of the user's VO-specific attributes. Each different federated administrative domain can manage RO-specific user attributes (i.e. in a LDAP server) whereas VO-specific user attributes are kept in a separate repository belonging to the VO domain. In this way, a VO domain can define its own policies for controlling resource access (e.g. by using the eXtensible Access Control Markup Language, XACML [12]).

In DAM, each administrative domain maintains full control over internal user privileges by defining RO-specific user attributes in IdP. VO-specific user attributes are defined in the VO Attribute Authority within the VO domain. By introducing this jurisdiction separation, VO resources need only trust the VO AA, instead of all real organization IdPs.

As in CAM, the DAM approach adopts the use of Shib-enabled Gateways for transparent access to different VO resources, but enriches this use with the domain separation model - as depicted in Figure 3 and explained below.

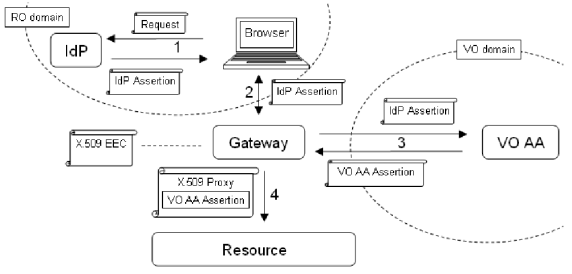


**Fig. 3.** Separation between RO and VO domains

During the authentication step against her IdP (step 1) the user retrieves IdP attributes as SAML assertions. The user then delegates these IdP attributes to the gateway (step 2), at which point the gateway can retrieve VO-specific user attributes from VO AA (step 3). Finally (step 4), the gateway binds the VO-specific user attributes to the gateway proxy certificate (alternatively, a user proxy certificate may be obtained from the VO CA, as depicted in Figure 2).

This approach has two key advantages: (1) the VO authorization mechanism is based on VO domain policies, thus VO resources can enforce authorization locally [13]; and (2) domains remain protected even if an IdP is compromised.

In Figure 3 the *user-gateway full trust* scenario is assumed in the interaction between the Gateway and the VO AA. If the gateway is not fully trusted by the user, as in the *user-gateway partial trust* scenario, then the interaction between the Gateway and the VO AA can be subject to user's consent, as will be explained shortly (section 3.3).

### 3.3 User-Gateway Partial Trust Scenario in DAM

In DAM the RO and the VO domains are linked together by a Gateway which acts as a bridge. In order to meet the requirements addressed by the *user-gateway partial trust* scenario, the DAM also integrates the OAuth model. OAuth is an open protocol defining how a user can authorize a consumer to access the user's resources protected by a service provider (SP), without requiring the user to disclose her own SP credentials to the consumer. Thus, OAuth can act as a means to enforce user control interaction upon VO-specific attributes retrieval. In DAM terms, the consumer is embodied in the gateway, while the service provider is the VO AA (storing the user's attributes as protected resources).

As described in Figure 4 the user first logs into the gateway (step 1). The gateway then requests user attributes from the VO AA (step 2) - which returns a Request token as response. This token is redirected to the user for approval (step 3). Provided that the VO AA is Shib-protected, the user can authenticate locally at her own IdP (step 4) and then present the IdP authentication assertion at the VO AA along with the request token approval/denial. If approved, the VO AA exchanges the request token with an access token and passes it to the gateway. The access token is eventually used by the gateway to actually retrieve the VO-specific user's attributes.

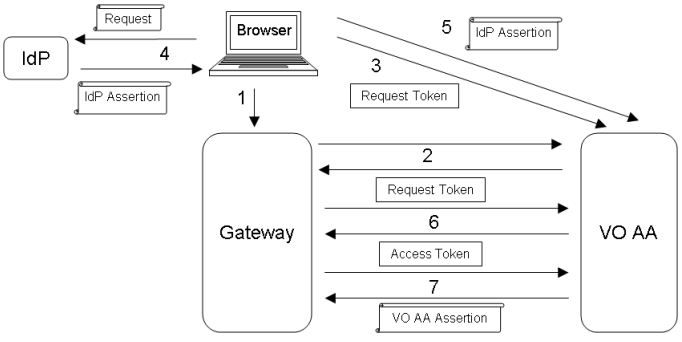


**Fig. 4.** OAuth model integration in DAM

The *user-gateway partial trust* scenario can also act as a means to enforce user control interaction upon user's proxy credentials retrieval. In this case the interaction flow is the same described in Figure 4, but the service provider is now embodied in the VO CA.

## 4 Conclusions

In this paper we introduced the Domain Account Model (DAM) as an extension of existing CAM and GridShib models. The motivations behind the DAM design are threefold. First, to support interoperability between attribute and identity based authorizations. Second, to enable and contextualize resource access for users belonging to different administrative domains. Third, to improve the user's control over resource usage by delegated entities.

An outstanding non-technical issue concerns the integration of DAM with grids regulated by policies defined by the International Grid Trust Federation (IGTF) [14] (such as EGEE [15] and OSG [16]). The DAM's use of online Certificaton Authorities does not comply with such regulations. Future work will focus on experimenting DAM within different scenarios in which VOMS [17] serve as the VO AA. Planned extensions include the definition of a VO policy framework based on a standard language (e.g. XACML), and the addition of auditing functionalities.

## Acknowledgements

This work is carried out by the Grid Research Unit of Engineering Ingegneria Informatica S.p.A. (http://www.eng.it) in the context of the GriFin - Grid For Finance project (http://www.grifin.eu).

## References


1. Introduction to the laws of identity (2005), http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
2. Foster, I., Kesselman, C., Tuecke, S.: The anatomy of the Grid. International J. Supercomputer Applications 15 (2001)
3. MyProxy Credentials Management Service, http://grid.ncsa.uiuc.edu/myproxy
4. Shibboleth Architecture, http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-200509.pdf
5. OpenID, http://openid.net
6. OASIS Security Services (SAML) Technical Committee, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
7. Welch, V., Barlow, J., Basney, J., Marcusiu, D., Wilkins-Diehr, N.: A AAAA model to support science gateways with community accounts. Concurrency and Computation: Practice and Experience 19(6), 893–904 (2006)
8. GridShib Deployement Scenarios, http://gridshib.globus.org/about.html#gridshib-deploy
9. Scavo, T., Welch, V.: A Grid Authorization Model for Science Gateways. Concurrency and Computation: Practice and Experience (to appear), http://gridfarm007.ucs.indiana.edu/gce07/images/e/e4/Scavo.pdf
10. Ferraiolo, D., Kuhn, R.: Role-based Access Control. In: Proceedings of 15th National Computer Security Conference (1992)
11. OAuth Core 1.0 Final Specfications, http://oauth.net/core/1.0/
12. XACML 2.0 Core: Specification Document, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdfvo
13. Core and hierarchical role based access control (RBAC) profile of XACML v2.0, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf
14. International Grid Trust Federation, www.gridpma.org/IGTF-Federation-Constitution.pdf
15. Enabling Grids for E-science (EGEE), http://www.eu-egee.org/
16. Open Science Grid, http://www.opensciencegrid.org
17. Alfieri, R., Cecchini, R., Ciaschini, V., dell'Agnello, L., Frohner, Á., Gianoli, A., Lörentey, K., Spataro, F.: VOMS, an Authorization System for Virtual Organizations. In: Fernández Rivera, F., Bubak, M., Gómez Tato, A., Doallo, R. (eds.) Across Grids 2003. LNCS, vol. 2970, pp. 33–40. Springer, Heidelberg (2004)