Collaboration and the Knowledge Economy: Issues, Applications, Case Studies
Paul Cunningham and Miriam Cunningham (Eds)
IOS Press, 2008 Amsterdam
ISBN 978–1–58603–924-0

Enabling True Single Sign-On for Grid Portals

Efstathios KARANASTASIS[1], Piotr GRABOWSKI[2], Vassiliki ANDRONIKOU[1],
Michael RUSSELL[2], Piotr DZIUBECKI[2], Dominik TARNAWCZYK[2],
Dawid SZEJNFELD[2], Tomasz KUCZYNSKI[2], Theodora VARVARIGOU[1], Jarek NABRZYSKI[2]
[1] *National Technical University of Athens, 9 Iroon Polytechniou, Zografou, 15773, Greece*
Tel: +30 210 7722558, Fax: +30 210 7722569, Email: karanastasis@telecom.ntua.gr
[2] *Poznan Supercomputing and Networking Center, Noskowskiego 10, Poznan, 61-704, Poland*
Tel: +48 61 8582174, Fax: + 48 61 8582151, Email: piotrg@man.poznan.pl

Abstract: This paper discusses the security issues arising when incorporating Grid portals in business environments and proposes a viable and robust integrated security solution, which is easy to incorporate into existing platforms, to use and to maintain. The proposed solution enables Single Sign-Up, an innovative concept for automatic user registration in domain specific middleware and remote services, Single Sign-On, and advanced user management. These mechanisms cooperate seamlessly, offering high levels of security, promoting the overall business processes, and thus comprising an important improvement towards the business adoption of the Grid. The design and implementation of the system is based and will be tested on several real life business cases from different sectors.

Keywords: business, Grid, portal, security, registration, authentication, Single Sign-Up, Single Sign-On, user management, toolkit, application, Web

1. Introduction

As “Grid” [1] makes its way to the mainstream, many businesses are looking to see how Grid can enhance their business models to drive growth, improve efficiency and increase production. Here, standards-based approaches to resource management, meta-scheduling, and federation of data and services are considered fundamental reasons to adopt Grid. Another key reason to adopt Grid is to benefit from the plethora of open-source software and tools now available on the market that support the Grid computing paradigm, such as to reduce the overall cost of the IT solution or simply to be inline with current trends in computing. While most open-source Grid platforms offer mechanisms for managing security and trust issues in federated environments, most do not offer practical means for integrating these security mechanisms with Web portals.

Grid portals comprise a collaborative environment which provides a simple and common Web interface to heterogeneous computational Grid resources and services. The offered functionality ranges from the submission and monitoring of computational jobs to the management of remote workspaces, accounting and provision of user and resource related statistics. A Grid portal also simplifies administration and problem solving by offering mechanisms for controlling access and monitoring user actions.

This paper discusses the security issues arising when incorporating Grid portals in business environments. It describes the methodology followed in the framework of the BEinGRID project [3], designing and developing components related to portals security, based on the needs of several real life business cases from different sectors. The components were implemented as enhancements and extensions to the Vine Toolkit [2]. The document describes the design of the proposed solution and the technology choices made. It further presents screenshots of the implementations and discusses their business impact and benefits when using them.

2. Objectives

This paper discusses how the Vine Toolkit, driven by business scenarios examined within the context of the BEinGRID project , aims to fill the Web-to-Grid gap to enable businesses to transparently connect their user communities to their Grid-enabled infrastructures in a secure and easy way. Vine, a Java-based framework that supports a variety of application environments, provides an extensible model for defining how users are granted identities and security tokens for multiple Grid environments, as well as how to introduce that registration process into the Web-site sign-up process. Moreover, it provides a complimentary collection of reusable Web 2.0 [4] interfaces that support user account sign-up and administration and can be adapted to any Java Servlet [5] or Portlet [6] based portal environment.

3. Methodology

The development and evaluation of the Vine Toolkit is based on the technical and business needs of ten different business cases from the aerospace, architectural, financial, environmental engineering, automotive, pharmaceutical, textile, chemistry, IT and geological sectors.

The portal security and user management requirements of these business cases were examined and detailed during the first year of the BEinGRID project. Substantial weight was also given to specific business requirements and the promotion of the overall business processes. Analyses of these requirements led to the design of a general model, which was refined several times in a constant interaction process with the involved businesses. The outcome of this procedure was a set of common components at the portal presentation layer as well at the business-logic layer, which represent viable solutions to address the requested functionality and can be adapted to the various Grid middleware and use-cases represented by the business cases that were analysed. Requirements and designs from the OMII-Europe project [7] were also included in this effort. The design has been implemented as enhancements and extensions to the Vine Toolkit and verified on a number of small testbeds deployed at the Poznan Supercomputing and Networking Center (PSNC) [8]. One of the main goals comprises the application and evolvement of this work in new business cases within BEinGRID as well as other real-world business problems.

4. Technology

Web portals, whether used internally or as a public offering for products and services, are vital enablers for commerce and production in business today. The most successful Web portals make it easy for users to join and become active members, that is, obtain accounts on the portal, its back-end services and partner sites. Thus, in order for Grid to become truly mainstream, it too needs to support Web-based user registration, the familiar email-verified "sign-up" model we see on many Web-sites today, as well as Web-based "Single Sign-On" and online tools for administering access to resources. Moreover, it must be possible to integrate this support into existing portal platforms.

The Vine Toolkit consists of a core project that defines a base API and programming model upon which sub projects are built. Each sub project addresses a particular problem area. Some, like the Grid Vine, build upon core Vine to define more general concepts and extensible elements. Others, like the Globus Toolkit 4 Vine, are concerned with adding support for particular third party libraries and services. At the time this paper was written, Vine had inherited support for several middleware and standards, including gLite 3 [9], Globus Toolkit 4 [10], JSDL 1.0 [11], OGSA-DAI 2.2 [12], UNICORE 6 [13], Storage Resource Broker [14], and others. Each Vine project conforms to a particular file structure that defines how source code is built as well as how third party libraries and configuration files are packaged and deployed. Users can select the specific Vine projects they require for their applications. Naturally, there are dependencies between certain projects that must also be taken into account.

When Vine is deployed, Vine's build system will deploy and package only those source files that are relevant to the target environment. Source files that are included in the main source tree for each project are deployed to all types of target environments, while source files contained in a project's web source tree are deployed for use only with Web applications. Typically, web source trees include user interfaces developed in one or more Web UI frameworks, such as the Google Web Toolkit [15] or Adobe Flex [16], as well as Java servlets, portlets and any Web services that are intended for use by that project.

Resources are perhaps the most important concept modeled in the Vine Toolkit. Vine defines a resource as anything that can be utilised. A computer, an application, a software library, a person, these are all resources in Vine. In fact, in Vine, resources define the application just as they define Grids. At their most basic level, Grids are collections of resources with policies describing how to use those resources. In order for the different resources to be properly accessible and functional, they must be identified in the resource registry file. Using the Vine Toolkit, one composes applications as collections of resources and services for utilizing those resources. The Vine Toolkit makes it possible to organize resources into a hierarchy of domains to represent one or more virtual organizations (VOs).

The Vine Toolkit is using a standard method of access control that enables a user to only login once and gain access to all resources configured for use with the system, without the need to login separately to each of them (Single Sign-On). It also implements a non-standard method for registering users into the portal system and underlying middleware (Single Sign-Up). Due to non existing standards for this scope, the developers had to implement a novel method supporting this idea. For managing users’ credentials, which is required in order to enable Single Sign-On, the MyProxy Credential Management Service [23] is used. The MyProxy client in the Vine Toolkit is using a standard protocol for storing and retrieving X.509 proxy credentials (RFC3820) [24] to and from a server. Vine security is mainly using the authentication and authorisation capabilities of the portlet container and existing MyProxy credential repositories or, in some cases, the component’s internal CA and credential repository, thus giving the end user a useful tool that allows using existing middleware and infrastructures. User Management in Vine can be fully integrated with the portal container and the underlying libraries may use different standards for different purposes. For example, Hibernate [25] may be used for database management, or the Java Database Connectivity (JDBC) API [26], an industry standard for database-independent connectivity, may be used.

As mentioned above, the Vine Toolkit was tested on a number of small testbeds deployed at the Poznan Supercomputing and Networking Center (PSNC) running different configurations, including:

- Fury.man.poznan.pl: Fedora 3, Globus Toolkit 4.0.1
- Seagrass.man.poznan.pl: Gentoo, UNICORE 6
- Omiidemo.man.poznan.pl: Gentoo, Globus Toolkit 4.0.4
- Node2.qoscosgrid.man.poznan.pl: Gentoo, OpenDSP
- Desktop / notebook computers running Windows XP, Mac OS, or different versions of Linux.

5. Developments

In order to support seamless integration with application containers, Vine offers several entry points for introducing security. This section focuses on a wide range of security needs of a typical Web portal application, which are addressed by the Vine Toolkit. However, most of the topics discussed here can apply to other application environments.

The high-level logic of the Vine Toolkit in terms of security related operations is presented in Figure 1. In reality, quite complex business-logic patterns and related components were implemented in order to support this logic.

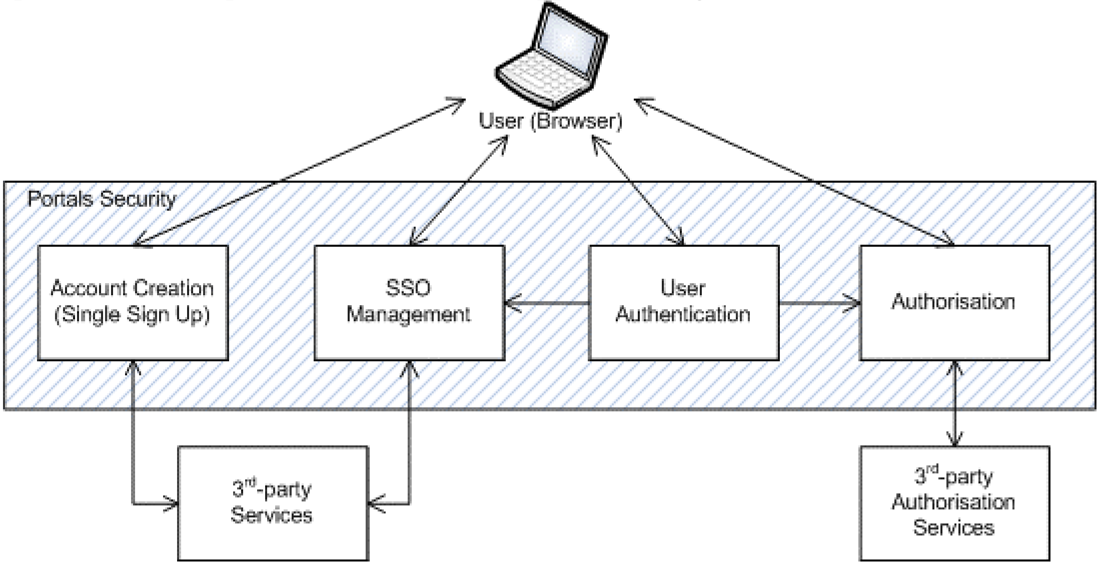


Figure 1: High-Level Architecture of Security in Vine

In brief, Vine offers a number of interfaces covering a Grid portal's security needs, serving at user registration and authentication. It allows automatic creation of user accounts and registration in a number of chosen middleware and services during sign-up or after account approval, simplifying the process of generating credentials and registering them with Grid middleware, or creating accounts on remote systems. It further enables Single Sign-On (SSO), allowing the usage of integrated third party security services in a common way. The mechanism behind this is Security contexts.

Security contexts are Vine services that provide capabilities to other Vine services for handling particular types of security problems, making it easy to add support for third party security libraries and services in a common way. Security contexts include a number of middleware-specific registration and authentication modules. The Grid Vine project provides a General Security Services (GSS) [17] security context for obtaining access to GSS credentials delegated to a Vine application for a particular user. The latest version of Vine incorporates a number of GSS and non-GSS registration and authentication modules supporting, among others, Globus Tooklit 4, UNICORE 6 and VOMS [18] (gLite 3).

Whenever a user accesses resources within a portal, such as a fragment of html or a portlet, or external resources via the portal, such as a file or remote information service, typically some mechanism is required to check whether that user is authorised to access that resource and what level of access they have been granted. Vine does not currently handle authorisation mechanisms explicitly but rather leaves it up to the application programmer to address how authorisation is performed. This is because at times authorisation to portal resources can be performed by the web application server or portal container application to which a Vine application has been deployed. Likewise, authorisation to external resources is often performed by the third party services a Vine application utilises to make those resources available to users.

5.1 User Registration and Single Sign-Up

The moment a portal user first obtains a user account comprises also the appropriate time for the registration of that user with any third party services configured for use with a given

Vine application. Registration with third party services may involve a complex set of procedures and/or human intervention by a portal administrator. The Vine Toolkit provides complete mechanisms for handing user registration, promoting the innovative concept of Single Sign-Up.

An account represents permission by a person to use a Vine application. We call this person a "user" of the application. In order to use a Vine application (i.e. a Vine Grid portal in the context of this paper) a user must first request an account. An account is created when an account request is approved by an account manager module. An account manager is responsible for handling account requests and managing the accounts that result from the approval of account requests. Account manager modules can be configured to automatically accept account requests submitted to them or require manual acceptance.

Account requests have three basic attributes: a unique username, a private password, and a unique and valid email address. An account has an additional attribute, a unique identifier used internally by Vine. Both account request and account may have more attributes depending on the application. As also explained below, an account can have zero or more registrations associated with it. The registrations associated with an account depend on how a Vine application's resource registry is configured and which registration requests have been approved for that account. Once an account request is accepted, an account manager module will process each registration request associated with that account request.

A registration generally represents permission to use one or more third party services configured for use with a Vine application, such as a Grid middleware platform in order to support access to remote computational resources. Their attributes depend on the registration module to which the request is submitted. A registration module is responsible for managing registration requests and the registrations that result by the approval of requests. Registration modules can be configured to automatically accept registration requests submitted to them or require manual acceptance. Registration requests can be submitted to a registration module directly or by an account manager for a given account request. If the registration request has been approved, then a registration is created and managed by the particular registration module.

In case the registration request is part of an account request, then a registration will only be created if the associated account request has been also approved. If a registration’s parent account request is denied or fails any time during its processing, then a registration will not be created even if its associated registration request was approved. Instead, that registration request will be rolled back. In the same manner, an account will only be created if all the corresponding registration requests have been approved.

Accounts and registrations have two basic states, active or inactive, permitting or preventing a user from using a Vine application or a service respectively, and their lifetime is configurable. A registration module will notify its parent account manager whenever the status of a registration request changes. Account and registration requests both have a well defined lifecycle, as illustrated in Figure 2.

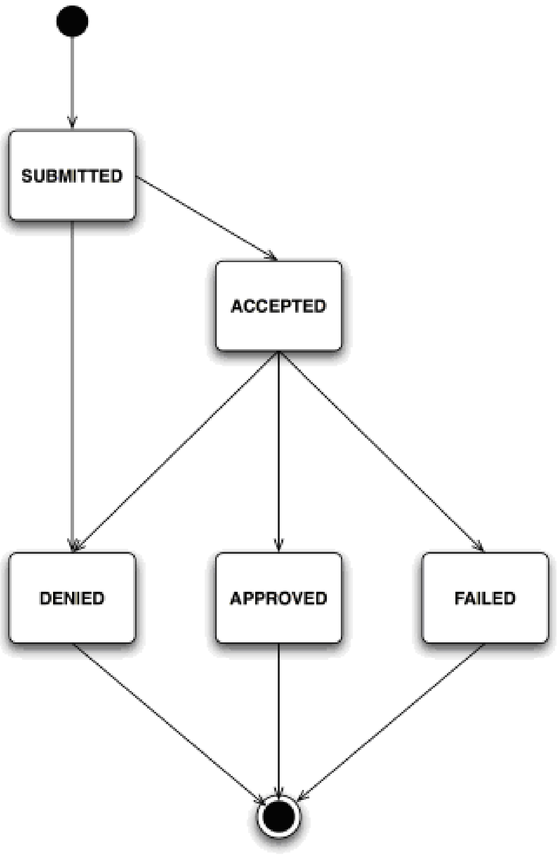


Figure 2: Account Request and Registration Request Lifecycle

5.2 User Authentication and Single Sign-On

When a portal user logs in to a portal, Vine authenticates that user with the third party services configured for use with a given Vine application. Typically, a username and password are supplied at login time. This information can be passed to third party services to which the user has been registered in order to obtain access to resources for as long the user is logged in to the portal. The Vine Toolkit provides authentication modules for handing user authentication issues and enabling single sing-on. Authentication modules, also mentioned above, are Vine services invoked to authenticate a user attempting to create a Vine session. All activity in a Vine application is handled in one or more sessions. Sessions are used to create service contexts.

Authentication to third party services usually results in some credential or security token that is granted to a Vine application to enable Vine to access resources via one or more third party services that accept the given security token. Vine has an extensible mechanism to make these security tokens available to application programmers, as explained above.

5.3 User Management

The User Management in Vine provides the ability for managing accounts of portal users and user-groups and their access to content or resources. This also includes the need for users to manage their own personal information and view information of other users, if authorised. In addition, the portal administrator can manage a user-group and change their access rights to content / resources, resulting in consequent changes to the environment presented to the user and/or the users permissions. This includes changing the list of portlets displayed to a specific user-group, for example a standard user or a first time logged in user, and arranging their layout. As a result of this, the user can only see and navigate the portlets chosen by the administrator. Portlets requiring administrative access rights cannot be presented to a user who does not hold the required privileges.

The high-level logic of the Vine Toolkit in terms of user management related operations is presented in Figure 3. Vine provides the ability to plug into the user account management mechanisms of its container environment, as well as to manage user accounts in standalone applications and services.

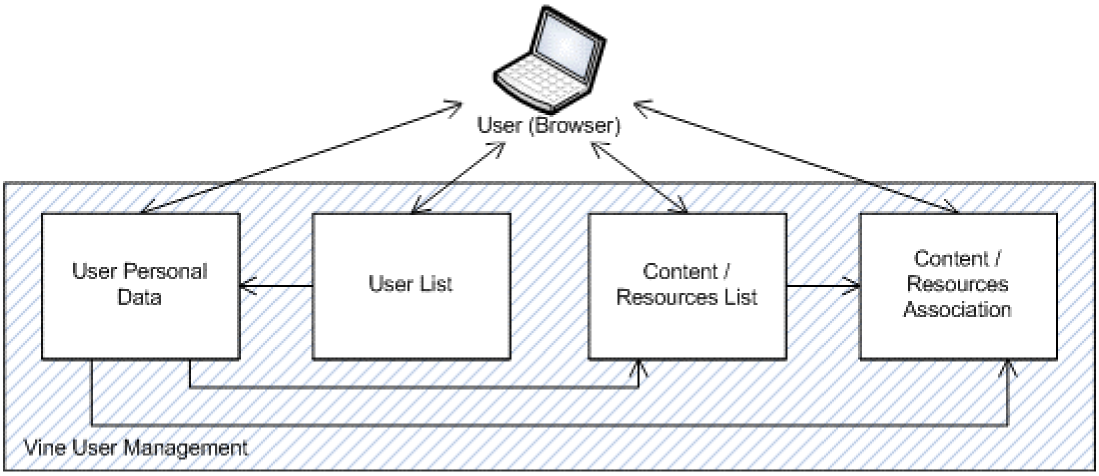


Figure 3: High-Level Architecture of User Management in Vine

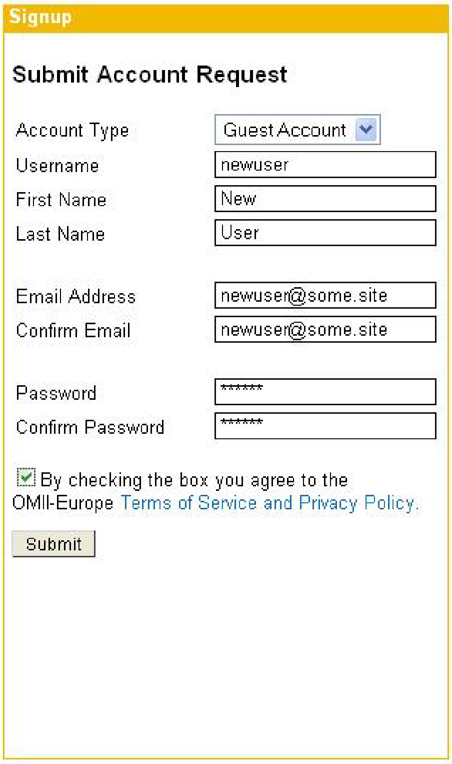
In specific, the User Personal Data operation allows users to view and change personal information, like first and last name or email address. The Users List operation, carried out by an account manager in the implementation of Vine, allows users or administrators to view or manage (e.g. add, delete) accounts of portal users. The Content/Resources Association operation covers the need for administrators changing the association between user accounts and Content or Resources. For example, the administrator can choose which components will be available to users and what their portal page will look like, according to their user group. Finally, the Content/Resources List operation serves at presenting the available portal resources users could possibly be assigned.

The reader should keep in mind the individual functionality provided by User Management, as well as the other aforementioned components, is important for achieving high levels of security, and simplicity in usage.

6. Results

The work committed on the Vine Toolkit was accompanied by a number of sample portlets representing the basic characteristics of the implemented business-logic. The figures below present screenshots of the developed portlets deployed in the GridSphere [19] portlet container.

Before a person can use the Grid portal, he/she will need to get an account on it. A guest user has to navigate to the homepage of the Grid portal and use the Signup portlet to request a new portal account (Figure 4). By following the steps presented, the guest fills in the required fields with his/her details, chooses an account type and submits an account request.



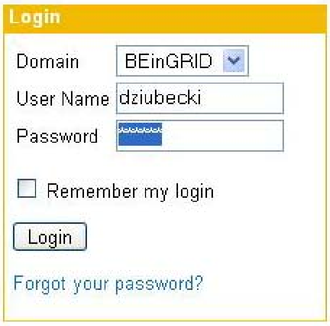
Signup

Submit Account Request

Account Type	Guest Account
Username	newuser
First Name	New
Last Name	User
Email Address	newuser@some.site
Confirm Email	newuser@some.site
Password	******
Confirm Password	******

☑ By checking the box you agree to the OMII-Europe Terms of Service and Privacy Policy.

Figure 4: Signup Portlet – New User Account Request



Login

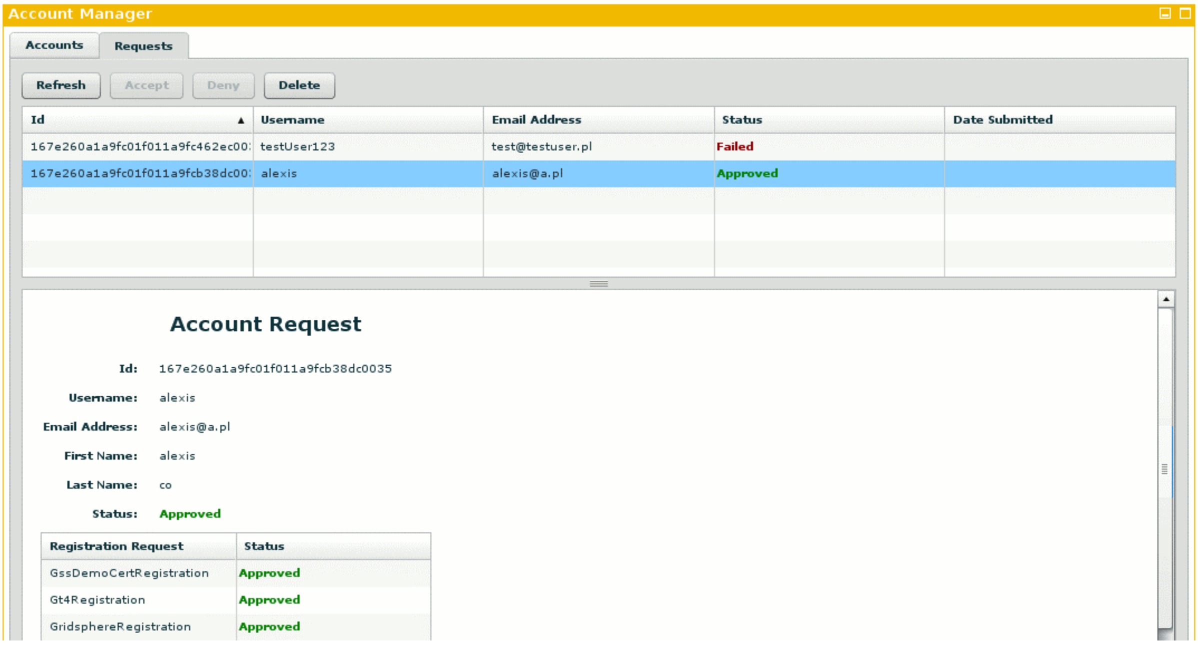
Domain	BEinGRID
User Name	dziubecki
Password	******

☐ Remember my login

Figure 5: Login Portlet – Login to Domain BEinGRID

When an account request is successfully approved by the administrator, the corresponding account is created and the requester is considered a registered user. Registered users are able to login to the portal by providing their chosen username and password in the Login portlet (Figure 5).

The portal administrator can use the “Requests” tab of the Account Manager portlet (Figure 6) to browse a list of registration requests, undertake the new user’s registrations with external middleware or services and finally approve the new user account. In the “Accounts” tab of the Account Manager portlet, the administrator can view and modify existing user accounts.



Id	Username	Email Address	Status	Date Submitted
167e260a1a9fc01f011a9fc462ec00:	testUser123	test@testuser.pl	Failed	
167e260a1a9fc01f011a9fcb38dc00:	alexis	alexis@a.pl	Approved	

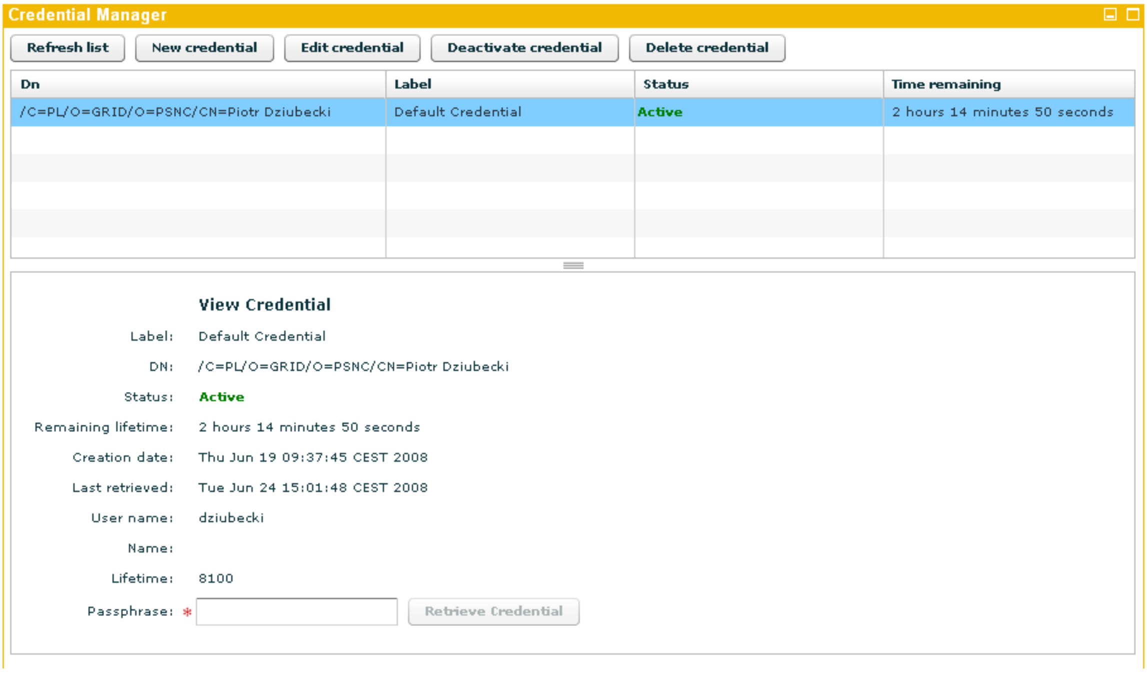
Account Request

Id:	167e260a1a9fc01f011a9fcb38dc0035
Username:	alexis
Email Address:	alexis@a.pl
First Name:	alexis
Last Name:	co
Status:	Approved

Registration Request	Status
GssDemoCertRegistration	Approved
Gt4Registration	Approved
GridsphereRegistration	Approved

Figure 6: Account Manager Portlet – Account Requests List

In the Credential Manager portlet (Figure 7), a user can view and manage his/her credentials. When viewing a credential, the following details are presented: credential's label, Distinguish Name of the credential owner, status of the credential (active/inactive), remaining lifetime, creation date and date of last retrieval, corresponding MyProxy username for the credential, credential name in MyProxy, and value of lifetime when the credential was retrieved. The user can also check which credential ("Default Credential") was automatically retrieved from MyProxy during the login phase. In the case when no appropriate credential exists and can be loaded, the user can use the "New credential" command to specify a credential to be retrieved from MyProxy to the portal.



Dn	Label	Status	Time remaining
/C=PL/O=GRID/O=PSNC/CN=Piotr Dziubecki	Default Credential	Active	2 hours 14 minutes 50 seconds

View Credential

Label:	Default Credential
DN:	/C=PL/O=GRID/O=PSNC/CN=Piotr Dziubecki
Status:	Active
Remaining lifetime:	2 hours 14 minutes 50 seconds
Creation date:	Thu Jun 19 09:37:45 CEST 2008
Last retrieved:	Tue Jun 24 15:01:48 CEST 2008
User name:	dziubecki
Name:	
Lifetime:	8100
Passphrase: *	

Figure 7: Credential Manager Portlet – View Credential Details

7. Business Benefits

Taking into account current market trends for support of collaborative environments as well as connecting and enabling communication among different businesses, collaboration, connectivity, communication [20] and synchronization of processes comprise decisive factors for business success. A variety of roles with different levels of authorization and varying Quality of Service (QoS) requirements, related among others to security, reliability and performance, must be served by Grid portals.

Grid portals comprise a solution for the rather limited usability of the Grid infrastructure for end users, by offering a user-friendly and much less complicated environment for them to transparently access and manage services and resources aggregated from different, distributed and heterogeneous sources. Moreover, given the customizability potential, based on different end user roles, Grid portals can provide personalized views of information, this way constituting a *significant enhancement* of the Grid business aspect.

Offering Web-based access and management of resources and service capabilities, however, poses strong security requirements. The threats are numerous; an attacker may gain access and manage the resources and the services for running their own jobs on the Grid, obtain information about registered users or retrieve the results of executed jobs, among others. [21] In a business environment, the security requirements become even stronger. Important business data may be exposed, and customers/enterprises may be charged for services they never used or face Denial of Service (DoS), all resulting to possible financial and other important malign problems to their business. An example could be taken from a strongly collaborative environment such as the supply chain, in a case where the system does not allow for customers to submit their orders or for suppliers to view the submitted orders and process them, or when orders and customer information are exposed to the supplier's competitors. The impact of such problems could range from delays in order processing, affecting the speed of the processes in the whole supply chain (distributors, manufacturers and customers) and resulting in a delayed order cycle, to the loss of customers.

Depending on the requirements of the businesses involved, related to data confidentiality, reliability and access control, a "successful" security attack may cause significant costs and have great impact on the reputation of the service providers. Thus, security comprises an important aspect of Grid portals. Data transformation and certificate establishment as well as user authentication, authorization and management work towards this direction. However, depending on the business-related security levels and the scale of the system, the above mentioned processes may be time-consuming and rather complicated for setting up as well as for maintenance. The proposed integration of these security mechanisms with Grid Web portals and the resulting abstraction of the users from the security mechanisms - reducing thus the complexity of the processes and the effort required to perform them - comprise an important improvement towards the business adoption of the Grid. Security and user management can this way be performed in a more cost-effective way and allow for IT staff to focus more on how to plug Grid into their business rather than wonder how to plug Grid into their technology.

Especially in the case of small local businesses that lack the capital to own resources (computational, informational, applications, etc), they can remain profitable and maintain or improve their market share by taking the step to bring Grid into their businesses and accessing resources through a secure portal solution. This way, local economies can remain viable.

By offering automatic creation of user accounts and registration in a number of chosen middleware and services during sign-up or after account approval, the Vine Toolkit enables a simplified process of generating credentials and registering them with Grid middleware, or creating accounts on remote systems through the user-friendly user setup and administration interfaces presented. In fact, our major marketing strategy comprises in demonstrating to Small and Medium-sized Enterprises (SMEs) this simplified process and the success stories produced after its application in real-world businesses within the BEinGRID project.

8. Conclusions and Future Work

In this paper we demonstrated the Web-based Single Sign-Up and Single Sign-On with the Vine Toolkit, which can be used in several Grid platforms employed by BEinGRID partners or other businesses today. We showed how User Registration, User Authorization and User Management are implemented seamlessly in one package designed to fulfill the real needs of secure and easy Web-access to Grid resources in business environments. The cooperation of the aforementioned mechanisms allows Vine applications to enable a true Single Sign-On capability.

The work in the Vine Toolkit was focused on giving the end user a useful tool that would allow reusing existing middleware and infrastructures. Additional effort was put into building an automated mechanism for user account creation in existing systems and various middleware. Globus Toolkit 4, UNICORE 6 and gLite 3 security is supported, amongst others. Vine was implemented having in mind how to improve business operations and provide business users with an easy to use environment through a Web portal. These characteristics make Vine ideal for use by businesses that wish to “Gridify” their existing infrastructure and processes, in order to remain competitive and exploit the benefits of Grid, as discussed above.

We would further like to point out that the presented software is open source (the Apache License 2.0 applies). Also, although this paper focused on security and user management, additional functionality is packaged in Vine. It supports the submission, monitoring and control of computational jobs in different Grid platforms, as well as the management of file repositories of different types. It thus comprises a fully integrated solution that can be used when building a Web Grid portal.

Although the Vine Toolkit is now in a mature state and available for usage through the Gridipedia [27] Web site, development is still on-going. The users’ feedback will lead to the further improvement of some detailed aspects of its functionality, and to fixing any discovered problems. Future work also includes, but is not limited to, testing and evaluating Vine in a new business case within BEinGRID. This business case is mainly concerned with complex computing workflows in Grid enabled enterprise B2B processes, focusing in the aerospace and defense sector and using Web 2.0 technologies. In the context of this work, we also expect to further evolve the functionality provided by all the components of the Vine Toolkit, as well as improve the presentation layer by the adoption of new UI technologies. Furthermore, we aim to the implementation of support for additional middleware and third party services, such as GRIA [22].

References

[1] I. Foster, “What is the Grid? A Three Point Checklist”. GRIDToday July 20, 2002.

[2] Russell M., Dziubecki P., Grabowski P., Krysinski M., Kuczynski T., Szjenfeld D., Tarnawczyk D., Wolniewicz G., Nabrzyski J., “The Vine Toolkit: A Java framework for developing Grid applications”, Proceedings of the Seventh International Conference on Parallel Processing and Applied Mathematics (PPAM’07), 2007.

[3] BEinGRID Project: http://www.beingrid.eu

[4] Paul Miller, “Web 2.0: Building the New Library”, http://www.ariadne.ac.uk/issue45/miller/

[5] Servlet 2.3 API: http://jcp.org/en/jsr/detail?id=53

[6] Java Portlet 1.0 API: http://jcp.org/aboutJava/communityprocess/_nal/jsr168/

[7] OMII-Europe Project: http://www.omii-europe.org
[8] PSNC: http://www.man.poznan.pl/
[9] E. Laure, S. M. Fisher, A. Frohner, C. Grandi, P. Kunszt, A. Krenek, O. Mulmo, F. Pacini, F. Prelz, J. White, M. Barroso, P. Buncic, F. Hemmer, A. Di Meglio, A. Edlund, "Programming the Grid with gLite", Computational Methods In Science And Technology , 2006
[10] I. Foster, "Globus Toolkit Version 4: Software for Service-Oriented Systems", Proceedings of IFIP International Conference on Network and Parallel Computing, 2006.
[11] Job Submission Description Language (JSDL) Specification, Version 1.0: http://www.ogf.org/documents/GFD.56.pdf, Global Grid Forum, Lemont, Illinois, U.S.A., GFD.56, November 2005
[12] Mario Antonioletti, et al., "The design and implementation of Grid database services in OGSA-DAI Concurrency and Computation: Practice and Experience" Volume 17, Issue 2-4
[13] Dietmar W. Erwin, David F. Snelling, "UNICORE: A Grid Computing Environment" Proceedings of Parallel Processing: 7th International Euro-Par Conference Manchester, 2001
[14] Arcot Rajasekar, et al., "Storage Resource Broker-Managing Distributed Data in a Grid Computer", Society of India Journal, Special Issue on SAN, 2003
[15] Google Web Toolkit: http://code.google.com/webtoolkit/
[16] Adobe Flex: http://www.adobe.com/products/ex/
[17] GSS-API: http://www.ietf.org/rfc/rfc2853.txt
[18] R. Alfieri et al., "From gridmap-file to VOMS: managing authorization in a Grid environment", Future Generation computer Systems, Volume 21, Issue 4, April 2005
[19] J Novotny, M Russell, O Wehrens, "GridSphere: a portal framework for building collaborations, Concurrency and Computation", Practice and Experience, Volume 16, Issue 5
[20] Vassiliadis B., Giotopoulos K., Votis K., Sioutas S., Bogonikolos N., Likothanassis S., "Application Service Provision through the Grid: Business models and Architectures", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), 2004.
[21] Wang, X. D, Yang, X., Allan, R., "Top Ten Questions To Design A Successful Grid Portal", Proceedings of the Second International Conference on Semantics, Knowledge, and Grid (SKG'06), 2006.
[22] Surridge, M. Taylor, S. De Roure, D. Zaluska, E., "Experiences with GRIA Industrial Applications on a Web Services Grid", Proceedings of the First International Conference on e-Science and Grid Computing, 2005
[23] MyProxy Credential Management Service: http://grid.ncsa.uiuc.edu/myproxy/
[24] RFC3820, S. Tuecke, V. Welch, D. Engert, L. Pearlman, and M. Thompson, "Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile," IETF RFC 3820, June 2004 http://www.ietf.org/rfc/rfc3820.txt
[25] Hibernate: http://www.hibernate.org/
[26] Java Database Connectivity (JDBC) API: http://java.sun.com/javase/technologies/database/
[27] Gridipedia: http://www.gridipedia.eu