computing@computingonline.net
www.computingonline.net

ISSN 1727-6209
International Journal of Computing

ENTERPRISE – UNIVERSITY FEDERATION AS DISTRIBUTED MEASUREMENT SYSTEM LABORATORY

Andrey Angelov Elenkov

Technical University of Sofia, 8 Kliment Ohridski boulevard,
1000 Sofia, Bulgaria, E-mail: aelenkov@tu-sofia.bg, www.tu-sofia.bg

Abstract: *Federation allows a user to associate two accounts with each other. In this paper one account is the enterprise, the other one is the university. The student is the user which associates the two accounts. The goal is the student's education from the university, for the enterprise's needs, using enterprise's infrastructure, especially enterprise distributed measurement system. A federation scenario for a distributed measurement system laboratory is discussed and a test system is built to test this scenario.*

Keywords: *distributed measurement system laboratory, federation, university.*

1. INTRODUCTION

The Virtual laboratory is a distributed workgroup environment, with the main task of providing a remote access to the various kinds of laboratory equipment and computational resources. The virtual laboratory must include real experiments. That means that users must be secured collecting real data. Virtual laboratories need to provide users with collaborative tools to overcome the inherent geographical separation of a distributed environment, such as the Internet. In other words the virtual laboratory must provide a global access. Internet communication allows a remote user to control and monitor devices and apparatus in the physical laboratory as if they were placed in front of the remote user [1].

The student's education into the measurement systems for the enterprise's needs using virtual laboratories in the university has a problem – the systems work not in real conditions [2]. On the other hand the students are not welcome to the enterprise because of security issues, where the second problem is the access to the resources and measurement info – identification and authorization [3].

The solution of the two problems is enterprise – university federation.

A Federation is a group of two or more trusted business partners with business and technical agreements, which allow a user from one federation partner, to seamlessly access resources from another partner in a secure and trustworthy manner. The key features are: Single Sign-On, Access Control and Single Sign-Off Account Linking and/or Identity Mapping across partners Secure Identity Exchange. Users decide who they want to federate their identity with. Federation is actually the linking of two accounts using a unique pseudonym. The user account must already exist in both locations.

Specification has evolved into a secure method of federating users and exchanging identity:

– *Liberty Identity Federation Framework* (ID-FF) – enables identity federation and management through features such as identity/account linkage, simplified sign-on and simple session management [4];

– *Liberty Identity Services Interface* Specifications (ID-SIS) – enables inter-operable identity services such as personal identity profile service, alert service, wallet service, contacts service, geo-location service, presence service and so on;

– *Liberty Identity Web Services Framework* (ID-WSF) – provides the framework for building inter-operable, permission based attributes sharing, identity service description and discovery and the associated security profiles [5].

Liberty specifications build on existing standards (SAML, SOAP, WSS, XML, etc...).

WS-Security, WS-Trust, and WS-Security Policy provide a basic model for federation between Identity Providers and Relying Parties. These specifications define mechanisms for codifying claims (assertions) about a requestor as security tokens which can be used to protect and authorize web services requests in accordance with policy.

WS-Federation extends this foundation by describing how the claim transformation model inherent in security token exchanges can enable richer trust relationships and advanced federation of services. This enables high value scenarios where authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. WS-Federation includes mechanisms for brokering of identity, attribute discovery and retrieval, authentication and authorization claims between federation partners, and protecting the privacy of these claims across organizational boundaries. These mechanisms are defined as extensions to the Security Token Service (STS) model defined in WS-Trust. In addition WS-Federation defines a mapping of these mechanisms, and the WS-Trust token issuance messages, onto HTTP such that WS-Federation can be leveraged within Web browser environments. The intention is to provide a common infrastructure for performing Federated Identity operations for both web services and browser-based applications. A common protocol provides economies with regard to development, testing, deployment and maintenance for vendors and customers alike [6].

The process of requiring a user account to already exist at an Identity Provider and Service Provider before they can be federated does not fit the enterprise model. The solution is when configuring any component that contains a Service Provider, the administrator will be able to select the resource as an Enterprise Service Provider.

Federation allows a user to associate two accounts with each other. This allows the user to log into one account and have access to the resources of the other account without logging in to the second account. It is one method for providing single sign-on when a user has accounts in multiple user stores.

In this paper one account is the enterprise, the other one is the university. The student is the user which associates the two accounts. The goal is the student's education from the university, for the enterprise's needs, using enterprise's infrastructure, especially the enterprise distributed measurement system.

2. ENTERPRISE-UNIVERSITY FEDERATION SCENARIO

Suppose Company A has a centralized user store that does the authentication for most of the company's internal resources on its inner Web site. But Company A also has a customer feedback application that employees and customers need access to, and for this application, a second user store has been created. This user store contains both employee and customer user accounts. The centralized user store can't be used, because it can contain only employee accounts. This means that the employee must log in to both accounts to access both the inner Web site and the customer feedback application. With federation, the employee can access the resources of both sites by using a single login.

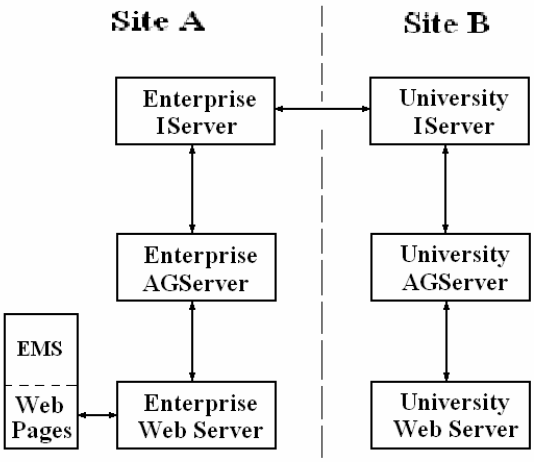

Fig. 1 – Using Federated Identities

Figure 1 illustrates such a network configuration where the user accounts of Site A (Enterprise) are configured to federate with the user accounts at Site B (University). The place of the customer is for the University and his students.

In Fig.1 EMS is the Enterprise's Measurement System, IServer – Identity Server and AGServer – Access Gateway Server.

In this configuration, Site A is the Identity Server for the corporate resources, and the employees authenticate to this site and have access to the resources on the Web server with the URL, e.g https://enterriseX.com/inner. Site B is the Identity Server for the EduTest application, and both employees and customers authenticate to this site to have access to the resources of the Web server with the URL of https://enterriseX.com/EduTest. After an account has been federated, the user can log in to Site A and the user have access to the resources on the Web servers of both Site A and Site B.

In this scenario, Site B (University) is not as secure a site as Site A (Enterprise), so federation is configured to go only one way, from Site A to Site B. This means that users who log in to Site A have access to the resources at Site A and B, but users who log in to Site B have access only to the resources at Site B. Federation can be configured to go both ways, so that it doesn't matter whether the user logs into Site A or Site B. When federation is configured to be bidirectional, both sites need to be equally secure.

The Access Gateways in Fig. 1 are service providers and are configured to use the Identity Servers as identity providers. The trusted relationship is automatically set up for the user when the user specify authentication settings for the Access Gateway and select an Identity Server Cluster.

Federation can be set up between providers in the same company or between providers of separate companies. For example, most companies have contracts with other companies for their user's health benefits and retirement accounts. Their users have accounts with these companies. These accounts can be federated with the user's employee account when both companies agree to set up the trusted relationship. Means the university and the company (enterprise) have to agree to set up the trusted relationship.

In case of use of the Novell® Identity Servers, e.g. the test system in this paper, setting up federation with providers other than Novell® Identity Servers requires the same basic tasks as setting up federation with Novell® Identity Servers, with some modifications. When you set up federation with identity providers and service providers that are controlled by a single company, you have access to the Administration Consoles for both Identity Servers and know the admin credentials. When setting up federation with another company, additional steps are required:

– You need to negotiate with the other company and gain approval for federation because metadata must be shared and both sites require configuration. You'll need to negotiate a schedule for these configuration changes;

– The other site might not being using Access Manager for its identity or service provider. The basic tasks need to be modified to accommodate how that implementation shares metadata, authentication methods, and roles. Many SAML 1.1 providers do not support a metadata URL, and the data has to be imported manually.

For example, instead of sharing URLs that allow you to import metadata, you might need to share the actual metadata and paste it into the configuration. The Novell® Identity Servers validates the metadata of another identity provider or service provider. Some implementations do not validate it. If the Identity Server determines that the metadata is invalid, you'll need to negotiate with the provider to send you metadata that has been validated.

Federation requires the configuration of a trusted relationship between an identity provider and a service provider. Before setting up a trusted relationship a choice of the protocol, the attributes to share and the user authentication has to be done.

3. REALIZATION OF THE SCENARIO

A test system based on Novell® solution, named Novell® Access Manager, has built to test the scenario. The solution is multiplatform, secure and easy for deployment.

The Fig.2 illustrates the components and process flow that make up the basic tested configuration.

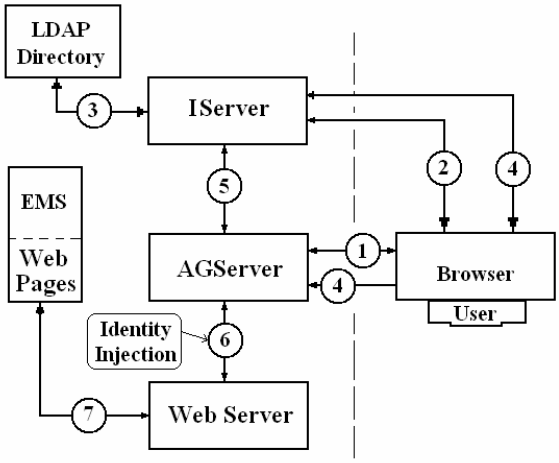

Fig. 2 – Basic Process Flow

1- The user requests the Access Gateway Server (AGServer) for access to a protected resource.

2- The AGServer redirects the user to the Identity Server (IServer), which prompts the user for a username and password.

3- The IServer verifies the username and password against an LDAP directory user store.

4- The IServer returns an authentication artifact to the AGServer.

5- The AGServer retrieves the user's credentials from the IServer.

6- The AGServer injects the basic authentication information into the HTTP header.

7- The Web server validates the authentication information and returns the requested Web page.

The Access Manager is configured so that a user can access a resource on a Web server whose name and address are hidden from the user.

This scenario has to correspond to the enterprise's Disaster Recovery planning.

Disaster Recovery planning is the process of preparing for recovery or continuation of Information and Communication Technologies (ICT) processing tasks that support critical business processes in the event of a threat to the ICT infrastructure. In some cases, ICT infrastructure would be recovered in a process that could take days (or weeks) while in other cases processing will continue immediately (or within minutes) at a remote site away from the threat [7].

The DR planning and testing process is not

generally regarded by ICT teams as the most exciting task to be involved in, and most would prefer to keep busy with 'cooler' projects such as virtualization or some new Web 2.0 technology. But business continuity and DR planning is critical for an organization and when the worst actually happens, there is always plenty of excitement to go around [8].

For additional capacity and for failover, a group of Identity Servers could be configured to act as a single server. Also could be created a cluster of Access Gateways and configured to act as a single server. Clustering enables the following features:

– Configuration Synchronization – the cluster is configured, and the configuration is synchronized to all members of the cluster;

– Session Sharing – each cluster member can handle sessions held by another server in the cluster. After a session is established, the same member usually handles all requests for that session. However, if that cluster member is not available to handle a request, another member steps in and processes the request. You can also provide fault tolerance for the configuration store on the Administration Console by installing secondary versions of the console. The following sections explain how to set up these components for fault tolerance.

The Administration Console contains an embedded version of Novell® eDirectory™, which contains all the configuration information for the Access Manager. It also contains a server communications module, which is in constant communication with the Access Manager modules. If the Administration Console goes down and any secondary consoles are not installed, the Access Manager components also go down and the protected resources become unavailable. The fault tolerance could be created by installing up to two secondary consoles. The recommendation is to install at least one secondary console.

A cluster of Identity Servers should reside behind an L4 switch. Clients access the virtual IP address of the cluster presented on the Layer 4 (L4) switch, and the L4 switch alleviates server load by balancing traffic across the cluster.

Whenever a user accesses the virtual IP address (port 8080) assigned to the L4 switch, the system routes the user to one of the Identity Servers in the cluster, as traffic necessitates. The system automatically enables clustering when multiple Identity Servers exist in a group. If only one Identity Server exists in a group, clustering is disabled. A cluster of Access Gateways must reside behind a L4 switch. Clients access the virtual IP on the L4, and the L4 alleviates server load by balancing traffic across the cluster of Access Gateways. Whenever a user enters the URL for an Access Gateway resource, the request is routed to the L4 switch, and the switch routes the user to one of the Access Gateways in the cluster, as traffic necessitates.

On the other hand Access Manager is not a firewall. It should be used with firewalls. Figure 3 illustrates a simple firewall set up for a basic Access Manager configuration of an Identity Server, an Access Gateway.

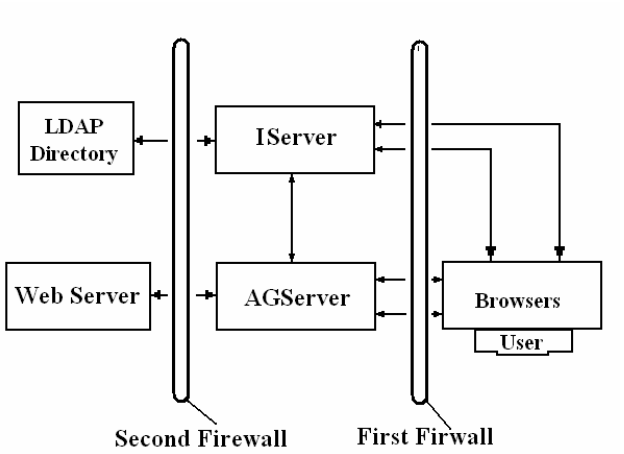

Fig. 3. – Access Manager Components between Firewals

For security reasons, the Access Manager configuration could be set up so that the Identity Server (IServer) is a resource protected by an Access Gateway Server (AGServer). It means only the AGServer is in the demilitarized zone between the two firewalls. This configuration reduces the number of ports you need to open between the outside world and your network. With this configuration, you do not need a switch to add multiple Identity Servers to a cluster configuration. When the IServer is configured to be a protected resource of the AGServer, the AGserver uses its Web server communication channel. Each Identity Server in the cluster must be added to the Web server list, and the Access Gateway uses its Web server load balancing and failover policies for the clustered Identity Servers.

This configuration has been tested with the Access Gateways plugged directly into the L4 switch. Then the following features were not supported in the tested configuration:

– The Identity Server cannot respond to Identity Provider introductions;

– Federation to an external service provider cannot be supported with this configuration;

– The proxy service that is protecting the Identity Server cannot be configured to use mutual SSL. For example with this configuration, X.509

authentication cannot be used for any proxy service.

To perform X.509 authentication (which is a form of mutual SSL), a user's browser must have direct access to the Identity Server. To configure Access Manager in this manner, the following changes to the basic tested configuration could be performed:

1 Must be changed the port of the Base URL of the Identity Server to 443. If a path-based multi-homing is used, the domain name of the Base URL must match the public DNS of the proxy service set up in the Access Gateway. If domain-based multi-homing is used, the domain name of the Base URL can be different than the Access Gateway, but the DNS server must resolve the name to the IP address of the Access Gateway.

2 (Conditional) In case of use of domain-based multi-homing, a wildcard certificate can be created to be used by the Identity Server and the Access Gateway. For example, *.xxxxx.com, where the Identity Server DNS is idp.xxxxx.com and the Access Gateway DNS is esp.xxxxx.com. In case of use of path-based multi-homing, the same certificate could be used for the Identity Server and the Access Gateway.

3 A proxy service must be set up on the Access Gateway for the Identity Server.

3a When creating the proxy service the following fields must be set to the specified values: Published DNS Name – The same name must be specified for the domain name of the Base URL of the Identity Server. The DNS server must be set up to resolve this name to the Access Gateway. Web Server IP Address – The IP address must be specified of the Identity Server. If the cluster configuration for the Identity Server contains more than one Identity Server, the IP address must be provided of one of the servers. This must be the actual IP address of the Identity Server and not the VIP address if the Identity Server is behind an L4 switch. Host Header – Web Server Host Name must be specified. Web Server Host Name – The domain name of the Base URL of the Identity Server must be specified. This entry matches what is specified in the Published DNS Name field. If proxy service is not the first proxy service of the reverse proxy, either domain-based or path-based multi-homing could be used.

3b (Conditional) For a domain-based proxy service, the Multi-Homing Type field to Domain-Based must be set.

3c (Conditional) For a path-based proxy service, the Multi-Homing Type field to Path-Based and the Path field must be set to /nidp. On the Path-Based Multi-Homing page, the Remove Path on Fill option must be not selected. The Identity Server needs the /nidp path.

4 A protected resource for the proxy service must be configured. The Contract field to None must be set. The Identity Server needs to be set up as a public resource. The URL Path of the protected resource must be set to /nidp/*.

5 The Access Gateway must be set to use SSL between the browsers and the Access Gateway.

6 SSL must be set up between the proxy service that is protecting the Identity Server and the Identity Server.

5. CONCLUSION

Based on the proposed and tested federation scenario students from the University's virtual measurement laboratory as EduTest-application through University Web Server should have Web-single-sign-on access to the Enterprise's measurement systems and they could access only the resources and applications they have given rights for. The tested scenario could be implemented for the educational needs of the large enterprises after negotiations between the university and the enterprise. The goal, which is the student's education in the university, for the enterprise's needs using enterprise's infrastructure, especially the enterprise distributed measurement system, could be achieved and will decrease time and spends for the education. On the other hand the enterprises will be involved in the education and will not have claims on it.

The proposed in this paper federation scenario for construction of a virtual measurement laboratory has no analogues and is not still implemented anywhere.

The proposed federation scenario could be implemented also like University – University Federation for remote education. In this case at the place of the Enterprise will be one of the two universities.

The solution has been chosen to be tested because it has comprehensive and scalable identity and access management capabilities, end-to-end integration across the entire suite for higher productivity and reduced complexity, supports heterogeneous platforms to provide unprecedented choice and openness, e.g. Windows, Linux etc.

The test system and the testing procedures were made in the Bulgarian Gold Novell Training and Solution Partner – Intepro Ltd.

6. REFERENCES

[1] J. Arzoz, V. Slavov, T. Tashev. Virtual laboratory research. *Proceeding of the 6th International Conference on Chalanges in Higher Education and Research in the 21st Century*, Sozopol, Bulgaria, 2008, pp. 403-407.

[2] S. Yordanova, P. Tzvetkov. Application of MATLAB for education on control and

measurement, *Proceeding of the 1st International Conference "Challenges in Higher Education and Research in the 21st Century*, Sozopol, Bulgaria, May 22-24, 2003, pp. 132 -136.

[3] A. Elenkov. The need of identity management when the measurement information has to be accessed. *16-th National Scientific Symposium with international participation Metrology and Metrology Assurance 2006*, Sozopol, Bulgaria, 2006, Vol. 1, pp. 114-116.

[4] T. Wason. Liberty ID-FF architecture overview. *Liberty Alliance Project version 2.0*, 2008.

[5] J. Tourzan, Y. Koga. Liberty ID-WSF Web services framework overview. *Liberty Alliance Project version 2.0*, 2008.

[6] M. Goodner, M. Hondo, A. Hadalin, M. McIndosh, D. Schmidt. Understanding WS-Federation – version 1, *Global XML Web Services Specifications*, May28, 2007.

[7] A. Elenkov. Measurement systems based on disaster recovery strategy. *16-th National Scientific Symposium with international participation Metrology and Metrology Assurance 2006*, Sozopol, Bulgaria, 2006, Vol. 1, pp. 111-113.

[8] A. Elenkov. Virtualization of virtual measurement machines as component of distributed artificial intelligence system. *Proceeding of the 8th WSEAS International Conference on Artificial Intelligence, Knowlidge & Data Bases (AIKED'09)*, University of Cambridge, UK, February 21-26, 2009.

Andrey Angelov Elenkov, *born 1959 town of Radomir, Bulgaria. Current position: Senior Assistant Professor, Technical University of Sofia, Faculty of Automation, Major field – Electrical Measurement. 1990 – Ph.D. from the Technical University of Sofia in Artificial Intelligence. 1985 – Dipl. Engineer of Computer Technology and Electronics, Technical University of Sofia.*

Areas of scientific interests: distributed artificial intelligence, measurement systems.