

# A Management Perspective on IBM Tivoli Access Manager for e-business

## The Question

Corporations have adopted Internet technology as the standard for both internal (intranet) and external (internet) oriented IT systems. In both cases provisions have to be made to :

- Uniquely identify the parties involved in a transaction (authentication)
- Determine and control access to information resources (authorization)
- Protect the privacy and integrity of the information exchanged.

In the early phases of this growth process, these capabilities have often been implemented on a platform or even application basis. The question is whether it makes sense to continue on this path or adopt the infrastructure model, which has been successfully deployed in mainframe environments for decades.

## The RealQuestion

Although nobody will deny the importance of security in today's open environment, there is a lot more at stake beyond the technological aspects. The real management issues behind the above are:

- Control operational costs : provide an effective way to manage users and user profiles on behalf of applications.
- Control development costs : avoid recurrent development efforts to manage user authentication and control access to resources.
- Time to market : increase the speed at which new business applications can be made available.
- Flexibility : how to easily integrate both existing and new applications, and provide a way to adopt new methods (e.g. for authentication) without affecting the entire system.
- Scalability & Availability : make sure that the infrastructure is available on a 24x7 basis and is able to scale to often unpredictable dimensions.

## The Answer

IBM Tivoli Access Manager (ITAM) is an authentication and authorization framework to provide security services for and on behalf of applications, based on industry standards. With ITAM corporations can build an infrastructure offering services such as :

- **Authentication** : ITAM supports almost any form of user authentication, such as userid/password, digital certificates and token-based systems. ITAM also seamlessly integrates with all major PKI infrastructures. In addition, the user's credentials can be passed to back-end application servers in order to simplify application design.
- **Single sign-on** : ITAM can seamlessly log-in users to web-enabled applications, allowing to create a simplified user experience and easily integrate existing applications.
- **Access Control** : ITAM provides a way to centrally define and delegate control of the Access Policy. It can do so on behalf of applications in a reversed proxy mode, and/or make this policy available to application developers through standards-based interfaces, such as the Open Group's aznAPI or the JAAS specification from the Java Developer Connection forum.
- **Logging & Audits** : ITAM offers a network-wide and consolidated collection of all relevant information related to the use of the infrastructure. This information can be used for detection of malicious usage as well as for statistical, billing or planning purposes.
- **Modularity & Fail-over** : all components of the ITAM framework can be implemented in a fail-over mode. Additional components can be added to cope with increased usage, without interrupting the service. In addition, ITAM provides dynamic load balancing to back-end application servers.

The framework concept also provides a way to easily integrate ITAM with the existing environment. User profiles can be managed by ITAM itself or captured from an external repository. ITAM's LDAP-based repository can also be synchronized with external sources. Similarly, the Access Policy can be managed through ITAM's graphical console or be imported from an external source.

Finally, ITAM for MQseries now also offers a way to secure transactions based on IBM's MQseries middleware, a strategic component in many large organizations. The Policy-based approach provides both access control to queues and messages, and allows to define the required Quality of Protection, such as encryption or digital signing.

## **How do you get there ?**

The implementation of such an infrastructure is not a trivial undertaking. In addition, many large organizations have already deployed web servers and web-based applications, which need to be migrated to such an infrastructure approach.

A phased implementation is often the recommended way to cope with both short term requirements and long term strategic objectives. The main phases of this approach consist of :

### **1. Single sign-on to existing Servers**

ITAM is implemented essentially as a proxy front-ending the existing servers, allowing to streamline the authentication process and seamlessly log-in the user to the back-end servers. In addition, some user profile information is forwarded to these servers.

Authorization management is in this phase limited to coarse grain access control to the back-end servers and user-dependent portal behavior.

### **2. Authentication and Authorization Management**

ITAM handles the authentication process on behalf of the applications, which no longer have to take care of user management. The infrastructure provides the user's credentials to the (new) applications and takes care of session management.

Access control services are provided in several ways:

- web-object level authorization and portal behavior is managed by the WebSEAL proxy server.
- The applications use the same Policy Database to control access to application objects. On an Application Server platform such as IBM Websphere or BEA Weblogic, this can be handled in a transparent way for application developers through the use of Permission Classes or EJB's, based on JAAS (Java Authentication and Authorization Specification).

The net result is that the definition and management of user profiles and access policies can be handled in a centralized way, independent from applications. This allows for significant reductions in operational as well as development costs, and will allow the organization to bring new business applications faster to market, a considerable asset in today's and tomorrow's e-commerce world.