Identity Management with TAM E-SSO (Privileged user IDs)

By

Humna Khan	**2008-NUST-BIT-78**
Isra Mashhadi	**2008-NUST-BIT-79**
Ittrat Wafa Hassan	**2008-NUST-BIT-80**

**A Project report submitted in partial fulfillment
of the requirement for the degree of
Bachelors in Information Technology**

Department of Computing

**School of Electrical Engineering & Computer Science
National University of Sciences & Technology
Islamabad, Pakistan
2012**

CERTIFICATE

It is certified that the contents and form of thesis entitled **“Identity Management with TAM E-SSO (Privileged user IDs)”** submitted by **Humna Khan (2008-NUST-BIT-78), Isra Mashhadi(2008-NUST-BIT-79), Ittrat Wafa Hassan (2008-NUST-BIT-80)** have been found satisfactory for the requirement of the degree.

Advisor: ______________________________

(Mr. Aatif Kamal)

Co-Advisor: ______________________________

(Mr. Mujtaba Haider)

DEDICATION

To Allah the Almighty

&

To my Parents and Faculty

ACKNOWLEDGEMENTS

I am deeply thankful to my advisor and Co-Advisor, Mr. Aatif Kamal, and Mr. Mujtaba Haider for helping me throughout the course in accomplishing my final project. Their guidance, support and motivation enabled me in achieving the objectives of the project.

Abstract

Privileged user id is a technique which allows user to access different hardware or software without knowing actual password. Through this technique user is given one login/password of TAM-ESSO and when logs on to a machine through TAM-ESSO, TAM-ESSO add all the allowed applications login/password to user account.

Out final year projects main objective is to implement PUids concept to manage SEECS lab users and allow them to access lab login protected machines or software without sharing with them the user id and password.

For example while using WAMP server in SEECS labs students require to login with administrator access rights which cannot be shared with them. Therefore we need such PUids solution that will allow them to admin access for limited time.

In order to solve this problem, we can use single sign on feature which can be achieved using two IBM products named as ITIM (IBM Tivoli Identity Manager) and TAM-ESSO (Tivoli access manager-enterprise single sign on). ITIM (IBM Tivoli Identity Manager) automates and centralizes access right management and provisioning across multiple systems such as applications and operating systems.

1. Allows central control of privileged data
2. Role based access control
3. Automated provisioning of access rights

TAM E-SSO (Tivoli access manager-enterprise single sign on) provides users with single sign on facility to log on to every application on both the company network and the internet. It is intelligent software that works by responding to log on request on behalf of the user directly from their desktop.

Table of Contents

List of Abbreviations

ITIM: IBM Tivoli Identity Manager

TAM E-SSO: Tivoli Access Manager Enterprise Single Sign On

AD: Active Directory

IMS: Integrated Management Server

AA: AccessAgent

SSO: Single Sign On

WAS: Web Application Server

OS: Operating System

RFID: Radio Frequency Identification

PC: Personal Computer

TDI: Tivoli Directory Integrator

RMI: Remote Method Invocation

SSL: Secure Socket Layer

List of Tables

List Of Figures

Chapter No.1

INTRODUCTION

1.1 Project Background

Basically there are two types of threats that can effect an organization and its operations. These threats are:

- External Threats
- Internal Threats

Internal threats are more dangerous than external threats for an organization. Identity theft is one of the internal threats.

Identity theft can be defined as stealing another person’s identity in which someone pretends to be someone else by assuming that person's identity to access resources or obtain credit and other benefits by that person's name.Organizations and individuals who are defrauded by the identity thief can also suffer adverse consequences and losses and to that extent are also victims. Privileged identity management is a way to combat this problem.

1.1.1 Privileged User Identity Management

Privileged users are required by every organization that deploys IT infrastructure. These privileged users include system administrators, accounts, managers, and business executives. They are granted administrative or special rights to manage business-related resources. These resources may be operating systems, ERP systems, databases, and many other applications, systems, and platforms. A pool of users usually share privileged ID’s which becomes cause of compliance issues and hence increase the risk of data theft. Data center consolidation, cloud computing, and virtualization can produce an even greater number of privileged IDs today.

Privileged Identity Management can provide services which can enable an organization to manage and audit their pool of privileged user IDs centrally. These IDs can be checked in and checked out by authorized people when required. It is basically a technique that provides the necessary technical controls to provide the account-sharing concept. This approach enables an organization to effectively control access, simplify privileged access manage all accounts, and maintain an audit structure which is consistent with regulatory requirements.

The term "Privileged Identities" refers to any type of user or account that holds special or extra permissions within the enterprise systems. These accounts are distinguished from general user IDs by assignment of their roles like security, administrative, or system authorities. Privileged identities are usually categorized into the following types:

- **Administrative Accounts** – these are non-personal accounts that exist in virtually every device or software application. These accounts hold privileges and are often shared among IT staff.
- **Privileged Personal Accounts** – these are powerful accounts that are used by business users and IT personnel. These accounts have a high level of privilege and their use can significantly affect the organization's business.
- **Application Accounts** – the accounts used by applications to access databases and other applications. These accounts typically have broad access to underlying business information in databases.
- **Emergency Accounts** – special generic accounts used by the enterprise when elevated privileges are required to fix urgent problems. Access to these accounts frequently requires managerial approval.

1.2 Problem Statement

“Implementation of Privilege User IDs concept to manage SEECS lab users and allow them to access lab login protected machines or software without sharing with them the user id and password.”

1.3 Aims and Objectives

- Provide convenient user access while protecting IT resources.
- Provide audit trail and reporting mechanisms for tracking privileged user’s activity.
- Providing access of e-mail server, LMS, putty, wamp and AIX to guest users at IBM lab, without sharing passwords.

1.4 Solution Architecture

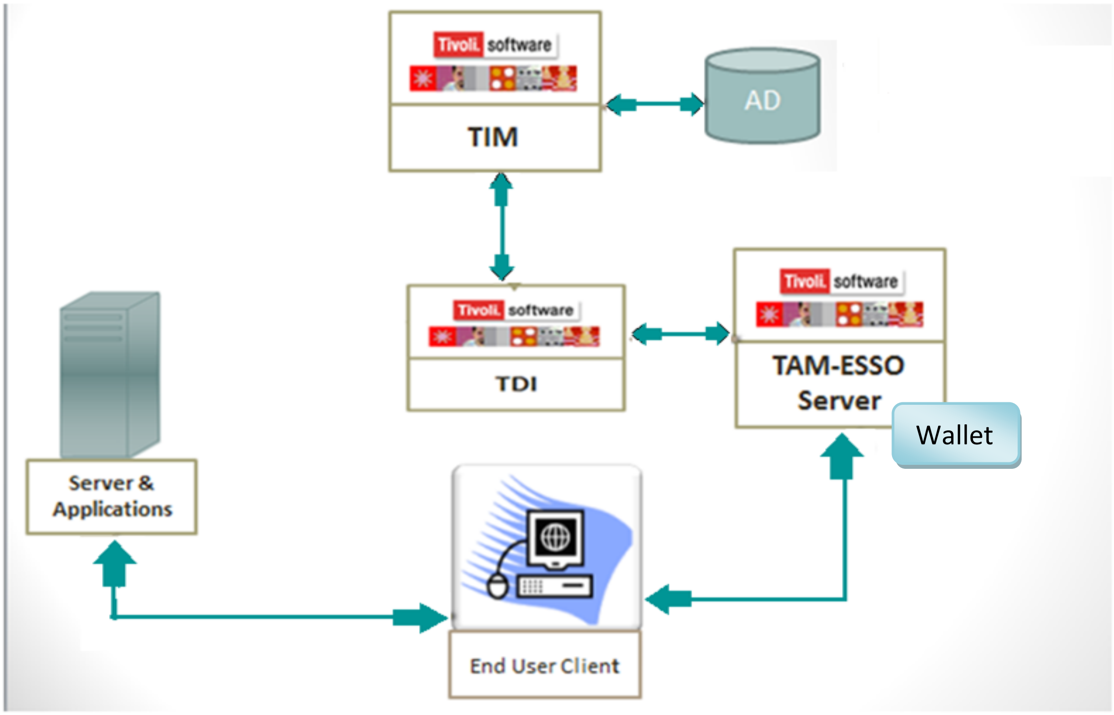


Figure 1.1 Project Architecture Diagram

1.5 Success Factors

- Understanding the User and its life cycle as an entity.
- Management of identities of an organization using IBM Tivoli Identity Manager (ITIM)
- Deployment of Tivoli Access Manager (E-SSO) on Windows Platform and management of ’role based access’
- Integration of IBM Tivoli Identity Manager and Tivoli Access Manager (E-SSO)
- Advance profiling to manage different IT resources like access of e-mail server, LMS, putty, wamp and AIX to guest users at ibm lab, without sharing passwords.

1.6 Block Diagram

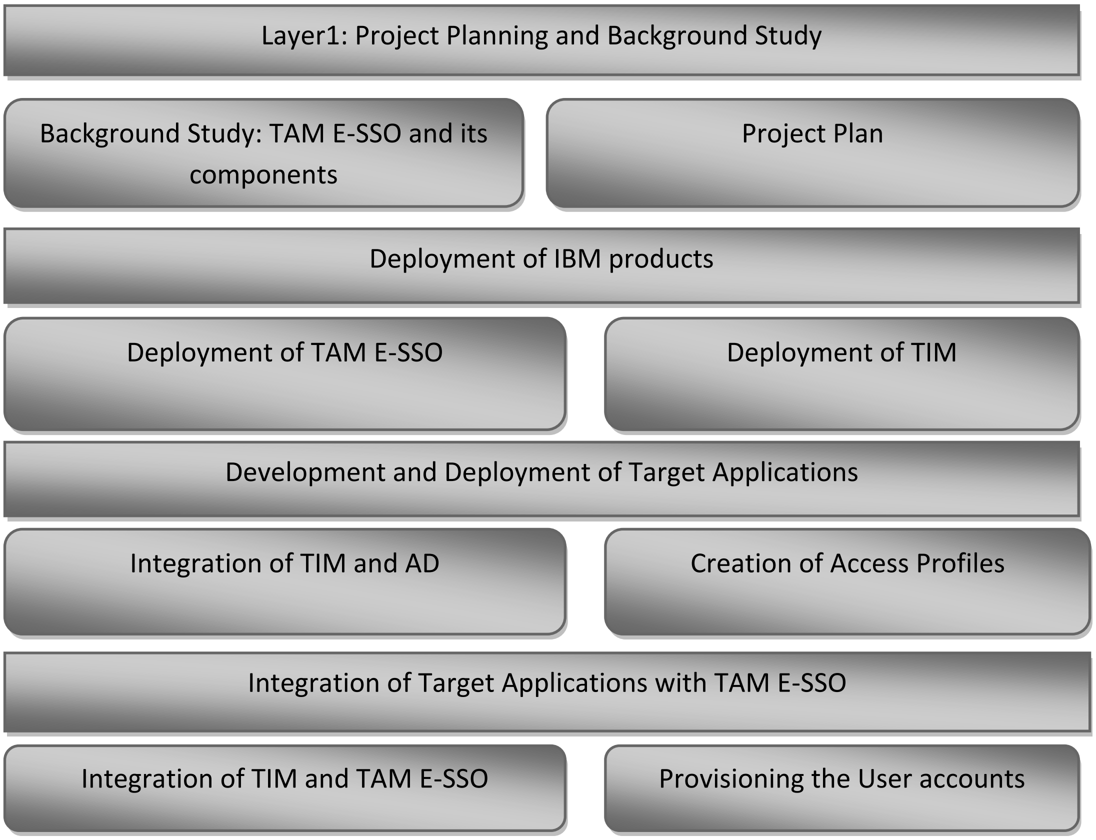

Layer1: Project Planning and Background Study
Background Study: TAM E-SSO and its components
Project Plan
Deployment of IBM products
Deployment of TAM E-SSO
Deployment of TIM
Development and Deployment of Target Applications
Integration of TIM and AD
Creation of Access Profiles
Integration of Target Applications with TAM E-SSO
Integration of TIM and TAM E-SSO
Provisioning the User accounts

Figure 1.2: Project Block Diagram

1.7 Software & Hardware Requirements

Table 1.1: Project Hardware Requirements

Hardware Name	Specification (in each machine)
Processor	2x Core 2 Duo
RAM	4GB
Hard Disk	160 GB
No of Machines required	2 or more (for demo)

Table 1.2: Project Software Requirements

Software Name	Version	Operating System
Windows Server	2008	Windows
Tivoli Identity Manager	5.1	Linux
Tivoli Access Manager	8.0	Windows
IBM DB2	9.7,9.1	Linux(ITIM),windows(TAM E-SSO)
WAS	7.0	Linux(ITIM),windows(TAM E-SSO)

1.8 Risk Analysis Chart

Table 1.3: Project Risk Analysis Chart

Risk	**Occurrence (1-10)**	**Severity (1-10)**	**Impact**
Lack of inputs from stakeholders	07	08	56
Availability of training material	03	08	24
Availability of Software	04	10	40
Availability of Hardware	01	10	10
Unfeasibility of TIM with TAM-ESSO	06	10	60
Continuous change in requirements	04	06	24
Timely completion of the project	05	10	50

1.9 Major Deliverables

Table 1.4: Project Major Deliverables

Deliverable Name	**Tentative Time**
Abstract	September 30, 2011
Proposal Defense	November 25, 2011
Proposal Document	December 2, 2011
Installation and Configuration of TIM, TAM-ESSO	December 2011
Integration of TIM and AD	January 2012
MID Defense	February 20, 2012 - February 25, 2012
Mid Defense Documentation	February 2012
Final Defense (Internal)	May 8, 2012
Testing and solving issues or challenges	May 2012
Final Defense	June 4, 2012 - June 7, 2012
Final Defense Documentation	June 2012

Chapter No.2

LITERATURE REVIEW

This Chapter will present an overview of the all the literature reviewed pertinent to this project. This chapter contains details about the basics of IBM Tivoli Identity Manager and IBM Tivoli Access Manager ESSO, its components, architecture and various other core functionalities. This chapter is mostly about the different reviews of red books and other IBM publications.

2.1 IBM Tivoli Identity Manager

IBM Tivoli Identity Manager is a policy-based identity and access governance solution that helps automate lifecycle management of user roles, identities and access rights. Tivoli Identity Manager is commonly abbreviated as ITIM. It provides with an identity management solution. ITIM provides administrator efficient way to manage user and their accounts, provisioning tasks and policies. Tivoli Identity Manager allows an organization to efficiently identities thus reducing the administrative overhead. Security guidelines are defined by the administrator and are put into practice in consistent manner. This includes password rules, account approvals, schedules recertification of the account etc.

2.1.1 Features

Tivoli Identity Manager delivers following capabilities:

- **Centralized user management** – Tivoli Identity Manager allows centralized user management through decentralized administrator. This helps is cost reduction of user management. Security policies are automatically enforced. The risk of a former employee accessing an organization resource is reduced.
- **Single interface** – Tivoli Identity Manager provides with centralized identity management and role-based access control over the administration of users.

This provides us with a common interface for administration of user identity. Thus reducing cost of maintenance.

- **Security policy enforcement** – Tivoli identity Manager allows us to implement identity management policy which complies with an organization's security policy. This creates a successful identity and credential management system. Centralized control accommodates both business and security policies, enabling administrator to implement it efficiently.
- **Central password management** – A user can typically have more than one account and password. Tivoli Identity Manager helps synchronize passwords across all application and makes it easier to use. Password policy can be applied across all the organization to create a password a certain length and character. Centralized user management allows user to change password for one or multiple accounts through single interface. It can also help change password for remote systems

2.1.2 Core Components

The logical component design of IBM Tivoli Identity Manager may be separated into three layers of responsibility, which are depicted in the following picture. They are as following:

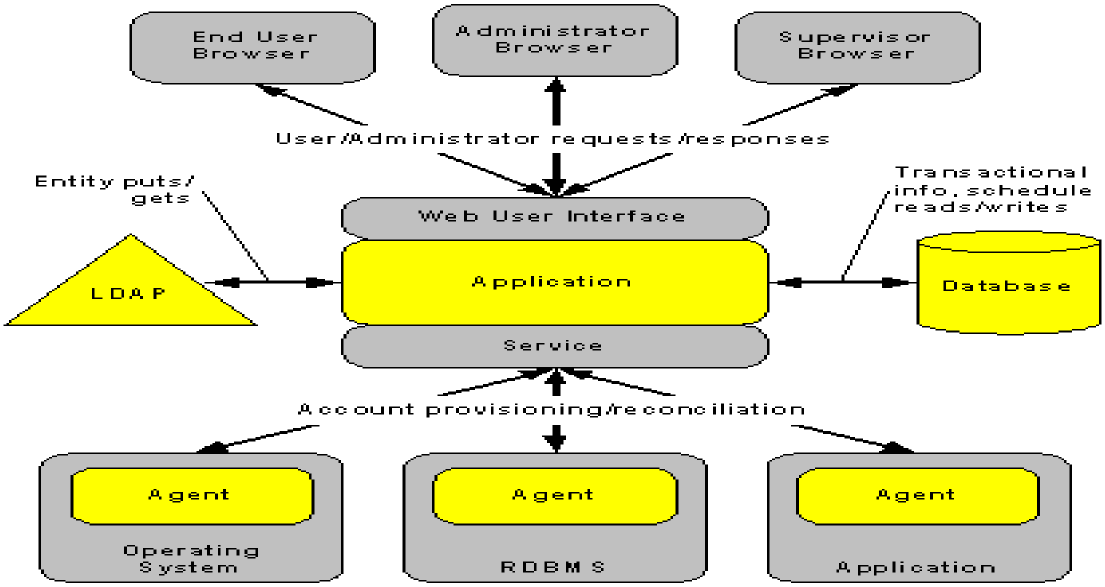


Figure 2.1 Components of Tivoli Identity Manager

- **Web User Interface Layer** – The Web User Interface module is a set of combined sub-processes that provide content to a user's browser and initiate applets (run both on the client and the server), such as the Workflow Design and the Form Creation. The Web User interface is the interconnecting layer between the user's browser and the identity management application layer. The Web User Interface subsystem contains all modules necessary to provide a Web based front end to the applications of the Applications subsystem, as shown in the following picture:

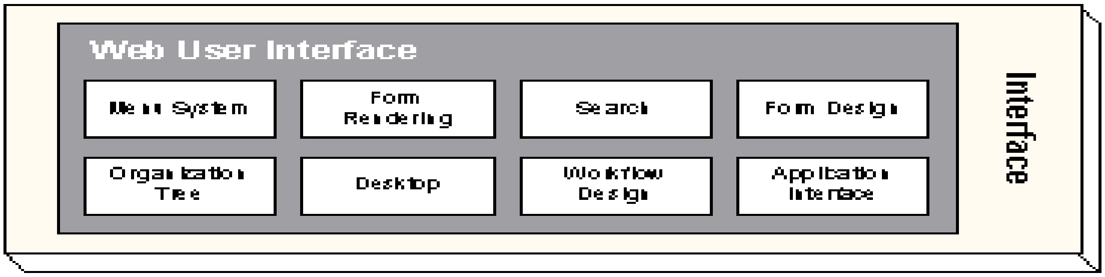


Figure 2.2 Web User Interface Layer

- **Application layer** – The most important component of Tivoli Identity Manager is the Application layer which resides on the Application Server. It provides the functionality of all other process objects. It is the application layer module that consists of user specific interface components.

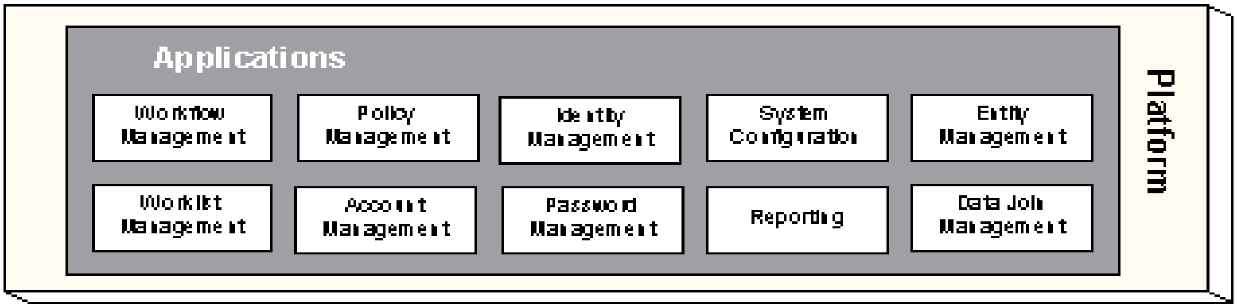


Figure 2.3 Application Layer

- **Service layer –** IBM Tivoli Identity Manager is an application of complex objects and application server runs those objects. The Service layer consists of the basic services that can be used when provisioning e.g. authentication, authorization, workflow etc.

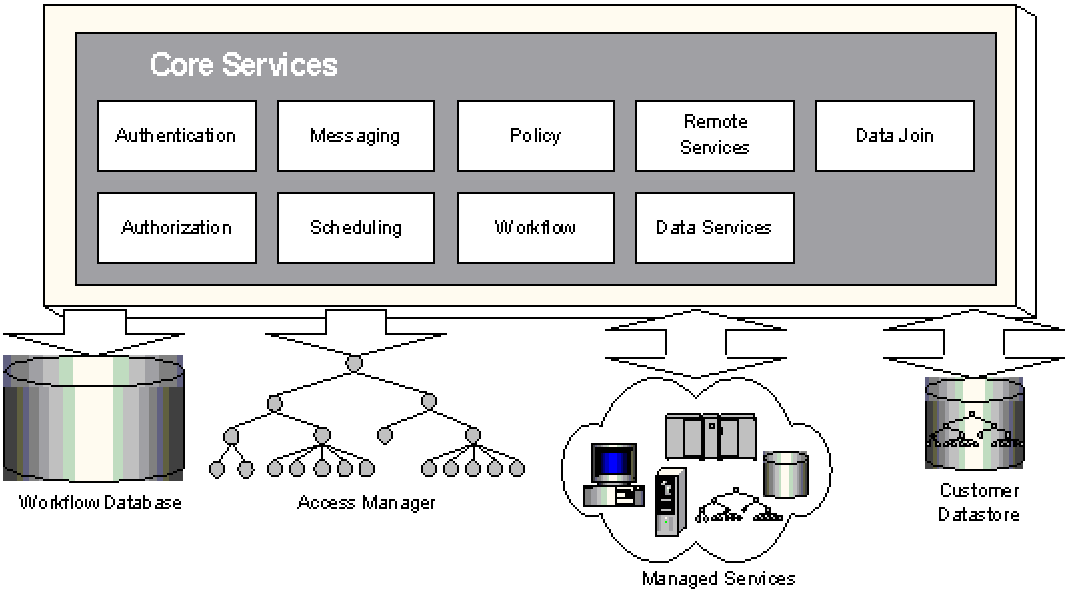


Figure 2.4 Service Layer

- **LDAP Directory** – The Tivoli Identity Manager uses LDAPv3 Directory Sever as its primary repository to store current state of an organization. This includes user, accounts, roles, organization chart etc.

- **Database** – Database is used to store the transactional and scheduling information. Basically a database has two instances, one is used by directory server to store the user related information while the other is used by the ITIM to store workflows**.**
- **Resource connectivity** – IBM Tivoli Identity Manager provides a very extensible framework for communicating directly to different services and resources. Built-in capability is used to communicate with a remote agent who used Directory Service Markup Language as communication mechanism.

2.2 Tivoli Access Manager for Enterprise Single Sign-On (E-SSO)

Change Management has become an essential part of managing IT system security. Often IT teams have to share login credentials for applications and resources over a netowrk. These privileged acounts provide unlimited access to a data and resources of a organization. If not properly maintained, this can cause serious risk to an organization.

Tivoli Access Manager for Enterprise Single Sign-On is the first enterprise access solution that allows an enterprise to simplify, strengthen and control access to the digital resources and physical system. It combines the single sign-on/sign-off automation, authentication management and user tracking to provide a seamless part to strong digital identity. It transparently increases security, enhances user convenience, and provides integrated access across existing information, network and physical system. Thus an organization does not have to choose between strong security and convenience, they can have both.

Tivoli Access Manager can efficiently manage business risks, achieve regulatory compliance, and decrease IT cost and increase user efficiency.

Single Sign-On (SSO) is basically entering one username and password to access multiple resources of an organization with single sign-on. There are two types of SSO products. Many SSO products are known as Simplified Single Sign-on or reduced sign-on products because they do not support all types of applications logon. Fortified Single Sign-On (FSSO) is single sign-on with enhanced security capabilities such as scrambling of passwords and the ability to upgrade the authentication process to use certificates.

Tivoli Access Manager provides use with fortified single sign-on with sign-on automation technology to augment security. Tivoli Access Manager uses fortified single sign-on because:

- It enhances security for enterprise by choosing from several authentication factors to provide two-factor authentication.

- Password for different applications can be strengthened by automating the periodic change an AccessAgent password to application-policy aware long randomized strings. You do not have to remember password and you do not have to share them to social engineering.

Tivoli Access Manager for Enterprise Single Sign-On delivers following capabilities without changing the existing IT infrastructure:

- **Workflow Automation –** Tivoli Access Manager for Enterprise Single Sign-On uses workflow automation on shared and personal workstations. The administrator can automate the entire workflow, such as application login, drive mapping, application launch, single sign-on, navigation to preferred screen, multistep logon, and so on. Single Sign-Off and configurable desktop protection policies ensure protection of confidential corporate applications from unauthorized access. If you forget to log out of an application, Tivoli Access Manager for Enterprise Single Sign-On can be configured to enforce inactivity timeout policies.
- **Strong Authentication for users group –** Tivoli Access Manager for Enterprise Single Sign-On provides strong authentication for all users groups. It prevents unauthorized access to confidential corporate information and IT networks. The solution uses multi-factor

authentication devices, such as smart cards, building access badges, proximity cards, mobile devices, photo badges, biometrics and one time password tokens.

- **Comprehensive session management capability –** Organizations can increase user convenience and improve information security through session management or fast user switching capabilities, depending on the access needs user groups. You can quickly sign on and sign off to share workstations without using the Windows domain login process. You can easily resume work from where you left off. You can maintain multiple unique user desktops on the same workstation by switching from one private desktop to another. This feature preserves your applications, documents, and network drive mappings, including those belonging to other users sharing the workstation. If you walk away from a session without logging out, you can set Tivoli Access Manager for Enterprise Single Sign-On to enforce inactivity timeout policies. It also supports hybrid desktops where organizations combine different session management capabilities to meet the needs of your user community.
- **User-centric access tracking for audit and compliance reporting –** The audit and compliance reporting feature assists organizations with data consolidation, user-centric audit log generation, security, and tamper-evident audit capabilities across all endpoints. Combined with strong authentication capabilities, the centric audit logs ensure secure access to confidential corporate information and accountability at all times. The logs provide the Meta information that can guide compliance and IT Administrators to a more detailed analysis – by user, by application, or by endpoint. The information is collated in a central relational database. These logs facilitate real-time monitoring and separate reporting with third-party reporting tools.

- **Secure remote access for easy, secure access anywhere, anytime –** Secure Remote Access provides Web browser-based single sign-on to all applications such as legacy, desktop, and Web applications from outside the firewall. Your organization can effectively and quickly enable secure remote access for the mobile workforce without installing any desktop software and modifying application servers. Remote workers require only one password and an optional second authentication factor to access corporate information from remote offices, home computers, and mobile devices. When granted access, you can single sign-on to corporate applications by clicking the application links available in the Tivoli Access Manager for Enterprise Single Sign-On portal. Access can be further protected through a Secure Sockets Layer (SSL) Virtual Private Network (VPN).
- **Integration with user provisioning technologies –** Tivoli Access Manager for Enterprise Single Sign-On combines with user provisioning technologies to provide end-to-end identity lifecycle management. New employees, partners, or contractors get fast and easy access to corporate information after being provisioned. When provisioned, you can use single sign-on to access all your applications on shared and personal workstations with one password. You do not have to register each user name and password, as all your credentials are automatically provisioned.

2.2.1 Components of TAM E-SSO:

The main components of TAM E-SSO are:

- Identity Wallet
- TAM E-SSO AccessAgent
- TAM E-SSO AccessAdmin
- TAM E-SSO AccessAssisstant
- TAM E-SSO AccessStudio

- TAM E-SSO IMS Server
- TAM E-SSO Web Workspace

Tivoli Access Manager for Enterprise Single Sign-On provides its single sign-on functionality by introducing a layer that authenticates a user once and then automatically detects and handles subsequent requests for user credentials. Figure 2-1 depicts and overview of the solution.

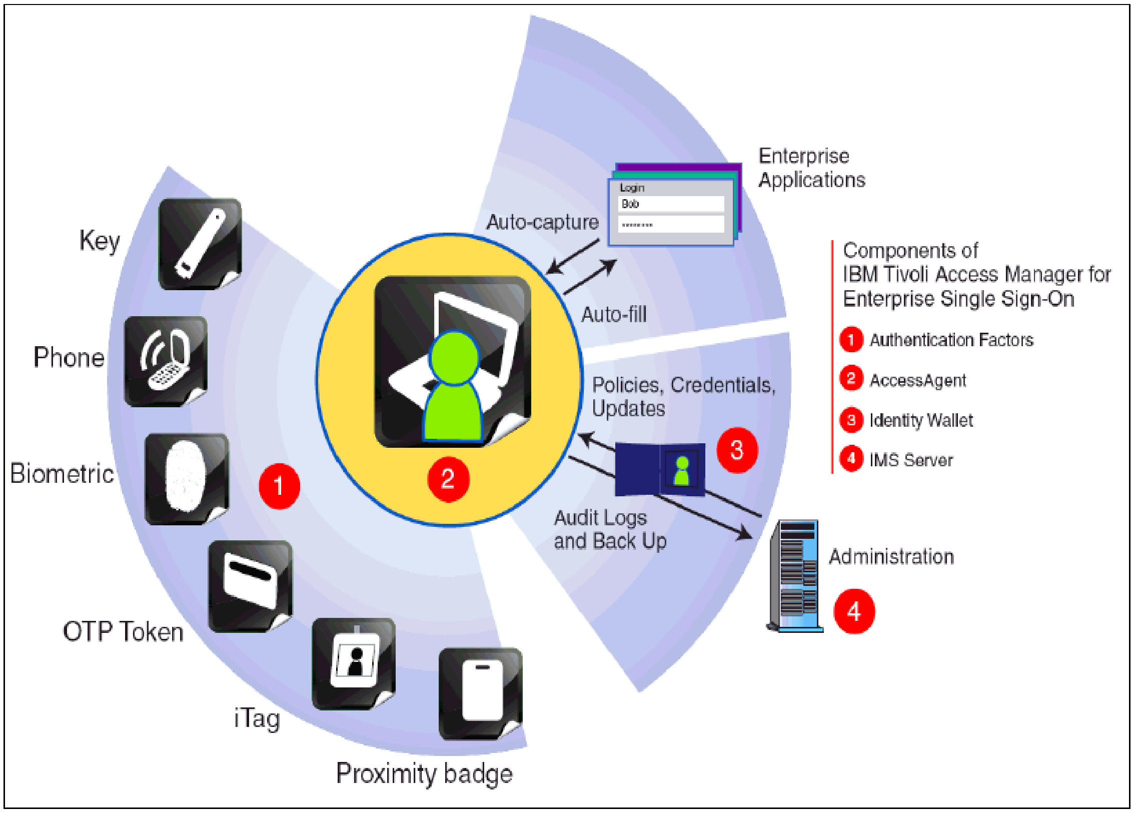


Figure 2.5 TAM-ESSO Product Overview

Tivoli Access Manager for Single Single-On can be divided into the following four functions:

- **Authentication factors** – Tivoli Access Manager for Enterprise Single Sign-On supports various authentication factors to authenticate the users. Besides the standard user name/password based authentication, the user can be authenticated by means of a proximity or building badge like active or passive RFID, a fingerprint, a one-time password provided by SMS or OTP (One-time token) token, or a USB token.

- **AccessAgent –** The AccessAgent runs on every Windows desktop endpoint, Microsoft Windows Server Terminal Services session, and Citrix MetaFrame Presentation Server session. The AccessAgent is responsible for authenticating the user. It can automate single sign-on into Windows and to the set of applications that are defined in AccessProfiles. The AccessAgent can extend the Windows Graphical Identification and Authentication (GINA) DLL chain to provide additional functions for self-service or strong authentication.
- **Identity Wallet –** The identity wallet (or Wallet) holds the user credentials that are required for single sign-on. It is loaded from the IMS Server into the AccessAgent after successful authentication of the user so that it is available even when the endpoint is disconnected from the computer network. To protect the credentials against tampering or stealing, the identify wallet is encrypted with a strong encryption mechanism.

The authentication factors may be used based on an organization's security policy:

- ActiveCode
- USB Key
- USB Proximity Key
- RFID card
- Active Proximity Badge
- Fingerprint Identification

2.2.1.1 Identity Wallet

The Wallet stores a user's access credentials and related information (including user IDs, passwords, certificates, encryption keys). Each user has a Wallet which is protected by a lock. The lock can be as simple as a password, or can be fortified with a second authentication factor. The Wallet is governed by a set of security policies. The Wallet can be accessed from any end point, either on a workstation where AccessAgent is installed or through a browser. A “cached” Wallet is an optional copy of the Wallet stored in the hard disk of the computer users sign up with. Users can retrieve the cached Wallet in emergencies, for example, for access without IMS Server connectivity. In an environment where workstations are regularly shared by several users, one user may have access to several workstations. In that scenario, caching a Wallet saves a lot of time, removing the need to download the Wallet from the IMS Server every time a user accesses another workstation.

2.2.1.2 TAM ESSO AccessAgent

TAM E-SSO AccessAgent is the client software that manages the user's Wallet, enabling automatic sign-on to applications and strong authentication. However, the TAM E-SSO AccessAgent does not store passwords. Passwords are stored in the Wallet, and known only to the rightful user. Users can also use it to conveniently manage credentials. The different functions of TAM E-SSO AccessAgent are as follows:

- **Password management** – The Wallet of AccessAgent stores and enters user names and passwords for different applications.

- **Consolidation of user credential** – In the background, the Wallet of AccessAgent remembers user names for different applications used by a user and sends them to the IMS Server for consolidation.

- **Backing up of user credentials**– AccessAgent synchronizes user credentials on the IMS Server to ensure that if users lose their authentication factors or forget their passwords; their user credentials can be recovered.

- **Enforcement of password policies –** Enterprise password policies that automatically change passwords to keep them dynamic are specified in IMS Server and enforced by AccessAgent.

- **Logging of user and system actions**– Actions performed by users or actions related to Wallet or AccessAgent are logged in log files, synchronized with the IMS Server and consolidated.

To use TAM E-SSO AccessAgent, the following must be set:

- Password
- Secret

The password can be fortified using a second authentication factor. The combination of the password and a USB Key, for example, strengthens the computer's security because both authentication factors must be present to access the computer.

2.2.1.3 TAM E-SSO AccessAdmin

The TAM E-SSO AccessAdmin is the management console used by individuals with the Administrator Role and/or the Help desk Role to administer the IMS Server, and to manage users and policies.

2.2.1.4 TAM E-SSO AccessAssistant

The TAM E-SSO AccessAssistant is the Web-based interface used to provide password self-help. Users use AccessAssistant to obtain the latest credentials to log on to their applications.Using AccessAssistant, users can access their application passwords from a Web browser without AccessAgent installed on the computer. This feature can be enabled or disabled for the user. Mobile ActiveCode or a Help desk-issued authorization code can be used as a second authentication factor for authentication to AccessAssistant. Secret questions and answers can also be used to bypass the authorization code requirement, so that users will not have to call Help desk.

2.2.1.5 TAM E-SSO AccessStudio

The TAM E-SSO AccessStudio is the wizard-based tool used by the Administrator to create and manage AccessProfiles and enable SSO, sign-off, and workflow automation. Each application is represented by an AccessProfile, which is a set of instructions that defines the workflow for that particular application.

2.2.1.6 TAM E-SSO IMS Server

The TAM E-SSO IMS Server is an integrated management system that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, and authentication policies. It also provides loss management of authentication tokens, certificate management and audit management for the enterprise. The IMS Server interfaces with other applications through IMS Connectors and IMS Bridges. It is the IMS Server that interfaces with other identity management systems. The IMS Server uses a special IMS Connector, called a messaging connector, to send MACs to users. See ActiveCode for a description of Mobile ActiveCode (MAC).The IMS Server can be configured via AccessAdmin, which is a Web interface for Administrators and Help desk to search for and provision users, set policies, and view audit logs and reports. Lower-level configuration settings for the IMS Server can be configured via the IMS Configuration Utility, which is accessible by Administrators.TAM E-SSO IMS Server is responsible for identity management, certificate management, and recording administrative, user and system actions in audit logs.A backup of the user's Wallet's contents is stored on the IMS Server, so AccessAgent can retrieve the backed-up information by connecting to the IMS Server with a proper authentication. The information is encrypted and cannot be read by anyone, including Help desk officers and Administrators.IMS Server is an application server that is used for:

- **Managing Wallet and authentication factors –**Help desk officers and Administrators can view the type of authentication factor the user is using. Using AccessAdmin, a Wallet can be revoked denying the user access to the Wallet and passwords. It can also be used a reference point to see all the identities the user has in the enterprise. The Administrator can then go into each application and turn off the user's access.
- **Managing policies –** TAM E-SSO uses policies to control the behavior of its components. These policies are configurable through various means, so TAM E-SSO can meet the requirements of specific organizational requirements. Policies have different visibility and scope; and are managed by different roles. Policies may be applicable system-wide, or only to certain groups of users. The applicability of a policy is determined by its scope, which can be System, User, or Machine.
    - **System**: Policy is system-wide
    - **User**: Policy affects only a specific user
    - **Machine**: Policy affects only a specific machine

All policies can be configured via AccessAdmin. Changes to these policies are propagated to clients the next time AccessAgent synchronizes with the IMS Server. Administrators can also choose to apply policies to a group of users, by using the search function to find a specific group of users, then applying a set of policies to the select group.

- **Managing certificates** – The IMS Server has a built-in Certificate Authority that manages certificates.
- **Maintaining logs**– Actions performed by users, Help desk officers, Administrators are all logged in log files providing a comprehensive audit trail.The IMS Server produces detailed logs of its activities and is also responsible for collating AccessAgent's logs. This provides the Administrator a centralized view of the enterprise's operations. All logs are stored in the database. TAM E-SSO IMS Server logs can be viewed using a custom report generator like Crystal Reports or customers can create their own reports.IMS service modules are add-on modules that extend the basic services (user management, policy management, and certificate issuance, etc.) provided by the IMS Server.
- **IMS bridge –** An IMS service module that enables applications to use the TAM E-SSO IMS Server as an authentication server.
- **IMS connector –** An IMS Service Module that enables the IMS Server to interface with other applications as a client, extending the capability of the IMS Server.

2.2.1.7 TAM E-SSO Web Workplace

The TAM E-SSO Web Workplace is a Web-based interface that gives users the ability to log on to enterprise Web applications by clicking on links, without remembering the passwords for individual applications. It can be integrated with the existing portal or SSL VPN.

Chapter No.3

Methodology

This chapter provides the overview of the methodology used in the project to obtain the desired results.

3.1 Basic Methodology

Here is the basic methodology of our project that will explain the working of our project. Firstly ITIM is installed and TAM E-SSO is deployed. All the identities are created in ITIM. ITIM will integrate with TAM E-SSO that will manage the access of IT resources like e-mail server, LMS, putty, wamp and AIX to guest users at ibm lab, without sharing passwords that are created in ITIM providing single sign on facility by which users are not required to remember their passwords for all the applications mentioned above as user's credentials will come from wallet (after authentication of users by ITIM) maintained by TAM E-SSO access agent.

3.2 Deployment of Tivoli Identity Manager:

Tivoli Identity Manager is deployed on RHEL 5.1. To install the Tivoli Identity Manager we need to first install following components:

- **DB2** – The main purpose for installing database is to store different data objects. DB2 will store two instances. One will be used by Tivoli Directory Server to store identities, accounts, policies etc. While other will be used by ITIM to store workflows and other transactional information etc. We need install database before any other component as the database is used further used during the installation for storing data objects.

- **IBM WebSphere Application Server** – Tivoli Identity Manager Server is java wed-based application and we need an application Server to run it. Therefore we use WAS to host Tivoli Identity Manager Server. This enables ITIM administrator and users to benefit from WAS clustering capabilities and Service Oriented Architecture (SOA). With WAS, we also need to install the WAS fix pack which updates WAS according to the requirements of ITIM.

- **Tivoli Directory Server** – TDS is IBM’s own LDAP database which is used for managing user, accounts, policies etc. With the installation of TDS, we also need to configure the company’s suffix for which we are deploying the ITIM.

- **Tivoli Directory Integrator** – It is optional to install TDI. It should be installed before TDS because TDI version provided by TDS installer is not sufficient. TDI is needed where we need to communicate to a managed resource or import complex HR feed. It host agent-less adapter based of RMI. We can install TDI remotely on a different machine or on the same machine where ITIM is installed.

- **Middleware Configuration of DB2 and Tivoli Directory Server** – Middleware Configuration tool configures DB2 and TDS with custom values needed by ITIM before installation of ITIM. The tool allows you to customize database according to your company’s environment. Both DB2 and TDS are configured independently. The company’s suffix is configured through the middleware configuration tool.

- **Installation Tivoli Identity Manager** – The installation program is platform specific. With the installation of ITIM, we also need to configure db2, TDS and WAS. Tivoli Identity Manager Installation program runs configuration tool automatically. It is used to edit commonly used properties for TDS and WAS settings used by Tivoli Identity Manager.

3.3 Integration of Tivoli Identity Manager with Windows Active Directory:

To integrate Tivoli Identity Manager with active directory, we need to follow the following steps:

- **Install Active Directory Adapter** – Basically the task of an adapter is to create accounts, suspend account etc. Therefore an adapter can be thought of as a virtual administrator on the target platform for account management. As Active Directory is an agent-based adapter, therefore it will be installed on the remote system which managed our resources.

- **Create a Service** – Active Directory Adapter needs a way to communicate with the Tivoli Identity Manager. Therefore we need to create a service for the

Adapter which helps us communicate with the adapter. For this purpose, we need to first import the Active Directory Profile i.e. ADprofile.jar into ITIM.

3.4 Deployment of TAM E-SSO

As described in the project architecture Deployment of TAM E-SSO is the requirement of the project.

The deployment of TAM E-SSO has three phases:

- Phase1: Planning
- Phase 2: Installation of TAM E-SSO

3.4.1 Phase 1: Planning

In this phase the structure of TAM E-SSO and its components are studied along with their prerequisites. The Hardware and Software requirements are given below:

Table 3.1 Hardware Requirements for TAM E-SSO

Hardware	**Specification**
Processor	3.0 Core 2 Duo
Memory	3GB
Hard Disk Space	40GB

Table 3.2 Software Requirements for TAM E-SSO

Software Name	**Specification**
Operating System	Windows Server 2008

3.4.2 Phase 2: Installation of TAM E-SSO

The following diagram shows the sequence of installation of TAM E-SSO and its components.

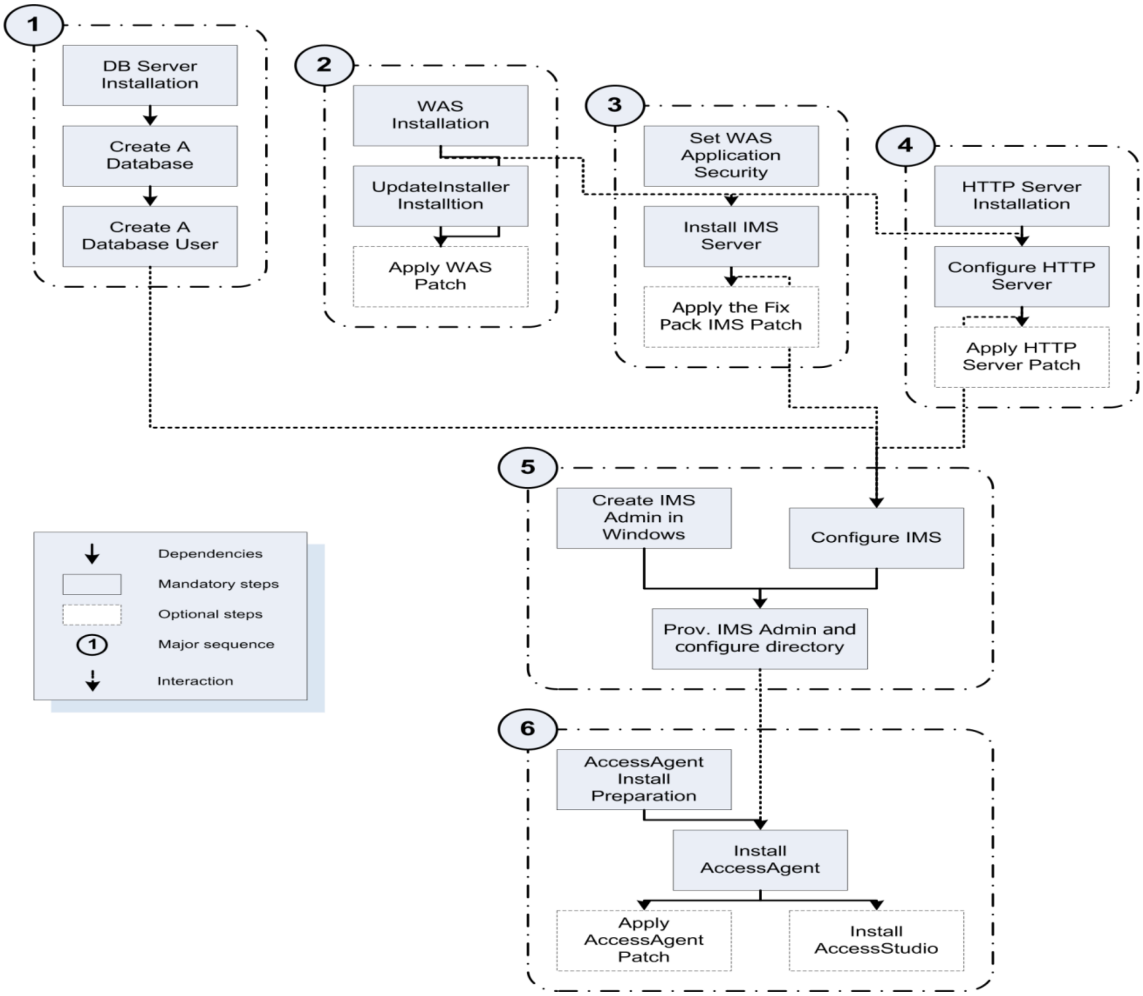


Figure 3.1 TAM E-SSO Installation Diagram

1. Installation of Database Server(DB2)
2. Installation of Application Server (Websphere Application Server)
3. Installation and configuration of IMS server
4. Installation and configuration of HTTP server
5. Installation of AccessAgent
6. Installation ofAccessStudio

3.5 Integration of IBM Tivoli Identity Manager and IBM Tivoli Access Manager (E-SSO)

3.5.1 Software and operating system requirements

Table 3.3: ITIM & TAM Integration Software requirements

Requirements	Version
IBM Tivoli Directory Integrator	
IBM Tivoli Identity Manager Server	5.1
IBM Tivoli Access Manager Server	8.1
IBM Tivoli Access Manager Java Runtime	Corresponding to the version of Access Manager
RMI Dispatcher Version	5.1.2 and above
IBM Tivoli Access Manager Connector	Supplied with the version

Following are the steps for integration of IBM Tivoli Identity Manager and IBM Tivoli Access Manager (E-SSO)

1. Software and operating system requirements
2. Installing RMI Dispatcher

3. Installing TAM E-SSO connector
4. Configure the TAM E-SSO IMS server
5. Configure the SSL connection between RMI Dispatcher and Tivoli Access
6. Importing the adapter profile into the Tivoli Identity Manager Server
7. Creating a Tivoli Access Manager E-SSO service
8. Configuring reconciliation operation for the adapter
9. Configuring Tivoli Access Manager E-SSO workflow extensions

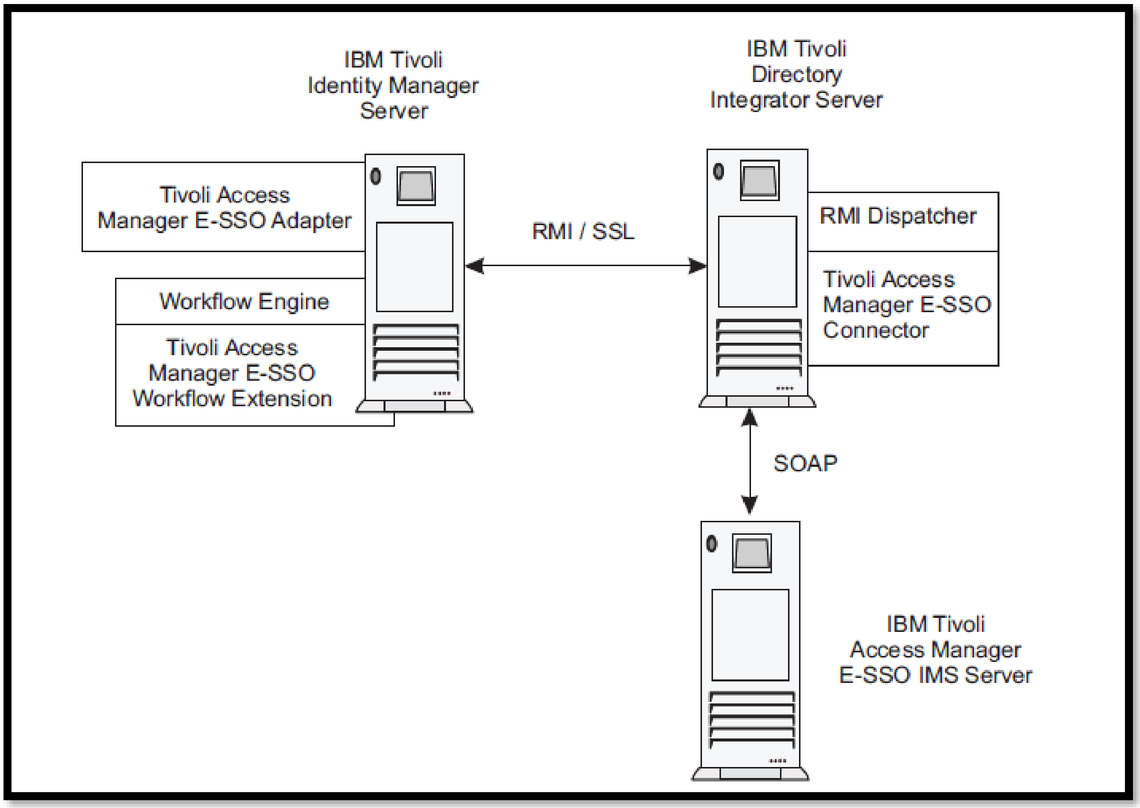

IBM Tivoli Identity Manager Server
IBM Tivoli Directory Integrator Server
Tivoli Access Manager E-SSO Adapter
Workflow Engine
Tivoli Access Manager E-SSO Workflow Extension
RMI / SSL
RMI Dispatcher
Tivoli Access Manager E-SSO Connector
SOAP
IBM Tivoli Access Manager E-SSO IMS Server

Figure 3.2: Integration Architecture

Chapter No.4

RESULTS

This chapter provides the overview of results that were obtained by the end of the project.

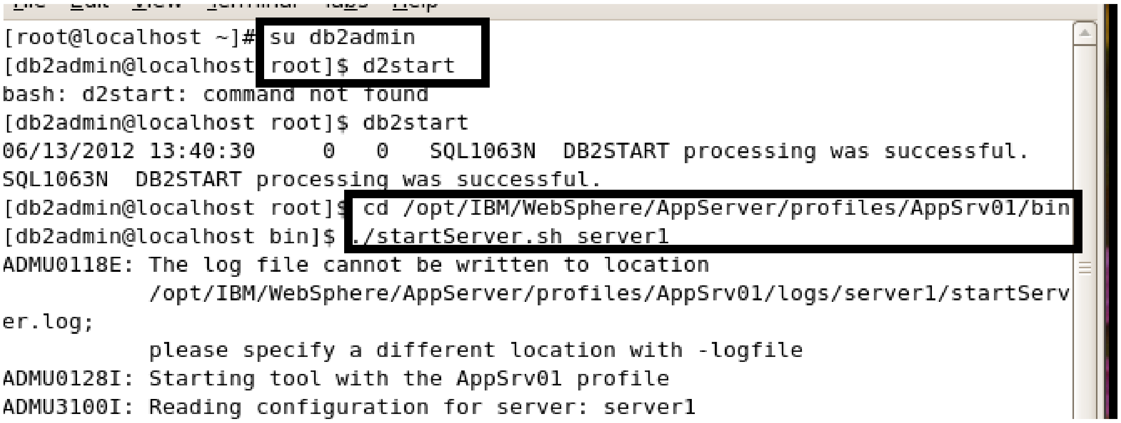
This project was basically a research and configuration based project which include successful deployment of servers and integrations between them and with the target systems to make a mechanism through which provisioning and granting access to users for different applications became easy, efficient and secure.

Basic part of the project is to make the administrative tasks more efficient, easy and secure. On the users end, access to different applications is made easy and efficient.

Main part of the project is Tivoli Access Manager Enterprise Single Sign on for Wallet and profile management to provide single sign on. Profiles are created and added to the wallet of the users depending upon the types of applications and other network or database resources they want to access.

5.1 Administration of IBM Tivoli Identity Manager

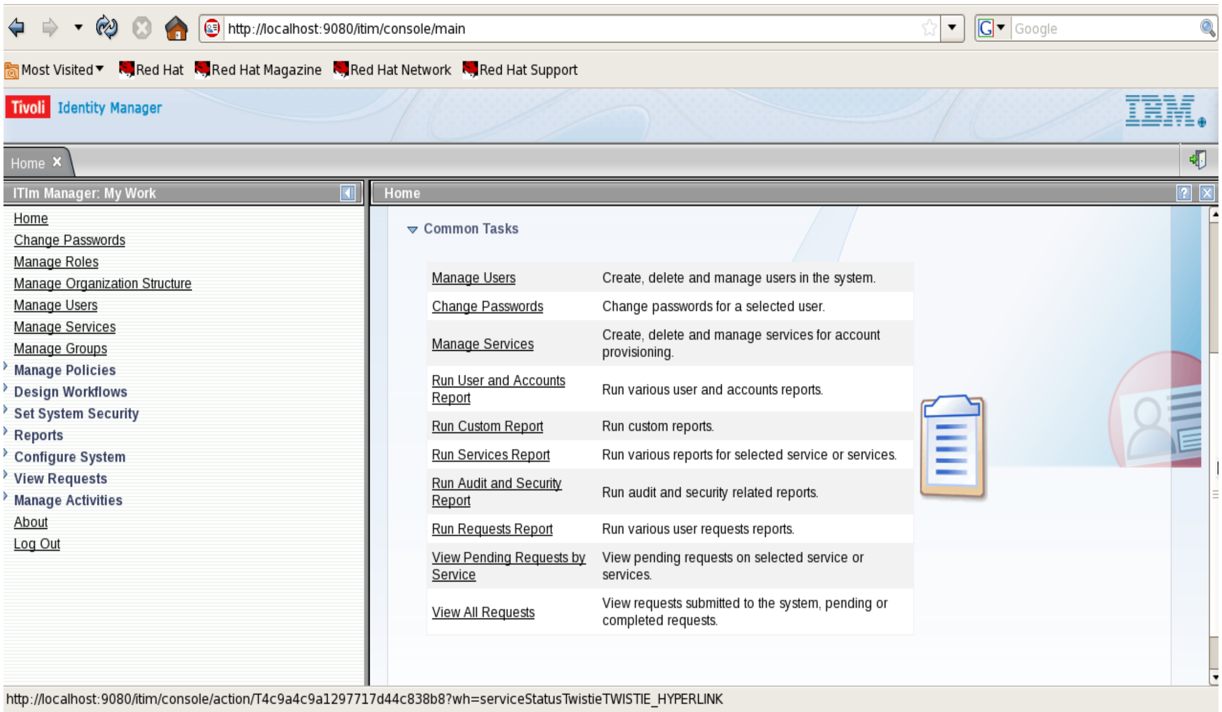
After successful installation of ITIM, there are certain commands which are used to make ITIM operational. As we have to provide provisioning for the user identities so we need to start the server and feed some identities in it so that they can be moved to Tivoli Access Manager Enterprise Single Sign On and log in through wallet to show how single sign on will work for employees.



```
[root@localhost ~]# su db2admin
[db2admin@localhost root]$ d2start
bash: d2start: command not found
[db2admin@localhost root]$ db2start
06/13/2012 13:40:30     0   0   SQL1063N  DB2START processing was successful.
SQL1063N  DB2START processing was successful.
[db2admin@localhost root]$ cd /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin
[db2admin@localhost bin]$ ./startServer.sh server1
ADMU0118E: The log file cannot be written to location
           /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/startServ
er.log;
           please specify a different location with -logfile
ADMU0128I: Starting tool with the AppSrv01 profile
ADMU3100I: Reading configuration for server: server1
```

Figure 4.1: Starting ITIM

Open the command prompt to run the commands highlighted above and type http://localhost:9080/itim/console in browser and login as ITIM Manager. After successful log in, a welcome screen appears shown below.

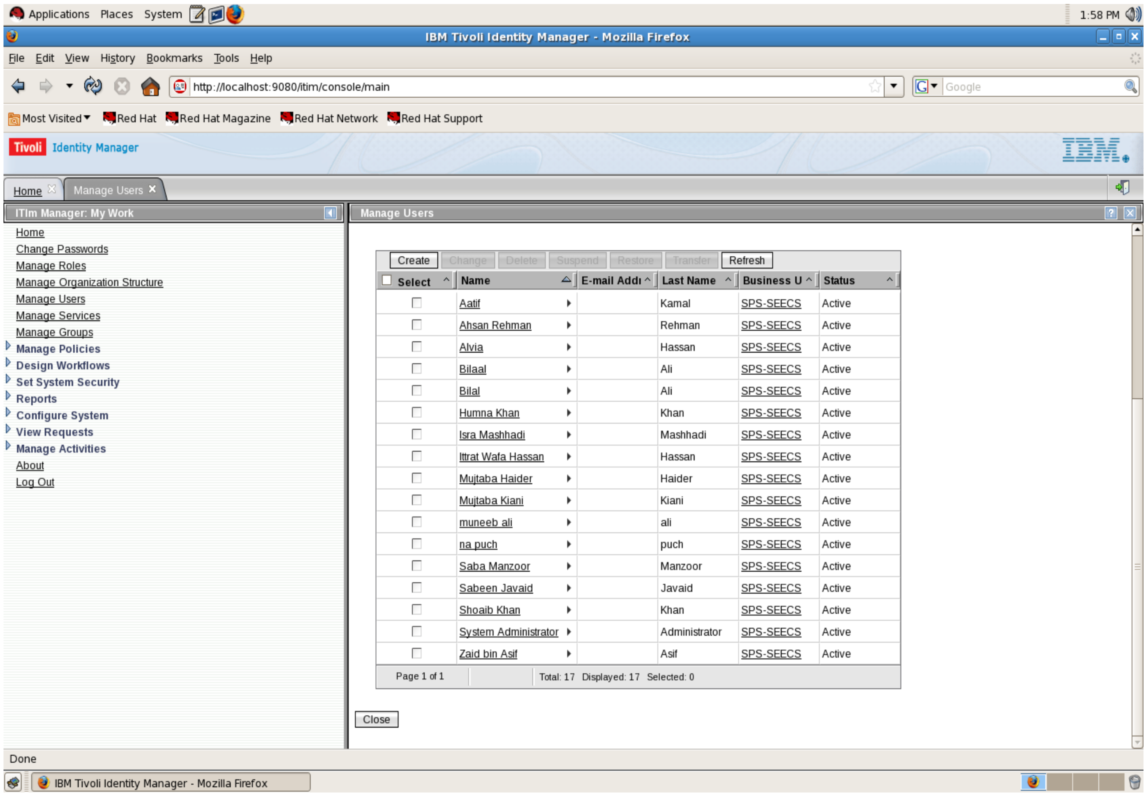


Manage Users	Create, delete and manage users in the system.
Change Passwords	Change passwords for a selected user.
Manage Services	Create, delete and manage services for account provisioning.
Run User and Accounts Report	Run various user and accounts reports.
Run Custom Report	Run custom reports.
Run Services Report	Run various reports for selected service or services.
Run Audit and Security Report	Run audit and security related reports.
Run Requests Report	Run various user requests reports.
View Pending Requests by Service	View pending requests on selected service or services.
View All Requests	View requests submitted to the system, pending or completed requests.

http://localhost:9080/itim/console/action/T4c9a4c9a1297717d44c838b8?wh=serviceStatusTwistieTWISTIE_HYPERLINK

Figure 4.2 Welcome Screen of ITIM

By identity feed import as much as accounts you want in your system and then provision these accounts with Tivoli Access Manager Single Sign On and log in wallet to prove that these users are successfully provisioned with TAM E-SSO as well. Identity feed may be Comma-Separated Value (CSV), DSML, AD OrganizationalPerson identity feed (Microsoft® Windows® Active Directory), INetOrgPerson (LDAP), IDI data feed.



□ Select	Name	E-mail Addı	Last Name	Business U	Status
□	Aatif		Kamal	SPS-SEECS	Active
□	Ahsan Rehman		Rehman	SPS-SEECS	Active
□	Alvia		Hassan	SPS-SEECS	Active
□	Bilaal		Ali	SPS-SEECS	Active
□	Bilal		Ali	SPS-SEECS	Active
□	Humna Khan		Khan	SPS-SEECS	Active
□	Isra Mashhadi		Mashhadi	SPS-SEECS	Active
□	Ittrat Wafa Hassan		Hassan	SPS-SEECS	Active
□	Mujtaba Haider		Haider	SPS-SEECS	Active
□	Mujtaba Kiani		Kiani	SPS-SEECS	Active
□	muneeb ali		ali	SPS-SEECS	Active
□	na puch		puch	SPS-SEECS	Active
□	Saba Manzoor		Manzoor	SPS-SEECS	Active
□	Sabeen Javaid		Javaid	SPS-SEECS	Active
□	Shoaib Khan		Khan	SPS-SEECS	Active
□	System Administrator		Administrator	SPS-SEECS	Active
□	Zaid bin Asif		Asif	SPS-SEECS	Active

Page 1 of 1 Total: 17 Displayed: 17 Selected: 0

Figure 4.3: ITIM Users

Now these users are also part of TAM E-SSO as well. They all have their wallet on client side managed by AccessAgent. Profiles are uploaded and synchronized with IMS server.

5.2 Administration of Tivoli Access Manager Enterprise Single Sign On

Users are added in TAM E-SSO server. The user in TAM E-SSO can manage their wallet, login options, security questions and all other credentials through AccessAgent.

These users added in TAM E-SSO can also log in trough their wallet and add applications to their wallet. Changes can be manually synchronized with IMS Server by user. If user does not synchronize manually, changes will automatically synchronize with IMS Server after almost 30 minutes. However this can be configured.

Once a user is logged into the AccessAgent, its status is as shown in tray bar.

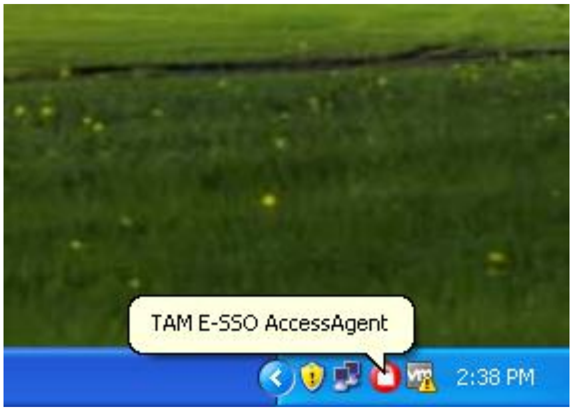
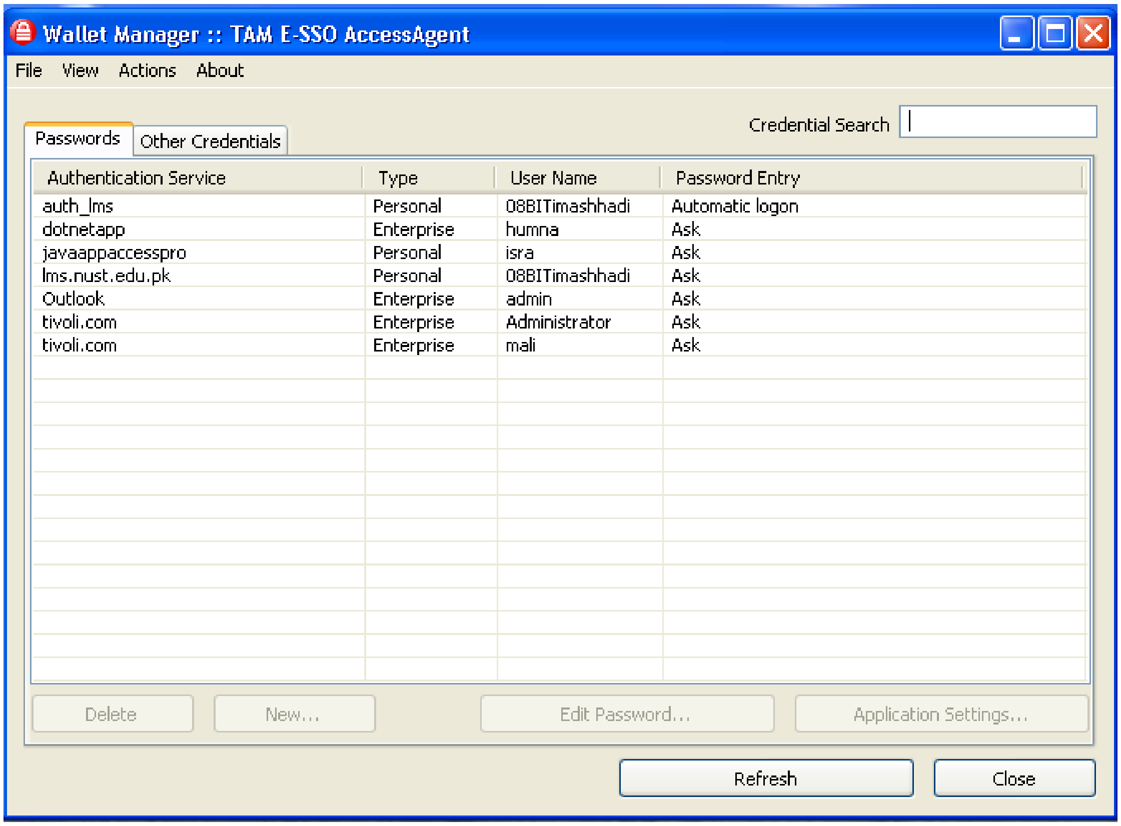


Figure 4.4: Status of AccessAgent

Wallet of the user shows applications that are added in it and their username. Password showing option is configurable which means that administrator can allow the users to see his user name with password or not.



Authentication Service	Type	User Name	Password Entry
auth_lms	Personal	08BITimashhadi	Automatic logon
dotnetapp	Enterprise	humna	Ask
javaappaccesspro	Personal	isra	Ask
lms.nust.edu.pk	Personal	08BITimashhadi	Ask
Outlook	Enterprise	admin	Ask
tivoli.com	Enterprise	Administrator	Ask
tivoli.com	Enterprise	mali	Ask

Figure 4.5: Wallet of a User

More applications can also be added in the wallet manually by ‘New’ button and they can be removed by using ‘Delete’ button if required. Passwords are also configurable.

Administrator can also add applications in the wallet of the users without asking users. As the applications used by the users and added by the administrator can be confidential and Organization does not want to share the passwords of the applications with the users so users have to use these applications without knowing usernames and passwords for those applications.

5.3 Domain Users

Like ITIM provision users in TAM E-SSO, one of the services in ITIM can also provision the users with Active Directory (AD) as well. It means that Domain users are ready in Active Directory with the same User ID and Password to log on to their windows account. These users can log on to their windows accounts and can do their work without creating an account in AD separately.

For the above mentioned purpose we need to import **ADProfile.jar** file in ITIM and a service is created in ITIM for AD. After importing ADProfile.jar and creating service for AD in ITIM, AD can easily communicate and user accounts can be provisioned more efficiently and securely.

Chapter No. 5

DISCUSSION

This chapter provides the overview of whole project and the way it was carried out throughout the process and the challenges faced.

Every organization that deploys IT infrastructure has privileged users are given special administrative right to manage the important and critical resources e.g. databases, operating systems and many other applications of an organization. These privileged users can be accountants, managers, executives. These privileged user identities are shared by a pool of user who uses these identities to access the resources. This can cause accountability and compliance issue and can increase the risk of sabotage and data theft. The purpose of our project is to provide access to resources without sharing with the username password credential.

Problem Statement: "Implementation of the privileged user ID concept to manage SEECS lab users and allow them to access lab login protected machines or software without sharing with them the user id and password."

In our project, we used IBM Tivoli Identity Manager and IBM Tivoli Access Manager-ESSO to resolve the above problem. We used the Tivoli Identity Manager to provision user into Tivoli Access Manager which were stored in Active Directory. Tivoli Access Manager is used to provide access to different resources through single sign-on. The user id and password for a certain resource are injected in the wallet of a specific user. Now when he/she wants to access the resource, the resource automatically logs in using the user id/password stored in the wallet.

For the successful deployment of our project, it was necessary to have detail understanding of the all the above mentioned products. So the first phase of our project was to conduct background study of Tivoli Identity Manager, Tivoli Access Manager and Active Directory which was later on included as the literature review. The outcome of the background study was:

- Understanding the purpose and architecture of Tivoli Identity Manager and its component in our project.
- Understanding the purpose and architecture of Tivoli Access Manager-ESSO and it components in our project.
- Understanding life cycle management of an identity and its roles and accesses for an organization.

- Understanding how privileged identities affect the security of an organization.
- Identifying the problems with sharing the user id and passwords.
- Understanding the concept of single sign-on, wallets and profiles.
- Understanding the business value of our projects and IBM products.

The second phase of our project was to deploy the above mentioned software's according to our SEECS lab environment. The Tivoli Identity Manager was deployed on Redhat 5.1 while Tivoli Access Manager was deployed on Windows Server 2003. While deploying the above software's, we had to keep in mind the compatibility issues and take certain precautions. While deploying each component, we had to keep backups due to load shedding as sudden shut down of a system corrupted the software's.

The third phase of our project was to integrated these software's and create a solution architecture proposed by us for solving the problem of privileged user identities management.

5.1 Challenges:

The domain is not new but we did not have much help on a lot of issues related which we sorted out ourselves by experimenting and some basic knowledge of the software's.

- Network Connection Issues: Identities were managed and used by different server on different machines running different operating systems. Tivoli Identity Manager, Tivoli Access Manager and Active Directory were to communicate to each other by creating SSL connection. For establishing a connection, we had to configure the telnet between two machines. At the same, we had to configure our DNS server for adding different client machines to our domain and for access agent to access the IMS Server. The dynamic IP address changes when the computer starts or when system shuts down suddenly. It caused the problem as both servers were configured on IP addresses and every time the system started, we had to configure the servers according to the new IP address assigned. In the end, we sorted out the problem, we assigning static IP's to all our servers and client machines.
- Lack of helping Material: Although guides are available for the installation and integration of Tivoli Access manager and Tivoli Identity Manager but these guides were brief and had general steps. We had to configure all the software according to our environment ourselves. Although sometimes we use to get help from the IBM forums.

Chapter No.6

CONCLUSION

This chapter describes the final output and achievements of the project.

Through the successful implementation of our project, we are able to manage and audit a pool of privileged user ids. This is done by integrating the Tivoli Identity Manager, Active Directory and Tivoli Access Manager ESSO. The user is provided access to a resource by injecting username password for that resource into the TAM-ESSO account wallet of the user. As along the user needs to access the resource the credentials will be available in his/her wallet. And when the user no longer needs to access the resource, the username password will be removed the person's wallet. Consider a student at NUST-SEECS who has username/password to access LMS. Now when the same student becomes a teacher assistant, he/she needs to access the teacher's account to manage grades, assignments etc. Now with our project, the teacher will automatically inject the username password into the student's wallet and does not have to share the password with the student. The student, on the other hand, can access the teacher's account without knowing the password. The wallet of the student stores two login credentials for LMS. The student can access both the accounts whenever he wants to. Now user can access the resources without manually entering username password. The user now does not need to know the passwords for accessing. This secures the privileged user identities of an organization.

Chapter No. 7

RECOMMENDATIONS

This chapter is all about future work that can be added to that system to make it more precise and user friendly for employees. If in SEECS there is someone to extend the work and provide a better solution we have some recommendation that can be followed to make it more precise and according to the user requirements. Thus, after knowing the business value and demand of the suite, the time is inevitable when this would become the need of every organization, wishing to secure the access to its resources and to automate the user but most of all providing them single sign on for easy log in and logout of numerous applications.

Before recommendations it would be better talk about successes that we have at the end of the project. We have successfully deployed and Administered Tivoli Identity Manager and Tivoli Access manager Enterprise Single Sign On on Linux Red Hat 5.1 and Windows Server 20003 respectively. We have successfully integrated ITIM with TAM E-SSO and ITIM with AD. We have successfully created and imported users for ITIM into TAM E-SSO, and provisioned those users by adding the credentials for specific applications in the user's wallet.

Let's look at the recommendations if these things are included in the system it will make the solution more precise and accurate.

8.1 Integration of RFID

By RFID implementation its security and the login process improve that is warmly acceptable by any employee. One is not needed to enter any username or password and can get into the application by just swapping the RFID card on reader.

8.2 Implementation for Lab/PC's

This project is also extendible I one can implement a scenario that once an employee enters in a lab or office swaps his RFID and his PC plus all the applications in the wallet are logged in. In this way once he leaves or moves about 5 meters away from the reader his AccessAgent gets locked along with all the application that he was using. In this way a better solution for security and easiness can be provided to employees using 5 to 30 applications.

REFERENCES

1. Axel Buecker, D. F. (2009). Identity Management Design Guide with Tivoli Identity Manager 5.0. Armonk, USA: IBM.
2. Muhammad Sohail's Installation Guide for Tivoli Access Manager 8.1 Installation guide SPS Islamabad, Pakistan.
3. IBM Tivoli Access Manager 8.1 TAM-ESSO Adapter Guide retrieved from inside the Adapter Software.
4. IBM RMI Dispatcher Guide retrieved from inside the dispatcher software.
5. TAMESSO_ProfileCookbook 2.2. Retrieved from IBM publib website.
6. IBM publib Website:

   http://publib.boulder.ibm.com/infocenter/iseries/v6r1m0/index.jsp

7. IBM DeveloperWorks Forum:

   www.ibm.com/developerworks/web/