Identity Lifecycle Management

Business Need
Organizations today are confronted with a number of identity and access challenges that ILM can help address. Chief among these are:

• Complexity of managing identities across several systems.
• The high cost and risk of provisioning and de-provisioning user accounts and access permissions.
• The risk to the business of operating with weak credentials.
• Help desk costs associated with password resets and smart card deployment.

These challenges impair business productivity and often result in higher complexity and cost for IT, lost productivity for the business user, and increased risk for the business.

Solution Overview
ILM 2007 is a solution that builds on the metadirectory and user provisioning capabilities in Microsoft Identity Integration Server 2003 (MIIS 2003) and adds new capabilities for managing strong credentials such as smart cards, providing an integrated approach that pulls together metadirectory, digital certificate and password management, and user provisioning across Windows® and other enterprise systems.

ILM 2007 simplifies the process of synchronizing and managing identity records from disparate data repositories, and prevents anomalies, such as active records for employees who have left the organization.

ILM 2007 provides IT with a policy framework to control and track the identity and access data that helps manage compliance. It also includes self-help tools for end users, enabling IT to improve efficiency by securely delegating many tasks to end users.

Another key feature of ILM is that it includes a Windows-based digital certificate management solution that integrates with the Windows Server™ 2003 operating system and Active Directory® to provide a turnkey solution for managing the end-to-end life cycle of smart cards and digital certificates.

The advanced ILM smart card management functionality uses a client-side Web module that provides the following features:

• Complete personal identification number (PIN) management features for user PINs and unblocking PINs.
• Complete reporting and auditability of all smart card life cycle activities.
• A smart card inventory system that updates upon activation of a smart card, simplifying initial distribution of cards.
Benefits

Simplifies Identity and Access management by:

• Keeping identity information synchronized and consistent across a wide range of directories, databases, and proprietary identity systems.
• Providing a single place for IT and end users to manage the life cycle of enterprise credentials from passwords to strong credentials such as certificates and smart cards.
• Integrating with Active Directory, other Microsoft servers such as Microsoft SQL Server for reporting, Microsoft System Management Server for asset and software management, and Microsoft Operations Manager for health monitoring.

Gives IT greater control by:

• Providing a best-in-class metadirectory engine, giving IT control and visibility over identity clean-up, synchronization, and reconciliation processes.
• Providing IT a robust, policy-based management solution for controlling and helping secure resources.
• Giving IT the tools to provide the control framework that allows them to effectively govern end users’ and business owners’ usage of self-service tools.

Offers flexible system that:

• Provides 30+ connectors out of the box to allow for integration into other enterprise systems.
• Offers extensibility to develop additional connectors.
• Delivers a platform that can be customized as needed by IT or ISV/SI partners, with a vast set of third-party solutions available.

How ILM 2007 Works

Identity Lifecycle Management

ILM manages identity information across multiple stores by aggregating this information in a central repository called the metaverse. Management agents serve as connectors that translate data from these connected stores to the metaverse. For example, the e-mail system can be linked to its HR database through the metaverse. When an employee joining the organization is added to the HR database, ILM can automatically provision that employee to the e-mail system. Each employee’s attributes, from the e-mail system and the HR database, are imported into the connector space through management agents. The e-mail system can then use individual attributes, from the employee entry that originated in the HR database, such as the employee telephone number. If an employee’s telephone number changes in the HR database, the new number will automatically be propagated to the e-mail system.

Certificate Management

ILM also provides sophisticated credential management features to Windows Server 2003 Certificate Authorities (CA) by acting as an administrative proxy. Once installed within an organization, all digital certificate and smart card management functions pass through ILM.

The certificate management solution in ILM consists of three components:

1) Server component: Provides a Web interface and is the focal point of administrative functions.
2) Certificate Authority plug-in: Communicates with the server, controls the behavior of the CA(s), and provides rich logging and auditing in a central location.
3) Client-side components:
   • Smart Card Self Service Control, which provides certificate management capabilities.
   • Smart Card Personalization Control, which provides Java card management.
   • Bulk Smart Card Issuance Tool, which is an application for centralized large scale smart card deployment scenarios.

Server System Requirements

Computer and processor: Pentium III or faster processor; Pentium IV recommended; 1 GHz or faster processor recommended
Memory: 1 GB or more of RAM; 2 GB of RAM recommended
Hard disk: 8 GB of available hard-disk space on an NTFS partition
Drive: CD-ROM drive
Display: Super VGA monitor; XGA recommended
Operating system: Windows Server 2003, Enterprise Edition or Datacenter Edition Service Pack 1 (SP1) or Service Pack 2 (SP2) for certificate management; certificate management requires Windows Server 2003 Certificate Services

Client System Requirements for Certificate Management

Operating system: Windows XP or Windows 2000 Service Pack 4 (SP4)
Browser: Microsoft Internet Explorer 6 or 7

Additional Resources

www.microsoft.com/ILM