

INSIGHT

Microsoft Identity Lifecycle Manager: Moving Beyond MIIS with Software to Automate and Simplify Workflow Processes, Synchronize Identities, and Manage Strong Authentication

Sally Hudson

IDC OPINION

Microsoft recently released Information Lifecycle Manager 2007 (ILM 2007). The software, which is an extension of Migration Identity Integration Server (MIIS), includes a workflow- and policy-based solution that enables organizations to manage the life cycle of digital certificates and smart cards. It is designed to significantly lower the costs associated with digital certificates and smart cards by enabling organizations to more efficiently deploy, manage, and maintain a certificate-based infrastructure. ILM 2007 is designed to help organizations:

- Simplify and automate the employee provisioning/deprovisioning process
 - Reduce the overall cost of system integration by providing a single platform for both identity workflow management and strong authentication
 - Extend and maximize their investment in Active Directory (AD)
-

IN THIS INSIGHT

This IDC Insight looks at Microsoft's recently announced Identity Lifecycle Manager 2007. The product builds on the functionality of MIIS 2003 by integrating the metadirectory and user provisioning features of MIIS 2003 with a management solution for strong credentials. This is designed to make ILM a strong platform for managing the entire identity life cycle of users and credentials in a straightforward, cost-effective manner. This Insight examines this announcement in the context of technology trends and customer needs in the identity and access management (IAM) market.

SITUATION OVERVIEW

IDC defines identity and access management as a comprehensive set of solutions used to identify users in a system (employees, customers, contractors, and so on) and to control their access to resources within that system by associating user rights and restrictions with the established identity. These solutions include Web SSO, federation, host SSO, user provisioning, advanced authentication, legacy authorization, public key infrastructure (PKI), and traditional hardware and USB token

technologies. Directory services function as a critical foundation underpinning an organization's identity and access management infrastructure.

Microsoft's IAM/MIIIS technologies fall within the area of the Active Directory software infrastructure platform and, as such, have enormous potential for customer adoption. ILM 2007 builds on the existing metadirectory and user provisioning capabilities in MIIIS 2003. New features include management of strong credentials such as smart cards and integration for metadirectory, digital certificate, password management, and user provisioning across Windows and other enterprise systems.

ILM 2007 brings together three key features:

- ☒ **Identity synchronization.** The software synchronizes user accounts and attributes in all of those systems, including synchronization of passwords. Directory synchronization saves time and money that is currently spent on keeping data consistent and enforcing data ownership rules.
- ☒ **User provisioning.** This feature allows the automatic creation of user accounts, mailboxes, and other identity information in target systems in real time. This allows IT and HR managers to provision new employees and allow them to be productive immediately. These capabilities also ensure that corporate resource access is instantly revoked for employees who leave the organization, which increases security and helps companies meet compliance regulations.
- ☒ **Certificate management.** Certificate Lifecycle Manager (CLM) is a policy- and workflow-driven technology that helps organizations manage the life cycle of digital certificates and smart cards. This technology is being released as a key component of ILM 2007. The technology has its roots in Alacris, the original developers of idNexus, which was acquired by Microsoft in late 2005. The product was subsequently rechristened Microsoft CLM and has now been integrated with Microsoft ILM 2007 to provide smart card and certificate life-cycle management.

ILM 2007 includes a workflow- and policy-based solution that enables organizations to manage the life cycle of digital certificates and smart cards. It is designed to significantly lower the costs associated with digital certificates and smart cards by enabling organizations to more efficiently deploy, manage, and maintain a certificate-based infrastructure.

IDC believes that technology that serves to streamline the provisioning, configuration, and management of digital certificates and smart cards for IT users will significantly accelerate the adoption of smart card technology over the next several years. In the past, the expertise required for integration and management of these functions limited implementations of smart cards and digital certificates to very large corporations and government organizations.

Microsoft has partnered with industry heavyweights in the smart card arena. For example, Gemalto, a world leader in smart card security, has integrated its .NET digital security solution with Microsoft ILM 2007. The Gemalto .NET cards make digital interactions more convenient and secure for people and organizations. ILM 2007 manages credentials and security-related information directly within the

Gemalto .NET card, which in turn works seamlessly in the Microsoft ILM 2007 architecture to replace weak username/password security with strong, device-based authentication.

Microsoft has included many large enterprise customers in its Technology Adoption Program for ILM. This program differs from a beta program in that it focuses on a small number of select enterprise organizations utilizing ILM technology. These organizations include several large pharmaceutical companies, an auto manufacturer, an investment bank, a defense manufacturer, a major insurer, and a major systems integrator (SI) with 120,000 seats. According to Microsoft, all of these organizations have deployed some of ILM in production model.

ILM is positioned to embrace the concept of enterprise integration from the outset, and, in addition to Microsoft-specific platform connectors, the vendor is including the following heterogeneous connectors in the box:

- IBM Tivoli Directory Server
- Novell eDirectory 8.6.2, 8.7, and 8.7.x
- Sun Directory Server (Netscape/iPlanet/SunONE) 4.x and 5.x
- IBM Resource Access Control Facility
- CA eTrust ACF2 and eTrust Top Secret
- Lotus Notes 6.x, 5.0, and 4.6
- SAP 5.0 and 4.7
- Telephone switches
- XML-based systems
- DSML-based systems
- IBM DB2 Oracle 10g, 9i, and 8i
- Directory Services Markup Language (DSML) 2.0
- LDAP Interchange Format (LDIF)

The vendor also provides an Extensible Management Agent for connectivity to all other systems.

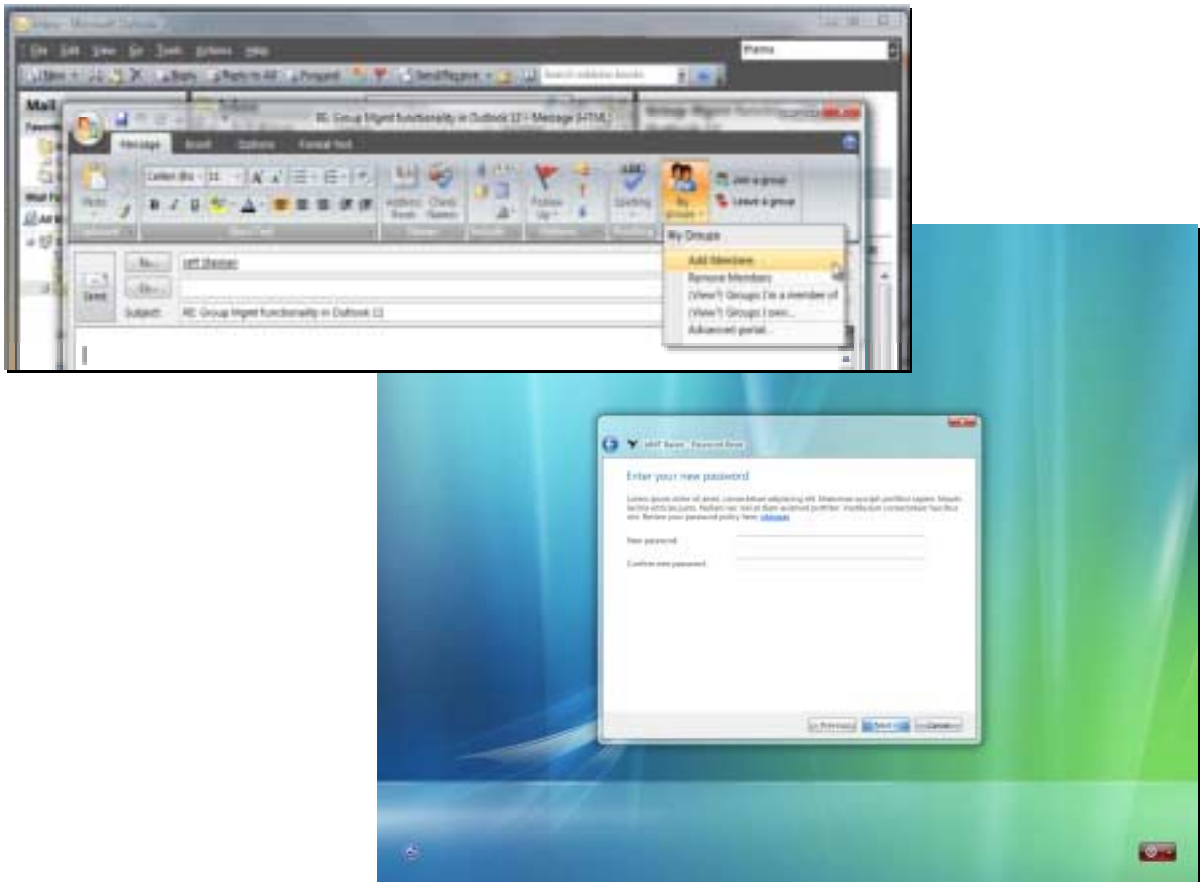
ILM 2007's full retail price is \$15,000 per server and \$25 per user client access license (CAL). A customer must acquire and assign a user CAL for each person for whom Identity Lifecycle Manager 2007 issues or manages one or more digital certificates. Otherwise, customers do not need user CALs only to access instances of the server software.

FUTURE OUTLOOK

Although the initial version of ILM 2007, as outlined above, streamlines and enhances the metadirectory, user provisioning, and CLM functionality, Microsoft has also announced that version 2 of ILM will be released in 2H07. According to the vendor, the next release will further refine and extend the identity management capabilities of AD. The focus is to provide more tools for IT managers to manage their current IT investments. Version 2 will include additional functionality in the areas of user management, access and credential management, and policy management. These areas will be aligned with an eye toward enforcement and auditing and will be implemented on a common platform. Version 2 will include WS-based APIs to make the software appealing from a programming perspective (see Figure 1).

FIGURE 1

ILM 2 Office and Windows Integration Examples



Source: Microsoft, 2007

The ultimate goal will be to deliver a rich workflow environment for Windows Workflow Engine, Server 2003, XP, Longhorn, and Vista — similar to the workflow found in Microsoft Office products today.

For the ILM 2 release, group and distribution list responsibilities can be delegated to designated end users, when appropriate. This is designed to enhance the self-service experience for end users in an office environment while reducing unnecessary tasks and headaches for the IT admin staff. Of course, IT administrators, in conjunction with human resources and management personnel, will determine just who within a corporation will have these access and distribution list privileges.

IDC believes that these announcements underscore and reinforce Microsoft's presence in the identity management market as they will allow customers to more easily and cost-effectively extend the capabilities of AD/MIIS into the next level of IAM. They should serve as a foundation to link the Microsoft identity platforms more firmly within existing enterprise environments as a functional component of seamless, end-to-end, manageable, and enforceable identity infrastructures. In addition, this technology should appeal to small and medium-sized business (SMB) organizations. Research shows that the SMB segment of the market typically encounters several stumbling blocks when implementing identity and access management technologies. Among these obstacles is the lack of IT staff, specific expertise, and resources sufficient to monitor and manage rapidly changing business processes while meeting regulatory compliance demands. The features and functions in ILM should help SMBs, especially those with a reliance on Active Directory, cross the IAM threshold.

By delivering a software platform that automatically synchronizes identities and manages multifactor authentication, Microsoft hopes to create a life-cycle management environment that will allow users to create a workable identity management discipline within their organizations.

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2007 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Published Under Services: Security Services and Identity Management