Certificate and Smart Card Management with Microsoft Identity Lifecycle Manager 2007

Microsoft Corporation

Published: January 2009

Abstract

This paper provides an overview of the business imperatives and Microsoft’s strategy for certificate and smart card management, with a focus on the benefits delivered through Microsoft Identity Lifecycle Manager 2007.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

 © 2009 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Server, Windows Vista, SQL Server, Office, Outlook, Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[Executive Summary 4](#_Toc205905057)

[Introduction 5](#_Toc205905058)

[Business Drivers for Strong Authentication 6](#_Toc205905059)

[Compliance 6](#_Toc205905060)

[Operational Efficiency 6](#_Toc205905061)

[IT Security 6](#_Toc205905062)

[Business Enablement 6](#_Toc205905063)

[Microsoft’s Certificate and Smart Card Management Approach 8](#_Toc205905064)

[Microsoft Identity Lifecycle Manager 2007 9](#_Toc205905065)

[Providing an Integrated Identity Lifecycle Management Solution 9](#_Toc205905066)

[Flexibility to Meet Organizations’ Unique Requirements 9](#_Toc205905067)

[Leveraging New Technologies as They Evolve 9](#_Toc205905068)

[Addressing the Business Drivers for Strong Authentication 10](#_Toc205905069)

[Conclusion 11](#_Toc205905070)

# Executive Summary

Increased pressure to provide trusted access to business assets and compliance with a range of regulatory requirements – combined with the distributed nature of business in today’s global economy – has made identity and access management one of the most critical IT security initiatives in enterprises today. Implementing stronger authentication solutions is a critical step in effectively addressing the identity assurance imperative.

User names and passwords have been around since the beginning of enterprise computing and are pervasive based on their simplicity. However, there are a range of business issues that are now driving enterprise organizations to recognize that a traditional user name/password approach is no longer sufficient to provide trusted access to sensitive business information. At the same time, the strategic value of IT environments is increasing and therefore driving enterprises to consider deploying stronger authentication technologies across a range of corporate applications and user scenarios.

The use of digital certificates and smart cards provide an excellent approach to deploying strong (multi-factor) authentication solutions across the enterprise. Digital certificates are commonly used as a second factor authenticator in a wide range of applications and user scenarios including user authentication, data encryption and digital signatures. Smart cards provide a highly portable and secure way to store digital certificates and cryptographic keys in a manner that is tightly bound to a user’s digital identity.

Though digital certificates and smart cards provide additional benefits and flexibility to support a range of strong authentication scenarios, the use of these technologies inherently requires a robust management system with rich workflows and the flexibility to meet a wide range of organizational requirements. Further, these technologies need to be deployed in a manner that is integrated with an organization’s overall user provisioning and identity management process.

Microsoft Identity Lifecycle Manager (ILM) 2007 provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. ILM 2007 provides identity synchronization, certificate and smart card management, password management and user provisioning in a single solution that works across Microsoft Windows and other organizational systems.

This document provides a closer look at the key business drivers motivating enterprise organizations to deploy strong authentication, Microsoft’s vision to helping enterprises address the broader identity assurance challenge and the benefits of using ILM 2007.

# Introduction

In today’s global economy, organizations are increasingly challenged to deploy enterprise IT security solutions that protect sensitive business information, assure digital identity and build trusted relationships with business partners, employees and customers.

Enterprises must deal with many issues related to digital identity. These include securing the enterprise by ensuring that users are appropriately authenticated, and then effectively synchronizing and managing those user identities through the entire identity lifecycle, in compliance with internal and external regulations. All of these challenges are complex but also closely related. Much of the complexity can be tied back to the fact that enterprises have many identity systems within their applications. Multiple, siloed identity systems all need to be tracked for compliance reasons and typically rely on a number of separate management components. The fact that enterprises have many disparate identity components and management systems is at the heart of the broader identity and access management challenge.

Implementing stronger authentication within the enterprise is a critical step in managing identities and represents value not only in its ability to provide more secure user access but in its ability to consolidate identity. Consolidated identity in turn has benefits for end users and for ongoing identity and credential lifecycle management in terms of improving operational efficiency. The value proposition for organizations to implement strong authentication is becoming stronger every day as the solutions improve and become more cost effective.

Once an enterprise invests in strong authentication, they are highly motivated to have all of their applications leverage the investment to the fullest degree possible. This is both to maximize the return on their investment in strong authentication but also for the intrinsic security benefits of strong authentication. This in turn sets up a dynamic that will encourage application vendors to increasingly leverage strong credentials as the means of authenticating to their applications with the net result of unifying enterprise identity, further increasing the value of strong authentication.

Even without the broader context of providing consolidation to enterprise identity management, there are many business drivers that are motivating organizations to consider and implement strong authentication solutions. A closer look at these business drivers is provided in the next section of this document.

# Business Drivers for Strong Authentication

The fundamental issue behind many of the business drivers for strong authentication is a recognition by a growing number of organizations that traditional user name/password based systems are simply not secure enough for an increasing number of enterprise environments. Attempts to increase the security of password-based systems usually involve increasing password complexity, which in turn increases costs to the organization in lost user productivity and the cost of help desk and support systems to handle more complex passwords. At the same time, total cost of ownership associated with strong authentication solutions is dropping and the functionality of the solutions is increasing. This trend is likely to continue making strong authentication more prevalent and more cost effective moving forward.

Implementing stronger authentication solutions is a critical step in the process of enterprises providing trusted access to corporate applications and sensitive business information. The key business drivers motivating enterprise organizations to consider and deploy stronger authentication solutions are primarily related to the four areas outlined below.

## Compliance

Compliance with a range of industry and/or government regulatory requirements continues to be a considerable driver for the deployment of strong authentication. Organizations need more assurance around the issuance and use of identity information in accordance with corporate IT security policies –particularly those that perform critical corporate functions. Organizations also need auditable processes for granting access privileges to business assets.

## Operational Efficiency

Enterprise IT organizations face increasing pressure to reduce the costs and risks associated with provisioning user identities across many disparate corporate applications. Organizations need an integrated management system that integrates the process of provisioning and de-provisioning digital identities, the issuance of associated authentication credentials and common management functions through the entire lifecycle of the digital identity. Organizations also need to provide greater end user self-service capabilities in accordance with corporate policy which in turn will help reduce the help desk burden to support user access and/or entitlement changes.

## IT Security

Enhanced IT security is still one of the biggest business drivers for the deployment of strong authentication. As organizations put more intellectual property into their corporate applications and distribute their identity information by opening their networks more and more to external users, the need for stronger user authentication is increasing. Organizations are moving to stronger techniques that include digital certificates and smart cards. As a result IT organizations need a single, integrated management system that will help consolidate and simplify the deployment of strong (multi-factor) authentication technologies across the enterprise.

## Business Enablement

Lastly, once an organization has the ability to perform strong user authentication or digital signatures, new business possibilities begin to arise. These opportunities are based on the fact that the organization has an identity system that establishes trust with employees and customers, which makes the organization willing to do more with their IT environments with fewer risks or concerns. Digital certificates also enable organizations to implement stronger trust relationships with partners that can improve and increase collaboration and therefore new business opportunities.

# Microsoft’s Certificate and Smart Card Management Approach

Microsoft has approached the broader identity management challenge with a vision that an enterprise identity has many attributes which all need to be managed. This includes provisioning those identities into any application that requires knowledge of the user, but also includes other attributes of the user like digital certificates.

Certificates are an important component of an identity management implementation. Certificates are an ideal authentication solution in a wide variety of situations because they are difficult to forge and are a mature technology. Commonly, certificates are used as a second factor authenticator for users (with or without smart cards), but they can also be used to authenticate devices such as Web servers, workstations, networking devices and many others. Most new applications today that require some form of strong authentication will use certificates as the foundation of that functionality.

This concept is a key element behind the design of the certificate and smart card management capabilities in ILM 2007, which provides a robust certificate management capability to address these scenarios. This management functionality has many components including enrollment, key escrow, certificate recovery, revocation, and reporting. ILM 2007 implements all of these features in a simple web-based interface that is configurable and flexible. The result is a full-featured certificate management capability that delivers the value of certificates without the management complexity.

Certificates can be stored on a computer, or for more security can also be stored on a smart card. The benefit of the smart card is it can provide better portability of the certificate and also better protection of the cryptographic keys. These two benefits come at the price of more complexity due to the management requirements of the smart card. ILM 2007 addresses this management challenge by providing rich management functionality for the smart card that makes it easier to manage these complex details.

# Microsoft Identity Lifecycle Manager 2007

Microsoft Identity Lifecycle Manager 2007 provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. ILM 2007 provides identity synchronization, certificate and smart card management, password management and user provisioning in a single solution that works across Microsoft Windows and other organizational systems.

Microsoft Identity Lifecycle Manager (ILM) 2007 provides a critical component in an enterprise’s evolution to stronger authentication. The certificate and smart card management features within ILM 2007 take a holistic view of strong authentication and tackle the most important aspects of a successful long-term solution. These include:

## Providing an Integrated Identity Lifecycle Management Solution

ILM 2007 provides organizations an integrated identity lifecycle management solution rather than another ‘stove-piped’ technology. ILM 2007 provides IT administrators an integrated user provisioning and credential management experience throughout the entire lifecycle of the user’s identity. Identity is increasingly becoming one of the most central and critical IT infrastructure components. As a result, it is increasingly important that certificate and smart card management features are tightly integrated with the rest of the organization’s IT environment. ILM 2007 does this by being tightly integrated with Active Directory (AD) and using AD user information, permissions and group information. This eliminates the need to create a separate collection of users, permissions and groups and the associated additional management overhead.

## Flexibility to Meet Organizations’ Unique Requirements

Every organization is unique and as a result, their identity and credential management system requirements will in turn be unique. Organizations vary based on size, geographic distribution and security requirements, as just a few relevant examples. Each of these elements will have an impact on how the organization manages their certificates and smart cards. This might include centralized management, or highly distributed management. It could also include self-service scenarios or multiple approvals. The key point is the management system needs to be flexible to support these capabilities without requiring customized development. ILM 2007 provides that flexibility and can be easily configured to use different workflows and approaches as an organization plans and continues to evolve their deployment.

## Leveraging New Technologies as They Evolve

ILM 2007 provides a hardware-independent solution that has the flexibility to adapt to new technologies as they become broadly available. Smart card hardware is evolving to include larger capacity storage, new smart card operating systems and generally new on-card features and applications. This innovation should occur independently of the management system, so the management system should have a generic and standardized approach to communicating with the cards. ILM 2007 is able to do this using a standardized interface to the smart card called the Microsoft Base CSP (Cryptographic Service Provider) and mini-drivers. Most major smart card vendors support mini-drivers and therefore ILM provides easy-to-implement hardware independence. This in turn provides significant value to enterprise organizations by enabling them to select the right strong authentication technology and vendor that best meets the unique requirements of the business -- both today and in the future.

## Addressing the Business Drivers for Strong Authentication

Deploying strong authentication solutions using digital certificates, smart cards and Microsoft ILM 2007 helps enterprise organizations to address the key business drivers for strong authentication – as outlined earlier in this document – and achieve their identity assurance business objectives.

**Compliance**

An increasingly popular approach to addressing identity assurance compliance requirements is to deploy digital certificate technology in combination with smart cards. The smart card and the associated management process that are delivered by Microsoft ILM 2007 provide better transparency into who has strong authentication devices, and of course the devices themselves provide better protection in terms of who can authenticate to corporate resources. ILM 2007 provides provisioning services and management processes that can be implemented and audited in relation to corporate security policy and compliance requirements.

**Operational Efficiency**

Deploying smart cards and/or certificate-based credentials within an integrated user provisioning experience provided by ILM 2007 can help IT organizations drive greater operational efficiency. ILM 2007 provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. Additionally, ILM 2007 includes self service certificate and smart card management features that can further reduce cost and overall efficiency by empowering the user and reducing help desk calls.

**IT Security**

Organizations are starting to plan beyond user names and passwords to stronger techniques that include digital certificates and smart cards. Digital certificates and smart cards provide an excellent approach to deploying stronger authentication solutions. However, these benefits do come at a price of additional complexity due to the issuance and lifecycle management requirements associated with these technologies. ILM 2007 simplifies the deployment and lifecycle management of strong (multi-factor) authentication technologies such as certificates and smart cards in a manner that leverages an organization’s existing IT infrastructure.

**Business Enablement**

Digital certificates enable organizations to implement stronger trust relationships with partners that can improve and increase collaboration and therefore new business opportunities. Deploying strong authentication solutions with integrated management systems such as ILM 2007 also enables organizations to leverage new technologies as they evolve over time – which in turn presents opportunities to drive new customer innovation. Organizations that are able to effectively deploy strong authentication in a more integrated and automated approach also free up valuable IT resources that are then able to focus on high value business activities.

# Conclusion

Organizational IT requirements are becoming more demanding with respect to security and compliance, and are driving scenarios for more effective identity and credential management. Implementing a strong authentication infrastructure using digital certificates and smart cards is a good response to those evolving requirements. Certificates and smart cards represent a mature and trusted set of technologies for delivering strong authentication. Microsoft ILM 2007 provides a rich set of tools and technologies to manage those credentials effectively. The combination of ILM 2007, certificates and smart cards provides organizations with well managed strong authentication that is also flexible and powerful to address a wide range of scenarios and requirements.

Microsoft ILM 2007 provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. The key capabilities provided by ILM 2007 include:

* A single administration point for digital certificates and smart cards
* The ability to support user self-service capabilities
* Configurable policy-based workflows for common tasks
* Detailed auditing and reporting capabilities
* Support for centralized, de-centralized and self-service scenarios
* Extensibility to support additional strong authentication technologies including one-time password (OTP) devices, physical access cards and biometrics
* Tight integration with Microsoft Certificate Services and Active Directory environments

The key business benefits of using an ILM 2007 based solutions approach include:

* Enhancing IT security through the use of strong authentication technologies
* Reducing the cost and complexity of deploying certificates and smart cards
* Facilitating stronger identity assurance and compliance enforcement
* Improving operational efficiency for user provisioning and credential management
* Reducing the help desk burden associated with user access and entitlement changes
* Leveraging your existing Microsoft IT infrastructure assets

For additional information, please refer to:

* [www.microsoft.com/ida](http://www.microsoft.com/ida) -- Microsoft’s Identity and Access Solutions
* [www.microsoft.com/ilm](http://www.microsoft.com/ilm) -- Microsoft Identity Lifecycle Manager