IdLifeMgr07_bL (6 x 2).tif

Certificate and Smart Card Management with  
Microsoft Identity Lifecycle Manager 2007

Technical Whitepaper

Published: December 2008

Abstract

This whitepaper provides a technical overview of the certificate and smart card management capabilities provided by Microsoft Identity Lifecycle Manager (ILM) 2007 FP1. Specifically, this document provides information on the business and technical drivers behind the adoption of strong (multi-factor) authentication management system products, an ILM 2007 architecture overview, implementation guidance and the benefits of using a Microsoft ILM 2007 solution approach.

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

[Document Overview 1](#_Toc217123925)

[Background 2](#_Toc217123926)

[Strong Authentication Deployment Challenges 4](#_Toc217123927)

[Business Challenges 4](#_Toc217123928)

[Technical Challenges 4](#_Toc217123929)

[Simplifying Strong Authentication with Microsoft ILM 2007 5](#_Toc217123930)

[ILM 2007 Architecture 6](#_Toc217123931)

[ILM 2007 Certificate Lifecycle Manager Functionality 6](#_Toc217123932)

[ILM 2007 Architecture 7](#_Toc217123933)

[ILM Component Architecture 8](#_Toc217123934)

[ILM Physical Architecture 8](#_Toc217123935)

[ILM 2007 Client 11](#_Toc217123936)

[Middleware 11](#_Toc217123937)

[Smart Cards and Tokens 12](#_Toc217123938)

[Protocols and Dependencies 13](#_Toc217123939)

[Operating ILM 2007 in the Enterprise 15](#_Toc217123940)

[Roles 15](#_Toc217123941)

[Permissions 15](#_Toc217123942)

[Subscribers 16](#_Toc217123943)

[User Authentication 17](#_Toc217123944)

[Managers 18](#_Toc217123945)

[Profile Templates 19](#_Toc217123946)

[Reporting 22](#_Toc217123947)

[Issue Resolution 23](#_Toc217123948)

[ILM 2007 Deployment Scenarios 24](#_Toc217123949)

[Smart Card Logon 24](#_Toc217123950)

[VPN (IPSEC, SSL) 26](#_Toc217123951)

[Secure Email (S/MIME) 28](#_Toc217123952)

[High Availability Architecture 29](#_Toc217123953)

[Benefits of a Microsoft ILM 2007 Approach 31](#_Toc217123954)

[Additional Resources 34](#_Toc217123955)

# Document Overview

This whitepaper is intended for Technical IT Managers, IT Architects, and IT Security Analysts to provide a technical overview of the certificate and smart card management capabilities provided by Microsoft’s Identity Lifecycle Manager (ILM) 2007 product offering. Specifically, the document provides information on the business and technical drivers behind the adoption of strong (multi-factor) authentication management systems products like Certificate Lifecycle Manager, an architecture level overview, implementation guidance, how tightly the product integrates with the rest of the Microsoft environment and the benefits of using a Microsoft ILM 2007 solution approach.

This whitepaper is divided into the following sections:

* Strong Authentication Deployment Challenges
* ILM 2007 Architecture
* Operating ILM 2007 in an Enterprise Environment
* ILM 2007 Deployment Scenarios
* Benefits of a Microsoft ILM 2007 Approach

Related links to additional resources are provided at the end of this whitepaper.

# Background

Usernames and passwords have been around since the beginning of enterprise computing and are pervasive based on their simplicity. At the same time, the strategic value of IT environments is increasing and therefore driving organizations to consider stronger authentication across a wide range of applications and user scenarios. This includes user authentication, data encryption and digital signatures as a starting point. These scenarios need sophisticated management because certificate management must also be included as an attribute of the broader identity management challenge.

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

Certificates are an important component of a longer term identity management implementation because they provide many features that are valuable to the enterprise. One of the properties of certificates is that they are difficult to forge and are a mature technology makes them an ideal authentication solution in a wide variety of situations. This includes using certificates 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. Certificates can also be used for more advanced functionality like digital signatures making them even more valuable from a business perspective. As a result, 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 ILM which provides a robust certificate lifecycle management capability to address many of these scenarios. ILM can also provide some management functionality for machine based certificates like Web Servers for example. Certificate management has many components including enrollment, key escrow, certificate recovery, revocation and others that are technically complex but important to the over usability of the solution. ILM implements all of these features in a simple web-based interface that is configurable and flexible. The result is a full feature certificate lifecycle 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 also addresses this management challenge by providing rich management functionality for the smart card that hides these complex details.

ILM 2007’s certificate and smart card management capabilities provide an integral component of an organization’s overall identity management approach by synchronizing the provisioning of multi-factor authentication credentials. For example, in a typical identity management workflow – an account name and password would be created and provisioned to authorized target applications. ILM 2007’s certificate and smart card management component augments this process by providing the rich management infrastructure required to issue and manage certificates and smart cards that are linked to user accounts in a synchronized provisioning process.

While the full ILM 2007 product addresses a wide range of identity management challenges including provisioning, data synchronization in addition to certificate / smart card management, the central focus of this paper is the certificate and smart card lifecycle management capabilities of ILM.

# Strong Authentication Deployment Challenges

While the use of digital certificates and smart cards provides an excellent approach to deploying stronger authentication over traditional username / password based systems, there are additional deployment considerations customers are faced with to provision and manage these technologies in a cost effect manner.

Deploying certificates and smart cards within a large enterprise environment can create a significant operational burden, unless tools are available to assist with the provisioning and lifecycle management process.

The business and technical challenges that customers typically face when deploying a certificate services based solution architecture that leverages a certificate and smart card management system such as ILM are described below.

## Business Challenges

**Ease of Use and End User Acceptance** – Users are reluctant to accept new authentication technology unless it can provide proven benefits, provides greater flexibility than their existing authentication solution, or is easier to use. Technologies that allow for user-self servicing must be simple enough for the user to perform the functions they need.

**Alignment with Corporate Security Policies and Standards** – The nature of IT security controls is that they are typically mandated for compliance reasons and reflect requirements as dictated by corporate policies and standards. The solution chosen must be flexible enough to meet these requirements.

**Reduction of Help Desk Burden and Minimization of Additional Management Overhead** – Any solution that is implemented must minimize the impact on help desk staff and network administrators. The solutions that have the greatest return on investment are those that reduce the existing access control management burden that is typically inherent in help desk operations today.

## Technical Challenges

**Selection of Correct Authentication Technology** – The technology and form factor selected for the authentication technology has to be able to meet security requirements, solve immediate security problems, position the organization for future requirements, and provide a simple and easy to use interface for end-users. The authentication technology selected should be scalable so that it can meet immediate authentication requirements and future encryption or digital signing requirements.

**Lost, Stolen or Forgotten Smart Cards** – There is a significant change for help desk staff and network administrators when the decision is made to migrate from user name and password based authentication to smart card or token based authentication. The management challenges and logistics concerning the replacement of lost, stolen or forgotten cards should not be overlooked and must be considered as part of overall certificate and authentication device management lifecycle.

**Deployment of Smart Card Middleware** – Until the release of BaseCSP[[1]](#footnote-2), the deployment of smart cards meant the installation of smart card middleware matched to each vendor’s smart card on each user’s desktop utilizing smart card services. If required, the deployment of smart card middleware must be considered as part of smart card roll-out and adoption strategy. BaseCSP compliant cards will reduce this burden significantly.

**Geographic Distribution** – IT Analysts that have deployed PKI technologies in the past understand that the secure distribution of certificates to users can be a significant challenge. This challenge increases with the number of users and the geographic disparity of the sites where the technology will be deployed. Distribution of certificates can be further complicated by the intended use of the certificate. For example if you are deploying certificates that will be used for digital signatures, you need to ensure that a user’s identity is validated before a credential is issued to them.

**Integration with an Overall Identity Management Framework or System** – Certificate and Smart Card Management Systems must integrate within an overall identity management framework within an enterprise environment. It is important that API’s, identity repositories and information stores are based on common technology infrastructures so that they can integrate with and leverage other identity management systems that are currently in place.

**Managing Certificates used for Encryption** – Certificates can be stored on smart cards or locally on computers where users log on. Certificates that are used to encrypt data such as when Encrypted File System (EFS) is configured to use certificates need to have a management solution for key recovery.

## Simplifying Strong Authentication with Microsoft ILM 2007

The release of Microsoft Identity Lifecycle Manager 2007 provides enterprise IT environments with the rich management tools that enable customers to address a range of business and technical challenges associated in deploying digital certificate and smart card based strong authentication solutions including those listed above.

The certificate and smart card management capabilities of ILM 2007 were inherently designed to reduce the cost and complexities of deploying strong authentication technologies such as smart cards and digital certificates within a single integrated lifecycle management solution.

The following sections of this whitepaper are intended to provide a technical overview of ILM 2007 and how customers can use ILM to support a range of strong authentication deployment scenarios across the enterprise. The benefits of using an ILM 2007 based approach to deploying strong authentication solutions are summarized in Section 7 (“Benefits of a Microsoft ILM 2007 Approach”).

# ILM 2007 Architecture

## ILM 2007 Certificate Lifecycle Manager Functionality

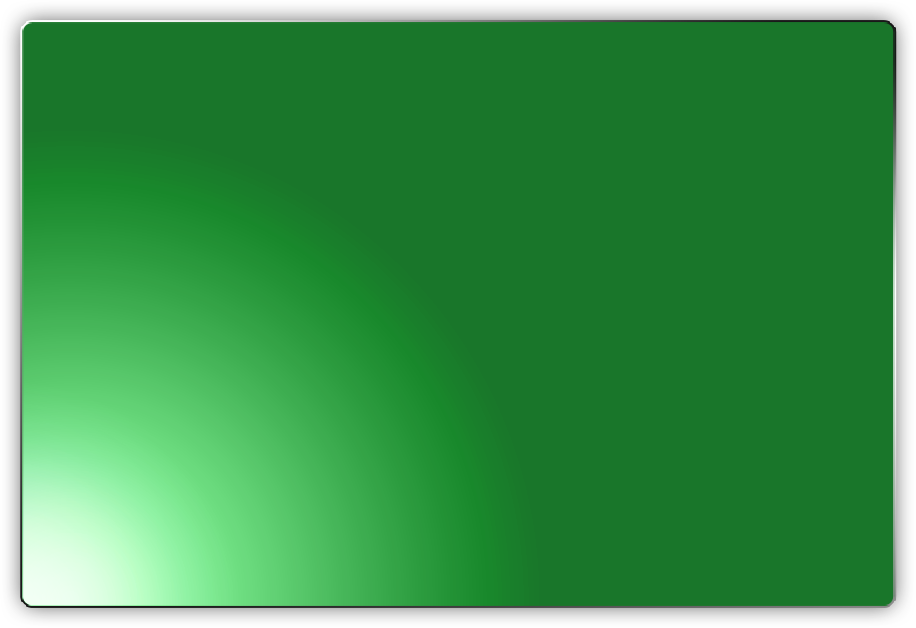
ILM’s Certificate Lifecycle Manager component provides enterprise grade certificate and smart card management capabilities for centralized or highly distributed enterprises. It allows security and system administrators to apply certificate management policies consistently across a wide range of certificate uses and to a diverse user base of clients.

ILM provides the following certificate and smart card lifecycle management capabilities:

* **Single administration point for digital certificates and smart cards** – ILM provides a web based interface that provides administrators access to a management portal for the management and administration of certificates and smart cards.
* **User self-service** – The ILM portal also provides users with the ability to perform self-registration process or to perform basic certificate and smart card lifecycle management tasks such as requesting new certificates or performing PIN resets.
* **Configurable policy-based workflows for common tasks –** ILM provides the ability to apply policies against common certificate and smart card management tasks from any given certificate or grouping of certificates through the use of profile templates. Profile templates provide a common set of policies for certificate enrollment, renewal, update, recovery, revocation and retirement. In addition, specialized policies have been created to handle lifecycle management challenges related to the management of smart cards such as temporary issuance of smart cards, smart card duplication, personalization and retirement.
* **Detailed auditing and reporting** – ILM provides a comprehensive set of reports for common reporting tasks. “Out-of-the-Box” reports include: certificate usage, certificate expiry summary report, smart card report, request report, certificate template settings report, profile template settings report, certificate template usage report, certificate revocation list report and smart card history reports. Granular auditing of all Certificate Lifecycle Management tasks is also available to the administrator through the web-based management interface.
* **Support for centralized, de-centralized and self-service scenarios** – ILM’s role and permissions architecture provides for a fine-grained level of control. This is achieved by leveraging the capabilities of Active Directory groups and ILM permissions. This allows for configurations that support centralized or de-centralized administration and management through designated accounts. It also provides for user self service scenarios where users are delegated specific pe**r**missions to perform their own self management tasks.
* **Tightly integrated with Certificate Services and Active Directory** – ILM is tightly integrated with underlying Microsoft technologies including the two Windows Server components Active Directory Certificate Services and Active Directory Domain Services. ILM’s Certificate Lifecycle Manager component integrates with Certificate Services by acting as a higher-level management interface (commonly referred to as a Registration Authority or RA) between administrators and certificate services (see architectural overview below) through the use of ILM policy and exit modules. This allows ILM to perform all day to day certificate management tasks which would previously be performed through the Certificate Services MMC. Integration with Active Directory is supported by extending the schema to support ILM objects and permissions. This allows enterprises to leverage existing infrastructure to the fullest extent and to extend the functionality of their existing investment.

## ILM 2007 Architecture

below provides an overview of the physical architecture of a typical ILM implementation -- showing a physical representation (servers) on the left and the associated logical components on the right.



ILM 2007

Server

Certificate Services

ILM 2007

Client

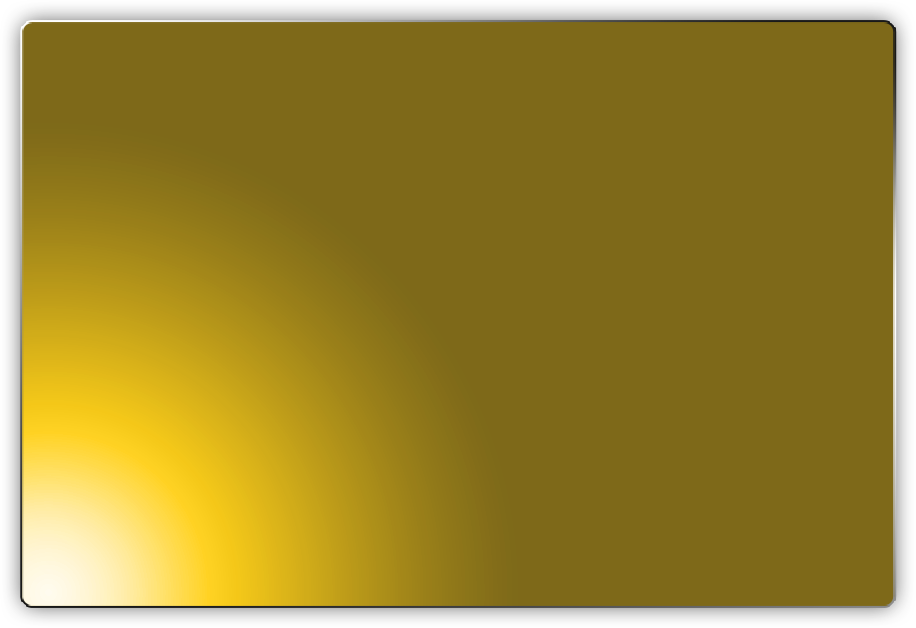
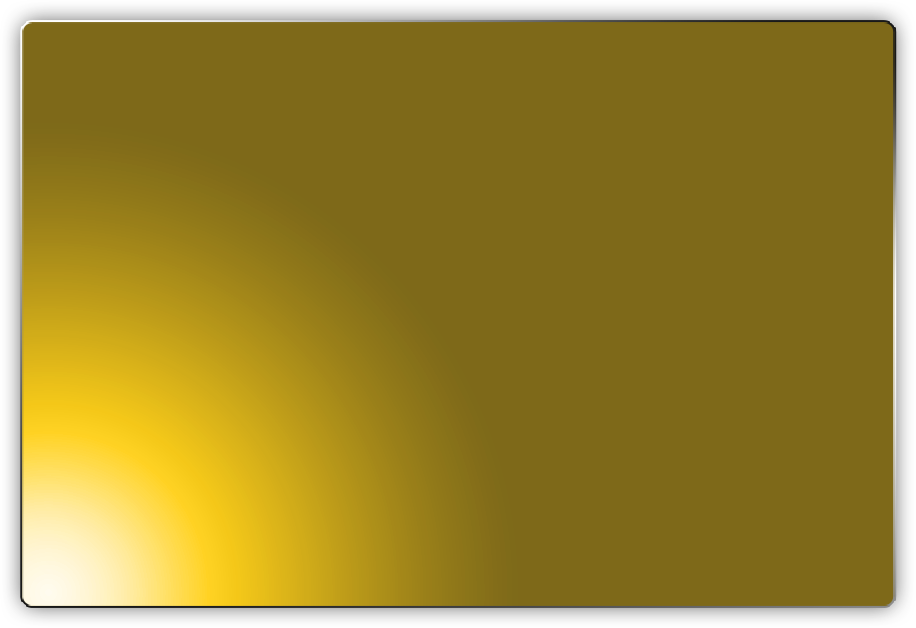
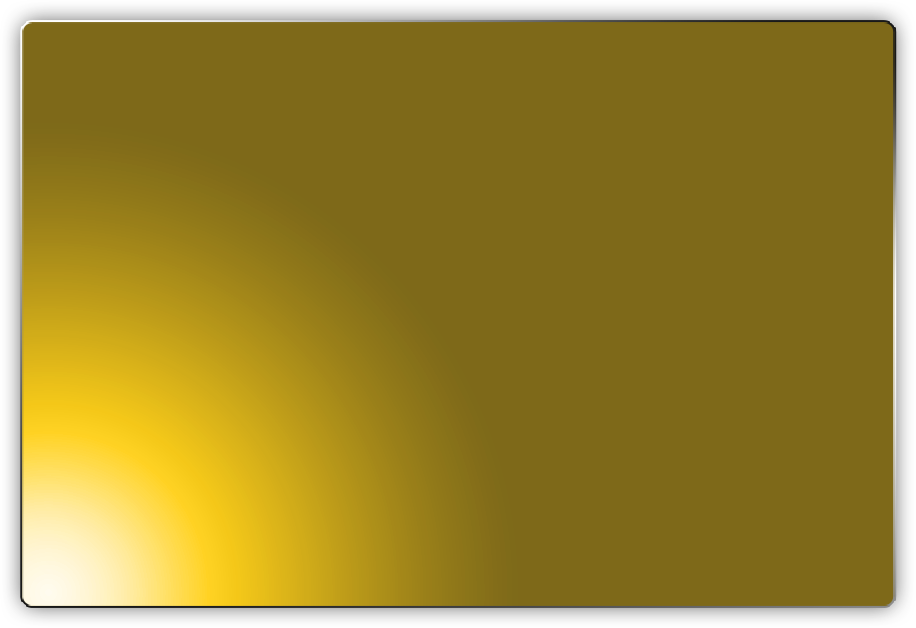
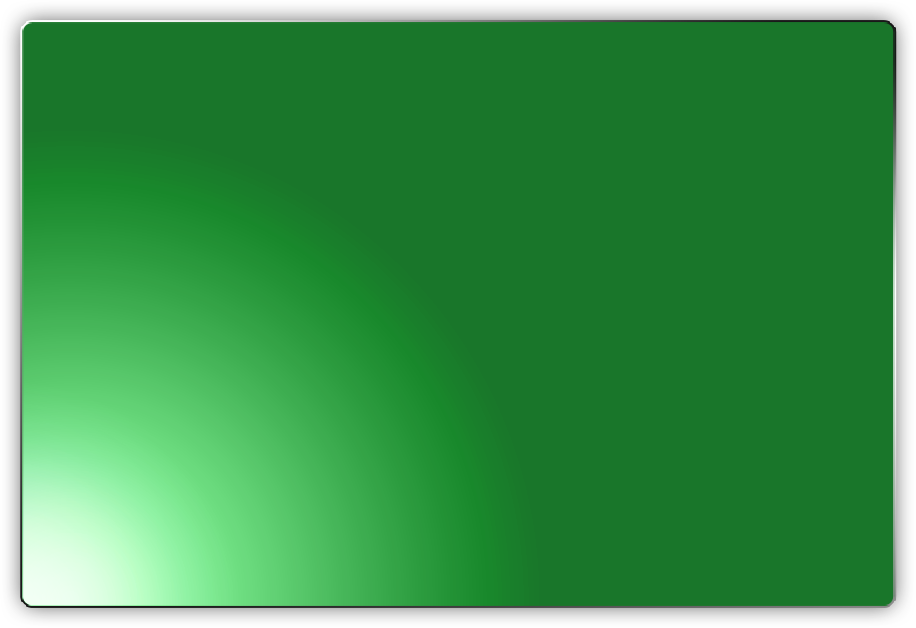
**Physical Architecture**

SQL Server

Active

Directory

E-mail



ILM Policy Module



ILM Exit Module



Internet Explorer



ILM Browser Control



ILM AD Integration



ILM Web App



Internet Information Server

**Component Architecture**



Microsoft Certificate Authority



Smart Card Middleware

**Figure 1** – ILM Architectural Overview

Each of these components is described in the following sections.

ILM Component Architecture

The core of the architecture is the ILM server, which is a web based ASP.NET application running on an IIS web server. The ILM server provides management services to Microsoft Certificate Authorities which integrates with the architecture utilizing a policy module and an exit module. The ILM server utilizes SQL Server as a repository for ILM profile templates and operational and management information. Users access the ILM portal via Internet Explorer utilizing an ActiveX control which integrates with local smart card middleware. ILM management functions are also made available through the ILM portal for authorized managers.

ILM provides sophisticated management features to Windows Server 2003 and 2008 CAs (single or multiple) by acting as an administrative proxy. Once installed within an organization, all digital certificate and smart card management functions can pass through ILM, with a single instance managing multiple issuing CAs.

A typical ILM deployment consists of at least one ILM server and one or more issuing CA’s. It is possible for a single ILM server to manage multiple CAs simultaneously, or for multiple ILM servers to manage a single CA. The ILM server consists of a Windows Server with ILM actings as an administrative proxy to the CAs. This server provides an easy-to-use Web interface to an application engine that is integrated with Active Directory Certificate Services and Directory Services. All application configuration information is stored in an SQL Server database that is accessed by the ILM server and the CA modules.

ILM Physical Architecture

#### Identity Lifecycle Manager 2007 Server

The ILM 2007 Server runs on both Windows Server 2003 and 2008 and Microsoft Internet Information Server (IIS). ILM is an ASP.NET application that requires the Microsoft .NET Framework to be installed on the server platform. The .NET Framework is a separate but mandatory installation component. The server stores all ILM management information in a Microsoft SQL Server database It can be located on a non-dedicated server such as an enterprise database server, and the ILM installation package can create the appropriate databases.

The ILM 2007 Server provides a web based interface to two key functions that are required to manage the full lifecycle of certificate management: a management portal and a subscriber portal. At the highest level, a certificate and smart card deployment has at least two roles: subscribers and managers. Subscribers are simply end users that need certificates with or without smart cards. Managers are users that have some level of permissions within ILM to either administer other users or to administer the application itself.

**Manager Web Portal** – Thiscomponent of the ILM solution interacts with ILM certificate managers and exposes functionality used for managing end-user certificates. The specific functionality available to ILM managers is based on their group memberships and permissions within Active Directory.

**Subscriber Web Portal** – This is the component of the ILM server that interacts directly with the certificate subscribers in a self-service mode. The specific functionality available to ILM users is based on their group memberships and permissions within Active Directory.

#### Microsoft Certificate Services

The Certificate Lifecycle Manager component of ILM 2007 is tightly integrated with Windows Server 2003 Certificate Services as well as Windows Server 2008 Active Directory Certificate Services. The ILM architecture augments the functionality of Certificate Services through the addition of modules that enhance its functionality. These modules include an ILM policy module and exit module.

The ILM policy modules determine whether certificate requests received by the CA should be automatically approved, denied or marked as pending and they can set specific attribute values in the certificates being request. The exit modules provide post-processing once after a certificate has been issued. ILM ships with policy modules that can provide additional functionality depending on the deployment scenario that is required. The included modules provide additional functionality in support of S/MIME certificates, certificate subject and subject alternative name customization, as well as configuring support for non-ILM generated requests. The ILM exit modules provides connectivity to the SQL database and ensures that processing is passed back to the ILM server once a certificate has been issued. The exit module also provides the capability to log and audit all certificates generated by the Certificate Server and makes this available through the ILM interface. This provides a significantly enhanced certificate logging and auditing capability available through the ILM interface versus the traditional method of tracking certificates via the Microsoft Management Console Certificate Authority interface.

#### Active Directory

The Certificate Lifecycle Manager component of ILM 2007 is tightly integrated with Active Directory for user authentication and the definition of user permissions within the application. During the Certificate Lifecycle Manager install, the Active Directory Schema is updated to support the additional objects and privileges required for ILM. This allows an organization to leverage an existing infrastructure component and a single management interface for their PKI infrastructure. It also allows ILM to leverage the administrative and management models configured within the organizations Enterprise Active Directory environment.

Similar to a standard certificate services installation, ILM continues to store published certificates into the Active Directory Certificate store for accessibility throughout the organization. The use of AD in this scenario allows organizations to fully benefit from their investment in a highly distributed and redundant directory environment.

#### SQL Server

The Certificate Lifecycle Manager component of ILM 2007 utilizes Microsoft SQL Server as its repository for all certificate and smart card management information. This includes profile templates and audit logs of all activities executed through Certificate Lifecycle Manager. Microsoft SQL Server 2000 and 2005 are currently supported with Identity Lifecycle Manager 2007 Feature Pack 1. For high-availability or disaster recovery scenarios ILM supports the utilization of SQL Server running in a cluster environment and the use of SQL Server log shipping functionality.

#### APIs

ILM is designed to support customizations and extensions that may be required by specific customers. These extensions can be developed using a variety of tools that support the .NET Framework including Microsoft Visual Studio® .NET. Within Visual Studio .NET, C# is the preferred development language for customizations. Three different APIs are natively supported within ILM.

**Provisioning API** – The provisioning API allows for custom applications to access smart card and certificate management workflows within ILM. This allows ILM to support customized registration applications or applications that integrate with smart cards that are not natively supported within ILM. The provision API could be used to integrate ILM with physical security systems or provide an interface for specialized registration requirements such as a FIPS-201 registration console.

**Notification API** – The notification API can be used to initiate custom code modules based on ILM events. This API provides an enhanced notification capability that can be used to augment ILM’s notification capabilities beyond what is currently provided. The notification API can be used for the distribution of one-time-passwords (OTPs) to devices such as cell phones or to integrate with custom applications that could perform actions based on ILM events such as initiating provisioning of account information to other applications.

**SQL API** – The SQL API provides an interface that allows developers to access ILM functionality by writing to the SQL Server database store through a defined interface. The SQL API allows developers to write custom applications to query and submit ILM requests that can then be processed using ILM profile templates. The functionality can be used for a wide range of applications such as customized registration interfaces and certificate management applications.

**Extensibility**

ILM also has the ability to use custom validators which are code modules that can be called from data item collectors attached to policies within profile templates. Custom validators are code modules that can use external code to validate data input during the enrollment process or at any policy that utilizes data collection. The custom validators provide a capability to validate input beyond native ILM functionality. Example applications of a custom validator are allowing the enrollment process to validate an employee number against information contained within an organization’s human resources database.

In addition to the API’s provided, Certificate Lifecycle Management capabilities integrates with ILM’s identity synchronization engine – enabling identity integration via ILM’s Management Agents. This allows ILM to take advantage of ILM connectivity to over 20 different platforms. ILM’s identity synchronization engine also provides a native ILM Management Agent which provides out-of-the box connectivity between ILM’s synchronization engine and CLM.

## ILM 2007 Client

ILM is designed to minimize the software components required on client workstations. Users access the ILM portal using a standard web browser which utilizes underlying software and the ILM client for smart card communications and profile management.

At a minimum, clients require Windows XP SP2 and Internet Explorer 6. The ILM portal has a minimum requirement of Internet Explorer 6.0 and full support for Windows Vista and Internet Explorer 7.0 in ILM 2007 Feature Pack 1. If ILM is used for smart card management scenarios, the ILM client requires either a Microsoft Base Cryptographic Service Provider (BaseCSP) compliant mini-driver or 3rd party smart card middleware from a supported vendor. BaseCSP mini-drivers and 3rd party middleware are discussed further in the next section. With the Vista client support in ILM 2007 FP1 it also supports off-line PIN unblock.

The ILM client provides additional functionality and software components to support client side user self-service capabilities related to managing the smart card. If self-service management (ie. PIN Change, Enrollment, etc.) is not required, then the ILM smart card client is also not required to be installed on the desktop. Specifically the ILM client adds the following components: the ActiveX Smart Card Self Service control which provides client-side certificate management capabilities and the smart card personalization control. The client also provides support for online update capabilities for certificate profiles as well as the tool for offline Smart Card PIN unblocking in Windows Vista.

## Middleware

One of the challenges that has existed in the smart card industry is a tight binding or association between smart cards, smart card drivers and the management infrastructure capable of managing the cards. This is largely due to a lack of standards at the smart card level or variations in the implementation of those standards making it difficult for a generic management system to effectively manage a range of smart cards.

One of the standards that has been implemented for the management and run-time use of smart cards is called PKCS#11. This standard has been widely implemented by smart card vendors but not always consistently enough for the purposes of a general management system. ILM 2007 does support PKCS#11 as a mechanism to manage smart cards from a number of smart card vendors. The support however is specific to each smart card vendors middleware and therefore there are specific dependencies and potentially issues in the future when that middleware changes. Another approach to smart card middleware is the implementation of a Microsoft BaseCSP compliant mini-driver. The Microsoft BaseCSP provides a robust mechanism for managing smart cards and allows smart card vendors to provide a relatively small component (called the mini-driver) to enable the card. ILM 2007 can then manage any smart card that has a compliant mini-driver. Microsoft additionally has testing requirements for mini-drivers that can be used to assess and evaluate the quality of mini-drivers further improving the success and ease of deployment.

While both of these approaches can produce a successful smart card deployment, it is the strategic direction for ILM smart card support to use the BaseCSP architecture. As a result, if an option exists to use this architecture it should probably be selected for future support reasons. BaseCSP support on the client side is available in Windows XP and Windows Vista.

## Smart Cards and Tokens

ILM’s Certificate Lifecycle Management component supports a wide range of smart cards and authentication tokens. Vendors provide smart card capabilities in many form factors including the traditional smart card and smart card reader and USB based tokens containing smart card chips. Recent advancements in smart card technology have allowed smart card vendors to integrate other functionality into smart cards and smart card tokens, including combination cards which support both physical and logical access control, smart cards and tokens that include one-time-password generators in addition to traditional smart card functionality, and smart cards that integrate data storage with certificate storage.

ILM has the ability to support a wide range of smart cards and smart card readers. ILM 2007 FP1 supports the following smart cards:

* BaseCSP Compliant Smart Cards
  + Gemalto’s .NET card
  + HID’s Crescendo C200 card
  + And any card that has been approved through Microsoft’s BaseCSP compliance program.
* PCKS#11 Compliant Cards and Middleware from the following vendors:
  + Axalto Client Software (ACS) v 5.2;
  + HID’s Crescendo C700 card
  + AET SafeSign v2.1;
  + Aladdin eToken RTE 3.6;
  + Gemplus GemSafe v4.2; and
  + Siemens HiPath SIcurity Card API v3.1.026.

## Protocols and Dependencies



**Figure 2** – ILM Protocol Dependencies

Figure 2above provides an illustration of the TCP/IP communications between various components of the architecture. A summary list of source/destinations, associated protocol and TCP/IP port numbers are provided in below. Many of these protocols allow for configuration of the TCP/IP port settings such as SQL, SMTP, and HTTPS. Kerberos, Active Directory related protocols and RPC ports are not configurable. It is important that firewalls or port filtering router permit communications using the ports identified for each of the hosts in the architecture.

Table 1 – Desktop Optimization Architecture TCP/IP Protocol Chart

|  |  |  |  |
| --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **TCP/IP Port** |
| ILM | SQL Server | SQL over TCP | 1433 |
| ILM | SQL Server | SQL Probe | 1434 |
| ILM | Active Directory | Kerberos | 88 |
| ILM | Active Directory | Microsoft-DS | 445 |
| ILM | Active Directory | Microsoft Global Catalog | 3268 |
| ILM | Active Directory | RPC | Random Greater than 1024 |
| ILM | SMTP Relay | SMTP | 25 |
| ILM | Microsoft Certificate Services | RPC | 135 |
| ILM | Microsoft Certificate Services | RPC | Random Greater than 1024 |
| Client | ILM | HTTPS | 443 |
| Client | Active Directory | Kerberos | 88 |
| Client | Active Directory |  | 1025 |

**Note:** Additional protocols may be required to support the specific application for which ILM’s certificate management capabilities will be used. For example, IPSEC, L2TP, PPTP or SSL for VPNs or additional Microsoft RPC ports for Secure Email. These port numbers are the standard ports and some companies choose to deploy for example SQL Server and SMTP running on other ports.

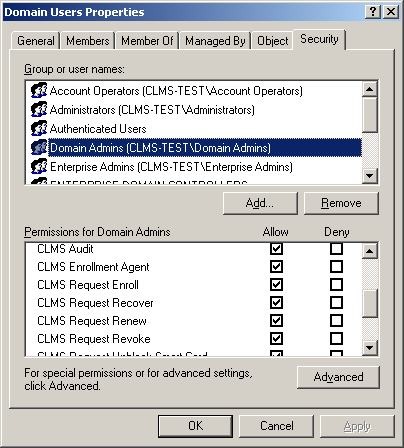
# Operating ILM 2007 in the Enterprise

## Roles

Operating ILM effectively generally means implementing policies in the software that are appropriate for the organization and allowing the software to expose those policies in its workflows. The workflows in turn may require different individuals performing a variety of functions that might be end user related, approval related, administrator related or others. These tasks can be applied to roles that are defined within Active Directory as groups and then utilized in ILM. This is the essence of a role in ILM – it is the creation of an AD group and associating ILM permissions with that group. That group can then be used within ILM and will only be able to perform the functions that have been granted via the permissions. This provides a flexible mechanism for organizations to create as many roles (AD groups) as they require and any combination of ILM permissions. The result is flexibility that can allow organizations to meet a wide range of requirements.

### Permissions

A flexible smart card and certificate management solution requires delegation of responsibilities, and therefore sophisticated role management and granular permissions. These roles determine permissions within the system to perform certificate management functions for specific users, as well as permissions to configure the application environment. ILM uses Active Directory extensively for this functionality and extends the environment to include CLM permissions as seen in Figure 3 below. The benefit of this approach is that the customer does not need to build a separate system of users and permissions for the certificate or smart card deployment but rather uses the existing infrastructure.



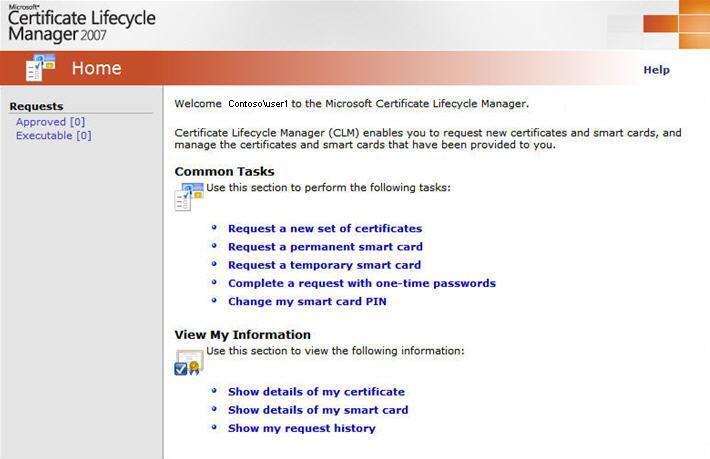
**Figure 3** – Managing permission settings through Active Directory Profiles

Certificate managers receive their permissions within the system based on their group memberships and permissions within Active Directory. Because the permission system within ILM actually uses Active Directory groups, there are few restrictions on how the management of the application and users can be delegated.

### Subscribers

A subscriber is an end user that requires a smart card and/or certificate services. This user may require a digital certificate for smart card logon, wireless access, secure e-mail, VPN services, or many other public key infrastructure (PKI)-aware applications. The goal of ILM is to make the management of these certificates as easy as possible for end users, while simultaneously providing the organization with an appropriate level of security.

ILM provides a subscriber Web portal that enables specific self-service management functions. Self-service functions can be attractive to organizations that are attempting to minimize administrative costs; however, self-service functions also have disadvantages from a pure security perspective. ILM handles this challenge by allowing organizations to define which functions should be available for self-service and which should not. This can be done on an individual profile template basis or user group basis, which means that one type of profile can be managed in a self-service fashion while another is not. All workflow functions can utilize email integration for notification and automatic distribution of authentication and approval information (if desired). Additional information regarding profile templates is provided in Section 5.2 (“Profile Templates”) of this whitepaper.



**Figure 4** – Subscriber Portal

Figure 4 shows a typical configuration for the subscriber portal. From this portal, it is possible for subscriber to view and manage their certificates and smart cards (based on configuration and policy). This includes potentially being able to request a smart card or recover a smart card. How the request is processed is determined by the profile template. Examples include the request being completed immediately, or potentially requiring an approval from help desk or some other individual such as the user’s manager.

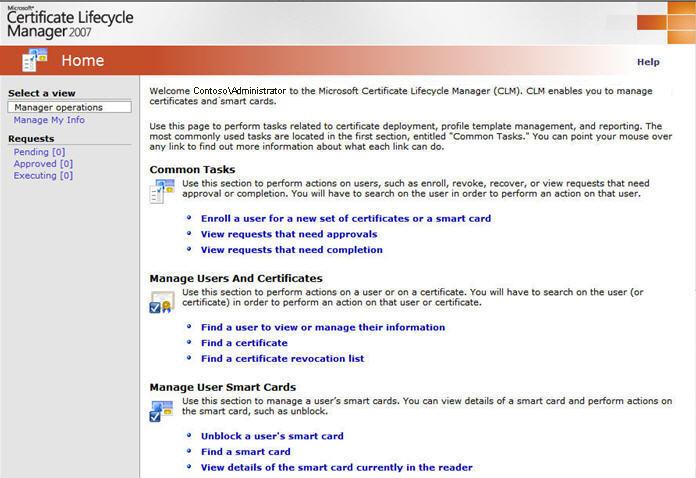
### User Authentication

ILM can use a variety of authentication mechanisms to the portal for subscribers and managers. Because ILM uses Active Directory to determine a user’s permissions, the user must ultimately authenticate with his or her domain credentials to the portal. ILM can be configured to use integrated authentication, in which case the user can simply navigate to the ILM portal, and if the user is authenticated to the domain, the user will not be prompted to authenticate again. Other options can also be used, including basic authentication (domain user name and password) or certificate/smart-card-based authentication, if desired. The most important implication of this approach is that ILM does not require a separate database of users, passwords, and permissions. It is possible to provide a group of users, such as a help desk, with access to ILM by simply granting the appropriate permissions to that user group within Active Directory. The rest is handled in a completely integrated fashion with the operating system and Active Directory.

### Managers

A manager within ILM is an individual that has been granted permissions to access the ILM manager Web portal (see Figure 5). This portal resides on the same ILM server as the certificate subscriber portal but exposes functionality used for managing other users and application information. Permissions are granted to a certificate manager using the standard Active Directory security management tools. Typically, this means users must be granted access to ILM and are then granted access to specific ILM functions such as enroll, recover, or revoke. Finally, they are given permissions to manage a particular group or groups of end users. Even more granularity is possible by granting access to specific certificate templates that they can manage, while restricting other certificate management functions.

Managers can also be granted permissions to approve the certificate requests of other managers or end users that have submitted self-service requests. These requests are handled through the easy-to-use Web portal, coupled with e-mail support once the requests have been processed. Reporting and auditing functions are then available to track activities and to perform analysis and verification of certificate management functions. Because auditing is a specific ILM permission, it is possible to configure a user role that is only able to generate reports and not perform any actual certificate management functions.



**Figure 5** – Administrator Portal

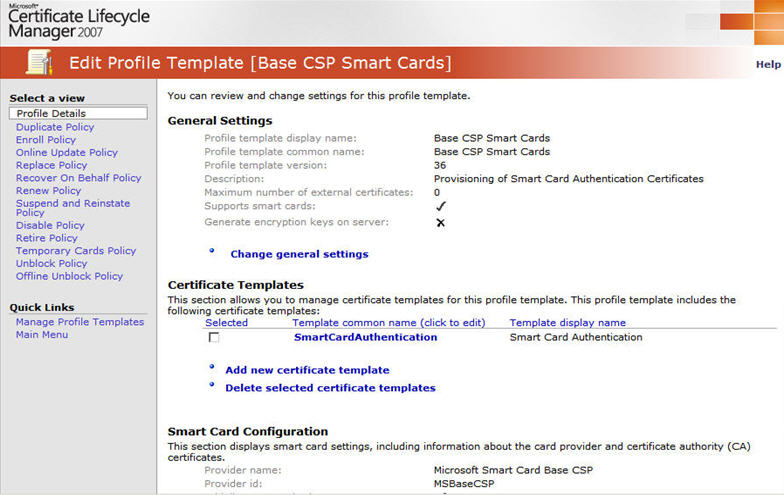
## Profile Templates

A profile template is a core component of all management activities within ILM. The purpose of a profile template is to provide a single administrative unit that includes all of the information necessary to manage multiple certificates that may be required by a user community throughout the certificate’s entire life cycle.

A profile template also includes information related to the final location for those certificates, which can be software-based (stored on the local computer) or hardware-based (stored on a smart card). In the case that the certificates are stored on a smart card, a ILM profile template is also configured with the information necessary to manage the smart card, and therefore provides a single point of administration for the smart card and the certificates.

A profile template can contain one or more certificate templates that can be managed as a single item. Without this approach, an organization is forced to manage multiple user certificates independently, which is expensive and prone to error. A profile template allows for the deployment of authentication and encryption type certificates in a single step.

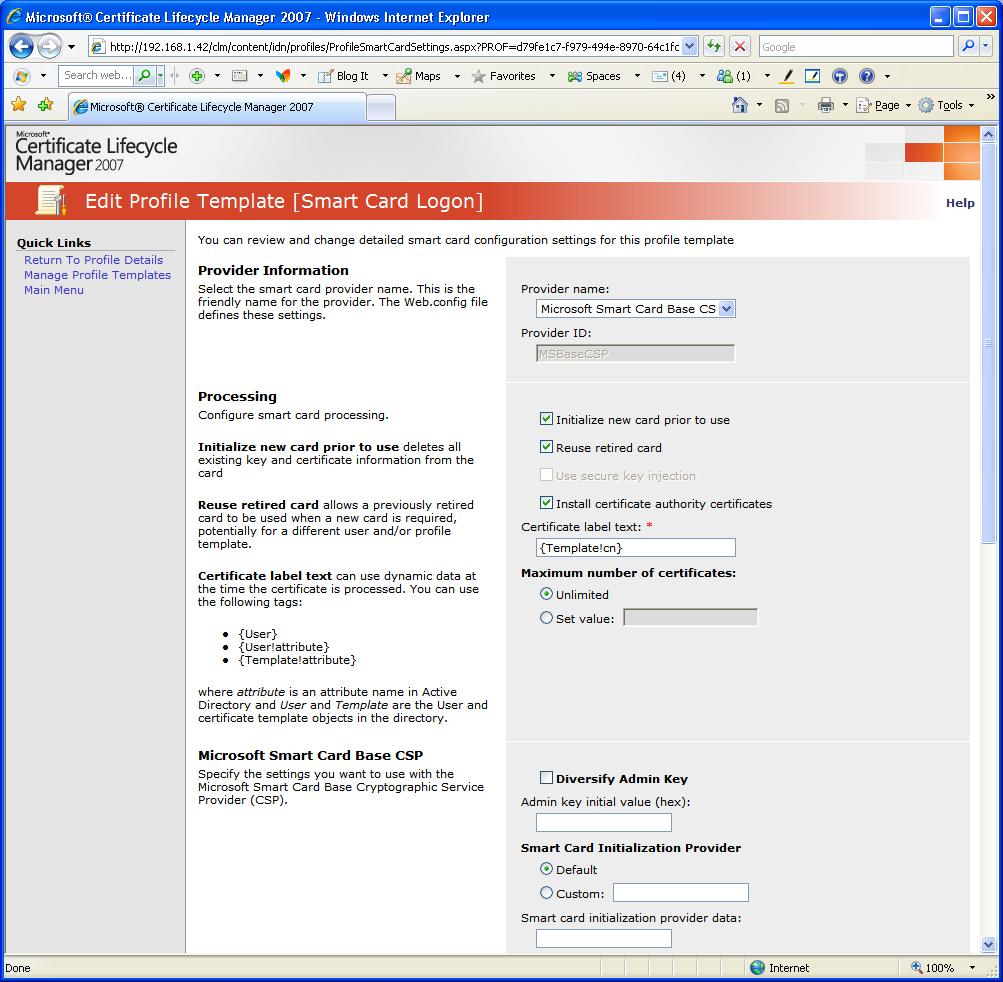
Additionally, ILM is able to handle authentication certificates and encryption certificates differently depending on whether the encryption certificates are backed up for future recovery. For example, when ILM is asked to recover a particular profile because a smart card may have been lost, the application generates new authentication certificates but recovers the existing encryption certificates. At the same time, ILM manages the administrative details associated with initializing the smart card.



**Figure 6** – ILM Profile Templates

6 shows the general configuration for a profile template and the various items that are included in that configuration. It allows the specification of the profile template as software-based or hardware-based (smart card). The certificate templates section provides the ability to add or remove certificate templates. These certificate templates are read directly from Active Directory and are issued from a selected certificate authority. If desired, the individual certificate templates can even be issued from different certificate authorities. In most cases, the collection of certificate templates includes a combination of signing/authentication and encryption certificates.

If the profile template is configured to support a smart card deployment, then management details for the actual smart card can be provided. Some of these details are shown in Figure 7 and include the smart card provider, password rules, and administrative password configuration.



**Figure 7** – Profile Template Smart Card Configuration

The profile template includes configuration for the management policies that are used to manage the deployed profile. These management tasks include:

* Enrollment
* Recover (Replace)
* Renewal
* Revocation
* Disable
* Unblock (for smart card profiles)
* Duplicate (for smart card profiles)

Each of these tasks can be configured separately so that the way a profile is enrolled might be different from how it is recovered or renewed. This provides the enterprise customer with a wide variety of choices in terms of how these tasks are managed.

Each management task can use Web forms to capture information that can be stored or validated against other data sources. This configuration is performed as part of the application management and does not require any custom development activities.

Furthermore, there can also be a predetermined approval mechanism and distribution of approval information such as e-mails and one-time passwords. All of this information is captured and configured at the profile template level. Once complete, the profile template is simply put into use and the software implements the rules, workflow, and permissions.

## Reporting

ILM’s Certificate Lifecycle Manager Component provides a rich auditing functionality and all the basic certificate lifecycle management reports required for an initial deployment. ILM stores all certificate lifecycle activity logs and auditing information in the SQL Server repository. All reports are accessible through a web based management interface.

Three different types of reports can be generated from ILM:

* **Summary Reports** – which provides graphical summaries of certificate lifecycle information;
* **Detail Reports** – which provide granular information on certificate lifecycle management objects or events; and
* **Settings Reports** – which provide reports on the configuration and settings of certificate templates or profile templates.

**Summary Reports**

* **Request report** – The certificate request report provides a drill-down summary of certificate requests that allows the administrator to focus on a particular certificate and track all activities that have occurred based on that certificate.
* **Certificate expiry summary report** – This report provides a graphical summary of the number of certificates that are expiring within any given window.
* **Certificate usage** – This report provides a summary of certificates that have been revoked or expired according to either certificate template or ILM profile template.
* **Smart Card inventory report** – This report provides a summary of all smart cards that have been issued by the system.

**Detail Reports**

* **Smart card report** – The smart card report provides detailed information on the smart cards that have been issued by ILM and are under active management by the system.
* **Smart card history report** – This report provides information on the request history of any of the smart cards managed by the system.
* **Certificate template usage report** – This report can provide a list of certificates organized according to the certificate template used to generate the certificate. This report is a useful tool for providing a report of which users have been issued a particular sort of certificate, and when those certificates will be expiring.
* **Certificate revocation list report** – The certificate revocation list report provides a list of all certificates that have been revoked and the reason for their revocation. It provides a report equivalent to the lasted published certificate revocation list within the PKI.

**Settings Reports**

* **Profile template settings report** - The profile template report provides a summary of the configuration of any given profile template used by ILM.
* **Certificate template settings report** – The certificate template report provides a summary of the configuration of any given certificate template used by ILM.

Each of these reports above can be exported in comma delimited format for further processing within another application, if required. Since ILM stores information in a SQL database, customization of reports can be performed by developers and DBAs familiar with Microsoft SQL Server tools. Additionally, ad hoc reports can also be developed using SQL Server Reporting Services. Direct queries to the SQL Server can also be performed for the generation of custom reports using any ODBC (Open DataBase Connectivity) compliant query tool.

## Issue Resolution

ILM provides several mechanisms to track issues and determine resolutions. These include providing messages to the Windows Event Viewer. ILM can also provide text based error tracing to a log file that can be configured in the Web.Config file. These two mechanisms provide a wide range of error reporting functionality.

# ILM 2007 Deployment Scenarios

ILM 2007 is highly scalable and can be configured to support a wide range of certificate management applications. Three typical ILM configurations are described below. Each of these scenarios builds on the base ILM 2007 architecture that has already been described in Section 4 (“ILM 2007 Architecture”) of this whitepaper. The scenarios also identify any additional components required to support the capability. Each scenario describes how ILM’s certificate lifecycle management policies can be leveraged to make each of these solutions easier to architect, deploy and support over the long term.

## Smart Card Logon



**Figure 8** – Diagram of Smart Card Logon

Figure 8, above provides an illustration of the components required in order to enable smart card logon. Essentially the only additional elements to the core infrastructure of Active Directory, Certificate Services, and MS SQL are a BaseCSP enabled Windows XP or Vista client. The domain controller must be configured to utilize a Windows Domain Controller Certificate template that has smart card logon enabled as shown in Figure 9 below.



**Figure 9** – Domain Controller with Smart Card Authentication Enabled

ILM’s Certificate Lifecycle Manager component is central to providing management capabilities in this scenario. It is used to enroll users and associate user accounts with smart cards. It can be used to manage smart cards once user are enrolled and handle situations such as smart card loss and the issuance of temporary cards. Through the use of ILM’s reporting features – deployment of smart cards across the enterprise can also be tracked and managed.

Once a user has been enrolled with a smart card – a variety of different applications are available: Smart Card Logon to the network, Smart Card authentication to any AD enabled application, and access to other applications depending on the types of certificates that have been configured on the card.

With smart card based logon enabled, Windows clients can utilize a smart card to authenticate to the Windows network environment. When prompted to logon, the Windows XP GINA recognizes that a smart card has been inserted into the device’s reader and prompts the user for their smart card PIN. Once the pin is received, the smart card certificate is read from the card and the certificate is used to initiate a Kerberos logon to the Windows network environment. Once the authentication is successful users can continue to access network resources or AD enabled applications using their smart card. If the smart card is removed from the workstation, the user session may be configured through GPO settings to lock or automatically log-off the user. Similarly, Smart Card logon for server administration can also be enabled. Smart card based authentication can be performed against any Windows Server 2003 or Windows Server 2008 server running BaseCSP. Any RDP session to the server can also utilize smart card based authentication – providing an AD integrated two factor authentication solution for server administration.

Once users are enrolled to use a smart card, any application that provides integrated Windows Authentication, can utilize smart card based authentication. Microsoft Internet Information Server based web applications using integrated authentication can leverage the credentials stored on the smart card to authenticate users to web applications without modification. Microsoft Exchange can also access the information on the smart card and use an S/MIME certificate to encrypt and sign emails (more on this scenario in Section 6.3 (“Secure Email - S/MIME”) below).

The use of smart card based authentication also opens the opportunity for integrated security applications such as using the smart card as a photo identification badge or utilizing a hybrid smart card that includes proximity technology for physical access control applications.

## VPN (IPSEC, SSL)



**Figure 10** – Diagram of VPN architecture

A typical strong authentication scenario is the authentication of remote users accessing a corporation network using VPN technology. VPNs devices are now available with a wide range of protocol support, but the architecture described below is equally application to IPSEC, L2TP, PPTP or SSL based VPNs. In each scenario mobile users who are either working from home or while travelling require access to the corporate network to access email, corporate applications, or other resources available through the corporate network. A secure method of authenticating the remote user is required – typically this is provided via a two factor authentication solution or through the use of software certificates resident on the user’s laptop.

Figure 9 above illustrates the architecture where ILM is used to enroll users for VPN certificates. The certificates could be SSL, IPSEC, or regular client authentication certificates depending on the specific VPN endpoint used. In this scenario, VPN client workstations would be issued a certificate using ILM. VPN endpoints would also require a certificate and would need to be configured to trust the Issuing CA and to check for revoked certificates using the certificate distribution points configured within the environment.

In this scenario, users logging in from a remote location would first authenticate to their local workstation before initiating a VPN session. When the VPN session was invoked the VPN client software would use the user’s software certificate or smart card to authenticate the session with the VPN endpoint. The VPN endpoint would check the validity of the software certificate or smart card with the enterprise certificate authority and if valid establish an encrypted session.

The primary certificate and lifecycle management issues related to this scenario are: enrollment of users, replacement of authentication cards and tokens, the issuance of temporary cards and revocation of certificates or smart cards. As part of the profile template settings, workflows could be defined for browser based enrollment of users. Similarly, policy settings could be enabled to allow for the temporary issuance of smart cards or authentication tokens in the event that the authenticator was lost, or if it were used to provide remote access to contractors. Finally, ILM could be used as the primary interface for revoking access when the employee exits the organization or no longer requires remote access.

If VPN access is provided in addition to smart card logon capability, the existing registration and management model could be leveraged. This would allow multiple authentication services to use the same management system and processes rather than requiring the information technology group to manage two different systems.

## Secure Email (S/MIME)



**Figure 11** – Diagram of Secure Email Usage Scenario

Figure 10 above illustrates a Secure Email architecture based on Microsoft Certificate Services and Microsoft Certificate Lifecycle Manager. In this scenario Microsoft Certificate Services is configured to issue S/MIME encryption and S/MIME signing certificates. Microsoft Exchange is used as the messaging platform, while Microsoft Outlook is utilized as the email client. In this scenario, ILM’s management capabilities are being leveraged to enroll users with S/MIME certificates and to manage the certificates once they have been issued. In terms of certificate storage, the S/MIME certificates could either be stored locally on a user’s workstation or on a smart card alongside an authentication certificate.

In this scenario, once users have enrolled for their S/MIME certificates they are downloaded to their workstations using the ILM user portal. The S/MIME certificates can either be stored locally on their workstations or on Smart Cards if the level of assurance requires it. The S/MIME certificates are also published to Active Directory so that users can lookup public key information to encrypt emails for receiving parties. Once a user has been enrolled for a certificate they can access Microsoft Outlook email encryption and signing functionality (Outlook 2003 and Outlook 2007 both support this functionality if configured). Email that is encrypted or signed is sent in the S/MIME mail format and cannot be read by intermediary parties as it travels between the sender and the receiver.

The use of digital signatures applied to emails is intriguing in this scenario as it provides a business enabler that could be of significant value to an organization. Digital signatures allow for legal binding transactions to occur electronically. Digitally signed emails could be used for electronic orders, signing of contracts between organizations, or for communications that require non-repudiation of the sending party.

Digitally signed and encrypted email poses its own challenges from a certificate lifecycle management perspective. There are two that are unique to this scenario: how do you ensure that a certificate used for digital signatures is tightly bound to an individual’s identity, and how do you recover encrypted emails when a user’s certificate is revoked when they leave the organization.

The flexibility of ILM’s enrollment policies allows the first challenge to be easily addressed. ILM’s enrollment policies are flexible enough to provide high assurance binding of the digital identity represented by the certificate and their physical identity through a variety of different controls. First, enrollment policies may be configured to gather additional information on the registrant which can be verified against other corroborating datastores such as a human resources system or another employee database. Secondly, enrollment policies may be configured to required explicit approvals once registration information has been collected and approved. This can allow a checkpoint for procedural controls such as verifying the registrant’s Photo ID or other physical credentials. Thirdly, the enrollment policy can require that the user completes the registration process themselves and applies either a password to a digital signature certificate or a PIN to smart card requiring an additional authentication whenever the certificate is used for digital signing purposes.

The second challenge of recovering encryption emails can also be addressed through ILM’s recovery policy. This policy allows authorized individuals to recover certificates and utilize them to decrypt information stored in emails that have been encrypted by users that are no longer with the organization. Obviously, this recovery process must occur in a controlled manner and only by individuals authorized to do so. Constraints and limitations may be configured within the recovery process for this as well as additional information gathering to validate the identity of the individual invoking the recovery process as well as capturing information on why the recovery was required.

ILM’s management functionality provides an ideal platform to provision email encryption certificates as well as deal with the management challenges that are specific to Email encryption.

## High Availability Architecture

The requirement for a high availability ILM solution varies depending on the specific business requirement for certificate management or smart card management within a given organization. Since ILM is dependent on an underlying Active Directory and Certificate Services infrastructure a combined architecture including ILM can only achieve the overall availability of all combined components. In order to understand the impact of failure on the various components of an ILM implementation, it is first necessary to consider the interrelationship of the underlying components and how each component affects the overall availability of the system. In this section, the impact of the failure of each component will be identified in conjunction with redundancy, failover and recovery strategies for each component of the architecture.

**Active Directory** – ILM is highly dependent on Active Directory which acts as its repository for certificates, certificate templates, profile templates, and manager and subscriber groups. If Active Directory is unavailable then ILM will be unable to operate as will any network operation that is dependent upon Active Directory. Active Directory’s architecture is highly robust and redundant when implemented on multiple server grade machines with an Enterprise environment.

**Microsoft Certificate Services** – ILM is dependent upon Microsoft Certificate Services for all certificate related transactions including certificate enrollment, renewals, revocation and recovery. If Certificate Services is unavailable ILM will not be able to perform task involving certificate management. However, end users utilizing certificates will still be operational. High availability strategies for Certificate Services including running issuing certificate authorities on enterprise grade server equipment with RAID storage, redundant CPUs and power supplies. A regular backup regime should be implement to assist in recovery should catastrophic failure occur.

Windows Server 2008 Active Directory Certificate Services provides additional options for supporting a high-availability certificate authority infrastructure. Specifically, this is referred to as CA cluster support. CA clustering provides the capability to configure two certificate authorities in an active / passive cluster configuration – where the passive CA becomes active once the primary server fails. The secondary CA then has full access to the primary CA’s certificate store and can continue certificate operations. ILM provides the capability to utilize this functionality through its enhanced support for Windows Server 2008 32 bit Active Directory Certificate Services and CA module support for Windows Server 2008 32-bit. For additional information on CA cluster support available in Windows Server 2008, please refer to <http://support.microsoft.com/Default.aspx?id=946797>.

**ILM Portal** – The core of the ILM’s management interface which is available through the ILM portal is dependent on Microsoft’s Internet Information Server. The impact of an outage on the portal interface is that all ILM management and user portal functions would be unavailable for the duration of the outage. Certificate or smart card based functions occurring at the client level would remain unaffected. ILM’s architecture permits traditional high availability web server architectures including Round Robin DNS, Network Load Balancing Services (NLBS) Clustering, Web Clustering, or the use of a network appliance can be implemented to ensure the availability of ILM servers within a multiple ILM server deployment.

**SQL Server** – The ILM portal is dependent on Microsoft SQL Server for storing all certificate and smart card management data. A failure with the ILM database and/or the ILM server running IIS would render the ILM web portal inaccessible. While certificates could still be issued from the Issuing Certificate Authority they would have to be re-imported into ILM once the system was brought back online. Fortunately, ILM’s datastore can leverage high availability and recovery architectures typically used for SQL Server including clustering and transactional replication. SQL clustering uses a common IP shared by two or more servers (with common disk storage) to provides fault tolerance. In the event of failure of one SQL node, communications are automatically redirected to another functioning node in the cluster. Transactional Replication is a real time backup strategy where data is replicated from a primary SQL Server to a secondary SQL Server according to a defined interval. In the event of primary server failure, the ILM configuration would have to be manually reconfigured to point to the secondary SQL Server.

Each of the high available strategies identified above can be applied to an ILM environment, building on standard high-availability and redundancy techniques used in other Microsoft products. If an enterprise has already invested in a Microsoft high-availability infrastructure, then it is highly likely that ILM can leverage it for its own services.

# Benefits of a Microsoft ILM 2007 Approach

Microsoft ILM 2007 provides enterprise organizations with an integrated and comprehensive set of management tools that enable customers to address a range of business and technical challenges associated in deploying digital certificate and smart card based strong authentication solutions.

The certificate and smart card management capabilities of ILM 2007 were inherently designed to reduce the cost and complexities of deploying strong authentication technologies such as smart cards and digital certificates within a single integrated lifecycle management solution.

The key business benefits of using an ILM 2007 approach to deploying digital certificate and smart card based strong authentications include:

* **Compliance with Corporate Security Policies and Regulatory Requirements**

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 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.

* **Increased Operational Efficiency and Reducing the Help Desk Burden**

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.

* **Enhanced IT Security Infrastructure**

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.

The key technical benefits of using an ILM 2007 approach to deploying digital certificate and smart card based strong authentications 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.

* **Ability to Select the Correct Authentication Technology and Platform Vendor**

ILM 2007 provides a hardware-independent solution that has the flexibility to support a range of strong authentication technologies and platform vendors – as well as leveraging new technologies as they become broadly available – using a standardized interface to the smart card called Microsoft BaseCSP 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.

* **Provides Full Certificate and Smart Card Lifecycle Management**

While the use of digital certificates and smart cards provides an excellent approach to deploying stronger authentication over traditional username / password based systems, 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. ILM 2007 provides an integrated and comprehensive solution for the provisioning and full lifecycle management of digital certificates and smart cards. ILM provides the ability to apply policies against common certificate and smart card management tasks from any given certificate or grouping of certificates through the use of profile templates. Profile templates provide a common set of policies for certificate enrollment, renewal, update, recovery, revocation and retirement. In addition, specialized policies have been created to handle lifecycle management challenges related to the management of smart cards such as temporary issuance of smart cards, smart card duplication, personalization and retirement.

* **Flexibility to Meet a Organization’s 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 the flexibility to support a range of deployment scenarios and can be easily configured to use different workflows and approaches as an organization plans and continues to evolve their deployment.

* + **Leveraging Existing Microsoft Infrastructure**

ILM 2007 is tightly integrated with underlying Microsoft technologies including the two Windows Server components Certificate Services and Active Directory. ILM 2007 integrates with Certificate Services by acting as a higher-level management interface (commonly referred to as a Registration Authority or RA) between administrators and certificate services through the use of a ILM policy and exit modules. This allows ILM to perform all day to day certificate management tasks which would previously be performed through the Certificate Services MMC. Integration with Active Directory is supported by extending the schema to support ILM objects and permissions. This allows enterprises to leverage existing infrastructure to the fullest extent and to extend the functionality of their existing investment.

# Additional Resources

* See " Windows Vista Smart Card Infrastructure" White paper at <http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en>
* See "Enterprise Smart Card Deployment in the Microsoft® Windows® Smart Card Framework" - <http://www.microsoft.com/downloads/details.aspx?FamilyID=fa7ec97c-11be-4e53-a0c4-04719b6a7ab6&DisplayLang=en>
* See “Description of the software update for Base Smart Card Cryptographic Service Provider" ” at <http://support.microsoft.com/kb/909520>
* See " ILM Techcenter on Technet" for more documentation at <http://technet.microsoft.com/en-us/ilm/default.aspx>
* See ILM product page for more general information at <http://www.microsoft.com/ilm>
* See ILM 2 product page for information on the upcoming release of Identity Lifecycle Manager at http://www.microsoft.com/ilm2

1. BaseCSP -- Microsoft Base Cryptographic Service Provider. Additional information about Microsoft BaseCSP mini-drivers is provided in the Middleware section of this document. [↑](#footnote-ref-2)