



Identity Lifecycle Manager 2007

Gestion des certificats

*Version 1.0*

*Publication : Avril 2008*

*Auteur : Stéphane Metenier*

*Contributeurs : Philippe Beraud, Christophe Dubos*

*Copyright*

*© 2008* [*Microsoft Corporation*](http://www.microsoft.com)*. Tous droits réservés.*

**Objectif**

Ce document a pour but de présenter fonctionnellement et techniquement la solution *Microsoft Identity Lifecycle Manager* (ILM) dans sa version ILM 2007 *Feature Pack* (FP) 1 et pour la composante *Gestion des certificats*.

Il offre ainsi une vue d’ensemble aux acteurs de la sécurité et des systèmes d’information pour appréhender les services proposés par Microsoft en matière de gestion de supports cryptographiques de type cartes à puce ou clés USB.

Pour être exhaustive la lecture de ce document devrait être complétée par celle concernant la présentation de l’IGC Windows Server 2003 (R2).



*© 2008 Microsoft Corporation. Tous droits réservés.*

*Les informations contenues dans ce document représentent le point de vue actuel de Microsoft Corporation sur les sujets traités à la date de publication. Etant donné que Microsoft doit s’adapter aux conditions changeantes du marché, ces informations ne doivent pas être interprétées comme un engagement de la part de Microsoft, et Microsoft n’est pas en mesure de garantir l’exactitude de toute information présentée après la date de publication.*

*Ce document n’est fourni qu’à titre d’information. MICROSOFT NE DONNE AUCUNE GARANTIE EXPRESSE OU IMPLICITE DANS CE DOCUMENT.*

*Les autres noms de produits ou de sociétés cités dans ce document peuvent être des marques de leurs propriétaires respectifs.*

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • Etats-Unis*

Sommaire

[1. Synthèse 1](#_Toc195340370)

[2. Introduction 2](#_Toc195340371)

[2.1. Facilité de déploiement 2](#_Toc195340372)

[2.2. Facilité de gestion 2](#_Toc195340373)

[2.3. Flexibilité 3](#_Toc195340374)

[3. Présentation d’ILM 4](#_Toc195340375)

[3.1. Les composants d’ILM 5](#_Toc195340376)

[3.2. Les outils de développement 9](#_Toc195340377)

[3.3. Montée en charge 9](#_Toc195340378)

[3.4. Capacité d’extension 10](#_Toc195340379)

[4. Caractéristiques avancées 11](#_Toc195340380)

[4.1. Les modèles de profils ILM 11](#_Toc195340381)

[4.2. Rôles et Permissions 14](#_Toc195340382)

[5. Exemples de processus du cycle de vie 19](#_Toc195340383)

[5.1. Enrôlement d’un support cryptographique 19](#_Toc195340384)

[5.2. Activation d’un support cryptographique 21](#_Toc195340385)

[5.3. Demande / exécution d’un renouvellement de certificat 21](#_Toc195340386)

[5.4. Déblocage de code PIN en mode connecté 22](#_Toc195340387)

[5.5. Déblocage de code PIN en mode déconnecté 23](#_Toc195340388)

[5.6. Changement de code PIN 23](#_Toc195340389)

[5.7. Emission d’un support temporaire 23](#_Toc195340390)

[5.8. Révocation du support cryptographique 24](#_Toc195340391)

[5.9. Récupération de clé 24](#_Toc195340392)

[5.10. Circuit d’approbation par des gestionnaires 25](#_Toc195340393)

[6. Mise en œuvre 26](#_Toc195340394)

[6.1. Méthodologie 26](#_Toc195340395)

[6.2. Procédure d’installation d’ILM 30](#_Toc195340396)

[6.3. Coûts 33](#_Toc195340397)

[7. Conclusion 34](#_Toc195340398)

# Synthèse

Les sociétés ouvrent de plus en plus leurs réseaux pour faciliter l'accès des employés aux ressources et simplifier les interactions avec leurs clients et partenaires. Tandis que cet accès étendu permet d’accroitre la productivité, il présente également des défis significatifs en termes de sécurité et d’authentification des utilisateurs. Beaucoup d’organisations se rendent compte que les solutions traditionnelles basées sur le nom et le mot de passe utilisateur ne sont plus suffisantes pour sécuriser l'accès aux moyens et aux données sensibles de l’entreprise. Pour répondre à ces besoins, de nombreux éditeurs proposent aujourd’hui des solutions sophistiquées d'authentification telles que les cartes à puce avec certificats numériques embarqués.

Microsoft Windows Server 2003 fournit une plateforme complète à même de délivrer des moyens d’accès sécurisés par certificat numérique pour un ensemble de services, ainsi que l’utilisation de support cryptographique pour de l’authentification forte. Bien que les certificats numériques et les supports cryptographiques soient une excellente solution, ils peuvent introduire une complexité de gestion supplémentaire. Pour répondre à ses nouvelles problématiques de gestion, les administrateurs ont besoin d'un point central de gestion des certificats numériques et des supports cryptographiques simples à mettre en œuvre et à exploiter. Cette technologie doit être flexible, fonctionner naturellement avec l'infrastructure existante et avoir la capacité à intégrer une large variété de systèmes.

La solution *Microsoft Identity Lifecycle Manager* (ILM) 20007 *Feature Pack* (FP) 1 apporte une réponse à ces problématiques. Pour se faire, cette dernière est basée sur un ensemble de règles et de processus (*workflows*) qui aident les entreprises à gérer le cycle de vie des certificats numériques et des cartes à puce. ILM permet de baisser de manière significative les coûts liés à la gestion des certificats numériques et des cartes à puce en offrant aux organisations une solution efficace pour déployer, contrôler et maintenir une infrastructure basée sur des certificats. Dans le même temps, elle améliore également l'approvisionnement, la configuration et la gestion des certificats numériques et des cartes à puce, tout en augmentant la sécurité par l’implémentation d’une technologie d'authentification forte et multi-facteurs.

La solution ILM a été conçue sur le principe que chaque entreprise est unique, et a donc des contraintes de sécurité et d’administration uniques. ILM est de ce fait flexible, notamment grâce à un modèle à base de workflows autorisant une configuration par règles du processus d’authentification. Un autre avantage d’ILM est qu’elle prend en compte la gestion du déploiement et du cycle de vie des certificats numériques avec ou sans cartes à puce. Pour les sociétés qui déploieraient ILM sans cartes à puce et décideraient plus tard de les ajouter, ILM peut faciliter cette migration sans ajout d'autres composants.

Les cartes à puce peuvent alors être gérées en tant qu'élément du même ensemble - y compris pour fixer les conditions d’authentification, et d’utilisation par des applications de type messagerie ou bien réseau privé virtuel (VPN) et autres exigences d'entreprise. Les fonctionnalités de gestion fournies par ILM prennent en compte la gestion des stocks, l’enrôlement des cartes, le recouvrement, le déverrouillage et autres processus nécessaires à la réussite d’un déploiement à grande échelle.

# Introduction

La solution ILM apporte un système de gestion à même de garantie de la fiabilité des données d’identités numériques afin de maximiser la confiance et la flexibilité associées à l’utilisation des certificats numériques au format X.509 v3 et des cartes à puce (sous différents facteurs de forme) en fournissant des moyens de gestion avancés sur Windows Server 2003. ILM simplifie les processus administratifs exigés pour assurer la confiance et permettre la distribution des certificats et des cartes d'une façon sécurisée et structurée. Le résultat est une solution hautement configurable et robuste d'enregistrement et de gestion qui permet un déploiement simplifié, une administration efficace et une flexibilité accrue.

## Facilité de déploiement

ILM est la seule solution de gestion de certificats basée sur la plateforme Windows qui fournisse un déploiement clé en mains et conçu pour n'exiger aucun développement pour sa mise en œuvre au sein des organisations même les plus complexes. ILM simplifie le déploiement de certificats numériques et de supports cryptographiques dans l’entreprise en capitalisant sur les services présents tels que l’annuaire Active Directory et en étendant les services de certification de Windows Server 2003, fournissant ainsi au final une solution intégrée de sécurité.

ILM est également capable de facilement évoluer en même temps que l’organisation et de s’adapter sans exiger de modification profonde du logiciel. Telle une application Web classique, ILM est composée de différents éléments : une base de données, des composants métier et une couche de présentation (Web). Ces couches peuvent être placées sur des serveurs physiquement séparés et suivant diverses combinaisons, maximisant la flexibilité de déploiement et l’adaptabilité. De plus, les technologies comme la répartition de charge, les services de clusterisation peuvent être employées pour faciliter la montée en charge et/ou la disponibilité.

## Facilité de gestion

ILM procure une gestion Web par workflows qui prend en compte aussi bien les besoins des utilisateurs que des administrateurs. De plus, cette technologie diminue le coût total des IGC et de support cryptographique en apportant des outils qui automatise les fonctions d’administration classiques et autorise les utilisateurs à exécuter eux-mêmes les taches d’administration quotidiennes.

En simplifiant les processus administratifs requis pour établir la confiance, ILM prend en charge la distribution d’une manière sécurisée et structurée. Les apports fonctionnels d’ILM sur Windows Server 2003 (R2) facilitent l’administration, pour une même entité externe (en agrégé EE) ou porteur, de multiples certificats, tirés (éventuellement selon le modèle de déploiement) de multiples autorités de certification (en abrégé AC ou CA pour *Certificate Authority* en anglais) ainsi que des certificats pour les postes clients et périphériques.

Pour réduire la charge d‘administration, ILM apporte un portail Web de libre-service pour les demandeurs souscripteurs et les gestionnaires ainsi que la génération de cartes temporaires pour les collaborateurs ayant oubliés leur carte, lorsque des supports cryptographiques sont utilisés en conjonction.

ILM fournit une solution permettant de mettre à jour l’information contenue dans un support cryptographique, ajouter un nouveau gabarit de certificat, renouveler des certificats et effectuer des fonctions de gestion d’applet de manière transparente et flexible.

ILM inclut aussi des fonctions de personnalisation et gère les applets nécessaires pour communiquer avec les différents types de supports cryptographiques, permettant aux sociétés de personnaliser les cartes à puce durant le processus d’enrôlement et de simplifier ainsi le processus global de déploiement.

## Flexibilité

ILM offre une grande flexibilité en apportant aux administrateurs les moyens de modifier les processus de gestion des certificats et des supports cryptographiques et d’adapter ILM à leurs contraintes organisationnelles et leur infrastructure.

ILM constitue une solution intégrée qui fournit une gestion simplifiée et facilite l’adoption par les utilisateurs grâce à l’utilisation des règles de gestion automatiques.

ILM est conçue sur le principe que chaque entreprise est unique et possède de fait des contraintes de sécurité et de gestion uniques. L’enregistrement de certificats varie de façon importante d’une organisation à une autre et ILM a été conçu pour adresser ce challenge en apportant une infrastructure de gestion et d’enregistrement de certificats utilisable dans tous les cas.

Le reste de ce document explore, d’un point de vue technique, le rôle d’ILM au sein d’une IGC comme autorité d’enregistrement (en abrégé AE) et comme système de gestion de supports cryptographiques (en abrégé CMS pour *Card Management System* en anglais) en abordant :



* L’architecture rendant les bénéfices cités possibles ;
* Les applications avec lesquelles ILM interagit ;
* Comment les rôles et les permissions peuvent être gérés de façon centralisée ;
* Le rôle d’ILM dans le cycle de vie d’un certificat et d’un support cryptographique.

# Présentation d’ILM

ILM apporte des fonctions de gestion évoluées aux AC basées sur les services de certificat de Windows Server 2003 (R2) (en mode entreprise) en agissant comme un intermédiaire administratif de type AE.

Une fois mis en œuvre, tout ou partie des fonctions de gestion de certificat et de support cryptographique peut être pris en charge par ILM.

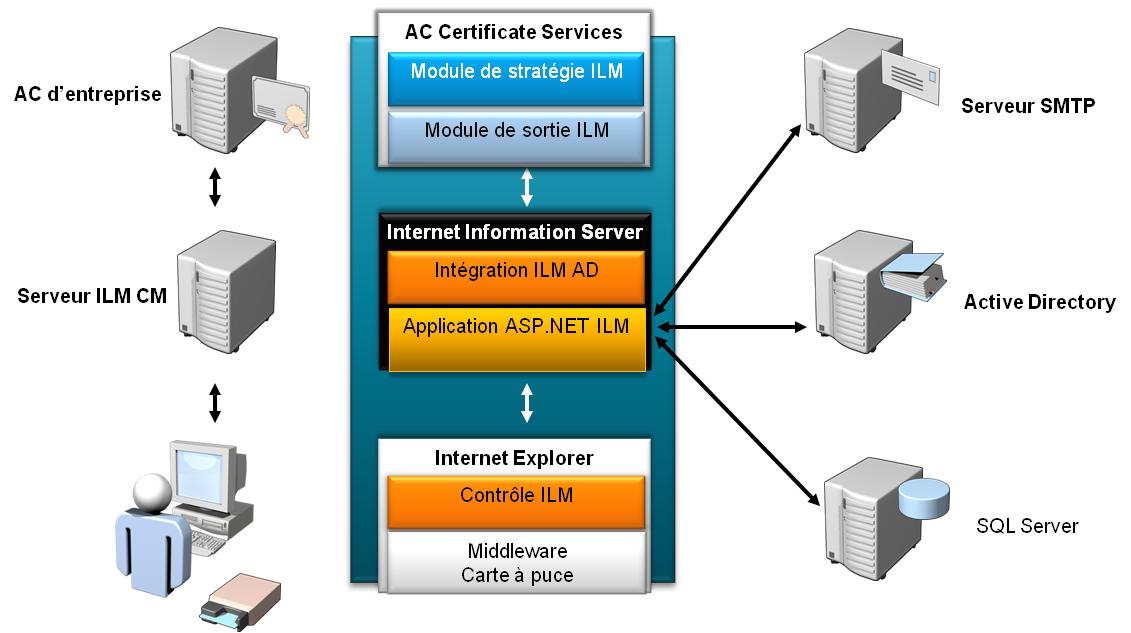
****

Figure 1 : Architecture d'ILM 2007

Cette architecture met en œuvre une solution logicielle basée sur 3 composants de haut niveau :



1. *Composants ILM côté serveur* **-** Le serveur ILM peut être mis en œuvre sous forme d’un serveur dédié ou bien peut être partagé avec la plateforme d’une AC ou peut être partagé avec d’autres applications. Le serveur fournit une interface et est le point focal des fonctions administratives. Il est responsable de l’implémentation de toutes les fonctionnalités d’ILM, de la communication avec la base de données (qui peut être dissociée), de la communication avec Active Directory et avec toutes les autres AC. Utiliser cette approche apporte au client une gestion riche du certificat pour une AC donnée, de même qu’une vue globale de l’ensemble des AC potentiellement présentes au sein de l’organisation.
2. *Modules ILM pour l’AC* **-** Pour gérer activement une AC, un module de stratégie (*policy module* en anglais et un module de sortie (*exit module* en anglais) ILM doivent être installés et configurés localement sur chaque AC. Ces modules communiquent avec le serveur ILM, contrôlent le comportement de l’AC et fournissent des journaux d’évènements et des audits complets de façon centralisée.
3. *Composants ILM côté client* **-** Le client ILM permet aux utilisateurs et aux administrateurs de gérer les cartes en apportant les interfaces entre les clients et les cartes.

Il comprend les éléments suivants :

1. *Smart Card Self Service Control*, qui fournit des fonctionnalités de gestion des certificats,
2. *Smart Card Personalization Control*, qui apporte l es fonctions de gestion des cartes,
3. *Bulk Smart Card Issuance Tool*, qui est une application pour les scenarii de déploiement centralisé à grande échelle de supports cryptographiques.

Les échanges entre chacun des composants de la solution ILM sont résumés dans le schéma suivant :

Figure : Schéma des échange entre les différents composants



## Les composants d’ILM

Les éléments d’un déploiement d’ILM consistent en au minimum un serveur ILM et une AC basée sur les services de certificat de Windows Server 2003 (R2) en mode entreprise.

Il est possible qu’un seul serveur ILM gère de multiple AC simultanément ou que plusieurs serveurs ILM gèrent une seule AC. Le serveur ILM est constitué d’un serveur Windows 2003 et agit comme intermédiaire administratif des AC. Ce serveur propose une interface Web simple à utiliser reposant sur un moteur d’application et intégrée à Active Directory et aux services de certificat. L’ensemble des informations de configuration est stocké dans une base de données SQL Server accessible par le serveur ILM et les modules de l’AC.

ILM est constituée de différents composants fonctionnels, chaque composant étant lui-même constitué de modules principaux. Ces composants fonctionnels sont :



* Une ou plusieurs AC basées sur les services de certificats de Windows Server 2003 (R2) en mode entreprise ;
* Les composants ILM côté serveur ;
* Les demandeurs et gestionnaires de certificat (via Microsoft Internet Explorer) ;
* Les supports cryptographiques (disponibles auprès de partenaires).

### IGC Windows

ILM agit comme une AE auprès d’AC basées sur les services de certificats de Windows Server 2003 (R2) en mode entreprise au sein d’une même forêt Active Directory. Le livre-blanc « Présentation de l’IGC Windows Server » corolaire de ce document offre une vue d’ensemble de ces services.

Pour se faire, ILM doit interagir et contrôler le comportement de l’AC, apportant ainsi une plus grande flexibilité et capacité d’administration. Ceci est réalisé via l’installation sur la ou les AC concernés d’un module de stratégie matérialisant une politique de certification, et d’un module de sortie permettant de publier notamment les certificats tirés.

### Les composants ILM côté serveur

Les composants ILM côté serveur comprennent un serveur d’application Web et une base de données relationnelle, Microsoft SQL Server. ILM n’impose pas un serveur SQL dédié, mais nécessite Windows Server 2003 et Microsoft Internet Information Server (IIS). Il peut être installé sur un serveur dédié ou celui hébergeant la base de données, dans ce cas le programme d’installation d’ILM créera automatiquement les bases de données appropriées. ILM est une application ASP.NET 2.0 reposant sur le Framework .NET qui devra être installé sur la plateforme. L’installation du Framework .NET 2.0 peut être réalisée de manière indépendante.

La solution ILM a été conçue pour s’intégrer étroitement avec Windows Server 2003 (R2) et Active Directory. Le but est de fournir des fonctions puissantes et fortement personnalisables de gestion de certificat, tout en maintenant une homogénéité des systèmes d’exploitation et utiliser leurs services quand cela est possible. Cette combinaison fait la démonstration flagrante de la valeur grandissante des services de certificats numériques en entreprise et ILM augmente cette valeur.

En plus du serveur ILM central, les capacités de gestion de supports cryptographiques comprennent deux composants principaux : un composant serveur intégré à l’application Web ILM et un client intégré au butineur Web utilisant le middleware du support à puce pour exécuter des actes de gestion.

Les composants serveur d’ILM fournissent diverses interfaces Web accessibles en fonction des permissions Active Directory. Ces interfaces comprennent portail web demandeur et un portail web gestionnaire.

Les composants serveur n’accèdent pas directement au support cryptographique, mais à la place fournissent les processus métiers et l’espace de stockage de l’information nécessaire au module de support cryptographique et à l’interaction avec le reste du système. Les composants serveur sont aussi responsables de la génération des workflows client et des interfaces web utilisateur.

Ces composants comprennent :

1. *Le portail Web « Demandeur »* - C’est le composant du serveur ILM qui interagit directement avec les demandeurs de certificat dans un mode libre service. Cette fonctionnalité utilisateur est basée sur leurs groupes et permissions Active Directory. Les permissions sont configurées en utilisant Active Directory et ses outils de gestion des permissions préalablement étendus pour inclure les permissions propres à ILM.
2. *Le portail Web « Gestionnaire »* - Ce composant interagit avec les gestionnaires de certificats et propose des fonctionnalités utiles pour gérer des certificats utilisateur. Les permissions des gestionnaires sont données en utilisant les outils de gestion de la sécurité d’Active Directory.

### Les demandeurs et gestionnaires de certificat

Internet Explorer fournit l’accès nécessaire à l’environnement ILM. Comme ILM utilise SSL/TLS pour l’ensemble du trafic d’administration des certificats, l’application est dépendante du butineur. De plus, l’application utilise du script avancé optimisé pour Internet Explorer versions 5, 6 et 7.

ILM ne nécessite aucun logiciel client pour la gestion de certificat logiciel.

ILM nécessite un composant client optionnel accessible via Internet Explorer pour des déploiements de certificats sur support cryptographique.

### Les supports cryptographiques

ILM supporte aussi des fonctionnalités de gestion avancées via un module Web côté client apportant les caractéristiques suivantes:

* Des fonctions complètes de gestion de code PIN (*Personal Identification Number* en anglais) incluant le déverrouillage et gérées de façon autogéré ou par un utilisateur fonctionnel ;
* Des capacités complètes de rapport et d’audit sur toutes les taches du cycle de vie du certificat ;
* Un système d’inventaire qui se met à jour sur activation du support, simplifiant la distribution initiale de carte ;
* Des processus de déploiement hautement flexible qui utilisent les processus et relations existantes dans l’entreprise ;

ILM supporte l’utilisation et le déploiement de support cryptographique type carte à puce, en s’appuyant sur la disponibilité des éléments suivants :

* Un support cryptographique supporté,
* Un lecteur de support cryptographique supporté,
* Certains middlewares PKCS #11 ou un fournisseur de services cryptographiques (CSP) pour CryptoAPI.

Le support doit disposer d’un lecteur supporté par la plateforme Windows. Cette dernière supporte PC/SC v1.0 (<http://www.pcscworkgroup.com/specifications/specdownloadV1.php>) du PC/SC Workgroup.

Par ailleurs, Windows Vista comporte en standard un pilote USB-CCID (<http://www.microsoft.com/whdc/device/input/smartcard/USB_CCID.mspx>); ce qui signifie que tout lecteur carte à puce USB conforme USB-CCID, ne nécessite pas l’installation d’un pilote additionnel. Ce pilote est également disponible sur Windows Update pour Windows 2000, Windows XP et Windows Server 2003.

Un lecteur de carte à puce et le pilote correspondant doivent se conformer au programme logo WHQL (<http://www.microsoft.com/whdc/whql/device/smartcard.mspx>) pour obtenir le « *Windows Logo for the Smart Card Reader* » et être rendus disponibles sur Windows Update.

 ILM 2007 supporte les middlewares PKCS#11 suivants ;

* Axalto Client Software (ACS) v 5.2,
* Gemplus GemSafe v4.2,
* AET SafeSign v2.1,
* Aladdin eToken RTE 3.6,
* Siemens HiPath SIcurity Card v3.1.026.

Ainsi que les mini-pilotes pour le CSP Microsoft Base Smart Card générique.

A ce titre, il convient de noter que la prise en compte d’un support suppose historiquement de disposer du CSP (monolithique) pour ce support. L’infrastructure carte à puce de la plateforme Windows (en abrégé WSCF pour *Microsoft Windows Smart Card Framework* en anglais) a vu l’introduction d’un CSP Microsoft Base Smart Card générique et d’un modèle à base de mini-pilotes pour les cartes à puce de façon à faciliter la prise en compte de nouveaux supports.

* + Le CSP Microsoft Base Smart Card est disponible sous forme de téléchargement gratuit et optionnel pour Windows 2000 SP4, Windows XP SP2, Windows 2003 Server SP1 sur le site Microsoft (<http://go.microsoft.com/fwlink/?LinkId=93341>). Il est présent nativement sur Windows Vista et Windows Server 2008.

La définition d’un mini-pilote pour un support demande un investissement limité, offre des bénéfices significatifs en termes de performances, de mécanismes de cache de données et de PINs, etc.

Après qualification et certification par le *Microsoft Smart Card Comptency Center* (en abrégé SCCC) (Cf. « Smart Card Minidriver Certification Requirements », <http://www.microsoft.com/whdc/device/input/smartcard/sc-minidriver_certreqs.mspx>), un mini-pilote peut être diffusé sur Windows Update. L’ensemble des fournisseurs proposent ou sont sur le point de proposer des mini-pilotes pour leur(s) carte(s).

La plateforme Windows est agnostique au système d’exploitation du support (Java Card, .NET, MultOS, etc.) à partir du moment où un module cryptographique (CSP monolithique « legacy » ou mini-pilote) est disponible. Pour information, voici quelques mini-pilotes actuellement disponibles

* ActivIdentity,
* Aladdin eToken,
* Athena ASECard et ASEKey,
* DNP (Dai Nippon Printing) lhPKI Card,
* Gemalto .NET Smart Card,
* G&D Sm@rtCafe Expert 2.0 Java Card,
* HID Crescendo Smart Card,
* Oberthur Card System IDOneClassic,
* Spyrus Rosetta Smart Card Series II.
  + La liste complète courante est disponible à l’adresse Internet <http://test.catalog.update.microsoft.com/v7/site/Search.aspx?q=umdf>.

## Les outils de développement

ILM est conçu pour être personnalisable et extensible. Les extensions peuvent être développées en utilisant tous les outils qui supportent l’infrastructure .NET tel Microsoft Visual Studio 2008, pour ne citer que la dernière version en date.

## Montée en charge

ILM est capable de s’adapter à la charge sans aucune modification logicielle. ILM est une application Web composée de plusieurs couches : une base de données, des composants métiers et une partie présentation (Web). Ces couches peuvent être placées physiquement sur des serveurs différents suivant diverses combinaisons.

Les technologies de répartition de charge (*Network Load Balancing* en anglais), de clustering peuvent être utilisées pour faciliter la montée en charge et/ou la disponibilité d’ILM. Les modules de stratégie et de sortie doivent être installés sur les AC et ne peuvent pas en être séparés.



Figure : Exemple d’implémentation en haute disponibilité

## Capacité d’extension

Le processus de gestion du cycle de vie des certificats peuvent varier fortement d’un contexte à un autre, rendant difficile le développement d’une solution packagée répondant à l’ensemble des besoins métiers. ILM est conçue pour adresser ce challenge en apportant une infrastructure de gestion et d’enregistrement de certificat documentée utilisable de différentes façons suivant les besoins. En plus, ILM est commercialisée avec une application portail Web complète exploitant cette infrastructure pour fournir une implémentation de gestion et d’enregistrement de certificats sur les services de certificat de Windows Server 2003 (R2).

# Caractéristiques avancées

ILM repose sur trois composants technologiques principaux pour réaliser les fonctions de gestion : Active Directory, AC basée sur les services de certificat de Windows Server 2003 (R2) en mode entreprise et les supports cryptographiques (si nécessaire).

La fonctionnalité principale d’ILM est de faire inter-opérer de façon transparente ces trois composants pour toutes les taches de gestion liées au cycle de vie complet des certificats numériques et des supports cryptographiques dans un environnement d’entreprise.

## Les modèles de profils ILM

Un modèle de profil constant la pierre angulaire pour toutes les activités de gestion au sein de la solution ILM.

Le but d’un modèle de profil est de fournir une interface d’administration unique incluant toutes les informations nécessaire pour gérer le cycle de vie des différents certificats utilisables par une population d’utilisateurs.

Un modèle de profil contient aussi l’information associée à la destination finale de ces certificats, et pouvant être logiciels (stockés sur le poste de travail) ou matériels (stocké sur un support cryptographique).

Dans le cas où les certificats sont stockés sur support cryptographique, un modèle de profil ILM est aussi configuré avec les informations nécessaires pour gérer le support cryptographique en tant que tel et apporte ainsi un point unique d’administration pour le support cryptographique et les certificats.

Un modèle de profil peut contenir un ou plusieurs gabarits de certificats gérés comme un seul élément. Sans cette approche, une organisation est obligée de gérer les multiples certificats utilisateurs de façon séparée, ce qui est plus onéreux et source d’erreur. Un modèle de profil autorise le déploiement de certificats d’authentification et de chiffrement en une seule étape.



Figure : Les modèles de profil ILM

ILM est aussi capable de gérer différemment les certificats d’authentification et de chiffrement dans le cas où les clés privées des certificats de chiffrement doivent être mises sous séquestre pour un recouvrement éventuel futur. Par exemple, lorsque l’on demande à ILM de récupérer un profil particulier suite à la perte d’une carte, l’application génère de nouveaux certificats authentification mais récupère les certificats de chiffrement existants (avec les clés associées). Dans le même temps, ILM gère les détails administratifs associés à l’initialisation du support.

La Figure 4 montre la configuration générale d’un modèle de profil et les différents éléments de configuration. Il permet la spécification d’un modèle de profil de type logiciel ou matériel (support cryptographique). ILM permet l’ajout ou la suppression de gabarits de certificats. Ces modèles sont lus directement à partir d’Active Directory depuis la partition de configuration et sont générés par des AC déterminées.

Si besoin est, les gabarits de certificat individuel peuvent même être publiés par différentes AC. Généralement, un ensemble de gabarits de certificat contient une combinaison de certificats de signature/authentification et de certificats de chiffrement.

Si le modèle de profil est configuré pour supporter l’utilisation de cartes à puce, alors les détails de gestion du support physique peuvent être fournis. Certains détails sont présentés dans la Figure 5 tel le fournisseur du support, les paramétrages du support ainsi que les règles de génération du code PIN utilisateur et administratif.



Figure : Configuration d’un modèle de profil de type support cryptographique

Le modèle de profil inclus la configuration des règles de gestion utilisées pour gérer le profil déployé.

Ces processus de gestion comprennent :

* La duplication (pour les profils),
* L’enrôlement,
* La mise à jour en ligne,
* La récupération (remplacement),
* La récupération par procuration,
* Le renouvellement,
* La suspension et réactivation,
* La désactivation,
* La révocation,
* L’émission de support temporaire,
* Le déverrouillage (pour les profils).

Chacun de ces processus peut être configuré séparément ainsi le profil peut-il gérer de manière différente l’enrôlement, la récupération ou le renouvellement. De façon à permettre aux organisations une grande liberté de choix dans la mise en œuvre de ces taches.

Chaque workflow peut nécessiter des saisies d’informations via des formulaires Web et de les stocker ou de les valider dans d’autres sources de données. Cette configuration est effectuée dans l’application de gestion et ne nécessite aucun développement complémentaire.

En outre, il peut aussi être défini des mécanismes d’approbation, de distribution des informations et des mots de passe à usage unique (en abrégé OTP pour *One-Time Passwords* en anglais) par mèls. L’ensemble de ces informations est saisi et configuré au niveau du profil. Une fois complété, le profil est simplement mis en œuvre et ILM applique les règles, le workflow et les permissions qu’il définit.

La présente un exemple de modèle de profil ILM.

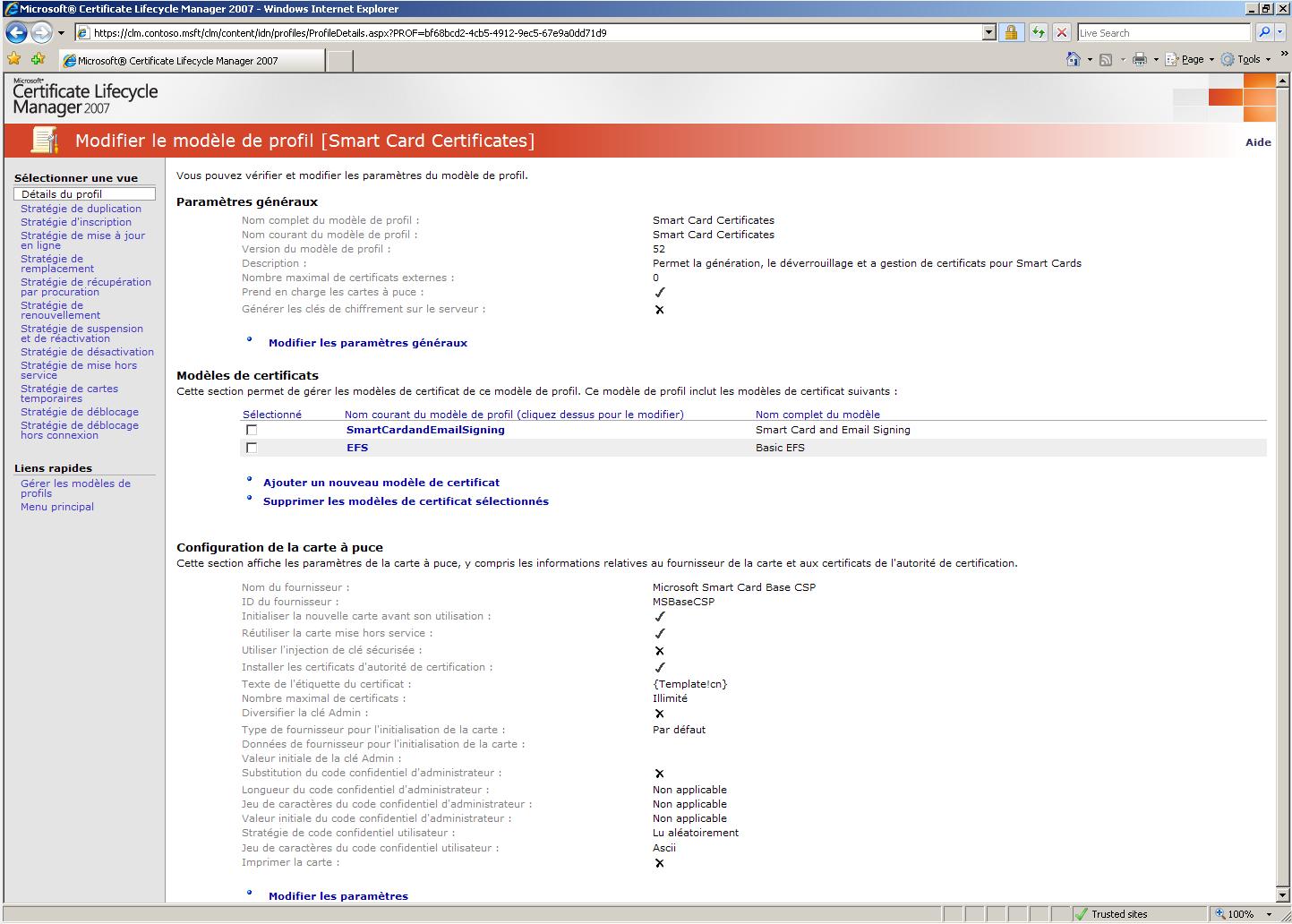
****

Figure 6 : Modèle de profil ILM pour un support cryptographique

## Rôles et Permissions

Une solution de gestion de certificats et de supports cryptographiques flexible demande une délégation des responsabilités et donc une gestion des rôles flexible et des permissions granulaires.

Les rôles déterminent les permissions au sein du système qui définissent les possibilités d’accès aux différentes fonctions de gestion des certificats, de même que les permissions pour configurer ILM. Pour ce faire, ILM s’appuie sur Active Directory et l’étend pour y inclure les permissions propres à ILM.

L’intérêt d’une telle approche est l’exploitation d’une infrastructure existante pour gérer les utilisateurs et les permissions pour le déploiement de certificats et de supports cryptographiques plutôt que de repartir de zéro et d’en construire une spécifique.

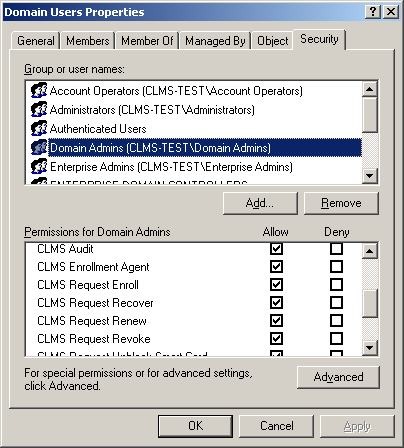


Figure 7 : Gestion des permissions via des profils Active Directory

Les gestionnaires de certificats reçoivent leurs permissions d’accès au système en fonction de leur appartenance aux groupes et des droits définis dans Active Directory. Les permissions sont configurées en utilisant Active Directory et les outils de gestion de permission étendues incluant les permissions ILM.

D’un point de vue global, le déploiement de certificat et de support cryptographique possède au minimum deux rôles: les demandeurs et les gestionnaires. Les demandeurs sont simplement les utilisateurs qui ont besoin de certificats avec ou sans support cryptographique. Les gestionnaires sont des utilisateurs ayant des permissions dans ILM pour soit administrer d’autres utilisateurs soit pour administrer l’application elle-même. Comme le système de permission d’ILM utilise les groupes Active Directory, il permet une grande flexibilité au niveau de la délégation de la gestion de l’application et des utilisateurs.

### Les demandeurs

Un demandeur est un utilisateur qui a besoin de certificats et, le cas échéant, d’un support cryptographique associé. Cet utilisateur peut nécessiter un certificat numérique pour des usages tels que de l’authentification par support cryptographique, l’accès sécurisé à un réseau sans fil, la messagerie sécurisée, des services VPN ou pour toutes applications faisant appel à une infrastructure de gestion de clés publiques (IGC). L’objectif d’ILM est de rendre la gestion de ces certificats (et du support) aussi simple que possible pour les utilisateurs tout en apportant aux organisations le niveau de sécurité approprié.

ILM fournit un portail Web pour les demandeurs contenant des fonctions spécifiques en mode libre-service. Les fonctions de libre-service permettent aux organisations de diminuer les coûts d’administration. Cependant, l’accès en libre-service à certaines fonctions peut aussi comporter des risques en termes de sécurité.

ILM gère donc cela en permettant aux organisations de définir quelles fonctions seront disponibles en libre-service et lesquelles ne le seront pas. Cela se paramètre via les modèles de profil individuels et via les groupes utilisateurs, ce qui signifie qu’un type de profil peut être géré en libre-service alors qu’un autre ne le sera pas.

Toutes les fonctions de workflows sont intégrées au système de messagerie du portail Web pour la notification et à la distribution automatique de l’information d’authentification et d’approbation (si souhaité).

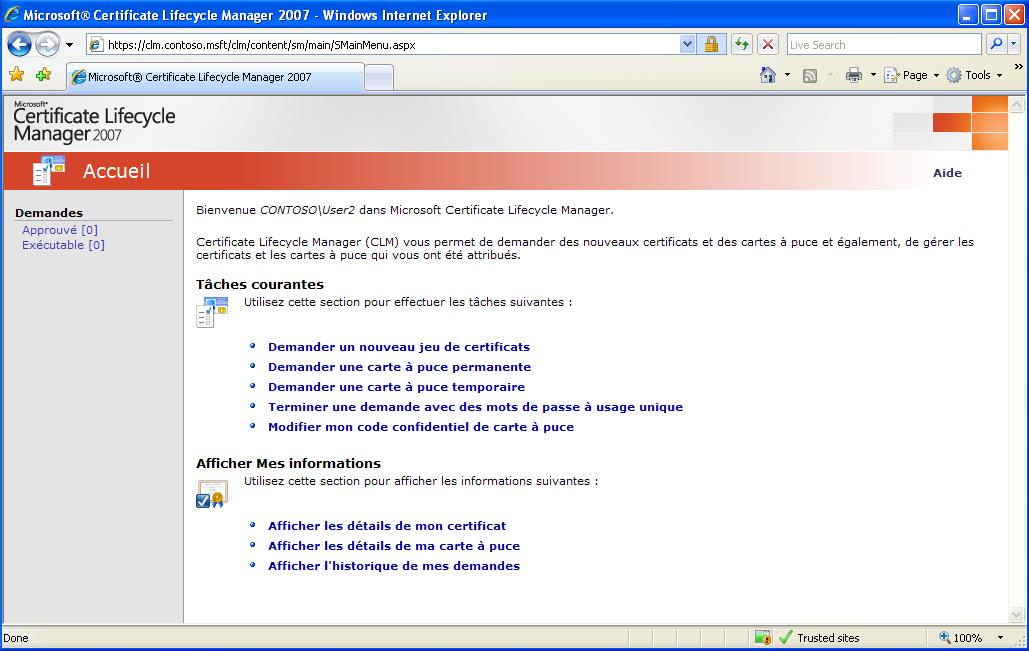


Figure 8 : Portail Demandeurs

La présente une configuration classique du portail demandeur. A partir de ce portail, il est possible pour les demandeurs de voir et de gérer leurs certificats et cartes à puce (selon la configuration et les règles paramétrées). Cela inclus aussi la possibilité de demander ou de d’activer un support cryptographique.

L’exécution de la demande dépend du modèle de profil. Les workflows permettent de prendre en compte différents types de demandes, à titre d’exemple une demande peut être complétée automatiquement ou nécessiter potentiellement l’approbation du groupe de personnes (ex. cellule d’assistance) ou d’une personne désignée comme le responsable du demandeur.

### L’authentification utilisateur

ILM peut utiliser divers mécanismes d’authentification pour le portail des demandeurs et gestionnaires. Parce-que ILM s’appuie sur Active Directory pour déterminer les permissions des accédants, l’utilisateur doit au final s’authentifier sur le portail avec son compte de domaine.

ILM peut être configuré pour utiliser l’authentification intégrée, dans ce cas l’utilisateur peut simplement naviguer sur le portail ILM et si l’utilisateur est authentifié au sein d’un domaine Active Directory, il ne lui sera pas demandé de s’authentifier de nouveau.

D’autres options peuvent aussi être utilisées, telle l’authentification basique (nom et mot de passe) ou l’authentification par certificat/support cryptographique (ou CAC pour *Client Authentication Certificate* en anglais), si désiré.

Le point le plus important de cette approche est qu’ILM ne nécessite pas de base de données supplémentaire pour les utilisateurs, les mots de passe et les permissions. Il est possible de définir un groupe d’utilisateurs, comme une cellule d’assistance, avec des droits d’accès à ILM en donnant simplement les permissions appropriées à ce groupe dans Active Directory. Le reste est pris en charge de façon totalement transparente par le système d’exploitation et Active Directory.

### Les gestionnaires

Un gestionnaire est une personne qui a les permissions d’accéder au portail gestionnaire d’ILM (Cf. ). Ce portail se situe sur le même serveur que le portail demandeur mais présente des fonctions de gestion des autres utilisateurs et de configuration. Les permissions sont données à un gestionnaire de certificat avec les outils classique de gestion de la sécurité d’Active Directory.

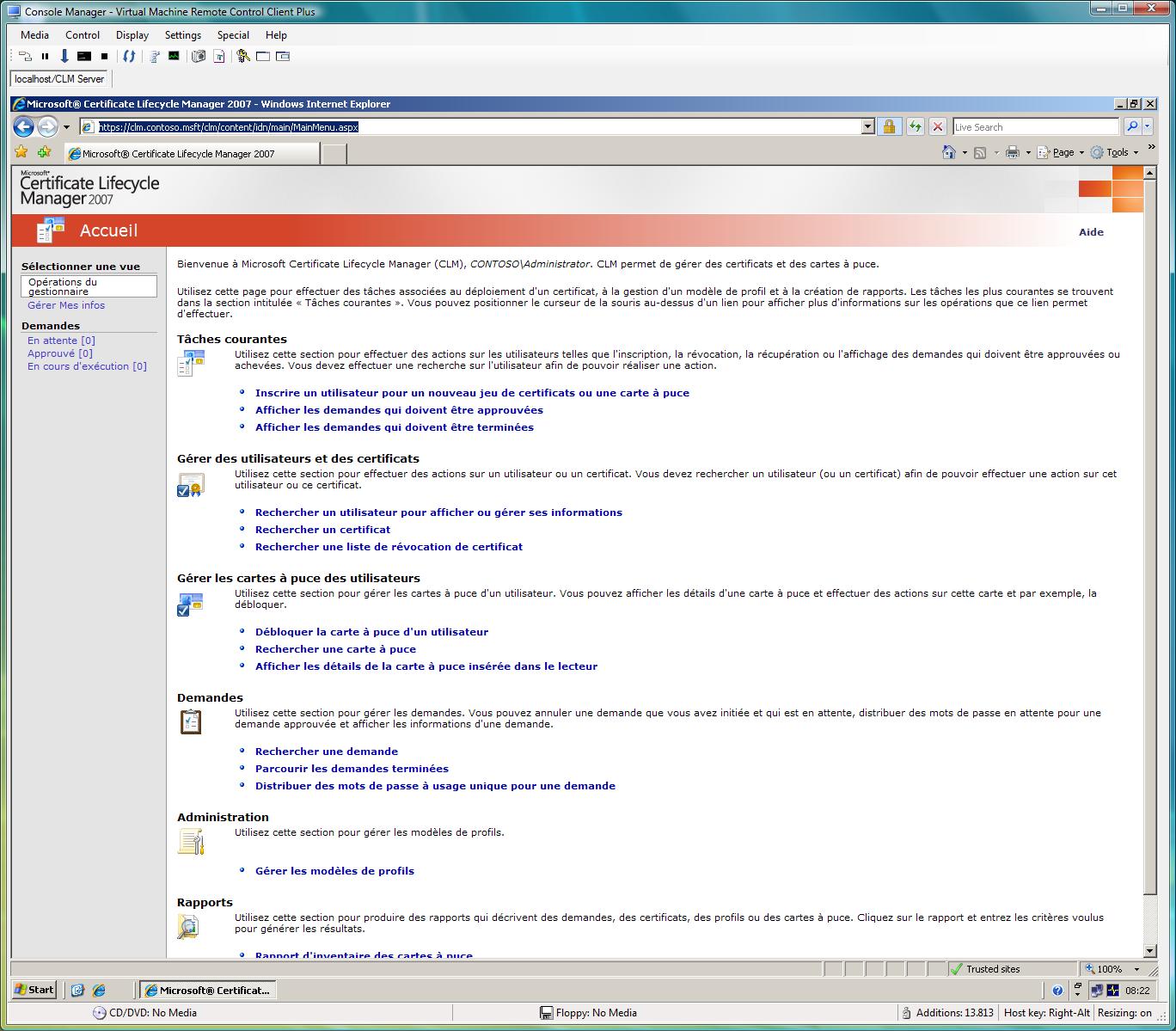


Figure 9 : Portail Gestionnaire

Concrètement, les utilisateurs doivent avoir reçu l’accès à ILM et sont alors autorisés à accéder aux fonctions spécifiques comme l’enrôlement, la récupération ou la révocation. Au final, ils ont reçu les permissions pour gérer un groupe donné ou des groupes d’utilisateurs. Une plus grande granularité est possible en autorisant la gestion de gabarits de certificat particuliers tout en restreignant les autres fonctions de gestion.

Les gestionnaires peuvent aussi avoir les permissions d’approuver les demandes de certificat d’autres gestionnaires ou d’utilisateurs ayant auto-émis des demandes. Ces demandes sont accessibles de manière très simple via le portail Web, et couplées à l’envoi de mèls. Les fonctions de journalisation et d’audit sont disponibles pour suivre les activités et pour effectuer l'analyse et la vérification de l’utilisation des fonctions d’administration des certificats et cartes à puce. Puisque l’audit est une permission spécifique dans ILM, il est possible de configurer un rôle utilisateur dédié à la génération de rapport et incapable d’exécuter une quelconque fonction de gestion de certificat.

# Exemples de processus du cycle de vie

Les opérations prisent en compte pour les supports cryptographiques et le cycle de vie d’un certificat sont les suivantes :

* Enrôlement d’un support cryptographique ;
* Activation un support cryptographique ;
* Demande / exécution d’un renouvellement de certificat ;
* Déblocage de code PIN en mode connecté ;
* Déblocage de code PIN en mode déconnecté ;
* Changement de code PIN ;
* Emission d’un support temporaire ;
* Révocation du support cryptographique ;
* Récupération de clé ;
* Circuit d’approbation par des gestionnaires.

## Enrôlement d’un support cryptographique

Ce processus d’initialisation du support peut inclure plusieurs étapes, y compris mettre à jour dans la base de données des cartes son numéro de série, changer le code PIN de déverrouillage, définir le code PIN utilisateur, déterminer le nom complet de l’utilisateur (*Distinguished Name* en anglais), créer la demande de certificat, etc. Le processus de gestion de certificat peut alors être configuré pour exiger des actions du gestionnaire ou une approbation

ILM met à disposition des interfaces web permettant de définir le processus de distribution des supports cryptographiques et ce par type de population.

ILM supporte toutes les politiques de distribution du support cryptographique (classé par ordre de sécurité croissant) :

* Libre-service ;
* Déléguée ;
* Centralisée ;
* Face-à-face.



Figure : Exemples de scénarii de remise de support cryptographique en face-à-face

Ces différentes politiques peuvent être mixées pour s’adapter à des populations et/ou des situations particulières.

ILM est suffisamment souple pour pouvoir s’adapter aux différents scenarii et aux populations citées.

Nous pouvons ainsi imaginer les processus métiers suivants avec ILM :

* Les utilisateurs du système d’information, authentifiés par leur compte Windows, accèdent sans se ré-authentifier au portail libre-service d’ILM. De là, ils peuvent avoir accès à un processus de demande d’attribution d’un support cryptographique, car ils ont à manipuler des données sensibles par exemple. Cette demande passe alors par un processus d’approbation qui peut aboutir à l’émission d’un support par la personne autorisée (gestionnaire, administrateur, agent de sécurité, etc.). La distribution du support peut alors suivre, selon le niveau de sécurité souhaité, une des 4 politiques listées ci-dessus.
* Les utilisateurs sensibles reçoivent généralement à leur arrivée ou suite à une demande (Cf. ci-dessus) un support cryptographique en face-à-face. Celui-ci peut être activé et pré-rempli avec des certificats (authentification, chiffrement et signature) lors de sa remise ou dans un second temps via le portail ILM. Dans ce dernier cas, l’utilisateur doit pouvoir s’authentifier la première fois sur le domaine avec son identifiant Windows avant de forcer l’authentification forte pour les sessions suivantes.
* Les utilisateurs de portables suivent les mêmes processus que les utilisateurs sensibles
* Les utilisateurs de portables nomades peuvent suivre dans des cas d’extrême nomadisme un scénario ou la distribution du support cryptographique se fait par voie postale (et non en face-à-face) avec une activation à distance en mode déconnecté (Cf. ci-dessous)

L’initialisation du processus d’émission d’un support peut être déclenchée automatiquement à partir d’un système de gestion des ressources humaines par exemple.

## Activation d’un support cryptographique

L’activation du support cryptographique passe par l’inscription sur ce support d’un code PIN utilisateur. Ce code peut être généré automatiquement lors de l’émission du support ou saisie par l’utilisateur.

ILM propose les modes d’émission ainsi que les distributions du code PIN suivantes :

* par mèl,
* par affichage écran,
* par impression sécurisée (moyennant l’utilisation d’une imprimante DATACARD).

Nous pouvons donc imaginer les scenarii d’activation des supports cryptographiques suivants sachant que chacun d’entre eux peut être affectés dans une même infrastructure ILM à une population d’utilisateurs particulière :

* L’activation par mot de passe unique (OTP). L’utilisateur reçoit un support cryptographique bloqué de la part d’un agent de sécurité ou d’un gestionnaire avec un premier OTP. En parallèle, il reçoit un second mot de passe à usage unique par courriel contenant aussi la procédure d’activation. Il se connecte donc au portail ILM en suivant le lien inscrit dans le courriel et entre les deux OTP reçus (qu’il est le seul à avoir), il peut alors saisir en toute confidentialité le code PIN respectant les règles édictées et qu’il est ainsi le seul à connaitre.
* Une autre méthode consiste à générer un code PIN automatiquement lors de la remise du support, à transmettre ce code à l’utilisateur (par affichage sur l’écran ou impression) et à forcer l’utilisateur à le changer lors de la première utilisation.
* Une alternative au deux scénarii précédent est de faire saisir le code PIN par l’utilisateur lors de la remise en face-à-face avec un agent de sécurité ou un gestionnaire

## Demande / exécution d’un renouvellement de certificat

ILM intègre un portail Web en libre-service permettant aux différents utilisateurs de déclencher et éventuellement d’exécuter un processus de renouvellement d’un ou de plusieurs de ses certificats que ceux-ci soient hébergés sur le poste ou sur support cryptographique.

Un service automatisé d’ILM peut aussi être utilisé pour simplement avertir l’utilisateur ou alors déclencher automatiquement le processus de renouvellement du certificat.



Figure : Mire Windows Vista de déverrouillage de code PIN

## Déblocage de code PIN en mode connecté

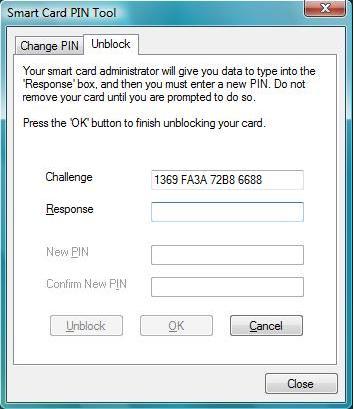


Figure : Déverrouillage de code PIN avec l’outil Smart Card PIN Tool

Un support cryptographique est un nouveau périphérique pour la plupart des utilisateurs et il est assez courant qu’ils bloquent leur carte en oubliant leur mot de passe (PIN). Cela a un impact sur la productivité des organisations et impliquer les équipes de support dans la résolution de ces problèmes peut être couteux. Une approche alternative est de fournir aux utilisateurs un mécanisme de type libre-service leur permettant de demander ou compléter une procédure de déverrouillage.

ILM permet de déclencher en mode connecté (par téléphone ou via un poste en libre service) la procédure de déverrouillage du support.

Cette procédure passe par l’envoi d’un ou de deux OTP à l’utilisateur de la même façon que lors de l’activation d’un support (Cf. ci-dessus).

## Déblocage de code PIN en mode déconnecté

Une autre méthode de réinitialisation d’un code PIN plutôt utilisé par les postes non connecté au réseau de l’entreprise (bien qu’utilisable en mode connecté) consiste en la génération d’un couple challenge/réponse.

Un utilisateur émet un challenge prouvant qu’il est en possession du support et contacte par téléphone le service technique qui après authentification de l’utilisateur et remise du challenge lui transmet une réponse (code alphanumérique valable une fois) lui donnant accès à la réinitialisation de son code PIN (Cf. copie d’écran joint).

Cette fonctionnalité est proposée seulement pour des cartes s’appuyant sur le CSP Microsoft Base Smart Card.

Elle est intégrée dans Windows Vista, donc accessible dès la mire d’authentification, et disponible pour Windows XP sous forme de l’outil *Smart Card PIN Tool*, donc nécessite pour l’utilisateur de pouvoir accéder sur son poste par un compte générique.

## Changement de code PIN

La fonctionnalité de changement de code PIN est accessible sur le portail libre-service d’ILM. L’utilisateur a besoin de connaitre le code PIN actuel pour effectuer l’opération.

Il peut aussi le faire en mode déconnecté par l’intermédiaire de l’outil *Smart Card PIN Tool*.

## Emission d’un support temporaire

Un utilisateur peut avoir oublié son support cryptographique et, dans ce cas là, il faut être en mesure de le lui remplacer le temps qu’il le retrouve.

La solution ILM propose donc le paramétrage de ce processus en prenant en compte les contraintes associées : temps d’utilisation du support temporaire, révocation complète ou temporaire des certificats associés, émission ou récupération des bi-clés.



Figure  : Exemple de workflow d’émission d’un support temporaire

Nous pouvons imaginer dans les scenarii citées la possibilité d’émission d’un support cryptographique temporaire pour une durée d’une journée pour les utilisateurs sensibles à quelques jours pour les nomades avec émission d’un nouveau certificat d’authentification et de signature et récupération du bi-clé de chiffrement ce qui permet aux utilisateurs de continuer à travailler sur leurs documents sensibles tout en évitant une utilisation frauduleuse de l’ancien support. Le déclenchement de ce processus pourrait se faire par l’utilisateur à partir d’un poste en libre-service ou d’un appel à une cellule d’assistance.

## Révocation du support cryptographique

Quand un utilisateur a perdu son support cryptographique ou lorsque l’utilisateur quitte l’entreprise il faut pouvoir révoquer ce support pour empêcher dorénavant son utilisation.

Cette phase peut d’ailleurs être précédée d’une phase de suspension du support avec ou sans émission d’un support cryptographique temporaire.

Elle est donc généralement déclencher par un gestionnaire ou automatiquement à partir d’une base de référence comme un système de gestion de ressources humaines par exemple.

## Récupération de clé

Quand un support cryptographique est endommagé ou perdu, il est parfois nécessaire de pouvoir recouvrer la clé privée de chiffrement de l’utilisateur. Les clés privées de signature sont la plupart du temps générées sur le support cryptographique et ne le quitte jamais ; d’une façon générale, aucun recouvrement n’est possible pour ces clés comme il n’y a jamais aucun séquestre préalable.

Ainsi, de nouvelles clés doivent être générées. En ce qui concerne les clés de chiffrement, elles doivent souvent être recouvrables comme certaines données ne peuvent être déchiffrées que sur la base de leur disponibilité ou, le cas échéant, recouvrement préalable.

Comme d’autres fonctions d’ILM, il est possible d’effectuer les opérations de recouvrement par un processus en mode libre-service ou piloté par un gestionnaire.

## Circuit d’approbation par des gestionnaires

Les gestionnaires peuvent approuver ou refuser les diverses procédures intervenant dans le cycle de vie d’un certificat ou d’un support cryptographique : enrôlement, révocation, mise à jour, etc.

Ces processus sont paramétrés pour nécessiter une approbation. Cela s’effectue via une simple interface web du portail gestionnaire. Une fois que la demande à reçue l’approbation finale, un mot de passe à usage unique (OTP) est généré et délivré suivant une des diverses méthodes citées plus haut dans ce document.

# Mise en œuvre

## Méthodologie

L’objectif de est de définir l’architecture de l’outil de gestion du cycle de vie des certificats par l’utilisation de la solution ILM.

Il est à noter que la mise en œuvre d’ILM doit être précédée de celle de l’IGC Windows avec les services de certificat de Windows Server 2003 (R2).

La décomposition des différentes tâches utiles sinon nécessaires à l’implémentation d’ILM au sein d’une entreprise peut être schématisée comme suit :



Les paragraphes suivants décrivent plus en détails ces différentes phases.

### Phase 1 – Vision et Périmètre

Cette phase a pour objectif d’identifier les besoins et contraintes liées à la mise en œuvre d’ILM et du cycle de vie des certificats et supports cryptographique.

Une bonne connaissance des environnements et processus existants est primordiale de façon à détecter les synergies possibles, les contraintes en terme de déploiement, les axes d’amélioration éventuels en ce qui concerne l’administration.

Certains processus seront aussi analysés dans l’objectif de pouvoir proposer des solutions techniques adaptées ou apportant une amélioration (gestion des changements, traitement des demandes des Entités Externes (en abrégé EE) « clients », processus de traitement des incidents, etc.).

Il est important de réaliser, dans cette étape, une étude de l’architecture du système d’information existant qui comprendra :

* *Organisation*- Bien comprendre votre organisation aidera à envisager les architectures les mieux appropriées à votre contexte.
* *Administration et Exploitation*- La description de l’organisation actuelle de l’administration et de l’exploitation permettra d’identifier les points devant être pris en compte et adaptés lors de la conception de l’architecture.
* *Environnement Windows*- Il est important de comprendre comment sont utilisés les systèmes Windows existants.
* *Environnement réseau*- Il est nécessaire d’obtenir des informations détaillées sur votre environnement réseau (topologie des sites géographiques, infrastructure physique, services réseaux, adressage réseau, etc.).

D’autres indicateurs seront nécessaires comme :

* Les besoins sécuritaires,
* La disponibilité,
* Le nombre d’utilisateurs,
* Le nombre de sites,
* L’évolutivité
* Etc.

Sur un projet de ce type, il est difficile, sans un travail préalable d’étude, de définir complètement la solution. Celle-ci devra être étudiée au niveau de chacun des sous projets ou lots. Il est par contre envisageable et souhaitable de définir les grandes orientations dans une phase amont de façon à permettre à l’équipe dans son ensemble de partager une même vision de la cible à atteindre. Il est possible que sur certains axes, les éléments nécessaires à la définition d’une vision de solution ne soient pas encore disponibles. Dans ce cas, cette phase permettra quand même de dégager des pistes permettant d’orienter les études ultérieures.

Cette phase consistera donc à définir et à partager une vision macroscopique de la solution à mettre en œuvre pour adresser le périmètre du projet. Elle permettra, en outre, de définir précisément le planning du projet.

Cette phase sera conduite sur la base de :

* Analyse de documents et/ou d’analyses qualitatives ou quantitatives existants (spécifications actuelles),
* Constitution de grille d’analyse,
* Réunions du groupe de travail,
* Analyses complémentaires éventuelles.

*Livrable*: un dossier d’analyse constituera le livrable de cette étape et décrira notamment :



* Une synthèse de l’existant,
* Les besoins et les contraintes liées à la mise en œuvre d’ILM,
* L’intégration d’ILM dans la vision de l’architecture de l’IGC (potentiellement plusieurs scénarii avec avantages, inconvénients et préconisations),
* La mise à jour du plan projet.

### Phase 2 – Planification

L’étape précédente, doit permettre de définir les grandes lignes de l’architecture ILM à mettre en œuvre. Dans cette hypothèse, cette étape a donc pour objectif d’affiner l’architecture générale de la solution ILM.

Il convient d’étudier plus précisément notamment :

* *Conception de l’architecture ILM* :
* Définition du nombre de serveurs ILM et leur localisation,
* Définition du nombre de serveurs de base de données et leur localisation et analyse des mutualisations possibles,
* Règles de convention de noms,
* Architecture de notification (SMTP),
* Plan d’intégration avec l’IGC.
* *Conception des configurations* :
* Dimensionnement des serveurs, RAID, bases de données/log localisation,
* Renforcement de la sécurité des serveurs (ILM, IIS pour les portails et SQL Server).
* *Stratégie de permission* :
* Délégation pour les non-administrateurs,
* Définition des permissions requises pour les requêtes (libre-service, initialisation, approbation, exécution et fin d’une requête)
* *Définition des modèles génériques en accord avec les règles définies pour l’IGC (compléments)* :
* Définition des modèles de profil,
* Définition des modèles d’enregistrement pour le déploiement des certificats,
* Définition des workflows d’enregistrement,
* Définition des stratégies de gestion pour les modèles de profil,
* Intégration des certificats non émis par le portail ILM dans le système,
* Définition des pré-requis pour le déploiement des certificats avec ILM,
* Définition des stratégies de recouvrement communes pour les certificats.
* *Rapports* :
* Description des pré-requis pour les rapports,
* Paramétrage des modèles de rapport :
  + Synthèse des demandes,
  + Synthèse d’utilisation des certificats,
  + Synthèse sur l’expiration des certificats,
  + Inventaire des supports cryptographiques,
  + Sur les supports cryptographiques,
  + Sur les demandes,
  + Sur les paramètres du gabarit de certificat,
  + Sur les paramètres du modèle de profil,
  + Sur l’utilisation du gabarit de certificat,
  + Révocation des certificats
  + Etc.
* *Conception du prototype de validation*

Cette phase sera conduite sur la base de réunions du groupe de travail.

*Livrable* : Le livrable de cette étape est constitué du document d’architecture générale de l’infrastructure ILM.



### Phase 3 – Réalisation

Cette étape a pour objectif de construire et tester l’infrastructure proposée. Comme précédemment, les choix techniques sont validés et affinés sur la base des prototypes.

L’architecture détaillée doit donner l’ensemble des informations nécessaires à l’installation de la solution en production.

C’est au cours de cette phase que sont réalisées, testées et documentées les procédures d’administration, d’installation et notamment :

* Les procédures de backup et restore (ILM, SQL Server, IIS),
* Les procédures de supervision,
* Les procédures d’installation,
* Le guide d’opération.

*Livrables* : Le livrable de cette étape est constitué du document d’architecture détaillée, intégrant les procédures d’administration et d’exploitation de l’architecture ILM.



### Phase 4 – Pilote

Cette phase se poursuit par une expérimentation pilote qui permet une validation finale du Lot avant la généralisation du déploiement. L’expérimentation pilote est réalisée en conditions réelles sur un sous-ensemble représentatif de la communauté des utilisateurs (une branche par exemple).

Il est nécessaire de déterminer quel site fera l’objet de l’expérimentation pilote. Le site choisi doit être :

* Représentatif de l’environnement de l’entreprise,
* Motivé pour l’expérimentation.

L’expérience Pilote permet de s’assurer, dans des conditions réelles, que l’architecture technique définie et testée dans le prototype est réellement opérationnelle et prête à être déployée et ce, en illustrant le bon fonctionnement de l’ensemble des composants constituant l’environnement cible du projet.

La mise en œuvre de la solution nécessite des installations utilisant les procédures d’installation finales.

Cette expérience pilote implique donc une logistique :

* Acquisition et livraison du matériel,
* Locaux réservés à l’installation,
* Acheminement du serveur vers le site final,
* Installation physique,
* Coordination avec la logistique réseau,
* Procédures de secours.

### Phase 5 – Déploiement

Il s’agit de la phase de généralisation du déploiement à l’ensemble du parc de l’entreprise. En effet, le site pilote permet de valider la solution en condition réelle. Il reste donc à généraliser cette solution pour tous les sites et ce conformément aux étapes de transitions qui ont été définies.

Pour ce faire, un plan de généralisation ou de déploiement est mis au point préalablement au déploiement final.

## Procédure d’installation d’ILM

Les grandes étapes de l’installation de la solution ILM peuvent être décomposées comme suit :

1. *Mise en place de l’infrastructure* :
2. Prise en compte des pré-requis matériels
3. Prise en compte des pré-requis logiciels
4. Extension du schéma AD
5. Installation de la base MS SQL
6. *Installation d’ILM* :
7. Préparation : des gabarits de certificats des AC et du serveur SMTP
8. Installation
9. *Configuration d’ILM* :

Lancement de l’assistant de configuration d’ILM permettant de configurer les liens avec les différents composants de la solution :

1. La forêt Active Directory, dont la publication du service et la configuration des comptes de services ILM,
2. La ou les AC basées sur les services de certificat de Windows Server 2003 (R2) en mode entreprise,
3. Le déploiement des certificats pour certains comptes de services,
4. La base SQL Server d’ILM,
5. Le serveur SMTP,
6. *Taches complémentaires* :
7. Installation des modules de stratégie et de sortie sur les AC,
8. Configuration du module de stratégie,
9. Définition des composants additionnels du module de stratégie,
10. Configurer le module de sortie.
11. *Déploiement des services* :
12. Déploiement du client ILM,
13. Implémentation du service automatisé d’ILM,
14. Déployer une station d’impression,

### Pré-requis matériel

ILM nécessite la configuration matérielle minimale suivant :

* CPU : Pentium 4 ou AMD Opteron 1.8 GHz ;
* RAM : 1 Go minimum, 2 Go recommandé ;
* Disque : 40 Go et supérieur ;

ILM 2007 FP1 n’est supporté que sur une plateforme 32-bits. Windows Server 64-bits n’est pas supporté.

### Pré-requis logiciel

ILM requiert que les éléments logiciel suivants soient préalablement installés et configures :

* Windows Server 2003 Enterprise ou Datacenter Edition ;
* Internet Information Services (IIS) 6.0 ou supérieur avec ASP.NET ;
* Framework.NET 2.0 ;
* Extension ASP.NET v2.0.50727 validée dans IIS ;

### Pré-requis d’infrastructure

#### Active Directory

Parce qu’ILM est étroitement lié au service d’annuaire Active Directory sur Windows 2000 ou Windows 2003, Active Directory est un des pré-requis nécessaire.

ILM nécessite avant son installation une extension du schéma Active Directory. Cette extension ajoute :

* Deux nouvelles classes d’objet ;
* Un nouvel attribut ;
* Et ajoute des permissions étendues pour effectuer les opérations suivantes :
  + Audit,
  + Demande d’enrôlement,
  + Demande de recouvrement,
  + Demande de renouvellement,
  + Demande de révocation,
  + Demande de déverrouillage de support cryptographique,
  + Agent d’enrôlement,
  + Enrôlement.

#### Base de données

ILM requiert Microsoft SQL Server 2000 avec le Service Pack 4 au minimum ou Microsoft SQL Server 2005 avec le Service Pack (SP) 1 ou supérieur. Le serveur SQL Server peut être installé sur le même serveur que le service ILM ou sur un serveur séparé.

#### Autorité de certification

Avant l’implantation d’ILM une ou plusieurs AC doivent avoir été précédemment installées sur des serveurs Windows Server 2003 Enterprise Edition ou supérieur et être de type AC Entreprise racine ou subordonnée. ILM requiert aussi l’utilisation de gabarit de certificat version 2, lesquels ne sont disponibles que sur une AC installée sur un Windows Server 2003 Enterprise Edition ou supérieur configuré comme une AC Entreprise.

ILM utilise trois certificats pour ses opérations:

1. Un certificat est utilisé pour signer et chiffrer les données ;
2. Un certificat est utilisé pour le recouvrement de clé ;
3. Un certificat est utilisé pour les demandes de certificat pour le compte d’utilisateurs.

Les trois gabarits de certificat appropriés doivent être publiés sur l’AC de façon qu’ILM puisse en faire la demande.

#### SMTP

ILM doit, en fonction du paramétrage des différents processus, effectuer des notifications et transmettre des mots de passe à usage unique (OTP). Pour se faire ILM nécessite donc l’utilisation d’un service de messagerie de type SMTP.

Le serveur SMTP doit pouvoir accepter le relais SMTP anonyme.

## Coûts

L’utilisation des fonctions de gestion du cycle de vie des certificats X.509 v3 (et des supports), apportées par la solution ILM nécessite l’acquisition de licences.

ILM rentre dans le modèle de licence associant :

* Une licence pour chaque serveur ;
* Une licence pour chaque accès client (en abrégé CAL pour *Client Access License en*)\* ;
* Une éventuelle licence de connecteur externe (facultative) ;

En revanche, les Services de certificats de Windows Server 2003 constituent l’un des services serveur de la plateforme Windows Server. Il n’y a donc pas de facturation spécifique aux fonctions nécessaires pour établir une infrastructure de confiance avec l’IGC Windows.

* + Vous trouverez une description détaillée du modèle de licence d’ILM à l’adresse suivante : <http://www.microsoftvolumelicensing.com/userights/ProductPage.aspx?pid=175>.

# Conclusion

Microsoft prévoit que les certificats et supports cryptographiques vont devenir des éléments critiques de la stratégie de gestion des identités et des accès des organisations.

ILM est un composant important dans la stratégie de Microsoft visant à fournir une solution de gestion des identités et des accès riche, simple à mettre en œuvre et à administrer, tout en s’assurant que les investissements réalisés dans les technologies telles que Windows Server seront pérennisés. Au moment où les nouvelles technologies exploitant les supports cryptographiques émergent au sein des organisations de toute taille, ILM a pour objectif d’aider à leur intégration dans les IGC existantes.

ILM permet aux organisations d’augmenter la sécurité du processus d’authentification tout en réduisant les coûts et la complexité de la gestion des certificats et des cartes à puce. ILM aide à déployer, gérer et maintenir plus efficacement des infrastructures basées sur des certificats ou des cartes à puce. En améliorant l‘enrôlement, la configuration et la gestion des supports cryptographiques grâce à des mécanismes de gestion pilotés par des règles et des workflows, ILM augmente la sécurité en facilitant l’exploitation des technologies d’authentification forte multi-facteur.

Contrairement à des solutions concurrentes - nécessitant des coûts de développement significatifs, du temps et des ressources - ILM fournit une solution complète de gestion du cycle de vie des certificats qui soit adaptable à la grande diversité des infrastructures des organisations et qui permette à nos clients de valoriser les investissements réalisés avec Windows, Active Directory et les services de certificat de Windows Server 2003 (R2). 