



Présentation de l’IGC Windows Server 2003

Version 1.0

Publication : Avril 2008

Auteur : Stéphane Metenier, Philippe Beraud

Contributeurs : Christophe Dubos

Copyright

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

Objectif

Ce livre-blanc a pour but de faire découvrir les services d’infrastructures de gestion de clés publiques (IGC) présents dans le système d’exploitation Windows Server 2003 (R2) sous la dénomination *Services de certificat* (*Certificate Services* en anglais). Ce document permet ainsi pour les administrateurs techniques mais également pour tout acteur de la sécurité d’avoir une vue d’ensemble permettant d’appréhender clairement ces services d’infrastructure de Windows Server 2003 (R2)et leur mise en œuvre et déploiement.

Un second document décrivant les services d’IGC de Windows Server 2008 est aussi disponible ici : [Livre Blanc à télécharger : Grille d’évaluation Services de certificats Active Directory V1.0](https://profile.microsoft.com/RegSysProfileCenter/wizard.aspx?wizid=62eb6114-c6be-4f01-997d-04409ee284af&lcid=1036)



*© 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. Introduction 4](#_Toc195340471)

[1.1. Contexte 4](#_Toc195340472)

[1.2. Usages d’une IGC 4](#_Toc195340473)

[2. Description des services d’IGC 11](#_Toc195340474)

[2.1. Introduction 11](#_Toc195340475)

[2.2. Présentation générale 12](#_Toc195340476)

[2.3. Fonctionnalités 14](#_Toc195340477)

[2.4. Architecture 21](#_Toc195340478)

[2.5. Administration et Exploitation 25](#_Toc195340479)

[2.6. Interopérabilité 28](#_Toc195340480)

[2.7. Standards supportés 30](#_Toc195340481)

[3. Mise en œuvre des services d’IGC 34](#_Toc195340482)

[3.1. Performances 34](#_Toc195340483)

[3.2. Dimensionnement et matériels 34](#_Toc195340484)

[3.3. Méthodologie 35](#_Toc195340485)

[3.4. Coûts 39](#_Toc195340486)

[3.5. Support 39](#_Toc195340487)

[4. Conclusion 40](#_Toc195340488)

[Annexe A. Références 41](#_Toc195340489)

[Annexe B. Pour des informations complémentaires 44](#_Toc195340490)

# Introduction

## Contexte

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 puces avec certificats numériques embarqués.

De même, sécuriser les échanges électroniques entre entreprises, particuliers et administrations est aujourd’hui devenu une nécessité pour la mise en place d’une informatique de confiance. Ces infrastructures mettent en place une sécurité accrue garantissant la qualité des échanges en renforçant les procédés d’authentification, l’intégrité des données, la confidentialité et la non répudiation.

Le déploiement de ces infrastructures répond également aux exigences imposées par les textes législatifs nationaux et communautaires en conférant à certains actes émis par voie électronique une véritable valeur juridique (ex : loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, <http://www.legifrance.gouv.fr/texteconsolide/AREBV.htm>).

Différents standards (Cf. Annexe A, section § « Standards issus du projet PKIX de l’IETF ») ont été établis et définissent les types de certificats utilisés afin de permettre une réelle interopérabilité avec les outils constitutifs des systèmes d’information et capables d’exploiter ces certificats pour garantir un niveau de sécurité.

Pour répondre à tous ces besoins, les infrastructures de gestion de clés publiques (en abrégé IGC), appelées également « PKI » (*Public Key Infrastructure* en anglais), apportent une réponse appropriée aux difficultés techniques, organisationnelles et juridiques que posent la sécurisation des accès et des échanges électroniques. Cette approche basée sur une cryptographie asymétrique (comprenant une clé privée secrète et une clé publique) permet, au-delà des signatures numériques, de sécuriser de nombreux types d’échanges tels que la messagerie sécurisée, les transactions commerciales en ligne via le protocole SSL/TLS, la mise en place de télé procédures spécifiques, l’accès aux ressources d’un réseau (grâce à IPsec), etc.

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.

## Usages d’une IGC

Un des enjeux majeurs en matière de sécurité pour les entreprises et les administrations est de déterminer un moyen de limiter l’accès à des ressources sensibles.

Une infrastructure de gestion de clés constitue un de ces moyens. Elle est un ensemble de composantes des technologies de l'information. Cet ensemble concourt à la sécurisation des bi-clés en générant, et en assurant la gestion complète de certificats de clés publiques.

Le réseau ainsi crée est déterminé par la confiance portée à un certificat qui dépend directement de la confiance portée à l'infrastructure de confiance toute entière. Cependant, la nature distribuée du système d'information constituant l'IGC rend difficile l'évaluation du niveau de confiance à accorder à une infrastructure de gestion de clés. Revenons à un instant sur les fondements même d’une telle infrastructure.

### Chiffrement à clé secrète

Pendant longtemps, le système cryptographique le plus utilisé a été le chiffrement symétrique qui repose sur des clés secrètes partagées (une seule et même clé permet de chiffrer et de déchiffrer).

L’émetteur et le récepteur partagent la même clé et chiffrent les données avec celle-ci, ainsi seules ces personnes ont accès aux ressources protégées par le chiffrement.

Un réseau de confiance se crée donc entre les différentes entités qui partagent la clé.

Si le secret de la clé est préservé, on s’assure que les échanges n’ont lieu qu’entre interlocuteurs de confiance.

Des difficultés subsistent quant à la méthode employée pour sécuriser le processus de délivrance de la clé (et de renouvellement de la clé dans le temps) puisque cette clé transitera nécessairement à un moment donné entre les deux entités pour que puisse s’établir une relation de confiance.

### Chiffrement à clé publique

Le chiffrement asymétrique ou à clé publique s’appuie sur clés reliées entre elles mathématiquement : une clé, dite « privée », permet de chiffrer et une autre, dite « publique », permet de déchiffrer ce que la première a chiffré et réciproquement.

Il n’est pas possible Il n’est pas possible de dériver la clé privée à partir de la simple connaissance de la clé publique en un temps raisonnable. En effet, les opérations cryptographiques liées au chiffrement asymétrique se basent sur une fonction mathématique à sens unique à porte dérobée (*trap-door* en anglais) plus facile à calculer dans une direction (sens aller) que dans la direction opposée (sens inverse) si l’on ne connait pas la porte dérobée : le sens aller peut prendre quelques secondes, le sens inverse peut prendre des mois, des années, etc.

La clé publique donne une information sur la fonction, la clé privée une information sur la porte dérobée :

* Celui qui connait la porte dérobée peut calculer la fonction facilement dans le sens inverse. Les autres, faute de porte dérobée, peuvent simplement aller dans le sens aller ;
* Le sens aller est utilisé pour le chiffrement et la vérification de la signature ;
* Le sens inverse est utilisé pour le déchiffrement et la génération de la signature ;

Les échanges de données s’appuient aujourd’hui sur des schémas de négociation de clé directement basé sur les principes de chiffrement à clé publique.  Une première proposition de négociation de clé a fait son apparition en 1976 avec l’algorithme Diffie-Hellman (en abrégé DH) proposé en tant que standard PKCS #3 [[PKCS#3](#PKCS3)][[1]](#footnote-2) qui permet à deux partenaires de négocier une valeur de clé secrète (de session) à la volée ; cet algorithme ne permet pas le chiffrement/déchiffrement des données en tant que tels.

Dans ce nouveau schéma, seules les clés publiques transitent entre les parties pour que puisse s’établir la relation de confiance. Le premier avantage tient au fait que seules les données à caractère public transiteront en clair sur le réseau avant d'établir une communication sécurisée pour acheminer les « données sensibles ».

De même le problème lié au processus d’acheminement de la clé secrète aux parties intéressées ne se pose plus.

Toutefois le problème de l’identification reste entier puisqu’il est toujours nécessaire de s’assurer que la personne qui fournit sa clé publique est bien celle qu’elle prétend être.

3 solutions sont envisageables pour pallier à cette difficulté :

1. Utiliser, comme dans le cas des clés secrètes, un échange « hors bande » (typiquement une disquette ou une clé USB) ;
2. Faire transiter la clé publique sur le réseau avec l’échange d’un condensé (dit *hash* en anglais) via une communication « hors bande » (typiquement le téléphone) ;
3. Utiliser une tierce partie de confiance reconnue comme telle par les deux parties : l’autorité de certification.

### Autorité de Certification

Chacune des deux parties fait confiance à l’autorité de certification (en abrégé AC ou AC pour *Certificate Authority* en anglais).

Elle délivre des « certificats a clé publique » (ou certificats dans la suite de ce document) qui sont des structures de données liant (à minima) la clé publique du propriétaire avec son identité, cela de façon non reproductible.

En produisant un certificat, l’autorité fournie un acte signé par un algorithme cryptographique :

« *Je, soussigné l’Autorité de Certification, certifie avoir suivi ma politique de sécurité et assure que la clé publique dans ce certificat appartient réellement à l’identité fournie dans ce certificat.*»

Cela signifie que l’autorité dispose d’un politique de sécurité (politique de certification), et qu’elle est mise à disposition des parties avant de commencer les opérations.



1. Soumission d’une demande de certificat à l’AC

Un des standards les plus utilisés pour les requêtes est PKCS #10 [[PKCS#10](#PKCS10)], qui consiste en un champ DN (*Distinguished Name* en anglais), une clé publique et optionnellement des attributs, le tout signé par l’Entité d’Extrémité (en abrégé EE) émettant la requête (ici « client »)

1. Validation de la requête de demande de certificat et tirage du certificat

L’AC, après validation de sa politique de sécurité (*Security Policy* en anglais), tire un certificat, le signe ; le client le récupère ensuite à l’issue du traitement (synchrone ou asynchrone) de sa requête.

Un certificat est donc le résultat signé du traitement favorable par l’AC d’une requête de demande de certificat reçu par celle-ci.

### IGC et sécurité

La sécurité repose ici toujours sur la clé privée, mais un nouvel acteur fait son apparition: l’AC.

L’AC est un élément sensible. On comprend bien que, si elle est compromise, toute relation de confiance est perdue: un attaquant pourrait par exemple délivrer ses propres certificats. Il est nécessaire de veiller à ce que cette autorité soit toujours bien protégée.

Comme en matière de chiffrement asymétrique élémentaire (utilisation simple d’une clé privée pour chiffrer et d’une clé publique pour déchiffrer), il est primordial de veiller à la conservation et non-divulgation des clés privées (celles des AC bien évidemment ainsi que celles des clients) car elles constituent la pierre angulaire de la confiance qui s’établit entre les différentes entités.

A compter de la délivrance du certificat, les clés privées ne transitent plus sur le réseau.

Il est d’ailleurs important de protéger la clé privée au moment où la demande de certificat (requête) est transmise à l’AC et lors de la délivrance de celui-ci.

Pour contourner ce problème et éviter que la clé privée ne circule sur le réseau, certaines IGC, telles que celle de Windows, permettent au requérant de générer sa propre paire de clés. Ci étant, pour certaines demandes de certificat non liée à la signature, la clé privée peut tout de même transiter de façon chiffrée du requérant à l’AC pour des besoins de séquestre de clés.

Techniquement, cela se traduit :

* Parfois par la présence de balises adéquates de type *<KEYGEN>* dans des pages Web et qui permettent au client de générer sa paire de clés de façon autonome,
* Ou, en ayant recours, par exemple, au travers de CryptoAPI, l’interface programmatique de gestion des opérations cryptographiques de l’environnement Windows, à un fournisseur de services cryptographiques (en abrégé CSP pour *Cryptographic Service Provider* en anglais). Il s’agit d’un module indépendant effectuant les opérations cryptographiques de façon logicielle ou de façon matérielle en relation avec un support cryptographique externe (par exemple une carte à puce dotée d’un processeur cryptographique).

### Composantes d’une IGC

Les composantes d’une IGC sont les suivantes :



* *Autorité de certification* (en abrégé AC) - Le rôle de l’AC est central dans le cadre d’une IGC. Cette entité calcule les clés et tire (édite) le certificat associé en le signant avec sa propre clé privée ce qui garantie l’authenticité du certificat. La livraison est sous sa responsabilité technique et légale. L’AC va gérer la liste des certificats révoqués et elle conserve le certificat de ses utilisateurs.

Elle peut déléguer le contrôle d’identité à une structure proche des utilisateurs qui sera reconnue sous le terme d’Autorité d’enregistrement (en abrégé AE ou RA pour *Registration Authority* en anglais). La livraison du certificat peut être réalisée en ligne, le certificat est récupéré directement sur l’Entité d’Extrémité (en abrégé EE), le poste client. L’AC peut également remettre par porteur ou *face à face* le certificat contenu sur disquette, carte, clé USB, etc. Une autorité de certification peut être désignée autorité racine en tant que référence certifiant d’autres AC.

* *Autorité de certification racine* (en abrégé ACR) - L’ACR a les mêmes caractéristiques qu’une AC mais se place au « sommet » de la chaîne de confiance de l’IGC.

Le certificat de cette autorité est « auto signé » et son rôle se borne à délivrer des certificats à d’autres autorités dites subordonnées.

* *Autorité administrative* (en abrégé AA) - Autorité responsable de l'IGC et assumant les fonctions d'autorité de sécurité, auxquelles s'ajoutent les fonctions de gestion. Elle a un pouvoir décisionnaire au sein de l'IGC
* *Autorité d’enregistrement* (en abrégé AE) - Composante de l’IGC qui vérifie les données propres au demandeur ou porteur de certificat ainsi que les contraintes liées à l’usage d’un certificat, conformément à la politique de certification. L’AE est une composante optionnelle de l’IGC qui dépend d’au moins une AC.

# Description des services d’IGC

## Introduction

Les services de certificat de la plateforme Windows Server 2003 (R2) proposent des services personnalisables pour la création et la gestion de certificats à clé publique X.509 v3 utilisés dans les applications, services, systèmes et dispositifs reposant sur les technologies à clé publique.

Les organisations peuvent s’appuyer sur ses services pour améliorer la sécurité en liant l’identité d’une personne, d’une machine, d’un dispositif ou d’un service à la clé privée correspondante. Ces derniers comprennent dans le même temps des fonctionnalités qui permettent la gestion de l’enrôlement et de la révocation des certificats dans un contexte d’environnements distribués.

Les différents composants des services de certificats de Windows Server 2003 (R2) permettent d’émettre et de gérer des certificats au format standard pour une utilisation par des applications, services et systèmes Microsoft, non Microsoft et/ou non Windows.

Ils autorisent ainsi la matérialisation d’une infrastructure de confiance au travers de la mise en œuvre de services d’IGC. Pour cette raison, ces services sont aussi simplement dénommés dans la suite du document IGC Windows.

L’IGC Windows constitue l’une des solutions de gestion d’identité et de contrôle d’accès de Microsoft, au même titre, par exemple, que :



* L’annuaire d’entreprise *Active Directory* avec lequel l’IGC Windows propose une intégration native important de nombreux services automatisés (Cf. plus bas)
* Le système de gestion du cycle de vie des identités, des certificats et supports cryptographiques *Identity Lifecycle Manager*(en abrégé ILM) 2007 qui offre les services :

1. D’AE évoluée pour des AC basés sur services de certificat Windows Server 2003 en « mode entreprise » avec le support de *workflows* personnalisables pour mettre en conformité les processus organisationnels des entreprises avec leurs politiques de sécurité et de certification pour la délivrance et la gestion des certificats X.509 utilisateur et des supports (carte à puce, jeton USB etc.) éventuellement associés ;
2. De système de gestion de supports cryptographiques (ou CMS pour *Card Management System* en anglais), cette fonction constituant un élément essentiel d’une infrastructure de confiance lorsque des supports (carte à puce, jeton USB etc.) sont par exemple déployés à grande échelle ;

* Le système de Web SSO, Web SSO extranet et de fédération d’identité *Active Directory Federation Service* (en abrégé AD FS) vis-à-vis duquel une AC basée sur les services de certificat de Windows Server 2003 peut délivrer des certificats (de signature de jeton SAML, d’authentification client, d’authentification de proxy AD FS, etc.) à destination de ses différentes composantes ;
  + Ces différentes solutions sont présentées dans le portail Web Microsoft IDA *(Identity and Access Solutions*) à l’adresse Internet <http://www.microsoft.com/identity>.



## Présentation générale

L’IGC Windows s’architecture autour des services d’AC ainsi que des services de point de publication en rendant disponible les certificats et les listes de révocation (en abrégé CRL pour *Certificate Revocation List* en anglais). Elle comprend également les outils de gestion des certificats (gestion des audits, des révocations, des émissions ou toutes les autres étapes dans la vie d’un certificat).

Ce service peut s’appuyer sur d’autres services comme :

* Un annuaire pour les identités numériques,
* Une AE,
* Une solution de gestion des supports cryptographiques,
* Un système de sécurisation matériel (en abrégé HSM pour *Hardware Storage Module* en anglais),
* Ainsi que des services réseaux classique DNS, SMTP, etc.

L’IGC Windows propose une intégration possible avec Active Directory permettant d’optimiser :

* La sécurité de la solution en authentifiant les demandes,
* Les coûts de mise en œuvre et d’exploitation au quotidien en utilisant les stratégies de groupes (en abrégé GPO pour *Group Policy Object* en anglais) pour automatiser les principales opérations d’émission / renouvellement / remplacement / révocation,
* La disponibilité de la solution via les fonctionnalités de réplication propres à Active Directory.

Cette intégration native permet par ailleurs de garantir un fonctionnement optimal dans les scénariis demandés ceux-ci ayant déjà été mis en œuvre par de nombreuses entreprises au niveau mondial avec des coûts d’intégration maitrisés.

Une AC basée sur les services de certificat Windows Server 2003 en mode entreprise, c'est-à-dire, quand elle est intégrée à Active Directory, propose les usages suivants :

* Authentification des demandes,
* Délégation d’administration au sein de l’autorité,
* Déploiement des certificats des autorités racines via les stratégies de groupe,
* Déploiement/renouvellement automatisés des certificats via les stratégies de groupe,
* Stockage des gabarits de certificats dans Active Directory,
* Renseignement optionnel des informations d’identité au sein des certificats lors de la génération du certificat,
* Publication optionnelle des certificats dans Active Directory.

Dans le cadre de ce livre-blanc nous proposons d’utiliser une solution comme Microsoft ILM 2007 pour rendre les services complémentaires d’AE et de gestion du support cryptographique (CMS) même si l’IGC Windows intègre quelques fonctionnalités pouvant couvrir partiellement ces besoins.

Différentes architectures sont envisageables :



* Autorité unique sans intégration à Active Directory (mode autonome) - Cette architecture n’est généralement pas préconisée car elle est moins riche fonctionnellement et la plus onéreuse à exploiter. En effet, toutes les demandes d’émission ou de renouvellement de certificats doivent être traitées manuellement.
* Autorité unique avec intégration à Active Directory (mode entreprise) - Cette architecture est essentiellement utilisée dans le cas ou il n’y a qu’une seule foret Active Directory.
* Autorités multiples avec intégration à Active Directory (mode entreprise) - Cette architecture est la plus souvent préconisée car elle est la plus riche fonctionnellement, sa mise en œuvre est la plus simple et elle est supportée nativement, en outre :
  1. Elle offre un niveau de sécurité identique à l’architecture AC unique via les mécanismes de délégation qui permettent de contrôler les types de certificats émis, les contraintes d’émission et les populations ciblées,
  2. Elle offre un niveau de disponibilité identique à l’architecture AC unique,
  3. Elle permet un regroupement géographique des autorités, permettant une administration centralisée,
  4. Et enfin, cette architecture est éprouvée.

Dans ce cadre, les grands principes d’architecture que nous pressentons sont illustrés au travers du schéma suivant :



Cette architecture est composée :

* D’une autorité de certification racine (hors ligne) en mode autonome (pas de rattachement à une forêt Active Directory) et assistée d’un boitier HSM,
* Pour chaque forêt Active Directory :

1. Une AC émettrice,
2. Une AE, ce service peut être couvert comme mentionné précédemment par la solution Microsoft ILM 2007.

* Un boitier HSM en réseau pour le séquestre des clés des différentes AC émettrice

Il est tout à fait envisageable d’avoir plusieurs niveaux de hiérarchie des AC. Ce schéma illustre simplement les principes d’architecture.

D’autre part, ce schéma ne fait pas apparaitre les solutions de redondance ou de reprise sur incident.

## Fonctionnalités

Les services de certificat de Windows Server 2003 (R2) proposent des services personnalisables pour la création et la gestion de certificats à clé publique X.509 v3 utilisés dans les applications, services, systèmes et dispositifs reposant sur les technologies à clé publique.

Ils autorisent ainsi la matérialisation d’une infrastructure de confiance au travers de la mise en œuvre de services d’IGC.

Ces derniers sont des éléments d’infrastructure par excellence et de ce fait ne sont par perçus par les utilisateurs. En effet, les interactions se feront dans les scénarii évoqués principalement par des autorités d’enregistrement.

Néanmoins la grande richesse fonctionnelle de l’IGC Windows autorise des scenarii ou des interactions entre l’IGC et l’utilisateur sont rendus transparent pour ce dernier de part la forte l’intégration des services de certificats de Windows Server 2003 (R2) avec l’environnement utilisateur. Le cycle de vie complet de certificats poste et utilisateur peut ainsi s’opérer sans intervention pour permettre la mise en œuvre de scénarii comme le Wifi sécurisé, le chiffrement de flux en IPsec, le chiffrement et la signature sans support cryptographique, etc.

Pour une compréhension des fonctionnalités de cette solution nous avons souhaités apporter un éclairage sur ses principales caractéristiques comme suit.

### Gestion des CRL et CRL différentielles

L’AC disponible au sein de Windows Server 2003 (R2) au travers des services de certificat supporte la publication des listes de révocation vers les différents emplacements mandatés par les RFC et permet leur accès via les protocoles HTTP [[RFC 2585](#RFC2585)], LDAP [[RFC 2587](#RFC2587)] et éventuellement CIFS.

Le ou les emplacements sont indiqués au sein de chaque certificat sous forme d’URL dans le champ CDP (*cRLDistributionPoint*).

Les emplacements de publications sont paramétrables et peuvent être multiples (chemin LDAP, chemin HTTP: ou fichier FILE:).

Dans une architecture distribuée ou à forte tolérance aux pannes, on privilégiera la publication de la CRL dans Active Directory (chemin LDAP).

### Enrôlement

L’AC Windows Server 2003 supporte en standard les requêtes de certification (en abrégé CSR pour *Certificate Signing Request* en anglais) au format PKCS #10 [[PKCS#10](#PKCS10)], ainsi que les messages PKCS #7 [[PKCS#7](#PKCS7)]/CMS (*Certificate Message Syntax* en anglais) [[RFC 3852](#RFC3852)] pour la fourniture du certificat signé en retour.

Le standard CMC (*Certificate Management over CMS* en anglais) [[RFC 2797](#RFC2797)] est supporté nativement et permet une gestion plus sécurisée de l’enrôlement, en particulier le séquestre de la clé de chiffrement.

Les balises KEYGEN pour l’enrôlement HTTP sont supportées.

### Annuaire

L’IGC Windows peut tirer parti de l’annuaire Active Directory pour la gestion de l’identité et de l’authentification.

En configuration « mode entreprise », une AC Windows Server 2003 peut délivrer automatiquement, mécanisme appelé « auto-enrôlement », des certificats à des entités (utilisateur, et/ou machines) dûment authentifiés et en suivant une politique de certification et d’enrôlement. L’auto-enrôlement gère non seulement la certification des utilisateurs et/ou de machines de manière automatique, mais aussi le cycle de vie des certificats, et en particulier leur renouvellement (ou remplacement selon un autre gabarit).

Une AC Windows Server 2003 en « mode entreprise » publie automatiquement les certificats émis dans l’annuaire AD. L’annuaire Active Directory est interrogeable via LDAP pour permettre aux applications d’accéder aux certificats de l’organisation.

Une AC Windows Server 2003 peut cependant être installée en « mode autonome », dans ce cas elle n’est pas couplée avec Active Directory.

La personnalisation de « module de stratégie » (*policy module* en anglais), matérialisant une politique de certification, et de « module de sortie » (*exit module* en anglais) permet de bâtir une véritable architecture de certification sur mesure mettant en œuvre des technologies de fournisseurs hétérogènes.

Par exemple, un « module de sortie » spécifique peut publier les certificats émis dans un annuaire LDAP. Il est fréquent de placer en amont d’une telle AC un serveur faisant office d’autorité d’enregistrement, comme par exemple Microsoft ILM 2007.

### Support des stratégies de groupe

Les stratégies de sécurité peuvent s'appliquer à des sites, à des domaines ou à des unités organisationnelles (OU) et affectent les groupes de sécurité associés, groupes qui contiennent des utilisateurs ou des ordinateurs. La stratégie de sécurité relative à l'IGC ne représente qu'une partie de la stratégie globale de sécurité de la plateforme Windows. Elle fournit un mécanisme permettant de définir et de gérer la stratégie de façon centralisée, tout en veillant à son application sur l'ensemble du système.

Les principaux aspects de la stratégie de sécurité de l'IGC sont décrits ci-dessous.

La fiabilité des AC racine peut être établie au moyen de stratégies, afin de créer les relations d'approbation que les clients de domaine utiliseront pour vérifier les certificats de clé publique. L'ensemble des AC de confiance est configuré à l'aide de l'*Éditeur de stratégies de groupe*. Il peut être configuré pour chacun des ordinateurs, puis appliqué globalement à tous les utilisateurs de cet ordinateur.

L'administrateur peut, après avoir défini une AC racine comme étant digne de confiance, configurer les propriétés d'utilisation associées à celle-ci. Ces propriétés permettent de limiter le nombre de cas dans lesquels les certificats émis par l'autorité de certification sont valides. Les restrictions spécifiées s'appuient sur les identificateurs d'objet (en abrégé OID pour *Object Identifier* en anglais), comme cela est expliqué pour les extensions *ExtendedKeyUsage* dans le document IETF PKIX.

* + La liste des OID utilisés au niveau de la plateforme Windows est précisée dans l’article 287547 « Object IDs Associated with Microsoft Cryptography » (<http://support.microsoft.com/default.aspx?scid=287547>).

Dans leur forme actuelle, ces restrictions permettent de limiter l'utilisation d'une combinaison quelconque des éléments ci-dessous :

* Authentification du serveur,
* Authentification du client,
* Signature de code,
* Courrier électronique,
* Système de terminaison de sécurité IP (IPsec),
* Tunnel IPsec,
* Utilisateur IPsec,
* Horodatage,
* Système de fichiers chiffrés (en abrégé EFS pour *Encryption File System* en anglais) pour le système de fichier NTFS.

Dans le cadre de l'intégration de l'IGC avec un environnement Active Directory, les mécanismes de stratégie ont été prévus pour prendre en charge un processus d'enrôlement automatique des certificats. Ce processus repose sur deux éléments clés : les gabarits (modèles) de certificat et les objets d'enrôlement automatique. Ceux-ci sont intégrés à l'objet stratégie de groupe (en abrégé GPO pour *Group Policy Object* en anglais) et peuvent être définis sur la base d'un site, d'un domaine, d'une unité organisationnelle, d'un ordinateur ou d'un utilisateur.

### Gabarits de certificat

Une AC émettrice en « mode entreprise » permet de définir et de s’appuyer sur des modèles (ou gabarits) de certificats.

Deux types de modèles sont ainsi proposés : version 1, version 2 (une version 3 a été ajoutée dans les services de certificat de Windows Server 2008). La version 1 correspond aux modèles introduits historiquement avec Windows Server 2000, la version 2 à ceux de Windows Server 2003.

Les modèles proposés par défaut sont complètement personnalisables et peuvent ainsi être dupliqués en versions 2 et modifiés de façon à répondre au(x) besoin(s) exprimé(s) tant vis-à-vis du serveur (extensions, OID de politique, etc.) que du client (module cryptographique, longueur de clé, clé exportable, etc.). Le gabarit définit différents éléments, tels que les règles d'attribution de noms, la période de validité, les CSP autorisés avec CryptoAPI pour la génération de clés privées, les algorithmes, ainsi que les extensions qui pourraient être ajoutées au certificat.

Les gabarits de certificats définissent aussi les fonctionnalités et les restrictions des types de certificats. En utilisant des gabarits version 2 les paramètres additionnels suivants peuvent être définis pour chaque type de certificat :

* Utilisation de l’auto-enrôlement pour la génération et le renouvellement de certificat ;
* Autoriser la séquestre de clé privée (en vue d’un recouvrement futur) ;
* Publier le certificat dans un objet de compte Active Directory ;
* Autoriser la génération et le stockage des clés par les CSP, ainsi que la longueur de clé minimum ;
* Les utilisateurs et groupes autorisés à enrôler ou auto-enrôler le certificat ;
* Les autres extensions de certificat, incluant les stratégies de génération et d’application.

D'une façon générale, chaque AC définit la liste des modèles qu’elle peut offrir à partir de la liste des modèles déclarés dans Active Directory. Une même AC permet d'offrir plusieurs modèles. L'AE liste à son niveau les types de certificats disponibles qui peut correspondre à un sous ensemble des modèles offerts par l'AC. L’entrée Services d’inscription au niveau d’Active Directory liste de façon globale les AE disponibles avec les modèles ainsi proposés.

* + La page Web « Certificate Templates Overview » (<http://technet2.microsoft.com/windowsserver/en/library/e42693ef-374b-40a9-af3c-569f0d1fe1c91033.mspx>) précise les 29 modèles proposés par défaut de Windows Server 2003 (R2).

Cette liste extensible par duplication et personnalisation d’un gabarit prédéfini comprend, entre autres, la signature, l'ouverture de session par carte à puces, la sécurisation de mèl, la signature de code logiciel, IPsec, 802.1X, l'authentification Internet via SSL/TLS (client et serveur), les politiques de restrictions logicielles Windows Server et le chiffrement EFS pour le système de fichiers NTFS.

### Auto-enrôlement / auto-renouvellement / auto-remplacement

Ce mode suppose une AC émettrice en mode entreprise dans la mesure où une intégration avec l’annuaire Active Directory est requise. Ce mode combine en effet les stratégies de groupe (GPO) et les gabarits de certificats (Cf. ci-dessus) publiés dans Active Directory.

Ce mode permet de disposer de mécanismes d’auto-enrôlement / auto-renouvellement / auto-remplacement pour les utilisateurs, machines et services. Ce mode peut être qualifié de modèle « tout-auto » offrant selon le niveau d’application des GPO une granularité fine quant à la population ciblée.

Ce modèle permet d’alléger les contraintes organisationnelles et techniques lors de la mise en œuvre d’une infrastructure d’IGC.

* + Le modèle « tout-auto » est décrit dans son ensemble dans le livre blanc « Certificate Autoenrollment in Windows Server 2003 » à l’adresse Internet <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx>.

Par ailleurs, il nous parait important de mentionner ici que ce modèle « tout-auto » a fait partie de la cible d’évaluation Critères Communs au niveau EAL 4+ (Cf. section § «  » ).

Enfin, le modèle « tout-auto » peut fonctionner de pair avec les services d’itinérance de crédentités (*Credential Roaming* en anglais) si ces derniers sont activés. Ces services permettent de délivrer les certificats à la session courante de la machine courante d’un utilisateur via la réplication Active Directory et les stratégies de groupes.

Ceci facilite l’usage de fonctions comme la messagerie sécurisée (S/MIME), l’authentification client TLS et propose une expérience utilisateur améliorée pour l’usage des supports (carte à puce, jeton USB) ;

* + L’article 935441 « Webcast: Credential Roaming Basics » à l’adresse Internet <http://support.microsoft.com/?id=935441> propose une vue d’ensemble de ce service.

### Délégation d’administration

Les services de certificats Active Directory de Windows Server 2003 intègrent un modèle d’administration qui permet de satisfaire aux exigences des critères communs (Cf. section éponyme § 2.5.3 et section §   «  » ) concernant la séparation des rôles et assurant ainsi qu’une seule personne ne soit pas capable de compromettre la sécurité des services d’IGC.

A ces rôles correspondent des droits d’accès à l’AC et au serveur qui l’héberge. Ces rôles possèdent également des équivalences en rôle d’administration Windows, facilitant ainsi leur implémentation.

L’activation de la séparation des rôles s’effectue via l’utilitaire *certutil.exe*.

Les « bonnes pratiques » à observer dans ce domaine pourraient se résumer ainsi :



* Assigner les rôles à des groupes (et non pas des comptes utilisateurs) ;
* S'assurer qu'un compte utilisateur ne se voit assigné qu'un seul rôle ;
* S’assurer que les groupes pour lesquels les rôles Gestionnaire de services d’IGC, et Gestionnaire de certificats sont assignés ne soient pas aussi administrateur local ;
* Garder à l'esprit que les administrateurs locaux restent tout puissants et ces droits sont nécessaires pour le renouvellement du certificat de l’AC ;

### Mise à disposition des certificats

Les services de certificat de Windows Server 2003 proposent les modes de mise à disposition de certificat logiciel suivants vers l’EE :

* L’enrôlement automatique par GPO,
* Par la MMC,
* Par l’interface web d’enrôlement,
* Par API.

Ces services proposent pour la mise à disposition de certificat sur support cryptographique l’enrôlement par délégation à un agent d’enrôlement (disposant d’un certificat d’agent d’enrôlement).

La publication par mail peut être réalisée via un module de sortie (*exit module* en anglais) spécifique ; ce dernier reçoit l’ensemble des notifications du moteur lorsque des opérations ont lieu (par exemple l’émission d’un certificat) et peut donc publier les informations nécessaires.

* + Une description de l’interface de ce module est disponible à l’adresse Internet <http://msdn2.microsoft.com/en-us/library/Aa382386.aspx>.

Microsoft ILM 2007 en tant qu’AE propose une souplesse accrue en termes de scénarii pour la mise à disposition de certificat sur l’EE ou sur le support cryptographique.

### Fonction de séquestre / recouvrement des clés de chiffrements

Les services de certificat de Windows Server 2003 permettent, par le biais des agents de récupération de clés (en abrégé KRA pour *Key Recovery Agent* en anglais), d’assurer des fonctions de séquestre et de recouvrement de la clé privée des utilisateurs.

Cette dernière est stockée dans la requête de l’utilisateur, elle-même stockée dans la base de données de l’AC.

Un aspect important de l’archivage et de la récupération des clés est qu’aucune clé permettant de déchiffrer les clés des utilisateurs, protégées par les KRA, ne réside sur l’AC. Cela afin de ne pas pouvoir compromettre la sécurité des clés archivées.

La fonction de séquestre et de recouvrement des clés de chiffrements permet :



* La fourniture par l’utilisateur de sa clé privée à l’AC avec la requête de certificat ;
* Le stockage sécurisé des clés avec les certificats X.509 v3 dans la base des certificats.

L'IGC Windows offre des mécanismes manuel et automatique de séquestre de clés de chiffrement.

Ceci requiert que l’AC soit configurée pour supporter cette fonctionnalité de séquestre et de recouvrement et que l’activation de la séparation des rôles, l’identification du ou des KRA et l’émission à leur intention d’un certificat KRA soient mis en œuvre.

Le mode manuel repose sur la commande *certutil.exe -importkms* qui permet le séquestre manuel de clé à partir d'un export de la clé dans un fichier PKCS #12 [[PKCS#12](#_PKCS)].

Le mode automatique s’appuie sur la fonctionnalité d’auto-enrôlement / auto-renouvellement. Il est nécessaire, dans ce cas, que le gabarit du certificat considéré ait la fonction de séquestre de clé activée.

La clé privée est alors automatiquement transmise sous forme chiffrée dans la requête d'enrôlement CMC conformément à la RFC 2797 [[RFC 2797](#RFC2797)] pour séquestre.

En terme de recouvrement, seul le gestionnaire de certificats, si la séparation des rôles est activée, peut extraire les clés séquestrées sous leur forme chiffrée (blob authentifié PKCS #7 [[PKCS# 7](#PKCS7)] - *ICertAdmin2::GetArchiveKey – Certadm.dll*) pour les fournir à un agent de recouvrement.

Cette opération est réalisée via la commande *certutil.exe –getkey* pour l’obtention du blob de recouvrement PKCS#7 [[PKCS# 7](#PKCS7)] depuis l’autorité de certification considérée et son écriture dans un fichier. Le blob est chiffré avec la clé publique du certificat du ou des KRA destinataire(s).

Le KRA utilise la commande *certutil.exe -recoverkey* pour (en conjonction avec sa clé privée) extraire la clé et la remettre dans un PKCS #12 [[PKCS#12](#_PKCS)] (.pfx) chiffré avec un mot de passe.

Ce fichier sera alors transmis à l'utilisateur.

Compte tenu de cette description succincte, le recouvrement d'une clé privée constitue un processus manuel qui exige, pour l'utilisateur qui a perdu sa clé privée, de contacter le gestionnaire de certificats afin de lui demander de procéder à son recouvrement. L'identification de l'utilisateur demandant le recouvrement, la transmission du fichier blob de recouvrement à l'agent de recouvrement et la transmission du fichier .pfx contenant la clé recouvrée avec son mot de passe à l'utilisateur constituent autant d’étapes qui doivent être soigneusement planifiées.

Ce modèle de recouvrement permet la séparation des rôles et des pouvoirs décisionnel et exécutif vis-à-vis desquels le gestionnaire de certificats et l’agent de recouvrement sont des personnes physiques différentes. Le gestionnaire de certificats peut décider de recouvrir une clé mais n’a pas accès à la clé alors que le KRA peut seulement accéder à une clé dont le recouvrement a été décidé.

### Support du protocole OCSP

Les services de certificat de Windows Server 2003 supportent le protocole *Online Certificate Status Protocol* (OCSP) [[RFC 2560](#RFC2560)] et s'appuient en termes de fournisseur et répondeur sur les offres tierces suivantes :

* Ascertia TrustFinder OCSP (<http://www.ascertia.com/products/tf_ocsp>),
* Corestreet Server Validation Extension (SerVE) (<http://www.corestreet.com/products/serve.html>),
* Tumbleweed Communications Valicert Validation Authority (VA) (<http://www.tumbleweed.com/products/validationauthority.html>),
* Kyberpass Validation Server (<http://www.kyberpass.com/products/trustplatform/index.html>),
* RSA Validation Solution (<http://www.rsasecurity.com/node.asp?id=1355>).

Par ailleurs, les services de certificat de Windows Server 2003 permettent de générer des certificats OCSP (emplacement de l’« *OCSP Responder* » précisé dans l’extension AIA) ainsi que des certificats « *OCSP Responder* » pour le répondeur en ligne.

Windows Server 2008 permet la mise en œuvre de la fonctionnalité de répondeur en ligne OCSP avec le décodage des requêtes de statut de révocation pour des certificats donnés, l’évaluation du statut de ces certificats, l’envoi en retour d’une réponse signée contenant l’information de statut demandée.

* + Ce service est décrit dans le livre blanc « Installing, Configuring, and Troubleshooting the Microsoft Online Responder » à l’adresse Internet <http://technet2.microsoft.com/windowsserver2008/en/library/045d2a97-1bff-43bd-8dea-f2df7e270e1f1033.mspx>.

## Architecture

### Hiérarchies d’AC

L’IGC Windows supporte un modèle d’AC hiérarchique. Une hiérarchie de certification apporte la montée en charge, la facilité d’administration et la liaison avec des offres d’IGC tierces.

Dans sa plus simple forme, une hiérarchie de certification consiste en une seule AC. Cependant, en général, une hiérarchie plusieurs AC avec des relations parent-enfant bien définies. Dans ce modèle, les AC enfants subordonnées sont certifiées par le certificat généré par leur AC parent, ce qui lie la clé publique d’une AC à son identité. L’AC au sommet de la hiérarchie est appelée ACR. Les AC enfants de l’autorité racine sont appelées AC subordonnées.

* Dans Windows XP et Windows Server 2003, si vous faites confiance à une ACR (car son certificat est référencé comme ACR de confiance dans le magasin de certificats), vous faites confiance à toutes les AC subordonnées de la hiérarchie, à moins qu’une AC subordonnée ait eu son certificat révoqué par son AC parent ou que son certificat soit expiré.

L’utilisation d’une hiérarchie d’AC introduit aussi un certains nombre de scénarii pratiques de mise en œuvre notamment :



* Par usage, des AC subordonnées sont alors dédiées à l’émission de certificats pour des besoins particuliers, tels que le courriel sécurisé ou l’authentification réseau ;
* Par organisation, des AC subordonnées émettent des certificats selon l’organisation de l’entreprise ;
* Par répartition géographique ;
* Pour de la répartition de charge, des AC subordonnées émettent les mêmes types de certificats ;
* Pour de la sauvegarde et de la tolérance aux pannes.

Une hiérarchie de certification fournit aussi les bénéfices suivants :

* Une configuration flexible de la sécurité de l’AC pour répartir au mieux sécurité et facilité d’utilisation, comme la force de la clé, la protection physique et la protection contre des attaques réseau ;
* La capacité d’arrêter une partie de la hiérarchie sans en affecter les autres membres.

Une sous-hiérarchie d’AC mise en œuvre au travers des services de certificat de Windows Server 2003 peut être rattachée à une hiérarchie mise en œuvre par des technologies non Windows. Dans ce cas, le certificat d’une AC Windows Server 2003 est signé par une AC non Windows.

A l’inverse, une AC Windows peut émettre des certificats pour des AC non-Windows permettant ainsi de rattacher à une racine (racine AC Windows, ou hiérarchie de AC Windows) une branche d’AC mise en œuvre par des technologies de fournisseurs tiers.



### Certification croisée

La notion de hiérarchie de type certification croisée (*Cross Certification* en anglais) est décrite dans la RFC 3280 [[RFC 3280](#RFC3280)].

Les services de certificats de Windows Server 2003 (R2) permettent la mise en œuvre de ce modèle par la subordination qualifiée qui autorise la définition de contraintes (contraintes élémentaires, contraintes de noms, contrainte de politique, contraintes application).

La subordination qualifiée offre deux applications pratiques :



1. Quels certificats d'un partenaire peut-on valider / accepter ? La subordination qualifiée permet d’offrir un contrôle plus précis de la confiance des certificats avec l’inclusion / exclusion d'usages (*purposes* en anglais). Par exemple, la subordination qualifiée peut permettre l'usage d'un certificat tiers pour mèl seulement, alors que le certificat spécifie e-mail et IPsec.
2. Contrôler l'émission des AC subordonnées. Ceci permet d’empêcher les AC d'émettre :
   * Dans des espaces de noms invalides / non autorisés ;
   * Avec des politiques d'émission invalides / non autorisées ;
   * Avec des politiques d'application invalide / non autorisées ;
   * La subordination qualifiée est complètement décrite dans le livre blanc « Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003 » à l’adresse Internet <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx>.

### Support de l’AC Pont

Le modèle AC Pont (*Bridge* en anglais) selon le principe *Federal Bridge Certification Authority* (FBCA) est également supporté par les services de certificatsde Windows Server 2003.

A ce titre, les services de certificat de Windows Server 2003 (R2) sont certifiés « *US Federal Bridge AC* » (Cf. <http://www.cio.gov/fbca/techio.htm>).

* + Un exemple de mise en œuvre est l’infrastructure de confiance *WISeKey Certify ID* (<http://www1.wisekey.com/index.aspx>).

L’utilisation de têtes de pont permet l’interopérabilité entre un nombre plus important de hiérarchies ou sous-hiérarchies IGC d’organisations séparées.

### Architecture physique

Un réseau ouvert avec une connectivité transparente entre toutes les connexions est le meilleur promoteur d’une IGC. Cependant, les réseaux complexes utilisent des pare-feu pour contrôler le trafic. De ce fait, une fonctionnalité comme l’auto-enrôlement (s’appuyant sur DCOM) ne sera pas disponible sur tous les points du réseau. Dans un environnement sécurisé, on privilégiera la fourniture de certificats via un enrôlement Web ou personnalisé.

Nous illustrons cela par un exemple d’architecture d’AC selon trois scénarii:



* Le *Centre de Données Centralisé* (en abrégé CDC, *Centralized Data Center* en anglais) ;
* Le *Centre de Données Extranet* (en abrégé CDE, *Extranet Data Center* en anglais) ;
* Le *Centre de Données Internet* (en abrégé CDI, *Internet Data Center* pour en anglais).

Les scénarii *Centre de Donnée Internet*, *Extranet* et *Centralisé* requièrent chacun leur propre infrastructure d’AC. Parce que le centre de données Internet est relativement indépendant de l’infrastructure de l’entreprise, il est raisonnable d’y installer une IGC séparée.

#### Figure 4. Physical Design Example for Certificate ServicesExemple d’infrastructure d’AC

##### Centre de Données Centralisé

Le scenario CDC exploite 2 principaux groupes d’AC émettrices (CA111 à AC 114) chainées à une seule AC intermédiaire hors-ligne, CA11. CA11 est elle-même chainée à CA1, racine de confiance de l’entreprise. Une seconde autorité CA2 auto-signée fait partie du CDC pour apporter les certificats routeur.

CA111 et CA112 sont des AC redondantes et en ligne qui émettent des certificats aux utilisateurs quand un processus de remise en main propre est nécessaire. CA113 et CA114 émettent des certificats nécessitant moins de contraintes de remise sécurisée, comme par exemple des certificats techniques. Toutes les AC peuvent publier leurs certificats utilisateurs dans Active Directory, si nécessaire.

Les deux AC, nommées CAx11 et CAx12, émettent des certificats dans les cas ou les utilisateurs communiquent avec des tiers extérieurs à l’entreprise. Les deux AC sont chainées à une ACR externe. Le certificat de l’ACR externe est déployé par le service de mise à jour de racine de Windows pour bénéficier de racines de confiance par défaut.

##### Centre de Données Extranet

Le scénario CDE exploite 3 AC émettrices chainées à une AC intermédiaire dédiée (CA12), laquelle est gérée par des administrateurs externes. CA12 est chainée à l’AC racine de l’entreprise, CA1. CA121 et CA122 sont redondantes et émettent des certificats pour les membres de l’extranet. Les deux AC émettrices publient les certificats utilisateur sur le contrôleur de domaine de l’extranet. CAx2 est chainé à une ACR publique et émet des certificats ou la confiance en la racine publique est nécessaire.

##### Centre de Donnée Intranet

Le scénario CDI utilise une hiérarchie séparée avec deux AC émettrices redondantes, CA31 et CA32. Les deux AC publient les certificats utilisateurs sur le contrôleur de domaine du CDI. Parce que le CDI est séparé des autres centres de données, il utilise une ACR séparée, CA3, qui est le parent de CA31 et de CA32. CAx3 est chainée à une AC racine publique pour émettre des certificats nécessitant une racine de confiance publique.

Pour établir une relation de confiance entre les CDI et CDC, une certification croisée avec subordination qualifiée doit être définie (Cf. section § 2.4.2 « Certification croisée » ci-dessus). Un cluster de serveur Web, présent dans la zone périmétrique, fournit une copie de chaque CRL à toutes les AC pour rendre les CRL disponibles publiquement.

Le serveur AD/AM de la zone périmétrique collecte les utilisateurs et les certificats de toutes les forêts et représente donc le référentiel central sécurisé des certificats. La synchronisation des données est effectuée par la solution Microsoft ILM 2007.

En fonction des différents niveaux de publication, les certificats sont visible pour différents groupes utilisateurs. Le serveur AD/AM fournit aussi les CRL et les certificats d’AC pour les clients qui ne peuvent pas ou ne doivent pas récupérer du contenu HTTP de l’Internet.

### Environnement multi-forêts

Dans un environnement ou de multiples forêts Active Directory sont présentes, il est nécessaire de fournir un référentiel des certificats qui autorise l’échange de certificat inter-forêts.

Par défaut, les informations de certificats, CRL et d’AC sont disponibles seulement dans leur propre forêt Active Directory.

Dans un environnement multi-forêts Active Directory, il est nécessaire de définir les AC membre de chaque forêt en fonction des contraintes applicatives et/ou de certificat.

Par exemple, pour fournir des certificats SSL à des serveurs Web de différentes forêts, il n’est pas obligatoire d’avoir des AC dans chacune d’entre elles car les serveurs SSL peuvent enrôler manuellement des certificats à partir d’une AC d’une autre forêt Active Directory.

* Dans les versions actuelles de Windows, une forêt définie la frontière externe d’une AC en mode entreprise; les entités qui appartiennent à différentes forêts nécessites donc des AC en mode entreprise séparées. Le nombre de domaines dans une forêt Active Directory ne joue, par contre, aucun rôle sur le nombre d’AC émettrices.

## Administration et Exploitation

L’AC disponible au sein de Windows Server 2003 permet une exploitation soit via une interface graphique de type console MMC soit via une interface mode ligne de commande.

### Sécurisation des accès logiques

La sécurisation des accès logiques passe, par exemple, par les actions d’administrations suivantes :



* Forcer une authentification par carte à puce ;
* Contrôler l’appartenance aux groupes sensibles ;
* Activer la séparation des rôles.

### Sécurisation des accès physiques

La sécurisation des accès physiques rentre dans le cadre de l’offre de services (livrables) qui accompagne la mise en œuvre d’une infrastructure de confiance.

### Délégation d’administration

Les services de certificats de Windows Server 2003 (R2) intègrent un modèle d’administration qui permet de satisfaire aux exigences des critères communs (Cf. section § «  » ) concernant la séparation des rôles et assurant ainsi qu’une seule personne ne soit pas capable de compromettre la sécurité des services d’IGC.

* + Les rôles que l’on peut ainsi mettre en œuvre sont conformes à ceux décrits dans le document « Certificate Issuing and Management Components Family of Protection Profiles » à l’adresse Internet <http://csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf>.

Une AC Windows Server 2003 (R2) propose en standard des rôles d’administration qui peuvent s’adapter à la plupart des processus de gestion du cycle de vie des certificats et des services d’IGC :

* *Gestionnaire de services d’IGC* - Configure et administre les serveurs de certificats, désigne les gestionnaires et renouvelle les certificats des autorités de certification ;
* *Gestionnaire de certificats* - Émet et révoque les certificats pour des groupes d'utilisateurs sur lesquels ils ont juridiction ;
* *Agent de recouvrement* ;
* *Demandeurs* - utilisateurs authentifiés étant autorisés à émettre une requête de certificat sur l’AC. Cela ne correspond pas à un rôle d’administration sur l’AC ;
* *Auditeur* - Audite les actions des administrateurs locaux, des gestionnaires de services et de certificats ;
* *Opérateur de sauvegardes*.

A ces rôles correspondent des droits d’accès à l’AC et au serveur qui l’héberge. Ces rôles possèdent également des équivalences en rôle d’administration Windows, facilitant ainsi leur implémentation.

### Plan de Reprise d’Activité (PRA)

La mise en œuvre d’une IGC doit nécessairement intégrer la définition de plans de reprise d’activité et de continuité d’activité afin d’assurer la meilleure disponibilité de se service. Il est nécessaire de distinguer les différents composants de l’architecture afin d’en définir le niveau de disponibilité attendu qui sera déterminé par l’impact en cas d’indisponibilité et la fréquence et la durée d’indisponibilité estimés.

De part nos retours d’expérience auprès des milliers de clients ayant mis en œuvre nos solutions, il apparaît que le composant le plus critique au bon fonctionnement de l’infrastructure de gestion de clés est l’accès aux CRL dont la consultation est obligatoire. Il est donc impératif que les CRL soient consultables en tout point de l’environnement et avec une garantie de disponibilité de 100%, il est possible d’obtenir ce type de disponibilité soit en multipliant les points de publication des listes de révocation définis de certificats émis soit en redondant et mettant en répartition de charge les points de publication par exemple à l’aide de moyens réseau redondés.

Dans une architecture distribuée, cette disponibilité pourra être obtenue par la publication de la CRL dans Active Directory, et donc par sa disponibilité au sein de chaque contrôleur de domaine.

La disponibilité des autres composants de l’IGC, AC et AE, n’est pas aussi critique que celle des CRL (ou de l’information de révocation) et devra être définie de manière précise lors de la phase de définition d’architecture détaillée de façon à déterminer le niveau protection nécessaire (depuis la mise en œuvre de procédures de sauvegarde et de restauration de type System State jusqu’à la mise en œuvre de solutions entièrement redondantes nécessitant de déployer un nombre deux fois plus important de machines hébergeant les services de l’autorité de certification).

Il est, par ailleurs, à noter que dans le cas de l’émission/renouvellement automatique des certificats les contrôleurs de domaine sont amenés à jouer un rôle d’AE et que dans ce cas la disponibilité/redondance est assurée par les mécanismes propres à Active Directory.

* + Vous trouverez de plus amples informations sur les recommandations en termes de sécurisation et de mise en œuvre de procédures de sauvegarde à l’adresse suivante : <https://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/mngpki.mspx>.

### Audit

Une AC Windows Server 2003 permet à la fois l’audit d’évènements réussis ou ayant échoués, qui sont inscris dans la file d’attente de Sécurité de la base d’évènements de Windows. Les catégories d’évènements suivants sont supportées :



* Sauvegarde et restauration de la base de l’AC ;
* Modification dans les configurations de l’AC ;
* Modification des paramètres de sécurité de l’AC ;
* Gestion et Génération de requêtes de certificats ;
* Révocation de certificats et publication de CRL ;
* Archivage et recouvrement de clés archivées ;
* Lancement & Arrêt des services de certificats.

### Gestion des traces

L’architecture de la plateforme Windows propose une structure d’accueil pour l’enregistrement d’évènements dans différents journaux (application, sécurité, système, etc.) avec des mécanismes de notification et de collecte, chaque évènement ayant des attributs clairement identifiés comme une source, un ID, un contexte de sécurité, etc.

Des interfaces d’instrumentation de la plate-forme comme *Windows Management Instrumentation* (en abrégé WMI) ou des solutions de supervision comme *Microsoft System Center Operation Manager* (en abrégé SCOM) tirent directement bénéfices de cette approche standard plateforme pour proposer une exploitation avancée de ces informations comme notamment de la corrélation d’évènements pour le déclenchement automatisé d’opérations de tâches d’exploitation.

Les journaux utilisés peuvent être dimensionnés en conséquence et offrent une gestion circulaire si besoin.

Comme toute application respectant les règles de développement de la plateforme Windows, les services de certificats de Windows Server 2003 (R2) s’appuient de façon appropriée sur ces journaux pour l’enregistrement des évènements qui lui sont relatifs. Le format d’exportation peut être converti au standard W3C.

Au-delà de ce comportement par défaut rien n’empêche la configuration d’un module de sortie; ce module recevant l’ensemble des notifications du moteur lorsque des opérations ont lieu (par exemple l’émission d’un certificat) peut donc stocker les logs dans une base SQL ou dans un fichier de log.

* + Il s’agit de l’un des deux points d’extensibilité du moteur tel que décrit dans la page MSDN « Certificate Services Architecture » à l’adresse Internet <http://msdn2.microsoft.com/en-us/library/Aa376540.aspx>.

L’utilisation d’un module de sortie personnalisé pour le stockage des logs dans une base Microsoft SQL Server conjointement à l’utilisation de Microsoft Reporting Services permet d’élaborer des états avancés.

Cette approche est, par exemple, celle suivie par la composante CMS de l’environnement Microsoft ILM 2007.

Il est possible de signer les fichiers, mais cette fonctionnalité n’est pas intégrée nativement.

D’autre part, il est possible de tracer les actions (modifications) sur les traces.

### Support de la virtualisation

Une seule AC peut être installée par instance serveur de Windows Server 2003. Par contre, une plateforme Windows Server 2003 comprenant le service de certificat est virtualisable dans une machine virtuelle gérée par Microsoft Virtual Server 2005.

* + La politique de support en environnement virtualisé est décrite à l’adresse Internet suivante : <http://support.microsoft.com/kb/897613>.
  + Les ressources techniques relatives à Microsoft Virtual Server sont disponibles à l’adresse Internet <http://www.microsoft.com/windowsserversystem/virtualserver/default.mspx>.

Une même License Windows Server 2003 permet d’utiliser sur la plateforme hôte jusqu’à 4 machines virtuelles Windows Server 2003.

## Interopérabilité

L’interopérabilité, aussi bien entre organisations, qu’au sein d’un environnement hétérogène d’une même organisation est assurée au travers du support des standards PKIX.

L’interopérabilité de l’AC Windows Server 2003 a été démontrée dans le cadre du projet *pki Challenge* (en abrégé pkiC), plus large projet d’interopérabilité IGC conduit à ce jour sous l’égide de l’EEMA, *the independent european association for e-business*, et cofinancé par le gouvernement suisse et la Commission Européenne. Ce projet vise à identifier, analyser et dépasser les problématiques d’interopérabilité entre les fournisseurs de solutions d’IGC.

* + Les différents rapports sont disponibles aux adresses Internet suivantes: <http://www.eema.org/index.cfm?fuseaction=focus.content&cmid=148&CFID=1265205&CFTOKEN=5d0b84ad83bfb3db-EE165315-FE45-BA16-A015751C772C5C43> et <http://www.eema.org/downloads/security_finished_papers/pkiC_final_report.pdf>.

L’autorité de certification Microsoft est par ailleurs certifiée « *US Federal Bridge AC* » (<http://www.cio.gov/fbca/techio.htm>)

### Boitiers HSM

Les services de certificats de Windows Server 2003 (R2) supportent l’utilisation de boitiers matériels (en abrégé HSM pour *Hardware Storage Module* en anglais) pour le stockage des bi-clés.

Ceci suppose simplement pour ces matériels la disponibilité d’un CSP comme c’est le cas avec :

* AEP SureWare Keyper Enterprise (<http://www.aepnetworks.com/products/key_management/keyper/ent_overview.aspx>) - FIPS 140-2 Level 4,
* Algorithmic Research PrivateServer (<http://www.arx.com/PrivateServer.html>) - FIPS 140-1 Level 3,
* Crysalis/Rainbow/SafeNet Luna SA (<http://www.safenet-inc.com/products/pki/lunaSA.asp>) - FIPS 140-2 Level 3,
* Crysalis/Rainbow/SafeNet Luna CA3 (<http://www.safenet-inc.com/products/pki/lunaCA3.asp>) - FIPS 140-1 Level 3,
* Eracom ProtectServer Orange (<http://www.eracom-tech.com/protectserver_orange.0.html>) - FIPS 140-1 Level 3,
* nCipher nShield (<http://www.ncipher.com/cryptographic_hardware/hardware_security_modules/8/nshield/>) - FIPS 140-2 Level-3 ;
* Et nCipher netHSM (<http://www.ncipher.com/cryptographic_hardware/hardware_security_modules/10/nethsm>) - FIPS 140-2 Level-3 ;

L’utilisation de boîtiers HSM est recommandée pour les AC en ligne. Cette dernière peut nécessiter plusieurs opérateurs/administrateurs pour démarrage, avec cartes.

### Evaluation Critères Communs

L’évaluation Critères Communs (en abrégé CC pour *Common Criteria* en anglais) est un standard international (ISO/CEI 15408) pour la [sécurité des systèmes d'information](http://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information). Le nom complet du standard est *Common Criteria for Information Technology Security Evaluation*.

Les Critères Communs a pour vocation d’être utilisés comme base pour l’évaluation des propriétés de sécurité des produits et systèmes des Technologies de l’Information. En établissant une telle base de critères communs, les résultats d’une évaluation de la sécurité des Technologies de l’Information seront significatifs pour une plus large audience.

Les CC permettent de comparer les résultats d’évaluations de sécurité menées indépendamment les unes des autres. Cela est rendu possible grâce à un ensemble commun d’exigences pour les fonctions de sécurité des produits et systèmes et pour les mesures d’assurance qui leur sont appliquées pendant une évaluation de sécurité. Le processus d’évaluation établit un niveau de confiance dans le fait que les fonctions de sécurité de tels produits et systèmes et les mesures d’assurance qui leur sont appliquées satisfont à ces exigences. Les résultats de l’évaluation peuvent aider les acheteurs à déterminer si le produit ou le système est suffisamment sûr pour l’application qu’ils envisagent et si les risques liés à la sécurité qui sont implicites dans son utilisation sont tolérables.

Les CC sont utiles en tant que guide pour le développement des produits ou systèmes incluant des fonctions de sécurité des Technologies de l’Information et pour l’approvisionnement de produits ou systèmes commerciaux dotés de telles fonctions. Pendant l’évaluation, un tel produit ou système est qualifié de cible d’évaluation (en abrégé TOE pour *Target Of Evaluation* en anglais). De telles TOE peuvent être par exemple des systèmes d’exploitation, des réseaux informatiques, des systèmes distribués et des applications.

* + Vous trouverez l’ensemble de la documentation relative au CC sur le site de la Direction Centrale de la Sécurité des Systèmes d’Information (en abrégé DCSSI)« Critères et méthodologie d'évaluation » à l’adresse Internet suivante : <http://www.ssi.gouv.fr/fr/confiance/methodologie.html>.

Les services de certificat de Windows Server 2003, ainsi que la plateforme Windows sous-jacente, ont fait et font, selon les versions considérées, l’objet d’une évaluation Critères Communs.

Ainsi, Les services de certificat de Windows Server 2003 sont aujourd’hui :

* EAL (*Evaluation Assurance Level*) 4+ : *EAL 4 Augmented with ALC\_FLR.3* (*Systematic Flaw Remediation*) *and AVA.VLA.4* (*Highly Resistant Vulnerability Analysis*) ;
* Conforme avec CIMC (*Certificate Issuing and Management Components*) *Security Level 3 Protection Profile*, version 1.0 ;
  + Le rapport d’évaluation Critères Communs correspondant est disponible à l’adresse Internet <http://www.commoncriteriaportal.org/public/files/epfiles/st_vid9507-vr.pdf> ainsi que sur le site du NIAP (*National Information Assurance Partnership*) à la page « NIAIP Certification for Windows Server 2003 Certificate Server » (<http://niap.nist.gov/cc-scheme/st/ST_VID4024.html>).

La plateforme Windows Server 2003 SP1 (tout comme Windows XP SP2) est également *EAL 4 Augmented with ALC\_FLR.3* (*Systematic Flaw Remediation*) *and AVA.VLA.4* (*Highly Resistant Vulnerability Analysis*).

* + Le rapport d’évaluation Critères Communs correspondant est disponible à l’adresse Internet <http://www.commoncriteriaportal.org/public/files/epfiles/st_vid9506-vr.pdf> ainsi que sur le site du NIAP à la page « NIAP Certification for Windows XP SP2 and Windows Server 2003 SP1 » (<http://niap.nist.gov/cc-scheme/st/ST_VID4025.html>).

## Standards supportés

L’IGC Windows respecte les standards mentionnées explicitement en Annexe A, section § « Standards issus du projet PKIX de l’IETF » issus du groupe de travail *Public Key Infrastructure X.509* (en abrégé PKIX. Il s’agit en particulier des standards tels que RFC 2459 [[RFC 2459](#RFC2459)], RFC 3280 [[RFC 3280](#RFC3280)], RFC 2560 [[RFC 2560](#RFC2560)].

Les certificats délivrés par l’IGC Windows sont au format X.509 v3 [[RFC 3280](#RFC3280)], ce qui permet de modifier les extensions des certificats pour répondre à des besoins spécifiques (des informations d’authentification par exemple) ce qui peut générer parfois des difficultés en matière d’interopérabilité.

L’IGC Windows permet de définir ses propres extensions dans des gabarits (nécessite une AC en « mode entreprise »), et contourne ainsi la difficulté.

L’IGC Windows se base également sur les standards RSA Security PKCS #1 [[PKCS#1](#PKCS1)], PKCS #7 [[PKCS#7](#PKCS7)], PKCS #10 [[PKCS#10](#PKCS10)], PKCS #12 [[PKCS#12](#PKCS12)].

Pour ce qui est de PKCS #11, Microsoft a pris la décision de ne pas le supporter ; ce dernier étant jugé inutilement lourd, compliqué et peu performant. PKCS #11 est, en effet une API très vaste rarement implémentée dans son ensemble.

L’ensemble des fonctions prévues par PKCS #11 est supporté en standard par CryptoAPI, l’API de gestion des opérations cryptographiques de la plaeforme Windows. CryptoAPI répond aux besoins cryptographiques des applications, et s’applique par conséquent aux traitements de son IGC.

Dans ce contexte, CryptoAPI permet nativement de :

* Les opérations de chiffrement avec les algorithmes standard (MD5, SHA-1, RC2, RC4, DES, 3DES, AES, RSA, DSS, DH),
* La gestion des messages de signature et de chiffrement aux formats standard (PKCS #7 [[PKCS#7](#PKCS7)], CMS [[RFC 3852](#RFC3852)]),
* La gestion des demandes de certificat, des certificats et des CRLs aux formats standards (PKCS #10 [PKCS#7], CMC [[RFC 2797](#RFC2797)], certificats X509v3 [[RFC 3280](#RFC3280)], CRL X509v2 [[RFC 3280](#RFC3280)])
* L’utilisation et la vérification des certificats, des signatures, des CRLs selon les standards tels que RFC 2459 [[RFC 2459](#RFC2459)] et 3280 [[RFC 3280](#RFC3280)]. L'architecture prend en compte la vérification en ligne telle qu’OCSP [[RFC 2560](#RFC2560)], etc.

### Formats des certificats et validation

Comme mentionné ci-dessus, l’IGC Windows respecte le format X.509 v3 pour les certificats et les profils associés pour l’utilisation de ces certificats, les listes de révocations y compris les CRL Delta [[RFC 3280](#RFC3280)], ainsi que le support d’OCSP ([[RFC 2560](#RFC2560)]. Le support standard (toutefois optionnel) des extensions CDP (*cRLDistributionPoint*) et AIA (*id-pe-authorityInfoAccess*) facilite grandement la validation des certificats (révocation et chaine de certification) entre technologies de fournisseurs tiers.

Les services de certificat de Windows Server 2003 (R2) permet d’émettre des certificats au format standard pour une utilisation par des applications non Microsoft et/ou non Windows respectueuses de ces standards.

Inversement, les applications Microsoft Windows (Outlook, Outlook Express, Outlook Web Access pour S/MIME, SSL/TLS, IPsec, etc.) s’appuient sur CryptoAPI et peuvent être déployées pour une utilisation de certificats émis par des AC non Windows.

L’architecture ouverte de CryptoAPI permet la validation en ligne (OCSP) par le biais d’un module client de validation (*Revocation Provider* en anglais) disponible auprès de fournisseurs tiers. Cette validation peut se faire contre un répondeur OCSP non Microsoft/non Windows.

Les nouvelles versions de la plateforme Windows (Vista et Windows Server 2008) intègrent une implémentation OCSP.

### Support des CRL et CRL différentielles

L’IGC Windows est conforme à la RFC 2459 [[RFC2459](#RFC2459)] qui définit les règles d'utilisation des certificats et CRL : validation de la signature avec l'autorité au-dessus, période de validité, non révocation, contraintes d'espace de noms, par rapport au sujet, politique, extensions critiques reconnues, certificat est de type AC (contraintes élémentaires).

L’IGC Windows supporte également les delta CRL tels que spécifié dans la RFC 3280 [[RFC 3280](#RFC3280)]. Une delta CRL permet de rafraîchir la CRL de base avant son expiration, en spécifiant une nouvelle base dans la delta CRL.

### Formats des requêtes de certificats

Les Services de certificats de Windows Server 2003 supportent nativement les requêtes de certification (en abrégé CSR pour *Certificate Signing Request* en anglais) au :

* Format  PKCS #10 [[PKCS#10](#PKCS10)] ;
* Standard CMC tel que décrit dans la RFC 2797 [[RFC 2797](#RFC2797)].

### Formats de mise à disposition des certificats et des clés

Les formats suivants sont supportés :

* PKCS #7 [[PKCS#7](#PKCS7)],
* PKCS #12 [[PKCS#12](#PKCS12)] (.p12 ou .pfx),
* PEM (.pem),
* DER (.der),
* CER (.cer).

Le format PEM est obtenu a partir d’une conversion par ligne de commande via la commande *certutil –encode*.

### Format PFX

Le standard PKCS #12 [[PKCS#12](#_PKCS)] permet la sauvegarde et l’échange d’une bi-clé RSA et de son certificat associe à l’aide d’un fichier protégé par mot de passe.

### Algorithmes de chiffrement

L’IGC Windows et, d’une façon générale Windows Server 2003, s’appuient sur CryptoAPI qui comporte une architecture ouverte de gestion d’opérations cryptographiques à base de CSP pour les opérations cryptographiques en tant que telles.

La liste ci-dessous représente un éventail (non exhaustif) des algorithmes supportes en standard sur la plateforme Windows :

* RC2, RC4, DES, 3DES, AES128, AES192, AES256,
* MD4, MD5, SHA-1,
* HMAC (MD5, SHA-1),
* RSA, DH, DSS.

### Longueur de clé

La longueur de clé est en partie déterminée par l’algorithme cryptographique sélectionné. Les longueurs de clés supportés par une AC Windows Server 2003 (R2) varient entre 384 bits et 16,384 bits, selon le CSP choisi. Dans un déploiement classique, les certificats utilisateurs ont des clés de 1,024 bits et ceux des AC racine ont 4,096 bit.

### Extensions supportées

Les extensions suivantes sont supportées :

* *KeyUsage*,
* *Enhanced* Key Usage,
* *BasicConstraints*,
* *SubjectKeyIdentifier*,
* *AuthorityKeyIdentifier*,
* *CRLDistributionPoints*,
* *CertificatePolicies*,
* *SubjectAltName*.

Les extensions suivantes relatives aux CRL sont supportées :

* *AuthorityKeyIdentifier*,
* *CRLNumber*.

# Mise en œuvre des services d’IGC

## Performances

L’AC disponible au sein de Windows Server 2003 (R2) au travers des services de certificat à été testée pour une capacité de stockage de plusieurs dizaines de millions de certificats émis et pour une capacité d’émission de plusieurs millions de certificats par jour (pour une longueur de clé publique de 2048 bits).

## Dimensionnement et matériels

La solution d’IGC Windows est implémentée dans les environnements serveur Windows Server 2003, objet de ce livre-blanc, et Windows Server 2008.

Pour ce qui est de Windows Server 2003, la version Windows Serveur 2003 Enterprise Edition est requise. Il est par ailleurs recommandé d’utiliser des boîtiers HSM.

Les pré-requis d’un serveur sont :

* Matériel : Pentium 4 1,8 Ghz, 1 Go RAM, 40 Go DD disponible
* Logiciel : Windows Server 2003 Enterprise Edition ou DataCenter Edition

Les pré-requis d’un poste client sont :

* Matériel : Pentium 4 1 Ghz, 512 Mo RAM
* Logiciel : Windows XP / Vista, Windows 2000 dans une moindre mesure

## Méthodologie

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



Les sections suivantes décrivent les différentes étapes de ce chantier.

### Phase 1 – Vision et Périmètre

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 des processus seront aussi analysés dans l’objectif de pouvoir proposer des solutions techniques adaptées ou apportant une amélioration (gestion des changements, traitement des demandes EE, processus de traitement des incidents, etc.).

Le but est 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 et équipements non-Windows :* il est important de comprendre comment sont utilisés ces systèmes 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.

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,
* Une 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, a permise de définir les grandes lignes de l’architecture pressentie suivant le contexte. Cette étape a donc pour objectif d’affiner l’architecture générale IGC.

Il convient d’étudier plus précisément notamment :

* *Conception de la hiérarchie d’AC* :
* Définition des rôles des AC dans la hiérarchie de confiance,
* Définition du nombre d’AC et leur localisation,
* Règles de convention de noms,
* Plan d’intégration avec Active Directory.
* *Conception des configurations* :
* Sécurisation du stockage des clés - type, nombre et localisation des HSM,
* Dimensionnement des serveurs, RAID, bases de données/log, localisation,
* Sécurisation des serveurs – l’ACR et les AC intermédiaires doivent être sécurisés et non utilisés,
* Renforcement de la sécurité des AC émettrices.
* *Conception des règles d’administration et de délégation* :
* Identification des rôles et des besoins de séparation des rôles pour l’administration des AC (sauvegarde/restauration, audit, etc.),
* Identification des utilisateurs (ou groupe) et assignation dans les rôles identifiés,
* Définition des règles de gestion pour chacun des rôles.
* *Création d’une politique générique d’enrôlement et de renouvellement des certificats*
* *Création d’une politique générique des gabarits de certificat*
* *Conception d’une stratégie de groupe (GPO) générique pour le déploiement des certificats*
* *Conception de la politique générique de révocation des certificats*
* Définition de la procédure de révocation (quand, pour quelles raisons, sur quels événements, etc.)
* Choix d’une localisation de la CRL et des méthodes d’accès (HTTP, LDAP),
* Choix du type de CRL (base, delta), de la fréquence de mise à jour et des périodes de validité.
* *Conception de la politique de recouvrement de clé*
* *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 IGC.



### Phase 3 – Réalisation

Cette étape a pour objectif de construire et tester l’infrastructure proposée. Les choix techniques sont validés et affinés en réalisant des prototypes.

Cette étape met donc en œuvre des :

* Prototypes de validation technique afin de tester les paramétrages, configurations, organisations, etc.

Ces prototypes identifiés préalablement sont nécessaires à ce stade pour affiner les différents paramètres des composantes du système cible. Ils peuvent également mettre en évidence des problèmes particuliers d’intégration. En effet, l’étude des environnements généraux, serveur, poste de travail et périphérique, conduit à la mise en place de sous-projets pour lesquels il convient de conserver une vue globale vis-à-vis de l’infrastructure générale cible.

* Prototypes opérationnels

Le but d’un prototype opérationnel est de disposer d’un ensemble cohérent de fonctionnalités du système cible dans le cadre d’exploitation prévu afin d’obtenir des réactions et corriger les éventuels problèmes.

Les prototypes permettent de recetter la plate-forme technique et la future architecture avant la généralisation de la solution et la définition des modalités d’industrialisation.

Ces prototypes opérationnels nécessitent la constitution d’une plate-forme d’intégration qui sera utilisée tout au long des étapes restantes (autres lots) du projet.

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

* Les procédures de sauvegarde et de restauration (AC, clés d’AC, CRL, etc.),
* Les procédures de supervision,
* Les procédures d’installation,
* Le guide d’opération.

procedure_dd*Livrable* : Le livrable de cette étape est constitué du document d’architecture détaillée intégrant les procédures d’administration et d’exploitation de l’architecture ainsi définie.

### Phase 4 – Pilote

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

Il est nécessaire de déterminer quel sous-ensemble fera l’objet de l’expérimentation pilote sachant qu’il 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. 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. Les transitions doivent être les plus douces possibles.

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

## Coûts

Les services de certificatsde Windows Server 2003 (R2) constituent l’un des services Serveur de la plateforme Windows Server 2003 (R2).

Il n’y a pas de facturation spécifique aux fonctions nécessaires pour établir une infrastructure de confiance avec l’IGC Windows.

Ces fonctions sont disponibles dans Windows Server 2003, et leur droit d’utilisation inclus dans le coût des licences associées.

## Support

Le niveau de support est le même que pour la plateforme Windows et suppose un contrat de support obtenu auprès de Microsoft ou de ses partenaires agréés.

Le niveau de disponibilité varie selon le type de contrat de support souscrit auprès de Microsoft ou de ses partenaires agréés.

* + La gamme des services de support disponibles auprès de Microsoft est décrite à l’adresse Internet <http://support.microsoft.com/default.aspx?scid=fh;FR;Offerings&ln=fr>.

Au sein de cette gamme, *Microsoft Support Premier* est un contrat de support adaptable, pouvant être personnalisé aux besoins et objectifs de l’organisation.

Les services principaux se composent des 2 éléments suivants :

1. Gestion technique du compte avec des services techniques personnalisés et proactifs ;
2. Accès hautement réactif aux experts techniques du support Microsoft, 24 heures sur 24, 7 jours sur 7.
   * Le support Premier est décrit à l’adresse Internet <http://support.microsoft.com/gp/premsup>.

# Conclusion

A l’heure ou les systèmes d’informations s’ouvrent de plus en plus vers l’extérieur et que les échanges s’accentuent la sécurité est devenue une nécessité pour s’assurer contre l’usurpation d’identité, les accès non autorisés, le vol ou la perte d’information, etc.

Dans la diversité des solutions de sécurité proposées l’IGC embarquée dans Windows Serveur 2003 possède de nombreux atouts pour devenir LA plateforme de référence :

* Basée sur des standards
* Incluant des fonctions de sécurités complètes :
* Authentification,
* Chiffrement,
* Signature.
* Exploitée par de nombreux services et applications
* Systèmes d’exploitation,
* Messagerie,
* Applications bureautiques,
* Protocoles réseaux,
* Etc.

Les services de certificat de Windows Server 2003 (R2) apportent tous les services d’une plateforme de confiance complète et est à même de délivrer des moyens d’accès sécurisés par certificat numérique, y compris les supports cryptographiques pour de l’authentification forte et le transport des secrets.

Reposant sur une architecture évolutive et ouverte vers l’extérieur, ce service possède l’avantage d’être inclus comme un service de la plateforme Windows Server ce qui porte son coût au seul coût d’acquisition de la plateforme Windows.

L’intégration avec Active Directory et Windows ainsi que l’utilisation de gabarit de certificat apporte des capacités de déploiement, de gestion et d’automatisation sans communes mesures avec les autres offres du marché.

Enfin, cette solution développée, améliorée, maintenue et intégrée au système d’exploitation depuis Windows NT 4.0 par Microsoft est un gage de pérennité pour une entreprise devant s’engager dans une IGC pendant des années.

1. Références

**Standards issus du projet PKIX de l’IETF**

Le groupe de travail *Public Key Infrastructure X.509* (en abrégé PKIX), formé en 1995 par l’*Internet Engineering Task Force* (en abrégé IETF), visait à la définition d’un ensemble de profils de certificats et de modèles opérationnelles qui conviendraient sur Internet.

Ce groupe est à l’origine de très nombreuses RFC aujourd’hui implémentées dans les solutions d’IGC. La liste complète est disponible sur la page d’accueil du groupe à l’adresse Internet <http://www.ietf.org/html.charters/pkix-charter.html>.

RFC 2527 « *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* », <http://tools.ietf.org/html/rfc2527>

RFC 2459 « *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* », <http://tools.ietf.org/html/rfc2459>

RFC 2560 « *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* », <http://tools.ietf.org/html/rfc2560>

RFC 2585 « *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP* », <http://tools.ietf.org/html/rfc2585>

RFC 2587 « *Internet X.509 Public Key Infrastructure LDAPv2 Schema*», <http://tools.ietf.org/html/rfc2587>

RFC 2797 « *Certificate Management Messages over CMS* », <http://tools.ietf.org/html/rfc2797>

RFC 3279 *« Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile »,* <http://tools.ietf.org/html/rfc3279>

RFC 3280 « *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* », <http://tools.ietf.org/html/rfc3280>

RFC 3647 « *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* », <http://tools.ietf.org/html/rfc3647>

RFC 3852 « *Cryptographic Message Syntax (CMS)* », <http://tools.ietf.org/html/rfc3852>

**Autres standards**

RFC 4556 « *Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)* », <http://tools.ietf.org/html/rfc4556>

RFC 4557 « *Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)* », <http://tools.ietf.org/html/rfc4557>

PKCS #1 « *RSA Cryptography Standard* », <http://www.rsa.com/rsalabs/node.asp?id=2125>

PKCS #3 « *Diffie-Hellman Key Agreement Standard* », <http://www.rsa.com/rsalabs/node.asp?id=2126>

PKCS #7 « *Cryptographic Message Syntax Standard* », <http://www.rsa.com/rsalabs/node.asp?id=2129>

PKCS #8 « *Private-Key Information Syntax Standard* », <http://www.rsa.com/rsalabs/node.asp?id=2130>

PKCS #10 « *Certification Request Syntax Standard* », <http://www.rsa.com/rsalabs/node.asp?id=2132>

PKCS #12 « *Personal Information Exchange Syntax Standard* », <http://www.rsa.com/rsalabs/node.asp?id=2138>

PC/SC v1.0, <http://www.pcscworkgroup.com/specifications/specdownloadV1.php>

SCEP, draft Internet IETF « *Cisco Systems' Simple Certificate Enrollment Protocol (SCEP)* », <http://www.ietf.org/internet-drafts/draft-nourse-scep-15.txt>

USB-CCID, <http://www.usb.org/developers/devclass_docs>

**Ressources Windows Server 2003**

Les ressources relatives aux services de certificat de Windows Server 2003 (R2) sont regroupées à l’adresse Internet suivante : [http://www.microsoft.com/Windowsserver2003/technologies/pki/default.mspx](http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx)

« Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure », <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx>

« Designing a Public Key Infrastructure (Windows Server 2003) », <http://go.microsoft.com/fwlink/?LinkID=84709>

« Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003 », <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx>

« Advanced Certificate Enrollment and Management », <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx>

« Certificate Autoenrollment in Windows Server 2003 », <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx>

« Implementing and Administering Certificate Templates in Windows Server 2003», <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspx>

« Key Archival and Management in Windows Server 2003 », <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/kyacws03.mspx>

« Windows Server 2003 PKI Operations Guide », <http://technet2.microsoft.com/WindowsServer/en/Library/e1d5a892-10e1-417c-be13-99d7147989a91033.mspx>

**Ressources Windows Vista**

« Windows Vista Smart Card Infrastructure », <http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en>

« Troubleshooting PKI Problems on Windows Vista », <http://go.microsoft.com/fwlink/?LinkId=85484>

1. Pour des informations complémentaires

Pour des informations générales sur les services de certificats de Windows Server 2003 (R2), vous pouvez consulter l’adresse Internet <http://www.microsoft.com/pki>

Pour des informations générales sur la solution Microsoft ILM 2007, vous pouvez consulter l’adresse Internet <http://www.microsoft.com/ilm>

Pour les dernières informations sur Windows Server System, vous pouvez consulter le site dédié à Windows Server System à l’adresse Internet <http://www.microsoft.com/windowsserversystem>.

1. RFC 2631 « *Diffie-Hellman Key Agreement Method* » (<http://tools.ietf.org/html/rfc2631>) en 1999 puis norme ANSI X9.42 en 2000. [↑](#footnote-ref-2)