

**Grille d’évaluation Services de certificats Active Directory (AD CS) 2008 (R2)**

Version 1.0

Publication : septembre 2009

Auteur : Philippe Beraud

Contributeurs : Frédéric Hervo, Stéphane Metenier, Cyril Voisin

Copyright

© 2009 [Microsoft Corporation](http://www.microsoft.com). Tous droits réservés.

Résumé

Le rôle serveur Services de certificats Active Directory (Active Directory Certificate Services en anglais ou AD CS en abrégé) au sein de la plateforme Windows Server 2008 (R2) propose 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.

Ce livre blanc propose une grille d’évaluation d’AD CS et intègre de nombreux liens sur la documentation disponible.

© 2009 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 1](#_Toc241044788)

[1.1 Objectifs et organisation du livre blanc 4](#_Toc241044789)

[1.2 Evaluation au sens des Critères Communs 5](#_Toc241044790)

[2 Enveloppe fonctionnelle 7](#_Toc241044791)

[2.1 Gestion des certificats et des clés 7](#_Toc241044792)

[2.2 Fonctionnalités connexes 21](#_Toc241044793)

[2.3 Administration et Exploitation 28](#_Toc241044794)

[3 Enveloppe technique 33](#_Toc241044795)

[3.1 Architecture 33](#_Toc241044796)

[3.2 Mise en place 40](#_Toc241044797)

[3.3 Performances 42](#_Toc241044798)

[3.4 Interopérabilité et options 43](#_Toc241044799)

[4 Coûts et services 45](#_Toc241044800)

[4.1 Coût 45](#_Toc241044801)

[4.2 Niveau de support 45](#_Toc241044802)

[4.3 Disponibilité du support 45](#_Toc241044803)

[Annexe A. Références 47](#_Toc241044804)

[Annexe B. Synthèse des composants et fonctionnalités 50](#_Toc241044805)

[Annexe C. Pour des informations complémentaires 52](#_Toc241044806)

# 

# Introduction

Le rôle serveur **Services de certificats Active Directory** (Active Directory Certificate Services en anglais ou AD CS en abrégé) dans la plateforme Windows Server 2008 (R2) propose 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. Ce rôle serveur correspond à la cinquième génération de ces services.

Les organisations peuvent s’appuyer sur AD CS 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. AD CS comprend dans le même temps des fonctionnalités qui permettent la gestion de l’enrôlement et de la révocation des certificats dans le contexte d’environnements distribués.

procedure_ddPour ce faire, les services du rôle (role service en anglais) ou composants suivants d’AD CS peuvent être installés sur une plateforme Windows Server 2008 (R2) au travers de l’option Services de certificats Active Directory (en anglais Active Directory Certificate Services) de l’assistant Ajouter des rôles (Add Roles en anglais) du Gestionnaire de serveur (Server Manager en anglais) :

* **Autorité de certification** (Certification Authority - CA) - Ce composant permet la mise en œuvre d’autorités de certification (AC ou CA en abrégé pour Certification Authority en anglais) racine et subordonnée(s) utilisées pour l’émission de certificats à destination d’utilisateurs, de machines et de services, ainsi que pour la gestion de leur validité.

Ce composant propose deux modes / types d’installation :

1. mode autonome destiné principalement aux AC racine et intermédiaire(s) hors ligne ;
2. mode entreprise destiné aux AC émettrices dans une infrastructure Active Directory.

Ce composant implémente le format X.509 v3 et les profils tels que décrits dans la RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [[RFC 3280](#RFC3280)] qui est une mise à jour de la RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile [[RFC 2459](#RFC2459)] pour l’utilisation de ces certificats, les listes de révocations (LRC ou CRL en abrégé pour Certificate Revocation List en anglais) X.509 v2 y compris les delta CRL.

* + Une description de ce composant est disponible à l’adresse <http://go.microsoft.com/fwlink/?LinkID=85473>.

Ce composant est supporté par une installation de type Server Core de Windows Server 2008 R2 qui fournit un environnement minimal pour l'exécution des rôles serveur spécifiques, réduisant ainsi de facto les exigences de gestion et de maintenance, ainsi que la surface d’attaque pour les rôles serveur considérés.

* **Inscription de l’autorité de certification via le Web** *(*CA Web Enrollment - CAWE*)* – L’enrôlement Web permet aux utilisateurs de se connecter à une AC au moyen d’un butineur afin d’effectuer une demande de certificat X.509 v3, obtenir des CRL X.509 v2, y compris les *delta CRL*, etc.
  + Une description de ce composant est disponible à l’adresse <http://go.microsoft.com/fwlink/?LinkId=85476>.
* **Répondeur en ligne**(Online Responder Service*)* – Le service Répondeur en ligne implémente Online Certificate Status Protocol (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 support est conforme à la RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP [[RFC 2560](#RFC2560)].

* + Une description de ce composant est disponible à l’adresse <http://go.microsoft.com/fwlink/?LinkID=85474>.
* **Service d’inscription de périphériques réseau** (Network Device Enrollment Service - NDES*)* – Le service NDES permet à des routeurs et à d’autres dispositifs ou équipements actifs de réseau d’obtenir des certificats X.509 sur la base du protocole Simple Certificate Enrollment Protocol (SCEP) [[SCEP](#SCEP)] de Cisco Systems Inc.

SCEP [[SCEP](#SCEP)] a été développé pour permettre l’émission sécurisée et évolutive de certificats à destination de dispositifs réseau par des AC. Le protocole supporte la distribution de la clé publique de l’AC ou celle de l’autorité d’enregistrement (AE ou RA en abrégé pour Registration Authority en anglais), l’enrôlement de certificat, la révocation de certificat, les requêtes de certificat et les requêtes de révocation de certificat.

* + Une description de ce composant est disponible à l’adresse <http://go.microsoft.com/fwlink/?LinkId=85475>.

A cette liste de composants, Windows Server 2008 R2 introduits deux nouveaux composants fondés :

* **Service Web de politique d’enrôlement de certificats** (Certificate Enrollment Policy Web Service - CES) – Ce service de type proxy permet l’obtention d’une politique de certificats sur un transport HTTPS
* **Service Web d’enrôlement de certificats** (Certificate Enrollment Web Service - CEP) – Ce service de type proxy permet l'enrôlement et le renouvellement de certificats sur un transport HTTPS.
  + Le livre blanc [Windows Server 2008 R2 Certificate Enrollment Web Services Whitepaper](http://download.microsoft.com/download/C/2/2/C229E624-36E4-4AD8-9D86-F564ED539A16/Windows%20Server%202008%20R2%20Certificate%20Enrollment%20Web%20Services.doc)[[1]](#footnote-1) explique les scénarios de déploiement, les exigences et les configurations recommandées et propose des procédures étape par étape pour vous aider à installer et configurer ces nouveaux services de rôle.

Les différents composants d’AD CS de Windows Server 2008 (R2) permettent d’émettre et de gérer des certificats X.509 au format standard pour une utilisation par des applications, services et systèmes Microsoft, non Microsoft et/ou non Windows respectant les protocoles et standards mentionnés le cas échéant ci-dessus.

Ils autorisent ainsi la matérialisation d’une infrastructure de confiance au travers de la mise en œuvre de services d’Infrastructure de Gestion de Clés (IGC ou PKI en abrégé pour Public Key Infrastructure en anglais).

procedure_ddAD CS constitue l’une des technologies plateforme des solutions Forefront d’identité et de sécurité de Microsoft, au même titre, par exemple, que :

* l’annuaire d’entreprise Active Directory (ou sa déclinaison applicative Active Directory Lightweight Directory Services ou AD LDS en abrégé) avec lequel une AC AD CS en mode entreprise peut s’intégrer et permettre alors :

1. la validation des identités des utilisateurs, des machines, des dispositifs ou des services ;
2. la publication de certificats, de CRL ;
3. mais également la publication de ressources globales d’une infrastructure de confiance à destination d’applications, services et systèmes reposant sur les technologies à clé publique comme, par exemple, les OID (Object Identifiers en anglais) déclarés, les modèles de certificats, les services d’enrôlements disponibles, les AC racines de confiance, les AC de confiance pour certains services comme l’ouverture de session par carte à puce (smartcard logon en anglais), Kerberos, etc.

* les technologies « Geneva » d’authentification ouverte vis-à-vis de laquelle une AC AD CS peut délivrer des certificats (de signature, d’authentification client, d’authentification serveur, etc.) à destination de ses différentes composantes ;

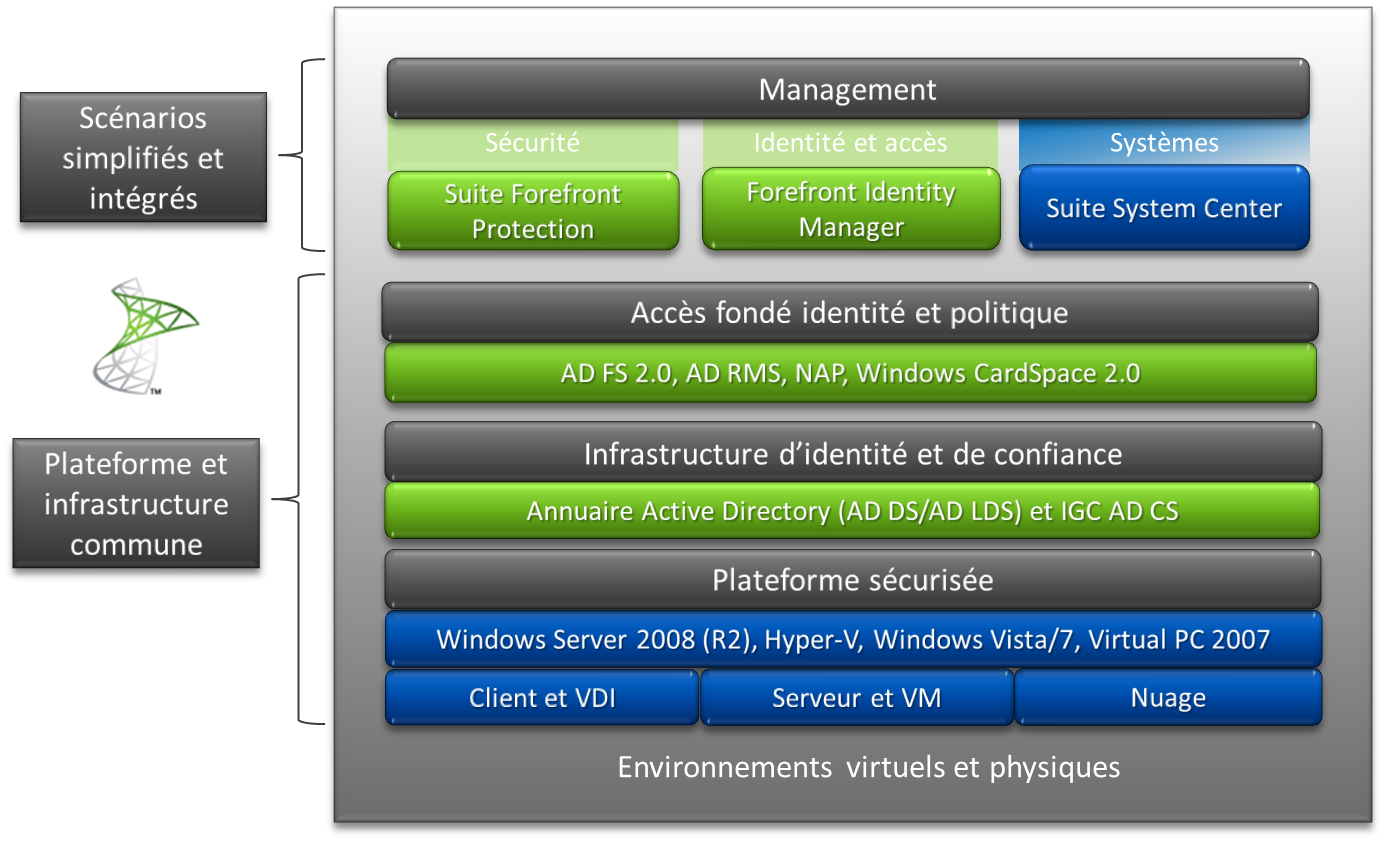
Les technologies “Geneva” primées dans la catégorie « Meilleure innovation » à l’occasion de la conférence EIC (European Identity Conference) 2009 et constituées d’Active Directory Federation Services (AD FS) 2.0, de Windows Identity Foundation (WIF) 1.0 et de Windows CardSpace 2.0, en interaction notamment avec la plateforme Windows Azure dans le nuage proposent :

* une nouvelle approche de l’identité et de l’authentification unique (SSO en abrégé pour Single Sign On en anglais) qui aide à simplifier au sein de l’entreprise, entre organisations, sur le Web et dans les nuages, l’accès aux applications, aux services Web et à d’autres systèmes.
* une interopérabilité native intégrée via des standards internationaux comme OASIS WS-Trust, WS-Federation, et SAML 2.0 et des revendications et implémente la vision de méta système d'identité pour une identité ouverte et interopérable quel que soit le contexte.

[](http://www.microsoft.com/forefront)Les solutions Forefront d’identité et de sécurité sont au cœur de la [stratégie Business Ready Security](http://www.microsoft.com/forefront/en/us/business-ready-security.aspx)[[2]](#footnote-2) de Microsoft. Ces dernières sont conçue autour de 6 scénarios principaux : messagerie sécurisée, collaboration sécurisée, hôte sécurisé, sécurité intégrée et gestion des identités et des accès.

* + Ces différentes solutions sont présentées dans le portail Web Microsoft Forefront à l’adresse <http://www.microsoft.com/forefront>.

Pour ce faire, la gamme Microsoft Forefront propose une ligne complète de technologies et produits d’identité et sécurité pour vous aider à développer votre entreprise en toute sécurité, et réduire vos coûts. Par leur intégration dans votre infrastructure informatique existante et par leur déploiement et leur administration simples à réaliser, ces technologies et produits assurent une plus grande protection, permettent une plus grande productivité en facilitant les accès sécurisés et un meilleur contrôle de votre entreprise grâce à leurs capacités de gestion.



Ainsi, dans le contexte de ce livre blanc, le produit Microsoft Forefront Identity Manager(en abrégé FIM) 2010 en tant que solution de gestion du cycle de vie des identités, des certificats et supports (carte à puce (smart card en anglais), jeton USB, etc.) offre les services :

1. d’autorité d’enregistrement (AE ou RA en abrégé pour Registration Authority en anglais) évoluée pour des AC AD CS 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 en abrégé 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.

Forefront fournit une protection qui prend en compte l’ensemble des systèmes et données de votre entreprise, tout en permettant l’accès de vos employés, en tout lieu, sur la base de leur identité. Côté gestion, Forefront sait également tirer parti des investissements existants sur la gamme de produits de gestion Microsoft System Center.

Enfin, Microsoft a une capacité à intervenir sur tous les maillons du système d’information de l’entreprise et de proposer des solutions soit hébergées en interne, soit dans le nuage, soit avec une combinaison des deux :

*« Microsoft is one of the few vendors that can truly go end-to-end (cloud-edge-server-client) to make businesses more secure.* »

Enterprise Strategy Group Eric Ogren, June 15, 2006

[At the Forefront of Microsoft Security](http://www.internetnews.com/bus-news/article.php/3613576), InternetNews.com

## Objectifs et organisation du livre blanc

Le document présent propose une grille de présentation / d’évaluation des services d’IGC proposés par Microsoft au travers d’AD CS, de ses différents composants, et de la complémentarité de l’offre Microsoft Forefront Identity Manager (FIM) 2010 (pour notamment les certificats utilisateurs X.509 v3). FIM 2010 est le successeur de Microsoft Identity Lifecycle Manager (ILM) 2007.

Ce livre blanc se veut un document compagnon :

* du Webcast de la session AD CS Windows Server 2008 enregistré lors des Microsoft TechDays 2008. La vidéo correspondante est disponible à l’adresse <http://www.microsoft.com/france/vision/mstechdays08/WebcastTechNet.aspx?EID=8e57e90e-f1e7-4ca4-bf39-2763ddbadacc> ;
* du Webcast AD CS Windows Server 2008 R2  enregistré lors des Microsoft TechDays 2009. ; La vidéo correspondante est disponible à l’adresse <http://www.microsoft.com/france/vision/mstechdays09/Webcast.aspx?EID=3d091e1c-e3f3-47ad-a411-251115c7c516>.

Et complète la vue d’ensemble proposé par l’article TechNet Magazine [PKI Enhancements in Windows 7 and Windows Server 2008 R2](http://technet.microsoft.com/en-us/magazine/2009.05.pki.aspx)[[3]](#footnote-3).

procedure_ddCette grille est envisagée dans le cadre de la mise en œuvre d’une infrastructure de confiance au sein d’une organisation ayant un environnement réparti et distribué sous l’angle des thèmes suivants :

* **Enveloppe fonctionnelle** développée dans le chapitre éponyme § 2

Ce premier volet envisage sous l’angle fonctionnel, notamment au travers de l’analyse des différentes fonctions à couvrir, du support de la délégation, de la séparation des rôles, les caractéristiques, les apports potentiels, etc. des composants d’AD CS ;

* **Enveloppe Technique** développée dans le chapitre éponyme § 3

Ce deuxième volet envisage cette fois sous l’angle technique, notamment au travers de l’analyse des architectures et modèles de hiérarchie supportés, de la mise en œuvre, des performances ou encore de l’interopérabilité les caractéristiques, le respect des standards, les apports potentiels, etc. des composants d’AD CS ;

* **Coût et Services** développés dans le chapitre éponyme § 4

Ce dernier volet s’intéresse enfin aux coûts associés aux composants d’AD CS, et des produits connexes comme FIM 2010, ainsi que les services associés notamment en termes de support ;

* + En complément, le site Microsoft TechNet propose de nombreuses ressources techniques sur AD CS de Windows Server 2008 disponibles à l’adresse <http://technet2.microsoft.com/windowsserver2008/en/servermanager/activedirectorycertificateservices.mspx>.

A ce propos, le guide d’évaluation [Windows Server Active Directory Certificate Services Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkID=85472)[[4]](#footnote-4)  propose une démarche d’évaluation guidée de ces composantes dans le cadre d’un environnement de test.

AD CS de Windows Server 2008 (R2) représente une évolution fonctionnelle et technique des différents services proposés par les services de certificats (Certificate Service*)* de Windows Server 2003 (R2) et de Windows Server 2008. Nombre de considérations et d’éléments techniques restent cependant communs entre ces deux versions ; c’est pourquoi, dans la grille d’évaluation de ce livre blanc, il peut être fait mention de liens techniques relatifs aux services de certificats de Windows Server 2003 (R2) et de Windows Server 2008 chaque fois que ces derniers peuvent représenter un éclairage technique complémentaire et pertinent dans le contexte.

## Evaluation au sens des Critères Communs

Avant d’aborder de façon plus précise la grille d’évaluation ainsi suggérée, il nous parait important de mentionner que le rôle Certificate Services ainsi que la plateforme Windows sous-jacente ont fait et font, selon les versions considérées, l’objet d’une évaluation selon les Critères Communs.

Les Critères Communs (CC en abrégé pour Common Criteria en anglais) correspondent à la norme [ISO/CEI 15408:2005 Information technology -- Security techniques -- Evaluation criteria for IT security](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40612)[[5]](#footnote-5) pour la sécurité des systèmes d'information.

Le texte normatif est disponible :

* en français en version 2.1 (août 1999) sur le site de l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI en abrégé) :
  1. [Critères Communs pour l’évaluation de la sécurité des Technologies de l’Information – partie 1 : Introduction et modèle générale](http://www.ssi.gouv.fr/site_documents/CC/CCpart1v21-fr.pdf)[[6]](#footnote-6),
  2. [Critères Communs pour l’évaluation de la sécurité des Technologies de l’Information – partie 2 : Exigences fonctionnelles de sécurité](http://www.ssi.gouv.fr/site_documents/CC/CCpart2v21-fr.pdf)[[7]](#footnote-7).
* en anglais en version 3.1 (septembre 2006) sur le site Web des Critères Communs à l’adresse <http://www.commoncriteriaportal.org/thecc.html>.

eal4+_logo_large Les services de certificats (Certificate Service*)* de Windows Server 2003 (R2) 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 ;
  + L’évaluation a été effectuée sur la base de la cible de sécurité que l’on peut trouver à l’adresse <http://www.commoncriteriaportal.org/files/epfiles/st_vid9507-st.pdf>. Le rapport d’évaluation Critères Communs correspondant est disponible sur le site du NIAP (National Information Assurance Partnership) à la page [NIAIP Certification for Windows Server 2003 Certificate Server](http://www.niap-ccevs.org/cc-scheme/st/vid9507/)[[8]](#footnote-8).

La plateforme Windows Server 2003 SP2 (y compris R2) (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).

* + L’évaluation a été effectuée sur la base de la cible de sécurité que l’on peut trouver à l’adresse <http://www.commoncriteriaportal.org/files/epfiles/20080303_st_vid10184-vr.pdf>. Le rapport d’évaluation Critères Communs correspondant est disponible sur le site du NIAP [NIAP Certification for Windows XP SP2 and Windows Server 2003 SP2 Including R2](http://www.niap-ccevs.org/cc-scheme/st/vid10184/)[[9]](#footnote-9).

Pour ce qui est de la mise en œuvre de cette évaluation de manière concrète, il convient de suivre l’ensemble des éléments précisés dans les guides suivants :

* [Windows Server 2003 SP2 R2 Common Criteria Configuration Guide 3.0](http://www.microsoft.com/downloads/details.aspx?familyid=4F7B6A93-0307-480F-A5AF-A20268CBD7CC&displaylang=en)[[10]](#footnote-10),
* [Windows Server 2003 SP2 R2 Common Criteria Administrator Guide 3.0](http://www.microsoft.com/downloads/details.aspx?familyid=4F7B6A93-0307-480F-A5AF-A20268CBD7CC&displaylang=en)[[11]](#footnote-11).

A son tour, Windows Server 2008 (R2), tout comme Windows Vista, fait désormais officiellement partie de la liste des systèmes en cours d'évaluation au sens des critères communs pour la même cible EAL4 Augmented with ALC\_FLR.3.

* + L’information associée est accessible à l’adresse <http://www.niap-ccevs.org/cc-scheme/in_evaluation.cfm#VID10291>.

Au-delà de l’évaluation selon les Critère Communs qui demande quelques années (à titre d’illustration l’évaluation précédente a commencé le 31/07/2007 et ses conclusions sont attendues pour le 31/12/2010, Cf. lien ci-avant), il est important de souligner que les composants d’AD CS ont été développé selon le processus de développement sécurisé SDL (Security Development Lifecycle).

* + Pour de plus amples informations sur SDL, vous pouvez vous consulter le site MSDN dédié à SDL à l’adresse <http://msdn.microsoft.com/en-us/security/cc448177.aspx>.

Nous proposons à présent au lectorat d’aborder la grille d’évaluation en tant que telle en commençant par l’enveloppe fonctionnelle.

# Enveloppe fonctionnelle

Jauge de progression (1/3)

Ce premier chapitre de la grille d’évaluation envisage sous l’angle fonctionnel, notamment au travers de l’analyse des différentes fonctions généralement à couvrir, du support de la délégation, de la séparation des rôles, etc., les caractéristiques et les apports potentiels des composants d’AD CS pour la mise en œuvre d’une infrastructure de confiance au sein d’une organisation dans le contexte d’un environnement réparti et distribué.

L’analyse prend également en considération la solution complémentaire Microsoft Forefront Identity Manager (FIM en abrégé) 2010 pour l’émission et la gestion de certificats utilisateur X.509. Lorsque tel est le cas, une analyse des seuls composants d’AD CS est proposée dans un premier temps (regroupée sous le sous-titre AD CS), analyse complétée dans un second temps par celle des compléments objectifs de FIM (regroupée sous le sous-titre FIM 2010 (et AD CS) pour les certificats utilisateur).

## Gestion des certificats et des clés

### Fonction d’enregistrement

#### AD CS

procedure_ddPour assurer ses fonctions, le rôle serveur AD CS de la plateforme Windows Server 2008 (R2) propose par défaut le support des modes d’enrôlement suivants :

* **Enrôlement automatique** – Ce mode suppose une AC émettrice AD CS en mode entreprise dans la mesure où une intégration avec l’annuaire Active Directory est requise.

Ce mode s’appuie sur la notion de politique d’enrôlement de certificats. Dans la pratique, une politique d’enrôlement est une collection de modèle de certificat (Cf. section § 1.3.9 Définition des modèles de certificat) avec des émetteurs et définit quels certificats un client (utilisateur, service, ordinateur) doit posséder. Un émetteur est un point de terminaison qui traite les requêtes et tire/émet en regard des certificats. La politique d’enrôlement constitue l’entité centrale de gestion. Elle est appliquée au travers des stratégies de groupe (Group Policy Object en anglaisou GPO en abrégé) (ou d’autres mécanismes selon les cas considérés).

Active Directory est le référentiel LDAP de publication pour la politique d‘enrôlement.

Ce mode permet donc d’assurer que le client possède un certificat valide pour chacune des politiques d‘enrôlement qui sont configurées.

Il permet d’alléger de fait les contraintes organisationnelles et techniques lors de la mise en œuvre d’une infrastructure d’IGC dans les contextes suivants :

1. **Au sein d’une forêt Active Directory** - Ce mode permet de disposer vis-à-vis des membres administrés (utilisateur, service, ordinateur) d’une forêt, 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.

Avec Windows Server 2008 et les versions antérieures, une AC AD CS est l’émetteur des certificats. Cette dernière utilise DCOM comme couche de transport, Kerberos pour l'authentification et repose sur la connectivité Active Directory et ce vis-à-vis de toute plateforme Windows XP et ultérieure considérée en tant que client.

* + Le modèle « tout-auto » est décrit dans son ensemble dans le livre blanc [Certificate Autoenrollment in Windows Server 2003](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx)[[12]](#footnote-12).
  + La spécification [MS-WCCE]: Windows Client Certificate Enrollment Protocol Specification [[MS-WCCE](#MSWCCE)] spécifie le protocole afférent qui se compose d'un ensemble d'interfaces DCOM.

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 § 1.2 Evaluation au sens des Critères Communs

1. **Entre forêts Active Directory** - Sur la base des considérations techniques précédentes, Windows Server 2008 R2 introduit le support de ce modèle « tout-auto » dans un contexte multi-forêts et ce vis-à-vis de toute plateforme Windows XP et ultérieure. Aucune extension de schéma Windows Server 2008 R2 n’est requise ; seul un niveau fonctionnel de forêt Windows Server 2003 est nécessaire.

Une relation d’approbation bidirectionnelle entre les forêt Active Directory Comptes et Ressource est également nécessaire. L’AC située dans la forêt Ressource doit, en effet, faire confiance à la forêt Compte dans laquelle les sujets résident afin de les authentifier. Inversement, une forêt Compte doit faire confiance à la forêt Ressource pour permettre à l'AC de lire les informations sur les sujets ; ceci suppose d’active le renvoi (referral en anglais) LDAP via la commande *Certutil.exe –setreg Policy\EditFlags +EDITF\_ENABLELDAPREFERRALS*.

L'établissement d'une approbation bidirectionnelle peut être considérée comme un risque par certaines organisations. Ce risque peut être atténué en activant l'[authentification sélective](http://technet2.microsoft.com/WindowsServer/en/library/9266b197-7fc9-4bd8-8864-4c119ceecc001033.mspx)[[13]](#footnote-13) au niveau de la relation d'approbation de forêt. L'authentification sélective permet aux administrateurs Active Directory de limiter la portée de la relation de confiance à des ressources spécifiques, tels que les serveurs qui héberge les AC.

* + Le livre blanc [Cross-forest Certificate Enrollment with Windows Server 2008 R2](http://go.microsoft.com/fwlink/?LinkId=139681)[[14]](#footnote-14), explique les scénarios de déploiement, les exigences et les configurations recommandées et propose procédures et script Windows PowerShell (*PKISync.ps1*) de gestion pour la mise en œuvre de ce modèle dans un contexte multi-forêts.

1. **Entre forêts Active Directory et au-delà** – Malgré le support de multiples forêts avec une AC AD CS Windows Server 2008 R2, la dépendance avec DCOM peut constituer un facteur limitant pour certains scénarios de déploiement. Ainsi, par exemple, l'enrôlement automatique d'un ordinateur qui n'est pas connecté directement au réseau de l'entreprise n'est pas possible.

Pour supprimer ces obstacles potentiels, fonction des besoins à prendre en considération, et de façon à ouvrir à l'enrôlement de certificats à un ensemble plus large de scénarios (tirage de certificats dans l’entreprise étendue, tirage de certificats à destination d’ordinateurs qui ne sont pas membres d’un domaine Active Directory, etc.), Windows Server 2008 R2 intègre deux nouveaux composants (service du rôle), en l’occurrence les services Web de politique d’enrôlement de certificats (CES en abrégé) et d’enrôlement de certificats (CEP en abrégé).

CEP permet l’obtention de la politique de certificats et CES, qui sert de proxy pour les requêtes à une AC AD CS, l'enrôlement (ou uniquement le renouvellement si on le souhaite) de certificats. Ces deux services se fondent sur HTTP via un transport TLS chiffré et ne dépendent pas uniquement Kerberos pour l'authentification.

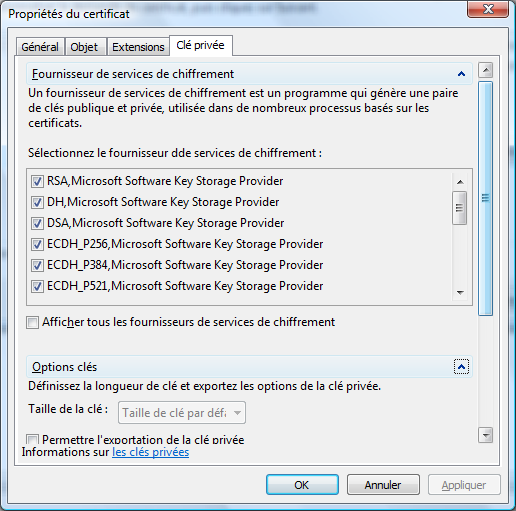
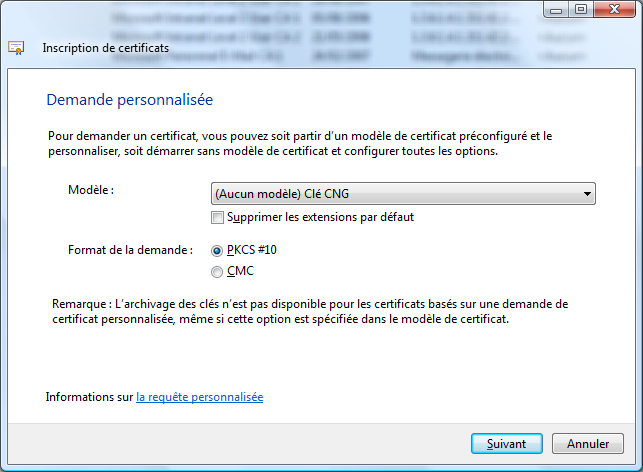
* + Le livre blanc [Windows Server 2008 R2 Certificate Enrollment Web Services Whitepaper](http://download.microsoft.com/download/C/2/2/C229E624-36E4-4AD8-9D86-F564ED539A16/Windows%20Server%202008%20R2%20Certificate%20Enrollment%20Web%20Services.doc)[[15]](#footnote-15) explique les scénarios de déploiement, les exigences et les configurations recommandées et propose des procédures étape par étape pour vous aider à installer et configurer ces nouveaux composants d’AD CS.
  + La spécification [MS-XCEP]: X.509 Certificate Enrollment Policy Protocol Specification, [[MS-XCEP](#MSXCEP)] spécifie le protocole de politique d’enrôlement de certificats X.509. Ce protocole définit les interactions entre un client demandeur et un composant serveur comme CEP pour l'échange d'une politique d'enrôlement de certificats.
  + La spécification [MS-WSTEP]: WS-Trust X.509v3 Token Enrollment Extensions [[MS-WSTEP](#MSWSTEP)] spécifie le nouveau protocole d'enrôlement fondé sur le standard OASIS WS-Trust (Cf. section § 1.6.10 Compatibilité avec le monde XML (protocole XKMS, WS-Trust)). La spécification définit les formats de message et le comportement serveur comme le proxy d’enrôlement CES pour l’enrôlement de certificat.

Cela permet l'enrôlement automatique à partir de clients Windows 7 et Windows 2008 R2 pour être utilisée au-delà des frontières de la forêt Active Directory et sur le Web. Pour cela, ces deux plateformes Windows supportent de multiples politiques d’enrôlement (liste des URI’s des serveurs de politiques) et implémente pour la composante client de ce modèle le support des protocoles DCOM ([[MS-WCCE](#MSWCCE)]) et HTTP ([[MS-XCEP](#MSXCEP)] et [[MS-WSTEP](#MSWSTEP)]).

Le modèle « tout-auto » ainsi décrit (fondé sur DCOM ou HTTP en fonction de la politique d’enrôlement) qu’il soit mono-forêt ou inter forêts Active Directory 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](http://support.microsoft.com/?id=935441)[[16]](#footnote-16) propose une vue d’ensemble de ce service.
* **Enrôlement via le composant enfichable MMC Certificats** (en anglais Certificates) - La requête émise par la plateforme client est soit :
  1. prédéfinie et tire directement partie des modèles de certificats (Cf. section § 1.3.9 « Définition des modèles de certificat ») publiés dans Active Directory et mis à disposition par les AC émettrices AD CS en mode entreprise ;
  2. entièrement paramétrable de façon graphique pour produire une requête au format PKCS #10 ou CMC (conformément à la RFC 2797 Certificate Management Messages over CMS  [[RFC 2797](#RFC2797)]). Windows Vista ou ultérieur est alors requis sur la plateforme client.



* **Délégation d'enrôlement (cartes à puce) via le composant enfichable MMC Certificats** (Certificates en anglais) - Windows Vista ou ultérieur est alors requis sur la plateforme client à l’origine de la requête. Les services de certificats AD CS de Windows Server 2008 (R2) supportent la notion d’agents d’enrôlement restreints (Restricted Enrollment Agent en anglais).
  + Cette fonctionnalité est décrite à l’adresse <http://msdn2.microsoft.com/en-us/library/aa374863.aspx>.
* **Enrôlement Web avec CAWE** - Ce mode d’enrôlement permet aux utilisateurs de se connecter à une AC au moyen d’un butineur afin d’effectuer une demande de certificat X.509 v3, obtenir des CRL X.509 v2, y compris les *delta CRL*, etc.

Les pages d’enrôlement prennent en compte nativement les balises « *Keygen* » supportées par les butineurs Netscape et successeurs comme décrits aux adresses Internet <http://wp.netscape.com/eng/security/comm4-keygen.html> et <http://wp.netscape.com/eng/security/ca-interface.html> ;

* + Ce mode d’enrôlement est décrit dans le livre blanc [Configuring and Troubleshooting Windows 2000 and Windows Server 2003 Certificate Services Web Enrollment](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/webenroll.mspx)[[17]](#footnote-17).
* **Enrôlement avec NDES** – Ce mode repose le Simple Certificate Enrollment Protocol (SCEP) [[SCEP](#SCEP)], Cf. section § 1.6.11 Support du protocole d’enregistrement SCEP ;
* **Enrôlement manuel spécifique** – Ce mode d’enrôlement permet de définir de personnaliser entièrement la requête de certificat ;
  + Ce mode d’enrôlement est décrit dans le livre blanc [Windows Server 2003 Advanced Certificate Enrollment and Management](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx)[[18]](#footnote-18).
* **Enrôlement par programme via notamment les API Certificate Enrollment (CertEnroll)** - Ces API, au travers d’une hiérarchie de classes spécifiquement conçue pour les opérations d’IGC, permettent de créer / gérer :

1. l’enrôlement (authentifié) en tant que tel vis-à-vis d’une AC émettrice AD CS ;
2. les requêtes de certificat aux formats standards (Cf. section § 1.6.3 Formats des requêtes de certificats) avec la prise en compte du bus cryptographique ouvert Cryptography API: Next Generation ou CNG en abrégé (Cf. section § 1.6.5 Taille de clé et algorithmes cryptographiques) notamment pour des certificats ECC (Elliptic Curve Cryptography en anglais) ;
3. les clés publique / privée ;
4. les propriétés / attributs /extensions des certificats X.509 v3.

Il convient de noter qu’un sous-ensemble de ces API peut être utilisé au niveau de scripts serveur pour la personnalisation de pages d’enrôlement Web de CAWE par exemple ;

* + Ces API sont décrites à l’adresse <http://msdn2.microsoft.com/en-us/library/aa374863.aspx>.
* **Enrôlement en masse** – Ce mode tire directement bénéfice de l’architecture ouverte du moteur d’une AC émettrice AD CS, Cf. section § 1.3.13 Gestion des certificats en masse ;

L'architecture du moteur tel que décrite dans la page MSDN [Certificate Services Architecture](http://msdn2.microsoft.com/en-us/library/Aa376540.aspx)[[19]](#footnote-19) offre deux points d’extensibilité, en l’occurrence :

1. la définition d’un module de politique (policy module en anglais) spécifique pour l’enregistrement. Une description de l’interface correspondante est proposée à l’adresse <http://msdn2.microsoft.com/en-us/library/Aa387348.aspx> ;
2. la définition d’un module de sortie (exit module en anglais) spécifique pour la publication, Cf. section § 1.3.5 Fonction de publication. Une description de l’interface correspondante est proposée à l’adresse <http://msdn2.microsoft.com/en-us/library/Aa382386.aspx>.

Au sein d’un environnement de confiance établi (éventuellement pour partie) sur la base des technologies Microsoft (Cf. section § 1.9 Interopérabilité et options), l’environnement FIM 2010 tire bénéfice de cette capacité d'ouverture pour assurer la gestion du cycle de vie des certificats X.509 v3 utilisateur (et des supports éventuellement associés, Cf. section § 1.4.5 Gestion des supports de certificats (carte à puce / jeton USB)).

#### FIM 2010 (et AD CS) pour les certificats utilisateur

Comme évoqué en introduction, FIM 2010 offre les services d’autorité d’enregistrement (AE en abrégé) et de système de gestion de cartes (Card Management System en anglais ou CMS en abrégé), cette seconde fonction constituant un élément essentiel d’une infrastructure de confiance lorsque des cartes à puce (smart cardsen anglais) sont déployées à grande échelle.

Pour ce faire, l’environnement FIM associe un ensemble de certificats X.509 v3 (modèles, Cf. section § 1.3.9 Définition des modèles de certificat) à :

* un profil logiciel (c'est-à-dire non associé à un support) ;
* et/ou un profil matériel (c'est-à-dire à un support).

Les certificats d’un même profil peuvent être émis par différentes AC : celles-ci doivent être des AC AD CS en mode entreprise et appartenir à une même forêt dans la version actuelle.

Un même utilisateur peut se voir attribuer simultanément, de par ses rôles et fonctions, plusieurs profils FIM.

procedure_ddCes profils autorisent ensuite la définition et la personnalisation des processus qui leur sont associés de façon à couvrir la gestion de l’ensemble du cycle de vie des certificats X.509 v3 et, le cas échéant, d’un support :

* émission / renouvellement / remplacement / révocation des certificats X.509 v3 ;
* émission / remplacement / retrait /désactivation des supports ;
* émission de supports temporaires / duplication des supports ;
* personnalisation des supports y compris impression.

Les politiques (règles) pour les workflows de gestion / d’automatisation de ces processus, la collecte de données associées, etc. permettent de matérialiser des scénarios allant de la centralisation au libre-service avec des capacités de personnalisation des requêtes et de délégations d’approbation flexibles.

En conséquence, la gestion des certificats X.509 v3 et des supports associés pour un même utilisateur s’effectue au travers de la solution FIM 2010 selon les processus de l’entreprise et, en toute transparence, vis-à-vis de multiples AC émettrice AD CS en mode entreprise.

### Fonction de révocation

#### AD CS

La fonction de révocation ne doit pas être confondue avec le moteur d’évaluation de la chaîne de certificats qui est un composant client qui permettra de remonter à l’application ou au service le statut, par exemple révoqué, du certificat présenté pour évaluation, Cf. section § 1.4.2 Fonction de validation de certificats.

La demande de révocation est engagée par l'utilisateur ou l'administrateur. Les sections § 1.6.13 Mode de publication des CRL et § 1.6.14 Protocole d’accès aux CRL décrivent respectivement la publication paramétrable de l’information associée ainsi que les protocoles supportés.

* + La page TechNet [Manage Certificate Revocation](http://technet2.microsoft.com/windowsserver/en/library/92a5e655-3eb2-4843-b9cb-58c84c0a91d61033.mspx)[[20]](#footnote-20) offre une vue d’ensemble sur cette fonction au-delà des éléments suscités.

Un mode de traitement par lot (mode *batch*) est possible via les interfaces programmatiques *ICertAdmin* et *ICertAdmin2* exposées par le moteur d’une AC AD CS, Cf. section § 2.1.11 Gestion des certificats en masse.

L’environnement FIM tire directement bénéfice de ces interfaces en intégrant la fonction de révocation dans la gestion du cycle de vie des certificats X.509 v3 et des éventuels supports matériels associés (carte à puce, jeton USB).

#### FIM 2010 (et AD CS) pour les certificats utilisateur

Comme évoqué précédemment, l’environnement FIM associe un ensemble de certificats X.509 v3 décrits sous forme de modèles à :

* un profil logiciel (c'est-à-dire non associé à un support) ;
* et/ou un profil matériel (c'est-à-dire à un support).

procedure_ddUn même utilisateur peut se voir attribuer simultanément, de par ses rôles et fonctions, plusieurs profils FIM. La base de données relationnelles de FIM s’appuie sur une base technique Microsoft SQL Server et maintient l’état de :

* l’ensemble des certificats X.509 v3 qui ont été émis par les AC émettrice AD CS en mode entreprise avec lesquelles la solution FIM 2010 est interfacée et ce, en association avec leur propriétaire, identité et compte Active Directory,
* l’ensemble des supports en association avec les certificats qui se trouvent sur ces supports.

Lorsqu’un certificat « compromis » ou un support « compromis » doivent être révoqués, la fonction de révocation assurée par la solution FIM 2010 permet de gérer l’opération dans sa globalité (en association avec la ou les AC AD CS concernées) en fonction du processus considéré : le remplacement, le retrait, la désactivation d’un support ou l’émission d’un support temporaire par exemple.

Un *workflow* de gestion assurera par exemple la révocation de l’ensemble des certificats présents sur le support attribué à l’utilisateur de façon temporaire ou définitive.

### Fonction de renouvellement

#### AD CS

Les certificats X.509 v3 déployés avec les mécanismes d’auto-enrôlement (Cf. section § 1.3.1 Fonction d’enregistrement) bénéficient de la capacité d'auto-renouvellement, y compris si les certificats et bi-clés sont stockés sur un support de type carte à puce ou jeton USB.

Ceci constitue le principal vecteur de renouvellement si la capacité d'auto-enrôlement a été utilisée.

* + Le mécanisme afférent est décrit dans le livre blanc [Certificate Autoenrollment in Windows Server 2003](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx)[[21]](#footnote-21).

Dans ce dernier cas, le renouvellement de la bi-clé dépend du type de fournisseur cryptographique (Cf. section § 1.6.7 Support des modules cryptographiques). Ainsi, la bi-clé est également systématiquement renouvelée avec un CSP (Cryptographique Service Provider en anglais) logiciel alors qu’avec un CSP matériel (support type carte à puce, jeton USB, etc.), la clé sera renouvelée tant que la carte n'est pas pleine.

Le renouvellement manuel est pris en charge très facilement au travers de l’API Certificate Enrollment (CertEnroll) pour une intégration sous la forme désirée : notification de renouvellement, page Web de renouvellement, etc.

* + Ces APIs sont décrites à l’adresse <http://msdn2.microsoft.com/en-us/library/aa374863.aspx>.

#### FIM 2010 (et AD CS) pour les certificats utilisateur

A l’instar des fonctions précédentes, l’environnement FIM permet d’intégrer la fonction de renouvellement dans la gestion du cycle de vie des certificats X.509 v3 et des (éventuels) supports (carte à puce et jeton USB) associés.

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

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.

#### AD CS

AD CS offre des mécanismes manuel et automatique de séquestre de clés de chiffrement.

Ceci requiert que l’AC AD CS soit configurée pour supporter cette fonctionnalité de séquestre et de recouvrement et que l’activation de la séparation des rôles (Cf. section § 1.5.1 Séparation des rôles) et l’identification d’agent(s) de recouvrement (Key Recovery Agent en anglais ou KRA en abrégé) 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](#PKCS12)].

Le mode automatique s’appuie sur la fonctionnalité d’auto-enrôlement / auto-renouvellement (Cf. section § 1.3.1 Fonction d’enregistrement). Il est nécessaire, dans ce cas, que le gabarit du certificat (Cf. section § 1.3.9 Définition des modèles de 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 Certificate Management Messages over CMS [[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’AC AD CS 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](#PKCS12)] (.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 clef 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 clef 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.

* + Le livre blanc [Key Archival and Recovery in Windows Server 2008](http://go.microsoft.com/fwlink/?LinkID=92523)[[22]](#footnote-22) offre une vue d’ensemble de ces mécanismes et des formats utilisés.

Les opérations manuelles de séquestre et de recouvrement décrites ci-avant peuvent être automatisées dans le respect de la séparation des rôles, Cf. section § 2.1.11 Gestion des certificats en masse.

#### FIM 2010 (et AD CS) pour les certificats utilisateur

A l’instar des fonctions précédentes, FIM 2010 permet d’intégrer la fonction de renouvellement dans la gestion du cycle de vie des certificats X.509 v3 et des éventuels supports associés.

### Fonction de publication

#### AD CS

Le module enfichable MMC Autorité de certification (Certification Authority en anglais), l'outil en ligne de commande *CertUtil.exe* ainsi que le fichier *CAPolicy.inf* d'installation d'une AC AD CS permettent le paramétrage complet de la publication des CRL (et delta CRL).

Les emplacements de publication des CRL peuvent être multiples et de type LDAP, HTTP ou fichier (Cf. section § 1.6.13 Mode de publication des CRL). Il en est de même pour la publication des certificats (Authority Information Access en anglais ou AIA en abrégé).

* + Le livre blanc [Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx)[[23]](#footnote-23) décrit les éléments de configuration associés. Ces derniers s’appliquent à une AC AD CS de Windows Server 2008 (R2).

Par ailleurs, l’intégration possible à Active Directory est un point fort d’AD CS de Windows Server 2008 (R2).

procedure_ddDans ce contexte, une AC AD CS d’entreprise émettrice supporte alors les usages suivants :

* publication optionnelle des certificats dans l’annuaire ;
* authentification des demandes ;
* délégation d’administration au sein de l’Autorité ;
* stockage des modèles de certificats (Cf. section § 1.3.9 Définition des modèles de certificat) ;
* renseignement optionnel des informations d’identité au sein des certificats lors de la génération du certificat ;
* déploiement des certificats des autorités racines via les stratégies de groupe (GPO) ;
* déploiement/renouvellement/remplacement automatisés des certificats via les modèles de certificats (Cf. section § 1.3.9 Définition des modèles de certificat) et les stratégies de groupe (Groupe Policy Object en anglais ou GPO en abrégé) : fonctionnalité « tout-auto » (auto-enrôlement / auto-renouvellement).

Pour les modes d’enrôlement (Cf. section § 1.3.1 Fonction d’enregistrement) qui ne s’appuient pas sur un gabarit (Cf. section § 1.3.9 Définition des modèles de certificat), et donc où le mode de publication est, en l’état, non précisé, la publication 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.

#### FIM 2010 (et AD CS) pour les certificats utilisateur

A l’instar des fonctions précédentes, FIM 2010 permet d’intégrer la fonction de renouvellement dans la gestion du cycle de vie des certificats X.509 v3 et des éventuels supports associés.

### Fonction de « dépublication »

#### AD CS

Cette fonctionnalité est intégrée de base dans le cadre de l’utilisation conjointe d’une AC AD CS d’entreprise et du modèle « tout-auto ».

* + Le livre blanc [Certificate Autoenrollment in Windows Server 2003](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx)[[24]](#footnote-24) traite notamment de ce point avec le nettoyage en standard dans Active Directory.

#### FIM 2010 (et AD CS) pour les certificats utilisateur

Comme pour les fonctions précédentes, l’environnement FIM 2010 permet d’intégrer la fonction de renouvellement dans la gestion du cycle de vie des certificats X.509 v3 et des éventuels supports associés.

### *Workflows* pour la gestion et la combinaison des processus organisationnels précédents

Comme prudemment abordé, l'architecture du moteur d’une AC AD CS permet la définition de modules de politique (policy module en anglais) spécifiques pour la validation d’une requête de certificat et de modules de sortie (exit module en anglais) pour l’émission et la publication de ce même certificat X.509 v3.

L’environnement FIM tire parti de cette capacité d'ouverture et permet de fournir ce type de *workflow* pour des AC émettrices AD CS en mode entreprise pour la gestion de certificats utilisateur.

Au sein d’une telle infrastructure de confiance, la solution FIM assure la gestion du cycle de vie des certificats X.509 v3 et des supports. L’environnement FIM offre les services d’autorité d’enregistrement (AE en abrégé) et de système de gestion de cartes (Card Management System en anglais ou CMS en abrégé), cette seconde fonction constituant un élément essentiel d’une infrastructure de confiance lorsque des supports (carte à puce, jeton USB, etc.) sont déployés à grande échelle.

### Génération des clés

#### AD CS

Une infrastructure d’IGC basée sur AD CS de Windows Server 2008 (R2) ne génère pas de bi-clés sauf exception comme la génération d’un certificat racine.

Par ailleurs, le support du protocole CMC pour l’enrôlement tel que décrit dans la RFC 2797 Certificate Management Messages over CMS [[RFC 2797](#RFC2797)] permet une signature des requêtes et offre dans le même temps un « véhicule » pour le séquestre de clés lors de l’enrôlement (Cf. Section § 1.3.4 Fonction de séquestre / recouvrement des clés de chiffrements).

#### FIM 2010 (et AD CS) pour les certificats utilisateur

L’environnement FIM permet le cas échéant la génération personnalisable des clés en relation ou non avec des boîtiers matériels (HSM en abrégé pour Hardware Storage Module en anglais) (Cf. section § 1.6.8 Stockage des clés des AC).

### Définition des modèles de certificat

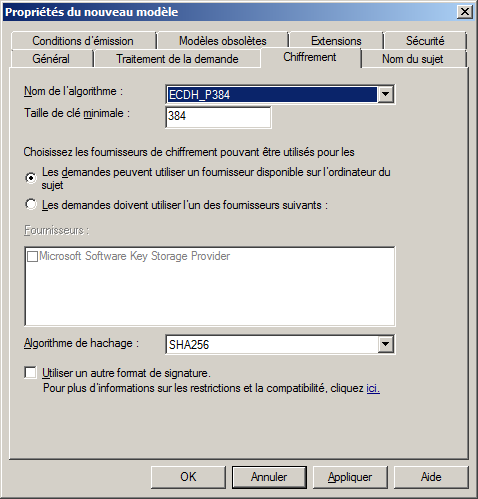
Une AC émettrice AD CS de Windows Server 2008 R2 en mode standard ou entreprise permet de définir et de s’appuyer sur des modèles (ou gabarits) de certificats.

Trois types de modèles sont ainsi proposés : version 1, version 2 et version 3. La version 1 correspond aux modèles introduits historiquement avec Windows Server 2000, la version 2 à ceux de Windows Server 2003 et la version 3 à ceux de Windows Server 2008 (R2).

Les modèles proposés par défaut (Cf. section suivante) sont complètement personnalisables et peuvent ainsi être dupliqués en versions 2 et 3 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 livre blanc [Implementing and Administering Certificate Templates in Windows Server 2008](http://go.microsoft.com/fwlink/?LinkID=92522)[[25]](#footnote-25) précise les fonctionnalités offertes.
  + La spécification [MS-CRTD]: Certificate Templates Structure Specification [[MS-CRTD](#MSCRTD)] spécifie la structure des modèles de certificats. Cette structure décrit la syntaxe et de l'interprétation des modèles de certificat.

Les modèles version 3 sont destinés à des plateformes Windows Vista, Windows Server 2008 et ultérieur dans la mesure où ces derniers permettent de préciser des algorithmes supportés par le nouvel environnement cryptographique Cryptography API: Next Generation (CNG en abrégé), bus cryptographique ouvert (Open Cryptographic Interface en anglais), appelé à remplacer la composante CryptoAPI 1.0 (opérations de chiffrement avec les algorithmes standards), Cf. section § 1.6.5 Taille de clé et algorithmes cryptographiques.



La version 3 introduit également le support de la signature discrète (PKCS#1 V2.1 [[PKCS #1](#PKCS1)]), ainsi que la possibilité de donner au compte Service réseau (Network Service en anglais) des machines destinatrices les permissions en lecture pour la clé privée de façon à éviter une opération manuelle sur le magasin de certificats machine.

* + Ces nouvelles fonctionnalités complémentaires introduites par la version 3 sont décrites dans le livre blanc [Active Directory Certificate Server Enhancements in Windows Server 2008](http://www.microsoft.com/downloads/details.aspx?FamilyID=9bf17231-d832-4ff9-8fb8-0539ba21ab95&DisplayLang=en)[[26]](#footnote-26).

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 (Enrollment Services en anglais) au niveau d’Active Directory liste de façon globale les AE disponibles avec les modèles ainsi proposés.

Seules les AC AD CS en mode entreprise (intégrées avec Active Directory) permettent de délivrer des certificats basés sur les modèles version 2 et version 3; ces derniers étant publiés au niveau de la forêt Active Directory.

Les modèles de certificat susceptibles d’être ainsi définis peuvent répondre aux exigences décrites par la Politique de Référencement Intersectorielle de Sécurité (PRIS) v2.1 de l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) et de la Direction Générale de la Modernisation de l’Etat (DGME).

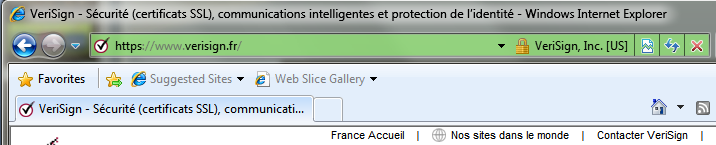
* + La PRIS est disponible sur le site de la DGME à l’adresse <http://synergies.modernisation.gouv.fr/rubrique.php?id_rubrique=285>.

#### Support des certificats EV pour les certificats à usage interne

Windows Server 2008 R2 propose la possibilité de configurer une hiérarchie d'AC internes afin d'émettre des certificats SSL qui peuvent être affichés comme des certificats SSL à validation renforcée (Extended Validation en anglais ou EV en abrégé) pour les sites Web internes.

Le billet [Extended Validation support for websites using internal certificates](http://blogs.technet.com/askds/archive/2009/08/14/extended-validation-support-for-websites-using-internal-certificates.aspx)[[27]](#footnote-27) précise les modalités de configuration avec les modèles de certificats.

Les certificats EV fournissent des informations à destination des navigateurs Web sécurisés afin d’identifier clairement l’identité de l’organisation d’un site Web.



De tels certificats sont aujourd’hui supportés, pour ce qui est de la plateforme Windows et d’Internet Explorer par :

* Windows XP SP3 et Windows 2003 SP2 avec Internet Explorer 8,
* Windows Vista SP1 et Windows Server 2008 avec Internet Explorer 7 et 8,
* Windows 7 et Windows Server 2008 R2 avec Internet Explorer 8.

Ils sont également supportés notamment par Firefox 3.0 et ultérieur.

* + Les critères et recommandations pour émettre des certificats EV sont définis dans le document version 1.1 [Guidelines for the issuance and management of extended validation certificates](http://cabforum.org/EV_Certificate_Guidelines_V11.pdf)[[28]](#footnote-28). Ce document est produit par le CA/Browser Forum (<http://www.cabforum.org/>), une organisation volontaire dont les membres comprennent des PSCE, des fournisseurs de logiciels Internet et/ou de sécurité, des représentants des professions juridiques et d’audit. La liste courante des membres est disponible à l’adresse <http://cabforum.org/forum.html>.

Des informations complémentaires sont disponibles au niveau du centre de ressources Certificats EV de l’AOTA (Authentication and Online Trust Alliance) à l’adresse <http://www.aotalliance.org/resources/EV>.

* + Le livre blanc [The Business Value of Extended Validation SSL Certificates](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9948298f-1586-4cda-bee1-47b2ade78245)[[29]](#footnote-29) peut être consulté à titre de complément.

#### Support de nouveaux scénarios avec des certificats de courte durée

De nouveaux scénarios IGC utilisent des certificats de courte durée de vie comme jetons de sécurité ; c’est le cas notamment dans le contexte de la mise en œuvre NAP (Network Access Protection) avec IPSec ou de l’utilisation d’OCSP (Cf. section § 2.2.2.2 Support d’OCSP (Online Certificate Status Protocol)).

L’usage de tels certificats conduit à l’augmentation significative de taille de la base données et des informations de révocation alors qu’aucune « rémanence » n’est souhaitable dans ce type de scénario.

Les modèles de certificat version 3 avec Windows Server 2008 R2 permettent de spécifier si :

* la requête afférente et le certificat résultant doivent être ou non consignés dans la base de l’AC AD CS, Cf. section § 3.1.15 Base de stockage locale,
* une information de révocation doit être ou non intégrée pour ce (type de) certificat.

Une AC AD CS Windows Server 2008 est donc à même de gérer si nécessaire des requêtes non persistantes de façon à s’adapter à ces nouveaux usages et éviter ainsi une gestion coûteuse du nettoyage.

#### Liste des principaux modèles gérés par défaut

La page TechNet [Certificate Templates Overview](http://technet2.microsoft.com/windowsserver/en/library/e42693ef-374b-40a9-af3c-569f0d1fe1c91033.mspx)[[30]](#footnote-30) précise les 29 modèles proposés par défaut par Windows Server 2003. Windows Server 2008 (R2) en ajoute deux : Authentification Kerberos (Kerberos Authentication en anglais) et Signature de la réponse OCSP (OCSP Response Signing en anglais).

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 pour le système de fichiers (Encryption File System en anglais ou EFS en abrégé).

#### Documentation des modèles de certificat

La description des modèles de certificat rentre dans le cadre de l’offre de services (livrables) qui accompagne la mise en œuvre d’une IGC.

La description des modèles telle que proposée dans le livre blanc [Implementing and Administering Certificate Templates in Windows Server 2008](http://go.microsoft.com/fwlink/?LinkID=92522)[[31]](#footnote-31) peut servir de canevas.

* + La liste des Object ID (OID en abrégé) utilisée par la plateforme Microsoft est précisée dans l’article [Object IDs associated with Microsoft cryptography](http://support.microsoft.com/?id=287547)[[32]](#footnote-32).

### Définition des modèles des listes de révocation

Les CRL X509v2 ainsi que les *delta CRL* (et ce conformément à la RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [[RFC 3280](#RFC3280)]) sont gérées.

Les modèles des listes de révocation répondent aux exigences décrites par la Politique de Référencement Intersectorielle de Sécurité (PRIS) v2.1 de l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) et de la Direction Générale de la Modernisation de l’Etat (DGME).

* + La PRIS est disponible sur le site de la DGME à l’adresse <http://synergies.modernisation.gouv.fr/rubrique.php?id_rubrique=285>.

### Gestion des certificats en masse

La gestion des certificats en masse est possible via les interfaces *ICertAdmin* et *ICertAdmin2* exposées par le moteur d’AD CS de Windows Server 2008 (R2) et décrites à l’adresse <http://msdn2.microsoft.com/en-us/library/Aa383234.aspx>.

* + La spécification [MS-CSRA]: Certificate Services Remote Administration Protocol Specification [[MS-CSRA](#MSCSRA)] spécifie le protocole afférent qui se compose des interfaces DCOM ci-dessus.

Ces interfaces sont notamment exploitées par l’utilitaire en ligne de commande *Certutil.exe* et la solution FIM 2010.

### Politique de certification

La définition de la politique de certification (en abrégé PC) rentre dans le cadre de l’offre de services (livrables) qui accompagne la mise en œuvre d’une infrastructure de confiance.

La RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [[RFC 3647](#RFC3647)] (anciennement RFC 2527 [RFC 2527]) offre le cadre pour la définition et rédaction de ce document (PC ou CP en abrégé pour Certification Policy en anglais) et de celui relatif à la déclaration des pratiques de certification (DPS ou CPS en abrégé pour Certification Practice Statement en anglais, Cf. section suivante).

procedure_ddDans le cadre d’une CP, un plan type généralement admis est le suivant :

* introduction (OID, destination et applications des certificats, contact) ;
* dispositions d’ordre général (publication de certificats et de CRL, réglementation) ;
* identification et authentification (garantie de l’identité) ;
* besoins opérationnels (cycle de vie des certificats, exploitation, journalisation) ;
* contrôles de sécurité physique, procédures, personnel ;
* contrôles techniques de sécurité (sécurité des clés) ;
* profils (modèles) des certificats et CRL ;
* administration des spécifications.
  + La liste des *Object ID* (OID) utilisée par la plateforme Microsoft est précisée dans l’article l’article [Object IDs associated with Microsoft cryptography](http://support.microsoft.com/?id=287547)[[33]](#footnote-33).

### Déclaration des pratiques de certification

Cf. section précédente.

### Gestion de l’historique de certification

Des développements via les extensions et interfaces proposées par le moteur permettent de le faire aisément (Cf. section § 1.9.4 API de développement).

Ceci est notamment proposé par l’environnement FIM qui s'intègre dans l'architecture flexible et extensible ainsi mise à disposition.

## Fonctionnalités connexes

### Fonction d’horodatage

Le rôle serveur AD CS de Windows Serveur 2008 (R2) n’offre pas de service d’horodatage.

### Fonction de validation de certificats

Le moteur d’évaluation de la chaîne de certificats est un composant client qui permet de remonter à l’application ou au service le statut du certificat si celui-ci est présenté.

* + Le livre blanc [Certificate Revocation and Status Checking](http://go.microsoft.com/fwlink/?LinkID=27081)[[34]](#footnote-34) décrit ce moteur proposé par CryptoAPI 2.0 pour le compte des applications et services.

Il convient de noter que Windows Vista, Windows Server 2008 et ultérieur disposent de l’instrumentation *CryptoAPI 2.0 Diagnostics* qui offre la possibilité de diagnostiquer et résoudre des problèmes IGC en collectant une information détaillée sur la validation des chaînes de certificats, des opérations relatives aux magasins de certificats, et de la vérification des signatures.

* + Cette composante est décrite dans le livre blanc [Troubleshooting PKI Problems on Windows Vista](http://technet2.microsoft.com/WindowsVista/en/library/771e1f29-4eba-40c9-9193-60043889bbf41033.mspx)[[35]](#footnote-35).

La fonction de validation de certificats entend le support partiel ou complet des mécanismes suivants :

#### Support des CRL et delta CRL

AD CS est conforme à la RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile [[RFC 2459](#RFC2459)] qui définit les règles d'utilisation des certificats et CRL pour l'Internet au niveau de la section § 6 : 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).

AD CS supporte également les *delta CRL* tels que spécifié dans la RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [[RFC 3280](#RFC3280)], mise à jour de la RFC 2459 [[RFC 2459](#RFC2459)]. Une *delta CRL* permet de rafraîchir la CRL de base avant son expiration, en spécifiant une nouvelle base dans la *delta CRL*.

Les CRL peuvent être testées unitairement avec la commande *certutil.exe –URL*. Ceci étant, le composant enfichable MMC PKI d’entreprise (Enterprise PKI en anglais) offre une vue graphique du statut des différentes CRL publiées par les AC AD CS de l’infrastructure de confiance, et ce pour l’ensemble des chemins de publication.

#### Support d’OCSP (Online Certificate Status Protocol)

Windows Server 2008 (R2) propose au sein du rôle Services de certificats Active Directory (Active Directory Certificate Services en anglais) le service de rôle Répondeur en ligne (Online Responder Service en anglais) conforme à la RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP [[RFC 2560](#RFC2560)].

* + Ce service est décrit dans le livre blanc [Installing, Configuring, and Troubleshooting the Microsoft Online Responder](http://technet2.microsoft.com/windowsserver2008/en/library/045d2a97-1bff-43bd-8dea-f2df7e270e1f1033.mspx)[[36]](#footnote-36).

Extrait de la RFC :

« *In order to convey to OCSP clients a well-known point of information access, CAs SHALL provide the capability to include the AuthorityInfoAccess extension (defined in [RFC2459], section 4.2.2.1) in certificates that can be checked using OCSP. Alternatively, the accessLocation for the OCSP provider may be configured locally at the OCSP client.* »

AD CS de Windows Server 2008 R2 permet de générer des certificats pour OCSP (où l’emplacement du répondeur OCSP est précisé dans l’extension AIA) ainsi que des certificats *Signature de la réponse OCSP* (OCSP Response Signing en anglais) pour le répondeur.

OCSP peut sembler contradictoire avec la fonction de vérification d’un certificat hors ligne, qui constitue l’un des avantages de l'approche IGC ; paradoxal également par rapport à la notion de confiance puisque OCSP nécessite de faire confiance à un validateur.

procedure_ddOCSP appelle également les commentaires suivants :

1. La plupart des répondeurs OCSP font appel à la CRL périodique pour l’obtention de l’information de révocation de certificats. De ce fait, ils n’éliminent donc pas complètement les limitations liées à la nature périodique des CRLs ;
2. Le répondeur OCSP est vulnérable aux attaques de déni de service où une pléthore de requêtes est soumise au répondeur. Le problème est aggravé par la nécessité de signer numériquement les réponses, ce qui est très consommateur en termes de CPU ;
3. Les messages d'erreur envoyés par le répondeur OCSP ne sont pas signés numériquement ; ce qui offre une capacité de renvoyer de faux messages d'erreur au demandeur. L’ensemble de l'information de statut de révocation est, par contre, signé.

OCSP offre cependant une réponse pertinente à certains scénarios d’usage. En fait, aucune technologie unique traitant la révocation ne peut répondre à l’ensemble des scénarios avec des utilisateurs perpétuellement mobiles et des transitions entre environnements (intranet, VPN/extranet, Internet, RPC sur HTTP, hors ligne).

Côté « client », la composante CryptoAPI 2.0 réalise pour le compte des applications et services l’évaluation des certificats.

En termes de mécanismes supportés par défaut par le moteur d’évaluation de CryptoAPI 2.0, deux situations sont à prendre en considération :

1. **Windows 2000, Windows XP et Windows Server 2003**. Ces environnements supportent deux mécanismes par défaut par le moteur d’évaluation : CRL et delta CRL avec une mise en cache.

CryptoAPI 2.0 supporte une architecture modulaire à base de modules plug-in appelés fournisseurs de révocation (Revocation Providers en anglais) pour l’évaluation de la révocation. Le support d’OCSP est possible via un tel module plug-in tiers.

* + L’article [Adding Revocation Providers to CryptoAPI for Identrus Applications](http://msdn2.microsoft.com/en-us/library/ms995348.aspx)[[37]](#footnote-37) peut être consulté à cet effet.
  + Le composant logiciel [Fournisseur de révocation GIP-CPS pour les plateformes Microsoft Windows](http://www.microsoft.com/france/interop/gip-cps/default.aspx)[[38]](#footnote-38) publié sous le contrat de licence de logiciel libre [CeCCIL-B](http://www.cecill.info/licences/Licence_CeCILL-B_V1-fr.html)[[39]](#footnote-39) permet de valider avec Crypto API l’état de révocation des certificats émis par le GIP-CPS sur les plateformes Windows et propose de fait un exemple complet accompagné de son code source d’un tel fournisseur.

1. **Windows Vista, Windows Server 2008 et ultérieur**. Ces environnements intègrent de façon native un fournisseur (client) OCSP conforme à la RFC 2560 [[RFC 2560](#RFC2560)] et supportent de fait les trois mécanismes du moteur d’évaluation : OCSP (défaut), CRL et delta CRL avec une mise en cache.

Dans le contexte spécifique de l’ouverture de session, il convient de noter que l’implémentation de PKINIT pour Kerberos conforme à la RFC 4556 Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) [[RFC 4556](#RFC4556)] offre un support d’OCSP conforme à la RFC 4557 Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) [[RFC 4557](#RFC4557)].

* + Ce support est décrit dans la section § OCSP support for PKINIT  à la page 57 du livre blanc [Windows Vista Smart Card Infrastructure](http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en)[[40]](#footnote-40).

Un KDC (Key Distribution Center en anglais) Kerberos Windows Server 2008 propose dans le même temps un mécanisme d’optimisation, le « *Kerberos Stapling* » en anglais, qui permet de communiquer au client le certificat de son contrôleur de domaine avec la réponse OCSP associée ; le client n’a pas alors à effectuer une demande spécifique auprès du répondeur.

Le Service Pack 3 (SP3) de Windows XP offre le même support.

La gestion de la révocation nécessite alors l’établissement d’un compromis entre l‘atténuation du risque et l’expérience utilisateur.

Aussi bien CryptoAPI 2.0 côté client que les services d’IGC Microsoft au travers de leur support de l’ensemble des mécanismes offrent la souplesse nécessaire pour répondre aux différents scénarios à envisager.

#### Support de SCVP (Simple Certificate Validation Protocol)

AD CS n’offre pas, dans la version courante, de support de SCVP.

#### Support d’ARL (Authority Revocation List)

AD CS n’offre pas de support d’ARL aujourd’hui. Dans la pratique, une AC racine publie une CRL, mais son certificat ne contient pas de CDP : il n’y a pas besoin de CDP (CRL) pour le certificat de l’AC racine.

Si l’AC racine est compromise, on retire son certificat des magasins et on révoque tous les certificats émis par l’AC racine.

### Fonction d’archivage

Des développements via les extensions et interfaces proposées par le moteur permettent d’implémenter facilement la fonction d’archivage (Cf. section § 1.9.4 API de développement).

Ceci est notamment proposé par l’environnement FIM qui s'intègre dans l'architecture flexible et extensible ainsi mise à disposition.

### Interfaçage avec applications existantes

procedure_ddL’interfaçage est multiple :

* intégration Windows avec l’ouverture de session par carte à puce (smartcard logon en anglais), le système de fichiers EFS (Encrypted File System en anglais), la signature de code Authenticode, etc. ;
* intégration Linux/Unix avec notamment l’ouverture de session par carte à puce via la solution Quest Authentication Services(<http://www.quest.com/authentication-services>) ;
* intégration aux applications courantes comme l’authentification SSL/TLS, la messagerie sécurisée avec le chiffrement et la signature S/MIME ;
* intégration à l'infrastructure avec l’authentification d'ordinateur client IPsec, l’authentification d'ordinateur client IPsec dans le cadre d'un VPN, l’authentification de serveur VPN IPsec, l’authentification de client sans fil, l’authentification de serveur IAS/NPS), etc. ;
* iIntégration avec des équipements réseau avec le support du protocole SCEP [[SCEP](#SCEP)] (Cf. section § 1.6.11 Support du protocole d’enregistrement SCEP).

### Gestion des supports de certificats (carte à puce / jeton USB)

Les services de certificats Active Directory (Active Directory Certificate Services en anglais) de Windows Server 2008 (R2) permettent d'offrir de façon native de la délégation d’enrôlement ou de l'enrôlement pour le compte d’un tiers et permettent dans ce cadre l'émission de cartes à puce ou d'autres facteurs de forme (jeton USB par exemple).

Ces fonctions peuvent être très largement étendues avec l’environnement FIM. FIM permet d’associer un ensemble de certificats (modèles) et un support (carte à puce, jeton USB) à un profil matériel. Un tel profil autorise ensuite la définition et personnalisation des processus qui lui sont associés de façon à couvrir la gestion de l’ensemble du cycle de vie des certificats X.509 v3 et de leurs supports associés.

FIM s’appuie sur la notion de numéro de série (SN en abrégé ou Serial Number en anglais) du support dans la gestion des cartes actives, retirées, etc. et leur attribution ou non à une identité Active Directory et permet d’offrir des états sur cette base.

La gestion des supports suppose, d’une façon générale, les éléments suivants.

#### Disponibilité d’un lecteur reconnu pour le support

Le support doit disposer d’un lecteur supporté par la plateforme Windows. Cette dernière supporte PC/SC v1.0 [[PCSC 1.0](#PCSC1)] du PC/SC workgroup.

Windows Vista, Windows Server 2008 et ultérieur comportent en standard un pilote USB-CCID comme mentionné à l’adresse <http://www.microsoft.com/whdc/device/input/smartcard/USB_CCID.mspx> ; ce qui signifie que tout lecteur de carte à puce USB conforme USB-CCID [[USB-CCID](#USBCCID)], ne nécessite pas l’installation d’un pilote additionnel.

Ce pilote est également disponible sur Windows Update pour Windows 2000, Windows XP et Windows Server 2003.

Un lecteur de carte à puce et le pilote correspondant doivent se conformer au programme logo WHQL décrit à l’adresse <http://www.microsoft.com/whdc/whql/device/smartcard.mspx> pour obtenir le « *Windows Logo for the Smart Card Reader* » et que ce dernier soit rendu disponible sur Windows Update.

#### Disponibilité d’un module cryptographique pour le support

Un module cryptographique de type CSP (Cryptographic Service Provider en anglais) monolithique (Cf. section § 1.6.7 Support des modules cryptographiques ) ou un mini-pilote pour la nouvelle architecture SmartCard Base CSP / SmartCard KSP doit être disponible pour le support. Nous détaillons ces éléments ci-après.

Une AC fondée sur les services de certificats Active Directory de Windows Server repose historiquement sur CryptoAPI 1.0 pour l’ensemble des opérations cryptographiques.

CryptoAPI 1.0 désigne les APIs de gestion relatives aux opérations de chiffrement avec les algorithmes standard, les opérations étant réalisées dans l’architecture modulaire proposée par un fournisseur de services de chiffrement (Cryptographic Service Provider en anglais ou CSP).

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

* + Le livre blanc [Enterprise Smart Card Deployment in the Microsoft Windows Smart Card Framework](http://www.microsoft.com/downloads/details.aspx?FamilyID=fa7ec97c-11be-4e53-a0c4-04719b6a7ab6&DisplayLang=en)[[41]](#footnote-41)propose une vue d’ensemble de WSCF.

Le SmartCard Base CSP est disponible sous forme de téléchargement gratuit et optionnel pour Windows 2000 SP4, Windows XP SP2, Windows 2003 Server SP1 sur le site Microsoft à l’adresse <http://go.microsoft.com/fwlink/?LinkId=93341>. Il est présent nativement sur Windows Vista, Windows Server 2008 et ultérieur.

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

Windows Vista, Windows Server 2008 et ultérieur intègrent l’environnement cryptographique Cryptography API: Next Generation (CNG), bus cryptographique ouvert (Open Cryptographic Interface en anglais), appelé à remplacer la composante CryptoAPI 1.0 (opérations de chiffrement avec les algorithmes standard).

* + La documentation relative à CNG est accessible notamment au travers du Kit de développement afférent à l’adresse <http://www.microsoft.com/downloads/details.aspx?familyid=1ef399e9-b018-49db-a98b-0ced7cb8ff6f&displaylang=en>.

Une AC AD CS peut reposer, selon configuration, sur CryptoAPI 1.0 ou CNG. Ceci permet notamment de supporter les Key Service Provider (KSP en abrégé) de CNG et par voie de conséquence, de supporter en standard les algorithmes à courbes elliptiques (ECC) et les condensés de type SHA de deuxième génération, à savoir :

* ECDH\_P256, ECDH\_P384, ECDH\_P521 pour l’échange de clé ;
* ECDSA\_P256, ECDSA\_P384, et ECDSA\_P521 pour la signature ;
* La famille SHA-2 (SHA256, SHA384, et SHA512) et HMAC à base de ces condensés ;
  + Les éléments de configuration associés sont décrits dans le livre blanc [Active Directory Certificate Server Enhancements in Windows Server 2008](http://www.microsoft.com/downloads/details.aspx?FamilyID=9bf17231-d832-4ff9-8fb8-0539ba21ab95&DisplayLang=en)[[42]](#footnote-42).

La prise en compte avec CNG d’un support suppose de disposer d’un KSP pour ce support. Windows Vista, Windows Server 2008 et ultérieur intègre nativement un SmartCard KSP qui est le pendant du SmartCard Base CSP pour CryptoAPI 1.0.

Ce dernier offre un support des scénarios suivants :

* Enrôlement de certificat ECC sur une carte à puce (ce qui requiert le support d’ECC au niveau de l’infrastructure de confiance) ;
* Signature ECDSA avec un certificat ECC sur un support ;
* Echanges de clé avec ECDH avec des clés privées sur un support (pour l’authentification client avec TLS par exemple) ;
* Prise en charge sur le support des fonctions de dérivation (KDF en abrégé pourKey Derivation Functions en anglais) en conformité avec FIPS 140-2.

Le SmartCard KSP s’appuie sur le même modèle à base de mini-pilotes pour les cartes à puce de façon à faciliter la prise en compte de nouveaux supports. Il est ainsi possible de développer des mini-pilotes pour CryptoAPI, pour CNG, ou duals pour CryptoAPI et CNG.

Après qualification et certification par le Microsoft Smart Card Competency Center (SCCC), un mini-pilote peut être diffusé sur Windows Update.

* + La liste des prérequis est précisée dans le document v6.0 [Smart Card Minidriver Certification Requirements](http://www.microsoft.com/whdc/device/input/smartcard/sc-minidriver_certreqs.mspx)[[43]](#footnote-43).
  + L’ensemble des encarteurs proposent ou sont sur le point de proposer des mini-pilotes pour leur(s) carte(s) comme en témoigne la liste courante à l’adresse <http://catalog.update.microsoft.com/v7/site/Search.aspx?q=umdf>.

Les SmartCard Base CSP et SmartCard KSP représentent une traduction de l’engagement de Microsoft vis-à-vis des supports et de l’évolution du support de l’infrastructure carte à puce WSCF.

Cette nouvelle architecture est conçue pour :

* simplifier le déploiement et la prise en charge des supports,
* offrir un cadre de cohérence pour les implémentations des interfaces carte à puce,
* et simplifier l’accès aux fonctions de gestion associées aux supports comme le changement de code PIN ou le déblocage de support par exemple.



Windows 7 et Windows Server 2008 R2 propose une expérience utilisateur de type Plug-and-Play : la première insertion d'une carte à puce dans un lecteur de carte à puce déclenche des événements Plug-and-Play qui induisent une recherche d'un mini-pilote approprié sur le site Windows Update et le cas échéant un téléchargement automatique suivi d’une installation. Le mécanisme afférent est décrit dans la spécification v7.06 [Windows Smart Card Minidriver Specification](http://www.microsoft.com/whdc/device/input/smartcard/sc-minidriver.mspx)[[44]](#footnote-44).

De ce fait, l’utilisation d’une carte à puce disposant d’un mini-pilote certifié et donc disponible sur Windows Update avec un lecteur carte à puce USB conforme USB-CCID (Cf. section § 2.2.5.1 Disponibilité d’un lecteur reconnu pour le support) depuis un ordinateur connecté à Internet ne requiert aucune intervention de la part de l’utilisateur.

L’infrastructure carte à puce WSCF propose de facto un support natif et aussi transparent que possible des cartes à puces dans la mesure où les deux conditions précédentes sont remplies.

De plus, Windows 7 et Windows Server 2008 R2 introduisent une nouvelle plateforme pour les périphériques biométriques, en l’occurrence le Windows Biometric Framework (WBF en abrégé).

* + Le document [Introduction to the Windows Biometric Framework (WBF)](http://www.microsoft.com/whdc/device/input/smartcard/WBFIntro.mspx)[[45]](#footnote-45) propose une vue d’ensemble de WBF.

L’utilisation de ce Framework dans le contexte de l’infrastructure carte à puce WSCF permet la collecte et le traitement des données biométriques pour déverrouiller une carte à puce.

#### Considérations relatives au support lui-même

Ainsi qu’illustré précédemment, la plateforme Windows est agnostique par rapport au système d’exploitation du support (Java Card, .NET, MultOS, etc.) à partir du moment où un module cryptographique (CSP monolithique « legacy » ou mini-pilote) est disponible.

procedure_ddPar contre, les contraintes suivantes du support peuvent être prises en considération comme :

1. les caractéristiques cryptographiques du support avec le support d’algorithmes de type ECC (courbes elliptiques).

Les services de certificats Active Directory de Windows Server 2008 (R2) peuvent s’appuyer sur les fonctionnalités de CNG.

* + Le livre blanc [Installing a Suite B only PKI](http://go.microsoft.com/fwlink/?LinkId=148802)[[46]](#footnote-46) illustre comment déployer les services de certificats Active Directory (AD CS) pour supporter les algorithmes précédents, qu’il s’agisse des algorithmes ECC et/ou des condensés de type SHA-2.

Offrant par exemple d’ores et déjà le support de l’ensemble des algorithmes prévu par la PRIS v2.1 de l’ANSSI et de la DGME, une autorité de certification prend en charge de ce fait des algorithmes de type ECC non (encore) gérés par un support donné ;

* Comme mentionné à la section § Smart card-based logon in Windows Vista à la page 44 du livre blanc [Windows Vista Smart Card Infrastructure](http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en)[[47]](#footnote-47), les certificats basés sur ECC ne sont pas supportés pour l’ouverture de session par carte à puce. PKINIT basé sur ECC est encore en cours de standardisation au niveau de l’IETF (Cf. <http://www.ietf.org/html.charters/krb-wg-charter.html>).

1. la capacité du support influe directement sur le nombre de certificats, fonction également de la taille des clés ;
2. le facteur de forme.

## Administration et Exploitation

### Séparation des rôles

Les services de certificats Active Directory de Windows Server 2008 (R2) intègrent un modèle d’administration qui permet de satisfaire aux exigences des critères communs (Common Criteria en anglais) 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](http://www.commoncriteriaportal.org/files/ppfiles/PP_CIMCPP_SL1-4_V1.0.pdf)[[48]](#footnote-48).

procedure_ddUne AC AD CS 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**(CA Administrator) - Configure et administre les serveurs de certificats, désigne les gestionnaires et renouvelle les certificats des autorités de certification (via le composant enfichable MMC Autorité de certification (Certificate Authority en anglais) ;
* **Gestionnaire de certificats** (Certificate Manager, Officer dans CIMC) - Émet et révoque les certificats pour des groupes d'utilisateurs sur lesquels ils ont juridiction via le composant enfichable MMC Autorité de certification (Certificate Authority en anglais) ;
* **Agent de recouvrement** (Key Recovery Agent - KRA) – Configuration des KRAs (certificats) via le composant enfichable MMC Autorité de certification (Certificate Authority en anglais) ;
* **Auditeur** (Auditor) - Audite les actions des administrateurs locaux, des gestionnaires de services et de certificats ;
* **Opérateur de sauvegardes**(Backup Operator);

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 la commande *Certutil -setreg ca\RoleSeparationEnabled 1*

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.

### Délégation des rôles

Ceci est réalisable notamment au travers de la séparation des rôles.

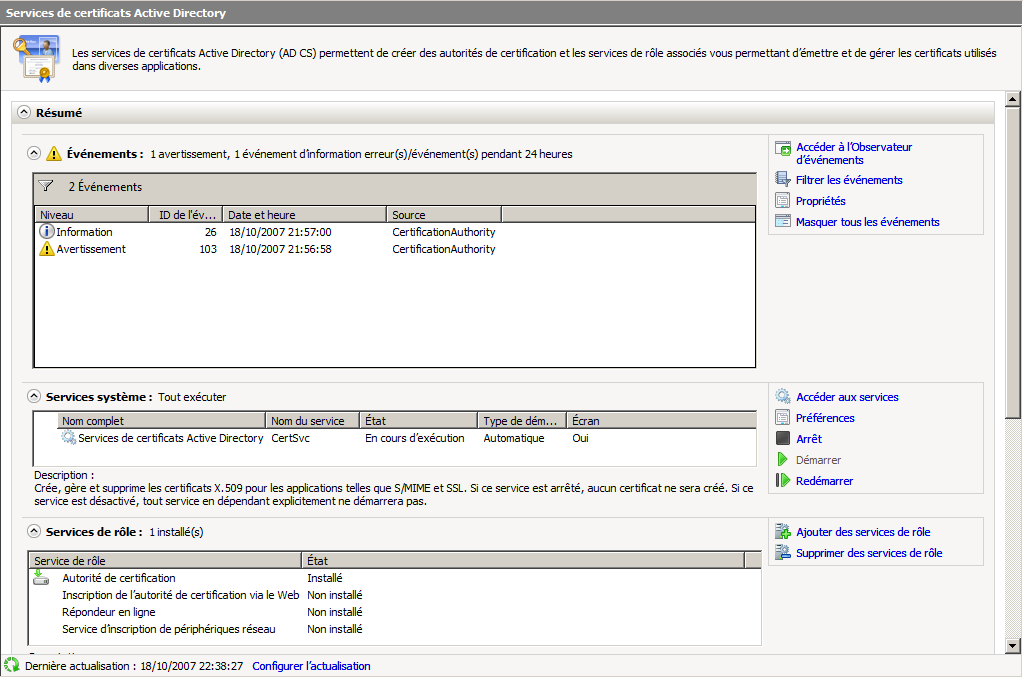
La version 3 des modèles de certificats permet d’aller plus loin dans la délégation par type de certificats et par type de populations (Cf. section § 1.3.9 Définition des modèles de certificat).

Enfin, l’environnement FIM permet de définir très précisément la gestion attendue pour les processus à prendre en considération.

### Type d’interface (Web ou autre)

Les interfaces utilisateurs sont aussi bien :

* de type Windows avec le Gestionnaire de serveur (Server Manager en anglais) et la fonction Gérer le rôle (Manage Role en anglais) pour le rôle Services de certificats Active Directory (Active Directory Certificate Services en anglais).



Différents composants enfichable MMC comme Modèles de certificat (Certificate Templates en anglais), Autorité de certification (Certification Authority en anglais), etc. sont alors utilisés.

* de type ligne de commandes avec les outils *Certutil.exe* (gestion de l'AC et des certificats) et *Certreq.exe* (requête de certificat vis-à-vis d'une AC ou pour la cross-certification) (ou encore, avec le Kit de Ressources Techniques, *Krt.exe* pour le recouvrement de clés ou *Chkcdp.exe* pour la vérification des extensions CDP et AIA d'un certificat).

Enfin, les fonctions AC et AE disposent d'une interface Web pour l’enrôlement (Cf. section § 1.3.1 Fonction d’enregistrement).

### Accès sécurisé aux interfaces

Dans le contexte d’une infrastructure Active Directory, un administrateur d’entreprise possède des privilèges élevés. Cependant, le compte d’administrateur d’entreprise par défaut n’est pas obligatoire pour installer et administrer les services et les ressources d’une IGC. Il est tout à fait possible de mettre en place la délégation de droits.

Au travers de l’activation de la séparation des rôles (Cf. section § 1.5.1 Séparation des rôles), les services de certificats Active Directory (AD CS) intègrent un modèle d’administration qui permet de satisfaire aux exigences des Critères Communs (Common Criteria en anglais) concernant la séparation de rôle, assurant ainsi qu’une seule personne n’est pas capable de compromettre la sécurité des services d’IGC.

Les rôles ainsi proposés sont Gestionnaire de services d’IGC, Gestionnaire de certificats, Agent de recouvrement, Auditeur et Opérateur de sauvegardes.

* + Ces aspects sont notamment abordés dans le livre blanc [Windows Server 2003 PKI Operations Guide](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspx)[[49]](#footnote-49).

L’administrateur d’entreprise peut in fine s’octroyer tout type de droits (comme tout administrateur système, quelle que soit la plate-forme considérée), mais cette action est auditable et peut être limitée en assurant une protection physique des serveurs concernés.

### Ergonomie

Les services de certificats Active Directory de Windows Server 2008 (R2) disposent de composants enfichables MMC, comme Autorité de certification (Certification Authority) ou encore de Modèles de certificats (Certificate Template) invoqués directement par le Gestionnaire de Serveur (Server Manager).

Ces composants MMC autorisent une administration entièrement graphique (et à distance si besoin) des différents services de ce rôle.

### *Provisionnement*

Une AC émettrice AD CS en mode entreprise fonctionne selon le principe de définition des droits d’accès lié à l’appartenance à des groupes de sécurité.

Ceci consiste simplement à positionner les utilisateurs dans des groupes (API AD).

Par ailleurs, la séparation des rôles peut être mise en place (Cf. section § 1.5.1 Séparation des rôles).

### Traçabilité

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, un numéro de séquence, etc.

Des interfaces d’instrumentation de la plate-forme comme WMI (Windows Management Instrumentation en anglais) ou des solutions de supervision comme Microsoft System Center Operation Manager (SCOM en abrégé) tirent directement bénéfices de cette approche standard plate-forme 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.

* + Pour des informations complémentaires sur SCOM, le lectorat pourra consulter les ressources techniques disponibles à l’adresse <http://www.microsoft.com/systemcenter/opsmgr/default.mspx>.

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

Comme toute application respectant les règles de développement plateforme, les services de certificats Active Directory (AD CS) de Windows Server 2008 (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.

### Archive de la trace

Au-delà de ce comportement par défaut décrit à la section précédente, rien n’empêche la configuration d’un module de sortie (exit module en anglais), l’un des deux points d’extensibilité du moteur tel que décrit dans la page MSDN [Certificate Services Architecture](http://msdn2.microsoft.com/en-us/library/Aa376540.aspx)[[50]](#footnote-50) ; ce dernier recevant l’ensemble des notifications du moteur lorsque des opérations ont lieu (par exemple l’émission d’un certificat) et peut donc stocker les logs dans une base SQL ou dans un fichier de log.

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 (Card Management System en anglais) de l’environnement FIM.

Alternativement, des solutions partenaires comme Quest InTrust décrite à l’adresse <http://www.quest.com/intrust/> peuvent être utilisées.

### Intégrité de la trace

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.

Enfin, dans le contexte de la mise en œuvre de SCOM, le service ACS (Audit Collection Services) collecte les événements qui sont entrés dans le journal de sécurité et stocke ces événements dans une base de données centrale en quasi temps réel via les notifications WMI. Lorsque la connexion est établie entre un redirecteur (forwarder en anglais) ACS et le collecteur (collector en anglais) ACS, le redirecteur ACS envoie les événements d'audit au collecteur ACS dès qu'ils se produisent. Lors de l'envoi d'événements immédiatement au référentiel central, la fenêtre donnée à un attaquant pour altérer la trace d'audit et supprimer des éléments de preuve d'une attaque se trouve des plus réduite.

Au-delà d’une authentification mutuelle du redirecteur ACS et du collecteur ACS et du chiffrement de la communication résultante, ACS assure sa propre sécurité en offrant une détection des lacunes dans les données transmises avec un mécanisme d’alerte. Les lacunes dans les données transmises pourraient signifier qu'un attaquant a falsifié/altéré le redirecteur ACS. Techniquement, comme précisé précédemment, chaque événement dispose d’un numéro de séquence uniformément croissant exprimé sous la forme d'un entier 32 bits. ACS mémorise le numéro de séquence de chaque événement et s'attend à ce que le prochain numéro de séquence soit supérieur d’un à celui en cours. Si ce n'est pas le cas, une alerte est générée. ACS peut différencier un journal effacé vs. un journal « wrappé » dans le conteste de la gestion circulaire vs. un numéro de séquence « wrappé »  vs. une falsification/altération.

### Supervision

Par défaut, les services de certificats Active Directory (de Windows Server 2008 (R2) proposent le composant enfichable MMC PKI d’entreprise (Enterprise PKI en anglais) qui permet de valider le statut d’une hiérarchie d’AC.

Un pack de gestion est également proposé à destination de SCOM ; ce pack exploite la journalisation effectuée par AD CS ainsi que les compteurs de performances exposés par AD CS (Cf. section § 1.8.3 Suivi des performances).

* + Pour des informations complémentaires sur SCOM, le lectorat pourra consulter les ressources techniques disponibles à l’adresse <http://www.microsoft.com/systemcenter/opsmgr/default.mspx>.

Du fait du faible niveau de sécurité proposé par le Simple Network Management Protocol (SNMP), il n’est pas possible d’utiliser ce protocole pour superviser la solution, d’ailleurs aucun des acteurs du marché de la supervision (comme notamment HP OV, CA TNG et IBM TIVOLI) n’utilise SNMP pour la supervision des environnements Windows et ce, depuis de nombreuses années.

### Notification

Si les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) ne proposent pas directement cette fonctionnalité, il est possible par contre d’interfacer les AC AD CS avec une solution de supervision comme SCOM.

Par ailleurs, il convient de noter que les plateformes Windows Vista, Windows Server 2008 et ultérieures disposent de notifications d’expiration dans le cas du modèle d’auto-enrôlement de façon à améliorer les conditions d’usages notamment pour les scénarios hors ligne.

La mise en place de notifications d’expiration de certificats à destination de systèmes non-Windows peut se faire au travers des interfaces *ICertAdmin* et *ICertAdmin2* exposées par le moteur d’AD CS et mentionnées précédemment, Cf. section § 2.1.11 Gestion des certificats en masse.

C’est en substance l’utilisation de ces interfaces qui permet à la commande suivante de définir les certificats qui vont expirer dans les 30 jours : *Certutil –view –restrict "NotAfter<=September 5,2009 08:00AM,NotAfter>=August 24,2009 08:00AM" –out "RequestID,RequesterName"*

# Enveloppe technique

Jauge de progression (2/3)

Ce chapitre envisage cette fois sous l’angle technique, notamment au travers de l’analyse des architectures et modèles de hiérarchie supportés, de la mise en œuvre, des performances ou encore de l’interopérabilité les caractéristiques, le respect des standards, les apports potentiels, etc. des composants d’AD CS pour la mise en œuvre d’une infrastructure de confiance au sein d’une organisation dans le contexte d’un environnement réparti et distribué.

## Architecture

### Architecture de l’IGC (découpage des fonctions : AC, sous AC, AE, etc.)

Les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) offrent un découpage clair des fonctions de façon à permettre différents modèles de déploiement au sein des entreprises dans un contexte d’interopérabilité ou non en fonction de leur existant éventuel en termes d’infrastructure de confiance. (Cf. section § 1.9 Interopérabilité et options).

Les « bonnes pratiques » sont rappelées par le livre blanc [Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx)[[51]](#footnote-51).

* + Le livre blanc [Designing a Public Key Infrastructure](http://technet2.microsoft.com/windowsserver/en/library/b1ee9920-d7ef-4ce5-b63c-3661c72e0f0b1033.mspx?mfr=true)[[52]](#footnote-52) peut également être consulté en termes de choix d’architecture.

### Hiérarchie de certification

Les AC émettrices AD CS peuvent êtres subordonnées à une autorité racine ou intermédiaire tierce existante ; en d’autres termes, une sous-hiérarchie d’autorités de certification mise en œuvre par AD CS de Windows Server 2008 (R2) peut être rattachée (subordonnée) à une hiérarchie existante mise en œuvre par des technologies tierces, Cf. section § 1.9.1 Interopérabilité avec des IGC tierces. Dans ce dernier cas, le certificat d’une AC AD CS est signé par une AC non Microsoft.

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

D’une façon générale, les modèles « hiérarchie de type racine » et « hiérarchie de type certification croisée (Cross Certification en anglais) par la subordination qualifiée » sont supportés avec des technologies de fournisseurs tiers.

#### Hiérarchies de type certification croisée (Cross Certification) par la subordination qualifiée

La notion de hiérarchie de type certification croisée (*Cross Certification*) est décrite dans la RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile[[RFC 3280](#RFC3280)].

Les services de certificats Active Directory (AD CS) de Windows Server 2008 (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).

procedure_ddLa 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 :
3. dans des espaces de noms invalides / non autorisés ;
4. avec des politiques d'émission invalides / non autorisées ;
5. 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](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx)[[53]](#footnote-53).

#### Support de l’AC Pont

Le modèle AC Pont selon le principe Federal Bridge Certification Authority (FBCA en abrégé) est également supportée par les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2).

A ce titre, les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) sont certifiés « *US Federal Bridge CA* » (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>).

### Formats des requêtes de certificats

Les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) supportent nativement les requêtes de certification (Certificate Signing Request en anglais ou CSR en abrégé) au :

* Format  PKCS #10 [[PKCS #10](#PKCS10)] Certification Request Standard ;
* Standard CMC tel que décrit dans la RFC 2797 Certificate Management over CMS [[RFC 2797](#RFC2797)] ;

Ainsi que via le protocole Simple Certificate Enrollment Protocol (SCEP) [[SCEP](#SCEP)].

### 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 à partir d’une conversion par ligne de commande via la commande *certutil –encode*.

### Taille de clé et algorithmes cryptographiques

Une AC AD CS de Windows Server 2008 (R2) permet de générer des certificats de 384 bits jusqu’à 16 384 bits en RSA, de 512 bits à 1024 bits en DSA et de 256 à 521 en ECC.

* Attention, il convient au lectorat de noter que la problématique n’est pas la génération mais l’utilisation de ce type de clé.

Une AC AD CS s’appuie historiquement sur les APIs de gestion CryptoAPI 1.0 (opérations de chiffrement avec les algorithmes standard) qui comporte une architecture ouverte à base de fournisseurs cryptographiques (Cryptographic Service Provider en anglais ou CSP en abrégé) pour les opérations cryptographiques.

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.

Par ailleurs, l’environnement cryptographique Cryptography API: Next Generation (CNG), bus cryptographique ouvert (Open Cryptographic Interface en anglais), appelé à remplacer la composante CryptoAPI 1.0, est nativement intégré par une AC AD CS de Windows Server 2008 (R2).

* + La documentation relative à CNG est accessible notamment au travers du Kit de développement afférent (<http://www.microsoft.com/downloads/details.aspx?familyid=1ef399e9-b018-49db-a98b-0ced7cb8ff6f&displaylang=en>).

Ceci permet notamment de supporter les Key Service Provider (KSP en abrégé) de CNG et, par voie de conséquence, de supporter en standard les algorithmes à courbes elliptiques (ECC en abrégé) et les condensés de type SHA deuxième génération, à savoir :

* ECDH\_P256, ECDH\_P384, ECDH\_P521 pour l’échange de clé ;
* ECDSA\_P256, ECDSA\_P384, et ECDSA\_P521 pour la signature ;
* la famille SHA-2 (SHA256, SHA384, et SHA512) et HMAC à base de ces condensés.
  + Ce support et les éléments de configuration associés sont décrits dans le livre blanc [Active Directory Certificate Server Enhancements in Windows Server 2008](http://www.microsoft.com/downloads/details.aspx?FamilyID=9bf17231-d832-4ff9-8fb8-0539ba21ab95&DisplayLang=en)[[54]](#footnote-54).

Cette description appelle les deux remarques suivantes :

* une AC AD CS supporte dès aujourd’hui l’ensemble des algorithmes décrite par la Politique de Référencement Intersectorielle de Sécurité (PRIS) v2.1 de l’ANSSI et de la DGME ;
* l’introduction des algorithmes type ECC au sein d’un environnement existant suppose que les applications et services consommateur d’IGC soient à même de prendre en charge ces algorithmes.

Ceci peut conduire par ailleurs à déployer vis-à-vis de la hiérarchie en place une hiérarchie distincte avec certification croisée (cross certification en anglais) comme suggéré dans le livre blanc précédent.

* + Le livre blanc [Installing a Suite B only PKI](http://go.microsoft.com/fwlink/?LinkId=148802)[[55]](#footnote-55) illustre comment déployer les services de certificats Active Directory (AD CS) pour supporter les algorithmes précédents, qu’il s’agisse des algorithmes ECC et/ou des condensés de type SHA-2.

Les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) supportent ce type de scénario avec la subordination qualifiée qui permet de préciser, le cas échéant, les contraintes (contraintes élémentaires, contraintes de nom, contraintes de politique, contraintes application) et d’inclure/exclure les usages (purposes en anglais). Ainsi, la subordination qualifiée permet non seulement de contrôler l’émission des ACs subordonnées mais également d’offrir un contrôle plus précis de la confiance dans les certificats.

* + Le livre blanc [Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx)[[56]](#footnote-56) développe ces aspects.

### Taille de l’exposant de clé

Les fonctions IGC d’une AC AD CS de Windows Server 2008 (R2) reposent sur les API CryptoAPI (CryptoAPI 1.0 et CryptoAPI 2.0) et CNG de la plateforme Windows. Ce point est donc géré plutôt par ces API et non par l’AC elle-même.

CryptoAPI 1.0 et CNG permettent nativement les opérations de chiffrement avec les algorithmes standards, Cf. section § 1.6.5 Taille de clé et algorithmes cryptographiques.

Une infrastructure de confiance basée sur les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) ne permet pas de choisir l’exposant pour la génération de paires de clés RSA, la valeur est toujours 65537. Par contre, d’autres valeurs d’exposants sont supportées pour les clés qui ne sont pas générées par l’infrastructure d’IGC en tant que telle.

Windows Server 2008 (R2) (par le biais de CNG) met à disposition un bus cryptographique ouvert (Open Cryptographic Interface en anglais) qui permet le cas échéant d’exécuter sa propre implémentation de tel ou tel algorithme.

### Support des modules cryptographiques

La plateforme Windows repose nativement sur les API CryptoAPI (CryptoAPI 1.0 et CryptoAPI 2.0) et CNG (Windows Vista, Windows Server 2008 et ultérieur).

Les modules cryptographiques pour les opérations de chiffrement avec les algorithmes standard s’appuient sur les fournisseurs de service de chiffrement :

* CSP (Cryptography Service Provider en anglais) pour CryptoAPI 1.0 ;
* et KSP (Key Storage Provider en anglais) pour CNG.

Il est intéressant de noter que les modules de chiffrement de la plateforme Windows (2000, XP et 2003) sont certifiés FIPS 140-1/140-2 dans le cadre du programme CMV (Cryptographic Module Validation, <http://csrc.nist.gov/cryptval>) du Computer Security Division à la NIST.

* + Les CSP d’origine Microsoft utilisent un générateur de nombre aléatoire (Random Number Generator en anglais ou RNG en abrégé) qui respecte le cadre de génération aléatoire décrit à l’annexe 3 de la publication FIPS186-2 (<http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>) sur la signature numérique par le NIST (National Institute of Standards and Technology).

Le CSP Microsoft Enhanced Cryptographic Provider (dans le mode FIPS) est certifié FIPS 140-1 (certificat n°238 Enhanced Cryptographic Provider (RSAENH) by Microsoft Corporation, <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1010.pdf>).

Pour le développement de CSP, il est possible de consulter avec profit :

* [Cryptographic Service Provider Developer's Toolkit (CSPDK)](http://www.microsoft.com/downloads/details.aspx?familyid=0F436C75-2304-42BB-B81A-BA0C2C47BAC2&displaylang=en)[[57]](#footnote-57)
* [CSP Test Suite for testing CSPs](http://www.microsoft.com/downloads/details.aspx?FamilyID=5f3872f8-202e-4f13-b495-78ce6f17a84f&DisplayLang=en)[[58]](#footnote-58)
  + Les bibliothèques d’importation et les fichiers d’entête sont disponibles dans le Microsoft Platform SDK qui est téléchargeable depuis l’adresse <http://www.microsoft.com/downloads/details.aspx?FamilyId=A55B6B43-E24F-4EA3-A93E-40C0EC4F68E5&displaylang=en>.

### Stockage des clés des AC

Les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) supportent l’utilisation de boitiers matériels (HSM en abrégé ou Hardware Storage Module en anglais) pour (la génération et) 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.

### Support des standards (PKCS #7, PKCS#10, PKCS#12, CRL X.509v2, etc.)

Les fonctions IGC d’une AC AD CS de Windows Server 2008 (R2) reposent sur les API CryptoAPI (CryptoAPI 1.0 et CryptoAPI 2.0) et CNG de la plateforme Windows. Ce point est donc géré plutôt par ces API et non par l’AC elle-même.

Pour mémoire, CryptoAPI 1.0 et CNG permettent nativement les opérations de chiffrement avec les algorithmes standards, Cf. section § 1.6.5 Taille de clé et algorithmes cryptographiques.

CryptoAPI 2.0 permet nativement :

* La gestion des messages de signature et de chiffrement aux formats standards (PKCS #7 [[PKCS # 7](#PKCS7)], CMS [[RFC 3852](#RFC3852)]),
* La gestion des demandes de certificat, des certificats et des CRL aux formats standards (PKCS #10 [[PKCS #10](#PKCS10)], CMC [[RFC 2797](#RFC2797)], certificats X509v3, CRL X509v2)
* L’utilisation et la vérification des certificats, des signatures, des CRL selon les standards tels que définis par les RFC 2459 [[RFC 2459](#RFC2459)] et 3280 [[RFC 3280](#RFC3280)]. L'architecture prend en compte la vérification en ligne telle qu’OCSP en conformité avec la RFC 2560 [[RFC 2560](#RFC2560)], Cf. section § 1.6.14 Protocole d’accès aux CRL.

Sur la base de CryptoAPI 1.0 et/ou de CNG selon configuration.

### Compatibilité avec le monde XML (protocole XKMS, WS-Trust)

La recommandation XKMS (XML Key Manipulation Service) du W3C est destinée à être implémentée en tant que service Web permettant à un client d'accéder à des fonctions que l'on retrouve dans les standards de l’infrastructure d’IGC.

XKMS est composée de deux protocoles :

1. X-KISS (XML Key Information Service Specification) pour les requêtes de localisation et de validation des clés publiques ;
2. X-KRSS (XML Key Registration Service Specification) pour enregistrer, renouveler, révoquer et obtenir des clés.

Comme contributeur et co-auteur de la spécification XKMS , il nous apparaît, que le débat autour d’XKMS (qui ne bénéficie pas à ce jour d’implémentations majeures) à une tendance naturelle à s’orienter vers le standard OASIS WS-Trust des services Web avancés (pile standardisée WS-\*) pour les scénarios d’enrôlement X.509. Nos investissements vont clairement dans ce sens.

* + Le livre blanc [Introduction à l’architecture de services Web et ses spécifications WS-\*](http://www.microsoft.com/france/msdn/architects/intro-WS.mspx)[[59]](#footnote-59) donne une vue d’ensemble de la pile WS-\* et des spécifications/protocoles, recommandations W3C ou standards OASIS, qui la constituent. Ces standards résultants sont ouverts, publics et libres d’implémentation et disposent aujourd’hui de nombreuses implémentations quels que soient les environnements techniques.

Le standard OASIS WS-Trust définit en particulier un modèle de service de jetons de sécurité auprès duquel de tels jetons de sécurité peuvent être obtenus ainsi que le protocole pour converser avec ce service de jetons de sécurité. Un tel service est à même d’émettre, de valider et d’échanger des jetons de sécurité. (La notion d’échange induit la capacité transformation de jetons en termes de type de confiance, de format, de sémantique et des (valeurs des) revendications véhiculées par un jeton.)

Ce sujet renvoie également à celui de l’interopérabilité des infrastructures de gestion de clés publiques (Cf. section § 1.9 Interopérabilité et options).

En effet, de façon à proposer des services d’(auto-)enrôlement et d’(auto-)renouvellement fondés sur HTTP/WS-\*, Microsoft a défini des extensions du standard OASIS WS-Trust qui se traduisent par les deux spécifications [MS-WSTEP] : WS-Trust Enrollment Extensions [[MS-WSTEP](#MSWSTEP)] et [MS-XCEP] : X.509 Certificate Enrollment Policy Protocol Specification [[MS-XCEP](#MSXCEP)].

Ces spécifications sont implémentées dans les services Web d’enrôlement de certificats de Windows 7 et Windows Server 2008 R2 (Cf. section § 2.1.1 Fonction d’enregistrement).

Des travaux connexes sont en cours avec des éditeurs de logiciels, des autorités de certification commerciales afin de mettre à disposition des solutions interopérables. A ce titre, une mise en œuvre de ces protocoles vient d’être démontrée publiquement par GlobalSign dans le cadre de l‘évènement Microsoft TechEd US qui s’est déroulé du 11 au 15 mai 2009 pour l’enrôlement et le renouvellement de certificat SSL sur l’Internet.

### Support du protocole d’enregistrement SCEP

L’enrôlement via le protocole SCEP [[SCEP](#SCEP)] est supporté par les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) au travers du service de rôle Service d’inscription des périphériques réseau (Network Device Enrollment Services en anglais).

* + L’implémentation de ce protocole est décrite dans le livre blanc [Microsoft SCEP Implementation](http://www.microsoft.com/downloads/details.aspx?FamilyID=e11780de-819f-40d7-8b8e-10845bc8d446&DisplayLang=en)[[60]](#footnote-60).

### Systèmes d’exploitation supportés

Les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) constituent l’un des rôles serveur de Windows Server 2008 (R2).

Ce système est par voie de conséquence requis pour les fonctions serveur d’IGC.

### Mode de publication des CRL

Le module enfichable MMC Autorité de certification (Certification Authority en anglais) et l'outil en ligne de commande *Certutil.exe* ainsi que le fichier *CAPolicy.inf* d'installation d'une AC permettent le paramétrage complet de la publication des CRL (et delta CRL).

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

* + Le livre blanc [Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx)[[61]](#footnote-61) décrit les éléments de configuration associés. Ces derniers s’appliquent à une AC AD CS de Windows Server 2008.

### Protocole d’accès aux CRL

Au-delà du support des protocoles HTTP et de LDAP pour l’accès aux CRL, Windows Server 2008 (R2) propose, au sein du rôle Services de certificats Active Directory (Active Directory Certificate Services), le service de rôle Répondeur en ligne (Online Responder). Ce dernier offre une implémentation du protocole OCSP conforme à la RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP [[RFC 2560](#RFC2560)].

* + Ce service est décrit dans le livre blanc [Installing, Configuring, and Troubleshooting the Microsoft Online Responder](http://technet2.microsoft.com/windowsserver2008/en/library/045d2a97-1bff-43bd-8dea-f2df7e270e1f1033.mspx)[[62]](#footnote-62).

Il convient de noter que Windows Vista, Windows Server 2008 et ultérieur disposent de l’instrumentation *CryptoAPI 2.0 Diagnostics* qui offre la possibilité de diagnostiquer et résoudre des problèmes PKI en collectant une information détaillée sur la validation des chaînes de certificats, des opérations relatives aux magasins de certificats, et de la vérification des signatures.

* + Cette composante est décrite dans le livre blanc [Troubleshooting PKI Problems on Windows Vista](http://technet2.microsoft.com/WindowsVista/en/library/771e1f29-4eba-40c9-9193-60043889bbf41033.mspx)[[63]](#footnote-63).

Les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) n’offrent pas de support direct de la Liste des Autorités Révoquées (ARL en abrégé ou Authority Revocation List en anglais). Moyennant un processus manuel, il est possible de créer et de maintenir une « ARL artificielle ».

### Base de stockage locale

Les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) s’appuient sur une base de donnée locale basée sur la technologie Jet, et ce quel que soit le type d'AC (mode autonome vs. mode entreprise). Ceci permet de bénéficier de l’ensemble des outils disponibles pour cette technologie.

Les AC émettrices AD CS en mode entreprise s'appuient, en plus, sur des informations de configuration stockées dans la partition de configuration de leur forêt Active Directory d'appartenance.

## Mise en place

### Facilité d’installation

L’installation d’une AC AD CS est prise en charge par l’option Services de certificats Active Directory (Active Directory Certificate Services en anglais) de l’assistant Ajouter des rôles (Add Roles en anglais) du Gestionnaire de serveur (Server Manager en anglais).

L’Outil de gestion des rôles (Roles Management Tool en anglais ou RMT en abrégé) gère les dépendances internes en fonction des composantes sélectionnées (Cf. section § 1 Introduction) et installe les (autres) fonctionnalités (éventuellement) manquantes.

L’assistant d’installation propose une définition de valeurs par défaut pour l’ensemble des étapes (avec ou sans fichier *CAPolicy.inf* d’installation).

Depuis les premières versions, l’installation d’une AC AD CS peut être dans la pratique largement automatisée via la définition d’un fichier *CAPolicy.inf* d’installation et de scripts complémentaires fondés sur l’utilitaire en ligne de commande *Certutil.exe*.

* + Le livre blanc [Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx)[[64]](#footnote-64) décrit les éléments associés.

Ceci étant, Windows Server 2008 a introduit l’objet COM *certocm.CertSrvSetup* (*certocm.dll*) fondé sur l’interface *ICertSrvSetup* qui peut être utilisé pour contrôler complètement l'installation d’une AC. L’interface *ICertSrvSetup* définit à cet effet un ensemble de méthodes et de propriétés pour installer et désinstaller les composants (service du rôle) Autorité de certification (AC) et Inscription de l’autorité de certification via le Web(CAWE).

* + Les méthodes et les propriétés de l’interface *ICertSrvSetup* sont documentées à l’adresse <http://msdn.microsoft.com/en-us/library/bb736371(VS.85).aspx>.

Le billet [Automated CA installs using VB script on Windows Server 2008 and 2008 R2](http://blogs.technet.com/pki/archive/2009/09/18/automated-ca-installs-using-vb-script-on-windows-server-2008-and-2008r2.aspx)[[65]](#footnote-65) propose le script VBScript *SetupCA.vbs* (Cf. section § 3.4.5 Environnement de « scripting ») utilisé en interne par le groupe produit pour les tests du rôle Services de certificats Active Directory. Ce script qui repose sur l’objet COM précédent permet d’automatiser l’installation et la configuration des deux composants précédents. Il donne accès de façon automatisée à l’ensemble des fonctionnalités accessibles depuis l’interface graphique de l’assistant d’installation. Ainsi, la plupart des fonctionnalités offertes se traduisent par la simple définition de propriétés ; quelques fonctionnalités, telles que la réutilisation de clé/certificat, requièrent cependant un peu (plus) de code.

Il convient de noter que ce script permet également d’automatiser l’installation et la configuration d’une AC AD CS au niveau d’une installation de type Server Core de Windows Server 2008 R2 où par essence, aucune interface graphique n’est disponible pour l’installation. Ceci peut nécessiter quelques étapes additionnelles comme suit :

1. Si la fonctionnalité WoW64 est nécessaire, par exemple pour utiliser sur le système 64 bits un boîtier HSM réseau qui s’appuie sur des fichiers binaires 32 bits, la prise en charge WoW64 doit être installée via la commande *Start /w ocsetup ServerCore-WOW64* et nécessite un redémarrage à l’issue de l’installation du « package ».
2. Si l’AC doit fonctionner avec un boîtier HSM réseau ou non, le logiciel afférent doit être installé et configuré selon les instructions fournies.
3. Le script *SetupCA.vbs* précédent peut ensuite être utilisé pour procéder à l’installation en tant que telle de l’AC.

Le billet [Using VBScript to install CA on server core](http://blogs.technet.com/pki/archive/2009/09/18/using-vbscript-to-install-ca-on-server-core.aspx)[[66]](#footnote-66) décrit l’utilisation de ce script dans le contexte d’une installation de type Server Core.

Enfin, au-delà de ces éléments et vis-à-vis de la version précédente des services de certificats, l’ergonomie générale ainsi que les capacités de diagnostic se sont très sensiblement améliorées. A ce propos, Windows Server 2008 R2 introduit l’outil Analyseur des « bonnes pratiques » (Best Practices Analyzer en anglais ou BPA en abrégé).

### Configuration du produit

Le Gestionnaire de serveur (Server Manager en anglais) au travers notamment du composant enfichable MMC Autorité de certification (Certificate Authority en anglais) permet une configuration en mode graphique d’une AC AD CS.

L’utilitaire en ligne de commande *Certutil.exe* permet de réaliser ces opérations depuis une invite de commande.

* + Le guide [Windows Server 2003 Certificate Server Common Criteria Configuration Guide](http://download.microsoft.com/download/f/2/0/f206c1fe-b176-4910-a812-68767867ee01/WS03CertServer_Common_Criteria_Configuration_Guide.zip)[[67]](#footnote-67) décrit la configuration relative à l’évaluation CIMC (Certificate Issuing and Management Components) Security Level 3 Protection Profile qui a été réalisée d’AD CS (Cf. [NIAIP Certification for Windows Server 2003 Certificate Server](http://www.niap-ccevs.org/cc-scheme/st/vid9507/)).

### Sécurisation des accès logiques

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

1. Forcer une authentification par carte à puce pour l’accès en local des stratégies de groupes (Group Policy Object en anglais ou GPO en abrégé) adaptées ;
2. Contrôler l’appartenance aux groupes Active Directory sensibles ;
3. Activer la séparation des rôles (Cf. section § 1.5.1 Séparation des rôles) ;

Windows Server 2008 R2 permet d’aller encore plus loin et d’imposer le « carte à puce nécessaire » pour le contrôle d’accès quel que soit les modalités d’accès (en local ou à distance).

Pour ce faire, il convient d’associer un SID de groupe Active Directory à un OID de politique d’émission, de configurer un modèle de certificat (Cf. section § ) pour l’ouverture de session avec l’OID de politique d’émission précédent, de restreindre les accès aux objets en termes de liste de contrôle d’accès (Access Control List en anglais ou ACL en abrégé), d’enrôler les personnes concernées par le rôle souhaité avec un support physique. Lorsqu’une personne ouvre une session avec un certificat basé sur le modèle de certificat précédent, Kerberos ajoute automatiquement le SID du groupe dans le jeton Utilisateur.

Ces différentes actions sont des actions de configuration et de paramétrage.

### 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.

### Virtualisation du produit

Une seule AC AD CS peut être installée par instance Windows Server 2008 (R2). Par contre, AD CS est virtualisable au sens qu’une AC AD CS peut fonctionner dans une machine virtuelle gérée par Microsoft Hyper-V.

* + Les ressources techniques relatives à Microsoft Hyper-V sont disponibles à l’adresse <http://www.microsoft.com/hyper-v-server/en/us/default.aspx> comme le document [Hyper-V Planning and Deployment Guide](http://www.microsoft.com/downloads/details.aspx?familyid=5DA4058E-72CC-4B8D-BBB1-5E16A136EF42&displaylang=en)[[68]](#footnote-68).

Une même License Windows Server 2008 (R2) permet d’utiliser sur la plateforme hôte jusqu’à 4 machines virtuelles Windows Server 2008 (R2).

### Haute-disponibilité

3 niveaux de disponibilités sont à prendre en considération et possibles pour les services de certificats Active Directory :

1. CRL : critique, facilement redondé. Les approches possibles sont le round-robin DNS, le support du « scale-out » notamment avec le Service de répartition de charge réseau Microsoft (MicrosoftNetwork Load Balancing en anglais ou NLB en abrégé) de la plateforme Windows Server, etc. ;
2. OCSP : critique, facilement redondé. Les approches possibles sont le round-robin DNS, le support du « scale-out » notamment avec le Service de répartition de charge réseau Microsoft (MicrosoftNetwork Load Balancing en anglais ou NLB en abrégé) de la plateforme Windows Server, etc. ;
3. AC : selon besoins d’administration.

Au-delà de la virtualisation (Cf. section précédente), AD CS de Windows Server 2008 (R2) supporte la mise en œuvre des services de clusterisation Microsoft (Microsoft Cluster Service en anglais ou MSCS en abrégé) avec cluster à 2 nœuds (en mode actif-passif).

* + Le livre blanc [Overview of Failover Clustering with Windows Server 2008](http://download.microsoft.com/download/3/B/5/3B51A025-7522-4686-AA16-8AE2E536034D/Windows%20Server%202008%20Failover%20Clustering%20Architecture%20Overview.doc)[[69]](#footnote-69) offre une vue d’ensemble de ce service de la plateforme Windows Server.
  + Le livre blanc [Certification Authority Clustering Configuration and Troubleshooting Guide](http://go.microsoft.com/fwlink/?LinkId=118364)[[70]](#footnote-70) décrit la mise en œuvre associée et le billet [To Cluster or Not to Cluster CAs](http://blogs.technet.com/wincat/archive/2008/07/21/to-cluster-or-not-to-cluster-cas.aspx)[[71]](#footnote-71) quelques considérations associées.
  + Pour des informations complémentaires sur les services NLB et MSCS de la plateforme Windows Server 2008 (R2), le lectorat pourra consulter les ressources techniques disponibles à l’adresse <http://www.microsoft.com/windowsserver2008/en/us/high-availability.aspx>.

## Performances

### Nombre de requêtes par seconde

Comme l’indique la page TechNet [Evaluating CA Capacity, Performance, and Scalability](http://technet2.microsoft.com/windowsserver/en/library/61b3334a-eb6d-4d7d-b122-ca0c6ab18f5f1033.mspx)[[72]](#footnote-72) dont les éléments remontent à 2003, le nombre de certificats émis et les performances associées dépendent de nombreux facteurs.

Néanmoins, des tests effectués sur une AC autonome (sans HSM) il y a quelque temps ont montré les résultats suivants :

* Emission de certificats avec une clé de 512 : 52 certificats/seconde, 4 492 000 certificats/jour,
* Emission de certificats avec une clé de 2048 : 25 certificats/seconde, 2 246 000 certificats/jour.
* Emission continue jusqu'à 30 000 000 certificats pour une clé de 512 avec un taux moyen de 30 certificats/seconde.

Le billet [Scale testing the world’s largest PKI… all running on WS08R2 and Hyper-V](http://blogs.technet.com/wincat/archive/2009/08/10/scale-testing-the-world-s-largest-pki-all-running-on-ws08r2-and-hyper-v.aspx)[[73]](#footnote-73) propose des résultats de tests dans un contexte de mise en œuvre avec virtualisation via Hyper-V avec HSM. Les résultats mentionnés confirment les performances du moteur de l’AC.

### Volumétrie atteinte

Les tests mentionnés à la section précédente ont par ailleurs montré la capacité à générer jusqu’à 37 millions de certificats avec un tirage en continu. Compte tenu de l’évolution du matériel, ces chiffres sont aujourd’hui vraisemblablement à revoir sensiblement à la hausse.

### Suivi des performances

Par ailleurs, afin de suivre finement l’évolution des performances, AD CS de Windows Server 2008 propose de très nombreux compteurs de performances.

Les compteurs de performances sont installés en fonction des rôles serveur activé. Ainsi, par exemple, si une AC est installée, les compteurs pour les groupes Autorité de certification (Certification Authorityen anglais) et Connexions de l’autorité de certification (Certificate Authority Connections en anglais) sont également installés et une instance *certsrv* est ajoutée aux compteurs Base de données, Base de données ⇨ Instances, Base de données ⇨ TableClasses (respectivement Database, Database Instances et DatabaseTableClasses en anglais). De même, le rôle OCSP ajoute les compteurs pour Serveur OCSP et Connexions au serveur OCSP (OCSP Server et OCSP Server Connectionsen anglais).

Ces compteurs de performances AD CS peuvent être observes localement ou à distance depuis une machine Windows Server 2008 (R2), Windows 7, Windows Vista, Windows Server 2003 (R2), ou Windows XP. L’accès à distance suppose l’activation du service Registre à distance (Remote Registry en anglais).

### Montée en charge

La page TechNet [Evaluating CA Capacity, Performance, and Scalability](http://technet2.microsoft.com/windowsserver/en/library/61b3334a-eb6d-4d7d-b122-ca0c6ab18f5f1033.mspx)[[74]](#footnote-74) précise les éléments pouvant influer sur la montée en charge au-delà des performances intrinsèque du moteur.

## Interopérabilité et options

### Interopérabilité avec des IGC tierces

En termes d’interopérabilité, une AC AD CS a été la première à démontrer l’ensemble des tests dans le cadre du projet *pki Challenge* (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 visait à identifier, analyser et dépasser les problématiques d’interopérabilité entre les fournisseurs de solutions d’IGC.

* + Les différents rapports sont disponibles à l’adresse <http://www.eema.org/index.cfm?fuseaction=focus.content&cmid=148&CFID=975663&CFTOKEN=2bdf69d6cad49b86-3DDD99FF-DC10-06CC-FF7036B9F996558D>.

### Renommage des AC

Comme décrit dans l’article 231182 [Certificate Authority Servers Cannot Be Renamed or Removed from Network](http://support.microsoft.com/?id=231182)[[75]](#footnote-75), une AC AD CS ne peut pas être renommée.

### AC mise « hors ligne »

Une AC AD CS en mode autonome peut être mise « hors ligne ». Une AC AD CS d’Enterprise ne peut pas être hors ligne compte tenu du besoin de connectivité avec Active Directory.

### API de développement et extensibilité

Les différentes API sont publiques et documentées. Ainsi, la nouvelle API d’enrôlement Certificate Enrollment (CertEnroll) destinée à Windows Vista, Windows Server 2008 et ultérieur est disponible à la page MSDN [Certificate Enrollment API](http://msdn2.microsoft.com/en-us/library/aa374863.aspx)[[76]](#footnote-76).

Il en est de même pour :

* l’interface *ICertSrvSetup* pour installer et désinstaller les composants (service du rôle) Autorité de certification (AC) et Inscription de l’autorité de certification via le Web(CAWE). Cette dernière est décrite à l’adresse <http://msdn.microsoft.com/en-us/library/bb736371(VS.85).aspx>,
* ou encore les interfaces *ICertAdmin* et *ICertAdmin2* exposées par le moteur d’AD CS et mentionnées précédemment. Ces dernières sont décrites à l’adresse <http://msdn2.microsoft.com/en-us/library/Aa383234.aspx>.
  + La spécification [MS-CSRA]: Certificate Services Remote Administration Protocol Specification [[MS-CSRA](#MSCSRA)] spécifie le protocole afférent qui se compose des interfaces DCOM ci-dessus.

#### Personnalisation des fonctions d’AC

L'architecture du moteur est décrit dans la page MSDN [Certificate Services Architecture](http://msdn2.microsoft.com/en-us/library/Aa376540.aspx)[[77]](#footnote-77).

Cette dernière intègre les modules suivants :

* **Modules de politique**(Policy Modulesen anglais) - Modules utilisés lors de l’évaluation d’une requête de certificat ; ces programmes imposent les règles par lesquelles les *services de certificats* valident ou rejettent la demande.
  + Une description de l’interface de ce module est disponible à l’adresse <http://msdn2.microsoft.com/en-us/library/Aa387348.aspx>.
* **Modules de sortie** (Exit Modulesen anglais) - Modules qui reçoivent les notifications du moteur lorsque des opérations ont lieu, par exemple émission d’un certificat.
  + Une description de l’interface de ce module est disponible à l’adresse <http://msdn2.microsoft.com/en-us/library/Aa382386.aspx>.
* **Gestionnaires d’extension** (Extension Handlers en anglais) - Objets COM fournissant les routines pour l’encodage de types de données ou d’extensions plus complexes.
  + Une description de l’interface de ce module est disponible à l’adresse <http://msdn2.microsoft.com/en-us/library/Aa382414.aspx>.
* **Intermédiaires** (Intermediaries en anglais) - Programmes qui communiquent avec l’application cliente pour autoriser la soumission de requêtes de certificats.
  + Une description de l’interface de ce module est disponible à l’adresse <http://msdn2.microsoft.com/en-us/library/Aa386311.aspx>.

#### Personnalisation des fonctions d’AE de FIM 2010

La solution FIM dispose de son propre Kit de développement (ou SDK).

* + La documentation de ce dernier est accessible à l’adresse <http://msdn2.microsoft.com/en-us/library/bb491106.aspx>.

### Environnement de « scripting »

Les différentes API comme l’API d’enrôlement CertEnroll peuvent facilement être utilisé dans les environnements de script de la plateforme Windows, qu’il s’agisse de l’environnement historique Windows Scripting Host ou du nouvel environnement Windows PowerShell comme l’illustre le Weblog [My Nuggets](http://blogs.technet.com/vishalagarwal/)[[78]](#footnote-78).

* + Le [ScriptCenter TechNet](http://technet.microsoft.com/fr-fr/scriptcenter/dd742419(en-us).aspx)[[79]](#footnote-79) propose une bibliothèque de scripts prêts à l’emploi pour ces environnements de scripting.

Windows PowerShell, est une interface en ligne de commande et un langage de script fondé sur la programmation orientée objet et le framework Microsoft .NET. Windows PowerShell 1.0 constitue une fonctionnalité de Windows Server 2008. La version 2.0 est disponible en standard dans Windows 7 et Windows Server 2008 R2.

* + Pour de plus amples informations sur Windows PowerShell, vous pouvez consulter le guide [Windows PowerShell Owner Manual](http://www.microsoft.com/technet/scriptcenter/topics/winpsh/manual/default.mspx)[[80]](#footnote-80), le site TechNET [Windows PowerShell](http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx)[[81]](#footnote-81) ainsi que le Weblog [Windows PowerShell](file:///C:\Users\philber\Documents\Activités\DS&T\Sécurité\Livrables\FY10\Grille%20d'évaluation%20AD%20CS%20Windows%20Server%202008%20R2\Windows%20PowerShell%20Blog)[[82]](#footnote-82).

# Coûts et services

Jauge de progression (2/3)

Ce chapitre précise les coûts associés aux composants d’AD CS, et composantes connexes comme FIM, ainsi que les services associés notamment en termes de support pour la mise en œuvre d’une infrastructure de confiance au sein d’une organisation dans le contexte d’un environnement réparti et distribué.

## Coût

Les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2) constituent l’un des rôles serveur de Windows Server 2008 (R2).

Il n’y a pas de facturation « par certificat » associée aux fonctions nécessaires pour établir une infrastructure de confiance AD CS. Ces fonctions sont disponibles dans Windows Server 2008 (R2), et leur droit d’utilisation inclus dans le coût des licences associées.

En revanche, l’utilisation des fonctions de gestion du cycle de vie des certificats X.509 v3 (et des supports), apportées par le produit Microsoft Forefront Identity Manager (FIM) 2010 nécessite l’acquisition de licences.

FIM rentre dans le modèle de licence associant :

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

(\*) Extrait de la PUR octobre 2007 : comme définit dans le document dit de « *Product User Rights* » Microsoft, disponible sur le site web à l’adresse <http://www.microsoftvolumelicensing.com/userights/PUR.aspx>,

« *il existe deux types de licences d’accès client : un licence destinée aux dispositifs et une licence destinée aux utilisateurs…* ».

Dans le cas du produit FIM, un seul type d’accès client est disponible : celui destiné aux utilisateurs…

« *Chaque licence d’accès client, par utilisateur, autorise un utilisateur, utilisant n’importe quel dispositif, à accéder aux instances du logiciel serveur sur vos serveurs concédés sous licence.* »

L’utilisation des seules fonctions de synchronisation d’annuaire de FIM ne nécessite pas l’acquisition de CAL (ni de connecteur externe), mais seulement l’acquisition des serveurs.

## Niveau de 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.

## Disponibilité du support

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 <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 <http://support.microsoft.com/gp/premsup>.
3. Références

Cette annexe regroupe l’ensemble des liens mentionnés dans la présente grille d’évaluation vers les standards cités ainsi que les compléments d’informations sur les fonctionnalités des services Active Directory Certificate Services (AD CS) de la plateforme Windows Server 2008 (R2) pour la mise en œuvre d’une infrastructure de confiance.

**Standards**

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

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

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

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

RFC 3279Algorithms 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>

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 #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-19.txt>

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

**Protocoles AD CS**

Les protocoles suivants sont disponibles dans le cadre du programme WSPP (Windows Server Protocols)[[83]](#footnote-83) selon les termes de l’[OSP (Open Specification Promise en anglais)](http://www.microsoft.com/france/interop/osp/default.mspx)[[84]](#footnote-84).

[MS-CRTD]: Certificate Templates Structure Specification, <http://msdn.microsoft.com/en-us/library/cc226517(PROT.13).aspx>

[MS-CSRA]: Certificate Services Remote Administration Protocol Specification, <http://msdn.microsoft.com/en-us/library/cc226566(PROT.13).aspx>

[MS-DCOM]: Distributed Component Object Model (DCOM) Remote Protocol Specification, <http://msdn.microsoft.com/en-us/library/cc226801(PROT.13).aspx>

[MS-WCCE]: Windows Client Certificate Enrollment Protocol Specification, <http://msdn.microsoft.com/en-us/library/cc249879(PROT.13).aspx>

[MS-WSTEP]: WS-Trust X.509v3 Token Enrollment Extensions, <http://msdn.microsoft.com/en-us/library/dd340609(PROT.13).aspx>

[MS-XCEP]: X.509 Certificate Enrollment Policy Protocol Specification, <http://msdn.microsoft.com/en-us/library/dd302869(PROT.13).aspx>

**Ressources Windows Server 2008 R2**

Cross-forest Certificate Enrollment with Windows Server 2008 R2, <http://go.microsoft.com/fwlink/?LinkId=139681>

Windows Server 2008 R2 Certificate Enrollment Web Services Whitepaper, <http://download.microsoft.com/download/C/2/2/C229E624-36E4-4AD8-9D86-F564ED539A16/Windows%20Server%202008%20R2%20Certificate%20Enrollment%20Web%20Services.doc>

**Ressources Windows Server 2008**

Windows Server Active Directory Certificate Services Step-by-Step Guide, <http://go.microsoft.com/fwlink/?LinkID=85472>

Active Directory Certificate Server Enhancements in Windows Server 2008, <http://www.microsoft.com/downloads/details.aspx?FamilyID=9bf17231-d832-4ff9-8fb8-0539ba21ab95&DisplayLang=en>

Suite B PKI in Windows Server 2008, <http://go.microsoft.com/fwlink/?LinkId=148802>

Active Directory Certificate Services Upgrade and Migration Guide, <http://www.microsoft.com/downloads/details.aspx?familyid=C70BD7CD-9F03-484B-8C4B-279BC29A3413&displaylang=en>

Implementing and Administering Certificate Templates in Windows Server 2008, <http://go.microsoft.com/fwlink/?LinkID=92522>

Certification Authority Clustering Configuration and Troubleshooting Guide, <http://go.microsoft.com/fwlink/?LinkId=118364>

Key Archival and Recovery in Windows Server 2008, <http://go.microsoft.com/fwlink/?LinkID=92523>

Installing, Configuring, and Troubleshooting Microsoft Online Responder, <http://go.microsoft.com/fwlink/?LinkId=101269>

Microsoft SCEP Implementation, <http://www.microsoft.com/downloads/details.aspx?FamilyID=e11780de-819f-40d7-8b8e-10845bc8d446&DisplayLang=en>

**Ressources Windows Server 2003**

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 et Windows 7**

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. Synthèse des composants et fonctionnalités

Le tableau suivant propose une synthèse des composants et fonctionnalités disponibles pour AD CS en fonction des version et édition de Windows Server.

| Version et Edition de Windows Server | Composants (service de rôle) disponibles | Modèles de certificat disponible | Auto-enrôlement et séquestre de clé (vient avec la version 2 des modèles de certificat) | Module de sortie SMTP et séparation des rôles | Enrôlement multi-forêt (via le protocole DCOM) |
| --- | --- | --- | --- | --- | --- |
| Windows Web Server 2008 R2 | None | Non applicable | Non applicable | Non applicable | Non applicable |
| Windows Server 2008 R2 Standard ou Foundation | * Autorité de certification (CA) * Inscription de l’autorité de certification via le Web (CAWE) * Services Web d’enrôlement de certificats\* (CEP et CES) | Modèles de certificats versions 1, 2\*, et 3\* | Oui\* | Non | Non |
| Windows Server 2008 R2 Standard ou Foundation / installation Server Core | * Autorité de certification (CA)\* | Modèles de certificats versions 1, 2\*, et 3\* | Oui\* | Non | Non |
| Windows Server 2008 R2 Enterprise ou Datacenter | * Autorité de certification (CA) * Inscription de l’autorité de certification via le Web (CAWE) * Services Web d’enrôlement de certificats\* (CEP et CES) * Répondeur en ligne (OCSP) * Service d’inscription de périphériques réseau (NDES) | Modèles de certificats versions 1, 2, et 3 | Oui | Oui | Oui |
| Windows Server 2008 R2 Enterprise ou Datacenter / installation Server Core | * Autorité de certification (CA)\* | Modèles de certificats versions 1, 2, et 3 | Oui | Oui | Oui |
| Windows Server 2008 Standard Edition | * Autorité de certification (CA) * Inscription de l’autorité de certification via le Web (CAWE) | Modèles de certificats version 1 uniquement | Non | Non | Non |
| Windows Server 2008 Enterprise ou Datacenter Edition | * Autorité de certification (CA) * Inscription de l’autorité de certification via le Web (CAWE) * Répondeur en ligne (OCSP) * Service d’inscription de périphériques réseau (NDES) | Modèles de certificats versions 1, 2, et 3 | Oui | Oui | Non |
| Windows Server 2003 Standard Edition | * Autorité de certification (CA) * Inscription de l’autorité de certification via le Web (CAWE) | Modèles de certificats version 1 uniquement | Non | Non | Non |
| Windows Server 2003 Enterprise ou Datacenter Edition | * Autorité de certification (CA) * Inscription de l’autorité de certification via le Web (CAWE) * (NDES disponible en tant que « MSCEP » via le Kit de Ressources Techniques) | Modèles de certificats versions 1, et 2 | Oui | Oui | Non |

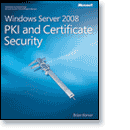
\*signifie que la fonction ou le support est nouveau dans Windows Server 2008 R2.

1. Pour des informations complémentaires

Pour des informations générales sur les services de certificats Active Directory (AD CS) de Windows Server 2008 (R2), vous pouvez consulter :

* le site Web Microsoft dédié à l’adresse <http://www.microsoft.com/pki>,
* ainsi que le Weblog Windows PKI associé à l’adresse <http://blogs.technet.com/pki>.

Nous conseillons également la lecture de l’ouvrage [Windows Server 2008 PKI and Certificate Security](http://www.microsoft.com/learning/en/us/book.aspx?ID=9549&locale=en-us)[[85]](#footnote-85) aux éditions Microsoft Press.



Pour des informations générales sur la solution Microsoft Forefront Identity Manager (FIM) 2010, vous pouvez consulter l’adresse <http://www.microsoft.com/forefront/en/us/identity-manager.aspx>.

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



1. Livre blanc Windows Server 2008 R2 Certificate Enrollment Web Services Whitepaper : http://download.microsoft.com/download/C/2/2/C229E624-36E4-4AD8-9D86-F564ED539A16/Windows%20Server%202008%20R2%20Certificate%20Enrollment%20Web%20Services.doc [↑](#footnote-ref-1)
2. Microsoft Business Ready Security : http://www.microsoft.com/forefront/en/us/business-ready-security.aspx [↑](#footnote-ref-2)
3. Article TechNet Magazine PKI Enhancements in Windows 7 and Windows Server 2008 R2 : http://technet.microsoft.com/en-us/magazine/2009.05.pki.aspx [↑](#footnote-ref-3)
4. Guide d’évaluation Windows Server Active Directory Certificate Services Step-by-Step Guide : http://go.microsoft.com/fwlink/?LinkID=85472 [↑](#footnote-ref-4)
5. Norme ISO/CEI 15408 Information technology -- Security techniques -- Evaluation criteria for IT security: http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=40612 [↑](#footnote-ref-5)
6. Critères Communs pour l’évaluation de la sécurité des Technologies de l’Information – partie 1 : Introduction et modèle générale : http://www.ssi.gouv.fr/site\_documents/CC/CCpart1v21-fr.pdf [↑](#footnote-ref-6)
7. Critères Communs pour l’évaluation de la sécurité des Technologies de l’Information – partie 1 Exigences fonctionnelles de sécurité : http://www.ssi.gouv.fr/site\_documents/CC/CCpart2v21-fr.pdf [↑](#footnote-ref-7)
8. Page NIAP Certification for Windows Server 2003 Certificate Server : http://www.niap-ccevs.org/cc-scheme/st/vid9507/ [↑](#footnote-ref-8)
9. Page NIAP Certification for Windows XP SP2 and Windows Server 2003 SP2 including R2 : http://www.niap-ccevs.org/cc-scheme/st/vid10184/ [↑](#footnote-ref-9)
10. Guide Windows Server 2003 SP2 R2 Common Criteria Configuration Guide 3.0 : http://www.microsoft.com/downloads/details.aspx?familyid=4F7B6A93-0307-480F-A5AF-A20268CBD7CC&displaylang=en [↑](#footnote-ref-10)
11. Guide Windows Server 2003 SP2 R2 Common Criteria Administrator Guide 3.0 : http://www.microsoft.com/downloads/details.aspx?familyid=4F7B6A93-0307-480F-A5AF-A20268CBD7CC&displaylang=en [↑](#footnote-ref-11)
12. Livre blanc Certificate Autoenrollment in Windows Server 2003 : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx [↑](#footnote-ref-12)
13. Authentification sélective : http://technet2.microsoft.com/WindowsServer/en/library/9266b197-7fc9-4bd8-8864-4c119ceecc001033.mspx [↑](#footnote-ref-13)
14. Livre blanc Cross-forest Certificate Enrollment with Windows Server 2008 R2 : http://go.microsoft.com/fwlink/?LinkId=139681 [↑](#footnote-ref-14)
15. Livre blanc Windows Server 2008 R2 Certificate Enrollment Web Services Whitepaper : http://download.microsoft.com/download/C/2/2/C229E624-36E4-4AD8-9D86-F564ED539A16/Windows%20Server%202008%20R2%20Certificate%20Enrollment%20Web%20Services.doc [↑](#footnote-ref-15)
16. Article 935441 Webcast: Credential Roaming Basics : http://support.microsoft.com/?id=935441 [↑](#footnote-ref-16)
17. Livre blanc Configuring and Troubleshooting Windows 2000 and Windows Server 2003 Certificate Services Web Enrollment : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/webenroll.mspx [↑](#footnote-ref-17)
18. Livre blanc Windows Server 2003 Advanced Certificate Enrollment and Management : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx [↑](#footnote-ref-18)
19. Page MSDN Certificate Services Architecture : http://msdn2.microsoft.com/en-us/library/Aa376540.aspx [↑](#footnote-ref-19)
20. Page TechNet Manage Certificate Revocation : http://technet2.microsoft.com/windowsserver/en/library/92a5e655-3eb2-4843-b9cb-58c84c0a91d61033.mspx [↑](#footnote-ref-20)
21. Livre blanc Certificate Autoenrollment in Windows Server 2003 : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx [↑](#footnote-ref-21)
22. Livre blanc Key Archival and Recovery in Windows Server 2008 : http://go.microsoft.com/fwlink/?LinkID=92523 [↑](#footnote-ref-22)
23. Livre blanc Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx [↑](#footnote-ref-23)
24. Livre blanc Certificate Autoenrollment in Windows Server 2003 : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx [↑](#footnote-ref-24)
25. Livre blanc Implementing and Administering Certificate Templates in Windows Server 2008 : http://go.microsoft.com/fwlink/?LinkID=92522 [↑](#footnote-ref-25)
26. Livre blanc Active Directory Certificate Server Enhancements in Windows Server 2008 : http://www.microsoft.com/downloads/details.aspx?FamilyID=9bf17231-d832-4ff9-8fb8-0539ba21ab95&DisplayLang=en [↑](#footnote-ref-26)
27. Billet Extended Validation support for websites using internal certificates: http://blogs.technet.com/askds/archive/2009/08/14/extended-validation-support-for-websites-using-internal-certificates.aspx [↑](#footnote-ref-27)
28. Document version 1.1 Guidelines for the issuance and management of extended validation certificates : http://cabforum.org/EV\_Certificate\_Guidelines\_V11.pdf [↑](#footnote-ref-28)
29. Livre blanc The Business Value of Extended Validation SSL Certificates : http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9948298f-1586-4cda-bee1-47b2ade78245 [↑](#footnote-ref-29)
30. Page TechNet Certificate Templates Overview : http://technet2.microsoft.com/windowsserver/en/library/e42693ef-374b-40a9-af3c-569f0d1fe1c91033.mspx [↑](#footnote-ref-30)
31. Livre blanc Implementing and Administering Certificate Templates in Windows Server 2008 : http://go.microsoft.com/fwlink/?LinkID=92522 [↑](#footnote-ref-31)
32. Article Object IDs associated with Microsoft cryptography : http://support.microsoft.com/?id=287547 [↑](#footnote-ref-32)
33. Article Object IDs associated with Microsoft cryptography : http://support.microsoft.com/?id=287547 [↑](#footnote-ref-33)
34. Livre blanc Certificate Revocation and Status Checking : http://go.microsoft.com/fwlink/?LinkID=27081 [↑](#footnote-ref-34)
35. Livre blanc Troubleshooting PKI Problems on Windows Vista : http://technet2.microsoft.com/WindowsVista/en/library/771e1f29-4eba-40c9-9193-60043889bbf41033.mspx [↑](#footnote-ref-35)
36. Livre blanc Installing, Configuring, and Troubleshooting the Microsoft Online Responder : http://technet2.microsoft.com/windowsserver2008/en/library/045d2a97-1bff-43bd-8dea-f2df7e270e1f1033.mspx [↑](#footnote-ref-36)
37. Article Adding Revocation Providers to CryptoAPI for Identrus Applications  : http://msdn2.microsoft.com/en-us/library/ms995348.aspx [↑](#footnote-ref-37)
38. Composant logiciel Fournisseur de révocation GIP-CPS pour les plateformes Microsoft Windows : http://www.microsoft.com/france/interop/gip-cps/default.aspx [↑](#footnote-ref-38)
39. Contrat de licence de logiciel libre CeCCIL-B : http://www.cecill.info/licences/Licence\_CeCILL-B\_V1-fr.html [↑](#footnote-ref-39)
40. Livre blanc Windows Vista Smart Card Infrastructure : http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en [↑](#footnote-ref-40)
41. Livre blanc Enterprise Smart Card Deployment in the Microsoft Windows Smart Card Framework : http://www.microsoft.com/downloads/details.aspx?FamilyID=fa7ec97c-11be-4e53-a0c4-04719b6a7ab6&DisplayLang=en [↑](#footnote-ref-41)
42. Livre blanc Active Directory Certificate Server Enhancements in Windows Server 2008 : http://www.microsoft.com/downloads/details.aspx?FamilyID=9bf17231-d832-4ff9-8fb8-0539ba21ab95&DisplayLang=en [↑](#footnote-ref-42)
43. Document Smart Card Minidriver Certification Requirements : http://www.microsoft.com/whdc/device/input/smartcard/sc-minidriver\_certreqs.mspx [↑](#footnote-ref-43)
44. Spécification v7.06 Windows Smart Card Minidriver Specification : http://www.microsoft.com/whdc/device/input/smartcard/sc-minidriver.mspx [↑](#footnote-ref-44)
45. Document Introduction to the Windows Biometric Framework (WBF) : http://www.microsoft.com/whdc/device/input/smartcard/WBFIntro.mspx [↑](#footnote-ref-45)
46. Livre blanc [Installing a Suite B only PKI](http://go.microsoft.com/fwlink/?LinkId=148802) : http://go.microsoft.com/fwlink/?LinkId=148802 [↑](#footnote-ref-46)
47. Livre blanc Windows Vista Smart Card Infrastructure : http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en [↑](#footnote-ref-47)
48. Document Certificate Issuing and Management Components Family of Protection Profiles : http://www.commoncriteriaportal.org/files/ppfiles/PP\_CIMCPP\_SL1-4\_V1.0.pdf [↑](#footnote-ref-48)
49. Livre blanc Windows Server 2003 PKI Operations Guide : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspx [↑](#footnote-ref-49)
50. Page MSDN Certificate Services Architecture : http://msdn2.microsoft.com/en-us/library/Aa376540.aspx [↑](#footnote-ref-50)
51. Livre blanc Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx [↑](#footnote-ref-51)
52. Livre blanc Designing a Public Key Infrastructure : http://technet2.microsoft.com/windowsserver/en/library/b1ee9920-d7ef-4ce5-b63c-3661c72e0f0b1033.mspx?mfr=true [↑](#footnote-ref-52)
53. Livre blanc Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003 : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx [↑](#footnote-ref-53)
54. Livre blanc Active Directory Certificate Server Enhancements in Windows Server 2008 : http://www.microsoft.com/downloads/details.aspx?FamilyID=9bf17231-d832-4ff9-8fb8-0539ba21ab95&DisplayLang=en [↑](#footnote-ref-54)
55. Livre blanc [Installing a Suite B only PKI](http://go.microsoft.com/fwlink/?LinkId=148802) : http://go.microsoft.com/fwlink/?LinkId=148802 [↑](#footnote-ref-55)
56. Livre blanc Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003 : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx [↑](#footnote-ref-56)
57. Cryptographic Service Provider Developer's Toolkit (CSPDK) : http://www.microsoft.com/downloads/details.aspx?familyid=0F436C75-2304-42BB-B81A-BA0C2C47BAC2&displaylang=en [↑](#footnote-ref-57)
58. CSP Test Suite for testing CSPs: http://www.microsoft.com/downloads/details.aspx?FamilyID=5f3872f8-202e-4f13-b495-78ce6f17a84f&DisplayLang=en [↑](#footnote-ref-58)
59. Livre blanc Introduction à l’architecture de services Web et ses spécifications WS-\* : http://www.microsoft.com/france/msdn/architects/intro-WS.mspx [↑](#footnote-ref-59)
60. Livre blanc Microsoft SCEP Implementation : http://www.microsoft.com/downloads/details.aspx?FamilyID=e11780de-819f-40d7-8b8e-10845bc8d446&DisplayLang=en [↑](#footnote-ref-60)
61. Livre blanc Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx [↑](#footnote-ref-61)
62. Livre blanc Installing, Configuring, and Troubleshooting the Microsoft Online Responder  : http://technet2.microsoft.com/windowsserver2008/en/library/045d2a97-1bff-43bd-8dea-f2df7e270e1f1033.mspx [↑](#footnote-ref-62)
63. Livre blanc Troubleshooting PKI Problems on Windows Vista : http://technet2.microsoft.com/WindowsVista/en/library/771e1f29-4eba-40c9-9193-60043889bbf41033.mspx [↑](#footnote-ref-63)
64. Livre blanc Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx [↑](#footnote-ref-64)
65. billet Automated CA installs using VB script on Windows Server 2008 and 2008 R2 : http://blogs.technet.com/pki/archive/2009/09/18/automated-ca-installs-using-vb-script-on-windows-server-2008-and-2008r2.aspx [↑](#footnote-ref-65)
66. Billet Using VBScript to install CA on server core : http://blogs.technet.com/pki/archive/2009/09/18/using-vbscript-to-install-ca-on-server-core.aspx [↑](#footnote-ref-66)
67. Guide Windows Server 2003 Certificate Server Common Criteria Configuration Guide : http://download.microsoft.com/download/f/2/0/f206c1fe-b176-4910-a812-68767867ee01/WS03CertServer\_Common\_Criteria\_Configuration\_Guide.zip [↑](#footnote-ref-67)
68. Document Hyper-V Planning and Deployment Guide : http://www.microsoft.com/downloads/details.aspx?familyid=5DA4058E-72CC-4B8D-BBB1-5E16A136EF42&displaylang=en [↑](#footnote-ref-68)
69. Livre blanc Overview of Failover Clustering with Windows Server 2008 : http://download.microsoft.com/download/3/B/5/3B51A025-7522-4686-AA16-8AE2E536034D/Windows%20Server%202008%20Failover%20Clustering%20Architecture%20Overview.doc [↑](#footnote-ref-69)
70. Livre blanc Certification Authority Clustering Configuration and Troubleshooting Guide : http://go.microsoft.com/fwlink/?LinkId=118364 [↑](#footnote-ref-70)
71. Billet To Cluster or Not to Cluster CAs : http://blogs.technet.com/wincat/archive/2008/07/21/to-cluster-or-not-to-cluster-cas.aspx [↑](#footnote-ref-71)
72. Page TechNet Evaluating CA Capacity, Performance, and Scalability : http://technet2.microsoft.com/windowsserver/en/library/61b3334a-eb6d-4d7d-b122-ca0c6ab18f5f1033.mspx [↑](#footnote-ref-72)
73. Billet Scale testing the world’s largest PKI… all running on WS08R2 and Hyper-V : http://blogs.technet.com/wincat/archive/2009/08/10/scale-testing-the-world-s-largest-pki-all-running-on-ws08r2-and-hyper-v.aspx [↑](#footnote-ref-73)
74. Page TechNet Evaluating CA Capacity, Performance, and Scalability : http://technet2.microsoft.com/windowsserver/en/library/61b3334a-eb6d-4d7d-b122-ca0c6ab18f5f1033.mspx [↑](#footnote-ref-74)
75. Article 231182 Certificate Authority Servers Cannot Be Renamed or Removed from Network : http://support.microsoft.com/?id=231182 [↑](#footnote-ref-75)
76. Page MSDN Certificate Enrollment API : http://msdn2.microsoft.com/en-us/library/aa374863.aspx [↑](#footnote-ref-76)
77. Page MSDN Certificate Services Architecture : http://msdn2.microsoft.com/en-us/library/Aa376540.aspx [↑](#footnote-ref-77)
78. Weblog My Nuggets : http://blogs.technet.com/vishalagarwal/ [↑](#footnote-ref-78)
79. ScriptCenter TechNet : http://technet.microsoft.com/fr-fr/scriptcenter/dd742419(en-us).aspx [↑](#footnote-ref-79)
80. Guide Windows PowerShell Owner Manual : http://www.microsoft.com/technet/scriptcenter/topics/winpsh/manual/default.mspx [↑](#footnote-ref-80)
81. Site TechNet Windows PowerShell : http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx [↑](#footnote-ref-81)
82. Weblog Windows PowerShell : http://blogs.msdn.com/powershell/default.aspx [↑](#footnote-ref-82)
83. Programme Windows Server Protocols (WSPP) : http://msdn.microsoft.com/en-us/library/cc964399.aspx [↑](#footnote-ref-83)
84. Open Specification Promise : http://www.microsoft.com/france/interop/osp/default.mspx [↑](#footnote-ref-84)
85. Ouvrage Windows Server 2008 PKI and Certificate Security : http://www.microsoft.com/learning/en/us/book.aspx?ID=9549&locale=en-us [↑](#footnote-ref-85)