ADRMS : Active Directory Right Management Services

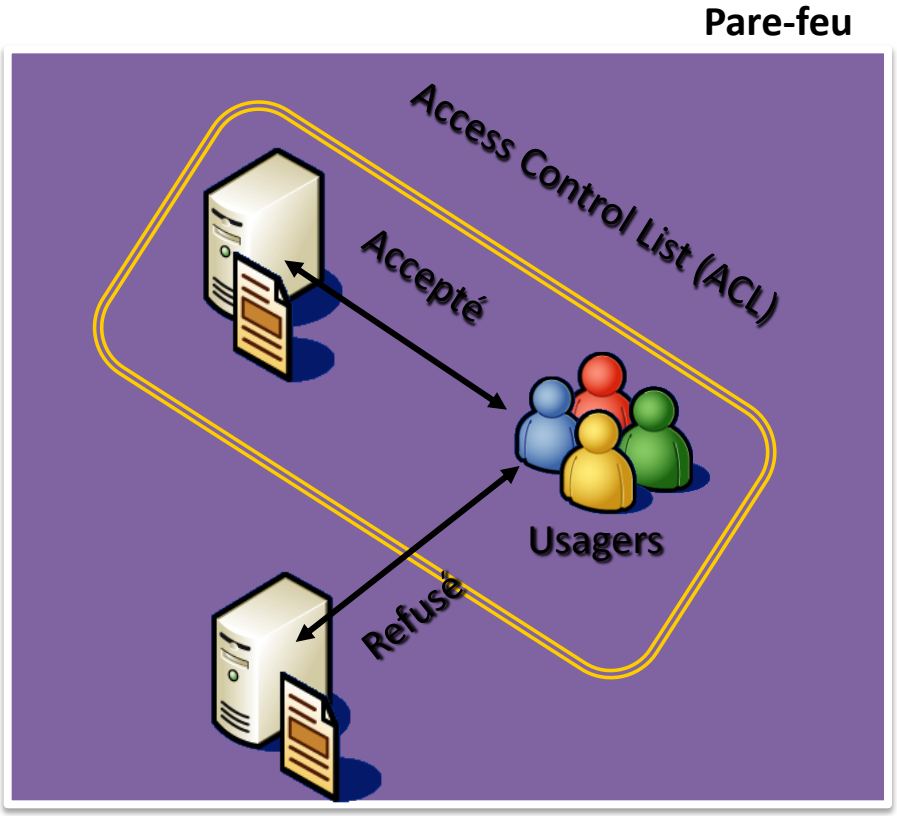
Introduction

Organisation de l'exposé

- ADRMS dans les grandes lignes
- Installation et configuration
- Fonctionnement d'ADRMS
- Limitations et concurrence

Contrôle d'accès classique

- Protection à base de périmètre de contrôle d'accès, et non lié à l'usage



Un utilisateur qui a accès à un partage peut copier, modifier et rediffuser des informations

➢ **Les ACLs ne restreignent pas ce que l'utilisateur peut faire avec un document**

Conséquences

Des information sensibles (documents, e-mails, contenu intranet, etc.) peuvent être divulguées accidentellement ou intentionnellement

Exemple, l'affaire Valéo :

En avril 2005, une étudiante chinoise stagiaire dans l'entreprise Valeo, équipementier automobile français, est soupçonnée d'avoir copié des données de l'entreprise sur un disque dur personnel.

Il lui est reproché l'accès frauduleux dans un système automatisé de données et abus de confiance. Selon la presse, au moment des faits la stagiaire aurait sorti des données de l'entreprise pour les emmener chez elle. Elle justifie son geste en affirmant avoir copié des données pour son rapport de stage.

Conséquences

Ces manques de sécurités peuvent avoir de lourdes conséquences:

- ☹ Perte de revenus
- ☹ Perte d'avantages concurrentiels
- ☹ Perte de la confiance de ses clients
- ☹ Problèmes diplomatiques

« Le vol d'informations propriétaires est la plus grande source de dommages financiers parmi tous les incidents de sécurité »

CSI/FBI Computer Crime and Security Survey, 2001

Les besoins

- Protection permanente des informations sensibles
- Facilement utilisable
- Souple, facilement déployable, et extensible
- Technologie qui aille au-delà du contrôle d'accès et du chiffrement
- Contrôle de l'utilisation des documents

THE solution

☺ **Technologie d'infrastructure destinée aux environnements d'entreprise pour la protection des documents et e-mails**

☺ **Permet non seulement le contrôle d'accès à l'information, mais surtout le contrôle de *l'usage* qui en est fait**

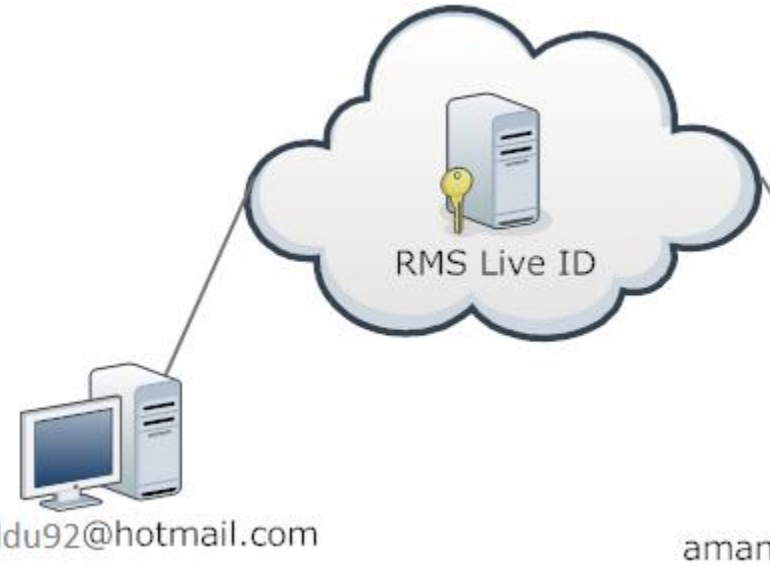
Ce que permet ADRMS

Utilisation	Application	Caractéristiques
Protéger des fichiers confidentiels	Microsoft Office: • Word • Excel® • PowerPoint	• Droits sur le document • Assigner une période de validité
Interdire : Impression de l'email Suivre le message	• Microsoft Office Outlook®: • Microsoft Exchange Server 2007 Service Pack 1 (SP1)	• Aide à prévenir l'envoi d'emails sensibles à l'exterieur de l'entreprise
Protéger le contenu de l'intranet	• Microsoft Office • SharePoint Services	• limite l'accès à la visualisation la modification et l'impression

Petit historique de la technologie

- Une première version en 2003 appelée IRM/RMS
- Logiciel externe fourni gratuitement par Microsoft
- Logiciel peu connu car pas de publicité autour

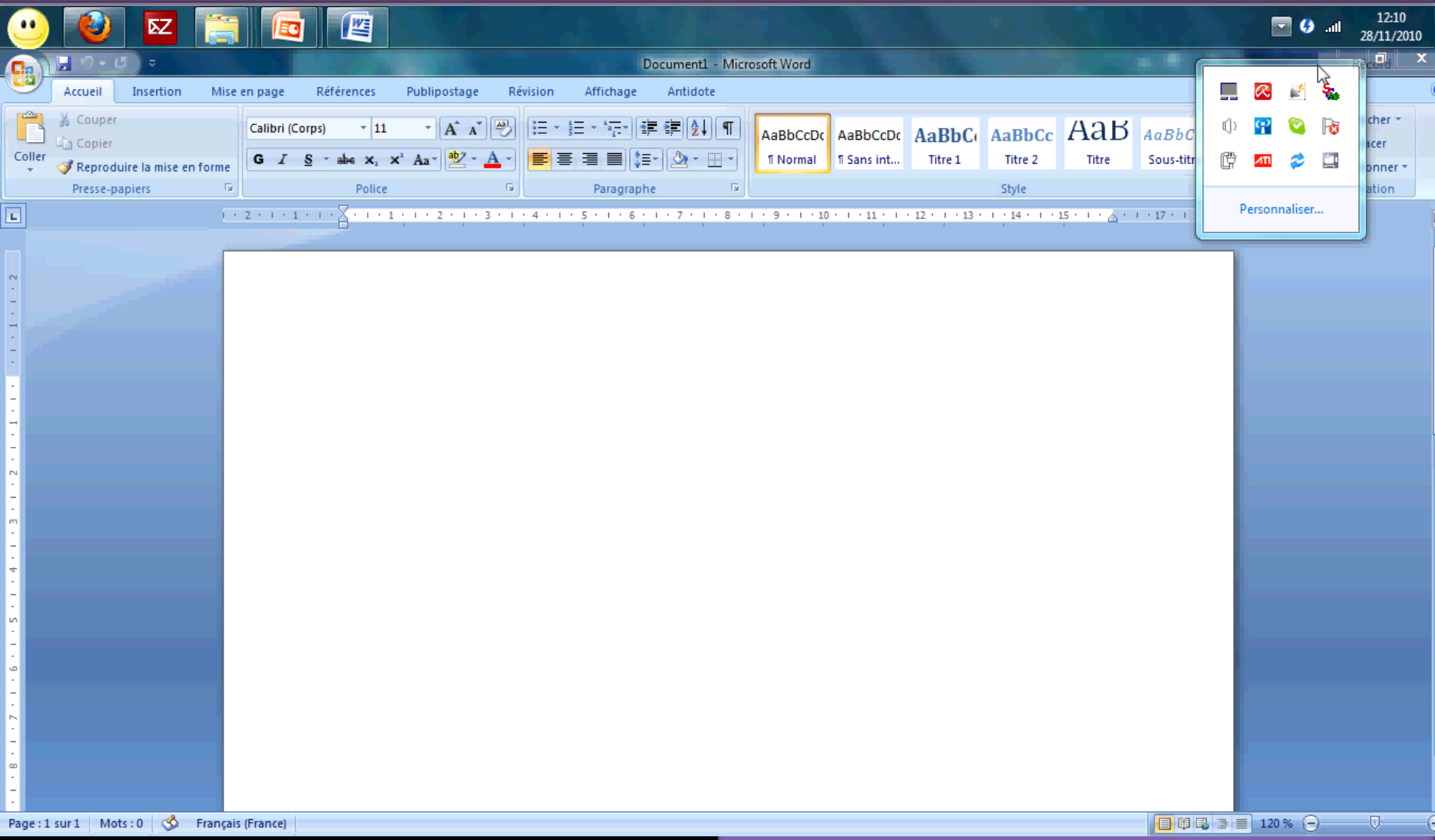
Scénario 1 : Utilisation par un particulier



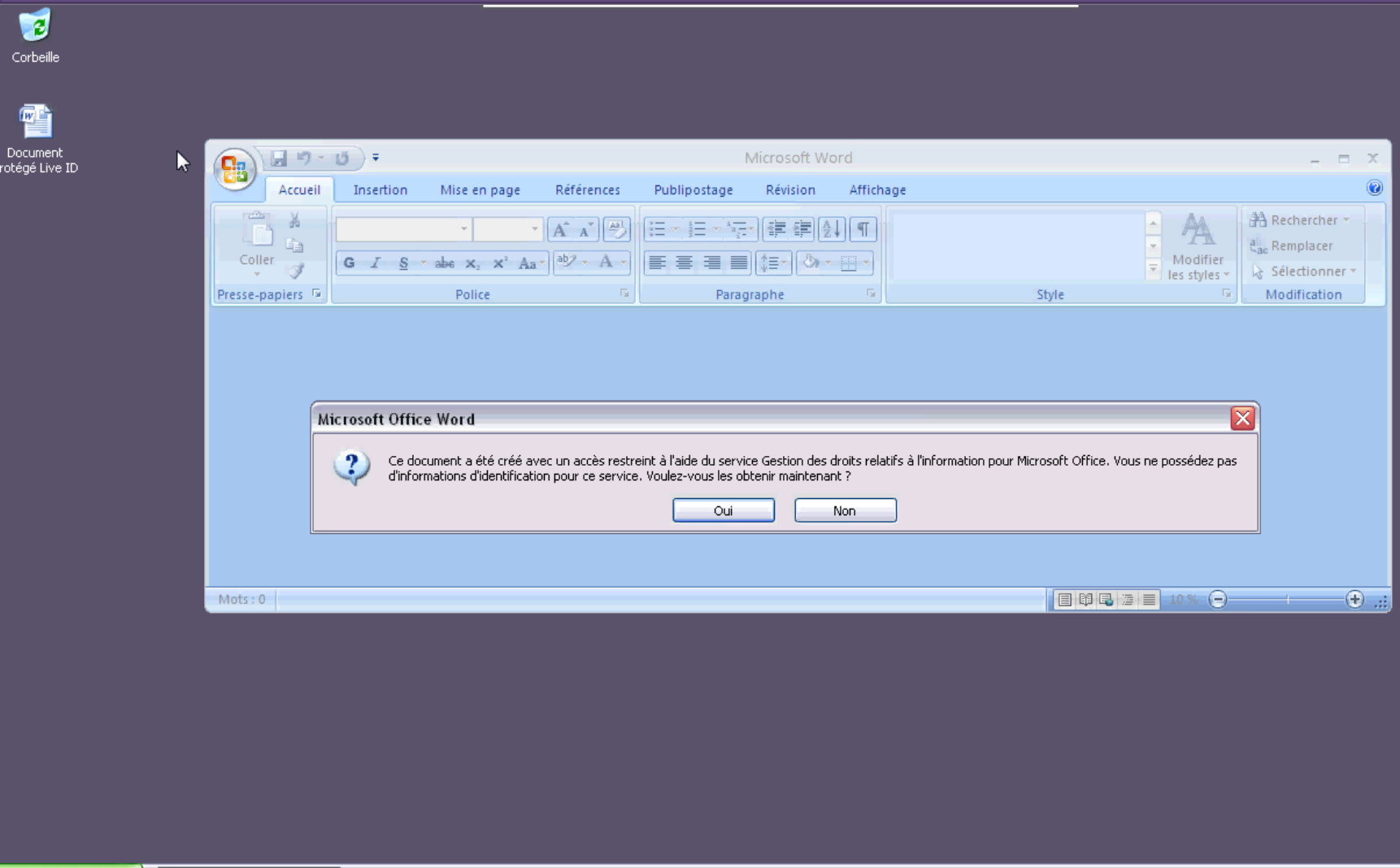
Nécessite :

- Un identifiant live ID
- Une application cliente RMS Enabled (Microsoft Office)
- Un connexion internet

II ► Utilisation par un particulier : Protection



Utilisation par un particulier : Ouverture



Prérequis matériel

Minimum requis	Recommandé
✓Un Pentium 4	✓Deux Pentium 4
✓512 Mo RAM	✓1024 Mo RAM
✓40 Go d'espace disque	✓80 Go d'espace disque

Prérequis systèmes et logiciels

Serveur membre du domaine Active Directory

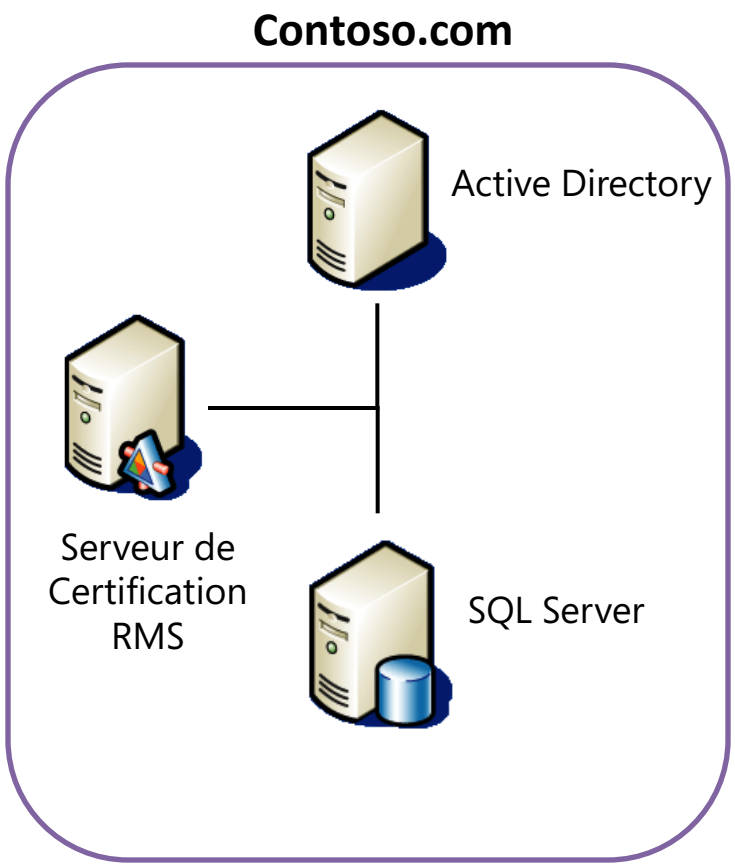
- Windows Server 2008
- IIS 6.0, ASP.NET et MSMQ installés

Active Directory

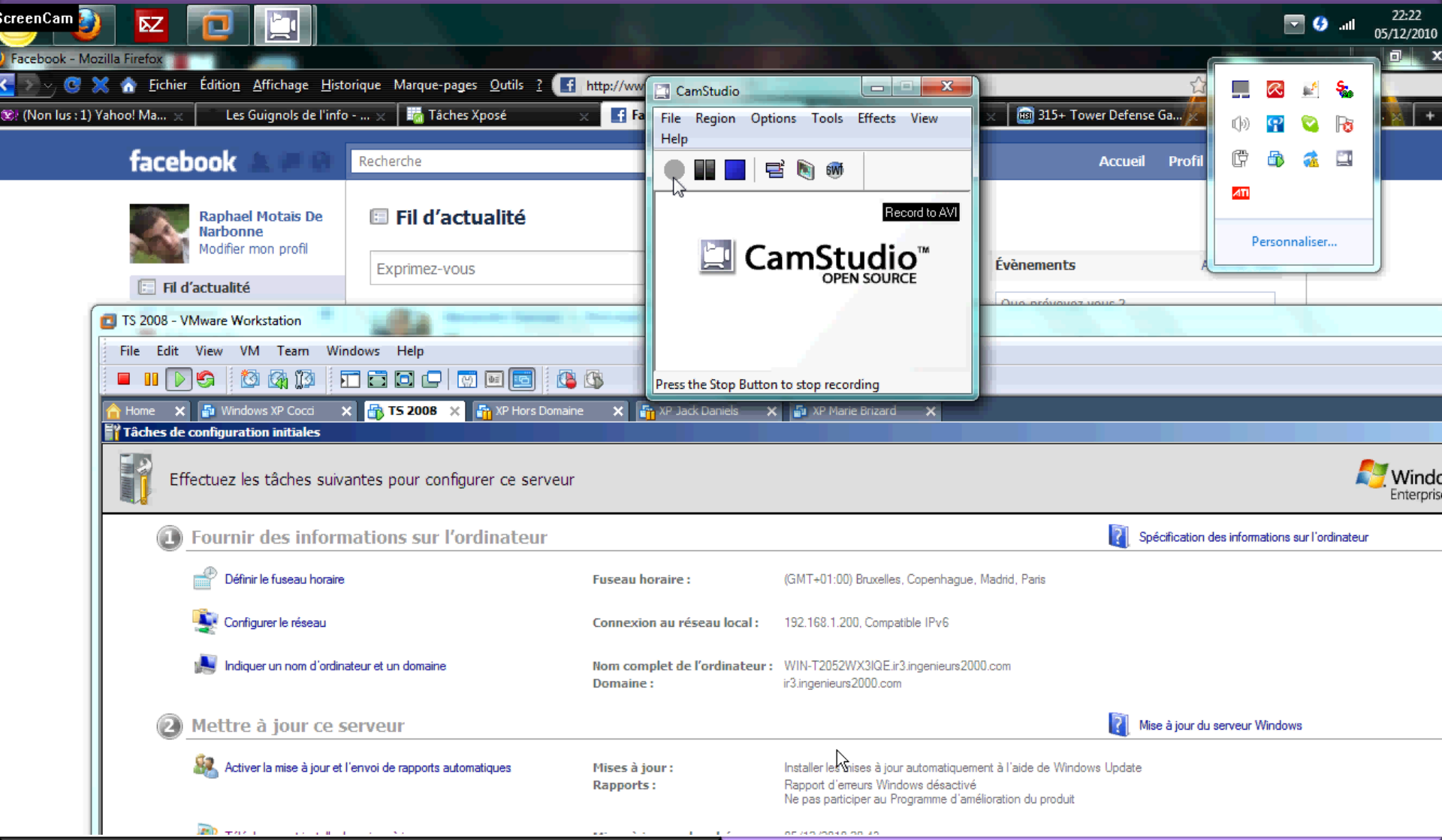
- Windows Server 2000 SP3 au Minimum
- Utilisé pour l'authentification, l'expansion de groupes et la localisation de services (SCP)

Serveur de base de données

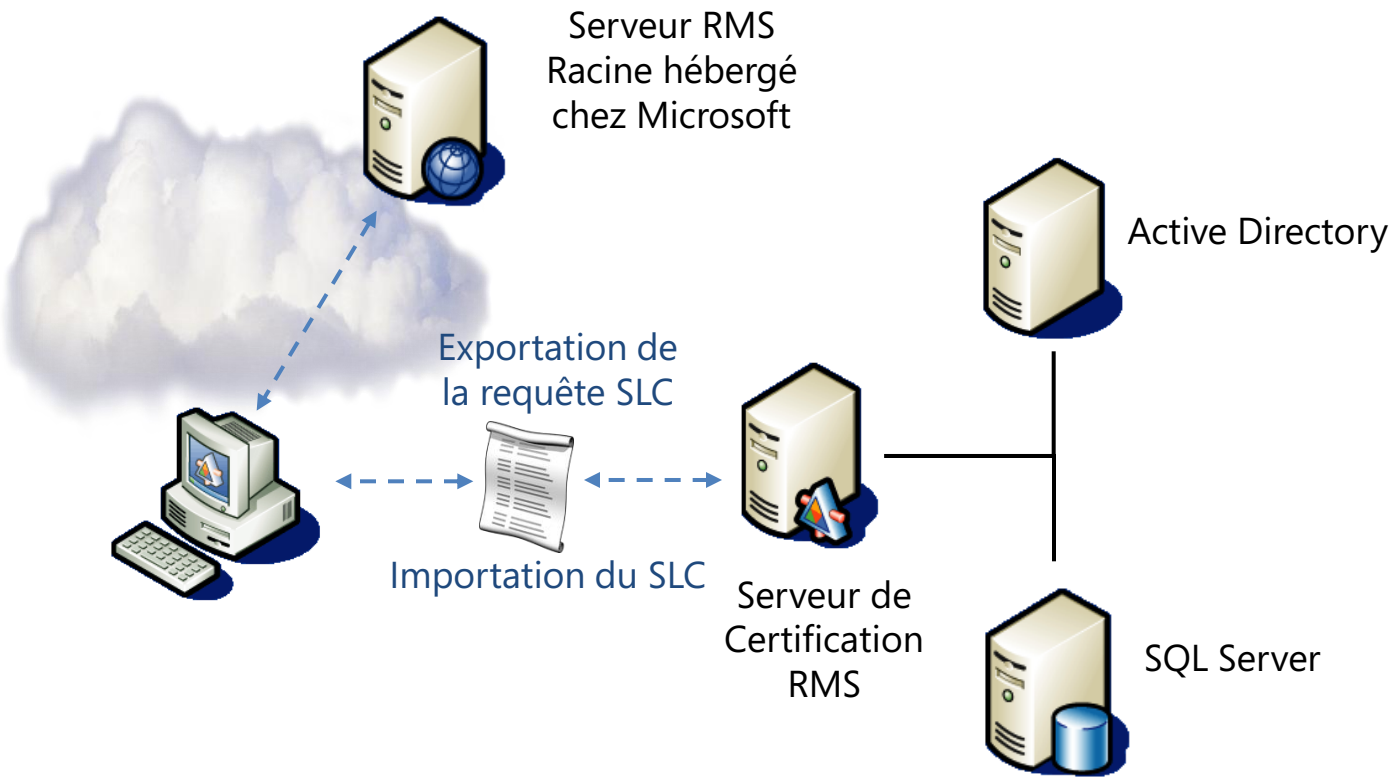
- SQL Server 2005 ou équivalent
- Utilisé pour le stockage de la configuration, les données de certification et de journalisation



Installation de l'infrastructure

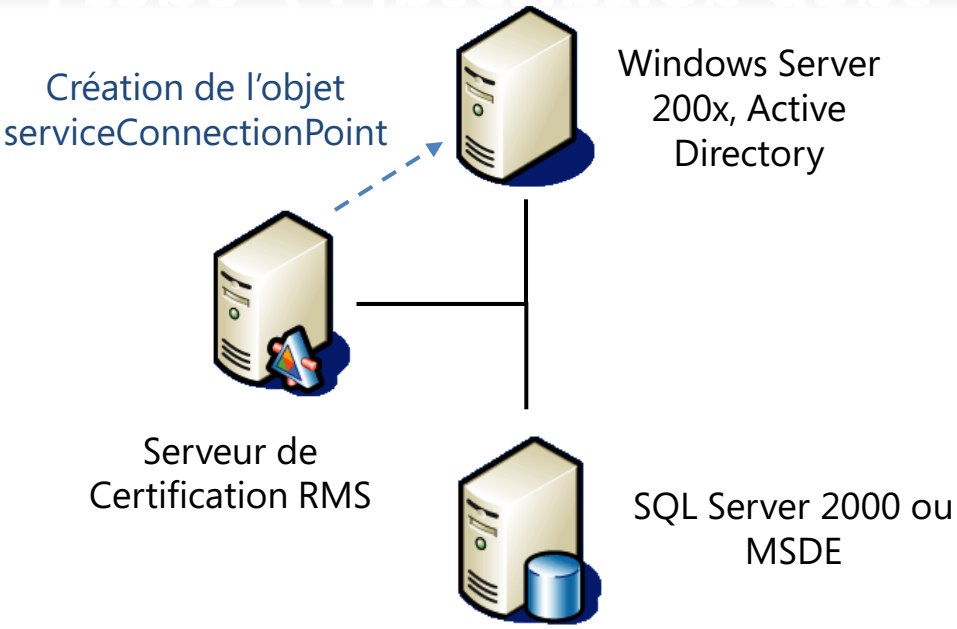


Etape 2 : Enrôlement du serveur



SLC = Server Licensor Certificate

Etape 3 : Inscription dans l'AD



Un objet ***serviceConnectionPoint*** avec l'URL du Serveur de Certification RMS est écrit dans AD

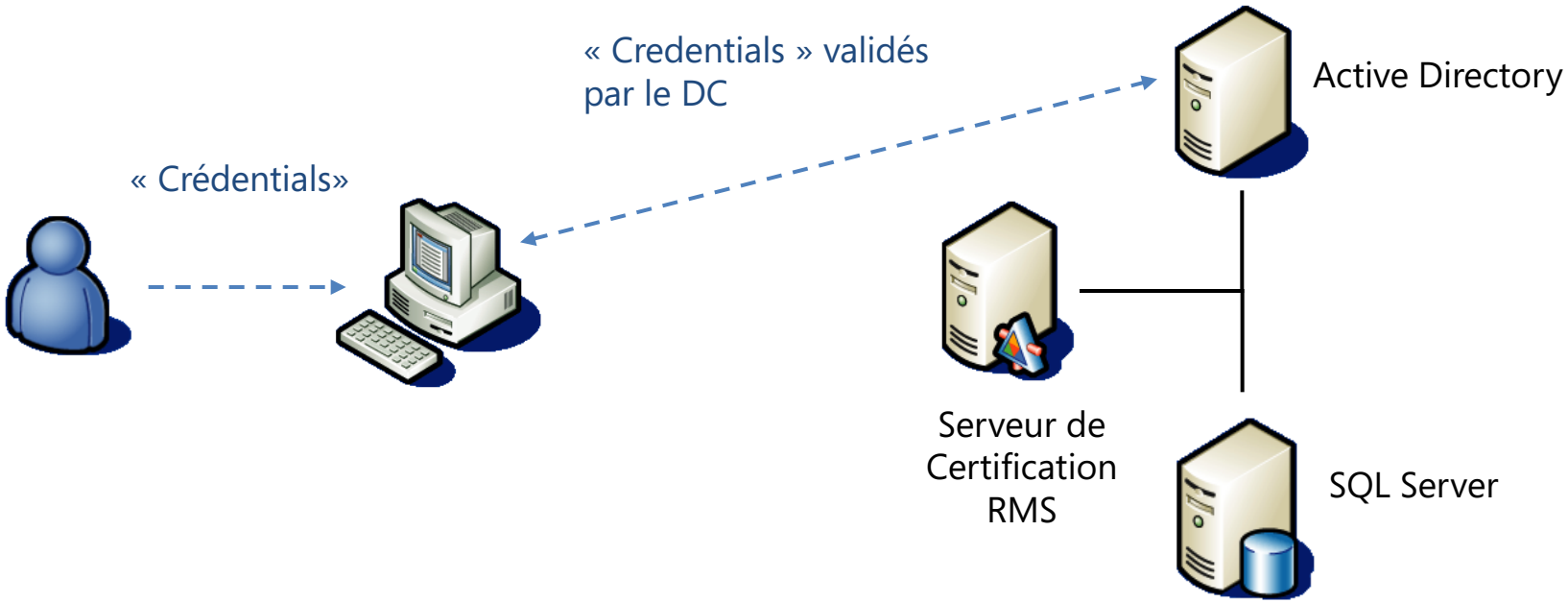
CN=SCP,CN=RightManagementServices,CN=Services,CN=Configuration,DC=<forest>,DC=com

Principes de fonctionnement

1) Définition d'entités de confiance (participants)
2) Assignation des droits à l'information
3) Protection de l'information et des droits associés
4) Distribution de l'information
5) Consommation du contenu à l'information

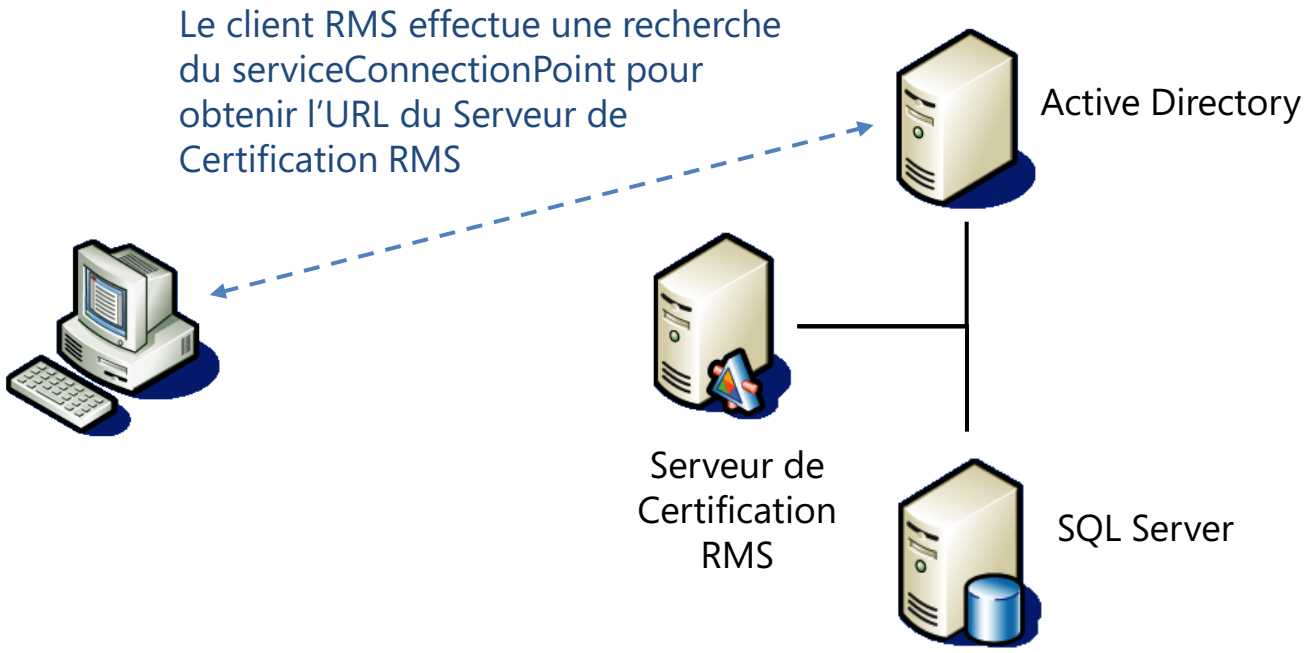
Publication de l'information

Étape 0 - L'utilisateur ouvre une session sur le domaine



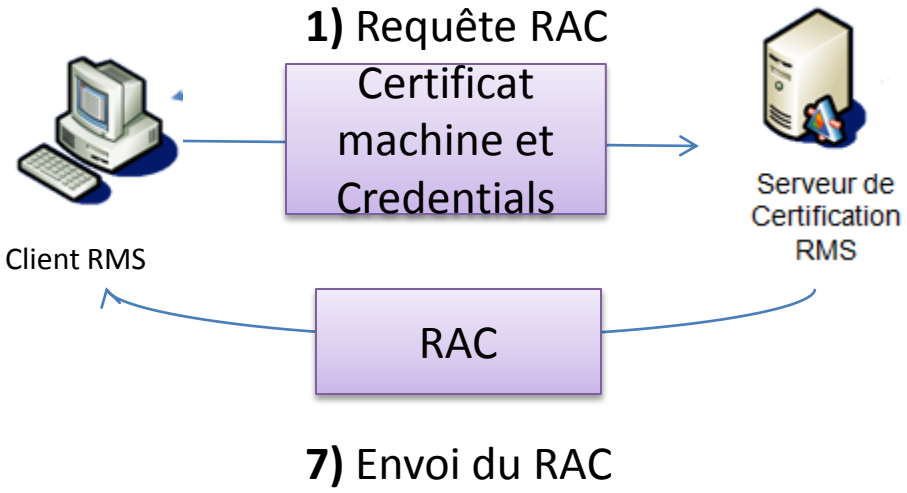
Publication de l'information

Étape 1 – Recherche du serveur RMS



Publication de l'information

Étape 2 – Obtention du *Rights Management Account Certificate* (RAC)



2) Le DC vérifie les crédentials
Le serveur RMS recherche une paire de clés existante

3) Sinon création d'une paire de clés RSA 1024 et enregistrement dans la base SQL

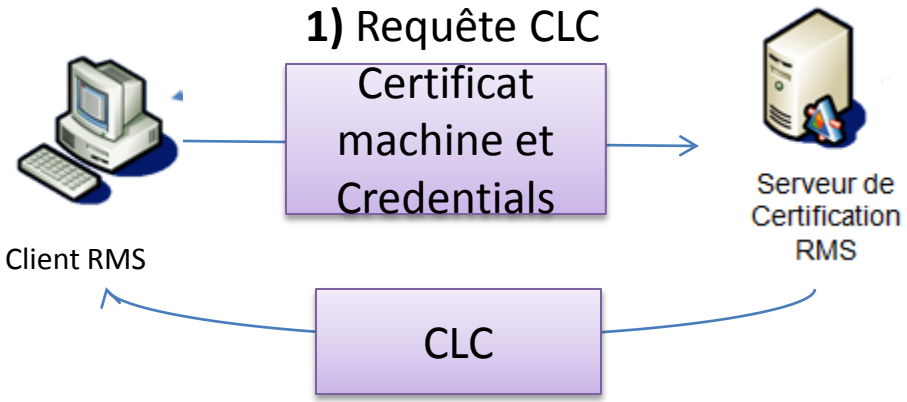
4) Chiffrement de la clé privée avec le Cert Machine et placement dans le RAC

5) Placement de la clé publique dans le RAC

6) Signature du RAC avec la clé privée du Serveur de Certification RMS

Publication de l'information

Étape 3 – Obtention du *Client Licensor Certificate* (CLC) si le client ne l'a pas



2) Le DC vérifie les crédentials

3) Les serveur RMS crée une paire de clés RSA 1024 différente de celle du RAC

4) Chiffrement de la clé privée avec le RAC et placement dans le CLC

5) Placement dans le CLC de :
- La clé publique
- La clé publique du serveur RMS
- L'URL du serveur RMS

6) Signature de la CLC en tant que clé de *Licensing* subordonnée

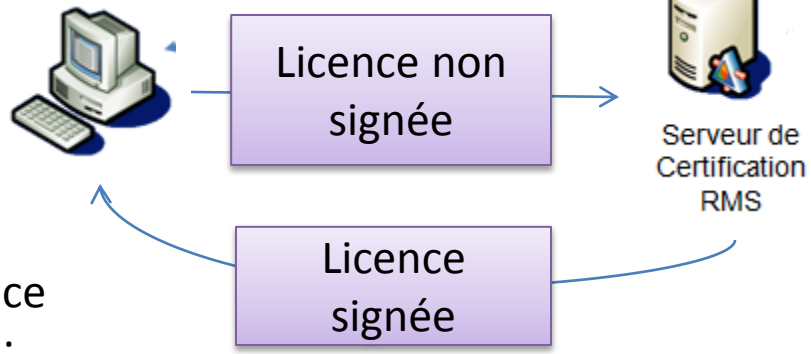
Publication de l'information

Étape 4 – Publication du contenu

1) Génération d'une clé de contenu symétrique (AES 128-bit)

2) Chiffrement du contenu

3) Préparation d'une Licence de Publication non signée :
- Acquisition du SLC
- Chiffrement des droits avec la clé de contenu
- Chiffrement de la clé de contenu avec le SLC



4) Envoi de la licence de publication non signée

5) Ajoute son URL

6) Signe la licence avec sa clé privée

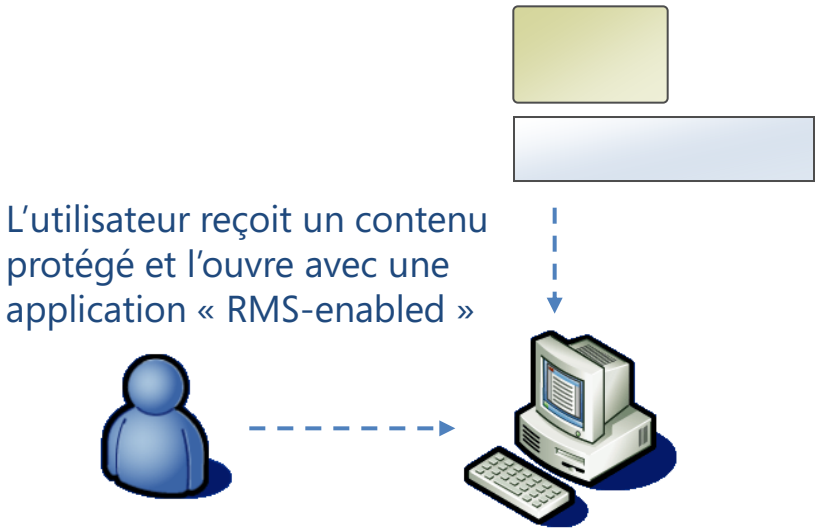
7) Envoi de la licence signée

8) Ajout par le client de la Licence de Publication au document

Consommation de l'information

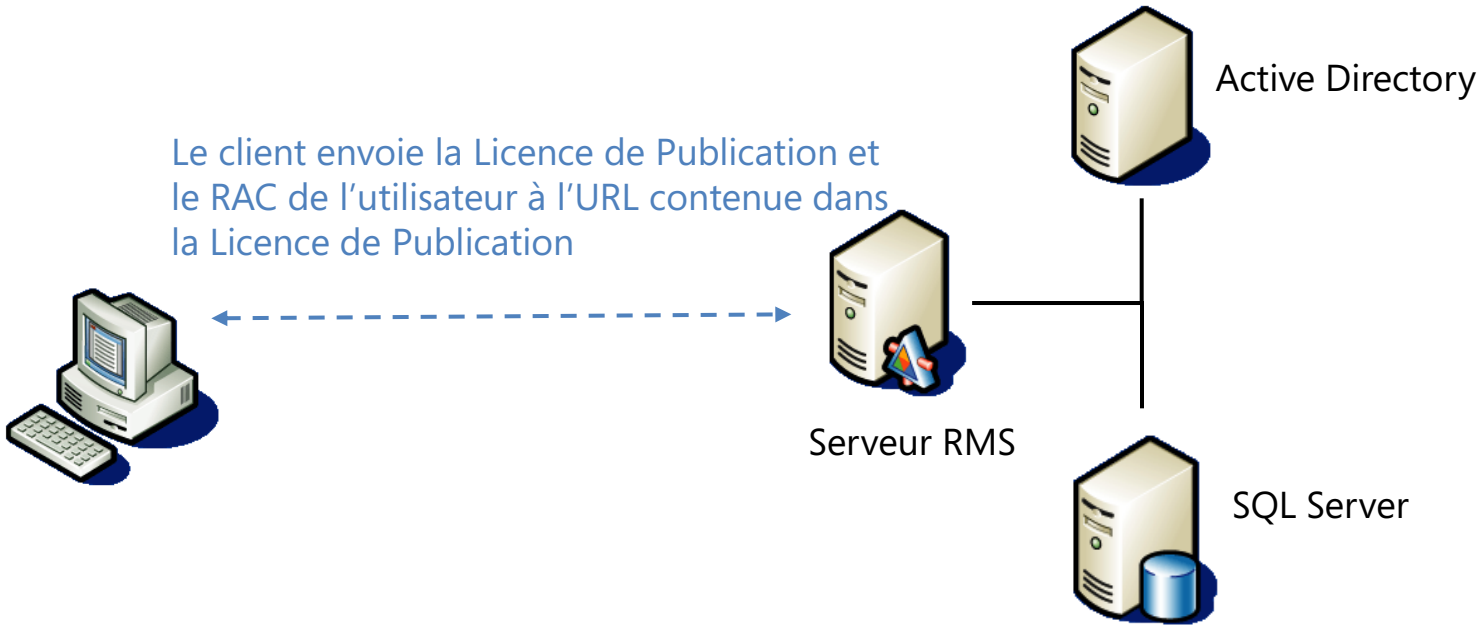
Étape 1 - L'utilisateur reçoit un contenu protégé en droits et l'ouvre à l'aide d'une application « RMS-enabled »

Si la machine n'est pas activée ou si l'utilisateur ne dispose pas d'un RAC, le client active alors la machine et va chercher un RAC



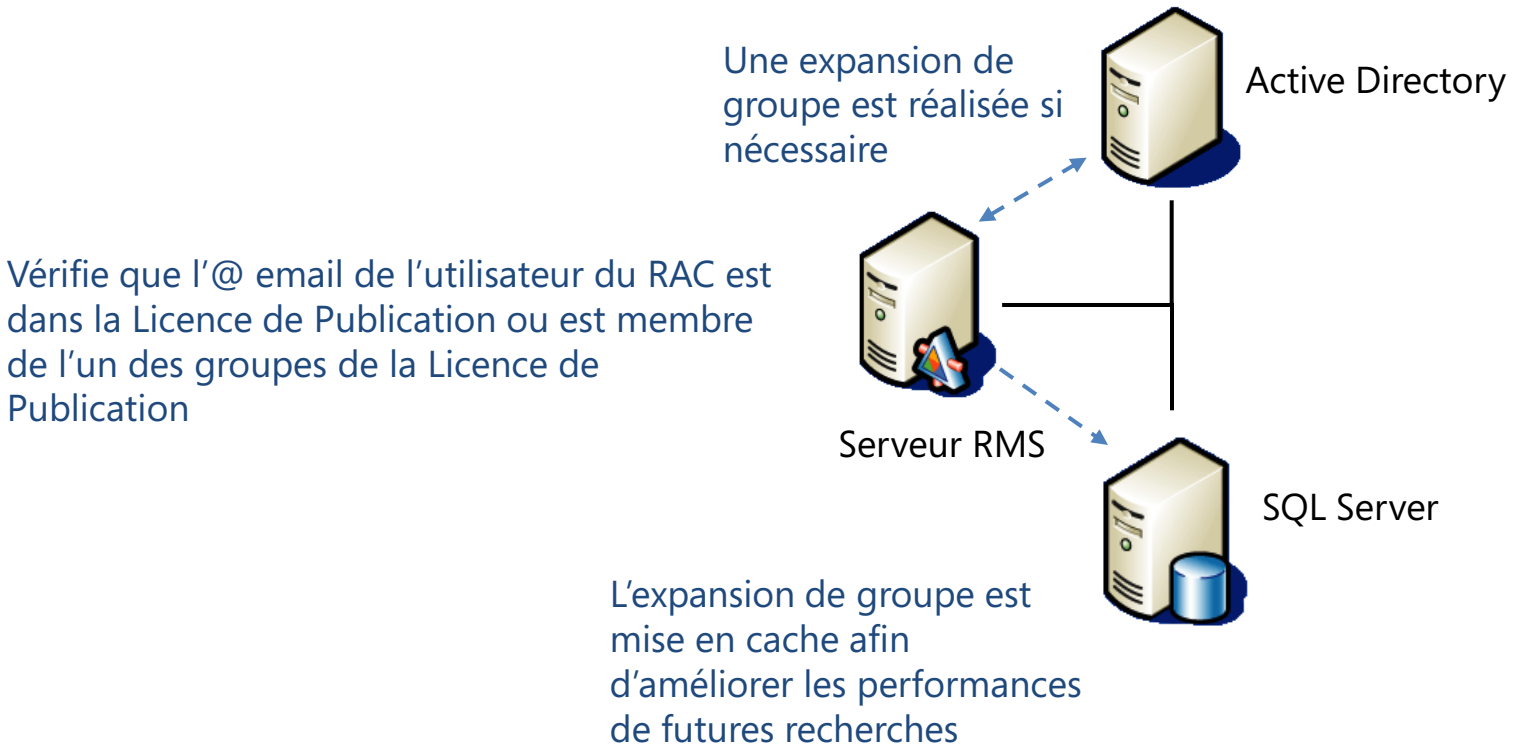
Consommation de l'information

Étape 2 - Le Client RMS extrait la Licence de Publication et l'envoie ainsi que le RAC de l'utilisateur au serveur RMS identifié par l'URL dans la Licence de Publication



Consommation de l'information

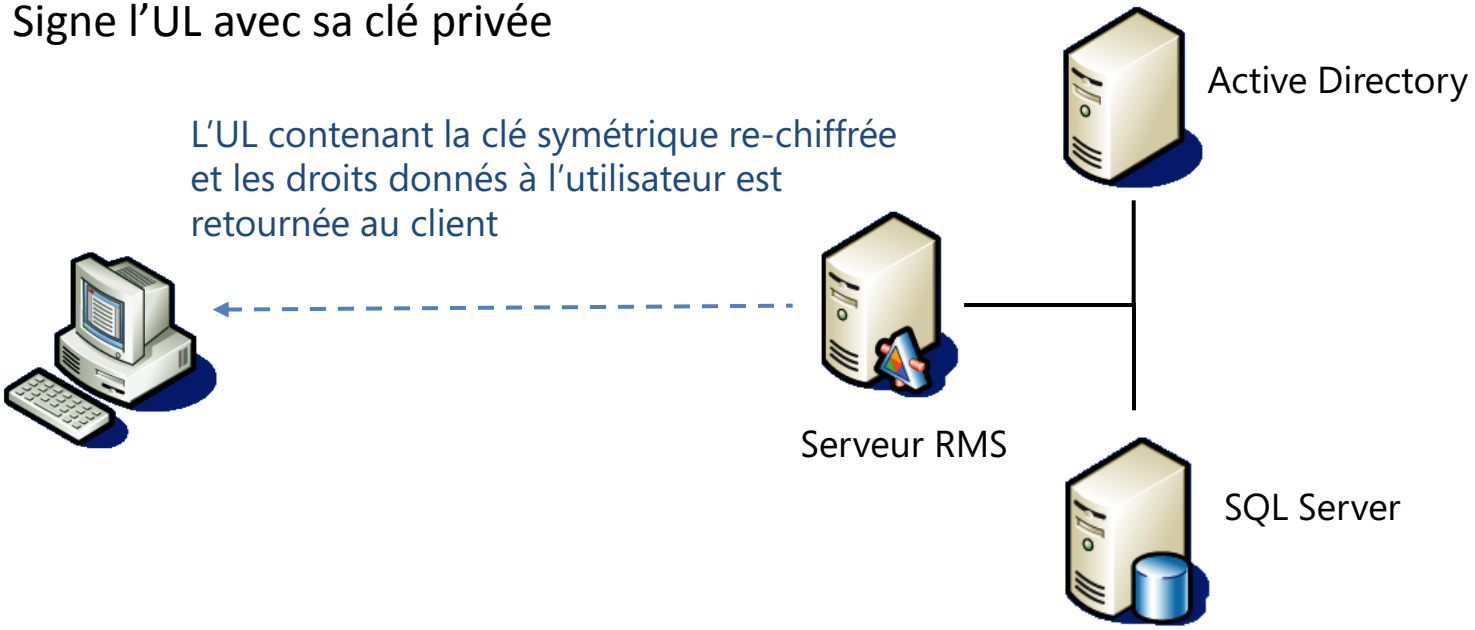
Étape 3 - Le Serveur RMS valide le RAC et vérifie que l'utilisateur possède un accès au contenu



Consommation de l'information

Étape 4 – Le Serveur RMS crée une Licence d'Utilisation (*Use License* ou UL)

1) Extrait la clé de contenu de la Licence de Publication et la déchiffre avec sa clé privée
2) Extrait la clé publique de l'utilisateur de son RAC
3) Chiffre la clé de contenu et les droits donnés à l'utilisateur avec le RAC
4) Signe l'UL avec sa clé privée



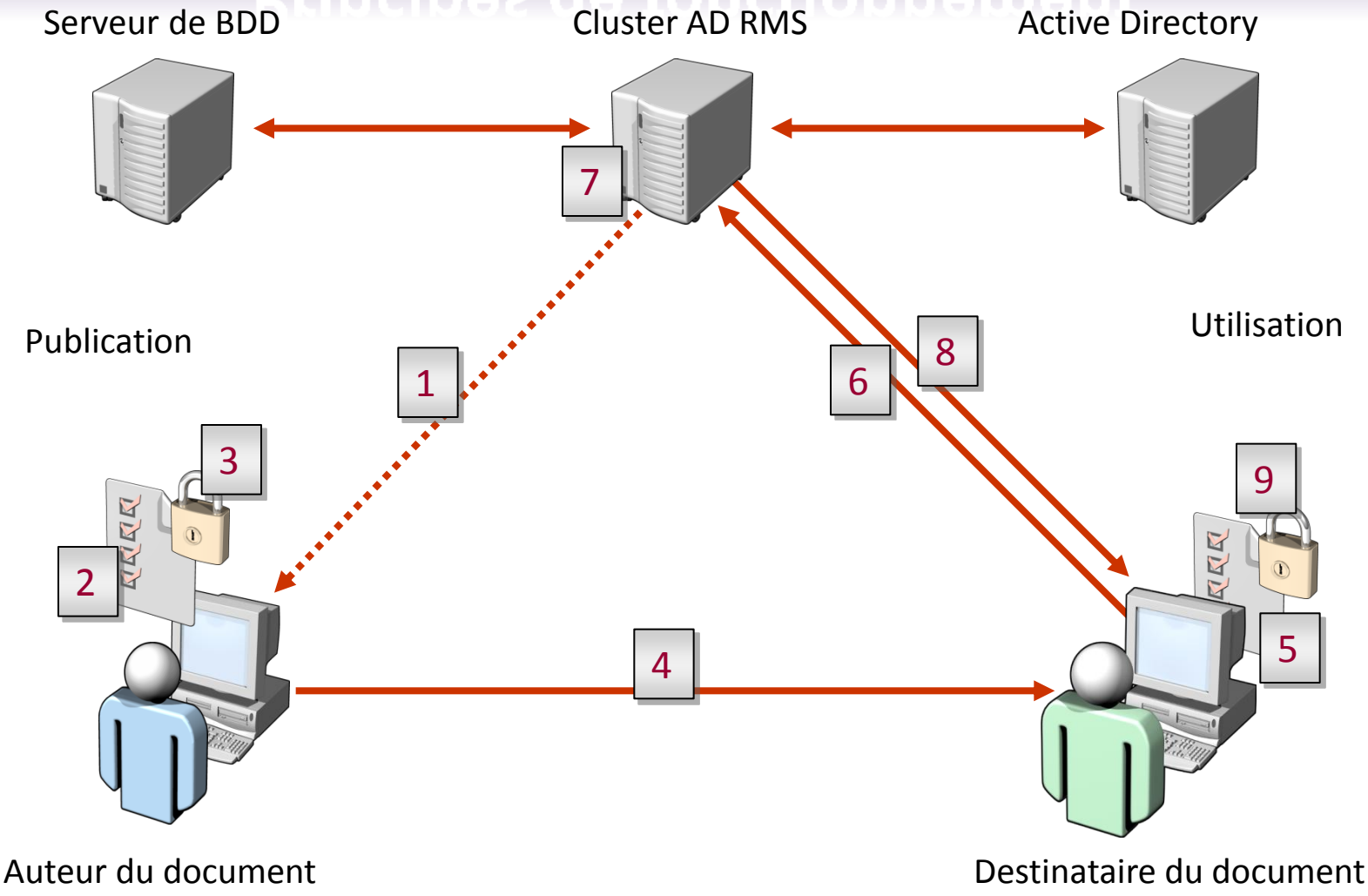
Consommation de l'information

Étape 5 - Le Client RMS retourne l'UL à l'application « RMS-enabled »

- La « lockbox » déchiffre la clé privée de l'utilisateur (RAC) avec la clé privée de la machine
- La « lockbox » déchiffre la clé de contenu avec la clé privée de l'utilisateur
- Déchiffrement du contenu et des droits avec la clé de contenu

La « Lockbox contient :
- Les algorithmes de chiffrement RSA, DES et AES 128
- La logique nécessaire à la génération, stockage et signature numérique des credentials machine

Principes de fonctionnement



Les limitations de cette technologie

Les limitations de cette technologie

Logiciels	Fonctionnement
	
	
	
	

Les limitations de cette technologie

Technologie qui nécessite des serveurs sauvegardés régulièrement et en cluster :

- Si les serveurs plantent, l'accès aux documents n'est pas garanti

Les concurrents

- Adobe LiveCycle Rights Management ES

Conclusion

- Une technologie sûre qui a des bases solides
- Une solution d'avenir

Sources

- **Microsoft Official Course :** Configuring Active Directory® Rights Management Services

- **Presentation de Philippe Beraud, Microsoft France :** Gestion de droits numériques en entreprise avec RMS SP1

- **Portail de la sécurité de l'information :** http://www.cases.public.lu/fr/risques

- **Microsoft TechNet :** http://technet.microsoft.com/en-us/library/cc771234%28WS.10%29.aspx

- **Blogs TechNet :**
  - http://blogs.technet.com/b/amolrb/
  - http://blogs.technet.com/b/manjesh/
  - http://blogs.technet.com/b/omers/


THANK YOU

Feature	AD RMS	S/MIME Signing	S/MIME Encryption	ACLs	EFS
Attests to the identity of the publisher	✓	✓		✓	
Differentiates permissions by a user	✓		✓	✓	✓
Prevents unauthorized viewing	✓				
Encrypts protected content	✓		✓		✓
Offers content expiration	✓				
Controls content reading	✓			✓ *	
Modifying or printing by user	✓			✓	
Extends protection beyond initial publication	✓	✓	✓		✓ *