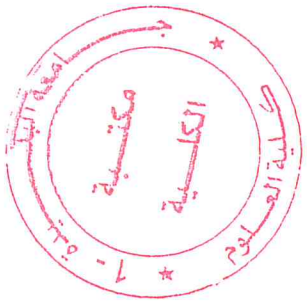
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahlab Blida1

Faculté des Sciences

Département d'Informatique



Mémoire de fin d'études

Pour l'obtention de diplôme de Master

Sécurité des systèmes d'information

Thème

La mise en place d'une infrastructure à clé publique pour le VPN et les emails

Réalisé par :

Abderrahmane Mohamed Ali

Settah Mohamed

Encadreur :

M. Ouchfoun Nadjib

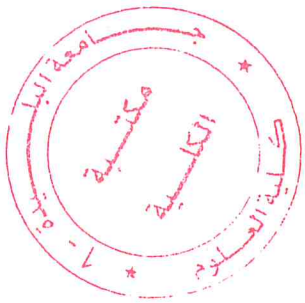
Promoteur :

Mme. Boumahdi Fatima

Promotion : 2016/2017

REMERCIEMENT

Ce travail a été réalisé dans le cadre du projet de fin d'études,
à l'entreprise UNIDEES Algérie.
Premièrement nous remercions Dieu de nous savoir donner foi, force et santé. Ensuite, nous remercions en particulier nos familles pour leurs prières et leurs encouragements tout le long de nos études.
Nous remercions notre promoteur de mémoire, Mme BOUMAHDI.F, pour ses précieux conseils et son orientation tout au long de notre travail.
Nous remercions aussi notre encadreur, Mr OUCHFOUN Nadjib, pour son entière disponibilité, son aide inestimable qui nous ont permis de découvrir un peu plus le monde de sécurité.
Nous remercions tous les membres de jury d'avoir accepté d'assister à la présentation de ce travail.
Nous remercions et dédions ce travail à nos familles et tous nos amis pour leur soutien et leur présence.



Sommaire

Liste des figures

Liste des tableaux

Résumé

Ce mémoire a été réalisé dans le cadre du stage de fin d'étude en vue d'obtenir le diplôme de Master en sécurité des systèmes d'information. Notre projet est réalisé au sein de l'entreprise UNIDEES consiste à mettre en place une infrastructure à clé publique pour le VPN et les emails.

Nous avons divisé notre mémoire en deux chapitres, une introduction et une conclusion. Le premier chapitre contient une présentation du sujet et quelques définitions en relation les infrastructures à clé publique. Le deuxième chapitre concerne la conception de notre système, discute les besoins, illustre les installations nécessaires pour mettre en place notre infrastructure et a la fin montre comment les emails et le VPN sont sécurisés a l'aide des certificats générés par notre infrastructure.

الملخص

لقد تم إنجاز هذه المذكرة في إطار تدريب نهاية الدراسة من أجل الحصول على شهادة الماستر في أمان الأنظمة المعلوماتية. يتم تنفيذ مشروعنا داخل الشركة أونيدي لإنشاء البنية ذات المفتاح العام للشبكة الإفتراضية الخاصة ورسائل البريد الإلكتروني.

لقد قسمنا المذكرة إلى فصلين، مقدمة وخاتمة. ويتضمن الفصل الأول عرضا للموضوع وبعض التعاريف المتعلقة بالبنية ذات المفتاح العام. ويتناول الفصل الثاني مفهوم نظامنا، ويناقش الاحتياجات، ويوضح التركيبات اللازمة لإنشاء بنيتنا، وفي النهاية يبين كيف يتم تأمين رسائل البريد الإلكتروني والشبكة الظاهرية الخاصة باستخدام الشهادات الناتجة عن البنية.

Abstract

This thesis was realized in the framework of the end of study training in order to obtain Master diploma in security of information systems. Our project is carried out within the company UNIDEES to set up a public key infrastructure for VPN and emails.

We have divided our thesis into two chapters, an introduction and a conclusion. The first chapter contains a presentation of the subject and some definitions related to public key infrastructures. The second chapter deals with the conception of our system, discusses the needs, illustrates the installations needed to set up our infrastructure and in the end shows how the emails and the VPN are secured using the certificates generated by our infrastructure.

Chapitre I : Fondations à l'infrastructure à clés publiques

1. Introduction

La cryptographie aujourd'hui est comme une phase obligatoire lors la conception de n'importe quel système informatique **[2]**. Son objectif fondamental est de chiffrer les données qui circulent dans le réseau pour les protéger. Cependant, elle ne puisse pas assurer la sécurité des transactions électroniques d'une manière efficace, c'est pourquoi nous avons besoins d'une infrastructure à clé publique qui fournit des politiques pour garantir cette sécurité.

Dans ce chapitre, nous apprendrons les bases d'une infrastructure à clé publique, ses différents composants et les rôles de chaque composant. Nous discuterons aussi les rôles des certificats numériques et enfin nous examinerons les domaines d'utilisation de cette infrastructure.

2. Présentation de l'organisme d'accueil

UNIDEES *Algérie*, entreprise spécialisée dans le conseil, l'intégration et l'infogérance en sécurité des systèmes d'information, évolue dans des environnements où l'exigence est permanente (Energie, Industries, Défense, Télécom…). Ses missions de conseil ainsi que son expérience des projets d'intégration et d'infogérance menés dans des environnements complexes, sensibles et critiques, lui permettent d'accompagner durablement ses clients dans leur activité, en répondant à leurs exigences de transformation.

La pérennité et la sûreté des systèmes font notamment partie des préoccupations essentielles d'**UNIDEES** Algérie, qui place la sécurité au cœur de chacun de ses projets. A cette culture de la rigueur s'ajoutent la détermination à prendre des engagements forts en termes de résultats et la conviction que la réussite se fonde sur la qualité des hommes, leurs compétences et leur éthique.

L'activité d'UNIDEES est basée sur les trois pôles ci-dessous :

- **IT Solutions :** Elle fournit toutes les prestations et solutions nécessaires au support et la disponibilité du système d'informations, en termes d'audit, de conseil, d'intégration et de maintenance des systèmes, des réseaux et de la sécurité.
- **Business solutions :** Regroupe toutes les solutions qui touchent Directement l'information disponible pour les utilisateurs finaux. Elle propose des solutions de communications unifiées, de travail collaboratif et de mobilité.
- **Training Solutions :** Propose plus de 300 formations management et informatique qui s'adressent aux managers et ingénieurs informatiques qui couvrent les méthodes

innovantes de gestion (PMP, prince2, ITIL, ISO, Ethical Hacking…) aux dernières techniques et technologies, des réseaux et de la sécurité.

Le diagramme suivant nous montre un organigramme global d'UNIDEES :

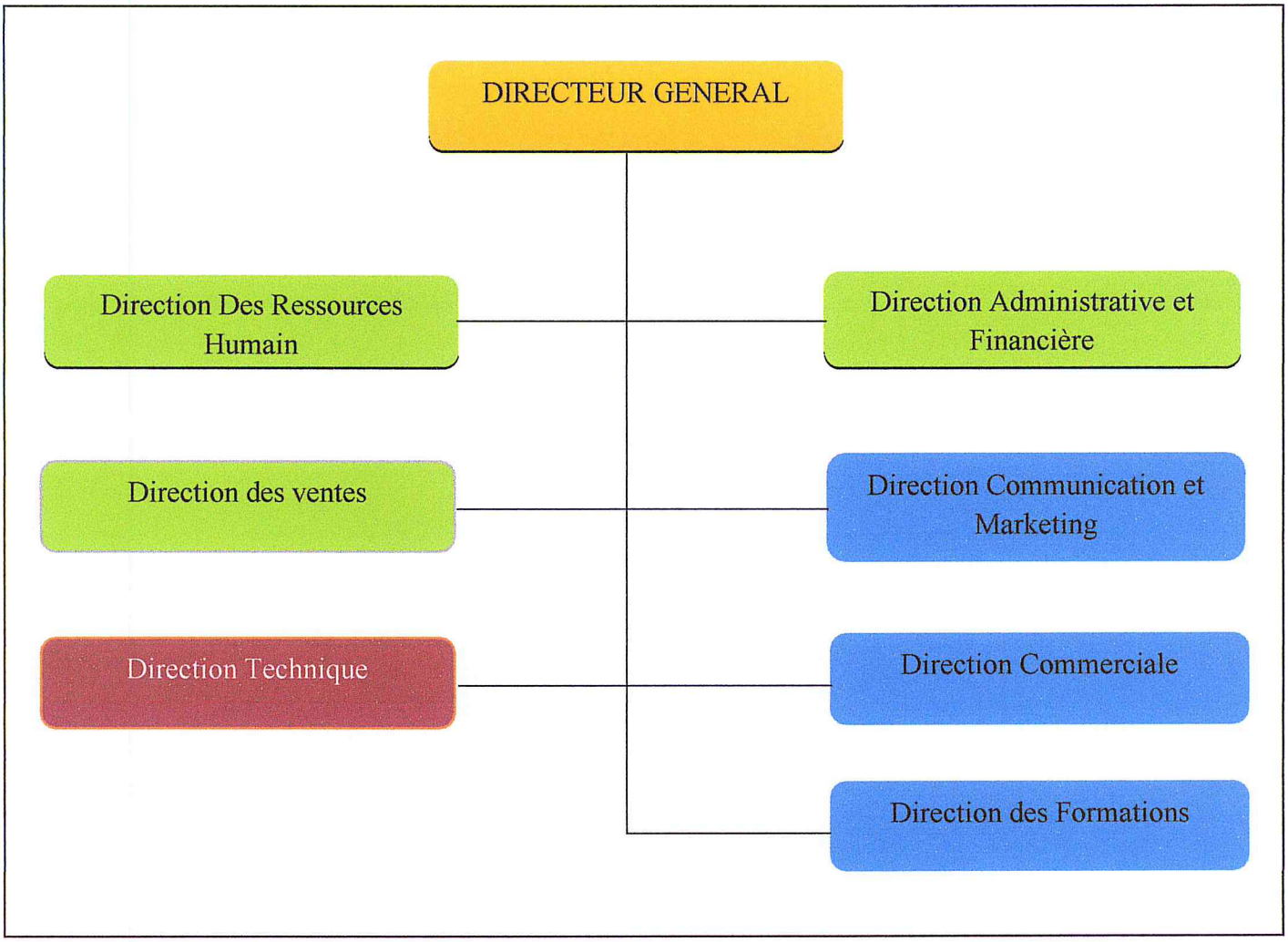


Figure 1.1 : Organigramme global d'UNIDEES

3. Définition de la cryptographie

La cryptographie est l'une des disciplines de la cryptologie qui consiste à protéger les données en utilisant des clés de chiffrement, donc les données deviennent incompréhensibles et seule la personne qui possède la clé de déchiffrement est capable de déchiffrer les données **[2]**.

- **Le but de la cryptographie :** L'envoi des données est devenu un acte habituel, mais aussi la sécurité de ces données est devenue un problème majeur. Il existe trois types de risque lorsque la transaction des données :

1. **Perte de confidentialité :** L'envoi des données en clair sur Internet permettre à des tierces parties de les lire facilement. Cela en générale arrive quand des informations sensibles, document commerciaux ou techniques sont envoyés (**Figure1.2 [3]**).

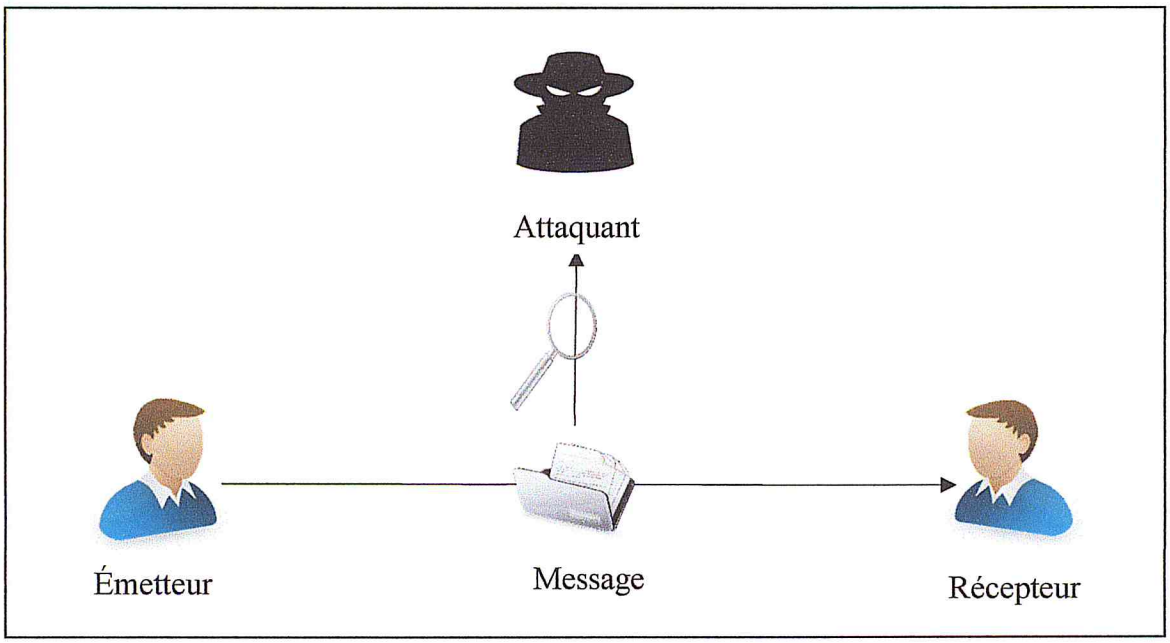


Figure 1.2 : Perte de confidentialité des données

2. **Usurpation d'identité :** Les données peuvent être fabriquées de toutes pièces, en indiquant une fausse identité pour l'expéditeur. Un attaquant peut alors prendre facilement l'identité d'une personne quelconque pour attaquer l'entreprise (**Figure1.3 [3]**).

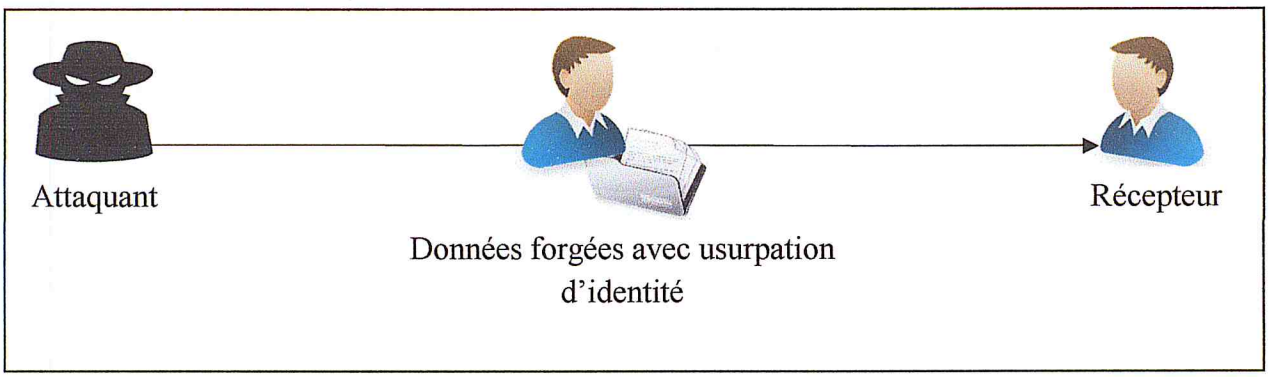


Figure 1.3 : Usurpation d'identité

3. **Modification du contenu d'un message :** Les données peuvent être interceptées, modifiées, puis relayées à son destinataire, donc rien ne garantit que ces données

que l'on reçoit correspondent bien à celui qui a été envoyé par son expéditeur (**Figure1.4 [3]**).

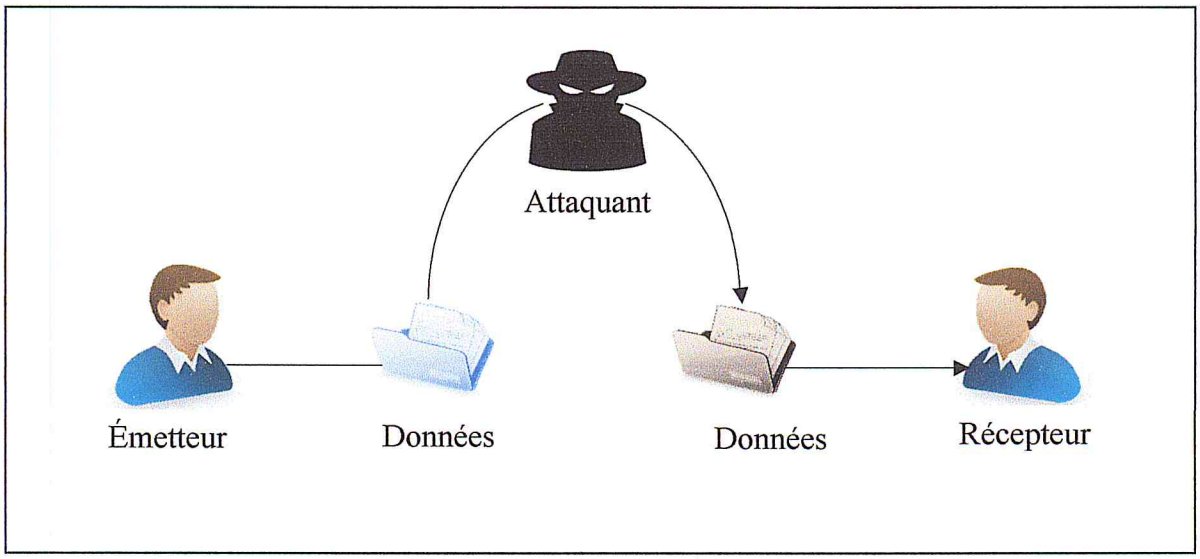


Figure 1.4 : Modification du contenu d'un message

La cryptographie permet donc de répondre à ces risques à l'aide des algorithmes cryptographiques qui assurent les propriétés de sécurité : la confidentialité, l'intégrité, l'authenticité.

4. Les types des algorithmes cryptographiques

La cryptographie supporte trois types des algorithmes cryptographiques, les algorithmes de cryptographie symétrique qui va garantir l'intégrité et la confidentialité des données, les algorithmes de cryptographie asymétrique qui va garantir la confidentialité, l'intégrité et l'authenticité et les fonctions de hachage qui sont utilisées pour vérifier si les données ont été modifiées.

a. **Les algorithmes symétriques :** Ce sont les algorithmes les plus anciennes et les plus simples pour augmenter le niveau de sécurité. Elles consistent à chiffrer et déchiffrer des messages à l'aide d'une même clé.

Parmi les algorithmes symétriques **: DES** (Data Encryption Standard), **RC4** (Rivest's Cipher version 4), **3DES** (Triple DES), **AES** (Advanced Encryption Standard).

- **Avantages :** Les algorithmes symétriques sont capables de chiffrer et déchiffrer des gros donnés rapidement grâce à l'utilisation d'une seule clé ainsi qu'ils sont plus simples que les algorithmes asymétriques.
- **Inconvénients :** Le risque majeur des algorithmes symétriques est la transmission de la clé en sécurité. Si un attaquant arrive à connaitre la clé symétrique il peut déchiffrer tous les données chiffrées avec cette clé.

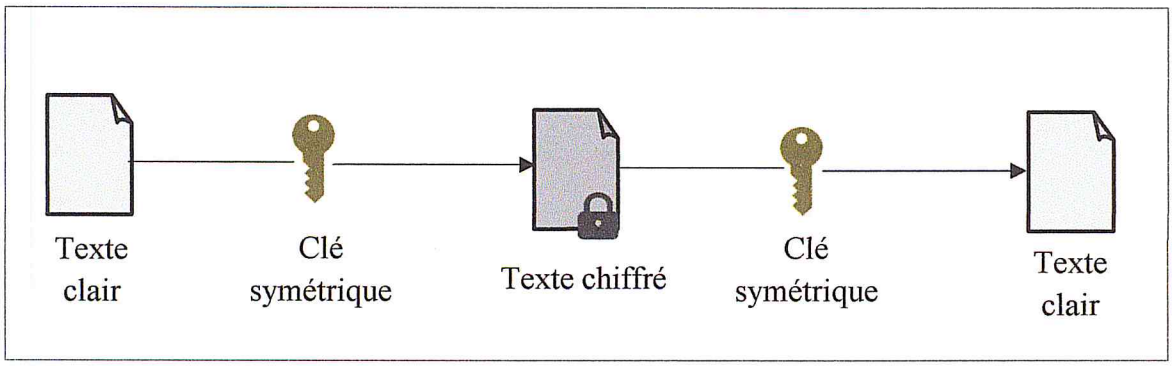


Figure 1.5 : Processus des algorithmes symétriques [2]

Le processus des algorithmes symétriques se déroulent de la manière suivante :

1. Génération de la clé secrète par l'émetteur.
2. Chiffrement du message par l'émetteur avec la clé secrète et l'envoyé au récepteur.
3. Déchiffrement du message par le récepteur avec la clé secrète reçue.

b. Les algorithmes asymétriques : Ce sont les algorithmes qui utilisent deux clés reliées mathématiquement, l'une est publique et l'autre est privée. Elles sont utilisées dans le processus de chiffrement et déchiffrement.

Parmi les algorithmes asymétriques : RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm), Deffie-Hellman.

- **Avantages :** Les algorithmes asymétriques augmentent le niveau de sécurité en utilisant deux clés séparées mais en relation mathématique. La clé privée détenue uniquement par l'utilisateur qui génère la paire de clés. La clé publique peut être distribuée à toute personne qui souhaite envoyer des données cryptées au détenteur de la clé privée.
- **Inconvénients :** La complexité des algorithmes asymétriques et l'utilisation de deux clés rendent le processus de chiffrement et déchiffrement plus lent. Les études ont montré que les algorithmes symétriques sont au moins cent fois plus

rapides que les algorithmes asymétriques lors de l'utilisation d'une cryptographie basée sur un logiciel, et peut être jusqu'à dix mille fois plus rapide en utilisant la cryptographie matérielle **[2]**.

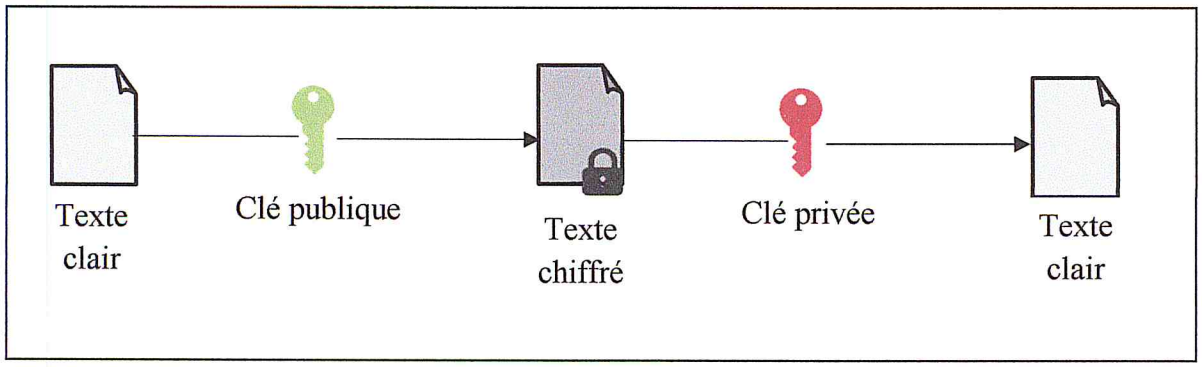


Figure 1.6 : Processus des algorithmes asymétriques [2]

Le processus des algorithmes asymétriques se déroulent de la manière suivante :

1. L'émetteur chiffre le texte clair par la clé publique du destinataire.
2. Le texte chiffré est envoyé et mis à la disposition du destinataire. Il n'est pas nécessaire d'envoyer la clé publique car le destinataire a déjà la clé privée requise pour décrypter le texte chiffré.
3. Le destinataire déchiffre le texte chiffré avec sa clé privée et le texte en clair résultant est le texte original.

c. Les fonctions de hachage : Les fonctions de hachage sont des programmes informatiques qui permettent de crée une signature (empreinte) d'un fichier de n'importe quel type (texte, image, vidéo…etc). Le principe est qu'un message clair de longueur quelconque doit être transformé en un message de longueur fixe. Les fonctions de hachage sont des fonctions irréversibles (One way function) c'est-à-dire que le calcul de la fonction de hachage est facile et rapide tandis que le calcul de sa fonction inverse est infaisable **[2]**.

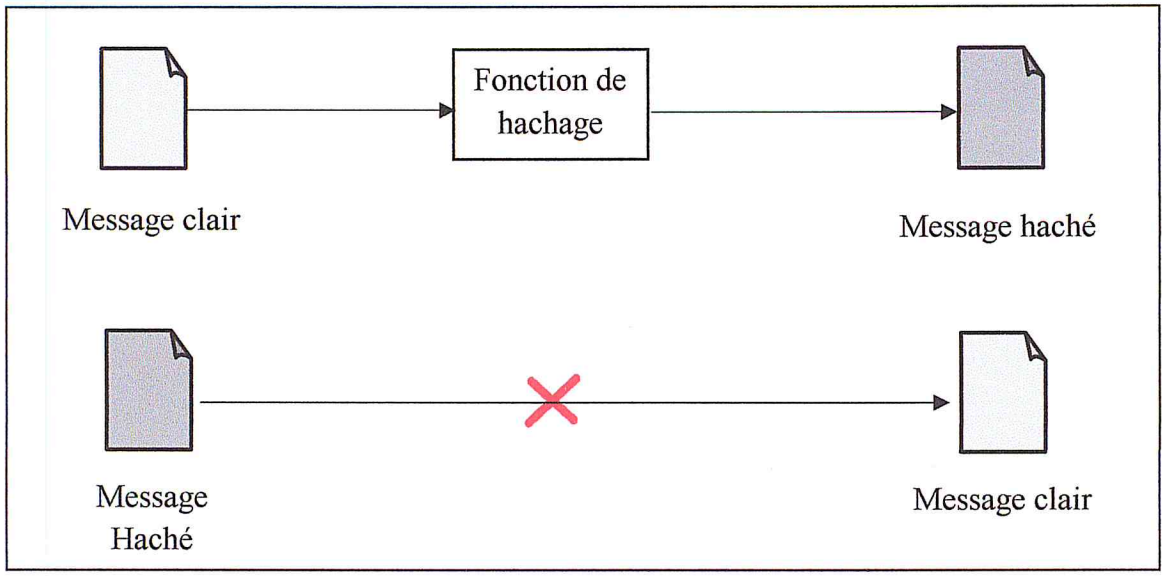


Figure 1.7: Processus de hachage

5. Combinaison de l'algorithme symétrique et asymétrique

Dans la plupart des applications, le chiffrement symétrique et le chiffrement asymétrique sont combinés pour tirer parti des forces de chaque méthode.

Quand le chiffrement symétrique et asymétrique sont combinés :

- Le chiffrement symétrique est utilisé pour convertir le texte clair en texte chiffré. Ceci profite de la vitesse de chiffrement symétrique.
- Le chiffrement asymétrique est utilisé pour échanger la clé symétrique utilisée pour le cryptage. Ceci profite de la sécurité du chiffrement asymétrique, en s'assurant que seul le destinataire peut décrypte la clé symétrique.

6. Les infrastructures à clé publique

Une **infrastructure à clé publique** (ICP) ou **infrastructure de gestion de clé** (IGC) ou encore **Public key infrastructure** (PKI) est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques), de procédures humaines (vérification, validation), règles, procédures et de logiciels (système et application) qui interagissent pour faire confiance aux identités. Elle permet de sécuriser de façon globale l'accès à un réseau, à des informations et données. La PKI est constituée d'un ensemble des services qui reposent sur l'utilisation de la cryptographie asymétrique et permet la gestion du cycle de vie des certificats numériques **[2]**.

6.1. Les fonctions d'une infrastructure à clé publique

Une infrastructure à clé publique fournit quatre services principaux **[4]** :

- **Fabrication de bi-clés :** L'autorité d'enregistrement fabrique un couple de clé (clé privée, clé publique). La clé privée sera transmise au client alors que la clé publique a l'autorité de certification pour l'ajouter au certificat.
- **Certification des entités :** Après que l'autorité de certification obtient la clé publique, elle l'ajoute au certificat qui sera envoyé aux entités authentifiées.
- **Publication des certificats :** L'autorité de certification doit publier les certificats valides et les certificats révoqués pour que les entités puissent vérifier la validité des certificats. L'autorité de certification doit publier le numéro de série de certificat et dans le cas des certificats révoqués la cause de révocation est ajoutée.
- **Révocation des certificats :** L'autorité de certification doit révoquer les certificats qui ne sont pas valide. Il y a plusieurs causes pour qu'un certificat soit révoqué : la date de fin de validité est dépassée, la perte ou la compromission de la clé privée associée au certificat, le changement d'au moins un champ relatif au propriétaire du certificat, la compromission de l'autorité de certification.

6.2. Les certificats numériques

Un certificat numérique (aussi appelé certificat électronique) est un fichier permettant de certifier l'identité du propriétaire d'une clé publique, un peu à la manière d'une carte d'identité. Actuellement, les certificats numériques sont reconnus à la norme X.509 version 3 **[5]**.

Ce format se compose de **[4]** :

- La version du certificat X.509 (actuellement la V3).
- Le numéro de série.
- L'algorithme de signature.
- Le nom de l'émetteur (autorité de certification).
- La date de début et de fin de validité.
- L'adresse électronique du propriétaire.
- La clé publique à transmettre.
- Le type de certificat.
- L'empreinte du certificat (signature électronique).
- Extensions : contient des informations optionnelles.

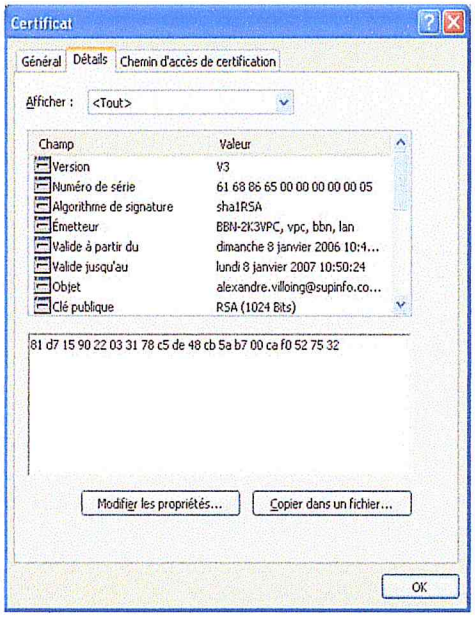


Figure 1.8 : Exemple d'un certificat numérique X.509 version 3 [6]

Les informations de certificat et la clé publique de demandeur seront signées par l'autorité de certification, en passant par une fonction de hachage qui va créer une empreinte de ces informations, puis chiffré cette empreinte par la clé privée de l'autorité de certification pour obtiendrai une signature (**Figure 1.9 [6]**).

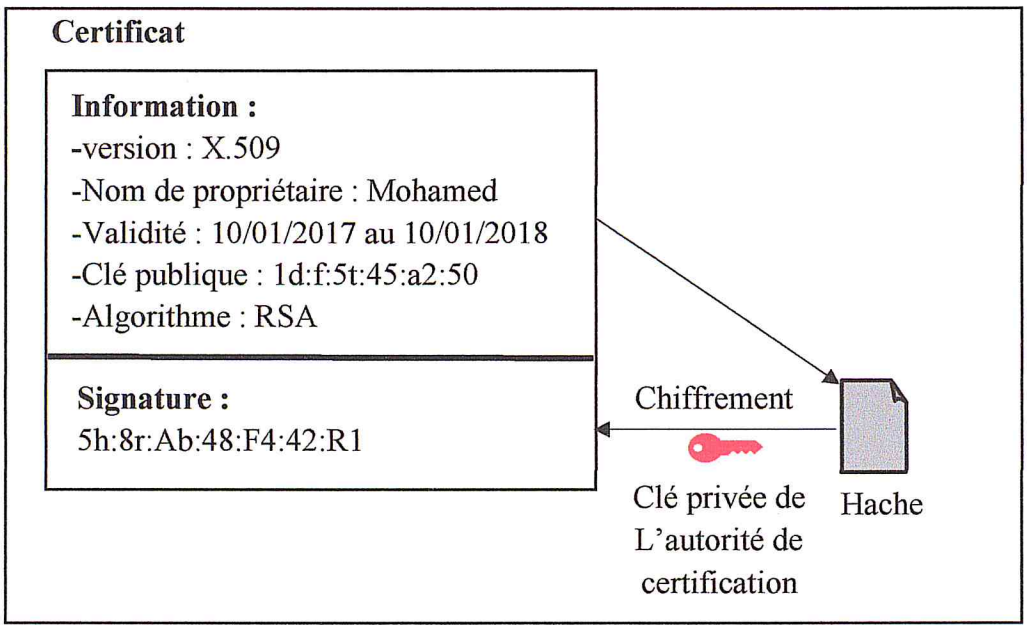


Figure 1.9 : Processus de signature d'un certificat

Avec cette structure, il est possible de vérifier la validité de message en appliquant la même fonction de hachage sur les informations de certificat, et en déchiffrant sa signature par la clé publique de l'autorité de certification. Les deux résultats seront comparés pour vérifier le non modification de certificat (**Figure 1.10 [6]**).

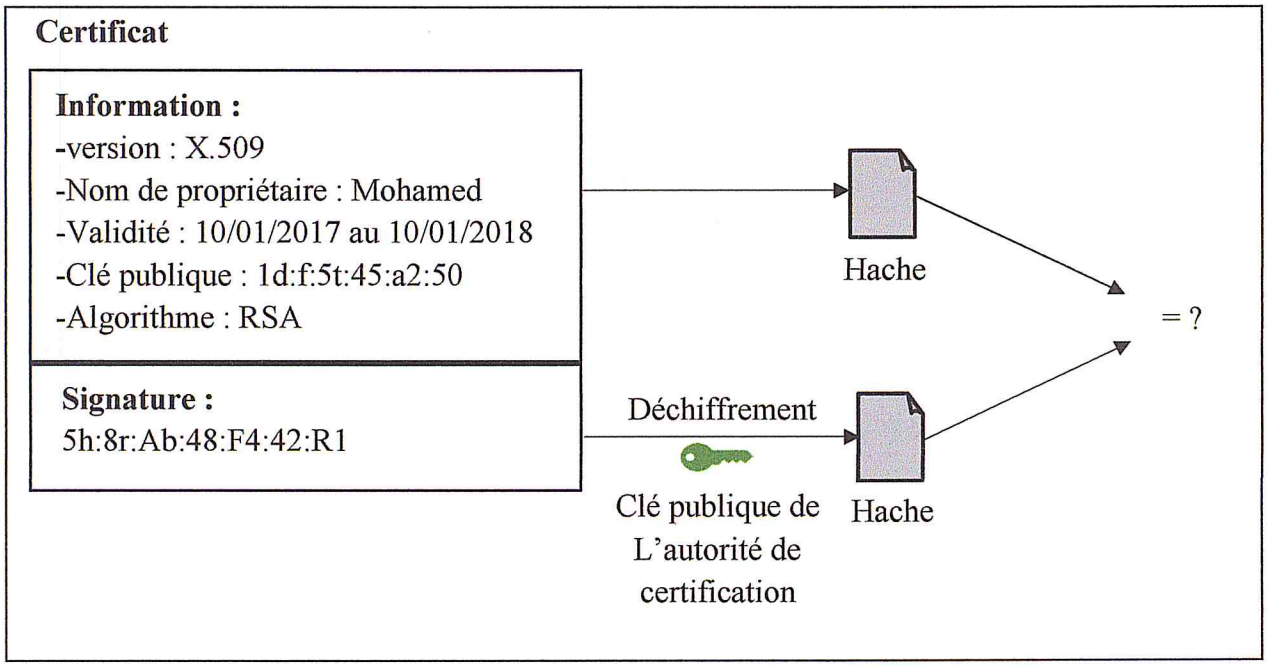


Figure 1.10 : Processus de vérification de la signature d'un certificat

6.3. Importance de la PKI

Une infrastructure à clés publiques délivre des certificats numériques. Ces certificats permettent d'effectuer des opérations cryptographiques, comme le chiffrement et la signature numérique qui offrent les garanties suivantes lors des transactions électroniques **[7]** :

- **La confidentialité :** Elle garantit que seul le destinataire peut en avoir une vision claire.
- **L'authentification :** Elle garantit à tout destinataire d'un message l'identité de l'expéditeur ou de l'utilisateur en question.
- **L'intégrité :** Elle garantit qu'un message n'a pas été modifié, accidentellement ou intentionnellement.
- **La non-répudiation :** Elle garantit à quiconque que l'auteur d'un message ne peut nier son œuvre, c'est-à-dire prétendre ne pas en être l'auteur.

6.4. Les composants de la PKI

Une infrastructure à clés publiques contient plusieurs composants principaux et essentiels à son bon fonctionnement **[8]** :

- **Une Autorité d'Enregistrement (AE) :** Son principal rôle est de vérifier la demande d'enregistrement d'un nouvel utilisateur ou les porteurs de certificat dans l'infrastructure.
- **Une Autorité de Certification (AC) :** Son principal rôle est de générer un certificat pour l'utilisateur. L'autorité de certification signera ce certificat avec sa clé privée qui sera lui-même certifié par une autorité supérieure et ainsi de suite jusqu'à la racine. On parle de chaîne de confiance dans une PKI car il s'agit de faire confiance à cette autorité de certification. L'autorité de certification aura aussi le rôle de mettre à jour la liste des certificats qu'il a signé afin de connaître les dates de validité de ses certificats. En effet, pour vérifier si un certificat est valide, il faudra demander à l'autorité de certification qu'il l'a généré si le certificat en question est toujours valide ou s'il a été révoqué. Cette autorité est la plus critique **[2]**.
- **Une Autorité de Dépôt (AD) :** Son principal rôle est de stocker les certificats valides ainsi que les certificats révoqués afin d'avoir un accès rapide à ces certificats. De plus, l'autorité de dépôt peut stocker les clés privées des utilisateurs dans le cadre du recouvrement de clé.
- **Les utilisateurs de la PKI :** Ce sont les personnes effectuant des demandes de certificat mais aussi ceux qui souhaitent vérifier l'identité d'un certificat qu'ils ont reçu.

6.5. Les options de la hiérarchie d'autorité de certification

L'un des aspects les plus importants de la conception d'une infrastructure à clé publique est la planification de sa hiérarchie. Il existe généralement trois types de hiérarchie : à un niveau, à deux niveaux et à trois niveaux :

- **Hiérarchie à un niveau** : Inclut une seule autorité de certification. L'autorité de certification est considérée comme l'autorité de certification racine et l'autorité de certification émettrice **[9]**. Pour des raisons de sécurité, les autorités de certification émettrices et racines sont normalement séparées, car l'autorité de certification émettrice doit être en ligne et donc plus susceptible d'être compromise. Pour ce raison, une hiérarchie à un seul niveau n'est suffisante que pour des implémentations simples

où la facilité de gestion et les coûts réduits l'emportent sur des niveaux plus élevés de sécurité ou de flexibilité.

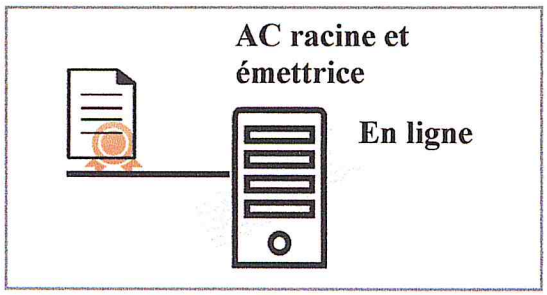


Figure 1.11 : Hiérarchie AC à un niveau [9]

- **Hiérarchie à trois niveaux :** Dans ce type de hiérarchie, il existe un niveau d'autorité de certification racine (hors connexion), un niveau d'autorités de certification émettrices et un niveau intermédiaire **[9]**. Le placement de cette autorité de certification intermédiaire peut avoir lieu pour plusieurs raisons par exemple l'utilisation du deuxième niveau d'autorité de certification comme autorité de certification de stratégie, une des autorités de certification de stratégie émet des certificats qui exigent qu'un utilisateur soit présent physiquement et une autre autorité de certification émet des certificats aux utilisateurs d'entreprise authentifiés. En d'autres termes, l'autorité de certification de stratégie est configurée pour émettre des certificats à l'autorité de certification émettrice qui est limitée concernant le type des certificats qu'elle émet.

  La sécurité augmente avec l'ajout d'un niveau et la flexibilité et l'extensibilité augmentent en raison des options de conception supplémentaires. En revanche, la facilité de gestion augmente, car il y a un plus grand nombre d'autorités de certification à gérer dans la hiérarchie et les coûts augmentent. Pour cette raison, les hiérarchies d'autorités de certification à trois niveaux ne sont généralement pas recommandées sauf pour les grandes entreprises.

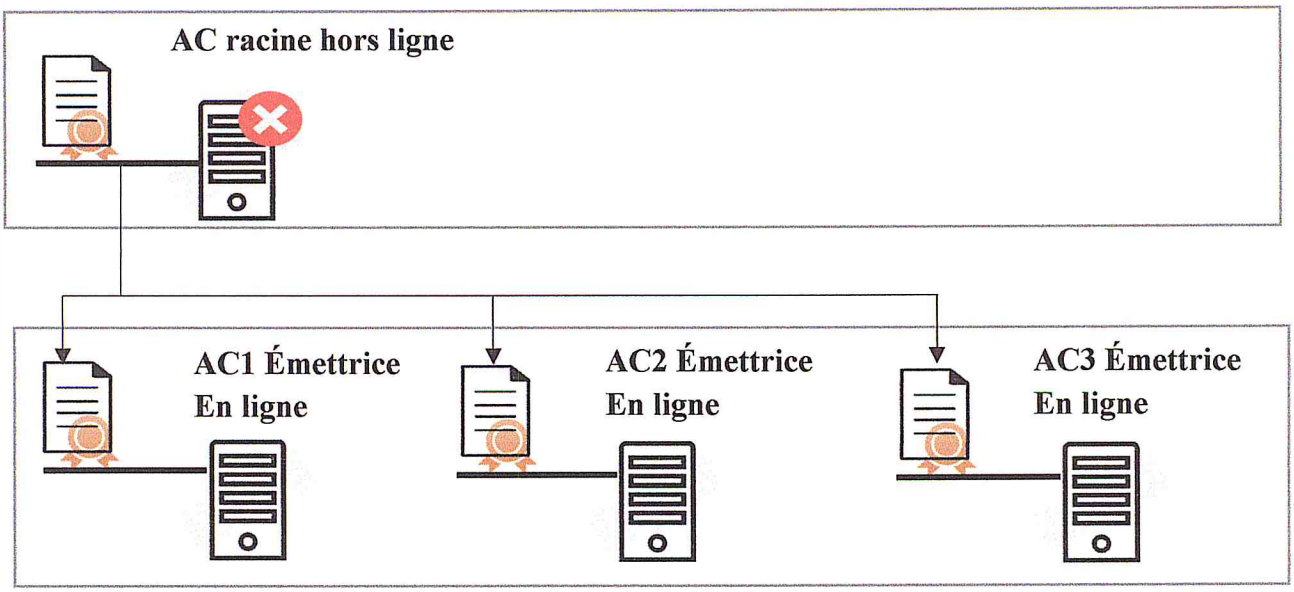


Figure 1.13 : Hiérarchie AC à deux niveaux [9]

7. Domaine d'utilisation de PKI

Plusieurs domaines utilisent les certificats générés par l'infrastructure à clé publique pour assurer leurs sécurités, parmi ces domaines les suivantes :

- **La messagerie instantanée et l'e-mail :** L'e-mail et la messagerie instantanée sécurisée utilisent un couple de clé pour le cryptage des fichiers et des messages. Le protocole de messagerie et e-mail sécurisées le plus connu et le S/MIME (Secure Multipurpose Internet Mail Extensions) qui est une extension de protocole MIME (Multipurpose Internet Mail Extensions) **[10]**.
- **L'accès web :** Les navigateurs et les serveurs web utilisent le cryptage pour assurer l'authenticité des utilisateurs, la confidentialité des données et ainsi pour sécuriser des applications contenant des transactions en ligne (le commerce et le paiement électronique par exemple) **[10]**.
- **La communication VPN :** Le cryptage et l'authenticité se sont les propriétés principales dans le VPN utilisé dans les communications site à site ou l'accès à distant sécurisée **[10]**.
- **L'authentification 802.1x pour le WIFI :** Les certificats sont utilisés pour contrôler l'accès au réseau et assurer l'identité des équipements connectés au réseau via le WIFI **[10]**.

- **L'authentification à deux facteurs (l'authentification forte) :** Plusieurs organisations implémentent l'authentification à deux facteurs pour augmenter la sécurité du réseau. Le principe de base est l'utilisation de deux différentes méthodes pour vérifier l'identité de l'utilisateur **[10]**.
- **Les documents électroniques :** Les certificats numériques permettent de faire confiance au contenu d'un document. Ils aident à déterminer qui a créer où signer un certain document et assurent aussi que le contenu du document n'a pas été changé **[10]**.

8. Les protocoles basés sur les infrastructures à clé publique

La plupart des protocoles de sécurité sont désignés à utiliser les infrastructures à clé publique, soit obligatoirement ou par choix, parmi ces protocoles **[11]** :

- **S /MIME (Secure Multipurpose Internet Mail Extensions) :** C'est le standard IETF (Internet Engineering Task Force) des emails sécurisés. Il utilise les PKI pour supporter la signature numérique et le cryptage des emails et des messages. La plus récente version du protocole S/MIME est la version 3 **[12]**.
- **SSL et TLS :** TLS (Transport Layer Security) et son prédécesseur SSL (Secure Socket Layer) sont les protocoles les plus importants pour garantir un accès sécurisé aux serveurs par les clients. Les deux protocoles dépendent des PKI pour la génération des certificats pour les clients et les serveurs **[12]**.
- **SET (Secure Electronic Transactions) :** C'est un protocole destiné spécialement à sécuriser les transactions Internet de paiement par carte bancaire. SET assure la confidentialité et l'intégrité des données à l'aide des clés de cryptage **[12]**.
- **IPSEC (Internet Protocol Security Protocol) :** C'est un standard IETF qui définit un ensemble de protocoles pour assurer des communications privées et protégées sur des réseaux IP en utilisant des algorithmes de cryptographie **[12]**. IPSEC est l'un des protocoles principaux pour déployer les VPNs.

9. Les processus de certification

Dans ce qui suit nous expliquons deux des plus importants processus dans la gestion de certification : La demande de certificat et la vérification de certificat.

9.1. Processus d'une demande d'un certificat

Lorsque l'Autorité d'enregistrement reçoit une demande de certificat par l'utilisateur, elle doit générer un couple de clés. L'une sera privée et envoyée à l'utilisateur, l'autre sera publique et envoyé à l'autorité de certification pour la mettre dans le certificat. Pour prouver que le certificat est réellement de cette autorité de certification, il doit être signé avec la clé privée de l'autorité de Certification. Le certificat signé doit être envoyé à l'utilisateur par L'autorité de certification qui va stocker une copie de ce certificat aux autorités de dépôt (**Figure 1.14 [5]**).

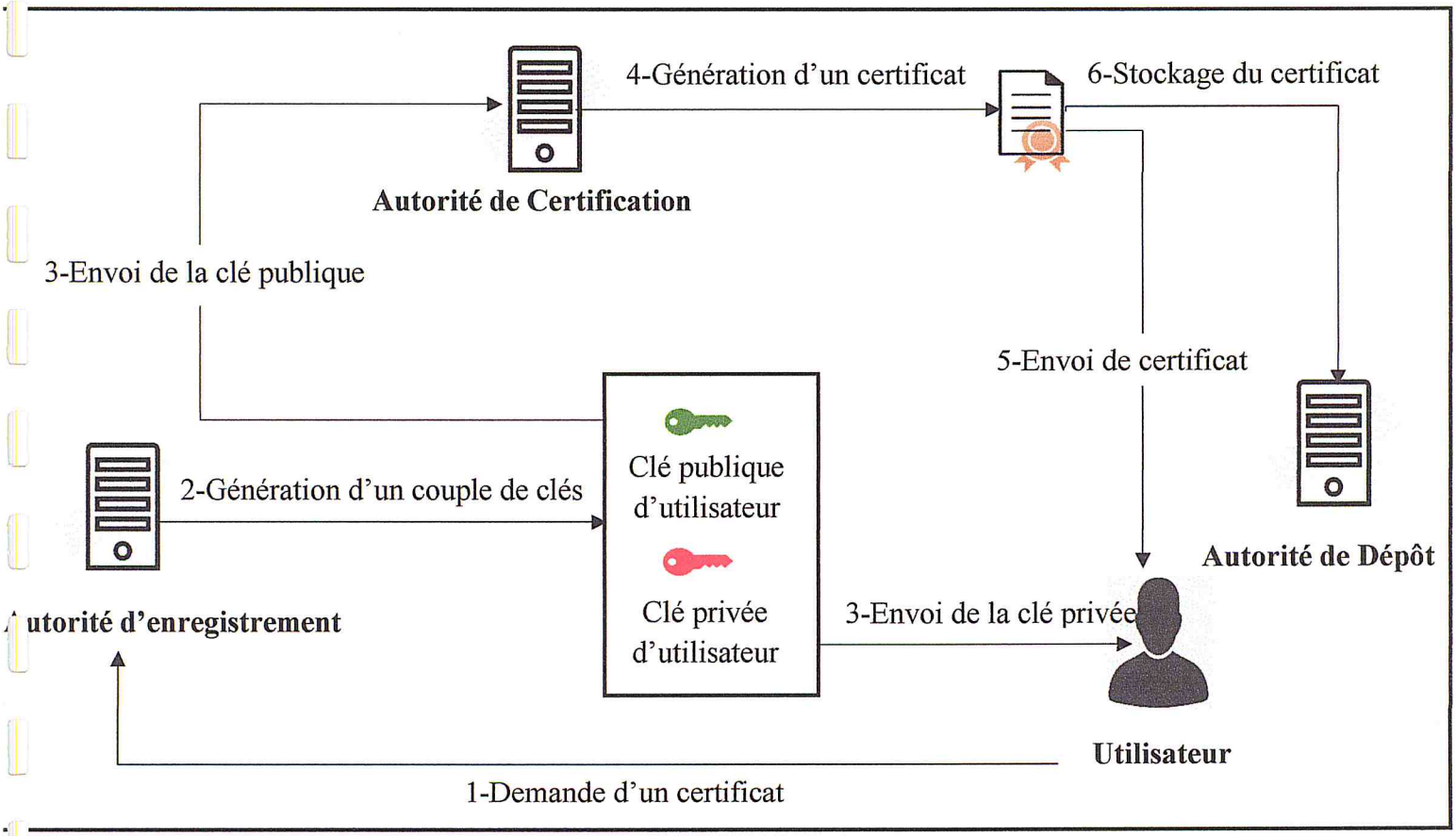


Figure 1.14 : Processus d'une demande d'un certificat [5]

9.2. Processus de vérification d'un certificat

Lorsqu'un utilisateur demande l'accès à un serveur il demande de montrer son certificat pour qu'il puisse lui faire confiance. Le serveur envoie son certificat à l'utilisateur qui va l'envoyer à l'autorité de certification pour vérifier si ce certificat est signé par la clé privée de l'autorité de certification ainsi que si sa durée de vie est encore valide. Si l'autorité de certification trouve que le certificat est valide elle va envoyer un avis favorable à l'utilisateur. L'utilisateur

va envoyer maintenant son certificat au serveur pour lui faire confiance avec le même processus pour vérifier la validité de certificat d'utilisateur. Maintenant l'accès sera protégé entre le serveur et le client (**Figure 1.15**).

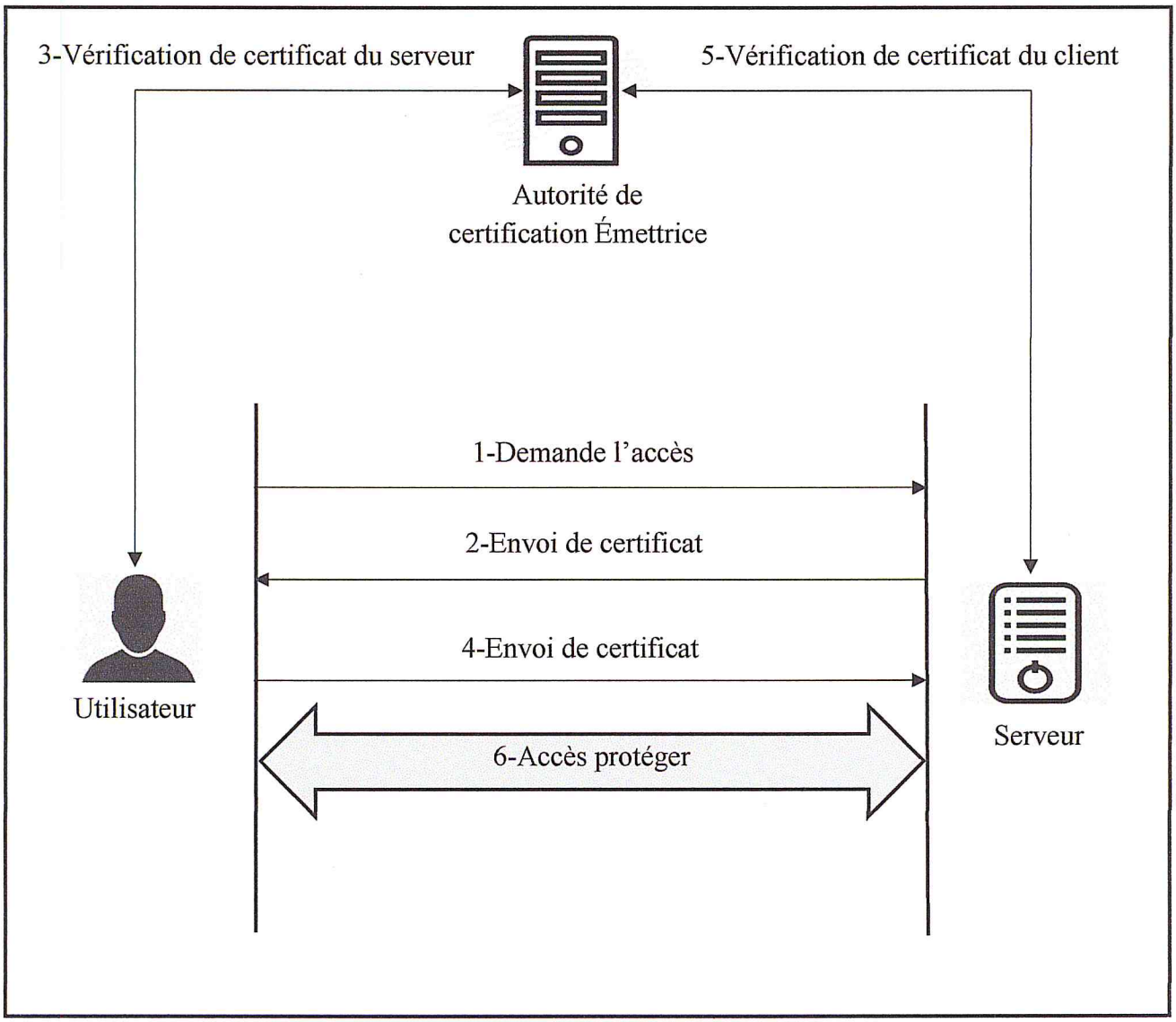


Figure 1.15 : Processus de vérification d'un certificat

10. La PKI dans les emails

Aujourd'hui toutes les entreprises utilisent les emails comme une méthode de communication entre les employés et les clients donc la sécurité de ces emails n'est pas seulement importante mais obligatoire. L'une des méthodes les plus utilisées pour sécuriser les emails est de protéger son contenu lui-même en implémentant le S/MIME (Secure Multipurpose Internet

Mail Extension). Le protocole S/MIME va garantir aux utilisateurs que leurs e-mails seront signés et chiffrés à la fois.

- **La signature numérique :** Permet non seulement de garantir l'origine de l'e-mail mais aussi de le protéger de toute modification non autorisée, garantissant ainsi son intégrité auprès du destinataire de l'e-mail.
- **Le chiffrement :** Assure la confidentialité du message et protège toute information sensible contre le vol.

10.1. La signature numérique

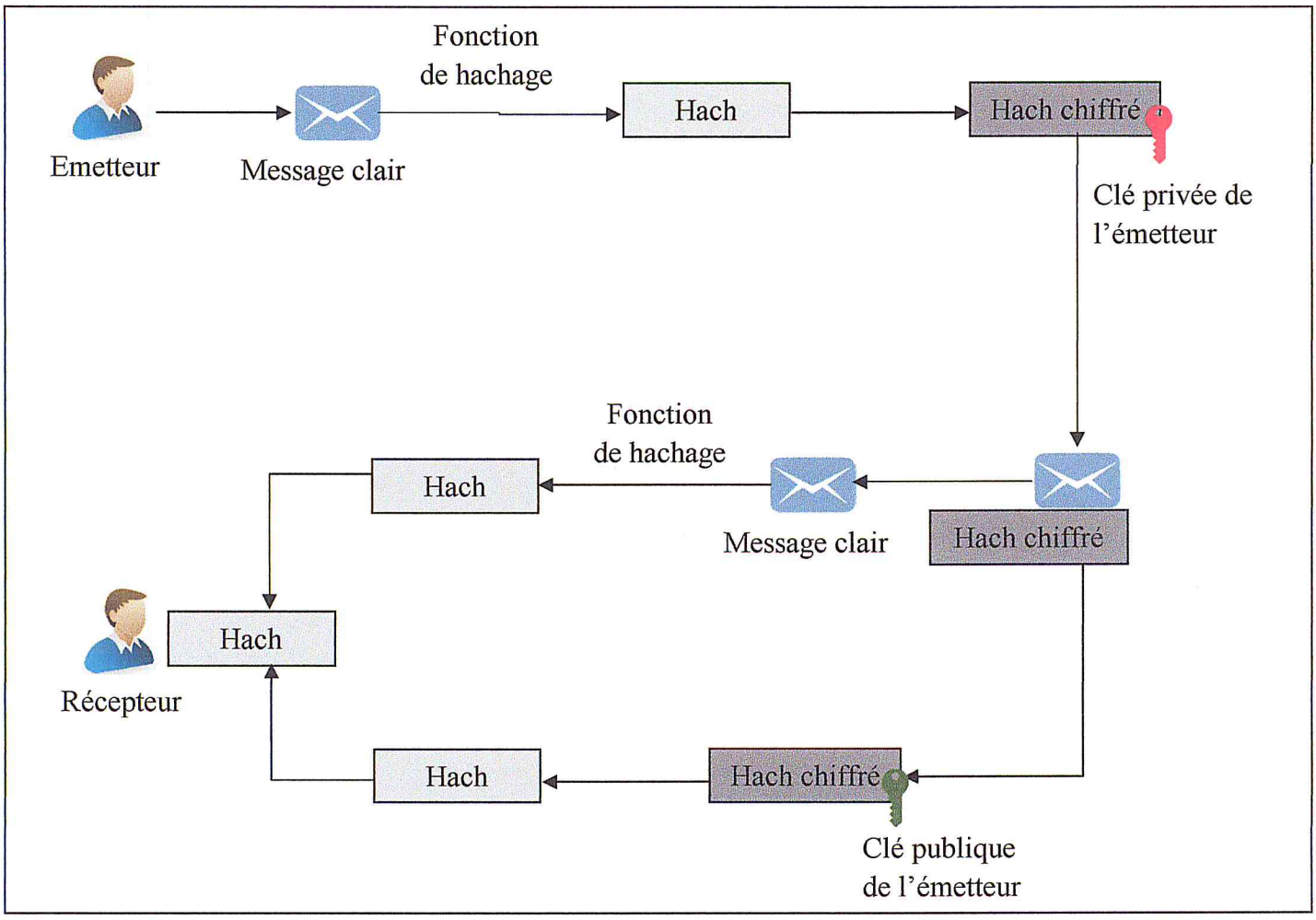


Figure 1.16 : Processus de la signature numérique des emails

La signature numérique se déroule de la manière suivante (**Figure 1.16 [2]**) :

1. L'émetteur crée un email.
2. Un algorithme de hachage est appliqué sur le message clair pour crier un hach.
3. Le message haché est chiffré par la clé privée de l'émetteur.
4. Le message clair et le message haché et chiffré sont envoyés au récepteur.

5. Le récepteur déchiffre le message haché et chiffré en utilisant la clé publique trouvée dans le certificat signé de l'émetteur.
6. Le même algorithme de hachage est appliqué sur le message clair.
7. Les deux messages hachés sont comparés. S'ils sont différés donc le message était modifié pendant sa transmission et sa signature sera invalide.

10.2. Le chiffrement

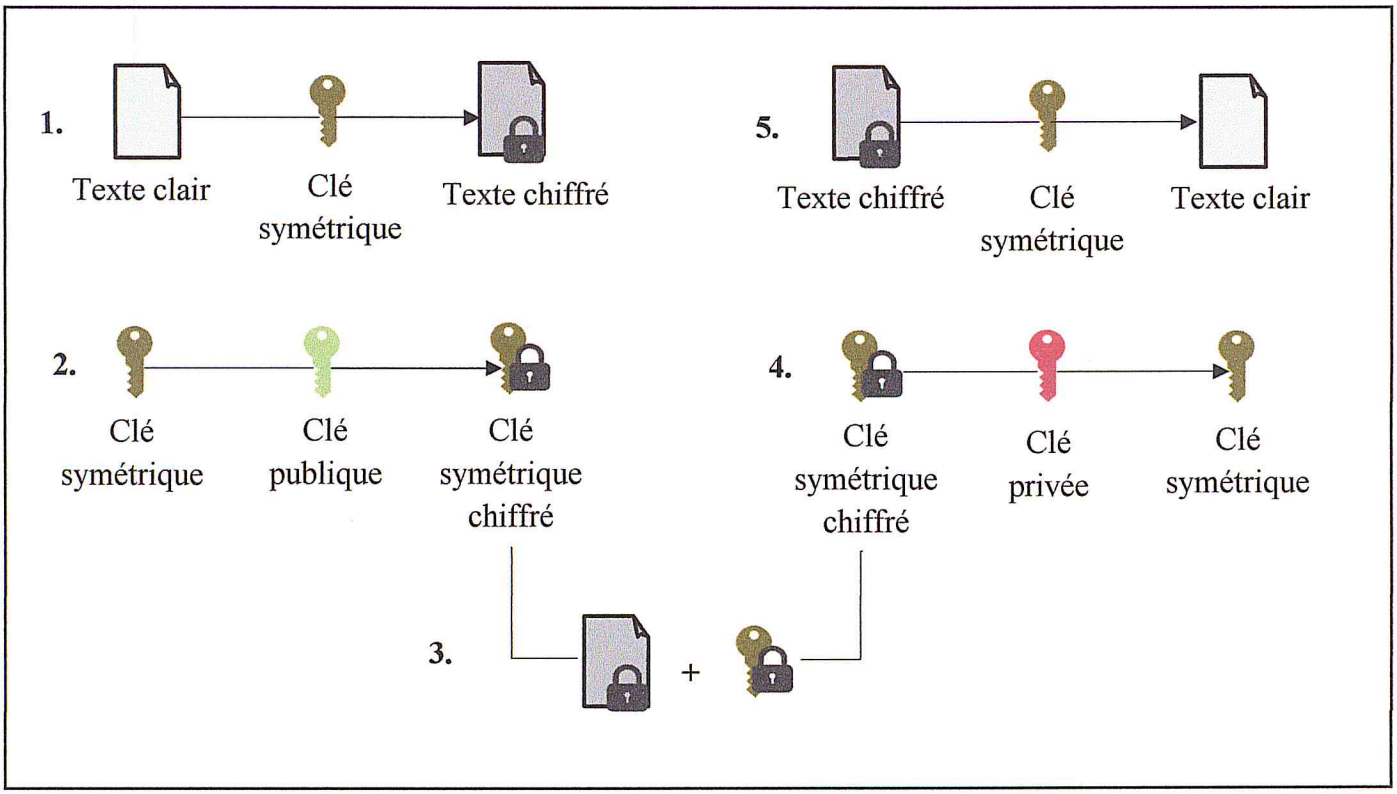


Figure 1.17 : Processus de chiffrement des emails

Le chiffrement des emails se déroule de la manière suivante (**Figure 1.17 [2]**) :

1. L'expéditeur génère une clé symétrique et utilise cette clé pour chiffrer les données d'origine.
2. La clé symétrique est cryptée avec la clé publique du destinataire pour empêcher que la clé symétrique ne soit interceptée pendant la transmission.
3. La clé symétrique cryptée et les données chiffrées sont fournies au destinataire prévu.
4. Le destinataire utilise sa clé privée pour déchiffrer la clé symétrique cryptée.
5. Les données chiffrées sont déchiffrées avec la clé symétrique, ce qui permet au destinataire d'obtenir les données d'origine.

11. La PKI dans le VPN

Dans le monde d'aujourd'hui, la concurrence a créé des partenariats entre les organisations situées à travers le monde. Pour cela, les employés de ces organisations sont besoin d'accéder à des données provenant de différents endroits même de leurs maisons **[2]**. Pour assurer le transfert sécurisé des informations, les organisations utilisent les VPN qui permettent la connectivité réseau sur une grande zone géographique.

Les VPN utilisent différents protocoles pour sécuriser les données qui circulent sur le réseau. Parmi ces protocoles le **IPSec** (déjà mentionné dans la partie 8 « Les protocoles basés sur l'infrastructure à clé publique ») et le **L2TP** :

- **L2TP (Layer Two Tunneling Protocol) :** L2TP est une extension du protocole PPTP (Point-to-Point Tunneling Protocol) utilisé pour permettre le fonctionnement d'un réseau privé virtuel (VPN). L2TP fusionne les meilleures fonctionnalités de deux autres protocoles de tunneling : PPTP (Point-to-Point Tunneling Protocol) de Microsoft et L2F de Systèmes Cisco. Il ne dispose pas d'un mécanisme de cryptage intégré, c'est pour cela qu'on le couple habituellement au protocole IPSEC (Internet Protocol Security) fournissant un système de chiffrage qui sécurise les transmissions des données **[12]**.

La méthode la plus sécurisée pour établir un tunnel entre deux hôtes est d'utiliser le protocole L2TP complété par IPSec qui supporte l'utilisation d'un système de certificat numérique (**Figure 1.18**).

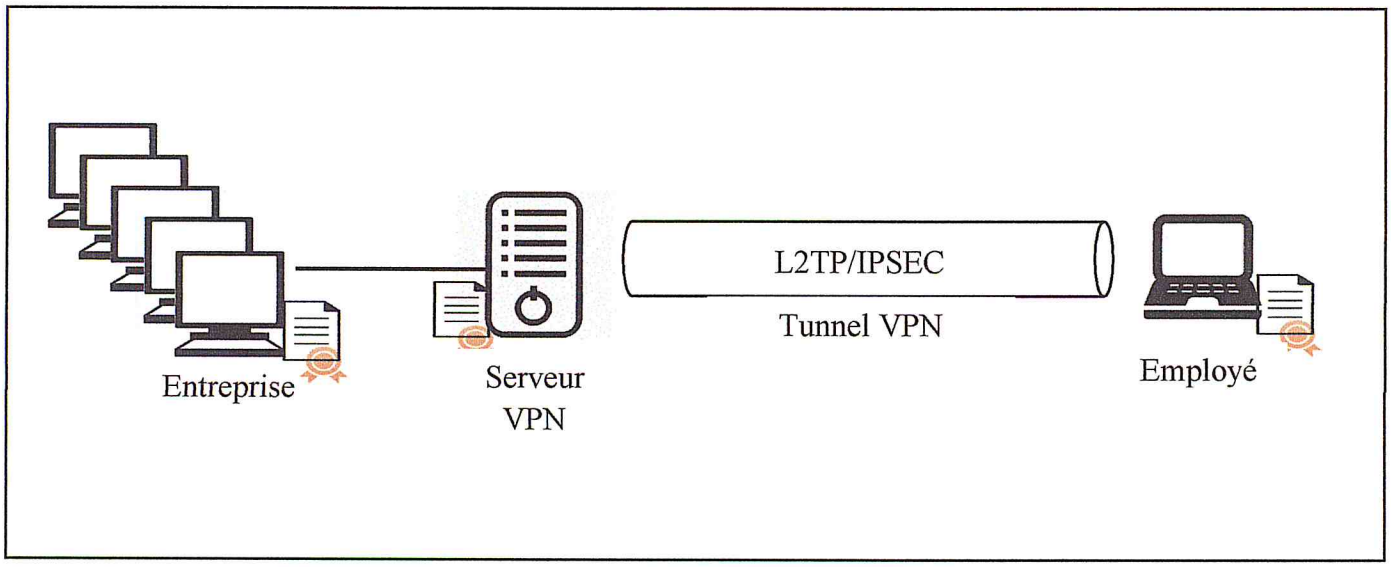


Figure 1.18 : Architecture d'un accès VPN sécurisé

12. Conclusion

Dans ce chapitre, nous avons présenté sur les bases des infrastructures à clés publiques, ses différents composants et l'utilité des certificats numériques. Nous avons discuté aussi les choix possible d'une architecture AC et enfin, les domaines d'utilisation d'une PKI.

Dans le chapitre qui suit, nous étudierons la conception de notre infrastructure à clés publiques, ensuite nous apprendrons la mise en place de cette infrastructure en précisant les étapes à suivre en détail.

Chapitre II : Mise en place d'une infrastructure à clés publiques

1. Introduction

Dans le chapitre précèdent, nous avons découvrir les infrastructures à clés publique et leurs diffèrent domaine d'utilisation.

Dans ce chapitre, nous allons étudier la conception de notre infrastructure à clés publiques, ensuite nous allons apprendre la mise en place de cette infrastructure en précisant les configurations recommandées.

2. La conception d'une PKI

Dans cette partie, nous allons étudier notre environnement de travail en détectant les besoins d'UNIDEES, ensuite, nous allons définir notre architecture AC choisi ainsi que les modèles de certificats à délivrer.

2.1. Les besoins

Unidees est une entreprise qui contient beaucoup d'employé. Ces employés doivent communiquer la majorité de temps par des courriers électroniques. Les e-mails peuvent contenir des documents électroniques importants et des informations sensibles. Par défaut, la sécurité d'un e-mail est équivalente à une carte postale anonyme.

D'autre part, quelques employés ont le droit d'accéder à distant aux donnés de l'entreprise. Même si l'accès aux données sera sécurisé par le VPN rien ne garantit l'identité d'utilisateur.

Donc les besoins de l'entreprise Unidees concernent la sécurité des e-mails échangés par ses employés et la sécurité des accès à distant de VPN. Donnons maintenant quelques exemples concrets de besoin :

- L'identité de l'émetteur et le récepteur des emails doit être garantie.
- L'intégrité et la confidentialité des emails doivent être bien assurées.
- Les employés qu'ils ont le droit d'accès a distant doivent être identifiés.

Il existe une solution simple pour sécuriser ces communications : l'utilisation des certificats électroniques. Il existe plusieurs fournisseuses publiques des certificats électroniques sur l'Internet, mais ces certificats coûtent chères. Donc pour rendre cette solution économique, il suffit de délivrer ce certificat électronique par notre propre autorité de certification entreprise.

Lorsqu'une infrastructure à clés publique sera totalement déployée à Unidees, chaque personnel disposera d'un certificat qui lui permettre d'envoyer des e-mails et accéder à distance on toute sécurité.

2.2. Les types d'AC

Windows Server 2008 R2 inclut les types d'autorité de certification suivante **[2]** :

- AC Entreprise.
- AC Autonome.

➢ **AC Entreprise :** AC Enterprise est une autorité de certification qui requiert un Active Directory pour émettre des certificats. Lorsqu'un Active Directory est installé, il est automatiquement ajouté en tant que référentiel des autorités de certification racine de confiance pour tous les ordinateurs et les utilisateurs d'un domaine.

Les fonctionnalités de la AC entreprise sont les suivantes :

- Émet des certificats aux utilisateurs et aux ordinateurs qui font partie d'une organisation.
- Vérifie l'identité du demandeur.
- Provoque ou refuse les demandes de certificat immédiatement. Il ne règle jamais le statut de la demande en attente.
- Utilise des modèles de certificat pour définir des certificats qui sont destinés à un but spécifique. Certains modèles définis sont l'administrateur, le contrôleur de domaine, l'utilisateur et le serveur Web. Chaque modèle possède une autorisation de sécurité, qui a été définie dans Active Directory. Cela permet de déterminer si le demandeur dispose de droits d'accès suffisants pour récupérer le certificat.

➢ **AC Autonome :** AC autonome est une autorité de certification qui n'utilise pas un Active Directory pour émettre des certificats. Lorsque nous soumettons une demande de certificat à une autorité de certification autonome, nous devons fournir des informations complètes sur nous-mêmes et le type de certificat que nous souhaitons.

Les fonctionnalités de la AC autonome sont les suivantes :

- Émet des certificats aux utilisateurs et aux ordinateurs qui ne font pas partie de l'organisation.

- Ne nécessite pas de services Active Directory. Par conséquent, le demandeur doit fournir toutes les informations requises pour l'identification.
- N'utilise pas de modèles de certificat.
- Définit le comportement par défaut pour toutes les requêtes de certificat en attente, jusqu'à ce qu'elles soient vérifiées par un administrateur d'AC autonome.

Dans notre cas, l'autorité de certification racine doit être hors ligne donc notre AC sera standard. Par contre l'autorité de certification secondaire doit être en ligne donc elle va être de type entreprise.

2.3. Choisir l'architecture AC

Après l'analyse de notre environnement, nous avons décidé de :

- Implémenter une infrastructure à clés publiques à deux niveaux.
- Vu qu'on est dans un environnement de test, l'autorité de certification (AC) va pris en charge des rôles de l'autorité d'enregistrement et l'autorité de dépôt.

Le schéma suivant nous montre l'architecture globale de notre infrastructure à clés publiques :

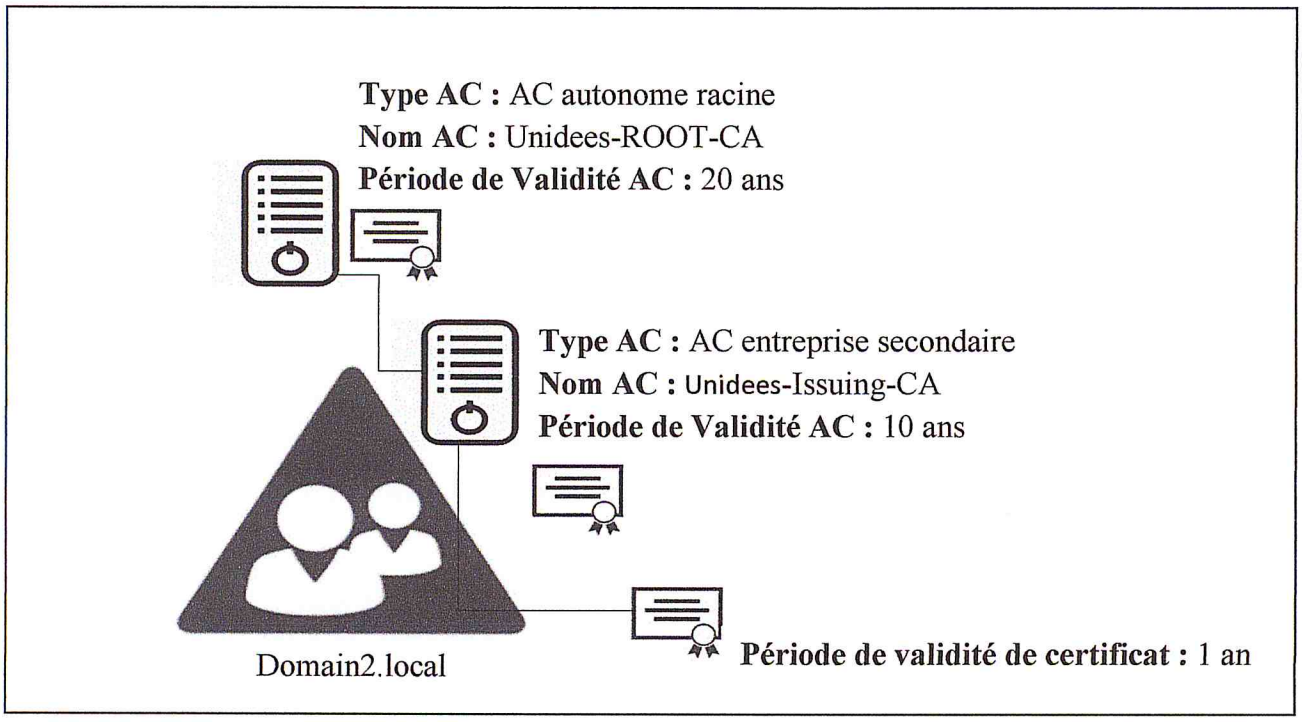


Figure 2.1 : Architecture globale de l'infrastructure à clés publiques UNIDEES

2.4. Le fichier CAPolicy.inf

Le fichier CAPolicy.inf définit les paramètres spécifiques aux AC racines ainsi que les paramètres qui affectent toutes les AC dans la hiérarchie de l'autorité de certification. Par défaut, le fichier CAPolicy.inf n'existe pas lorsque nous installons Windows Server 2008.Lorsque nous installons les services de certificats, le système d'exploitation applique les paramètres définis dans le fichier CAPolicy.inf **[2]**.

Il existe plusieurs sections prédéfinies dans le fichier CAPolicy.inf, chacune définissant des paramètres spécifiques pour les services de certificats **[2]**.

- **[Version] :** La section [Version] spécifie que le fichier INF utilise le format Microsoft Windows NT. Cette section doit exister pour l'installation d'AC racine et subordonnée.
- **[Certsrv_server] :** La section [certsrv_server] contient des entrées qui s'appliquent à toutes les AC de la hiérarchie de l'autorité de certification. Les entrées suivantes peuvent être définies dans cette section :
  - **RenewalKeyLength :** La longueur demandée de la clé privée et de la clé publique de l'autorité de certification lorsque le certificat AC est renouvelé. La valeur doit correspondre à la valeur attribuée à la longueur de clé de l'autorité de certification pendant l'installation initiale, sauf si une modification de la durée du certificat de l'autorité de certification se faite à l'heure de renouvellement.
  - **RenewalValidityPeriod :** L'unité de mesure de la période de validité. Les valeurs acceptées sont les années, les semaines et les jours, bien que l'utilisation de toute autre chose que les années soit rare.
  - **RenewalValidityPeriodUnits :** Le nombre spécifique d'unités pour la période de validité. Par exemple, si nous configurons une AC avec une période de validité de 10 ans, la valeur RenewalValidityPeriodUnits est 10.
  - **CRLPériode :** L'unité de mesure de l'intervalle de publication CRL. La valeur par défaut est les jours, mais les années, les semaines et les heures sont acceptables.
  - **CRLPeriodUnits :** Le nombre spécifique d'unités pour l'intervalle de publication CRL. La valeur par défaut est de sept, mais cette valeur est généralement modifiée en fonction de la conception de l'autorité de certification.

- **CRLOverlapUnits :** Fonctionne avec CRLOverlapPeriod pour spécifier la durée d'extension de la période de validité d'une CRL de base au-delà de l'intervalle de publication CRL de base spécifiée. Le CRLOverlapUnits est le nombre spécifique d'unités pour le chevauchement CRL de base.
- **CRLOverlapPeriod :** L'unité de mesure de la période de chevauchement CRL de base. La valeur par défaut est les jours, mais les années, les semaines, les minutes et les heures sont acceptables.
- **DiscreteSignatureAlgorithm :** L'option DiscreteSignatureAlgorithm, Lorsqu'elle est affectée d'une valeur de 1, permet de prendre en charge le format de signature PKCS#1 V2.1 (Public-Key Cryptography Standards) pour les certificats AC et les demandes de certificat AC. S'il est implémenté sur une autorité de certification racine, l'autorité de certification racine générera un certificat racine qui comprend le format de signature PKCS#1 V2.1. Si elle est implémentée sur une AC subordonnée, l'autorité de certification subordonnée génèrera une demande de certificat incluant le format de signature PKCS#1 V2.1.

2.5. Choix des modèles de certificats

Il y a deux méthodes différentes pour choisir notre propre certificat pour le cryptage et la signature :

- **Un seul certificat :** Consiste à utiliser le même certificat pour les opérations de signature et de cryptage.
  - **Avantage :** L'utilisateur doit gérer un seul certificat pour toutes les opérations.
  - **Inconvénient :** Si en met en œuvre l'archivage clé du certificat, il est possible qu'une autre personne puisse accéder à la signature de la clé privée associée au ce certificat.
- **Deux certificats :** Consiste à délivrer deux certificats distincts : un pour la signature numérique et un pour le cryptage.
  - **Avantage :** L'archivage de certificat de cryptage se faite correctement sans crainte de signer des imitations. La clé privée associée au certificat de signature n'est pas archivée, seule la clé privée pour le cryptage est archivée.

Après cet étude nous avons choisis de :

- Utiliser deux certificats pour le courrier électronique, un pour le chiffrement et l'autre pour la signature.
- Utiliser un seul certificat IPSec pour le VPN.

2.6. Diagramme de cas d'utilisation

Un diagramme de cas d'utilisation est un graphe d'acteur, un ensemble de cas d'utilisation englobés par la limite du système, des associations de communication entre les acteurs et les cas d'utilisation. Il est destiné à représenter les besoins des utilisateurs par rapport au système. **[13].**

La figure suivante montre le diagramme de cas d'utilisation de l'utilisateur :

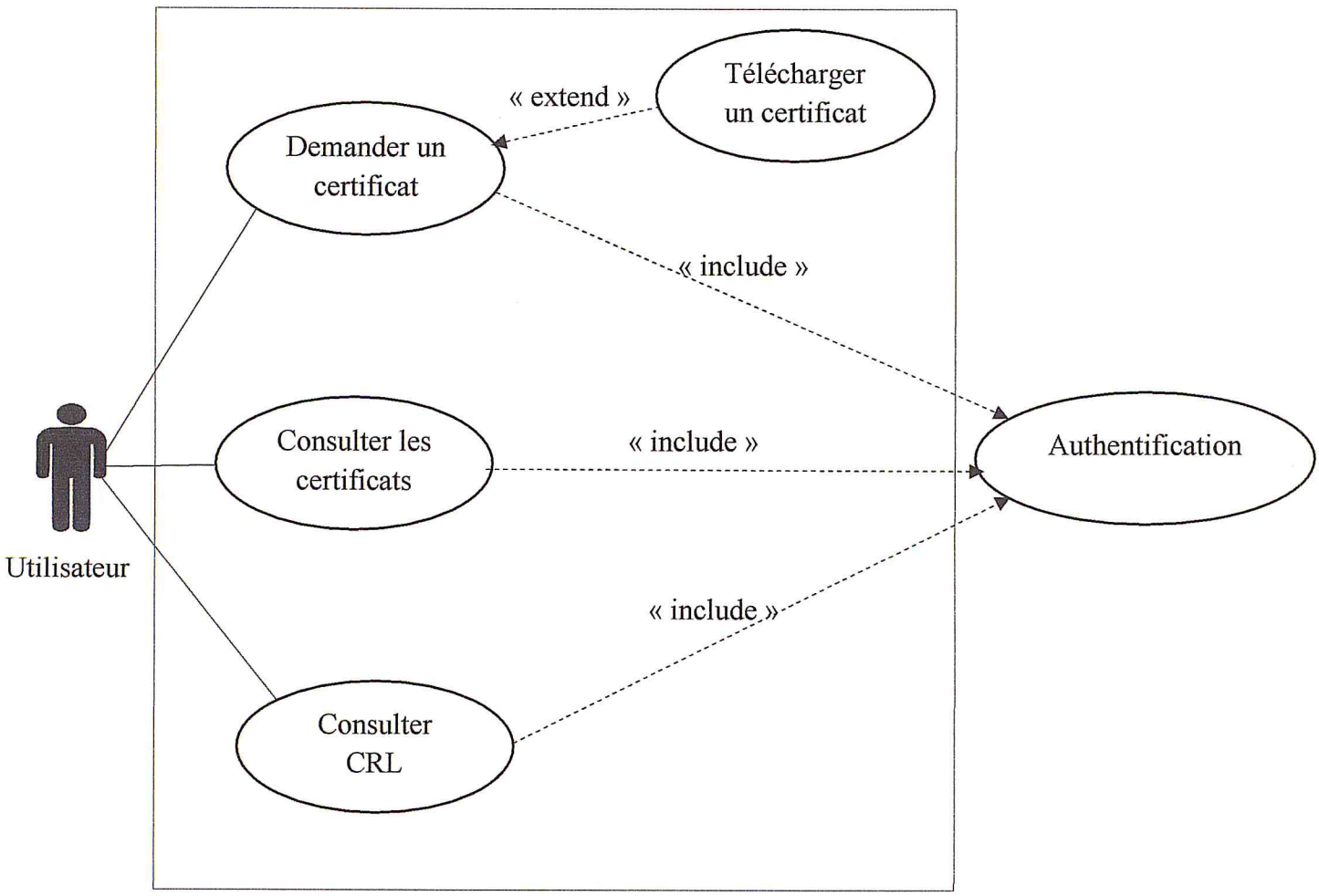


Figure 2.2: Diagramme de cas d'utilisation de l'utilisateur

Dans ce diagramme (**Figure 2.2**) nous donnons les différentes tâches exécutées par l'utilisateur. Après qu'il s'authentifie, l'utilisateur peut consulter les certificats et la CRL publier, demander un certificat et puis le télécharger.

La figure suivante montre le diagramme de cas d'utilisation de l'administrateur :

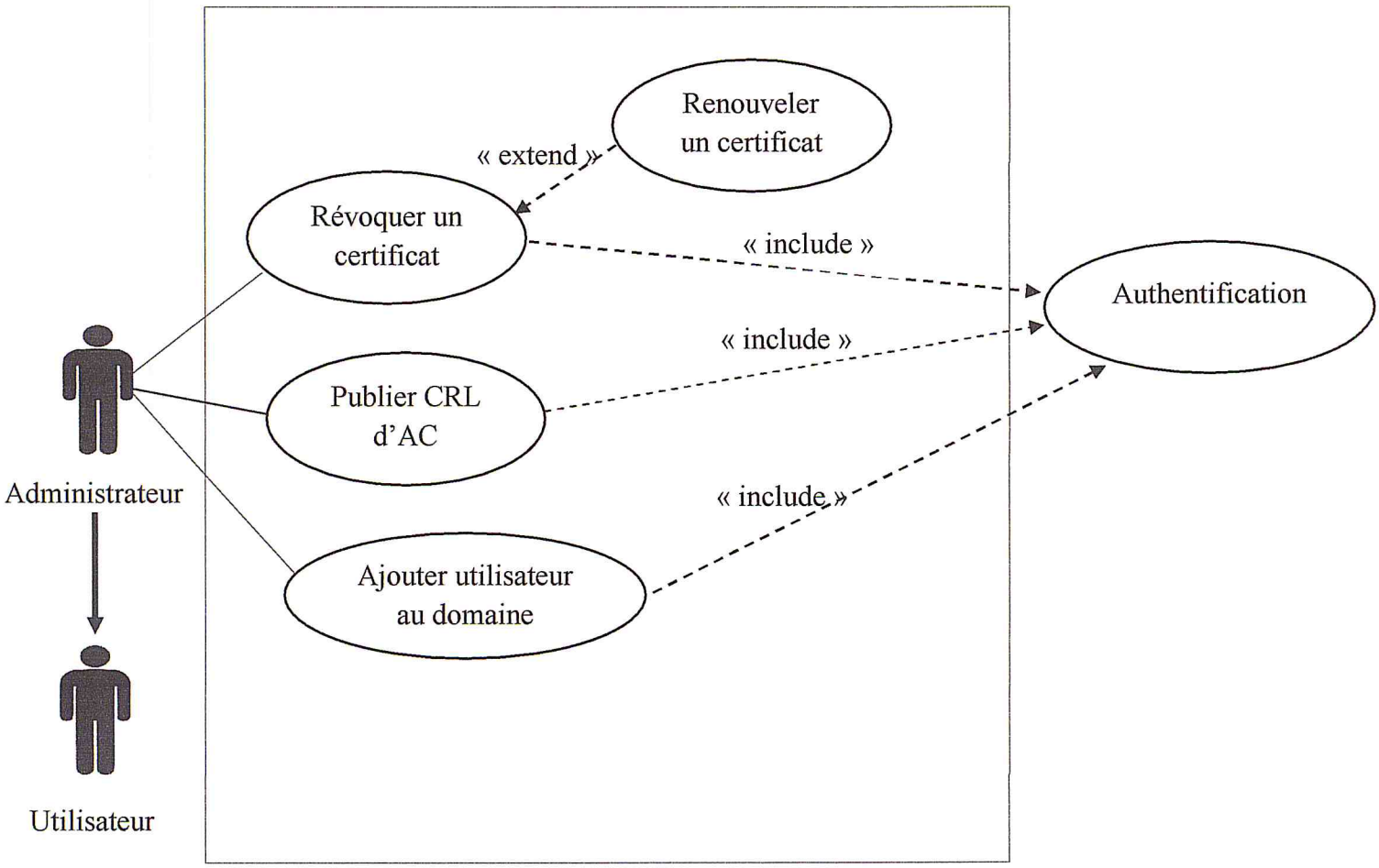


Figure 2.3: Diagramme de cas d'utilisation de l'administrateur

Dans ce diagramme (**Figure 2.3**) nous donnons les différentes tâches exécutées par l'administrateur. Il hérite les rôles de l'utilisateur en plus il peut révoquer ou renouveler un certificat, publier la CRL de l'autorité de certification et ajouter un utilisateur au domaine. Chaque opération nécessite l'authentification de l'utilisateur.

3. L'implémentation d'une PKI

Pour mettre en œuvre notre infrastructure à clés publiques, nous avons besoins de crier trois machines virtuelles pour l'Active Directory et les deux autorités de certification racine et émettrice.

3.1. Configuration d'Active directory

Active Directory (AD) est un service annuaire pour les systèmes d'exploitation Windows. Son principal objectif est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Le service d'annuaire Active Directory peut être mis en œuvre sur Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2012 et Windows server 2016 **[2]**.

Pour configurer le service de domaine active directory, il faut effectuer les étapes suivantes :

1. Cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Gestionnaire de serveur.
2. Dans la section Sommaire des rôles, cliquez sur Ajouter des rôles.
3. Si la page Avant de commencer s'affiche, cochez la case à cocher Passer cette page par défaut, puis cliquez sur Suivant.
4. Dans la page Sélectionner les rôles du serveur, activez la case à cocher Services de domaine Active Directory et lorsque le rôle est occupé, cliquez sur Suivant.

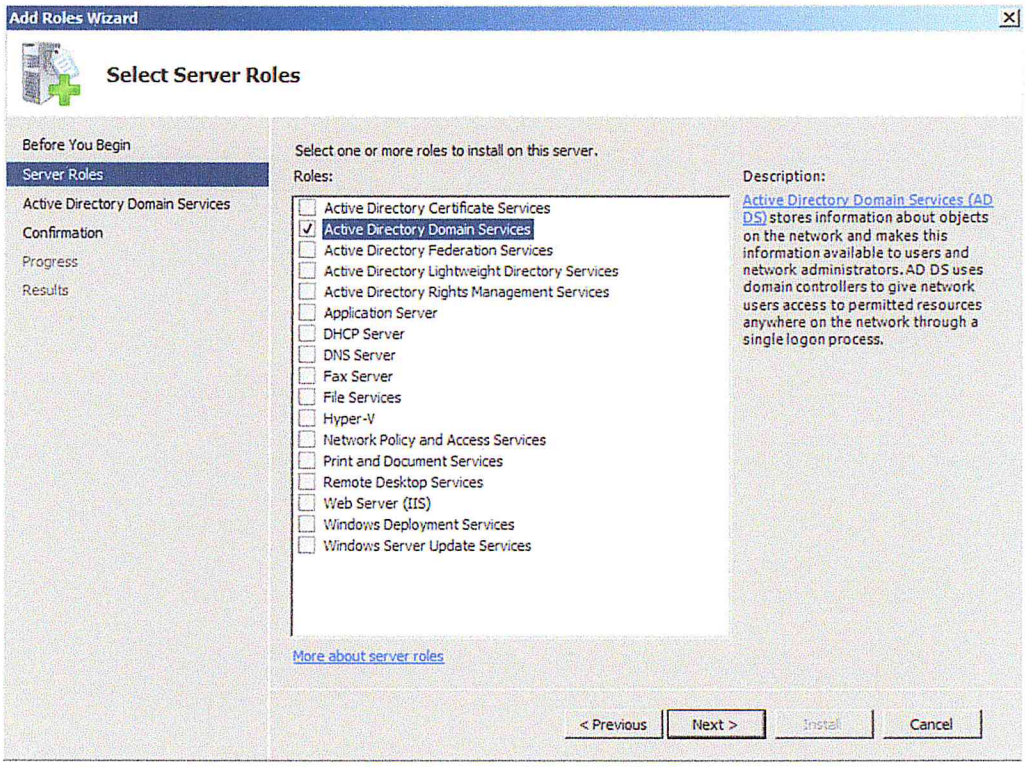


Figure 2.4 : Installation des services de domaine active directory

5. Dans la fenêtre qui s'affiche, confirmez l'installation de service de domaine AD.
6. Dans la page Résultats d'installation, examinez les informations sur l'écran de confirmation pour vérifier que l'installation a réussi, puis cliquez sur Fermer.

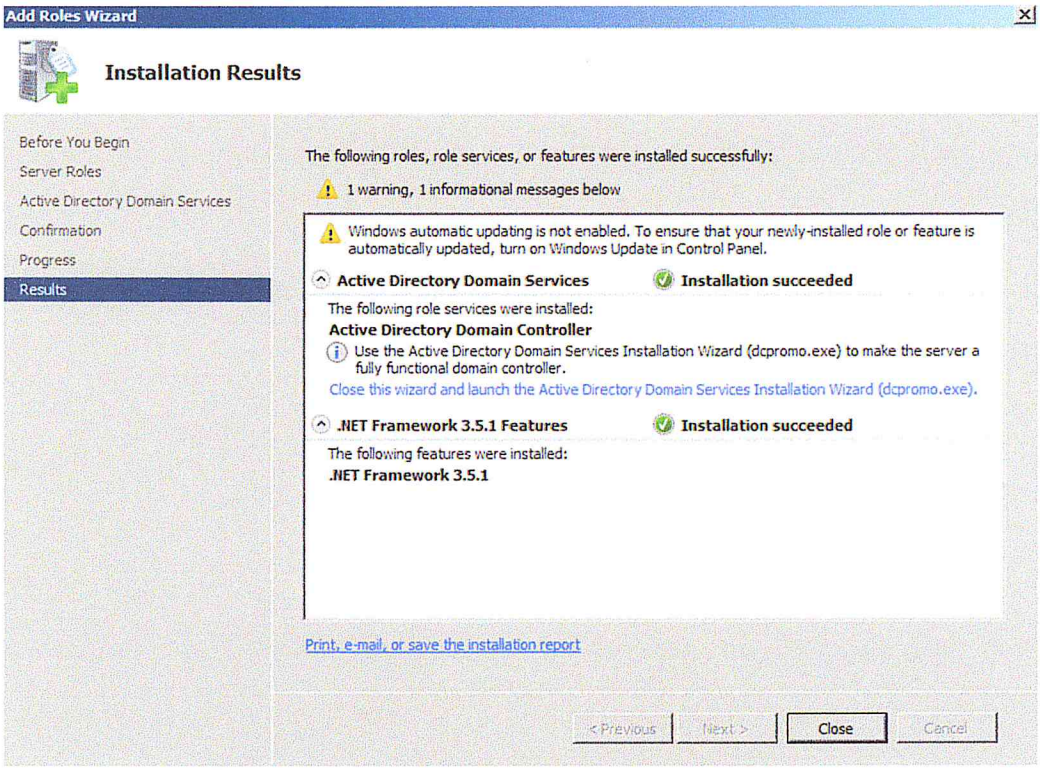


Figure 2.5 : Installation des services réussis

Après que l'installation est terminée, il faut ajouter le rôle contrôleur de domaine pour l'active directory. Pour faire cela il faut effectuer les étapes suivantes :

1. Dans la fenêtre Gestionnaire de serveur, cliquez sur service de domaine active directory, puis sur Exécuter l'assistant installation des services de domaine active directory (dcpromo.exe).
2. Dans la fenêtre Assistant d'installation des services de domaine active directory, cliquez sur créer un domaine dans un nouveau foret, puis cliquez sur suivant.

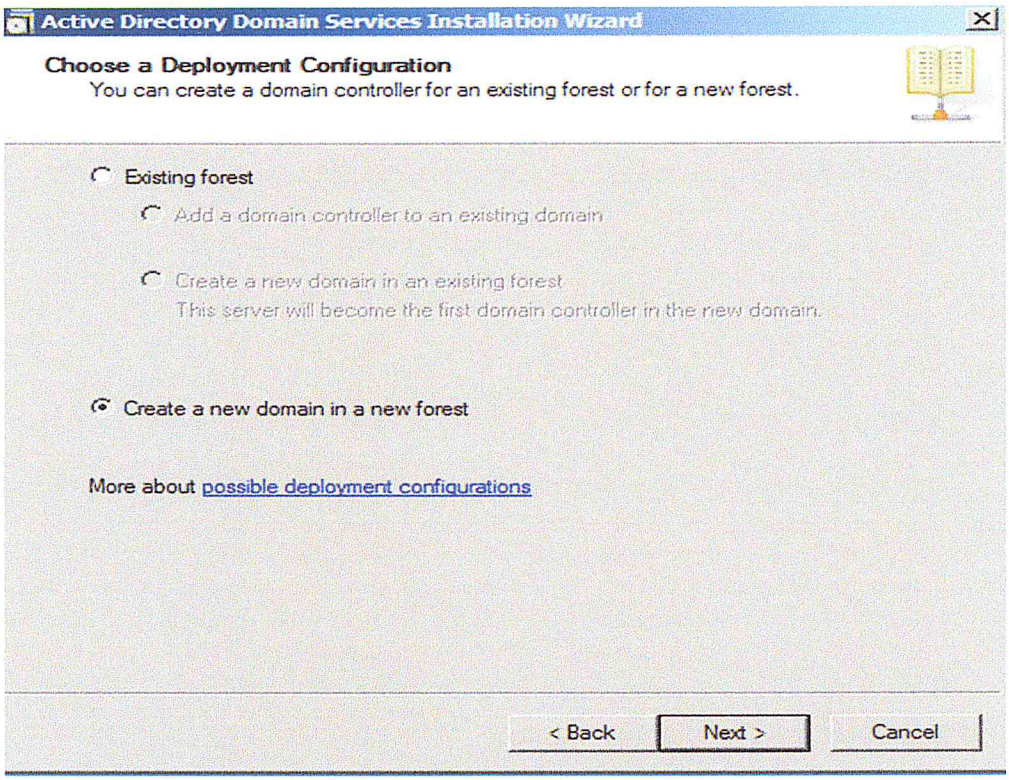


Figure 2.6 : Création d'un nouveau domaine

3. Choisissez un nom pour votre domaine (dans notre cas **domain2.local**), puis cliquez sur suivant.

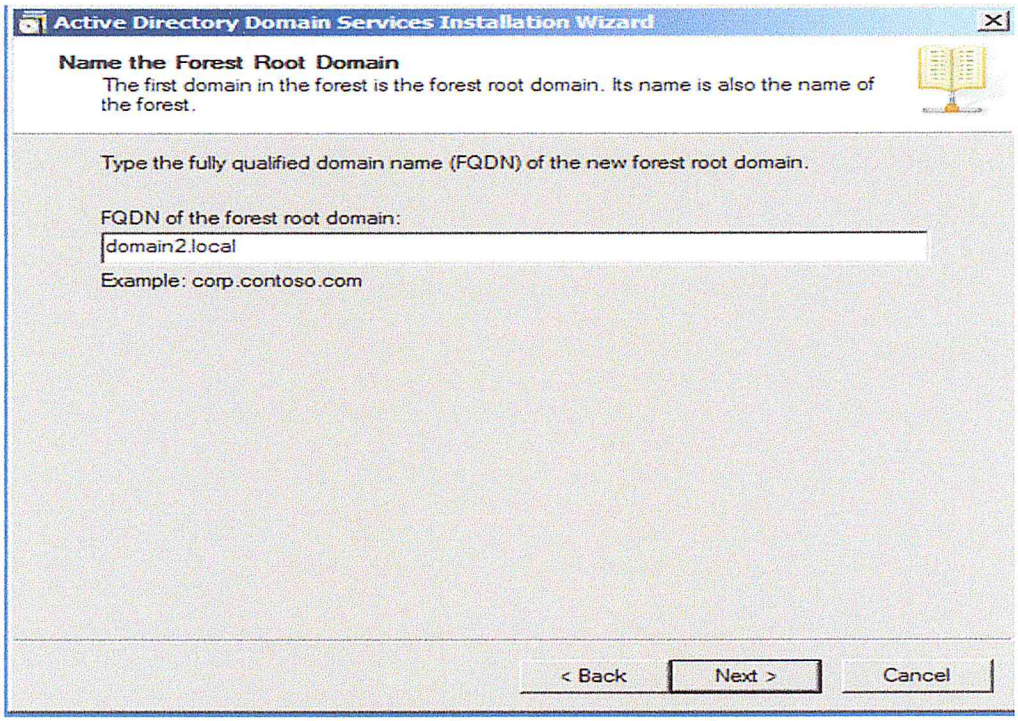


Figure 2.7 : Choisir un nom de domaine

4. Choisissez un mot de passe complexe, puis cliquer sur suivant.

5. Une fenêtre s'affiche pour redémarrer votre ordinateur, cliquez sur redémarrer.
6. Après le redémarrage de votre ordinateur votre mot de passe sera demandé pour terminer l'opération.

3.2. L'ajout d'une machine au domaine

Pour ajouter une machine au notre domaine, il faut d'abord configurer le DNS en suivant les étapes suivantes :

1. Ouvrir le centre réseau et partage.
2. Dans la fenêtre qui s'affiche cliquez sur Connexion au réseau local, puis cliquer sur propriété.
3. Dans la fenêtre Etat de connexion en réseau local, cliquez sur propriété, puis cliquez sur Protocole internet version 4 (TCP/IPv4).
4. Dans la case adresse DNS préféré, tapez l'adresse de votre serveur puis cliquer sur Ok, puis Fermer.

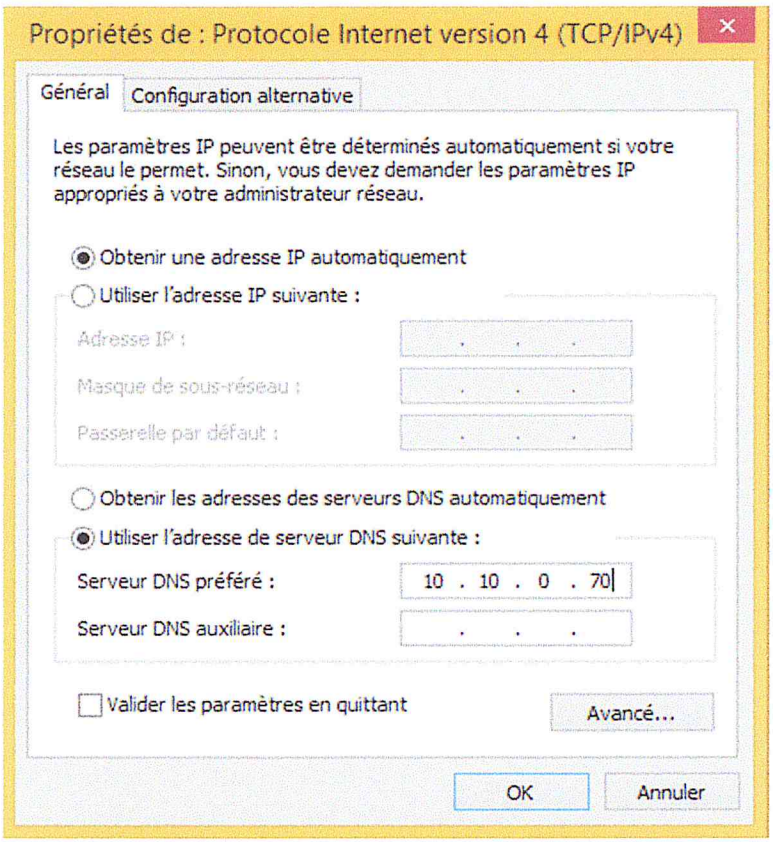


Figure 2.8 : Ajouter l'adresse DNS de serveur

Après que l'adresse DNS est configurée, on peut ajouter notre machine au domaine en effectuant les étapes suivantes :

1. Cliquez sur Démarrer, puis une clique droite sur Ordinateur, puis cliquez sur propriété.
2. Dans la fenêtre qui s'affiche, cliquez sur Paramètres système avancées, puis sur Nom de l'ordinateur, puis cliquer sur modifier.
3. Dans la fenêtre Modifier le domaine, cocher la case Domaine, puis tapez le nom de votre domaine et cliquez sur ok.

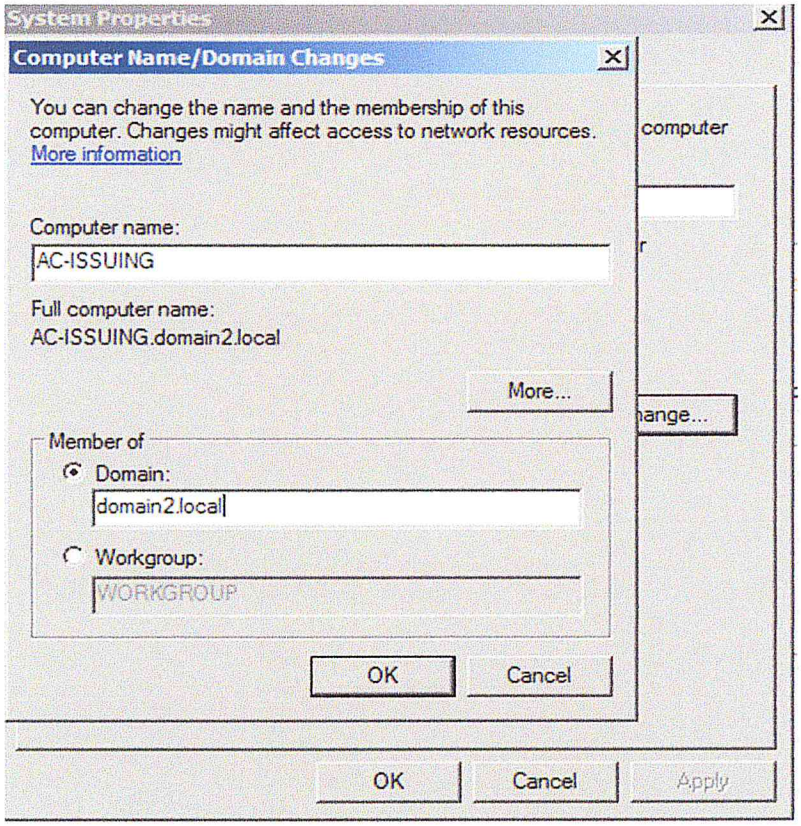


Figure 2.9 : Ajouter une machine au domaine

4. Dans la fenêtre de confirmation qui s'affiche, tapez Administrateur et votre mot de passe de domaine, puis cliquez sur ok.

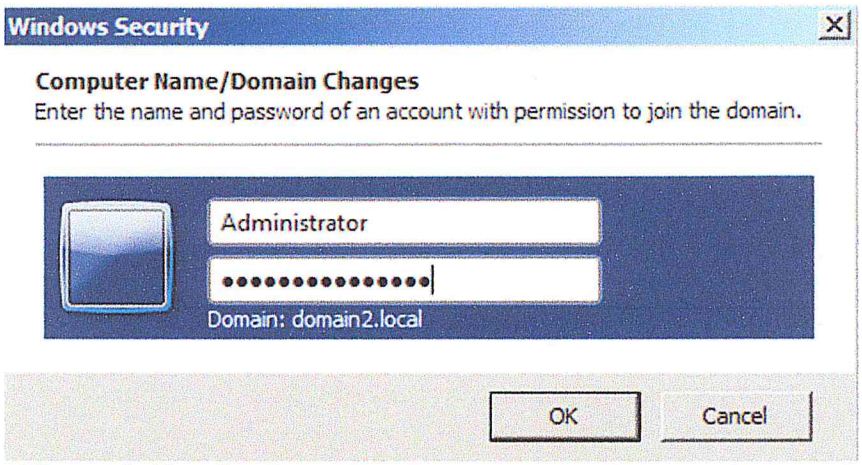


Figure 2.10 : Confirmation de nom et mot de passe de domaine

5. Une fenêtre sera affichée pour indiquer le réussisse de votre configuration

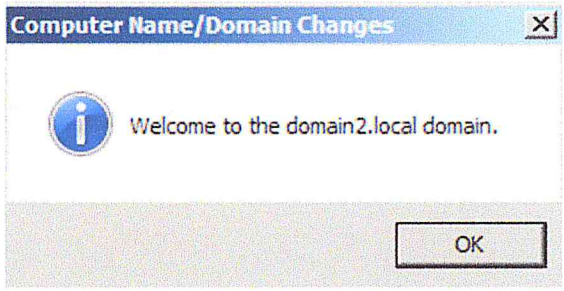


Figure 2.11 : L'ajout au domaine avec succès

3.3. Implémentation d'une hiérarchie AC

Comme on a choisi d'implémenter une hiérarchie AC a deux niveaux, il est temps de l'installer en suivant notre conception. L'implémentation d'une hiérarchie d'AC commence toujours par l'autorité de certification racine ensuite l'autorité de certification émettrice.

3.3.1. Installation d'une AC racine

Pour installer une autorité de certification racine, il faut établir les tâches suivantes :

- Configuration Prés-installation.
- Installation des services de certificats.
- Configuration post installation.

a. Configuration Pré-installation

Au niveau de cette tâche, nous devons créer notre fichier CAPolicy.inf. Ce fichier fait les hypothèses suivantes :

- L'autorité de certification racine utilise une longueur de clé de 2 048 bits.
- La période de validité du certificat de l'autorité de certification racine est de 20 ans.
- La CRL est publiée toutes les 26 semaines avec un chevauchement de 2 semaines.
- Les signatures discrètes doivent être activées dans le certificat AC racine pour permettre l'utilisation d'algorithmes CNG (Cryptography Next Generation) pour le hash et la signature des certificats.

Sur la base de ces hypothèses, on va créer manuellement le fichier CAPolicy.inf dans un dossier du système d'exploitation Microsoft Windows (**figure 2.12**)

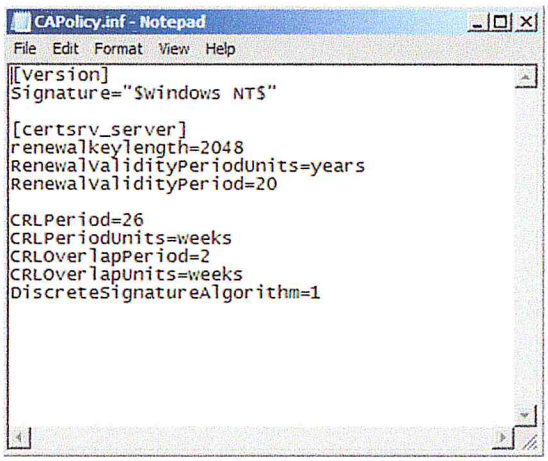


Figure 2.12 : Le fichier CAPolicy.inf pour AC racine

b. Installation des services de certificats

Une fois que le fichier CAPolicy.inf est crié, nous pouvons installer des services de certificats sur l'ordinateur d'AC racine. L'installation doit être effectuée par un membre du compte Administrateurs local sur l'ordinateur AC et l'ordinateur ne doit pas être membre d'un domaine. L'appartenance au domaine nécessiterait que l'ordinateur soit rattaché au réseau.
Pour installer l'autorité de certification racine d'entreprise, il faut effectuer les étapes suivantes :

1. Connectez-vous en tant que membre du groupe Administrateurs local.
2. Assurez-vous que la date et l'heure sur l'ordinateur AC racine est correcte.

3. Cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Gestionnaire de serveur.

4. Dans la section Sommaire des rôles, cliquez sur Ajouter des rôles.

5. Si la page Avant de commencer s'affiche, cochez la case à cocher Passer cette page par défaut, puis cliquez sur Suivant.

6. Dans la page Sélectionner les rôles du serveur, activez la case à cocher Services de certificats Active Directory et lorsque le rôle est occupé, cliquez sur Suivant.

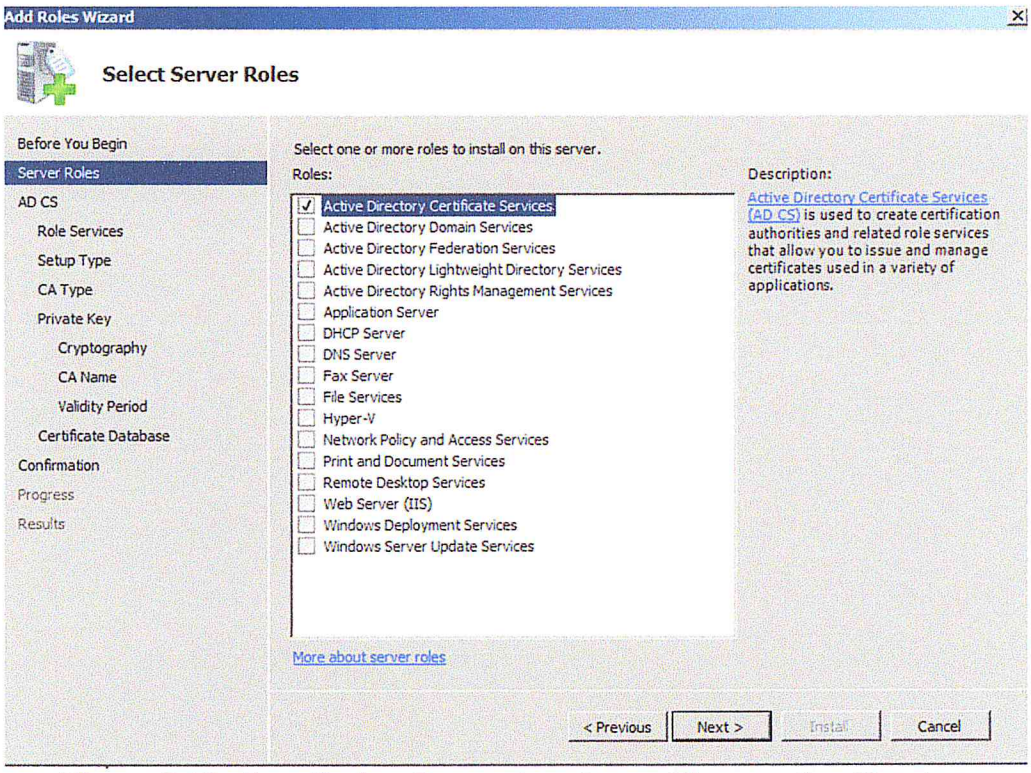


Figure 2.13 : Installation des services de certificats active directory

7. Dans la page Introduction aux services de certificats Active Directory, cliquez sur Suivant.
8. Dans la page Sélectionner les services de rôle, cochez la case Autorité de certification, puis cliquez sur Suivant.

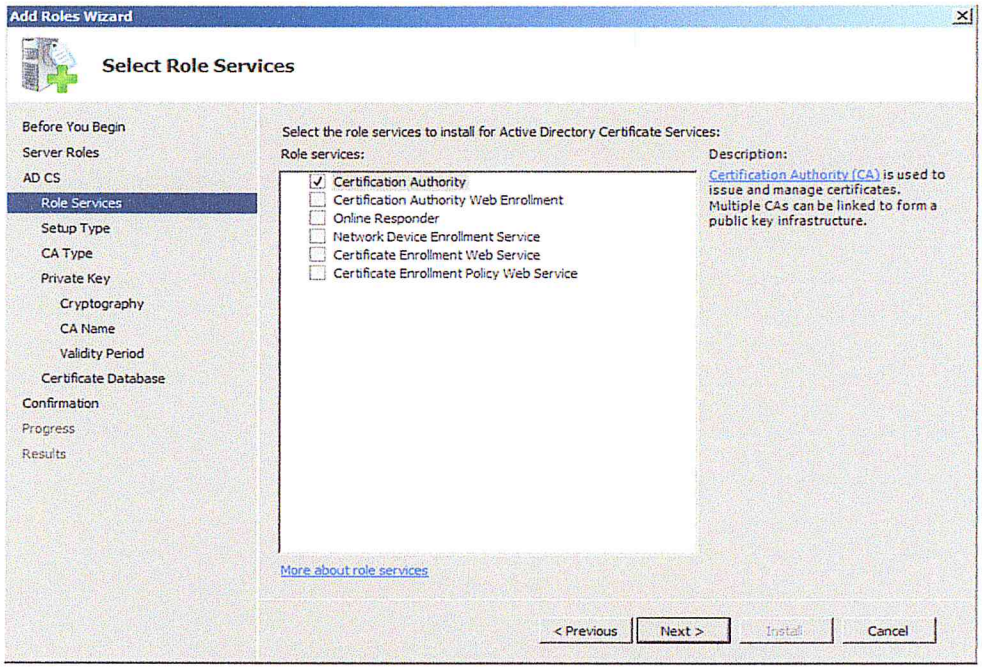


Figure 2.14 : Choisir le rôle autorité de certification

9. Dans la page Spécifier le type d'installation, cliquez sur Standard, puis cliquez sur Suivant.

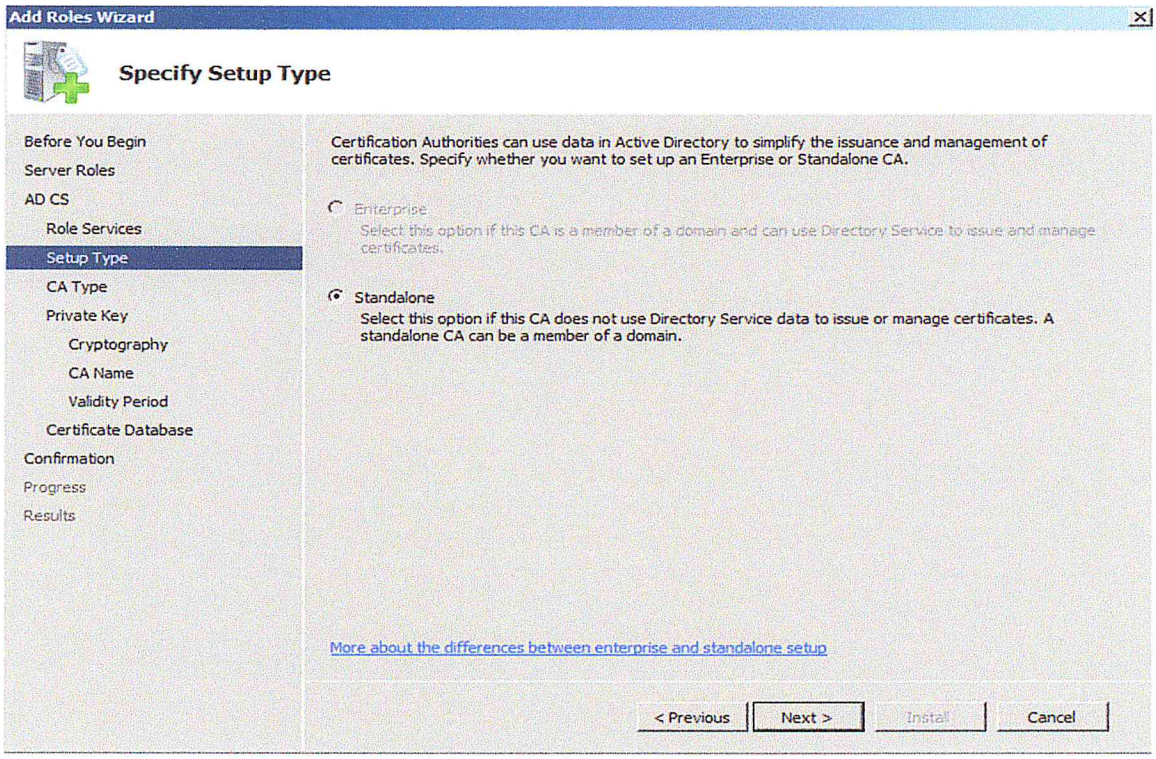


Figure 2.15 : Choisir le type de setup

10. Dans la page Spécifier le type d'AC, cliquez sur AC Racine, puis cliquez sur Suivant.

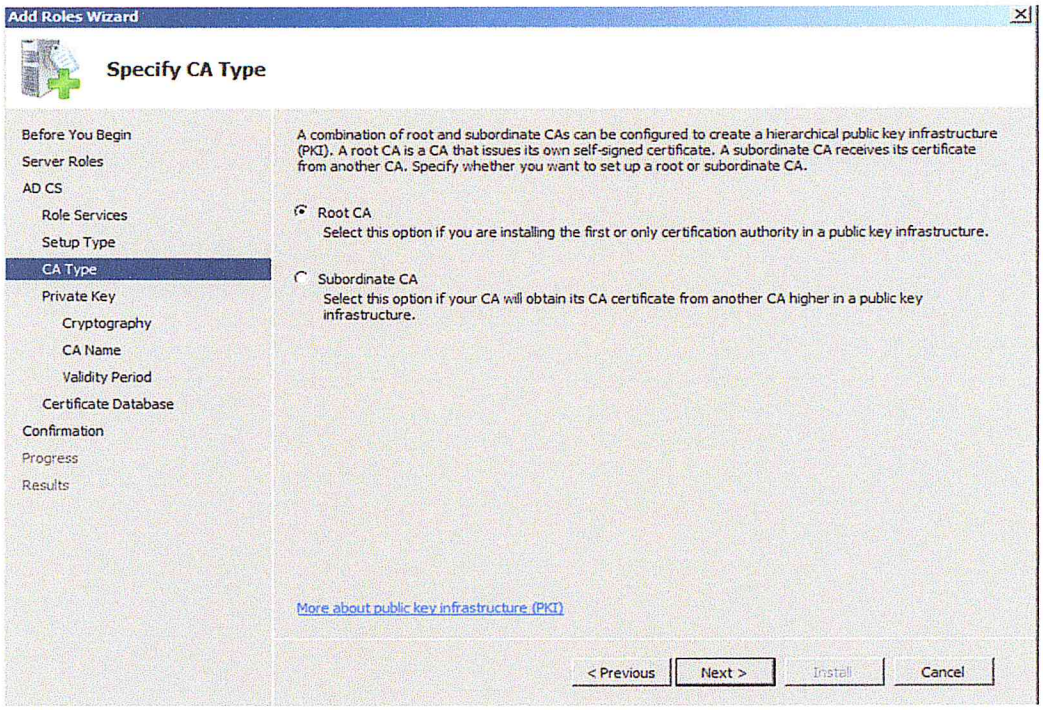


Figure 2.16 : Choisir le type d'AC

11. Dans la page Confirmer la clé privée, cliquez sur Créer une nouvelle clé privée, puis cliquez sur Suivant.
12. Sur la page Configuré la Cryptographie de AC, définissez les options suivantes, puis cliquez sur Suivant.
    - Sélectionnez un fournisseur de service cryptographique (CSP) : **RSA# Microsoft Software Key Storage Provider.**
    - Longueur du caractère : **2048**.
    - Sélectionnez l'algorithme de hash pour signer les certificats délivrés par cette Autorité : **sha256**.
13. Dans la page Configuré le nom de AC, fournissez les informations suivantes, puis cliquez sur Suivant.
    - Nom commun pour cette AC : **Unidees-ROOT-CA**.
    - Suffixe de nom distinctif : DC= **domain2**, DC = **local**.
14. Dans la page Définir période de validité, modifiez la période de validité à 20 ans, puis cliquez sur Suivant.
15. Dans la page Configuré la base de données des certificats, fournissez les paramètres suivants, puis cliquez sur Suivant :
    - Base de données de certificats : **D:\ CertDB**

- Journal de la base de données des certificats : **D:\ CertLog**

16. Après avoir vérifié les informations sur la page Confirmer les sélections d'installation, cliquez sur Installer.
17. Dans la page Résultats d'installation, examinez les informations sur l'écran de confirmation pour vérifier que l'installation a réussi, puis cliquez sur Fermer.

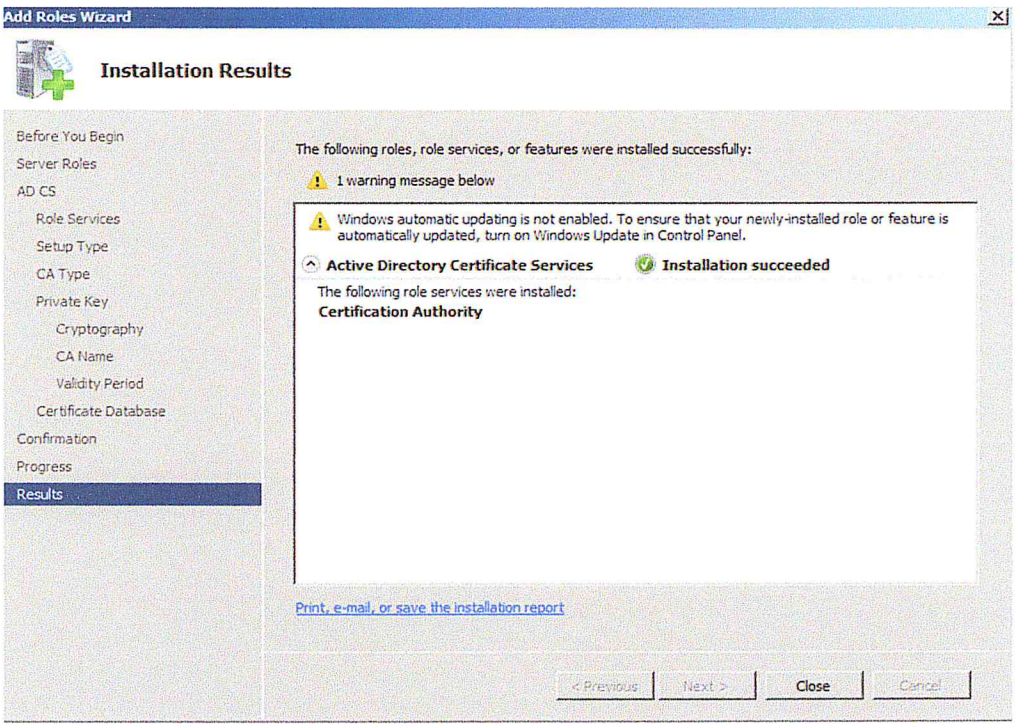


Figure 2.17 : Installation des services de certificats réussie

c. Configuration post-installation

Une fois que l'autorité de certification racine est installée, nous devons assurer que les paramètres de registre de l'autorité de certification racine sont configurés correctement. Les hypothèses suivantes sont faites en ce qui concerne notre réseau :

- L'autorité de certification secondaire sous l'autorité de certification racine dispose d'une période de validité de 10 ans.
- Toutes les options d'audit doivent être activées sur l'autorité de certification racine.
- Les signatures discrètes doivent être prises en charge et disponibles pour les demandes de certificats soumises à l'autorité de certification.

Le script de post-installation suivant peut configurer l'autorité de certification racine pour implémenter ces hypothèses de conception :

Script	But
certutil -setreg CA\DSConfigDN CN=Configuration, DC=domain2, DC=local	Declaration de la configuration
certutil -setreg CA\CRLPeriodUnits 26 certutil -setreg CA\CRLPeriod "Weeks" certutil -setreg CA\CRLOverlapPeriod "Weeks" certutil -setreg CA\CRLOverlapUnits 2	Définir les intervalles de publication CRL
certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\CertSrv\CertEnroll\%%3%%8.crl\ n6:http://%%1/ CertEnroll/ %%3%%8.crl"	Définir l'URL de publication de CRL de l'autorité de certification
certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\ n2:http://%%1/ CertEnroll /%%1_%%3%%4.crt"	Définir l'URL de publication de certificat de l'autorité de certification.
certutil -setreg CA\AuditFilter 127	Activer tous les événements d'audit pour l'autorité de certification racine
certutil -setreg CA\ValidityPeriodUnits 10 certutil -setreg CA\ValidityPeriod "Years"	Fixer une période de validité pour les certificats émis
Certutil -setreg CA\csp\DiscreteSignatureAlgorithm 1	Activer les signatures discrètes dans les certificats AC racine
certutil –crl	Publier la liste de révocation.

Table 2.1 : Le but de script post installation

Les variables utilisées dans la définition des URLs de publication des certificats et la CRL de l'autorité de certification sont définie dans le tableau suivant :

Variable	Description
%1	Nom de serveur web
%3	Nom de l'autorité de certification
%4	Nom de certificat
%8	Nom de CRL

Table 2.2 : Définitions des variables de configuration

3.3.2. Installation d'une AC émettrice

Le processus d'installation d'une AC émettrice en ligne est légèrement différent de celui de l'installation des AC hors connexion.

a. Configuration pré-installation

Avant l'installation des services de certificats sur l'autorité de certification émettrice, nous devons assurer que l'AC émettrice fait confiance à l'autorité de certification racine et peut télécharger le certificat d'autorité de certification et la CRL pour la vérification de révocation de certificats.

Ceci s'effectue en installant ou en publiant manuellement les certificats d'AC racine comme suit :

- **Installation de certificats localement à l'autorité de certification émettrice :** Nous pouvons installer manuellement les certificats dans le magasin d'ordinateurs local de l'autorité de certification émettrice.

  Le script suivant publie le certificat de l'autorité de certification racine et la CRL dans le magasin de machine local :

  ```
  for %%c in ("AC-root_Unidees-Root-CA.crt") do certutil -addstore -f Root "%%c"
  for %%c in ("Unidees-Root-CA.crl") do certutil -addstore -f Root "%%c"
  ```

- **Publication des certificats et CRL dans AD DS :** La méthode préférée pour publier les certificats AC et la CRL de la racine dans un environnement forestier est de les

publier dans AD DS. Lors de leur publication dans AD DS, les certificats AC et la CRL sont automatiquement téléchargés dans tous les membres de la forêt par auto-inscription.

Le script suivant publie le certificat de l'autorité de certification racine et la CRL dans AD

```
for %%c in ("AC-root_Unidees-Root-CA.crt") do certutil -dspublish -f "%%c"
for %%c in ("Unidees-Root-CA.crl") do certutil -dspublish -f "%%c"
```

- **Création de fichier CAPolicy.inf :** Une fois que les certificats AC et la CRL de la racine sont publiés, nous devons préparer un fichier CAPolicy.inf pour l'autorité de certification émettrice.

  Le fichier CAPolicy.inf pour une autorité de certification émettrice doit définir les paramètres de renouvellement de certificat et de publication CRL.

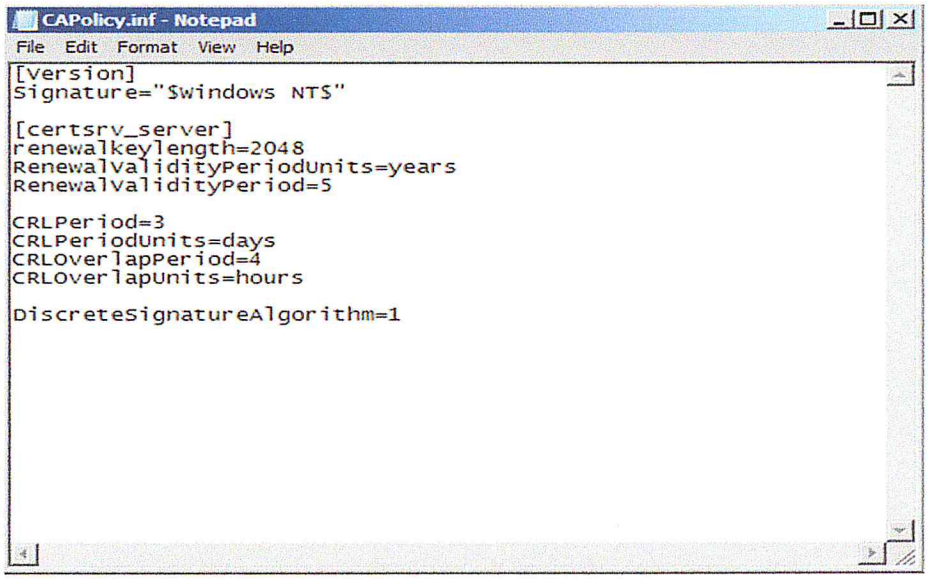


Figure 2.18 : Le fichier CAPolicy.inf pour AC émettrice

b. Installation des services de certificats

Une fois que le fichier CAPolicy.inf est en place, nous pouvons installer les services de certificats. Pour installer l'autorité de certification secondaire d'entreprise, il faut effectuer les étapes suivantes :

1. Assurez-vous que l'autorité de certification de l'entreprise est un membre d'un domaine dans la forêt.

2. Assurez-vous que la date et l'heure sont correctement définies.
3. Cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Gestionnaire de serveur.
4. Dans la section Sommaire des rôles, cliquez sur Ajouter des rôles.
5. Si la page Avant de commencer s'affiche, cochez la case à cocher Passer cette page par défaut, puis cliquez sur Suivant.
6. Dans la page Sélectionner les rôles du serveur, activez les cases à cocher Services de certificats Active Directory et serveur web (IIS), lorsque les rôles sont occupés, cliquez sur Suivant.
7. Dans la page Introduction aux services de certificats Active Directory, cliquez sur Suivant.
8. Dans la page Sélectionner les services de rôle, cochez la case Autorité de certification, puis cochez la case à cocher Inscription Web de l'autorité de certification.

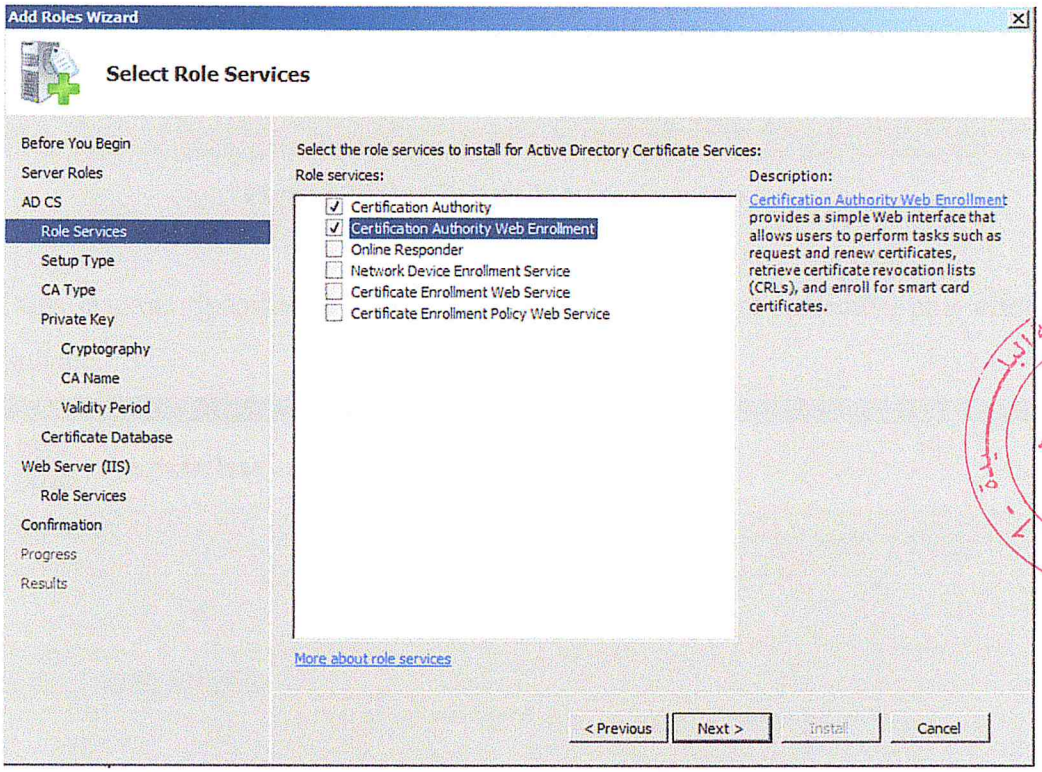


Figure 2.19 : Choisir les rôles autorité de certification et inscription web

9. Dans la page Sélectionner les services de rôle, cliquez sur Suivant.
10. Dans la page Spécifier le type d'installation, cliquez sur Enterprise, puis sur Suivant.

12. Dans la page Configurer la clé privée, cliquez sur Créer une nouvelle clé privée, puis cliquez sur Suivant.
13. Sur la page Configuré la cryptographie de AC, définissez les options suivantes, puis cliquez sur Suivant.
    - Sélectionnez un fournisseur de service cryptographique (CSP): **RSA# Microsoft Software Key Storage Provider**
    - Longueur du caractère : **2048**
    - Sélectionnez l'algorithme de hash pour signer les certificats délivrés par cette Autorité : **sha256**
14. Dans la page Configuré le nom de AC, fournissez les informations suivantes, puis cliquez sur Suivant.
    - Nom commun pour cette AC : **Unidees-Issuing-CA**
    - Suffixe de nom distinctif : DC = **domain2**, C = **local**
15. Sur la page Demande de certificat à partir d'une autorité de certification principale, cliquez sur Nom d'autorité de certification et sélectionner l'autorité de certification racine, puis cliquez sur Suivant.

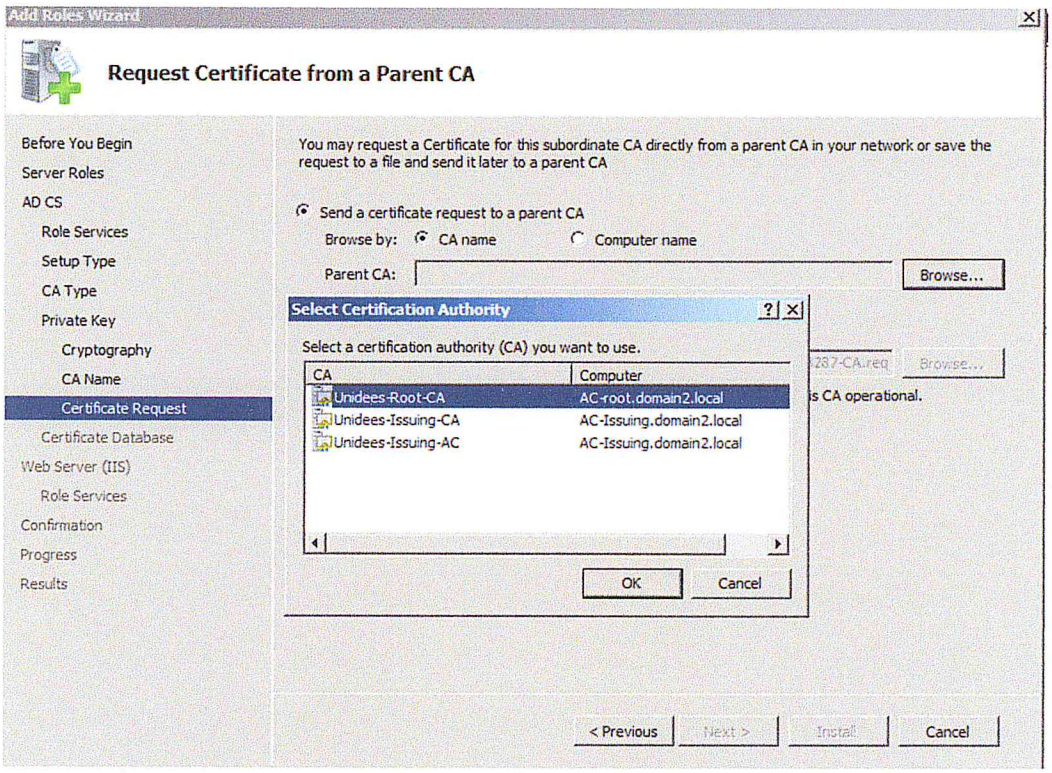


Figure 2.22 : Demander un certificat à partir d'une AC racine

16. Dans la page Configuré la base de données des certificats, fournissez les paramètres suivants, puis cliquez sur Suivant :
    - Base de données de certificats : **E: \ CertDB**
    - Journal de la base de données des certificats : **D: \ CertLog**
17. Sur la page Serveur Web (IIS), cliquez sur Suivant.
18. Dans la page Sélectionner les services de rôle, acceptez les services de rôle recommandés, puis cliquez sur Suivant.
19. Après avoir vérifié les informations sur la page Confirmer les sélections d'installation, cliquez sur Installer.
20. Dans la page Résultats d'installation, notez que l'installation des services de certificats Active Directory est incomplète alors que l'installation de Web Server (IIS) est terminée, puis cliquez sur Fermer.

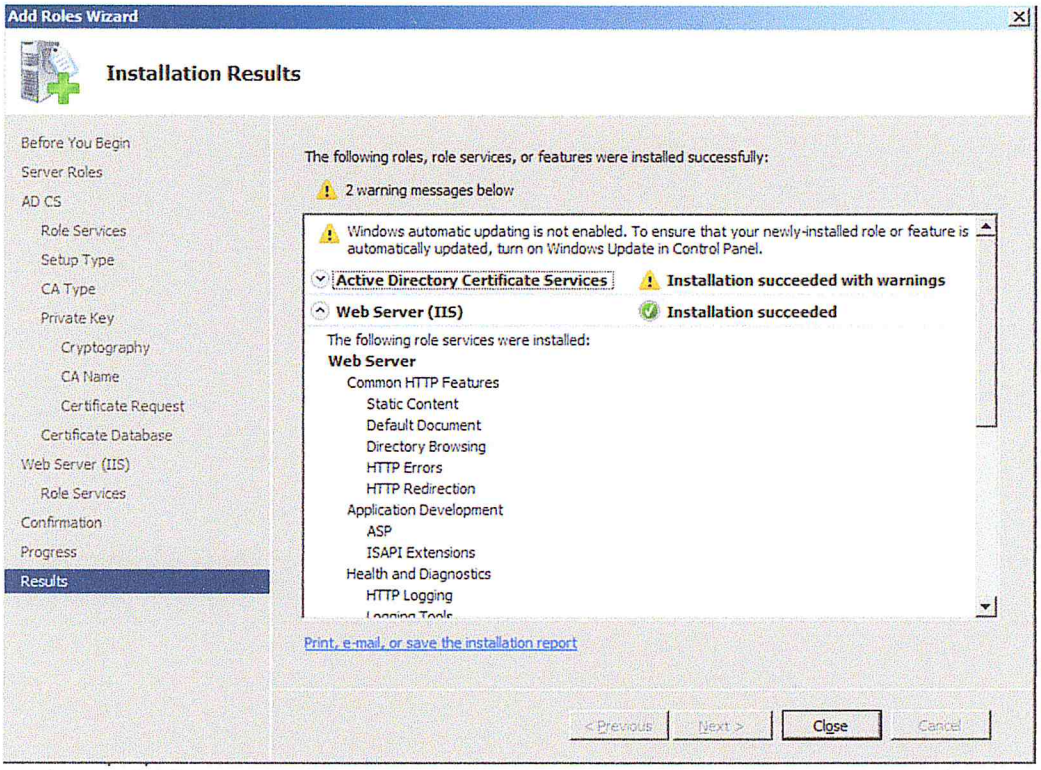


Figure 2.23 : Installation de serveur web et services de certificats réussie

c. Configuration post-installation

Une fois l'autorité de certification émettrice installée, nous devons assurer que les paramètres de registre de l'autorité de certification émettent correctement. Les hypothèses suivantes sont faites concernant notre réseau :

- Le certificat et la CRL de l'autorité de certification émettrice sont publiés dans AD DS et sur le service Web de l'autorité de certification émettrice.
- L'autorité de certification émet des certificats avec une période de validité maximale de 1 an - aux utilisateurs, aux ordinateurs, aux services et aux périphériques réseau.
- Toutes les options d'audit doivent être activées sur l'ordinateur AC émetteur.
- Les signatures discrètes doivent être prises en charge et disponibles pour les demandes de certificats soumises à l'autorité de certification.

Le script de configuration post-installation pour l'autorité de certification émettrice est le même avec le script de l'autorité de certification racine. La seule différence est la période de validité des certificats.

- Après la fin de l'installation de service les certificats et la CRL seront publiés dans l'interface « CertEnroll » qui peut être accéder par les utilisateurs pour les télécharger.

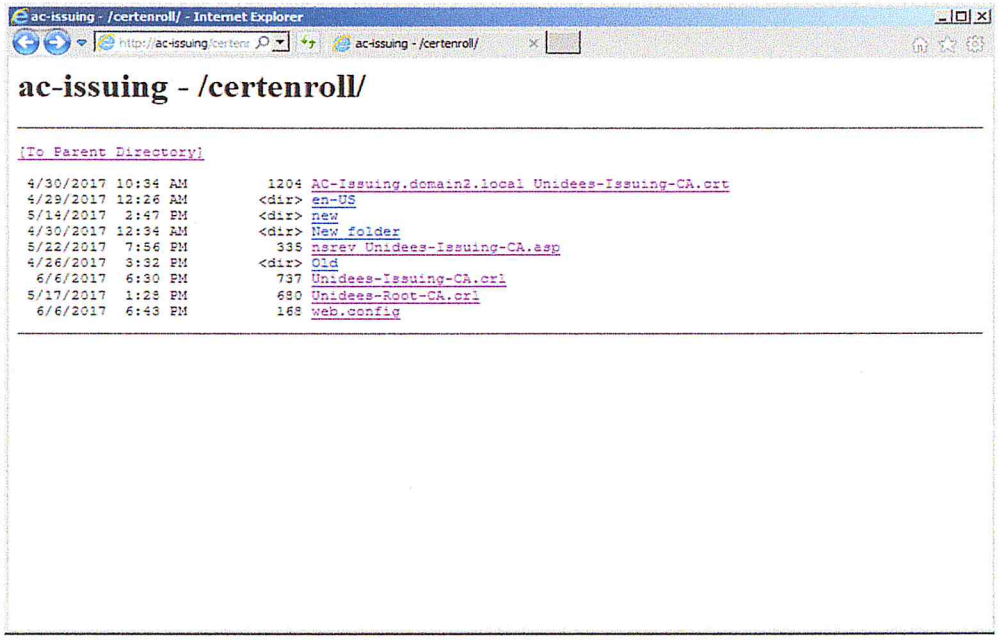


Figure 2.24 : L'interface CertEnroll

- L'autorité de certification émettrice obtient un certificat depuis l'autorité de certification racine. La **figure 2.25** montre le certificat en indiquant le chemin de confiance.

Figure 2.25 : Chemin de confiance

- L'installation de rôle Serveur Web (IIS) et le service Inscription Web de l'autorité de certification permet d'accéder au site web **Certsrv** (**Figure 2.26**) via l'URL **http://nom-serveur-web/certsrv** qui va nous permettre d'effectuer les trois opérations suivantes :

- **Demander un certificat :** Permet de demander plusieurs modèles de certificats.
- **Afficher le statut d'une requête de certificat en attente :** Permet dans le cas d'une autorité de certification autonome, d'afficher le statut d'un certificat et le récupérer après ayant été validé par l'administrateur.
- **Télécharger un certificat d'autorité de certification** : Permet de télécharger le certificat de l'autorité de certification ainsi que la liste de révocations des certificats de notre infrastructure.

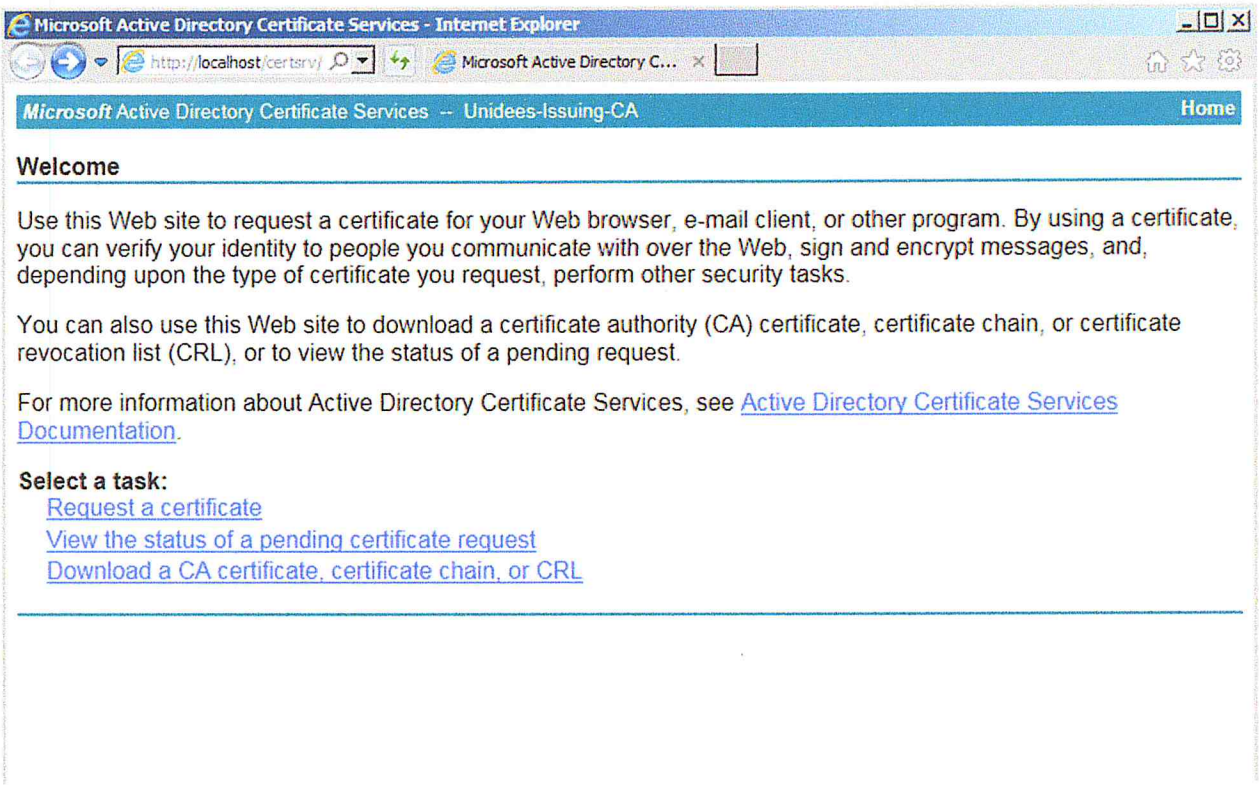


Figure 2.26 : Page d'accueil de l'interface web Certsrv

3.4. Révocation et renouvellement des certificats

Un certificat peut être révoqué à cause de plusieurs raisons. Par exemple si le certificat est devenu invalide pour une raison ou une autre, il doit être révoqué. Si la raison de révocation est annulée nous pouvons renouveler ce certificat.

3.4.1. Révoquer un certificat

Pour révoquer un certificat, nous devons effectuer les étapes suivantes :

1. Choisissez Démarrer → Programmes → Outils d'administration → Autorité de certification. La fenêtre Autorité de certification apparaît.
2. Dans le volet gauche de la fenêtre, sous Autorité de certification [Local], développez AC Entreprise.
3. Sélectionnez les certificats émis. La liste des certificats émis apparaît (**Figure 2.27**). Le volet droit répertorie tous les certificats émis.

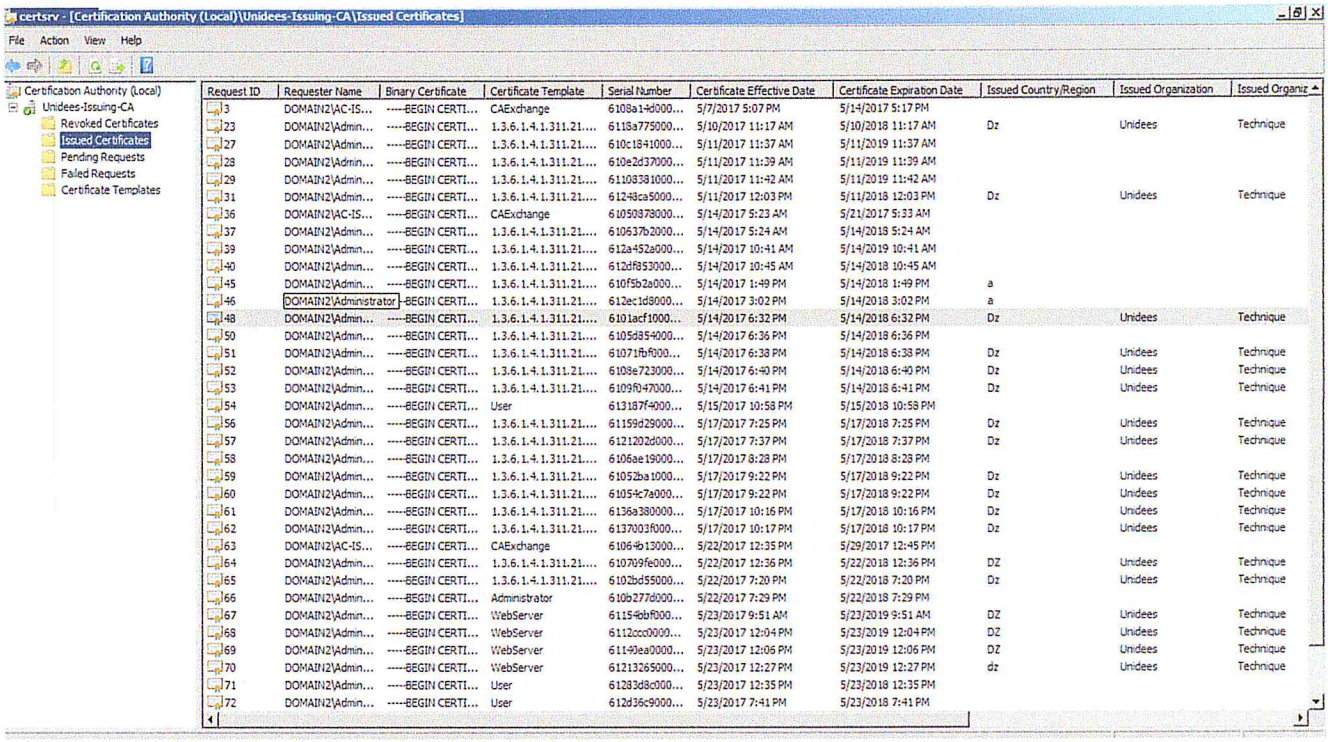


Figure 2.27 : Liste des certificats délivrés

4. Cliquez avec le bouton droit sur le certificat et sélectionnez Toutes les tâches → Révocation du certificat dans le menu contextuel. La boîte de dialogue Code de motif apparaît. Cette boîte de dialogue s'affiche à **la figure 2.28**. Il vous invite à préciser le motif de la révocation du certificat. Dans la liste des codes Reason, sélectionnez Key Compromise.

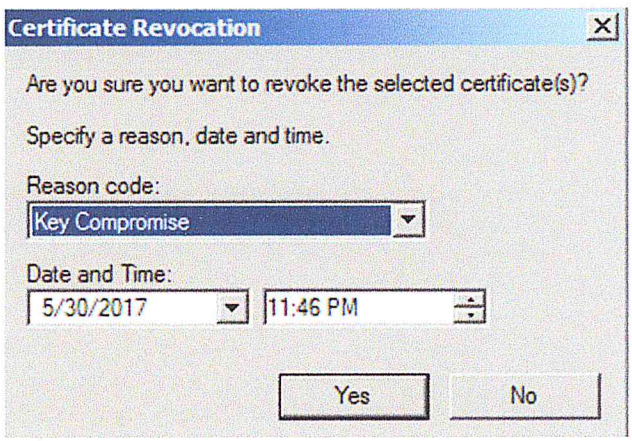


Figure 2.28: boîte de dialogue de la liste des raisons de révocations

5. Cliquez sur Oui pour révoquer le certificat.
6. Dans le volet droit, vous pouvez voir que le certificat que vous avez révoqué n'existe plus dans la liste des certificats émis.
7. Dans le volet gauche, sélectionnez Certificat révoqué. Dans le volet droit, le certificat que vous avez révoqué apparaît maintenant dans cette liste, comme le montre **la figure 2.29**.

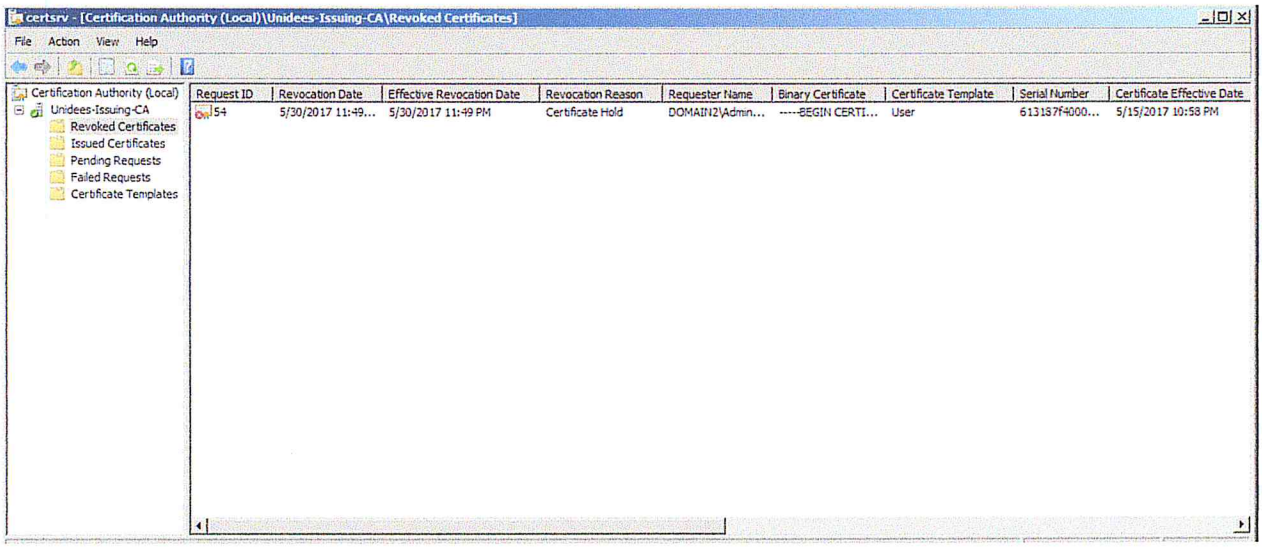


Figure 2.29 : la liste des certificats révoqués

3.4.2. Renouveler un certificat

Un certificat peut être renouveler si sa période de validité est expirée par exemple. Pour renouveler un certificat nous devons effectuer les étapes suivantes :

1. Dans le volet gauche de la fenêtre Autorité de certification, choisir votre certificat à renouveler.
2. Une clique droite sur le nom de certificat, puis sélectionnez Renouveler le certificat d'autorité de certification dans le menu Toutes les taches.

3.5. Publication de CRL d'AC

Une fois un certificat est révoqué, les informations de révocation sont publiées dans la CRL de l'autorité de certification. Nous devrions publier la CRL fréquemment parce qu'elle doit avoir des informations mises à jour à chaque fois qu'un certificat est révoqué. Pour publier la CRL, nous devons effectuer les étapes suivantes :

1. Dans le volet gauche de la fenêtre Autorité de certification, cliquez avec le bouton droit de la souris sur Certificats révoqués → Toutes les tâches → Publier.
2. Une boîte de message indique que la dernière CRL est toujours valide et peut être utilisée par les clients. Il vous demande si vous voulez toujours publier la nouvelle CRL.
3. Cliquez sur Oui pour publier la CRL.

4. La demande d'un certificat

Après avoir installé notre infrastructure à clés publiques, on peut demander un certificat de l'autorité de certification. Il y a plusieurs méthodes pour déployer les certificats personnalisés, parmi ces méthodes :

4.1. MMC (Microsoft Management Console)

MMC est un gestionnaire de console virtuelle incorporé dans Microsoft Windows qui sert de conteneur pour des interfaces graphiques de configuration. Elle permet d'effectuer plusieurs opérations, parmi les opérations qui nous intéressent **[5]** :

- La création d'une demande de certificat personnalisé.
- La demande d'un certificat.

L'opération « demande d'un certificat » va être détaillée dans la demande des certificats de signature et chiffrement.

4.2. Inscription web

Un utilisateur possédant une appartenance au domaine peut inscrire et demander des certificats en utilisant les pages d'inscription Web des services de certificats. Pour effectuer une nouvelle demande de certificat, les utilisateurs peuvent se connecter à l'aide d'un navigateur sur le site Web **http://ac-issuing/certsrv** (**Figure 2.30**).

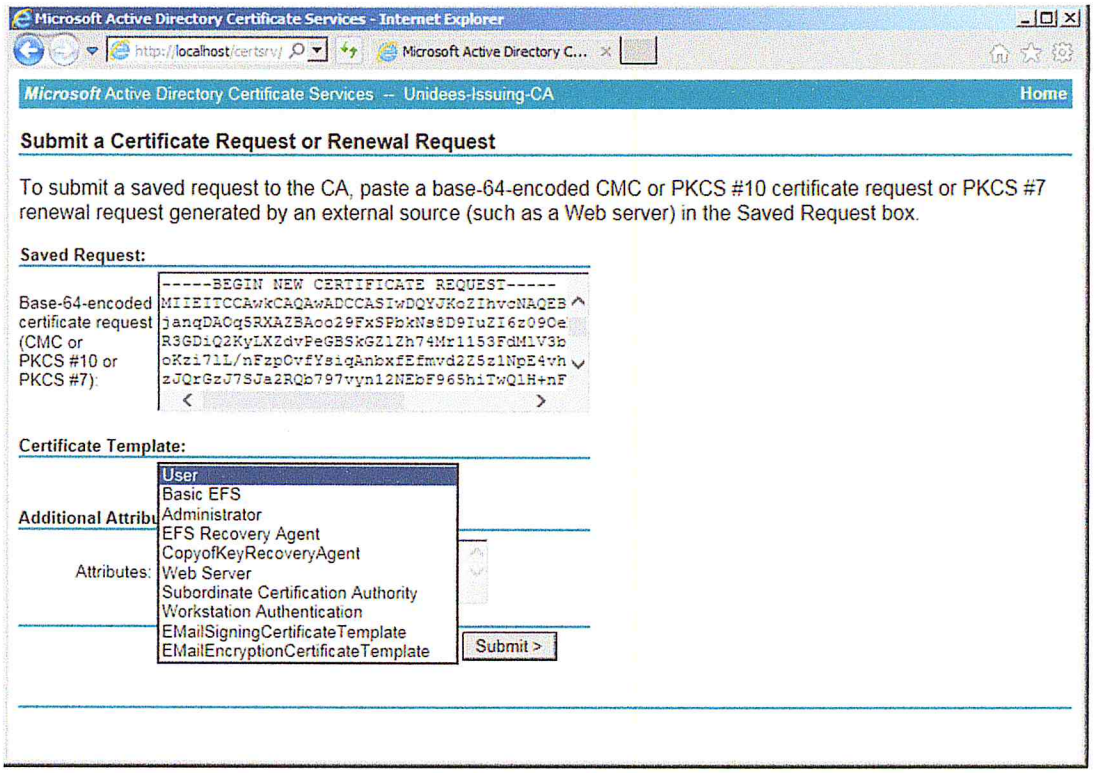


Figure 2.30 : Interface de demande d'un certificat

Pour demander un certificat, il faut tout d'abord ajouter une demande qui est générée dans la **MMC**, ensuite choisir un modèle de certificat (utilisateur, serveur web, chiffrement …) selon le besoin.

Après que le certificat a été délivré il faut le télécharger et l'installer (**Figure 2.31**).

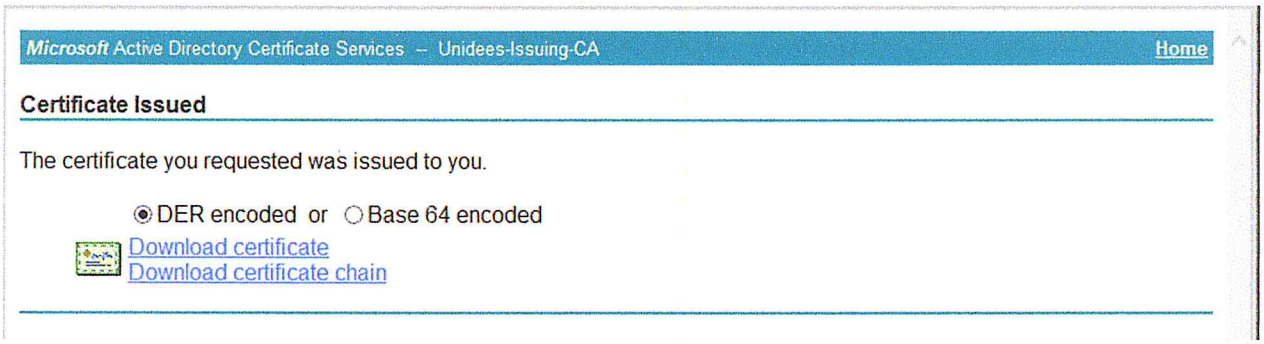


Figure 2.31 : Interface d'obtention de certificat

Pour faire confiance aux certificats émis par cette autorité de certification, il faut installer la chaîne de certificats d'autorité de certification.

5. Implémentation du SSL pour l'interface Certsrv

Il est possible de sécuriser les pages Web du serveur IIS à l'aide du protocole SSL (Secure Sockets Layer). Les données qui circuleront entre l'utilisateur et l'autorité de certification seront chiffrées.

5.1. Demande de certificat de serveur web

Pour demander un certificat de serveur web il faut suivre les étapes suivantes :

1. Dans les outils d'administrations cliquez sur Gestionnaire des services Internet (IIS).
2. Dans la console qui s'affiche, cliquez deux fois sur le nom de serveur.
3. Cliquez sur Certificats de Serveur, puis sur créer un certificat de domaine.
4. Remplissez les informations pour le certificat dans le formulaire qui s'affiche et cliquez sur suivant.

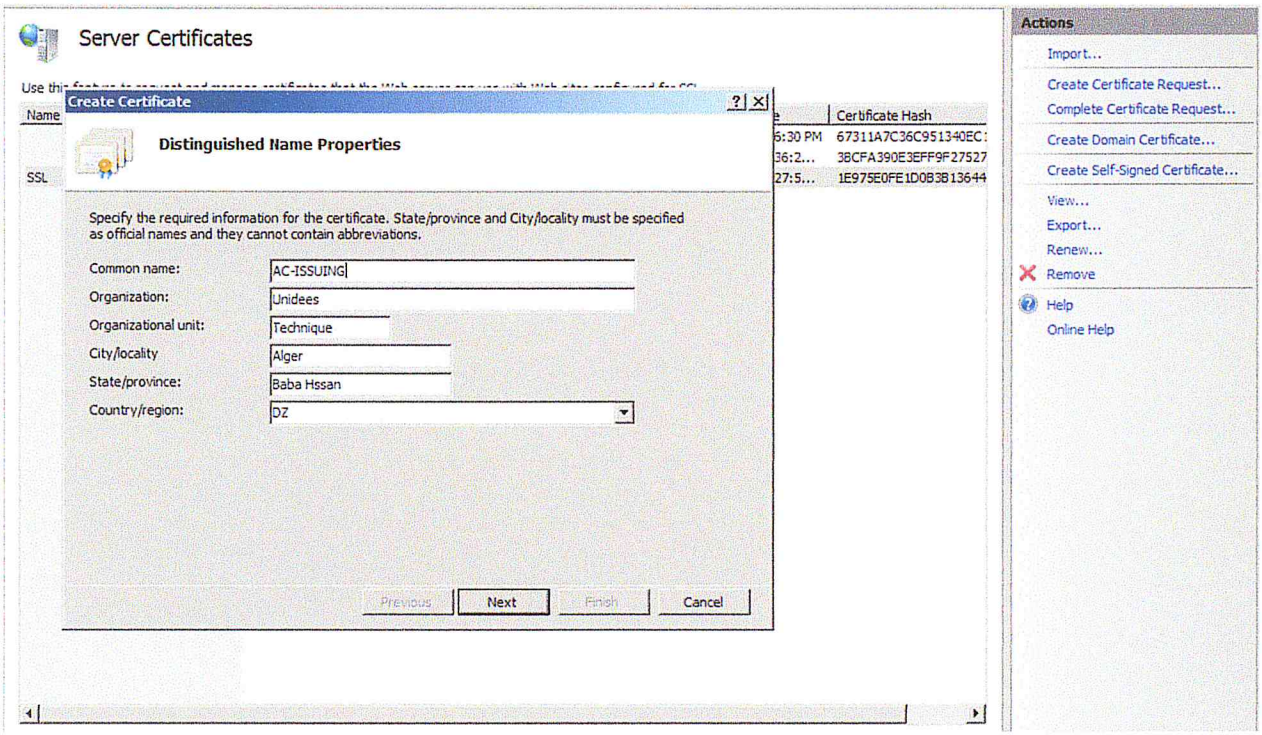


Figure 2.32 : Formulaire de création de certificat serveur web

5. Mentionnez l'autorité de certification qui va délivrer le certificat, puis nommez le certificat et cliquez sur terminer.
6. Le certificat serveur web sera ajouté au Certificats de Serveur.

5.2. Configuration de serveur web

Après avoir demandé le certificat de serveur web, il faut configurer le serveur pour lier le certificat avec l'interface Certsrv et activer le https. Pour cela il faut suivre les étapes suivantes :

1. Dans les outils d'administrations cliquez sur Gestionnaire des services Internet (IIS).
2. Dans la console qui s'affiche, cliquez deux fois sur le nom de serveur.
3. Cliquez sur Site Web par défaut, puis sur Bindings et puis sur ajouter.
4. Dans la fenêtre qui s'affiche sélectionnez le type https, puis choisissez le certificat de serveur web et cliquez sur OK, puis fermer.

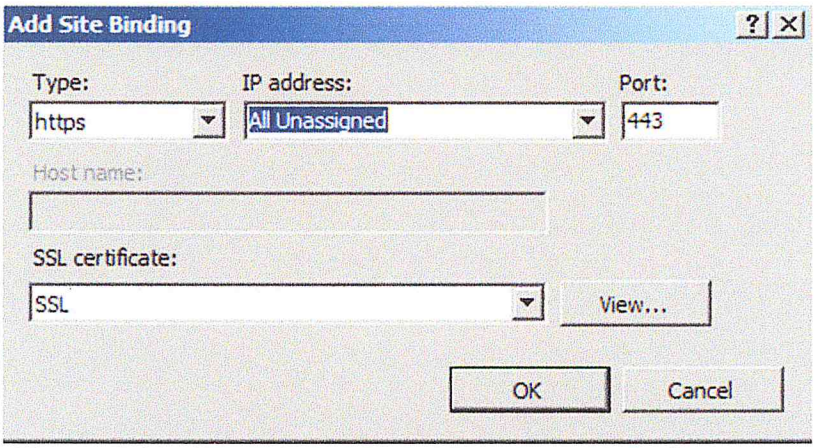


Figure 2.33 : La liaison de certificat avec l'interface certsrv

5. Dans la console de Gestionnaire des services Internet (IIS) cliquez sur le site Certsrv, puis sur paramètres de SSL.
6. Cochez la case Exiger SSL puis cliquez sur appliquer.

Figure 2.34 : Activation de SSL

6. Sécurisé les E-mails

Dans cette partie, nous avons besoin de crier deux autres machines virtuelles pour deux utilisateurs, ensuite nous devons installer Microsoft Office Outlook 2007 sur les deux machines pour faire une communication sécurisé par les emails.

En raison des risques liés à l'archivage de la clé privée associée à un certificat de signature S/MIME, nous mettrons en place des certificats distincts pour la signature et le cryptage par courrier électronique.

6.1. Modèle de certificat de signature numérique

Lors l'implémentation d'un modèle de certificat distinct pour la signature par courrier électronique, il est recommandé de dupliquer le modèle de certificat « Signature d'échange uniquement ».

Il est conseillé d'utiliser ces recommandations pour chaque onglet :

- **Onglet Général :** Dans l'onglet Général, il est recommandé de ne pas sélectionner la case à cocher Publier un certificat dans Active Directory. Un utilisateur ne doit pas récupérer le certificat de l'utilisateur pour vérifier la signature sur un message électronique, car le certificat est inclus dans la charge utile du message.
- **Onglet Gestion des demandes :** Lorsque on déployer le certificat de signature de courrier électronique comme un certificat stocké dans le profil de l'utilisateur, les paramètres suivants sont recommandés pour l'onglet Demande de traitement :
  - But : **Signature**.
  - Autoriser l'exportation de la clé privée : **désactivée**.
  - Demander l'utilisateur pendant l'inscription et exiger l'entrée de l'utilisateur lorsque la clé privée est utilisée : **activée**.
  - CSP: **Microsoft Enhanced Cryptographic Provider v1.0**.

- **Nom du sujet :** Activer le remplissage du sujet à partir des informations stockées dans AD DS. Aux fins de S/MIME, le sujet du certificat doit inclure l'adresse électronique de l'utilisateur dans le champ Sujet.
- **Sécurité :** Un groupe universel ou global personnalisé qui contient tous les utilisateurs qui effectuent la signature et le cryptage numériques S/MIME doit recevoir les autorisations Lecture, Enregistrement et Autorisation automatique.

6.2. Modèle de certificat de chiffrement

Lors l'implémentation d'un certificat distinct pour le cryptage du courrier électronique, il est recommandé de dupliquer le modèle de certificat de « User Exchange ». Le certificat de chiffrement de messagerie séparé nous permet d'activer l'archivage des clés pour le certificat de cryptage.

Les mêmes modifications recommandées pour la signature et le certificat de cryptage. La seule différence concerne les paramètres de l'onglet Général et l'onglet Gestion des demandes.

- **Onglet Général :** Sélectionner la case à cocher Publier un certificat dans Active Directory afin que les autres utilisateurs puissent récupérer le certificat de l'utilisateur à partir du catalogue global lors de l'envoi d'un courrier électronique chiffré à l'utilisateur.
- **Onglet Gestion des demandes :** Les paramètres suivants sont recommandés :
  - But : **Cryptage**
  - Clé privée du cryptage du sujet de l'archive : **activée**.
  - Inclure des algorithmes symétriques autorisés par le sujet : **activé**
  - Autoriser l'exportation de la clé privée : **activée**
  - Demander l'utilisateur pendant l'inscription et exiger l'entrée de l'utilisateur lorsque la clé privée est utilisée : **activée**
  - CSP: **Microsoft Enhanced Cryptographic Provider v1.0**

6.3. Demande des certificats de signature et chiffrement

Pour obtenir les certificats de signature et chiffrement, nous avons utilisés la mmc. Pour cela il faut effectuer les étapes suivantes :

1. Ouvrez la console microsoft management.
2. Cliquez sur Fichier, puis sur Ajouter/Supprimer composant logiciel enfichable.
3. Ajoutez les certificats [compte utilisateur].
4. Une clique droite sur le repertoire Personnel
5. Choisissez toutes les taches et puis cliquer sur créer une demande de certificat
6. Cliquez suivant jusqu'arrivant a la page de selection de modèle de certificat demandée.
7. Choisissez les modèles de chiffrement et signature et puis cliquez sur inscrire.

Les **figures 2.35** et **2.36** montrent l'inscription des demandes de certificats et son resultats :

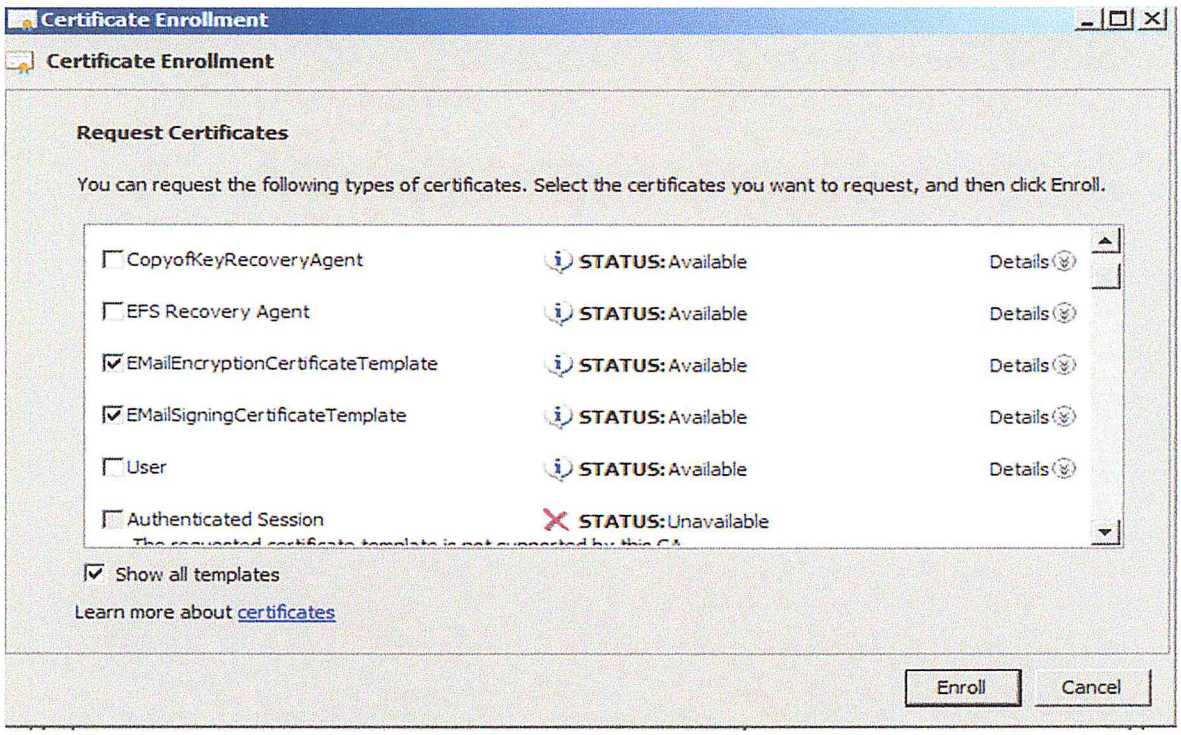


Figure 2.35 : Inscription de demande des certificats

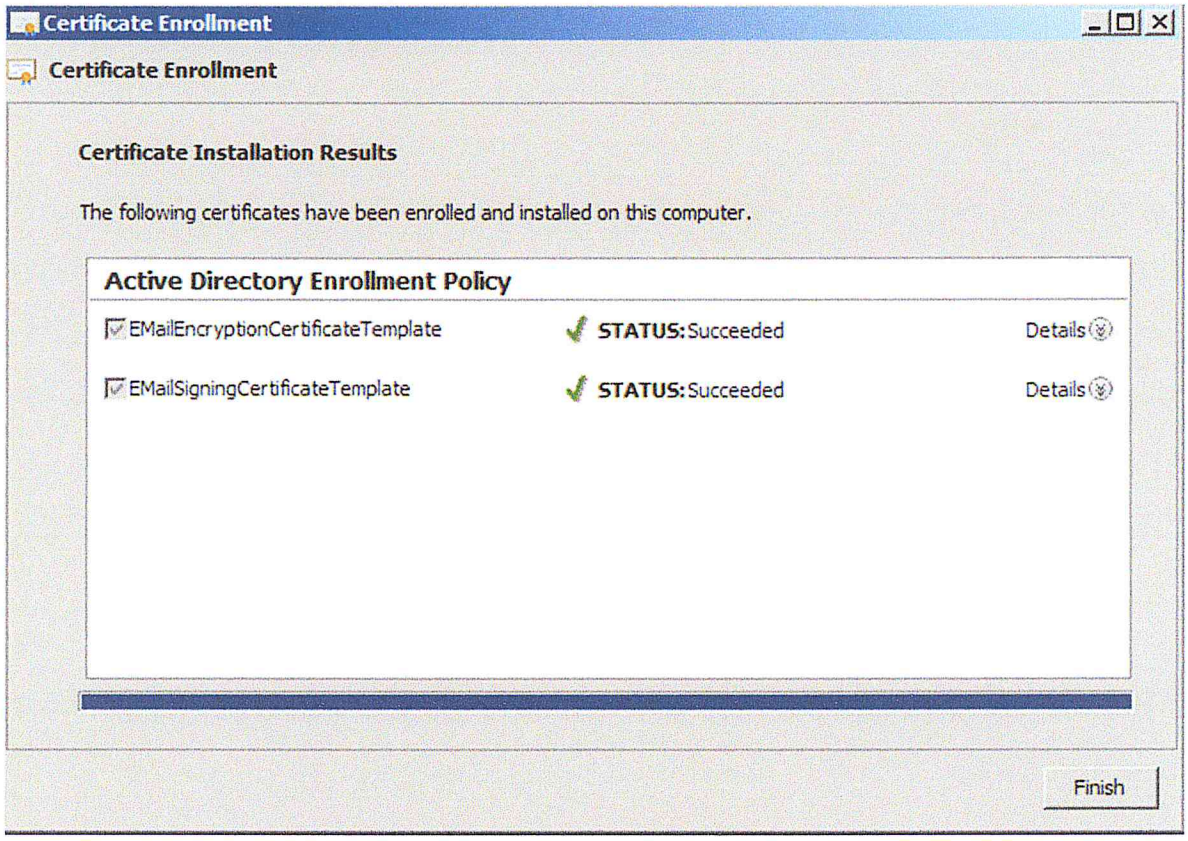


Figure 2.36 : Resultat d'inscription

6.4. Activation du courrier électronique sécurisé

Une fois que nous avons déployé les certificats avec succès aux utilisateurs, chaque utilisateur doit configurer sa demande de courrier électronique pour utiliser ces certificats de messagerie pour protéger les emails. La section suivante détaille comment activer la sécurité S/MIME dans Microsoft Office Outlook 2007.

On peut ajouter des certificats et spécifier les algorithmes de cryptage et de signature en utilisant la procédure suivante :

1. Ouvrez Outlook.
2. Dans le menu Outils, cliquez sur Centre de gestion de la confidentialité.
3. Dans la boîte de dialogue Centre de gestion de la confidentialité, cliquez sur Sécurité de messagerie électronique.
4. Dans la boîte de dialogue Modifier les paramètres de sécurité, assurez-vous que les paramètres suivants sont configurés (**Figure 2.37**) :
    - Cryptographie Format : S/MIME
    - Paramètres de sécurité par défaut pour ce format de message chiffré : **activé**
    - Paramètres de sécurité par défaut pour tous les messages chiffrés : **activé**
    - Algorithme de hachage : **SHA256**.
    - Algorithme de chiffrement : **AES (256 bits)**.
    - Envoyer ces certificats avec les messages signés : **activé**.

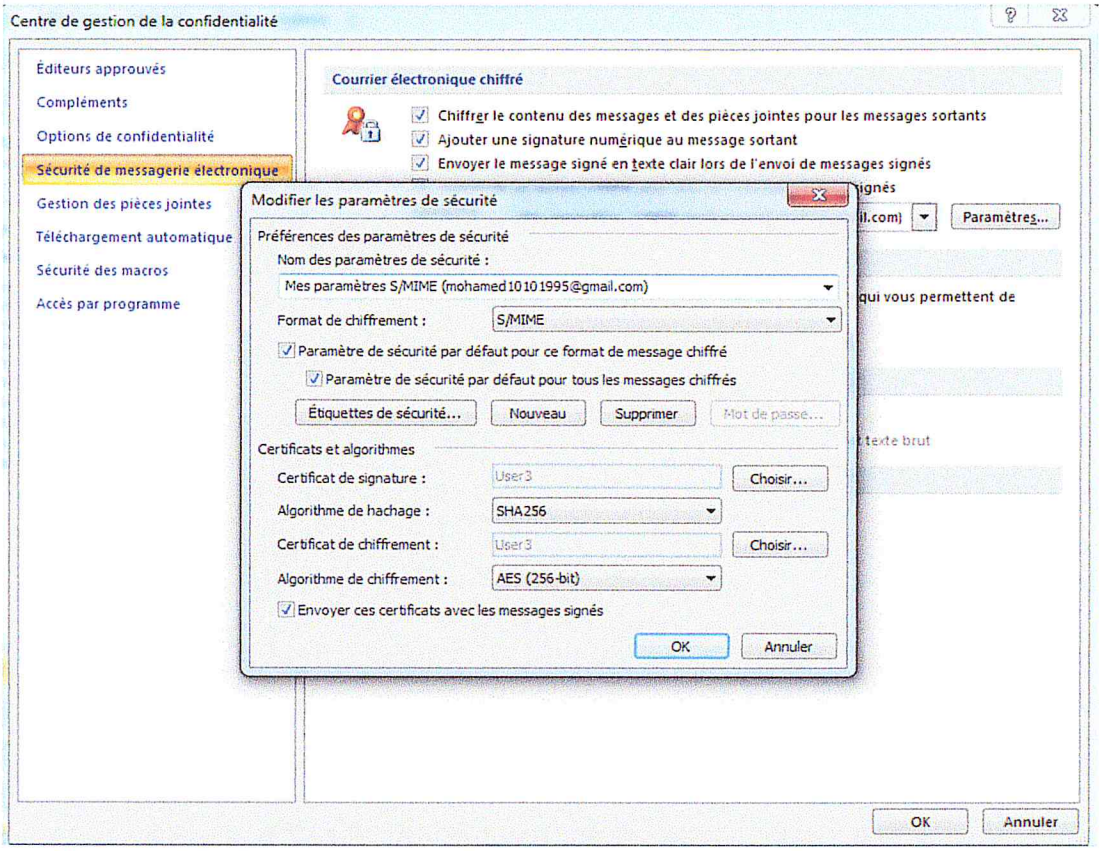


Figure 2.37 : Les paramètres d'activation de courrier électronique sécurisé

5. Dans la boîte de dialogue Modifier les paramètres de sécurité, cliquez sur OK.
6. Dans la boîte de dialogue Centre de gestion de la confidentialité, cliquez sur OK

6.5. Communication avec courrier électronique sécurisé

Une fois que le S/MIME est activé dans le courrier électronique, la décision d'envoyer un email sécurisé est faite pour chaque message envoyé par le participant par courrier électronique.

La **figure 2.38** montre une fenêtre de message dans Outlook 2007 qui est activée pour la signature numérique et le cryptage du courrier électronique. En sélectionnant le bouton Signature numérique et le bouton Chiffrer, l'expéditeur peut décider d'implémenter la signature, le cryptage ou le cryptage et la signature du message électronique sortant.

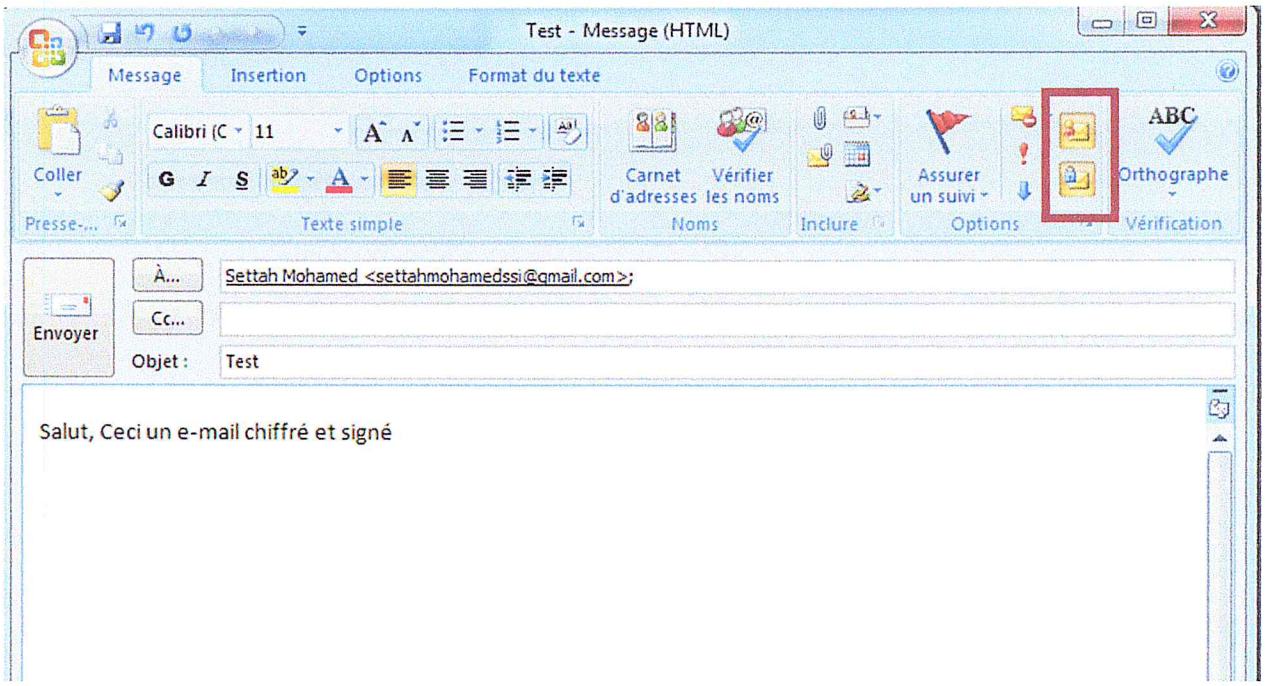


Figure 2.38 : L'envoi d'un message chiffré et signé

La **figure 2.39** montre que le récepteur a reçu un message chiffré et signé depuis l'émetteur.

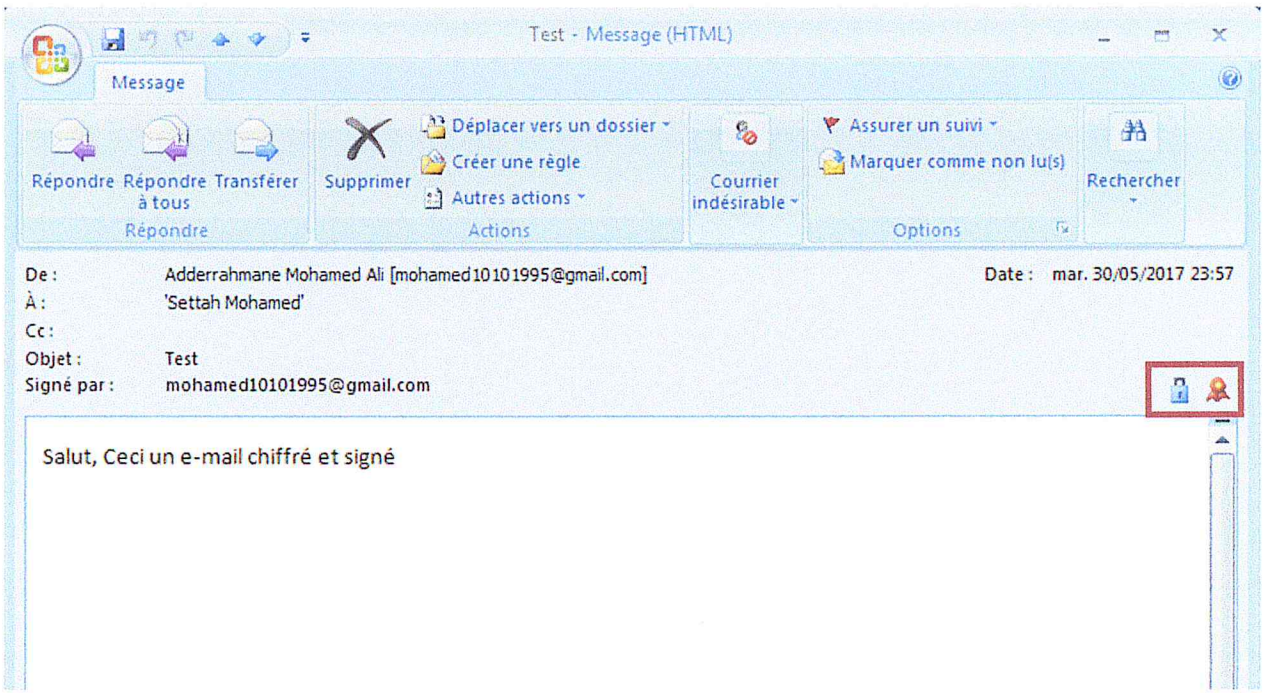


Figure 2.39 : Réception d'un message chiffré et signé

Si on clique sur les boutons de chiffrement ou signature on peut voir le certificat de l'émetteur comme la figure **2.40** illustre.

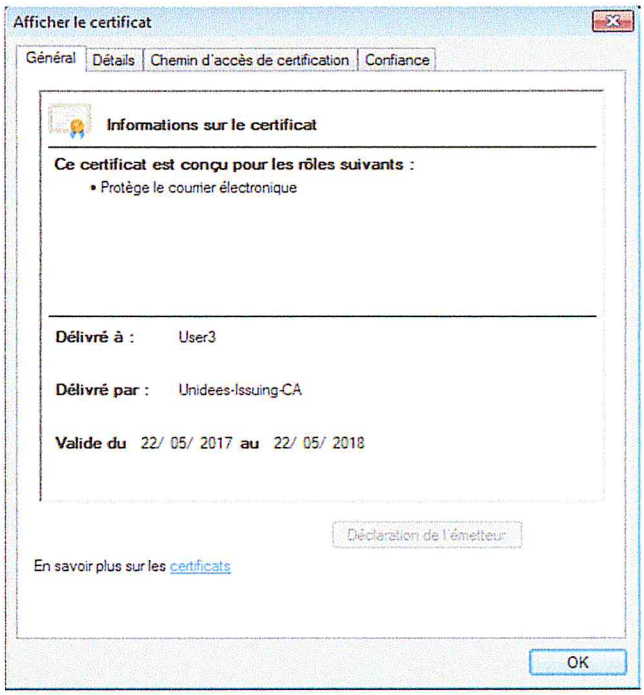


Figure 2.40 : Certificat conçu pour la protection des emails de l'émetteur

7. Protégé l'accès VPN

Pour la partie VPN nous avons que délivré des certificats IPSec aux utilisateurs.

La demande d'un certificat IPSec se fait de la même manière que pour les certificats e-mail à part la sélection de modèle. Dans ce cas le modèle est IPSEC.

Les figures **2.41** et **2.42** nous montre l'inscription de demande et le resultat d'inscription.

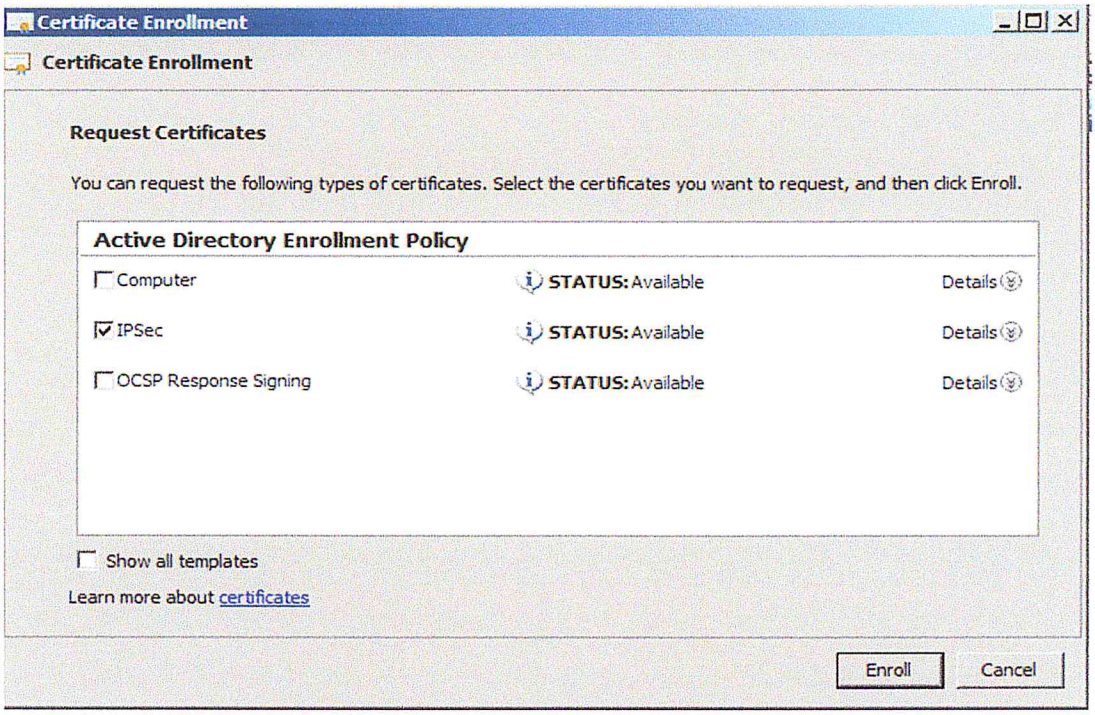


Figure 2.41 : Inscription de demandes des certificat IPSec

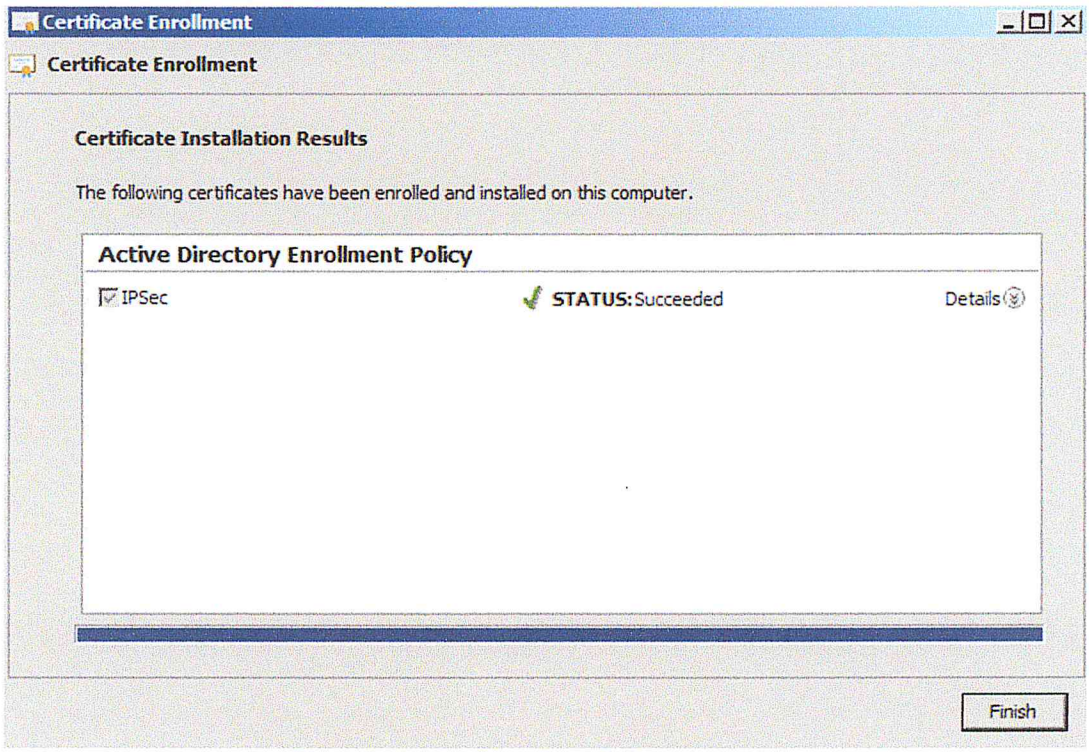


Figure 2.42 : Résultat d'inscription

8. Les mesures de sécurité

La sécurité de notre infrastructure à clés publiques est le facteur le plus important dans notre conception et implémentation. Ces mesures peuvent être catégorisées comme suit :

- **Les mesures de configuration d'AC :** C'est la configuration qui concerne les services des certificats ou le système d'exploitation.
- **Les mesures de sécurité physique :** A l'addition aux mesures de sécurité logiques nous devons implémenter plusieurs mesures de sécurité physique pour protéger nos serveurs.

Parmi les mesures de configuration d'AC qui nous avons abordé :

- **Le choix de l'architecture :** Nous avons choisis une architecture a deux niveaux (AC racine et AC émettrice) qui nous a donné une simplicité au système et une augmentation de niveau de sécurité parce que la racine est hors ligne qui implique une protection totale à sa clé privée.
- **Le choix de modèle de certificat :** Nous avons utilisés deux certificats numériques pour la protection des emails, un certificat pour le chiffrement qui va être archivé, et un autre certificat pour la signature qui ne sera jamais archivé donc sa clé privée sera protéger.
- **L'utilisation de protocole SSL :** Nous avons générés un certificat SSL pour l'interface web « Certsrv » pour garantir que tous les échanges entre l'utilisateur et l'autorité de certification (demande d'un certificat, téléchargement d'un certificat …) seront chiffré.
- **L'algorithme de hachage :** Nous avons utilisé l'algorithme de hachage SHA-256 (Secure Hash Algorithm) qu'il est non cassable jusqu'au aujourd'hui pour vérifier la validité de la signature de certificat.
- **L'algorithme de chiffrement :** Nous avons utilisé l'algorithme AES-256 bits qui est un algorithme asymétrique très puissant pour le chiffrement.
- **La minimisation des rôles de serveur :** Nous avons séparé entre les rôles de nos serveurs pour augmenter le niveau de sécurité et mieux éviter les attaques. Le rôle d'active directory est dans un serveur séparé par rapport aux rôles de notre autorités de certification.
- **L'activation des options d'audits dans les autorités de certification :** Nous avons activé tous les options d'audits pour que les logs de sécurité de Windows contiennent

tous les évènements de sécurité en relation avec les opérations des services de certificat.

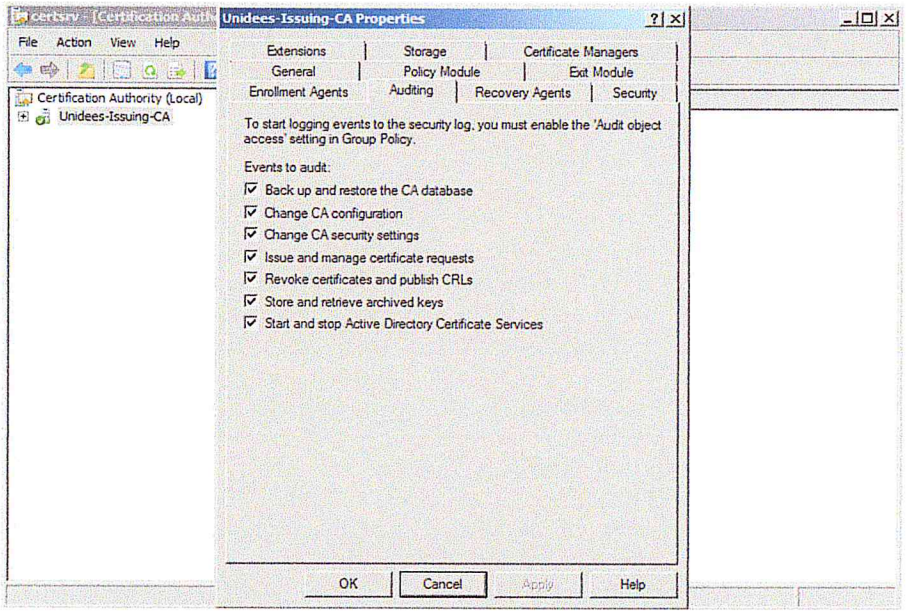


Figure 2.43 : Les options d'audits

- **Limiter le nombre des membres du groupe des administrateurs locaux :** Par défaut tous les membres du groupe des administrateurs locaux ont le droit d'accéder et exporter la clé privée de l'autorité qui est sauvegardé dans le dépôt local de la machine. Donc par limiter le nombre des membres du groupe, nous avons limité le nombre des utilisateurs qui ont accès à la clé privée.
- **L'utilisation de l'assistant de configuration de sécurité :** L'assistant de configuration de sécurité analyse les rôles et les services installés. Il identifie les rôles installés, désactive les services qui ne sont pas nécessaires, implémente la sécurité de réseau, configure les options des registres qui sécurisent l'authentification, les propriétés de système et les propriétés d'audit par défaut.

Figure 2.44 : L'assistant de configuration de sécurité

- **L'implémentation d'un agent pour la récupération de clé :** Nous avons installé un agent qui a le droit de récupérer la clé privée en cas où l'utilisateur perde sa clé de chiffrement. La récupération se faite si l'un des raisons suivantes arrivent :
  - Suppression de profil de l'utilisateur.
  - Endommagement de disque dure.
  - Réinstallation de système.
  - Vol ou perte d'un ordinateur.

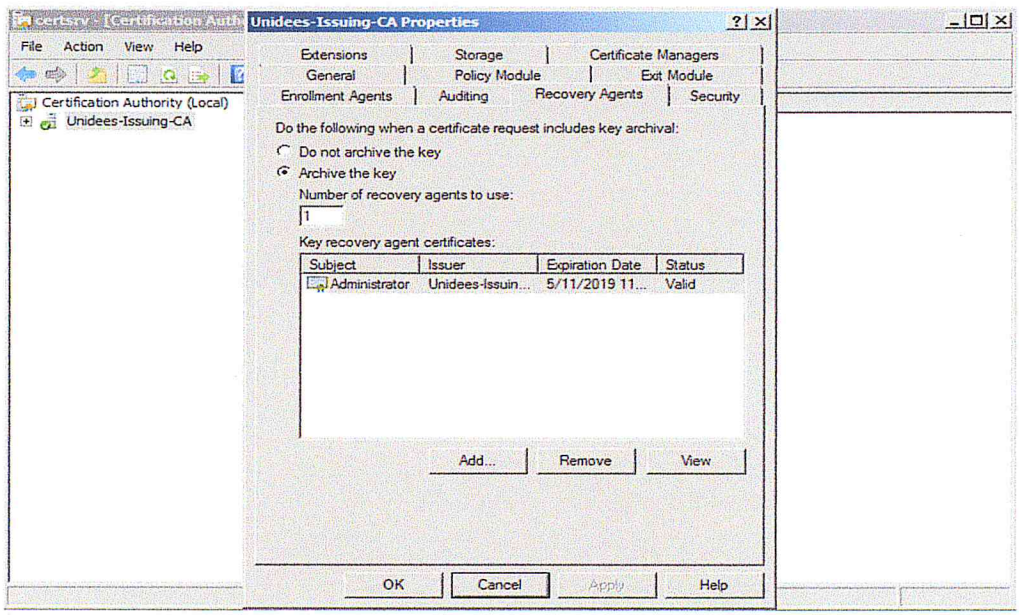


Figure 2.45 : L'agent de récupération de clé

- **Etablir une sauvegarde pour l'autorité de certification :** La sauvegarde est très importante en cas d'une défaillance. Elle nous permettre de faire une restauration en un temps minimal qui annule ces défaillances.

Parmi les mesures de sécurité physique :

- Stockez l'autorité de certification hors ligne dans une chambre physiquement sécurisé.
- Stockez les autorités de certification dans une cage sécurisée.
- Stockez le matériel de l'autorité de certification hors ligne dans un emplacement séparé et sécurisé.
- Stockez la clé privée dans le dépôt locale de machine.

9. Conclusion

Dans ce chapitre, nous avons montré comment implémenter une infrastructure à clés publiques étape par étape, ensuite nous avons délivré des certificats tels que les certificats de signature et de chiffrement des emails et le certificat IPSec. Enfin nous avons prouvé l'utilité des certificats pour la protection de courrier électronique.

CONCLUSION GENERALE

La communication électronique est devenue un acte habituel entre les personnes. Ces communications sont exposées pour différents types de risque de sécurité. Les données qui circulent dans le réseau peuvent être interceptées, modifiées ou usurpée par des tierces parties sans être détecté.

Lors de la transmission des données sur le réseau, elles passent par plusieurs périphériques comme un serveur des emails ou de VPN, donc rien ne garantit que les administrateurs accèdent, modifient ou copient ces données sans être détectés.

Pour protéger ces données, nous avons proposé une solution simple et économique pour sécuriser ces communications : l'utilisation des certificats électroniques délivrer par notre propre autorité de certification entreprise.

L'objectif de ce travail était de réaliser un système permettant d'éliminer et/ou de minimiser les risques de sécurité lors la transaction des données. La conception et la réalisation d'un tel système nous ont permis de :

- Approfondir dans le cadre professionnel.
- Analyser les besoins et l'identification des objectifs.
- Apprendre de nouveaux protocoles de sécurité telle que le SSL, S/MIME et le IPSec.
- Concevoir et réaliser un système fiable.

A l'issu de ce projet de fin d'étude dont les objectifs nous ont été assignés par notre encadreur, nous pouvons dire que les travaux effectués ont abouti aux résultats attendus à savoir une infrastructure à clé publique efficace qui permette de délivrer différents types de certificats aux employés afin de sécuriser leurs communications par email et protéger leurs accès VPN.

Le système réalisé a atteint les objectifs fixés. Toutefois, il peut être sujette à des améliorations comme :

- La génération d'autre type de certificats pour sécuriser les documents électroniques, contrôler l'accès au réseau via le WIFI et l'authentification forte …etc.
- La configuration d'un système VPN pour qu'il peut utiliser le certificat IPSec générer par notre infrastructure.

Bibliographie

[1] https://www.arobase.org/actu/chiffres-email.htm , Statistique par Radicati Group en Mars 2016, consulté le 10 Juin 2017.

[2] Windows server 2008 PKI and certificate security par Brian KOMAR en 4 October 2008.

[3] Sécuriser les échanges d'information par email. Article par David ISAL en Octobre 2013

[4] PKI. Cour par Anas ABOU EL KALAM

[5] Implémenter une infrastructure à clés publiques dans un environnement Windows Server 2003 par Alexandre VILLOING en 2 Mai 2006.

[6] Les certificats, Article réalisé sous la direction de Jean-François PILLOU en Septembre 2015.

[7] Certification électronique et E-Services, 24 Avril 2011

[8] Infrastructure à clés publiques par Nicolas BROISIN en 9 janvier 2013

[9] https://msdn.microsoft.com/fr-fr/library/dn786436(v=ws.11).aspx. Site web officiel de Microsoft, consulté le 05 Juin 2017.

[10] Understanding public key infrastructure. Article par San MATEO.

[11] A guide to PKIs and Open–source Implementations par Symeon XENITELLIS en 2000.

[12] Mise en place progressive d'une IGC au CNRS. Article par Jean-Luc Archimbaud en 2 Février 2011.

[13] Pascal PARE, Camille ROSENTHAL-SABROUX, Nasser KETTANI et Dominique MIGNET.De Merise a UML. Eryolles France edition, Octobre 2001.