DEDICACES

À MES PARENTS

REMERCIEMENTS

Nous saisissons cette opportunité pour remercier tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce mémoire.

Nos remerciements vont particulièrement :

- Au **Président** et aux **membres du jury** d'avoir accepté d'évaluer ce travail.
- Au **Pr. MOUANGUE Ruben Martin**, Directeur de l'École Nationale Supérieure Polytechnique de Douala (ENSPD) pour son dynamisme et l'abnégation au travail bien fait.
- A **KOTTO Jean-Yves**, **Directeur Général d'INTELCIA Cameroun** et son personnel pour l'immense formation pratique dont nous avons bénéficié.
- Au **Dr. Jean NDOUMBE**, chef de département de la filière Génie Informatique et Télécommunications (GIT) à l'Ecole Nationale Supérieure Polytechnique de Douala pour sa clairvoyance, ses conseils et l'endurance au travail qu'il a cultivé en nous durant notre formation d'ingénieurs.
- A **Dr MATANGA JACQUES** et **DR TOTTO PHILIPPE** mes encadreurs académique pour leur grande disponibilité, leurs encouragements, leurs sacrifices et efforts consentis pendant le suivi et la mise en œuvre de ce travail.
- A **M.NDOUMI NZOMI Ronny**, encadreur professionnel pour son suivi, son accompagnement, son soutien et l'entière disponibilité dans le cadre de la réalisation de ce travail.
- A **M.FOTSING Hervé Pascal**, Responsable des stagiaires pour son suivi, son accompagnement, son soutien et l'entière disponibilité dans le cadre de la réalisation de ce travail.
- A toute la team IT de l'entreprise INTELCIA pour leur convivialité, leurs conseils durant notre stage et leur apport sur le plan socioprofessionnel.
- A tout le corps enseignant l'École Nationale Supérieure Polytechnique de Douala pour leur grande rigueur dans le travail.
- A tout le personnel de l'entreprise INTELCIA pour leur convivialité, leurs conseils durant notre stage et leur apport sur le plan socioprofessionnel.
- A mes camarades de classe pour leur présence et leurs apports critiques constructifs.
- A mes camarades de stages pour leur sens du travail et leurs encouragements.
- A tous ceux qui de près ou de loin ont contribué à la réussite de ce travail.

AVANT-PROPOS

L'Ecole Nationale Supérieure Polytechnique de Douala (ENSPD), née de la transformation de l'ex-Faculté de Génie Industriel, ayant vu le jour par le décret présidentiel N°2020/272 du 11 Mai 2020, est l'une des institutions de l'Université de Douala. Elle a pour mission principale de former des citoyens aptes à diriger des travaux d'art ou d'industrie, en vue de donner un nouveau souffle à son développement technologique et de lutter contre le sous-développement. Elle offre les domaines de formations suivants :

- Ingénierie de la Production et de la Maîtrise de l'Energie ;
- Génie Frigorifique et Climatique ;
- Ingénierie des Systèmes Mécatroniques ;
- Ingénierie Automobile ;
- Ingénierie des Opérations – Capitaine de Pêche ;
- Electromécanique Navale ;
- Ingénierie de l'Energie Electrique ;
- Ingénierie des Systèmes Automatisés ;
- Qualité et Normalisation ;
- Hygiène Industrielle ;
- Sécurité Industrielle ;
- Environnement Industriel ;
- Construction Mécanique et Productique ;
- Construction Métallique et Tuyauterie ;
- Bâtiments et Constructions Industrielles ;
- Travaux Publics et Ouvrages ;
- Réseaux et Télécommunications ;
- Génie Logiciel ;
- Sécurité des Systèmes d'Information ;
- Management des Systèmes d'Information ;
- Chimie Industrielle ;
- Bioprocédés Industriels ;
- Génie Pharmaceutique ;
- Capteurs, Instrumentations et Mesures ;

- Technologie Biomédicale ;
- Mécanique et Matériau ;
- Géophysique, Eau et Environnement ;
- Electronique, Electrotechnique et Automatique ;
- Energie.

Les étudiants y sont admis par voie de concours en 1ère année et en 3ème année pour les cursus d'ingénieur et sciences de l'ingénieur et sur étude de dossier pour le master professionnel. Les enseignements y sont organisés en cours magistraux, travaux dirigés, travaux pratiques, travaux personnels, visites d'entreprise et stages techniques.

Les études sont effectuées en trois cycles. Les enseignements du 1er cycle s'étalent sur six semestres et ont pour principal objectif « d'initier les étudiants aux techniques industrielles » afin d'assister les ingénieurs. La validation de toutes les Unités d'Enseignement (UE) du 1er cycle correspondant au quota requis donne droit à une admission au 2nd cycle et à l'obtention d'une Licence en science de l'ingénieur pour le cursus science de l'ingénieur.

Le second cycle s'étend sur quatre semestres dit de « spécialisation ». Les étudiants ayant choisi leur filière en fin de premier cycle se spécialisent en choisissant un axe pour l'élaboration d'un profil particulier et personnel. En effet, l'étudiant a un quota d'unités d'enseignements obligatoires et des optionnelles au choix en fonction de son profil. Les objectifs du 2nd cycle sont :

- Donner à l'étudiant les connaissances professionnelles, technologiques et managériales de pointes pour une compétence efficiente en entreprise ;
- D'initier l'étudiant à la recherche.

Les études du 2nd cycle sont sanctionnées par la validation de tous les stages et Unités d'Enseignement correspondant au nombre de crédits indiqués et, l'obtention du Diplôme d'Ingénieur de l'Ecole Nationale Supérieure Polytechnique de Douala pour le cursus d'ingénieur, celui de master 2 en science de l'ingénieur pour le cursus science de l'ingénieur donnant lieu au passage au 3ème cycle et celui de master 2 professionnel pour le cursus master professionnel. A la fin de nos études, il est obligatoire de produire un mémoire qui sera présenté devant un jury compétent.

RESUME

Ce mémoire présente l'étude et la mise en place d'une infrastructure à clé publique pour sécuriser le réseau informatique d'Intelcia. Dans l'optique d'assurer la fiabilité, l'intégrité, la confidentialité et la disponibilité des données utilisées par Intelcia, nous avons orienté nos travaux vers le déploiement d'un système de sécurité informatique qui utilise la cryptographie à clé publique et des certificats numériques pour garantir la sécurité des communications dans le réseau. Pour atteindre nos objectifs, nous avons créé notre propre autorité de certification grâce au service AD CS de Windows Server, et nous avons distribué les différents certificats créés grâce aux GPO et à l'inscription via le site web de demande de certificat. Tout ce processus a conduit à l'obtention de notre infrastructure de gestion des clés publiques. Par la suite, nous avons pu sécuriser un site web qui est diffusé dans notre réseau local et effectuer les différents tests qui prouvent que les données qui circulent sont désormais chiffrées. Cependant, notre solution pourrait être améliorée en hiérarchisant nos autorités de certification.

Mots clés : Chiffrées, clé publique, certificats numériques, Cryptographie

ABSTRACT

This thesis presents the study and implementation of a public key infrastructure to secure the Intelcia computer network. With the aim of ensuring reliability, integrity, confidentiality, and availability of data used by Intelcia, our work focused on deploying a computer security system that uses public key cryptography and digital certificates to ensure secure communication within the network. To achieve our objectives, we created our own certification authority using the Windows Server AD CS service and distributed the various certificates created through GPO and registration via the certificate request website. The entire process led to the establishment of our public key management infrastructure. Subsequently, we were able to secure a website that is broadcast on our local network and perform various tests that prove that the data circulating is now encrypted. However, our solution could be improved by hierarchizing our certification authorities.

Keywords: Encrypted, public key, digital certificate, Cryptography

TABLE DE MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABREVIATIONS

AC : Autorité de certification

AD DS : Active Directory Domain Services.

AD CS : Active Directory Certificate Services.

AE : Autorité d'enregistrement

AES : Advanced Encryption Standard

BPO : business process outsourcing

CA : Certificate Authority

CCS : Change Cipher Security

CRL : Certificates Revocation List

DAG : Direction de l'Audit Général

DCO : Direction Centrale des Opérations

DC : Domain Controller

DCM : Direction de la Communication et du Marketing

DDRH : La Direction du Développement des ressources humaines

DES : Data Encryption Standard

DHCP : Dynamic Host Configuration Protocol.

DINT : Direction de l'Information et des Nouvelles Technologies

DMG : Direction des Moyens Généraux

DN : Distinguished Name

DNS : Domain Name System.

DSA : Digital Signature Algorithm

DSRM : Directory Services Restore Mode

ECC ; Error-Correcting Code

ECMQV : Elliptic Curve Menezes-Qu-Vanstone

ECDH : Elliptic Curve Diffie-Hellman)

EE : End entity

FTP : File Transfert Protocol

GPO : Group Policy Objects

HTTP : Hyper Text Transfer Protocol

HTTPS : Hyper Text Transfer Protocol Secure

IBM : International Business Machines Corporation

ICP : Infrastructure à clé publique

IDEA : International Data Encryption Algorithm

IETF : Internet Engineering Task Force

IIS : Internet Information Services

ISO : International Organization for Standardization

LDAPS : Lightweight Directory Access Protocol Secure

LDAP : Lightweight Directory Access Protocol

MAC : Meadia Access Control

MD5 : Message Digest 5

NTIC : Nouvelles Technologies De L'information Et De La Communication

OSCP : Online Certificate Status Protocol

PC : Personnal Computers

PGP : Pretty Good Privacy

PKI : Public-Key Infrastructure

PKIX : Public-Key Infrastructure X.509

RAM : Random Access Memory

RC : Rivest Cipher

RDS : Remote Desktop Service

RFC : Request For Comments

RSA : R.Rivest, A.Shamir et l.Adleman

SAN : Subject Alternative Name

SHA : Secure Hash Algorithm

SHS : Secure Hash Standard

SMTP : Simple Mail Transfert Protocol

S/MIME : Secure/Mutlipurpose Internet Mail Extensions

SSL : Secure Socket Layer

TLS : Transport Layer Security

TCP : Transfert Control Protocol

UDP : User Datagram Protocol

UO : Unite d'Organisation

INTRODUCTION GENERALE

De nos jours, un flux croissant et important de données transite via internet. Grâce aux multiples services qu'il offre, l'échange et le partage des données deviennent de plus en plus aisés. Internet est aujourd'hui utilisé par toutes les grandes entreprises pour les échanges à l'international. Intelcia étant une entreprise qui s'étend sur plusieurs pays et offre une pléthore de services, il est donc normal d'utiliser les nouvelles technologies de l'information et de la communication pour faire transiter ses différentes données.

L'utilisation des NTIC est un moyen de faciliter les échanges d'informations, mais cela ne présente pas que des avantages. Des personnes mal intentionnées, souvent appelées hackers ou pirates informatiques, pourraient intercepter, modifier ou même analyser les informations qui transitent sur internet. D'où la nécessité de sécuriser nos échanges. Intelcia a accès aux données bancaires de ses différents clients. Ces données transitent via internet pour être envoyées aux différents sites de résolution des problèmes des clients. Si ces données étaient interceptées lors de leur envoi, cela pourrait mettre toute la société dans une situation très délicate. Cela nous pousse à nous interroger sur l'authenticité des données qui transitent sur internet, sur la confidentialité des informations que nous échangeons, sur le niveau de sécurité disponible dans nos réseaux. C'est dans le but de répondre à ces interrogations que nous travaillons sur **la mise en place d'une infrastructure à clé publique (PKI)**.

Notre travail s'orientera tout d'abord sur l'état de l'art et l'état des lieux sur l'infrastructure PKI, puis sur les matériels et méthodes liés au PKI, et enfin nous présenterons les résultats de l'environnement mis en place.

CHAPITRE 1 : ETAT DE L'ART ET ETAT DES LIEUX

INTRODUCTION

Au fil des ans, l'utilisation d'Internet et des réseaux informatiques a considérablement augmenté, ce qui a entraîné une croissance exponentielle de la quantité de données échangées en ligne. Cependant, cette croissance a également engendré de nombreux risques de sécurité, tels que la perte de données sensibles et les attaques de piratage. Pour répondre à ces défis, les infrastructures à clé publique (PKI) ont été développées pour fournir un moyen sécurisé pour la communication en ligne. Une PKI est un système de cryptographie à clé publique qui utilise des certificats numériques pour assurer l'authenticité et la confidentialité des données échangées sur Internet.[1]

Au cours des dernières décennies, de nombreux travaux de recherche ont été menés dans le domaine des PKI pour améliorer la sécurité et la fiabilité de l'échange de données en ligne. Les recherches ont porté sur des sujets tels que la gestion des clés, la validation des certificats, les politiques de confiance et les protocoles de sécurité de la PKI. Dans cette étude de l'existant sur les PKI, nous allons explorer les recherches et les développements les plus récents dans le domaine de la PKI.

1.1 ETAT DE L'ART SUR LES INFRASTRUCTURE A CLE PUBLIQUES (PKI)

1.1.1 La sécurité informatique

1.1.1.1 Définition

La sécurité informatique est définie comme étant l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires, mis en place pour conserver, rétablir et garantir la sécurité des systèmes informatiques. Elle a pour objectif d'assurer les quatre principales fonctionnalités suivantes : l'authentification, la confidentialité, l'intégrité et la non-répudiation. Ces exigences sont vitales si l'on désire effectuer une communication sécurisée à travers un réseau informatique tel qu'Internet.[2]

1.1.1.2 Objectifs

1.1.1.2.1 Authentification

L'authentification est un mécanisme qui sert à s'assurer que l'identité de la personne avec laquelle on communique est bel est bien celle qu'elle prétend être. Elle est généralement mise en œuvre grâce à une combinaison d'un nom d'utilisateur et d'un mot de passe. Une partie du processus d'authentification consiste à identifier correctement un utilisateur, une application, ou un groupe.

1.1.1.2.2 Confidentialité

La confidentialité est la propriété qu'une information n'est ni disponible ni révélée aux individus, entités ou processus non autorisés. Les données transportées lors d'une communication ne peuvent pas être lues par un adversaire espionnant les communications. La confidentialité a donc pour but d'assurer que seul le destinataire peut connaître le contenu des messages ou des données sensibles dites «confidentielles » qui lui sont transmises.

1.1.1.2.3 Intégrité

L'intégrité des données est la propriété qui assure que le traitement, transmission, et conservation des données, ne subissent aucun changement ou destruction volontaire (par un intrus) ou accidentelle.

Si une partie intermédiaire modifie les données d'origines envoyées par l'expéditeur, le destinataire final devrait être capable de détecter qu'il y a eu des changements.

1.1.1.2.4 Non répudiation

La non-répudiation est définie par l'impossibilité pour une des entités impliquées dans une communication de nier avoir participé à l'ensemble ou à une partie de la communication. Elle assure, ainsi, une protection contre le faux démenti d'une entité d'être impliquée dans une communication.

1.1.2 La Cryptographie

1.1.2.1 Définition

La cryptographie est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. La cryptographie sert à stocker des données sensibles ou de les transmettre par des réseaux de communication non sûrs comme Internet, dans le but qu'elles ne puissent être interceptées par personne à l'exception du destinataire souhaité.[3]

1.1.2.2 Chiffrement / Déchiffrement

Le chiffrement est le mécanisme cryptographique par lequel un message (fichier, courriel, etc.) dit « en clair », est transformé à l'aide d'un algorithme mathématique et d'une clé, de manière à le rendre incompréhensible. Le déchiffrement est l'opération inverse qui, par un procédé similaire, applique une transformation sur un message chiffré, de manière à le ramener dans sa forme compréhensible. Le chiffrement a pour objectif d'assurer la ***confidentialité*** des données.

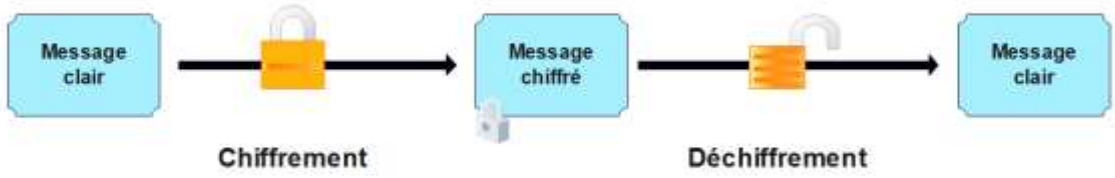

Figure 1.1 : Chiffrement et déchiffrement d'un message

1.1.2.3 Les Clés

Une clé est une valeur qui est utilisée avec un algorithme cryptographique pour produire un texte chiffré spécifique. Les clés sont, à la base de très grands nombres. La taille d'une clé se mesure en bits; et le nombre qui peut être représenté par une clé de 1024 bits est vraiment immense. Plus grande est la clé, plus grande est la sécurité, mais les algorithmes utilisés pour chaque type de cryptographie sont très différents. Par exemple, en matière de cryptographie à clé publique, plus la clé est grande, plus le chiffrement est sûr.

Il existe deux sortes de clés :

- Clé Publique : quantité numérique, attachée à une ressource ou un individu qui la distribue aux autres afin qu'ils puissent lui envoyer des données chiffrées ou déchiffrer sa signature.
- Clé Privée : quantité numérique secrète attachée à une ressource ou à un individu, lui permettant de déchiffrer des données chiffrées avec la clé publique correspondante ou d'apposer une signature au bas de messages envoyés vers des destinataires.

1.1.2.4 Les familles cryptographiques

1.1.2.4.1 Cryptographie Symétrique (A clé secrète)

Dans la cryptographie symétrique, aussi appelée chiffrement conventionnel ou à clé secrète, une seule et même clé est utilisée à la fois pour le chiffrement et le déchiffrement. Cette clé doit être gardée secrète. La sécurité d'un algorithme à clé symétrique repose donc sur la clé : si celle-ci est dévoilée, alors n'importe qui peut chiffrer ou déchiffrer des messages.

Les algorithmes à clé symétrique sont des algorithmes où la clé de chiffrement peut être calculée à partir de la clé de déchiffrement ou vice versa. Dans la plupart des cas, la clé de chiffrement et la clé de déchiffrement sont identiques. Pour de tels algorithmes, l'émetteur et le destinataire doivent se mettre d'accord sur une clé à utiliser avant d'échanger des messages chiffrés.

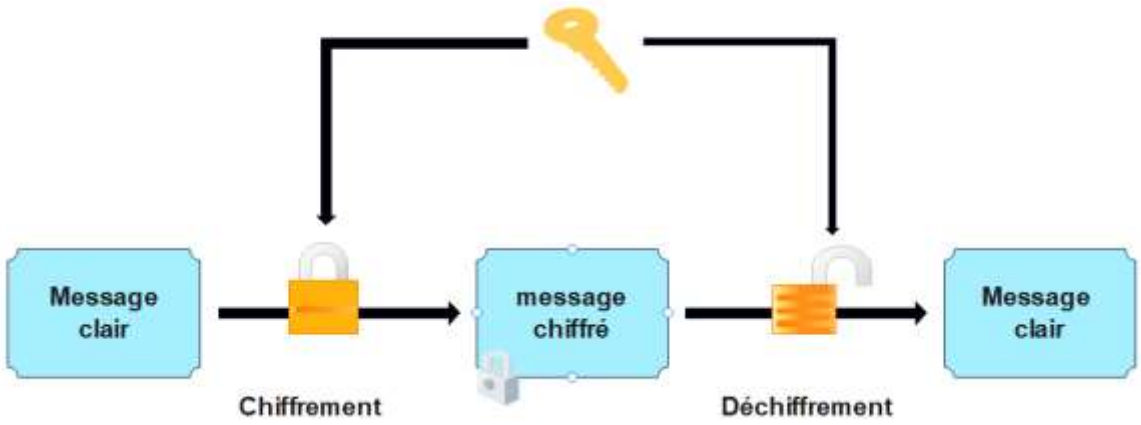

Figure 1.2: Cryptographie symétrique

Il existe plusieurs algorithmes qui fonctionnent sur ce principe :

Tableau 1.1: Algorithme symétrique

Algorithme	Description
DES (Data Encryption Standard), 1974	Conçu par IBM, ce système de chiffrement par blocs est fondé sur une clé de 56 bits. Longtemps standard de chiffrement des communications gouvernementales non classées secrètes, il a été remplacé récemment par AES. L'algorithme a été rendu public.
IDEA (International Data Encryption Algorithm), 1990	Conçu par X. Lai et J. Massey, ce système de chiffrement par blocs s'appuie sur une clé de 128 bits. L'algorithme a été rendu public.
AES (Advanced Encryption Standard), 2000	Conçu par J. Daemen et V. Rijmen, ce système de chiffrement par blocs s'appuie sur une clé de 128 à 256 bits. Il s'agit du standard de chiffrement pour les communications gouvernementales non classées secrètes. L'algorithme a été rendu public.

1.1.2.4.2 Cryptographie asymétrique (A clé publique)

Dans les algorithmes à clé secrète, tout reposait sur le secret d'une clé commune qui devait être échangée dans la confidentialité la plus totale. Les problèmes de distribution de clé sont résolus par la cryptographie à clé publique, dont le concept fut inventé par Whitfield Diffie et Martin Hellman en1975.

La cryptographie à clé publique repose sur un schéma asymétrique qui utilise une paire de clés pour le chiffrement: une clé publique, qui chiffre les données et une clé privée correspondante, qui sera utilisée pour le déchiffrement.

Les algorithmes à clé asymétrique ou clé publique sont conçus de telle manière que la clé de chiffrement soit différente de la clé de déchiffrement. Il est donc mathématiquement impossible de déduire la clé privée de la clé publique.

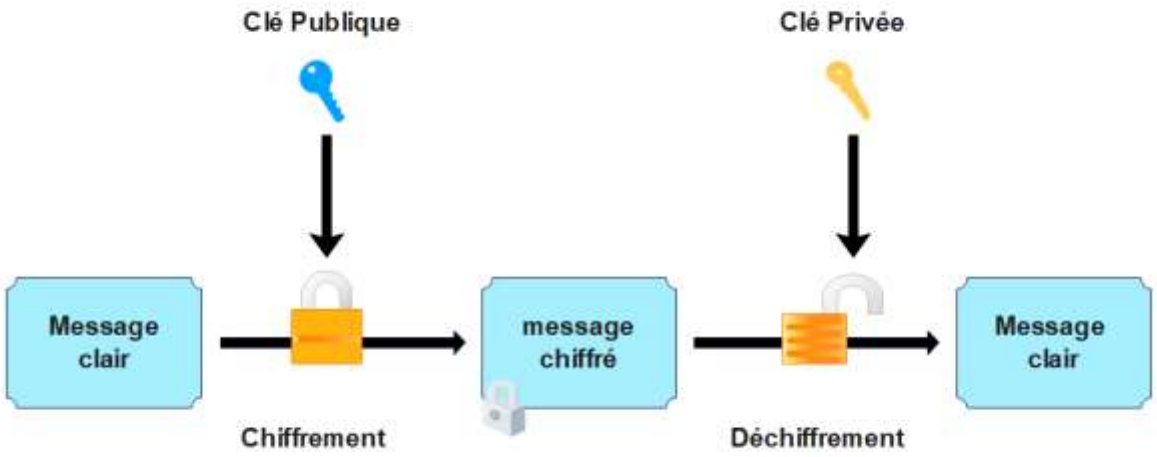

Figure 1.3 : Cryptographie Asymétrique

RSA baptisé ainsi d'après le nom de ces créateurs Ron Rivest, Adi Shamir et Leonard Adleman, est l'exemple le plus populaire des algorithmes asymétriques.

Le tableau suivant énumère les principaux algorithmes asymétriques ainsi que l'usage pour lequel ceux-ci ont été conçus.

Tableau 1.2 : Algorithme asymétrique

Algorithme	Description
Diffie-Hellman, 1976	Conçu par W. Diffie et M. E. Hellman, cet algorithme permet de partager un secret commun après un protocole d'échange de données. La sécurité du schéma de DiffieHellman repose sur la difficulté de calculer un logarithme discret. L'algorithme a été rendu public.

RSA (Rivest Shamir Adleman), 1978	Conçu par R. Rivest, A. Shamir et L. Adleman, cet algorithme permet de partager un secret commun après un protocole d'échange de données. La sécurité du schéma repose sur la difficulté de la factorisation en nombres premiers. L'algorithme a été rendu public.
Les cryptosystèmes à courbes elliptiques, 1985-2005 : – ECMQV (Elliptic Curve Menezes-Qu-Vanstone) – ECDH (Elliptic Curve Diffie-Hellman)	Introduits par V. Miller et N. Koblitz, de nombreux travaux ont déjà été menés sur ce type de système offrant de solides protections (pour des longueurs de clés plus petites que d'autres types d'algorithmes) contre la cryptanalyse. La sécurité du schéma repose sur la difficulté de calculer un logarithme discret. La société Certicom détient de nombreux brevets dans ce domaine.

1.1.2.5 Fonction de hachage

Une fonction de hachage est une méthode permettant de caractériser une information. Elle prend en entrée un message de taille quelconque, applique une suite de traitements reproductibles à cette entrée et obtient à la sortie une chaine de caractères hexadécimaux, une empreinte servant à identifier la donnée initiale appelée aussi le condensé. Cette sortie résume en quelque sorte l'information et a une taille fixe qui varie selon les algorithmes.[3]

Les fonctions de hachage les plus connues sont MD4, MD5 (« MD » pour « Message Digest »), SHA (Secure Hash Algorithm) et SHS (Secure Hash Standard).Toutes ces fonctions sont quasiment similaires mais plus ou moins rapides.

Tableau 1.3 : Tableau résumant les fonctions de hachage[4]

Fonction de hachage	Mode de fonctionnement
MD4	L'algorithme prend en entrée un message de longueur arbitraire et produit en sortie une empreinte de 128-bit « empreinte digitale » ou « message digest » de l'entrée.
MD5	L'algorithme MD5 est une extension de MD4, il est légèrement plus lent que MD4, mais il est plus «conservateur» dans la conception. L'algorithme MD5 est placé dans le domaine public pour examen et adoption éventuelle en tant que norme.
SHA-1	C'est une fonction de hachage cryptographique qui fournit une empreinte de 160 bits.
SHA-256	C'est une fonction de hachage cryptographique dérivée de SHA-1 qui fournit une empreinte de 256 bits.
SHS	Il fournit des empreintes de 160 bits. Sa structure est identique à MD4 et MD5, mais potentiellement plus fiable, la taille de la clé étant de 160 bits au lieu de 128 bits.

1.1.2.6 Signature numérique

Une signature numérique est une signature électronique qui est utilisé pour authentifier l'identité de l'expéditeur d'un message ou le signataire d'un document, et sert à garantir que le contenu original du message ou document qui a été envoyé reste inchangé. Les signatures

numériques sont facilement transportables, ne peuvent pas être imités par quelqu'un d'autre, et peuvent être automatiquement horodaté. La capacité de s'assurer que le message original signé est arrivé signifie que l'expéditeur ne peut pas facilement répudier plus tard. Une signature numérique peut être utilisée avec n'importe quel genre de message, soit crypté ou non, simplement pour que le récepteur soit sûr de l'identité de l'expéditeur et que le message est arrivé intact. Un certificat numérique contient la signature numérique de l'autorité de certification émettrice afin que chacun puisse vérifier que le certificat est bien réel.

Il existe deux sortes de signature numérique :

• **Signature numérique simple :** le message est signé directement par la clé privée et la vérification est faite en utilisant la clé publique.

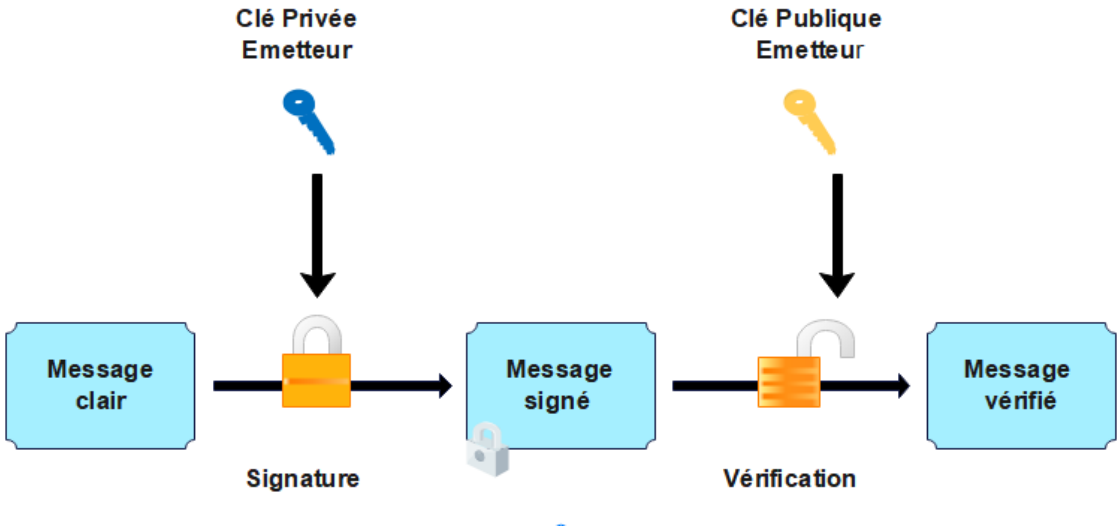

Figure 1.4 : Signature numérique simple d'un message

• **Signature numérique sécurisée :** le message à signer subit d'abord une fonction de hachage produisant ainsi un condensé. Après, le hach résultant est signé avec la clé privée.

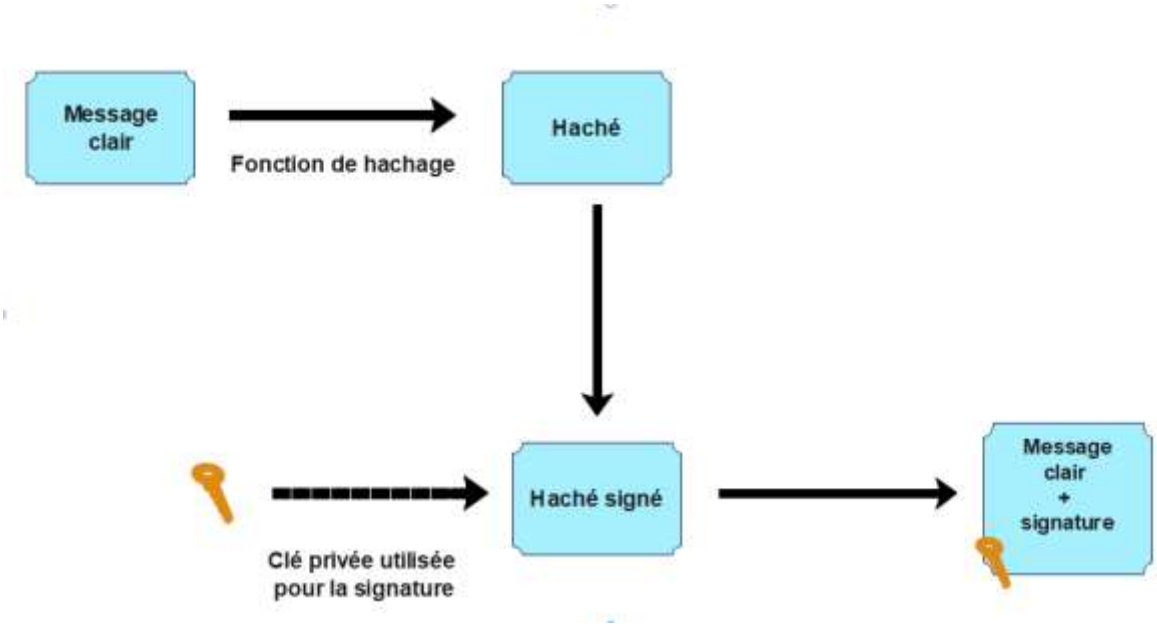

Figure 1.5 : Signature numérique sécurisée d'un message.

1.1.2.7 Certificats Numériques

Un certificat électronique est une carte d'identité numérique dont l'objet est d'identifier une entité physique ou non-physique. Le certificat numérique ou électronique est un lien entre l'entité physique et l'entité numérique (Virtuel). L'autorité de certification fait foi de tiers de confiance et atteste du lien entre l'identité physique et l'entité numérique. Le standard le plus utilisé pour la création des certificats numérique est le X.509.[5]

1.1.2.7.1 Contenu d'un certificat

Les utilisateurs de certificats étant de plus en plus nombreux, le format de ce certificat doit de ce fait être commun à tous les utilisateurs. Sans cela, il sera impossible d'intégrer ces certificats dans des applications logicielles développées par des différents fournisseurs. Pour cette raison, les certificats numériques sont soumis à un standard.

Bien qu'il existe plusieurs formats de certificats : X.509, PGP (Pretty Good Privacy),…le format X.509 est aujourd'hui la norme de l'industrie qui permet d'assurer l'interopérabilité entre les différents systèmes. Il est normalisé par l'ISO et réalisé par l'IETF.

La figure « Figure 1.6 » est un exemple de certificat répondant à la norme X.509.

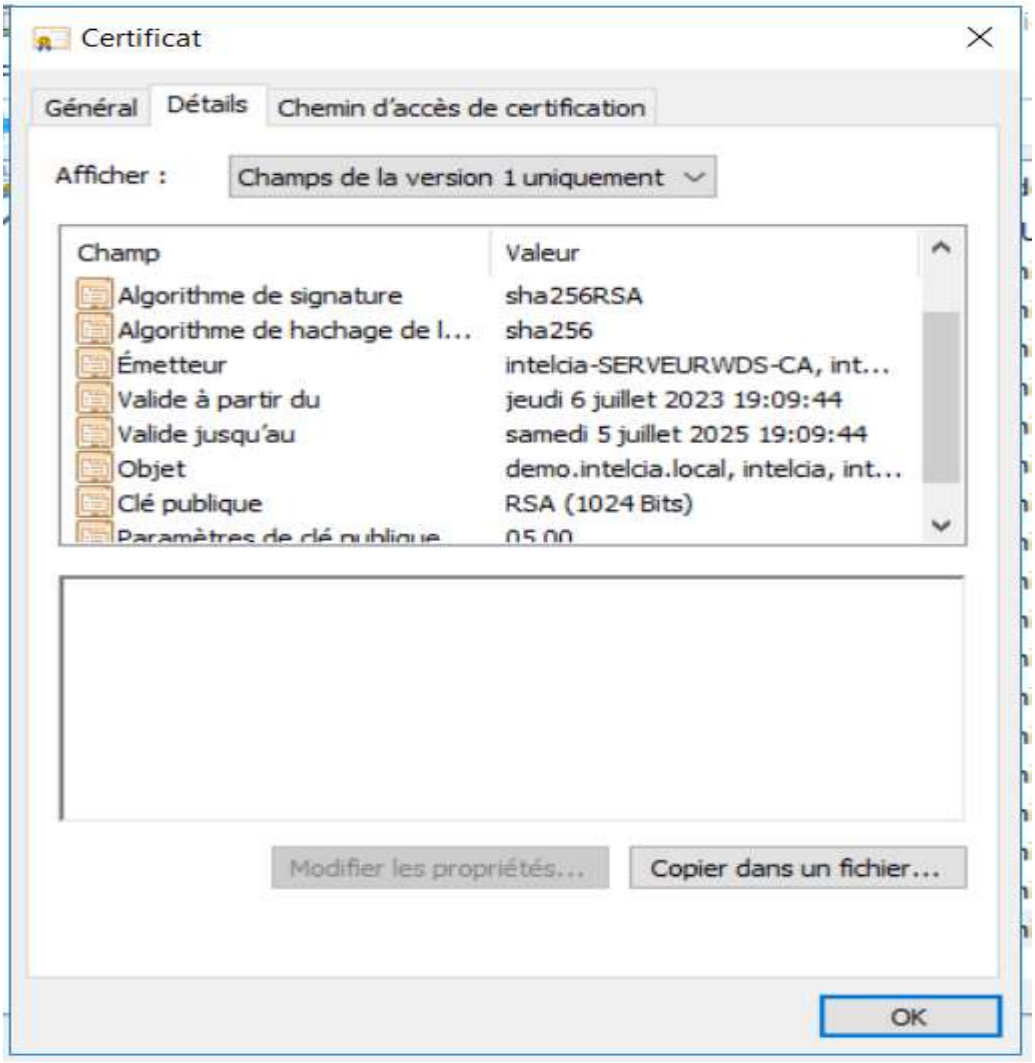

Figure 1.6 : Certificat numérique X.509.

Globalement, la composition d'un certificat X.509 est la suivante :

- **Sujet du certificat (DN) :** Ce champ identifie l'identité du propriétaire du couple clés privée/publique à certifier. Il existe là aussi un formalisme pour nommer ce champ.

- **Version du protocole X.509 (v3 actuellement) :** Ce champ identifie la version de la norme X.509 qui est utilisée dans le certificat. À ce jour, trois versions de la norme X.509 ont été définis. La dernière version utilisée est la version 3.
- **Numéro de série (unique par CA) :** Le numéro de série est un numéro unique qui est utilisé pour identifier le certificat X.509.
- **Algorithme de signature de l'autorité de certification :** Ce champ identifie l'algorithme utilisé par l'autorité de certification pour signer numériquement le certificat X.509.
- **Nom du CA (DN) :** Permet d'identifier l'autorité de certification qui a délivré le certificat. Il existe un formalisme bien défini pour attribuer un nom à chaque entité sans ambigüité (la position géographique entre en compte).
- **Période de validité** : Ce champ définit la période pendant laquelle la clé publique du certificat X.509est valide.
- **Extensions (facultatif) :** Ce champ a été introduit dans la version 3 du X.509. Il permet aux autorités de certification de rajouter leurs propres informations aux certificats qu'elles délivrent. Parmi ces informations on peut citer :
    - **authorityKeyIdentifier :** Cette extension fournis un moyen d'identifier la clé publique liée à la clé privée utilisée pour la signature du certificat.
    - **subjectKeyIdentifier :** Cette extension fournis un moyen d'identifier un certificat contenant une clé publique particulière.
    - **keyUsage :** Ce champ renseigne sur l'utilisation qui doit être faite de la clé, par exemple : Digital Signature, NonRepudiation, KeyEncipherment, DataEnciphement, CRLSign, …
    - **extendedKeyUsage :** Ce champ indique une ou plusieurs fonctionnalités pour lesquelles la clé publique certifiée peut être employée, en complément des champs fournis par Key Usage. Par exemple : Serveur authentification, client authentification, signature de réponses OCSP,…
    - **Basic Constraints :** L'extension des contraintes de base permet de définir si le sujet du certificat est un AC et la profondeur maximale de la chaîne de certification l'incluant.
- **Signature numérique :** Contient l'identifiant de l'algorithme (fonction de hachage) utilisé par l'autorité de certification pour signer le certificat, ainsi que la valeur de la signature numérique.

1.1.2.7.2 Types de certificat

Le groupe de travail PKIX de l'IETF fait état de l'existence de deux classes de certificats à clés publiques, soit :

- **Les certificats d'entités d'extrémité (end-entity) :** Ce sont des certificats émis par une AC, pour des entités qui ne sont pas des émetteurs de certificats.
- **Les certificats d'AC :** Ceux sont des certificats émis par une AC, pour des entités qui sont elles-mêmes des AC capables d'émettre des certificats à clé publique. Les certificats d'AC peuvent aussi être classés en trois sous-catégories, soit :
    - **Les certificats auto-émis (self-issuedcertificates) :** Certificats dont l'émetteur et le sujet représentent la même entité. Une AC pourrait, par exemple, utiliser ce type de certificat durant l'opération de rotation de clés, afin d'offrir la confiance de l'ancienne clé vers la nouvelle.
    - **Les certificats auto-signés (self-signedcertificates) :** Cas spécial de certificats auto-émis, où la clé privée utilisée par l'AC pour signer le certificat correspond à la clé publique contenue dans ce même certificat. Une autorité de certification à la racine d'un chemin de certification va générer puis signer elle-même sa propre clé puisqu'il n'existe aucune AC au-*dessus de celle-ci.*
    - **Les certificats croisés (cross-certificates) :** Certificat d'AC pour lequel l'émetteur et le sujet sont des entités différentes. Ce certificat permet de reconnaitre l'existence d'une autre AC dans un modèle de confiance en réseau.

1.1.3 Secure Socket Layer (SSL) / Transport Layer Security (SSL)

1.1.3.1 Définition

Conçu et développé par Netscape, le protocole SSL a été développé au-dessus de la couche TCP afin d'offrir aux navigateurs Internet la possibilité d'établir des sessions authentifiées et chiffrées. La première version de SSL date de 1994. La version actuelle est la v3.[6]
Théoriquement, le protocole SSL permet la sécurisation de tout protocole applicatif qui s'appuie sur la pile TCP/IP, tels que HTTP, LDAP, SMTP, FTP,...

Dans la pratique, les implémentations de SSL éprouvées s'appliquent surtout à http et LDAP, donnant ainsi naissance aux protocoles biens connus HTTPS (HTTP sur SSL) et LDAPS (LDAP sur SSL).

1.1.3.2 Fonctionnement

Les protocoles SSL/TLS fonctionnent entre le protocole transport (TCP ou UDP) et le niveau applicatif pour sécuriser un protocole nativement peu sûr. Citons par exemple le protocole HTTPS (port 443) ou le protocole LDAPS (port 636).

Les protocoles SSL et TLS sont subdivisés en quatre sous protocoles :

- **Handshake :** *Handshake* est le protocole d'établissement d'une connexion SSL. Il permet d'authentifier les parties client-serveur et de négocier les paramètres cryptographiques (choix de l'algorithme de chiffrement, de l'algorithme de calcul du code d'authentification MAC, des clés de chiffrement, etc.).
- **Record :** *Record* est un protocole d'enregistrement. Pour une même connexion SSL, il offre à la fois les services de confidentialité, par le biais de l'algorithme cryptographique à clé secrète retenu, et d'intégrité des messages échangés, par le biais du calcul du code d'authentification MAC pour chaque message échangé. Des fonctions de fragmentation et de compression des données sont en outre réalisées.
- **Alert :** *Alert* est un protocole d'alerte. Il permet d'échanger des messages prédéfini sur les états d'une connexion SSL, tels que la fermeture d'une connexion, notamment lorsqu'un certificat a été révoqué, qu'il a expiré, qu'il est vicié, etc.
- **CCS :** *CCS* (Change Cipher Security) est un protocole de modification des spécifications de chiffrement. Il permet de modifier les paramètres de chiffrement d'une connexion SSL.

Ces quatre sous-protocoles s'organisent comme présenté dans la figure suivante :

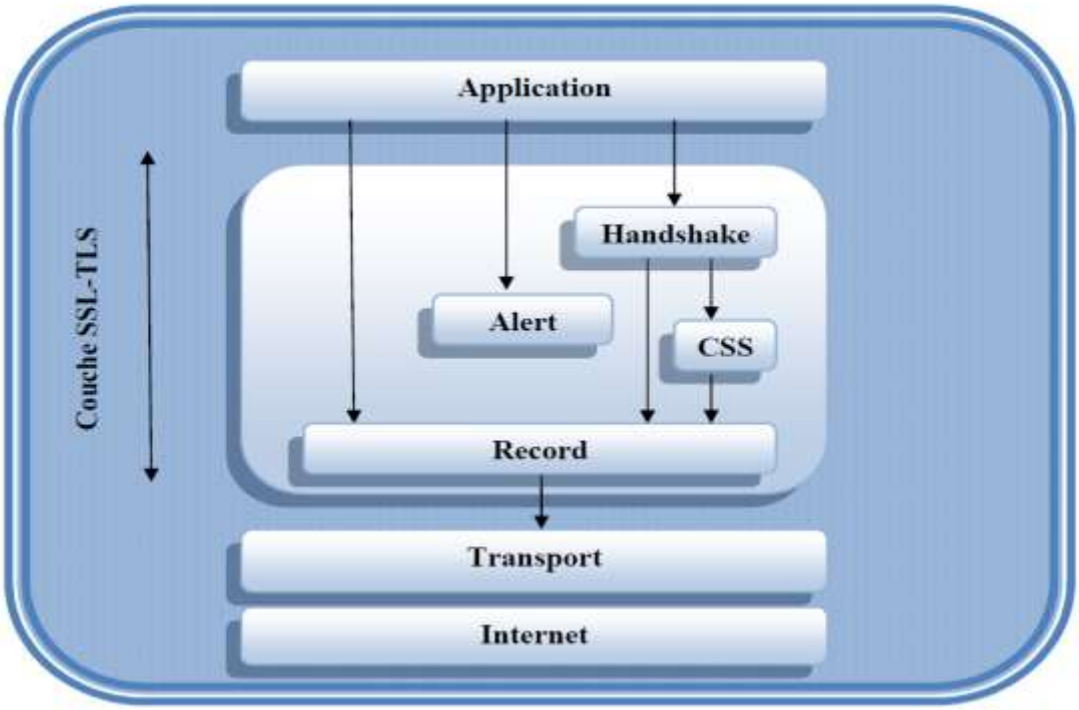

Figure 1.7 : Protocole SSL/TLS

1.1.3.3 La négociation SSL (Traduire ce processus sous forme de schéma)

La sécurisation des transactions par SSL est basée sur un échange de clés entre client et serveur. Le mécanisme est le suivant[7] :

1. Le client envoie au serveur plusieurs informations pour définir notamment la version du protocole SSL utilisé, les paramètres de chiffrement utilisés, etc.
2. Le serveur envoie ensuite au client son certificat de clé publique. Il demande éventuellement au client qu'il envoie son propre certificat si une authentification du client par certificat est requise.
3. Le client utilise les informations du certificat du serveur pour authentifier le serveur.
4. Le client est alors en mesure d'envoyer au serveur une « pré » clé secrète, qu'il chiffre avec la clé publique du serveur.

5. Le serveur peut déchiffrer ensuite la « pré » clé secrète à l'aide de sa clé privée. Le serveur et le client réalisent une même série d'opérations pour obtenir des clés secrètes de session à partir de la « pré » clé secrète et des données aléatoires échangées dans les étapes précédentes.

6. Le client envoie ensuite un avertissement au serveur indiquant que les prochains messages seront chiffrés. Puis il envoie un message (chiffré cette fois) qui signifie que la phase de négociation est terminée.

7. Le serveur envoie alors lui aussi un avertissement au client qui indique que les prochains messages seront chiffrés. Il envoie un message (chiffré cette fois) qui signale que la phase de négociation est terminée. La session SSL est ainsi complètement établie.

1.1.4 Infrastructure à clé publique (PKI)

1.1.4.1 Présentation des PKI

Comme son nom l'indique, une infrastructure à clés publiques (PKI) appelée aussi PKI est un ensemble de moyens matériels, de logiciels, de composants cryptographiques, mis en œuvre par des personnes, combinés par des politiques, des pratiques et des procédures requises, qui permettent de créer, gérer, conserver, distribuer et révoquer des certificats basés sur la cryptographie asymétrique[5].

Cette infrastructure va permettre de mettre en œuvre des services de sécurité tels que l'authentification, l'intégrité, la confidentialité et la non-répudiation des échanges électroniques.

L'infrastructure de gestion de clés publiques offre en plus les services suivants :

- service d'enregistrement des utilisateurs ;
- service de génération de certificats ;
- service de renouvellement de certificats ;
- service de révocation de certificats CRL ;
- service de publication de certificats ;
- service de publication des listes de révocation ;

- service d’identification et d’authentification.

1.1.4.2 Composante d’une PKI

La PKI est une association de plusieurs composants qui interviennent à différentes étapes mises en œuvre depuis la création du certificat jusqu'à l’utilisation de celui-ci. On distingue ainsi 5 entités dans la PKI[8] :

- ***L’entité d’extrémité (EE) :*** Les entités d’extrémités sont des utilisateurs, tel qu'un client-mail, un serveur Web ou un navigateur Web. Elles ne sont pas autorisées à délivrer des certificats à d'autres entités.
- ***L'autorité de certification (AC) :*** Composante s’acquittant de la signature des certificats numériques servant à la diffusion des clés publiques, ainsi que du maintien du statut de révocation de ceux-ci.
- ***L'autorité d'enregistrement (AE) :*** Une AE ou RA (RegistryAuthority) est une fonction administrative qui enregistre les entités de la PKI. L’AE est digne de confiance pour identifier et authentifier les entités en fonction de la politique de CA. Il peut y avoir une ou plusieurs RA connectées à chaque autorité de certification de la PKI.
- ***L’émetteur de liste de révocation de certificats (CRL) :*** Composante qui s’acquitte de la génération des listes de révocation de certificats. Cette tâche est souvent réalisée par l’AC.
- ***l’autorité de dépôt (Repository)*****:** Système distribué où sont stockés les certificats ainsi que les listes de révocation, afin que les utilisateurs puissent les récupérer librement. Ce dépôt prend généralement la forme d’un annuaire de type LDAP.

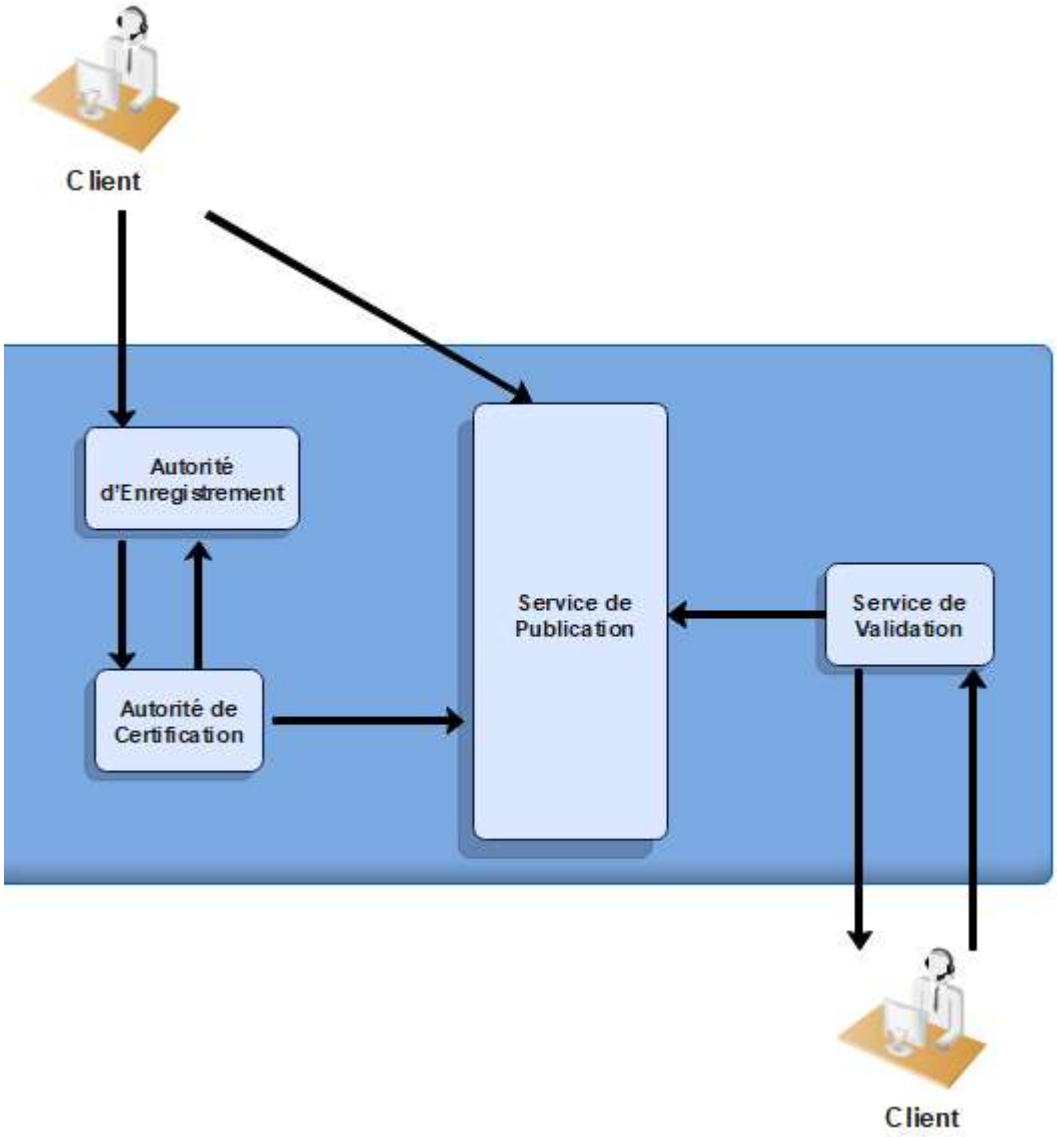

Figure 1.8 : Les composants d'une PKI.

La figure « Figure 1.8 » montre la place de chaque composante et le processus de gestion des certificats. Ce dernier inclut les étapes suivantes :

1. L'utilisateur fait sa demande à l'autorité d'enregistrement

2. L'autorité d'enregistrement vérifie les données d'identification, la possession de la clé privée et valide la requête qui est transférée à l'autorité de certification

3. L'autorité de certification vérifie la validité de la requête et génère le certificat. Le certificat est publié dans l'annuaire et transmis à L'autorité d'enregistrement

4. L'autorité d'enregistrement avertit l'utilisateur que son certificat est disponible

5. L'utilisateur récupère le certificat dans l'annuaire

6. L'utilisateur envoie au répondeur OCSP une requête pour vérifier l'état du certificat.

7. Le répondeur OCSP récupère la liste des certificats révoqués à partir du service de publication
8. Le répondeur OCSP envoie la réponse à l'utilisateur.

Il existe d'autres composantes non mentionnées dans les documents de l'IETF, mais qui peuvent être nécessaires dans certains cas :

- ***l'Autorité de séquestre :*** Composante qui détient les clés nécessaires pour déchiffrer les données chiffrées. Dans certaines circonstances, l'autorité de séquestre permet à un tiers autorisé d'accéder à ces clés.
- ***Serveur OCSP :*** Composante ayant pour but de vérifier la validité d'un certificat numérique en obtenant son statut de révocation. Le protocole OCSP est définit dans la norme IETF *RFC2560*. Il est un protocole de requête / réponse où un client OCSP récupère le statut de révocation de certificats à partir d'un serveur (répondeur) OSCP au lieu de le récupéré dans la liste de révocation.
- ***Serveur d'horodatage :*** Composante ayant pour mission de garantir électroniquement la date et l'heure d'une opération selon la méthode décrite dans la norme IETF.

1.1.4.3 Cycle de vie des clés et des certificats

L'utilisation de bi-clefs certifiées entraîne la nécessité de la publication en toute confiance de la clef publique. Cette publication doit assurer la validité de clé et l'appartenance de cette clé à la bonne personne. La publication des certificats (des clefs publiques) est faite en utilisant généralement les structures d'annuaires de type LDAP (Lightweight Directory Access

Protocol). Les certificats révoqués sont regroupés dans des listes de révocations (CRL) qui sont des structures de données signées et dont le format est défini par le protocole X509 V2.

Le cycle de vie d'un certificat commence par la création des deux clés publique et privée. Ilse poursuit par la demande de certificat de la part du détenteur des clés, puis par la validation des justificatifs apportés. Viennent ensuite les étapes d'émission du certificat et de son acceptation. La phase suivante comporte l'utilisation des clés et du certificat, la validation du certificat, sa suspension ou sa révocation. Le cycle s'achève à l'expiration des clés et du certificat et recommence à la phase première.

1.2 ETAT DES LIEUX

1.2.1 Présentation de l'entreprise

1.2.1.1 Historique

La structure **Intelcia** voit le jour en 2000. Elle s'est progressivement imposée comme un acteur majeur des métiers de l'externalisation. Le développement au Maroc et à l'international s'est accéléré avec l'acquisition de la firme **Eurocall** (Maroc) en 2010, de **The Marketingroup** (France) fin 2011, de **Clienteos** (Cameroun) en 2015, d'**Atento** Maroc (opérations pour les marchés français et marocains) ainsi qu'une première implantation au **Sénégal** en 2016.[9]

Grâce à une stratégie basée sur la proximité de ses clients et de ses collaborateurs, et l'excellence dans ses opérations, le groupe a porté en quelques années son chiffre d'affaires à plus de 100 millions d'euros en 2016 et a développé une relation de confiance avec des grands donneurs d'ordres internationaux.

Intelcia fournit une offre globale Onshore-Nearshore-Offshore et plusieurs services avec une démarche de partenaire à valeur ajoutée. **Intelcia** a notamment développé une expertise dans plusieurs métiers : le **BPO** (business process outsourcing) **commercial**, la

gestion proactive de la relation client, le **support technique**, le **service client**, les **enquêtes et sondages**, et l'insourcing.

On retrouve Intelcia en **France**, au **Maroc**, en **Côte d'Ivoire**, au **Sénégal** et au **Cameroun**.

Au Cameroun nous n'avons qu'un seul site et à sa tête se trouve son illustre Directeur Général M. **Jean-Yves Kotto**.

1.2.1.2 Fiche d'identification

Les informations relatives à la structure (INTELCIA) qui nous accueillit sont répertoriées dans le tableau ci-dessous :

Tableau 1.4 : Fiche d'identification d'INTELCIA

Raison Sociale	**INTELCIA CAMEROUN**
Date de Création	**2015**
Forme Juridique	**S.A**
Capital Social	**10 000 000 €**
Boite Postale	**12995 DOUALA**
Activité Principale	**Externalisation des services**
Téléphone	**233503110**
Directeur Général	**Jean-Yves KOTTO**
Siège Social	**Ancienne SONEL, Rue Bebey EYIDI**
Email	**www.Intelcia.com**

1.2.1.3 Valeurs

❖ **Le service à la clientèle** : En tant qu'organisation de classe mondiale, nous comprenons que nous existons pour servir et satisfaire nos différents clients selon leurs multiples besoins. Nous tissons des liens solides avec nos clients et nous prenons l'intimité ; l'intégrité et l'apprentissage comme fer de lance.

❖ **L'esprit d'entreprise** : Nous cherchons continuellement à développer de nouvelles affaires en utilisant des méthodes nous permettant de conserver notre position de leader sur le marché de l'externalisation.

❖ **Excellence :** Intelcia est une grande organisation, en travaillant de façon soudée et en s'appuyant sur l'expérience de ses employés et sur ses différentes années sur le marché, la société fournit et commercialise des produits avec une qualité supérieure.

❖ **Leadership :** Il asphyxie littéralement ses concurrents, il est le meneur incontestable et incontesté du marché de l'externalisation au Cameroun.

1.2.1.4 Activités

Intelcia offre comme services :

❖ L'externalisation des services ; Infogérance

❖ Gestion des services en multicanal ; Publicité digitale ; Production de contenu digital

1.2.1.5 Organisation de l'entreprise

L'entreprise INTELCIA CAMEROUN possède une structure basée sur trois catégories de fonctions principales à savoir : les fonctions administratives, les fonctions managériales et les fonctions opérationnelles :

Fonctions administratives :

➢ **La Direction Générale**

La direction générale a pour vocation première de définir la politique générale d'Intelcia en rapport avec son objet. Elle élabore et met en œuvre la stratégie

d'accomplissement de l'objet social en louant les ressources humaines, matérielles et financières. Elle est aussi chargée de l'exécution des orientations et programmes arrêtés en vue de l'atteinte des objectifs fixés.

- **Les Directions Centrales**

Elles sont placées sous la hiérarchie de la Direction Générale. Elles constituent les organes de préparation, d'orientation et d'application des lignes directrices tracées par la Direction Générale.

Elles sont constituées comme décrit ci-dessous :

- **La Direction de l'Audit Général (DAG)**
- **La Direction Centrale des Opérations (DCO)**
- **La Direction du Développement des ressources humaines (DDRH)**
- **La Direction de la Communication et du Marketing (DCM)**
- **La Direction de l'Information et des Nouvelles Technologies (DINT)**
- **La Direction des Moyens Généraux (DMG)**
- **La Direction de l'Organisation et de la Qualité**
- **Les fonctions opérationnelles** :

- **Le chargé de clientèle**
- **Le télé-enquêteur**
- **L'ingénieur support technique**
- **Le conseiller marketing**
- **L'ingénieur commercial**

- **Les fonctions managériales :**

- **Le responsable d'équipe**
- **Le coordinateur d'activité**
- **Le manager d'activité**

1.2.2 Architecture de l'existant

Ce schéma décrit l'architecture globale du réseau.

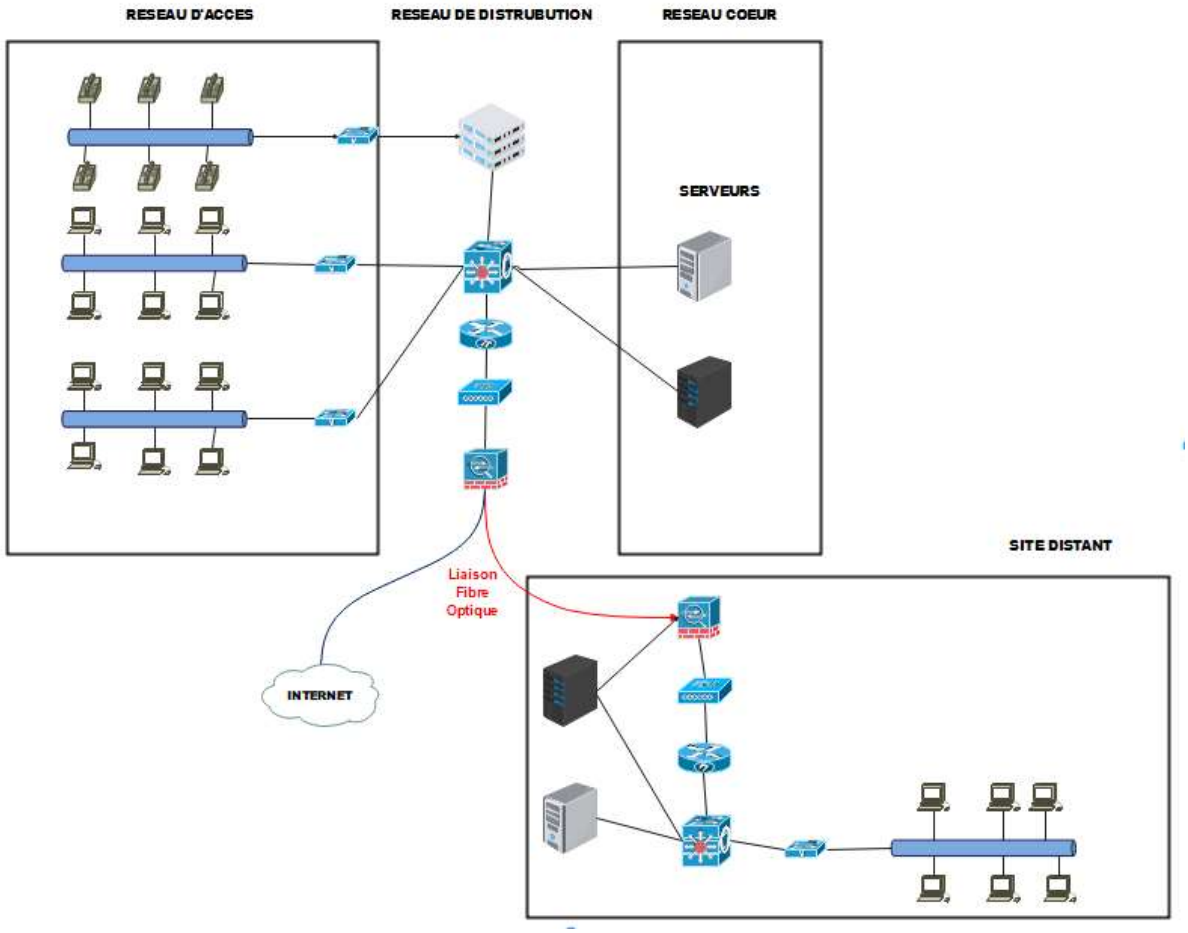

Figure 1.9 : Architecture du réseau de l'entreprise

1.2.3 Limites de l'existant

L'Internet fait du monde un endroit plus agréable à vivre, mais les décisions prises aujourd'hui façonneront le paysage en ligne et la façon dont nous l'utiliserons tous pendant des décennies. Car aujourd'hui bien qu'internet offre une pléthore de services uniques pour l'innovation, la créativité et les activités économiques, il est aussi le terrain de jeu préféré des cybercriminels, des virus de toutes natures et des fraudes. L'infrastructure d'INTELCIA est donc exposée aux attaques de cybercriminels vu que la sécurité n'est pas optimale. Les pare-feu présents sur le site et les logiciels visant à extraire les logiciels malveillants n'assurent pas

sur tous les différents aspects de la sécurité ce qui crée des insuffisances dans le système informatique.
L'infrastructure IT d'INTELCIA rencontre donc plusieurs difficultés liées à la sécurité informatique à savoir :

- Sécurisation des serveurs de messagerie professionnelle d'INTELCIA
- La sécurisation des emails
- La gestion des identités et accès au réseau, aux applications
- La prévention des intrusions et de cryptage du trafic réseau

CONCLUSION

Dans ce chapitre, nous avons explicité la notion d'infrastructure à clé publique et son rôle important dans la sécurité des réseaux informatiques. En effet, au fil des ans, de nombreux travaux de recherche ont été menés pour améliorer la sécurité et la fiabilité des PKI. Des normes et des recommandations ont été développées pour assurer l'interopérabilité et la sécurité des PKI à travers différents systèmes et applications. Les PKI utilisent des certificats numériques pour garantir l'authenticité et la confidentialité des données, et elles sont utilisées dans de nombreux domaines, tels que les transactions bancaires en ligne, les systèmes de gestion des identités, les échanges de courriers électroniques sécurisés, et bien plus encore. Dans le chapitre suivant, nous allons présenter notre projet ainsi que les outils utilisés.

CHAPITRE 2 : MATERIEL ET METHODES

INTRODUCTION

Dans cette partie de notre étude, nous allons nous concentrer sur les méthodes et les matériels utilisés pour mettre en place une PKI. Nous allons explorer les différentes étapes de la mise en place d'une PKI, telles que la génération de clés, la création de certificats, et la mise en place des politiques de sécurité. Nous allons également examiner les différents outils et méthodes de déploiement utilisés pour la mise en place d'une PKI.

2.1 MATERIEL ET OUTILS

2.1.1 Outils de création des certificats

2.1.1.1 OpenSSL

OpenSSL est une boîte à outils cryptographiques implémentant les protocoles SSL et TLS qui offre[10] :

1. une bibliothèque de programmation en C permettant de réaliser des applications client/serveur sécurisées s'appuyant sur SSL/TLS.
2. une commande en ligne (openssl) permettant
    - la création de clés RSA, DSA (signature)
    - la création de certificats X509
    - le calcul d'empreintes (MD5, SHA, RIPEMD160, ...)
    - le chiffrement et déchiffrement (DES, IDEA, RC2, RC4, Blowfish, ...)
    - la réalisation de tests de clients et serveurs SSL/TLS
    - la signature et le chiffrement de courriers (S/MIME)

Pour connaître toutes les fonctionnalités de openSSL : man openssl.

La syntaxe générale de la commande openssl est :

$ openssl <commande> <options>

2.1.1.2 Outils de gestion des certificats

Ce tableau résume quelques outils de certification :

Tableau 2.1 : Comparaison entre les différentes CA

Outils	**Sectigo**	**GlobalSign**	**Digicert**
Protection de domaine	1 seul domaine	1 ou plusieurs domaines	Plusieurs domaines
Coût	Moyen	Élevé	Élevé
Chiffrement	SHA 2	SHA 256, ECC	RSA, DSA, ECC

2.1.1.3 Service AD CS

Selon Microsoft, AD CS joue le "rôle de serveur qui vous permet de construire une infrastructure à clé publique (PKI) et de fournir des fonctionnalités de cryptographie à clé publique, de certificats numériques et de signature numérique à votre organisation".

En réalité, il est relativement simple de créer votre propre AC et de signer une poignée de certificats avec des outils tels qu'OpenSSL. Vous pouvez également acheter quelques certificats auprès d'une AC comme GlobalSign et les installer manuellement. Mais AD CS fait plus que cela. Il permet à votre organisation de distribuer des certificats à partir d'une AC à grande échelle, pour des entreprises comptant des milliers d'employés et encore plus de machines. Comment cela fonctionne ?

Comme son nom l'indique, Active Directory est un service d'annuaire pour les réseaux de domaines Windows. Par conséquent, la pierre angulaire de chaque mise en œuvre d'Active Directory est le service de domaine Active Directory (AD DS). AD DS stocke des informations sur les utilisateurs, les ordinateurs et les groupes au sein d'un domaine (tel que globalsign.com),

mais vérifie également leurs informations d'identification et définit les droits d'accès. De la même manière que chaque employé d'une entreprise est enregistré auprès des RH et dispose d'un dossier détaillant toutes ses informations pertinentes, AD DS conserve ces informations pour les membres du domaine. AD DS étant l'annuaire fondamental, les informations qui sont enregistrées dans cet annuaire peuvent être exploitées par d'autres services Active Directory - tels qu'AD CS.[8]

2.1.2 Matériels utilisés

2.1.2.1 Partie matérielle

Pour la réalisation de ce projet on a disposé de :

- Ordinateur portable ayant pour caractéristiques : 8Go de RAM, Disque dur : 700 Go, core i5 de 3eme génération

2.1.2.2 Partie Logicielle

Comme outils logiciels utilisés, on peut citer :

- VMWare Workstation pro
- Phpmyadmin
- Mysql serveur
- Whireshark
- Systèmes d'exploitation : Windows 10, Windows Server 2016
- Navigateurs web : Google Chrome

2.2 METHODES DE MISE EN PLACE DE NOTRE INFRACSTRUTURE PKI

2.2.1 Présentation générale de la solution

Sous Windows Server, vous pouvez déployer une autorité de certification dans l'intranet de votre entreprise en installant le rôle "**Services de certificats Active Directory (AD CS)**".La création d'une autorité de certification dans un intranet vous permet de sécuriser gratuitement de nombreux services accessibles uniquement depuis les ordinateurs de votre entreprise.[11]

Les avantages de déployer une autorité de certification sont notamment :

- **Le prix :** pas besoin d'acheter des certificats SSL onéreux chez GeoTrust, digicert, ...
- **La sécurité :** si le serveur où est installé l'autorité de certification est bien protégé, vous pourrez protéger toutes les communications dans votre réseau local grâce au protocole HTTPS de chaque service (serveur web, serveur RDS, ...)
- **La validité des certificats :** les certificats générés émaneront d'une autorité de certification de confiance (si les ordinateurs clients sont correctement configurés) et ne seront pas auto-signés. En sachant que les certificats auto-signés peuvent être interdits dans certains cas (notamment pour les connexions distantes permettant d'accéder aux RemoteApp).
- **Une seule configuration côté client est requise :** il suffit d'importer le certificat de votre autorité dans le magasin d'autorités de confiances de vos PC clients pour que tous vos certificats soient considérés comme valides.

2.2.2 Préparation de notre Windows serveur

- **Initialisation du serveur**
    - Configurer un mot de passe pour le compte administrateur lors de l'installation

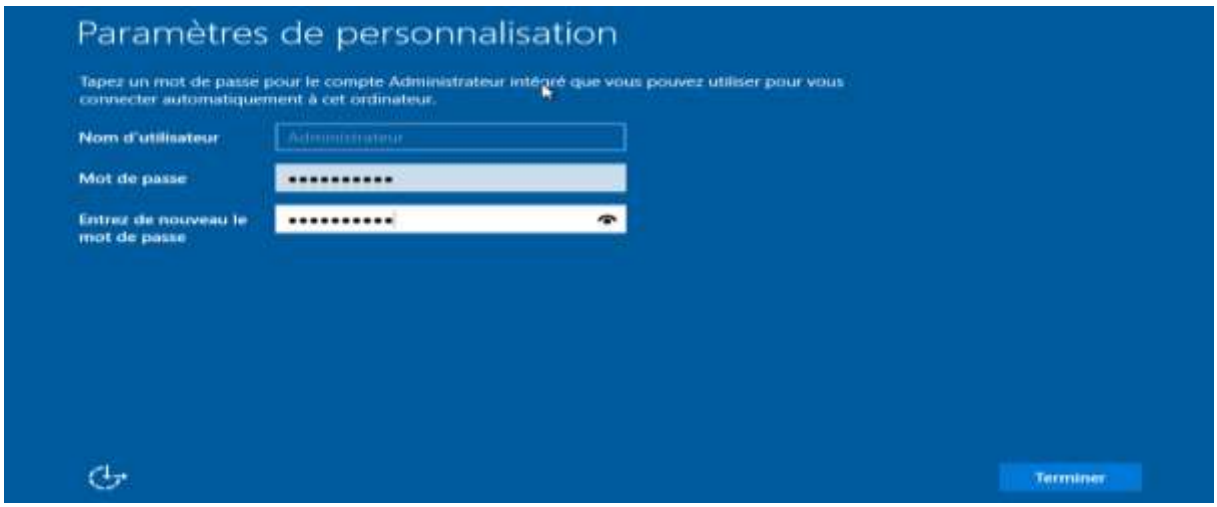

Figure 2.1 : Mot de passe administrateur

- Attribution d'un nom au serveur

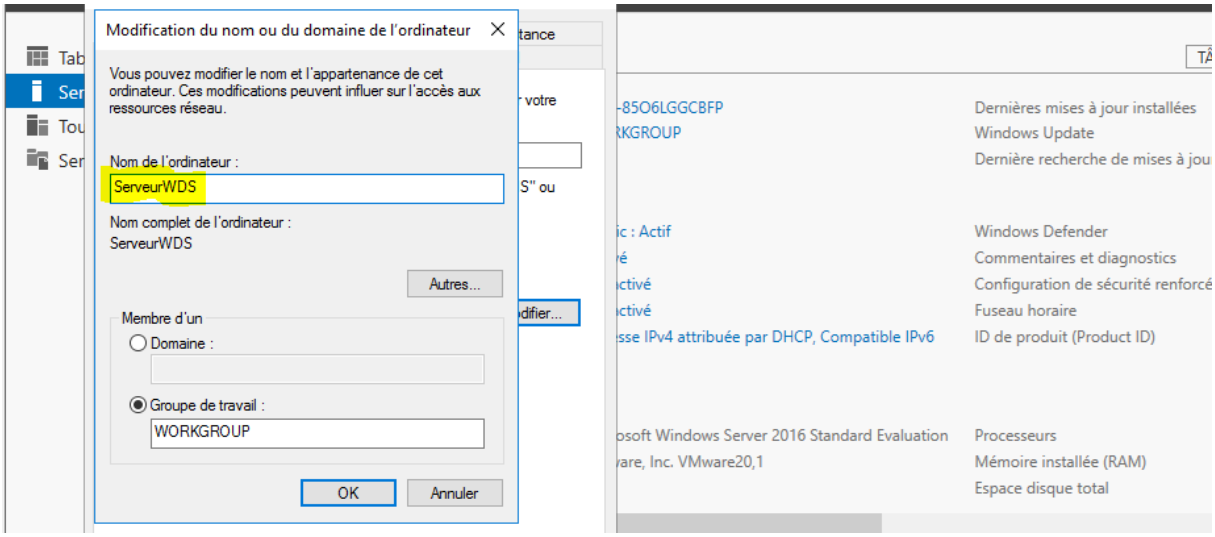

Figure 2.2 : Attribution d'un nom à notre serveur

- Modification de l'adresse IP

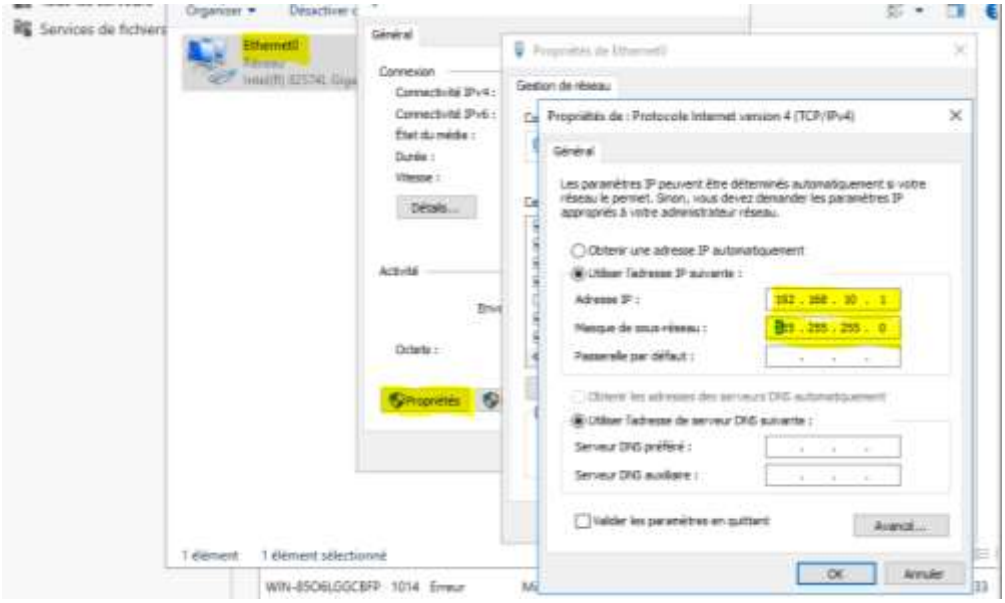

Figure 2.3 : Attribution d'une adresse IP a notre serveur

➢ **Rôles AD DS**

- Ajout du rôle AD DS

Figure 2.4 : Ajouter un rôle

Faites suivant jusqu'à cette fenêtre :

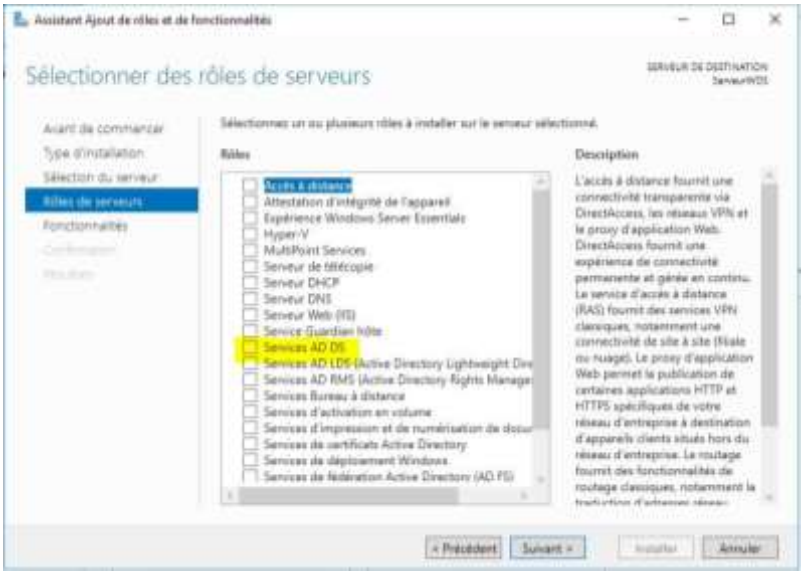

Figure 2.5 : Ajout du service AD DS

Ensuite faite suivant jusqu'à installer :

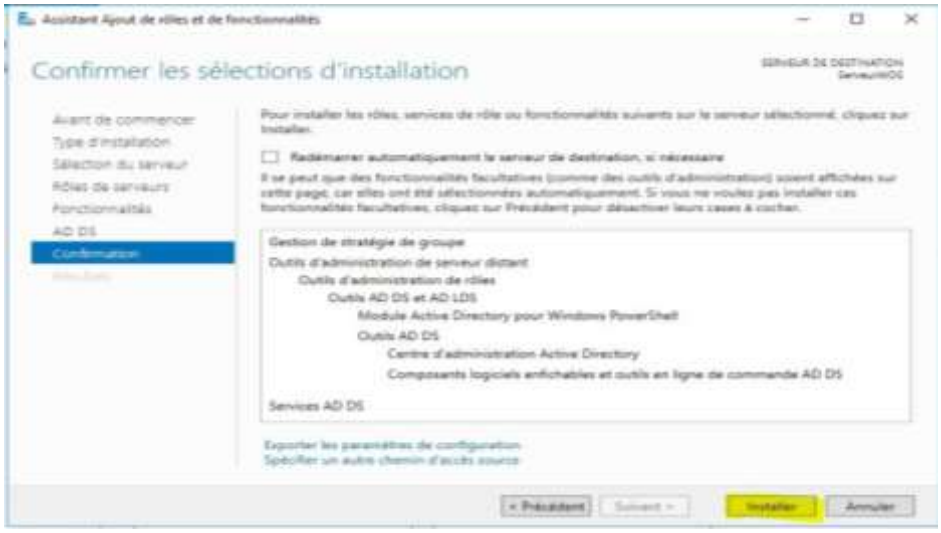

Figure 2.6 : Installation d'AD DS

- **Rôles DNS**
  - Promouvoir ce serveur en contrôleur de domaine[12]

Figure 2.7 : Promotion en contrôleur de domaine

- Entrer le nom du domaine

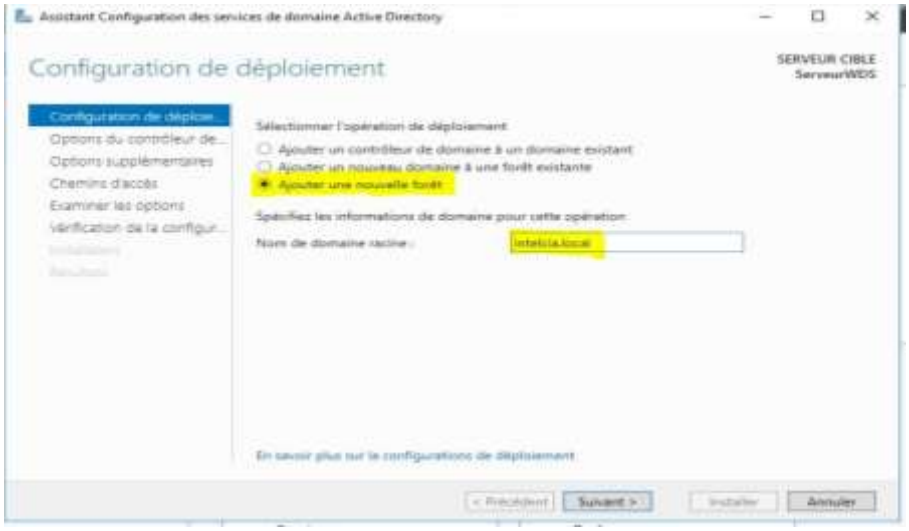

Figure 2.8 : Création d'une nouvelle foret

- Installer le serveur DNS

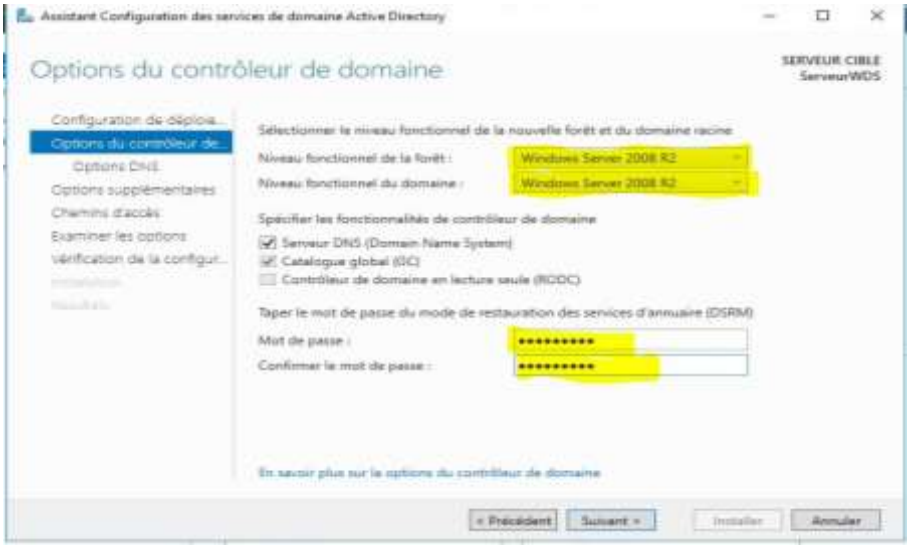

Figure 2.9 : Configuration du mot de passe DSRM

Faites suivants jusqu'à la fenêtre qui nous invite à terminer l'installation.

Votre Serveur va redémarrer et vous demander d'entrer votre mot de passe Administrateur

Figure 2.10 : Première connexion au compte administrateur

- **Rôles DHCP**
    - Ajout du rôle DHCP [13]

Pur ajouter le rôle DHCP faites comme avec le rôle DNS, Ensuite faite suivant jusqu'à cette fenêtre :

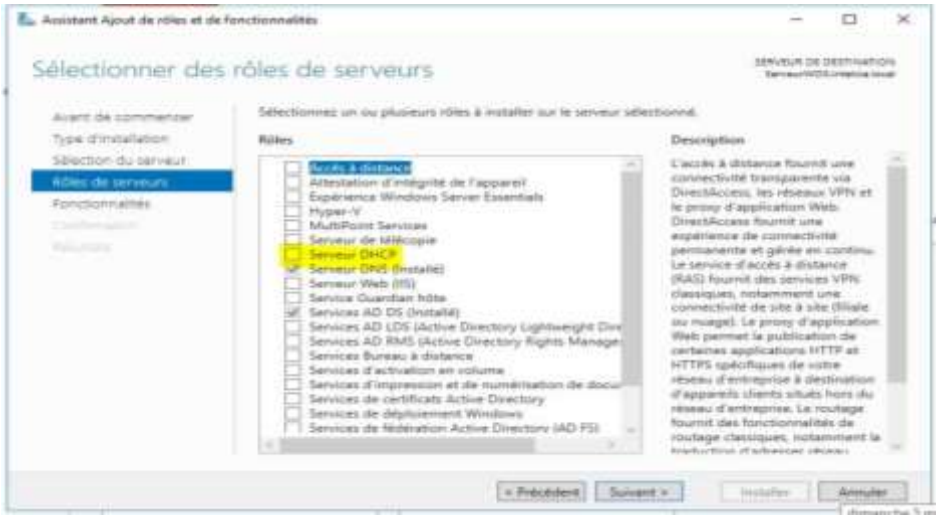

Figure 2.11 : Ajout du rôle DHCP

Puis avancer jusqu'à la fenêtre qui nous invite à terminer l'installation, et lancer l'installation de notre service

- Activation du serveur DHCP

Figure 2.12 : Finaliser la configuration DHCP

Puis suivre les étapes et revenir à la fenêtre principale de Windows server.

- Création d’une étendue DHCP

Pour créer notre étendue DHCP il nous faut aller dans le *Gestionnaire de serveur* > *outils* > *DHCP* Puis créer une nouvelle étendue IPV4

Figure 2.13 : Création de l’étendue DHCP

- Entrer un nom d’étendue et entrer une plage d’adresse pour l’attribution des adresses de manières automatiques

Figure 2.14 : Attribution de la plage DHCP

- Une fois terminé il ne nous reste plus qu’à activer l’étendue

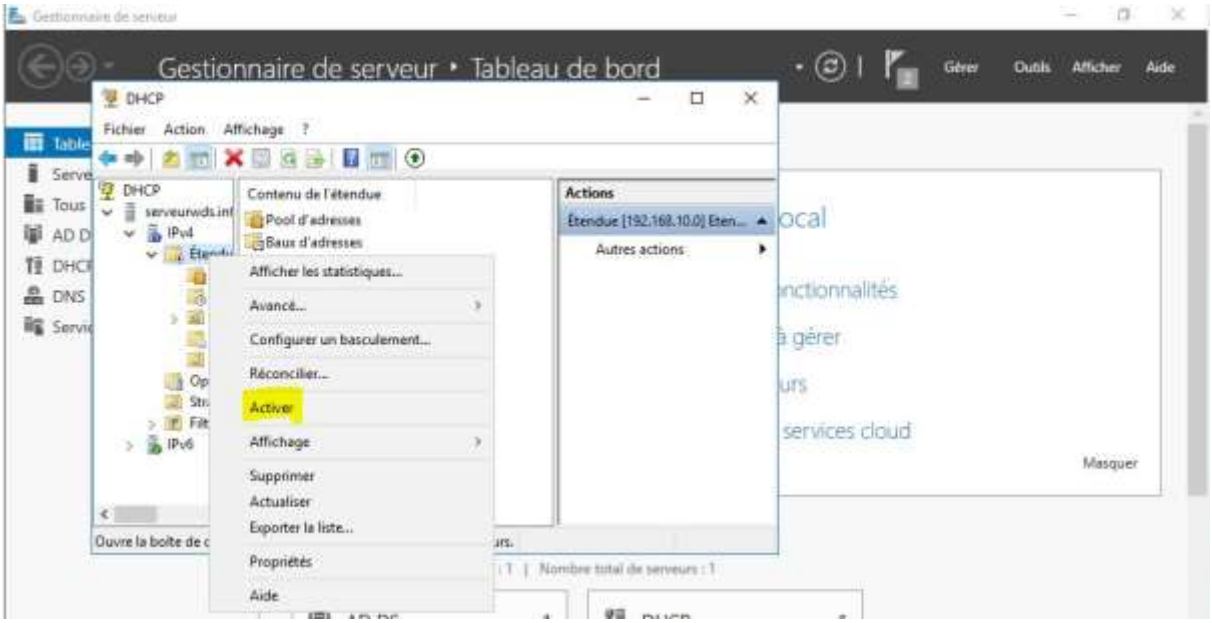

Figure 2.15 : Activation de l'étendue DHCP

2.2.3 Procédure de mise en place de l'autorité de certification

2.2.3.1 Service AD CS

- **Ajout du rôle AD CS**

Pour ajouter le rôle AD CS on procède comme avec les services précèdent, Ensuite faite suivant jusqu'à cette fenêtre [14]:

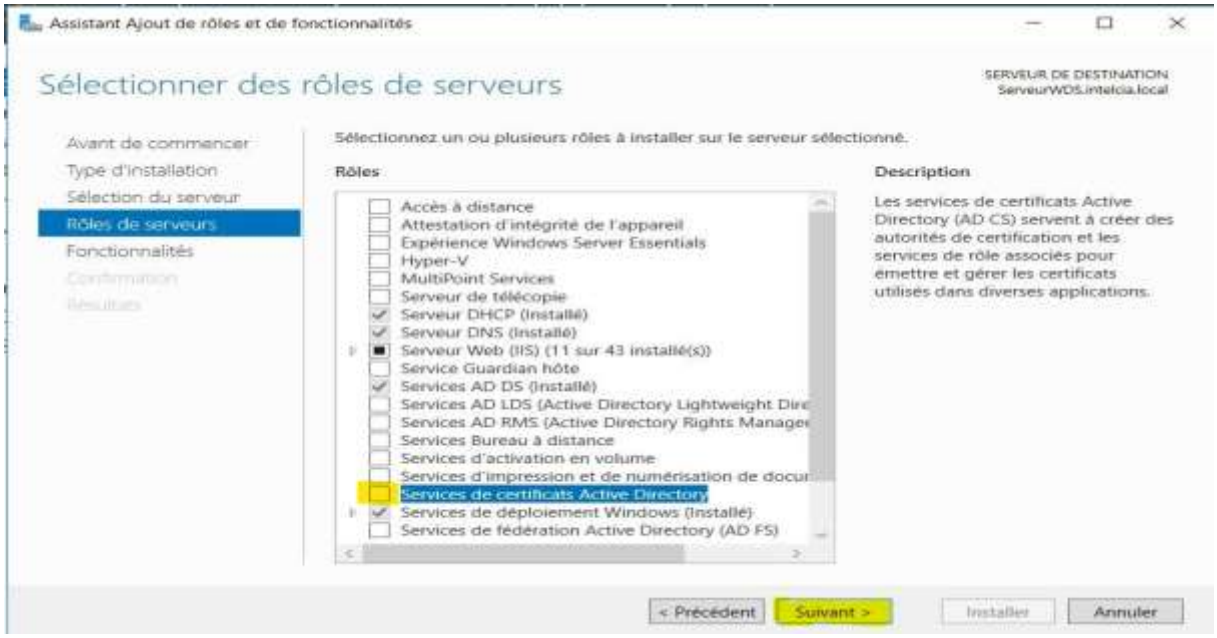

Figure 2.16 : Ajout du rôle AD CS

Puis avancer jusqu'à cette étape ou il faut cocher les deux cases indiquer sur la figure :

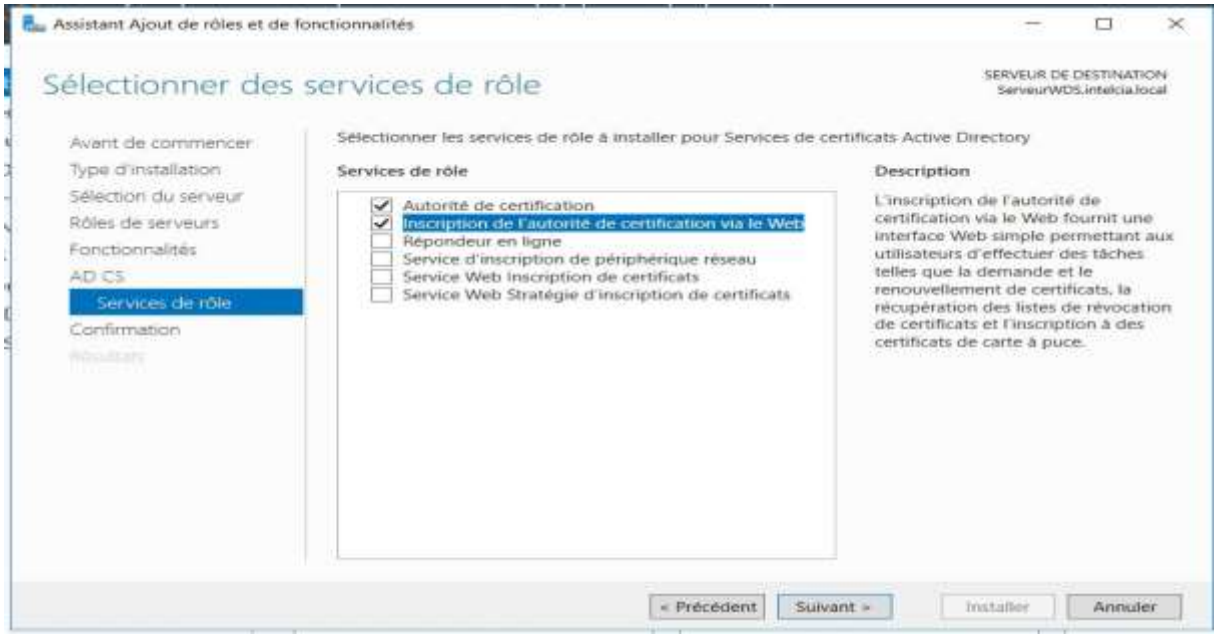

Figure 2.17 : Activer l'inscripteur Web et L'autorité de certification

Puis valider l'installation.

- **Configuration de notre Autorité de certification**

Cliquer sur configurer les services de certificats active directory

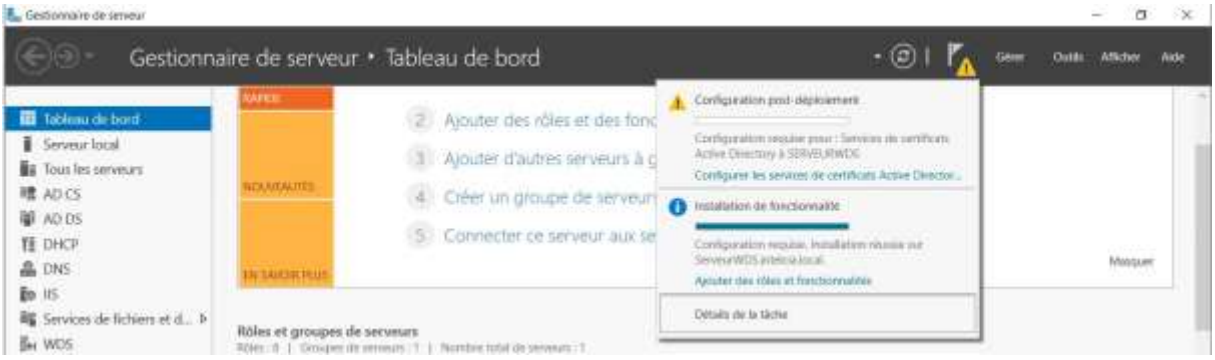

Figure 2.18 : Configuration des Services AD CS

Faire suivan et sélectionner Autorité de certification et inscription de l'autorité via le web :

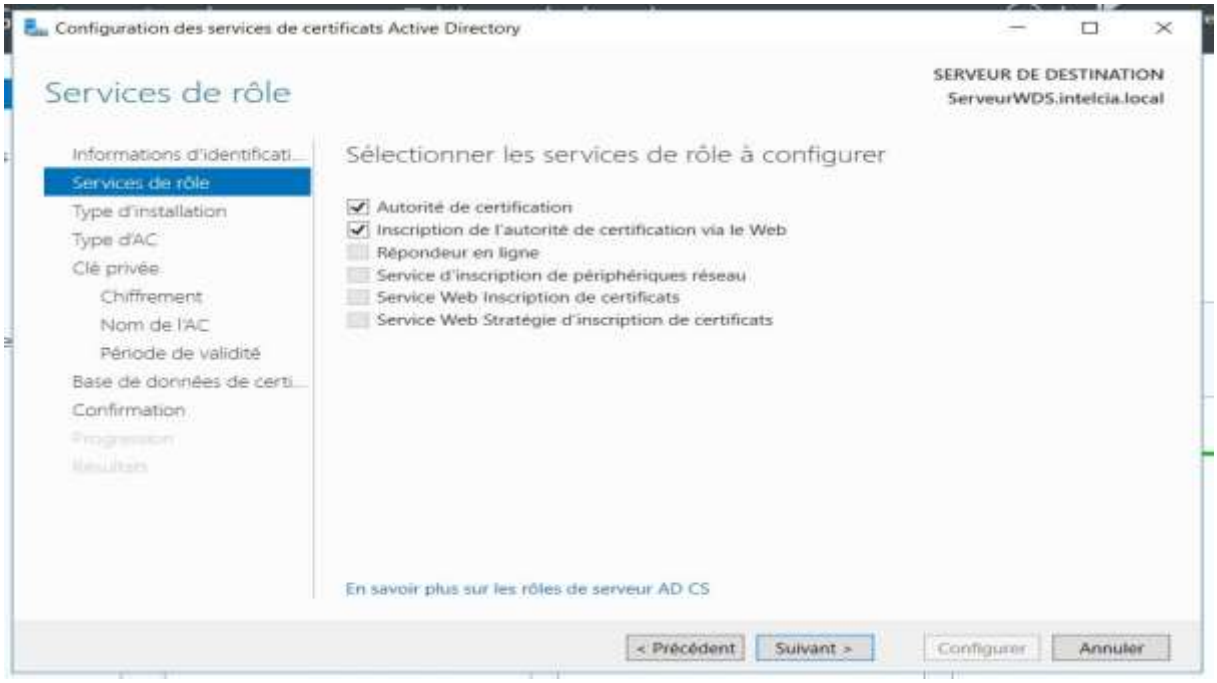

Figure 2.19 : Configuration des services AD CS

Faire suivant

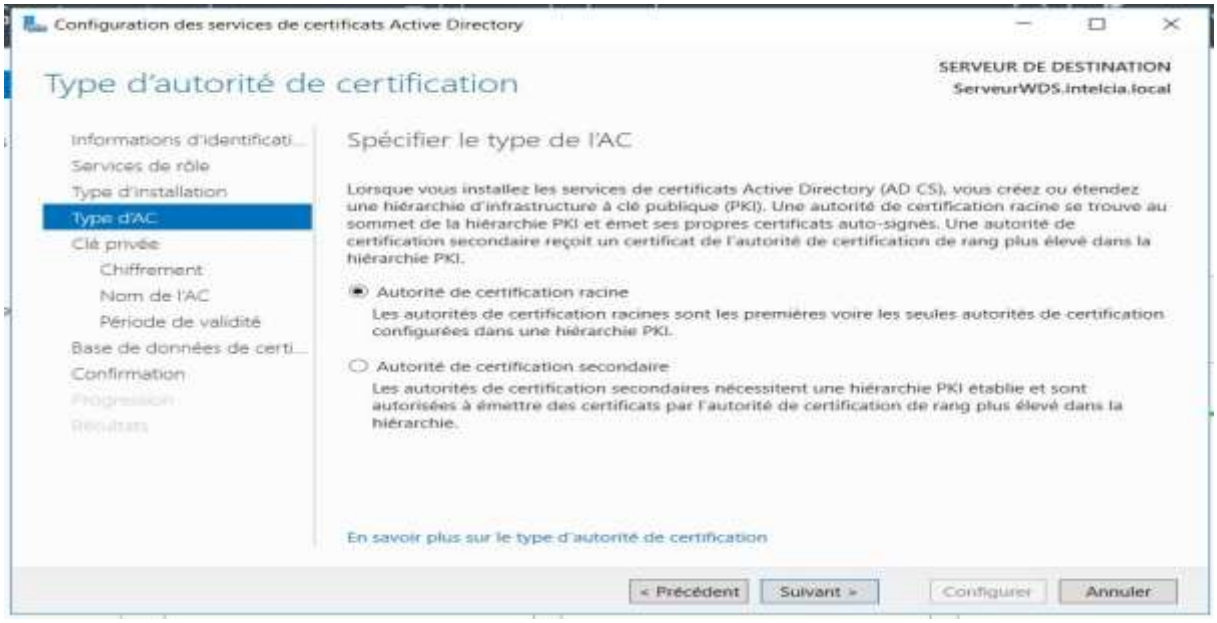

Figure 2.20 : Choix du type d'autorité de certification

Créons notre propre clé privé[14] :

- Selectionner un algorithme de chiffrement

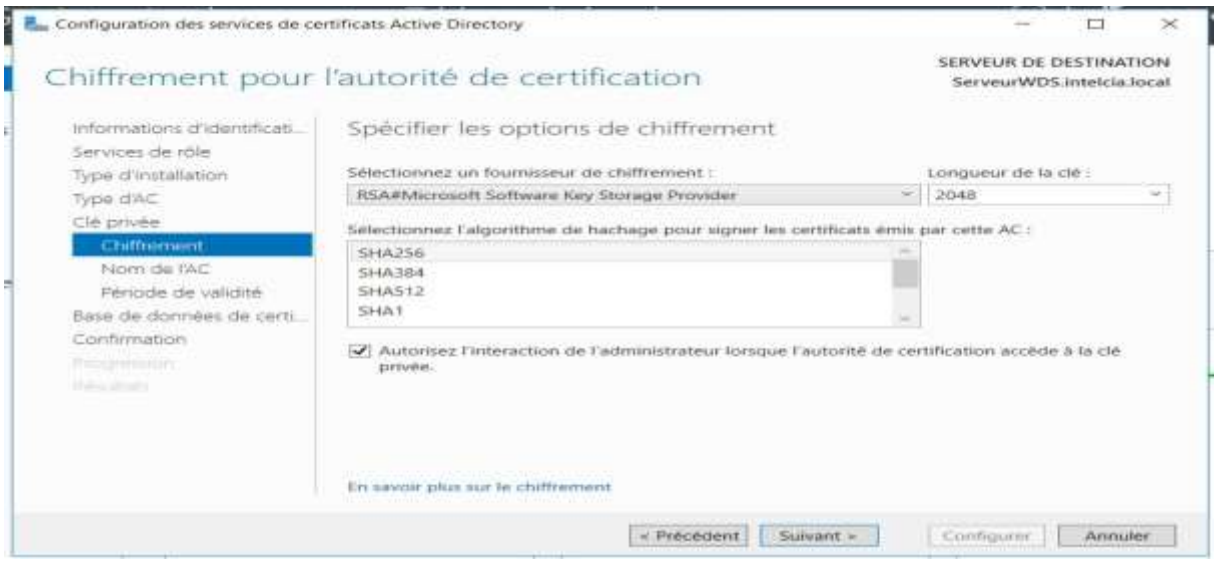

Figure 2.21 : Choix de l'algorithme de chiffrement

Choisir un nom pour notre AC

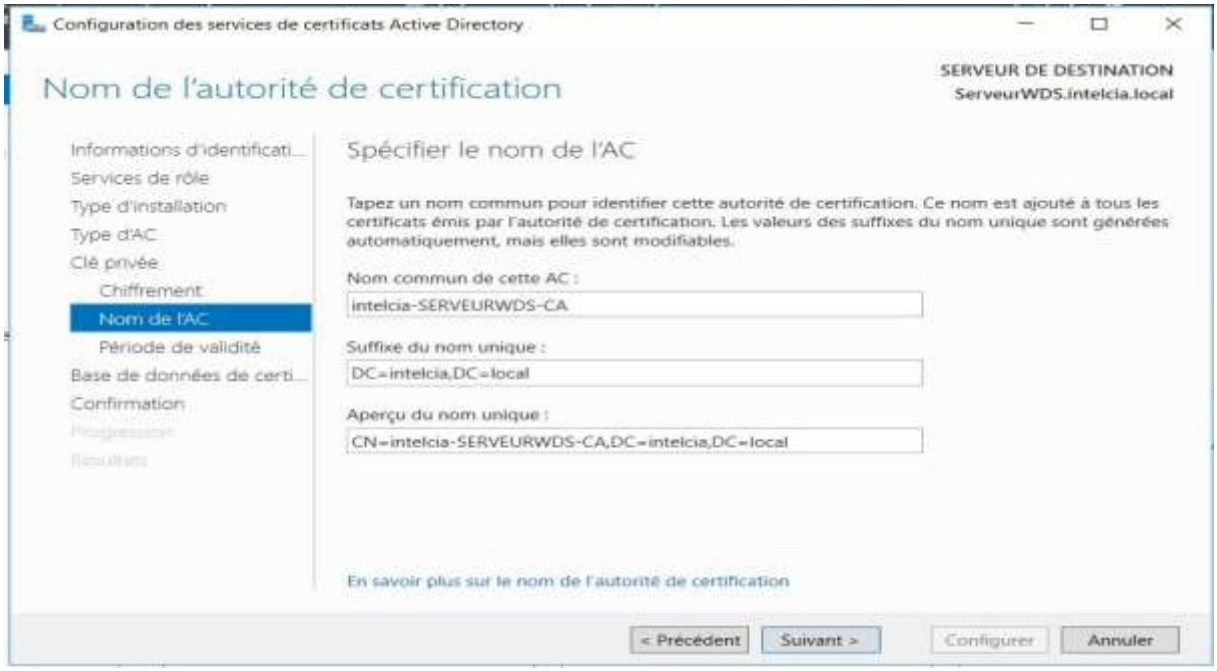

Figure 2.22 : Nom de notre Autorité de certification

Choisir la durée de validité du certificat de l'autorité de certification

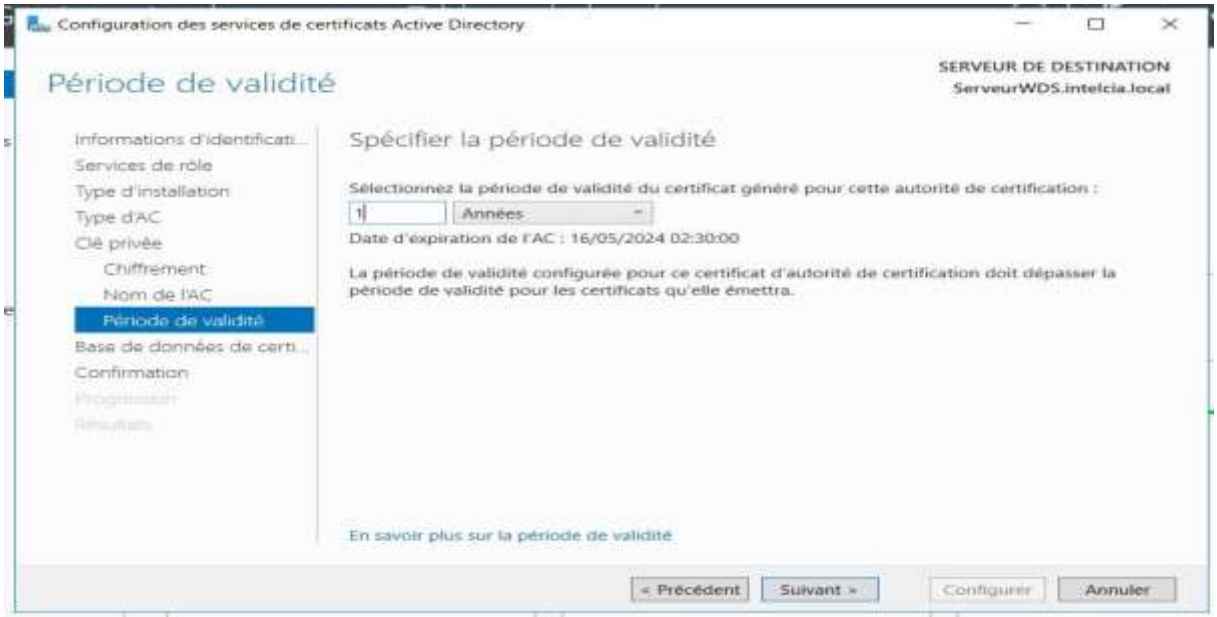

Figure 2.23 : Choix de la durée de validité du certificat

Ici nous avons le résumé de toutes les informations que nous avons choisi

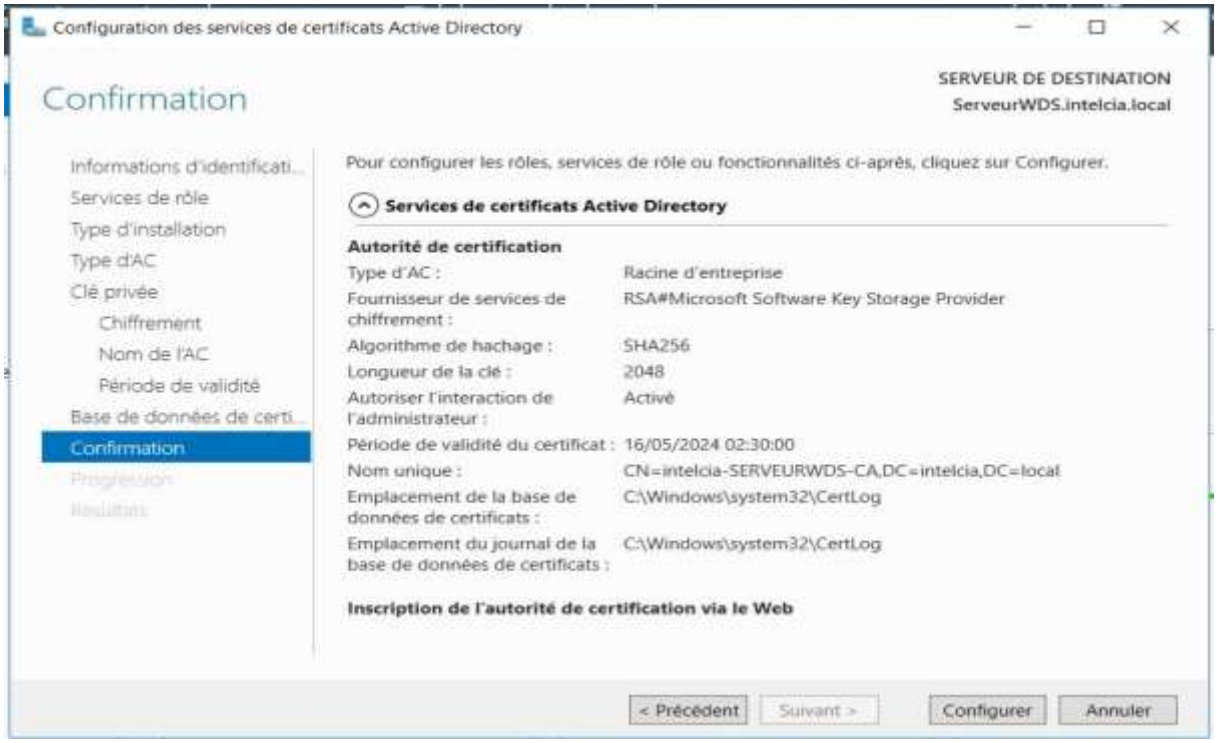

Figure 2.24 : Configurations globale de notre Autorité de certification

C’est bon nous avons configuré notre autorité de certification :

L’outil Autorité de certification s’affiche désormais dans le gestionnaire d’outils

Notre gestionnaire de certificat est desormais disponible

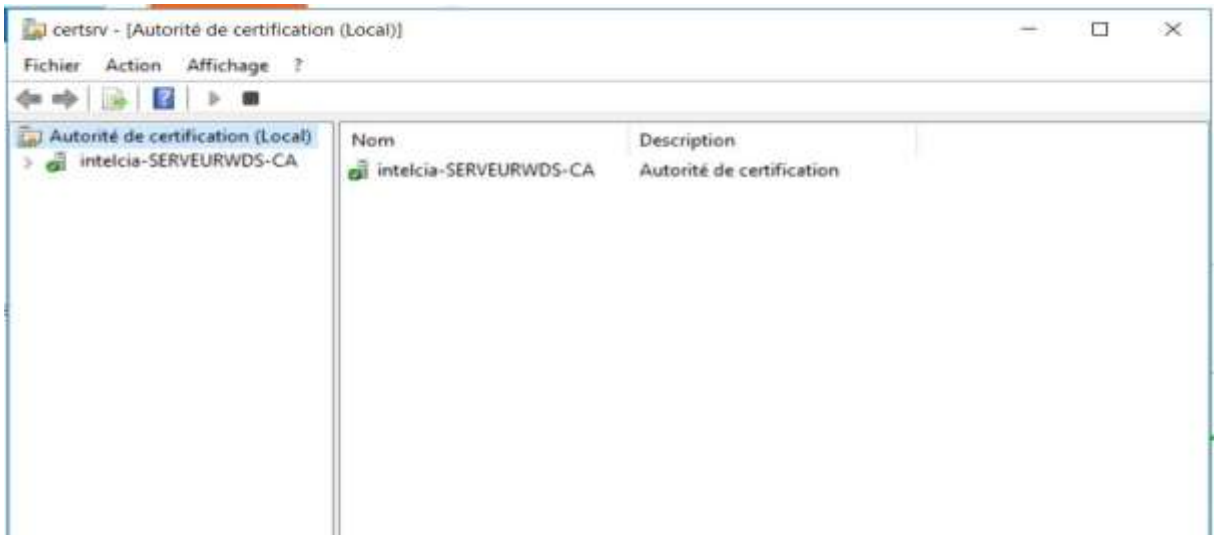

Figure 2.25 : Interface de gestion des certificats

2.2.3.2 Publication d'un certificat via GPO

Pour diffuser efficacement nos certificat dans le réseau on peut utiliser l'outil Windows serveur appelé GPO .une GPO est .Il s'applique à un groupe de sécurité précis ou à tout le domaine. Nous allons donc au préalable créer notre groupe de sécurité ensuite y'ajouter un utilisateur.[15]

Pour créer une GPO il suffit de faire un clic droit sur le nom du GDS et choisir créer et lier une GPO. Désormais il suffit juste de cliquer sur la GPO créer choisir modifier puis sélectionner l'emplacement de la figure suivante :

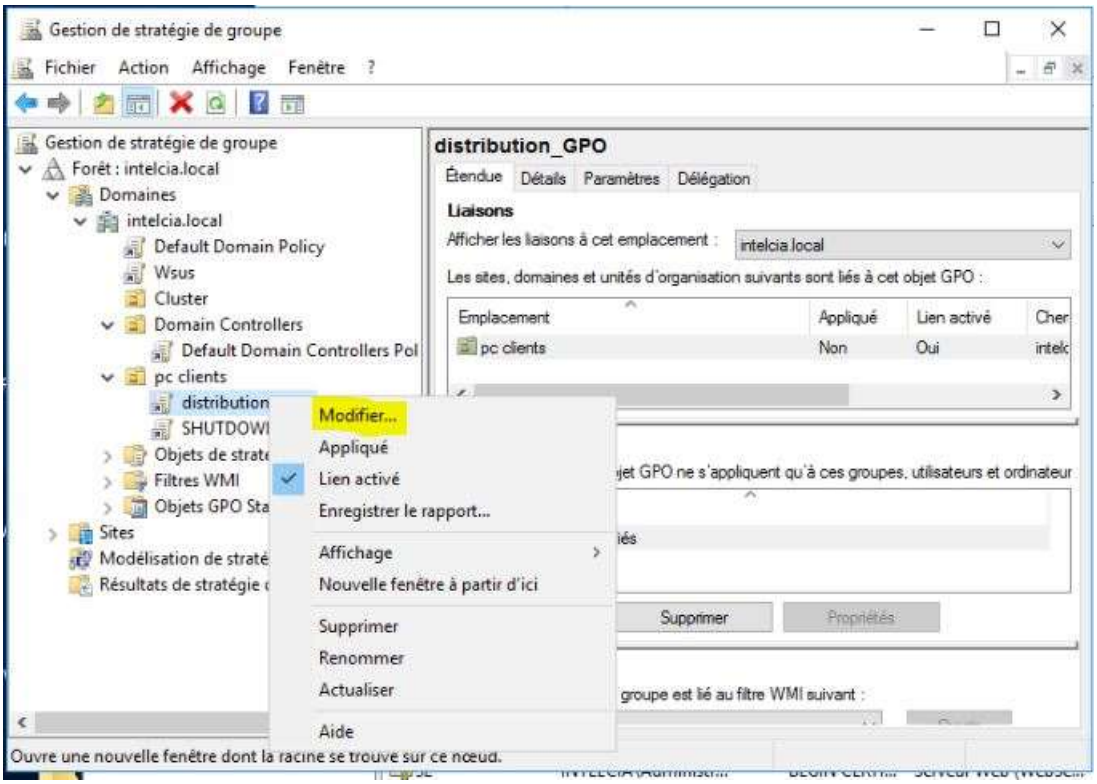

Figure 2.26 : configurer notre GPO

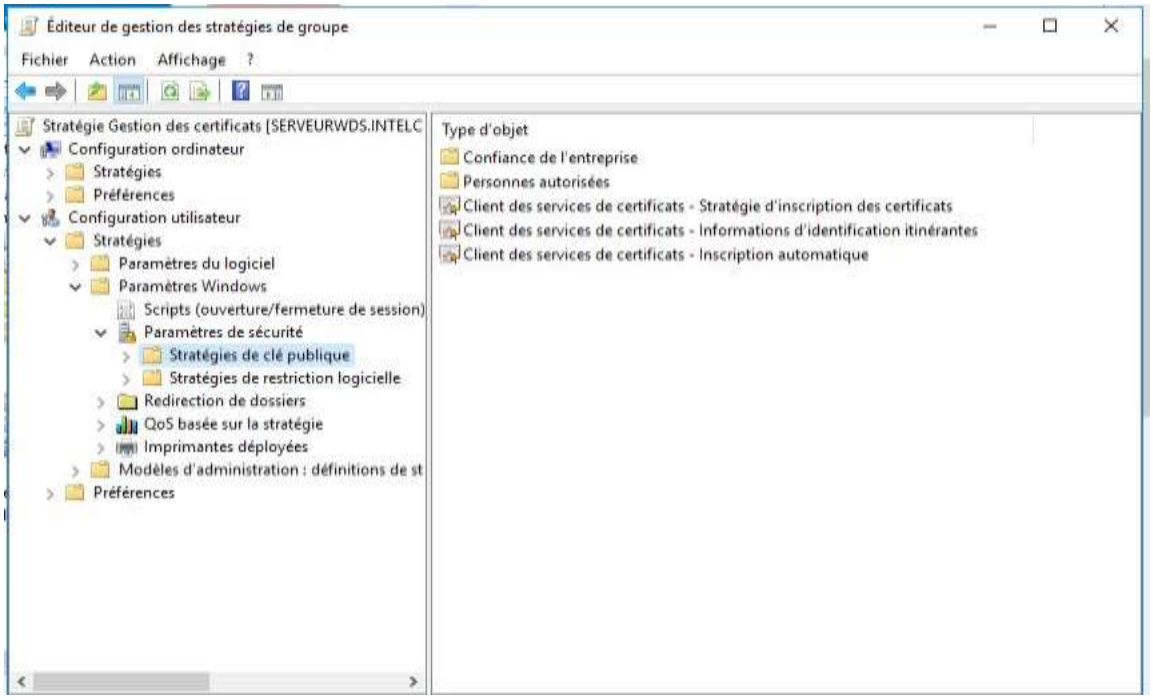

Figure 2.27 : Choix des options de notre GPO

Cocher les différentes options

Figure 2.28 : Configuration des options de la GPO

2.2.3.3 Configuration de l'interface WEB

Une fois le service installé comme nous avons choisi précédemment inscription via le web nous aurons désormais les possibilités de faire la demande de certificat via un site web accessible en tapant le nom de notre serveur suivi de /CertsSrv sur notre navigateur.

On doit renseigner les identifiants d'un utilisateur ayant le droit de faire des demandes ces autorisations peuvent être modifiées dans l'active directory

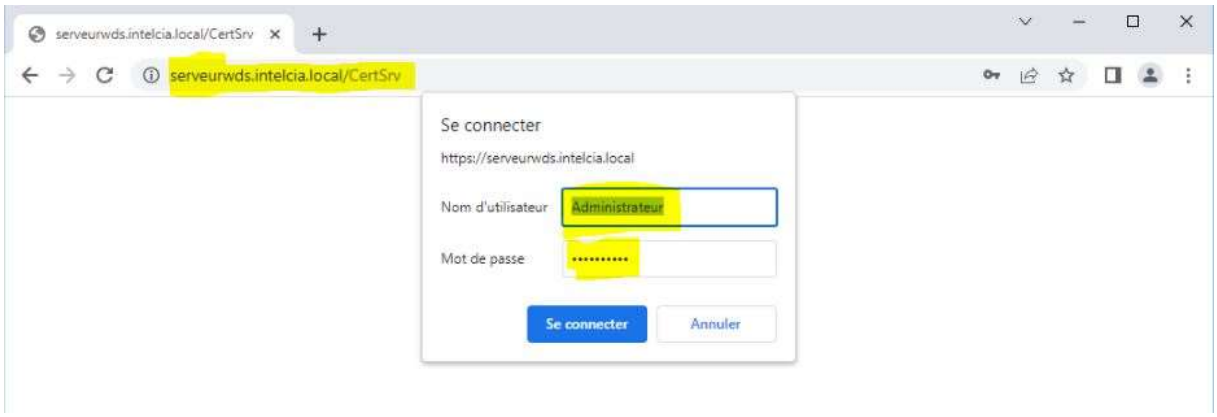

Figure 2.29 : Connexion à l'interface web

On tombe sur cette interface

Figure 2.30 : Page d'accueil de l'interface web

2.2.3.4 Demande d'un certificat

Il existe deux maniérés de faire une demande de certificat la façon manuelle ou l'utilisation du site web. Il suffit d'utiliser le site web offert par Windows serveur pour faire la demande [5]:

Figure 2.31 : Demande de certificat depuis le site web

Ensuite Choisir la méthode demande de certificat

Figure 2.32 : Méthode de demande de certificat

2.2.4 Sécurisation d'un site intranet

2.2.4.1 Hébergement d'un site local sur IIS

Windows server offre un service web appelé IIS qui permet d'héberger nos sites web.

Il suffit de faire un clic droit sur Sites web et choisir ajouter un site web

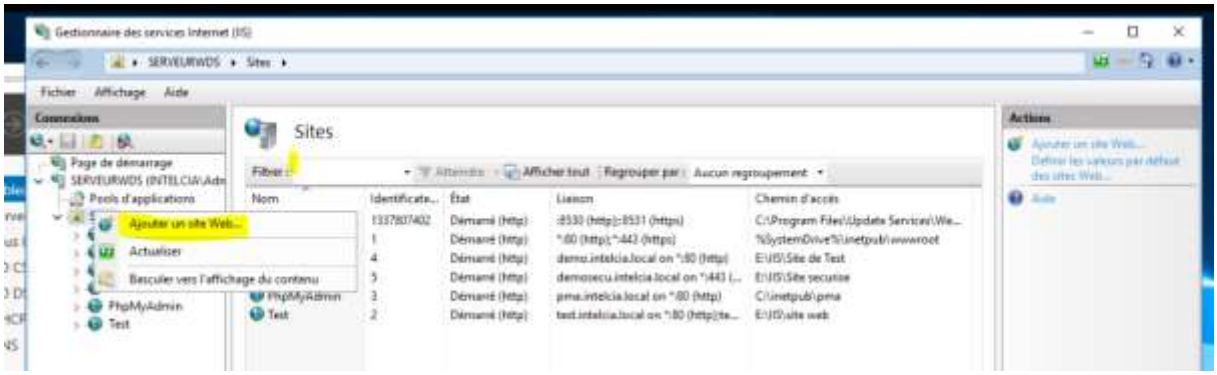

Figure 2.33 : Création d'un nouveau site web

Il faut choisir un nom pour notre site web, un nom de domaine et sélection l'emplacement des fichiers liés au site[16]

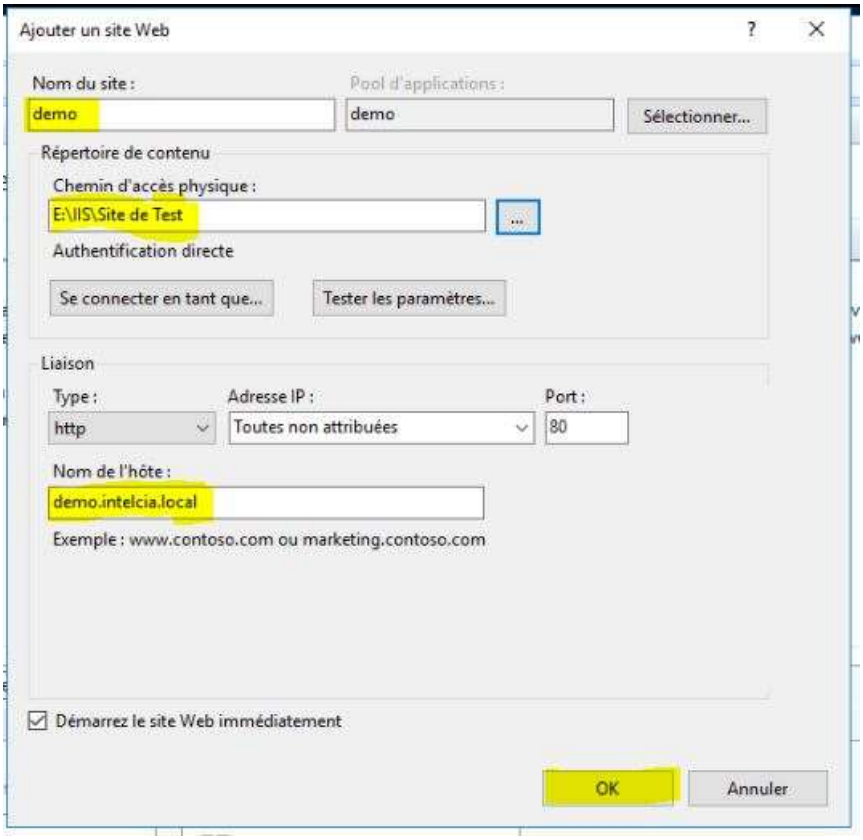

Figure 2.34 : Informations de notre site web

Notre site web a été bien créé pour le rendre accessible depuis n'importe quel PC du réseau il faut l'ajouter dans les noms DNS.

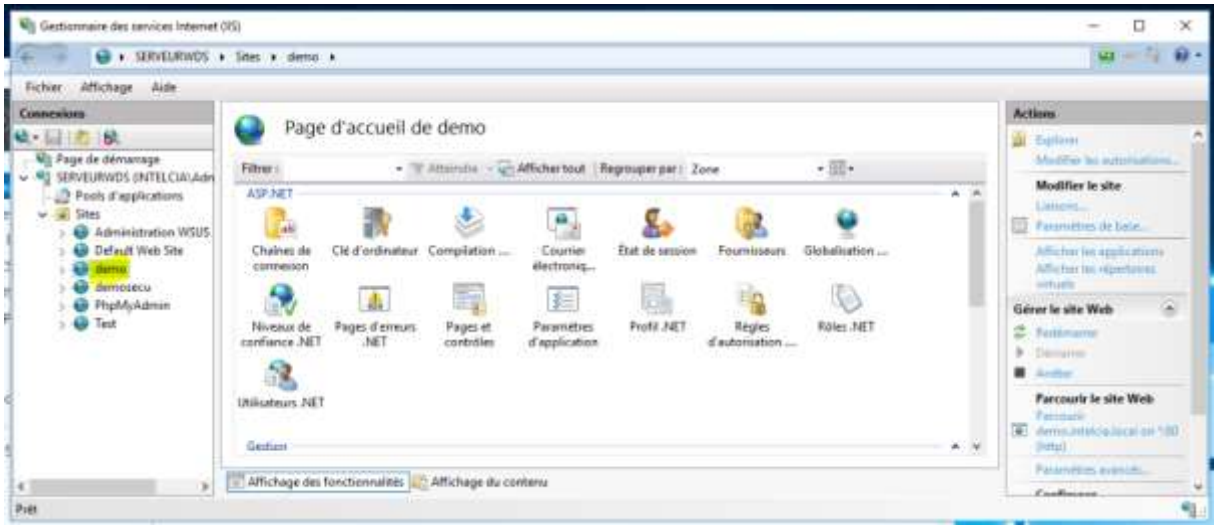

Figure 2.35 : Consol de gestion des sites web

2.2.4.2 Créer un certificat pour notre site

Pour sécuriser notre site web il faut lui associer un certificat

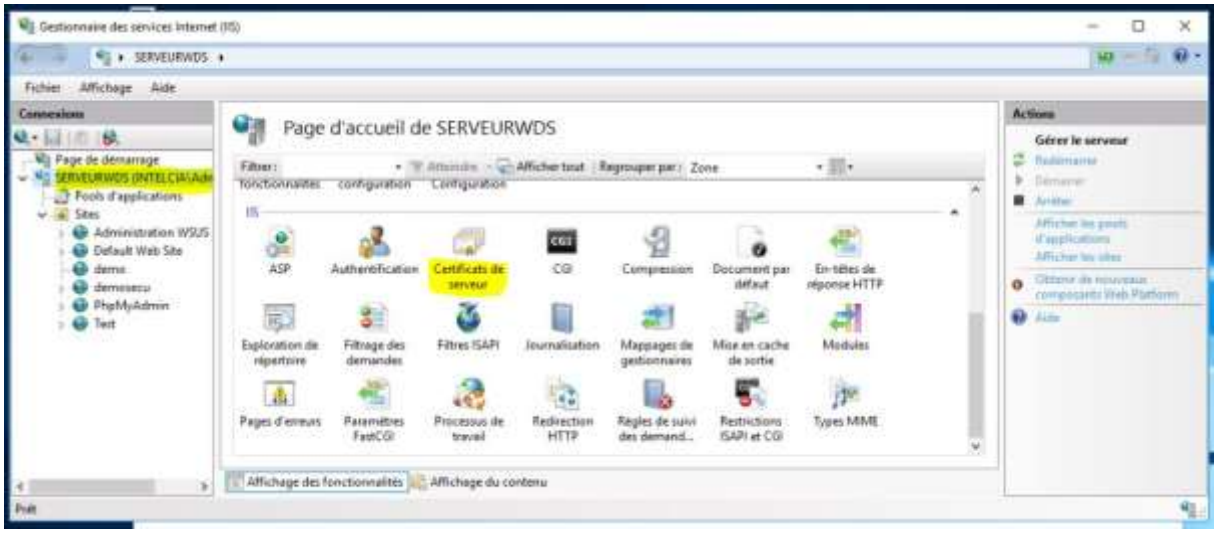

Figure 2.36 : Configuration des certificats

On creeffg une demande de certificat pour notre site web

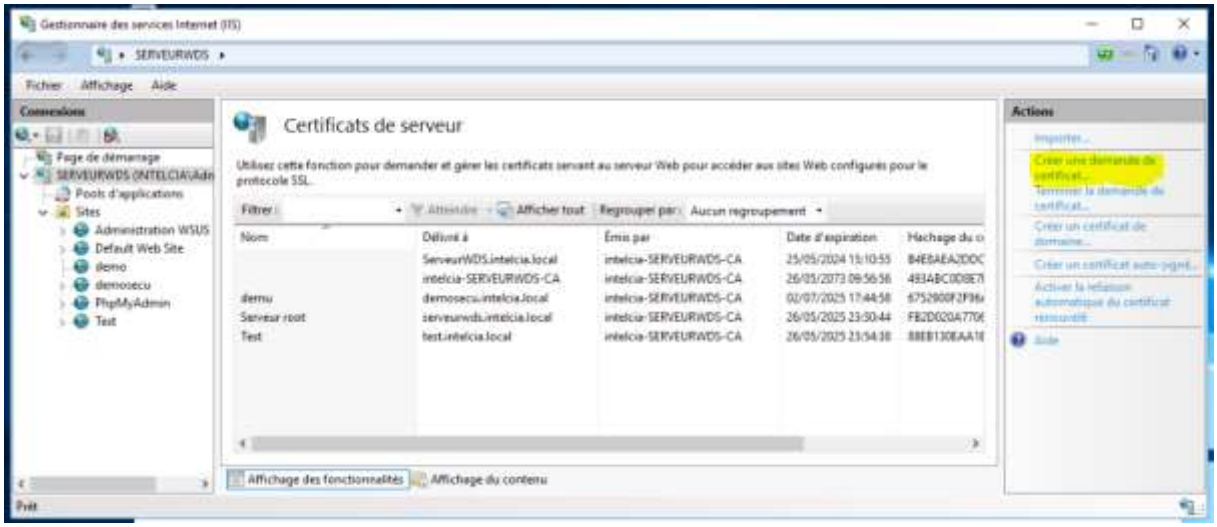

Figure 2.37 : création d'une demande de certificat

On doit entrer les informations d'identification de notre site web (nom de domaine, Organisation, etc.)

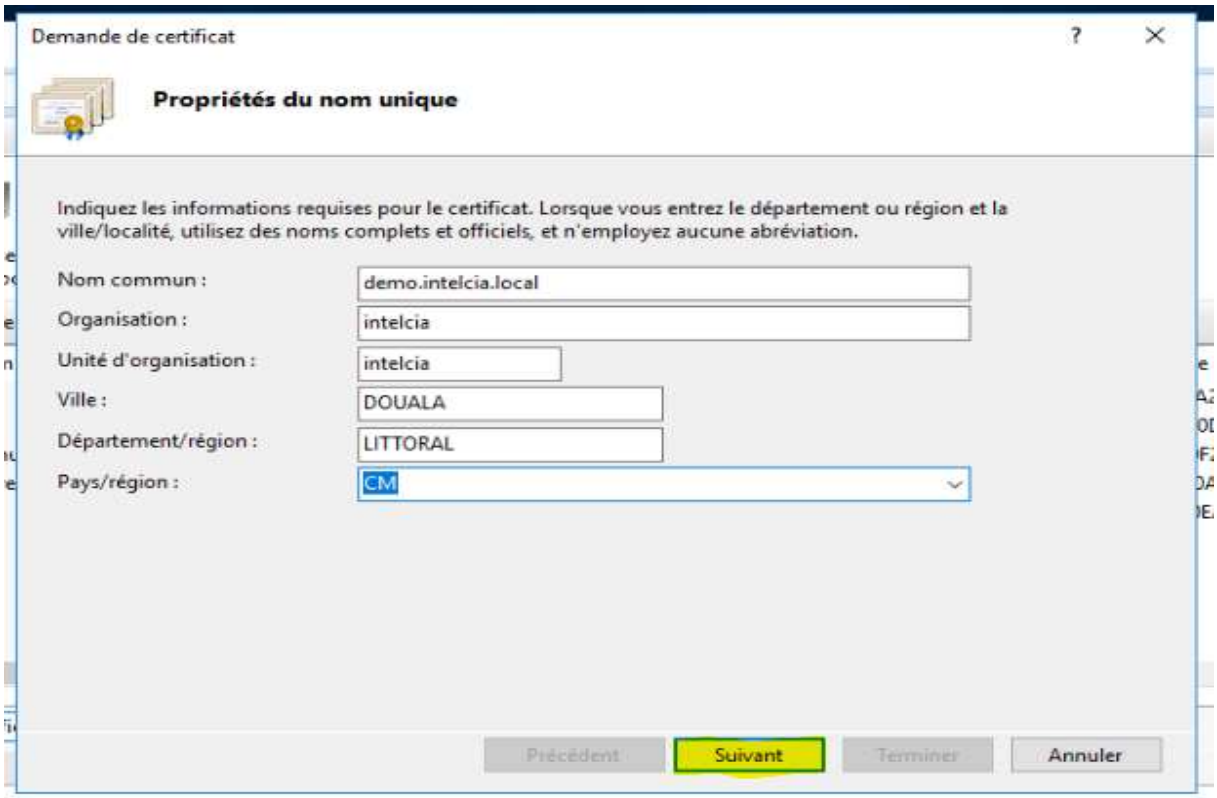

Figure 2.38 : Informations d'identification du demandeur

Choisir la taille de la clé de chiffrement

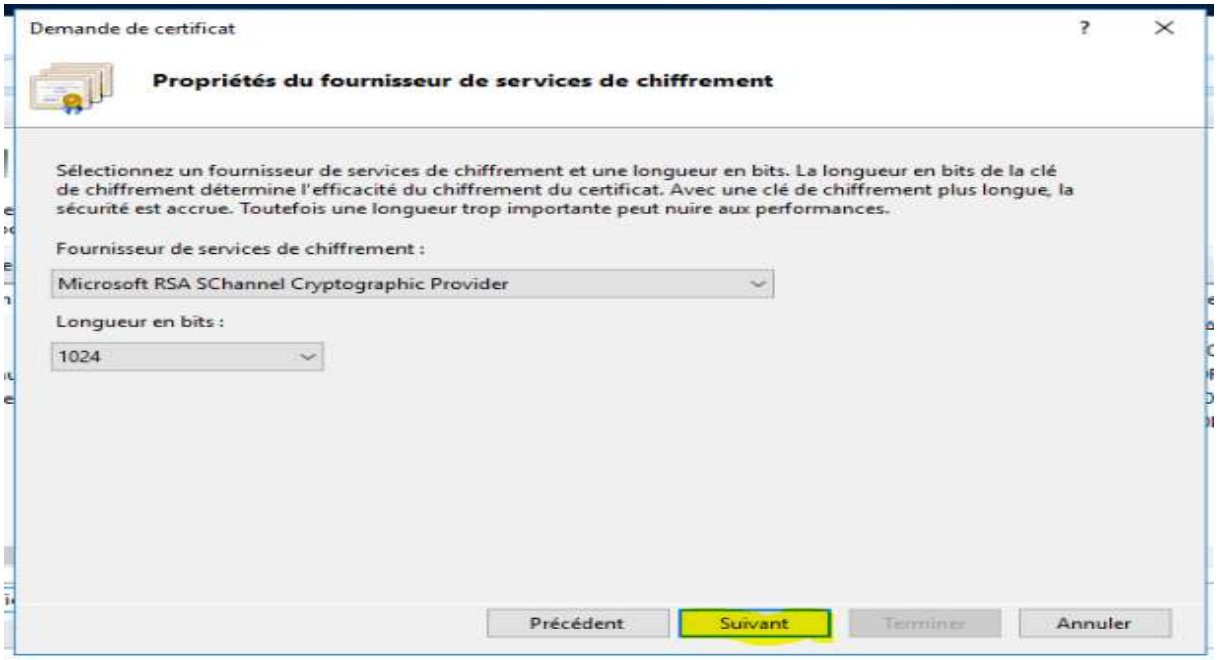

Figure 2.39 : Configuration de la clé du certificat

Sélectionner un fichier texte ou stocker la demande de certificat

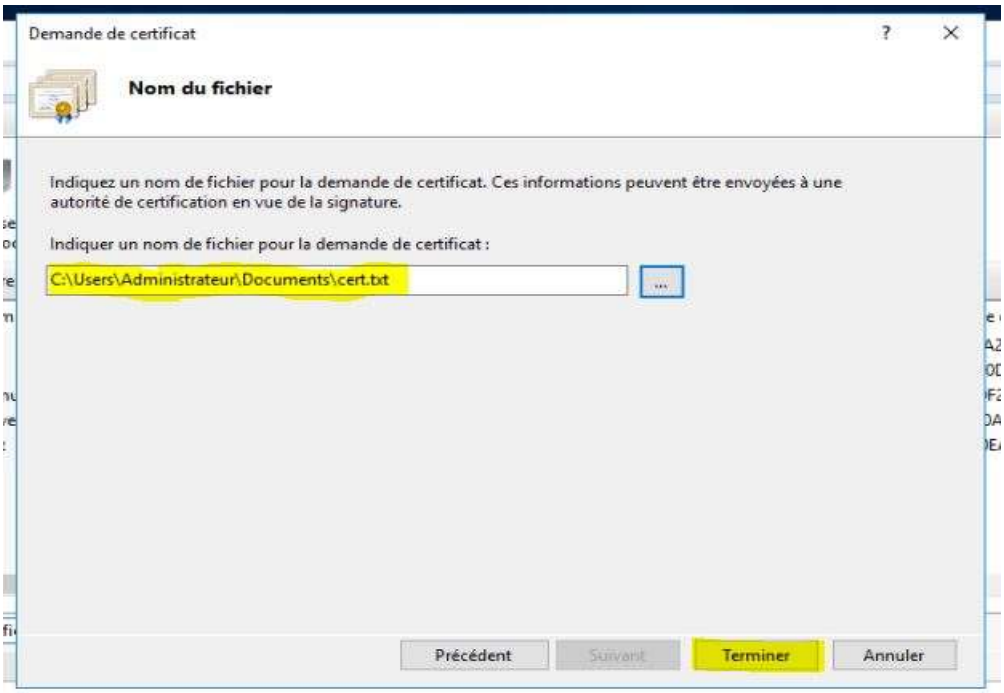

Figure 2.40 : Fichier de demande de certificat

Une fois le fichier de demande en notre possession on doit se rendre sur le site web pour demander un certificat associer à notre fichier de demande

Choisir demande de certificat avanceeggh

Figure 2.41 : Demande de certificat avancé

Puis copier le contenu du fichier Cert.txt dans la zone de demande, choisir serveur web dans le choix des modèles de certificat et ajouter l'attribut autres noms en entrant la commande [17]:

san :dns=demosecu.intelcia.local

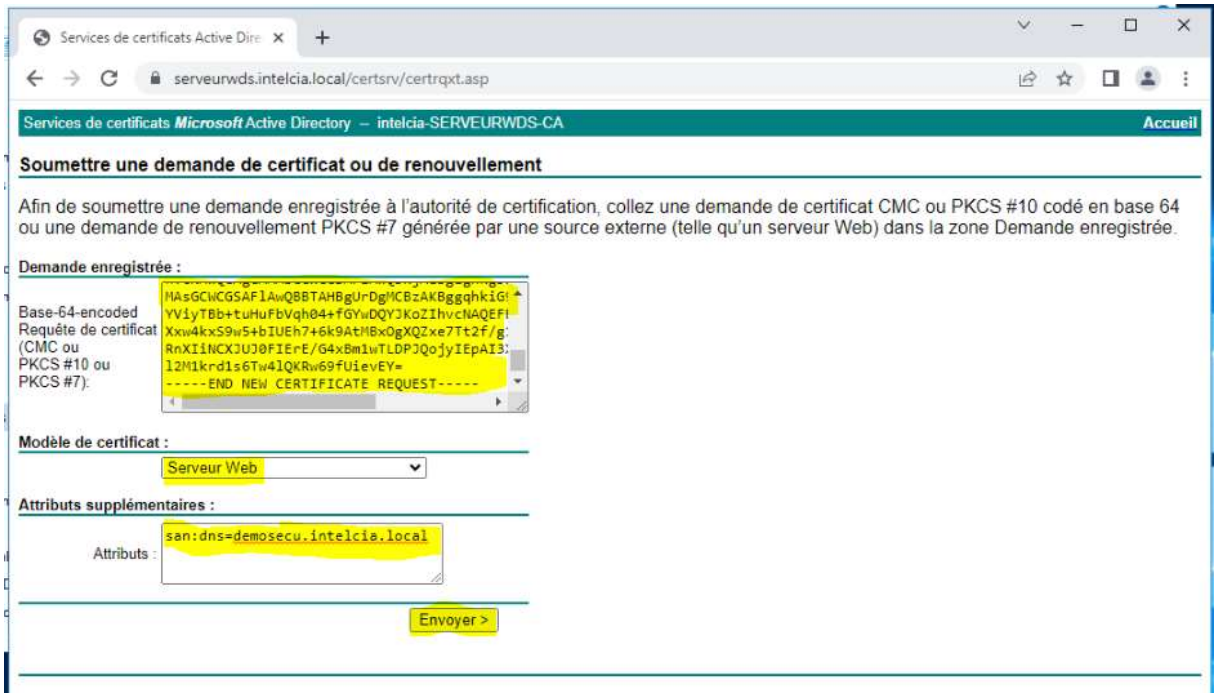

Figure 2.42 : Choix des informations pour la demande de certificat

Il ne nous reste plus qu'à télécharger notre certificat

Figure 2.43 : Contenu de notre fichier de demande Cert.txt

Figure 2.44 : Téléchargement de notre certificat

Puis revenez dans le gestionnaires IIS pour terminer la demande

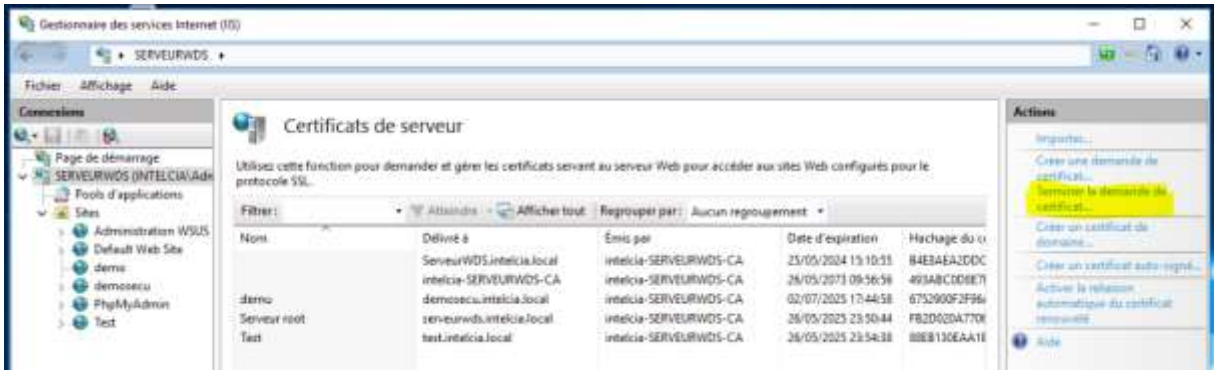

Figure 2.45 : Terminer la demande de certificat

Entrez le nom de notre certificat apres avoirs selectionner l'emplacement de celui-ci

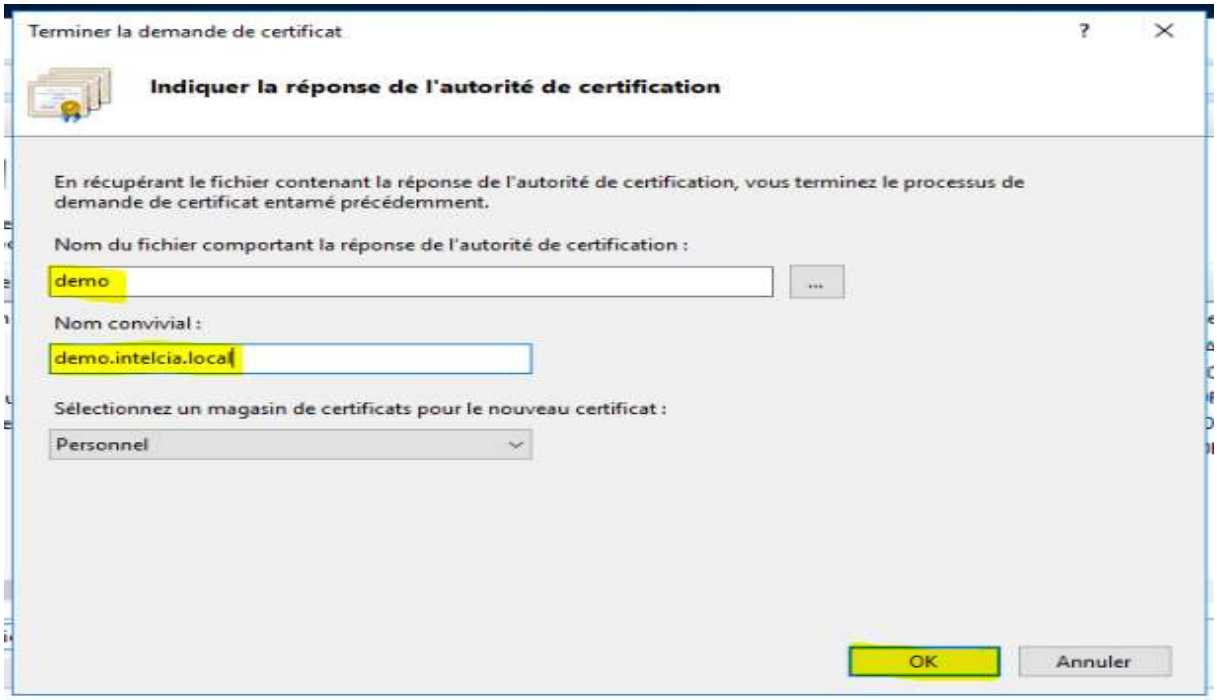

Figure 2.46 : Choix du nom de notre certificat

Le certificat s'affiche dans notre gestionnaire de certifat IIS mais egalement au niveau de notre gestionnaire chez l'Autorite de certification.

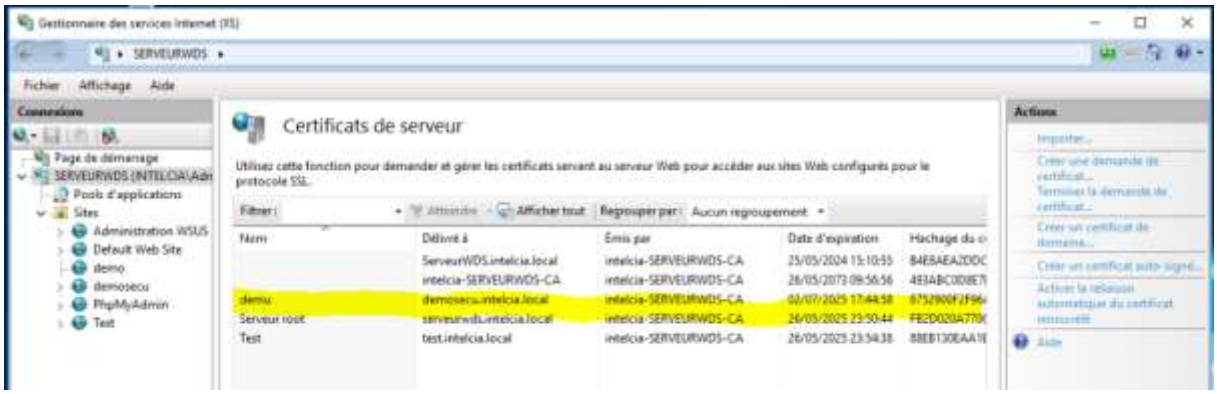

Figure 2.47 : Certificat demu pour le site demosecu.intelcia.local

2.2.4.3 Sécuriser notre site web en HTTPS

Il suffit desormais de lier notre certificat avec notre site web en HTTPS

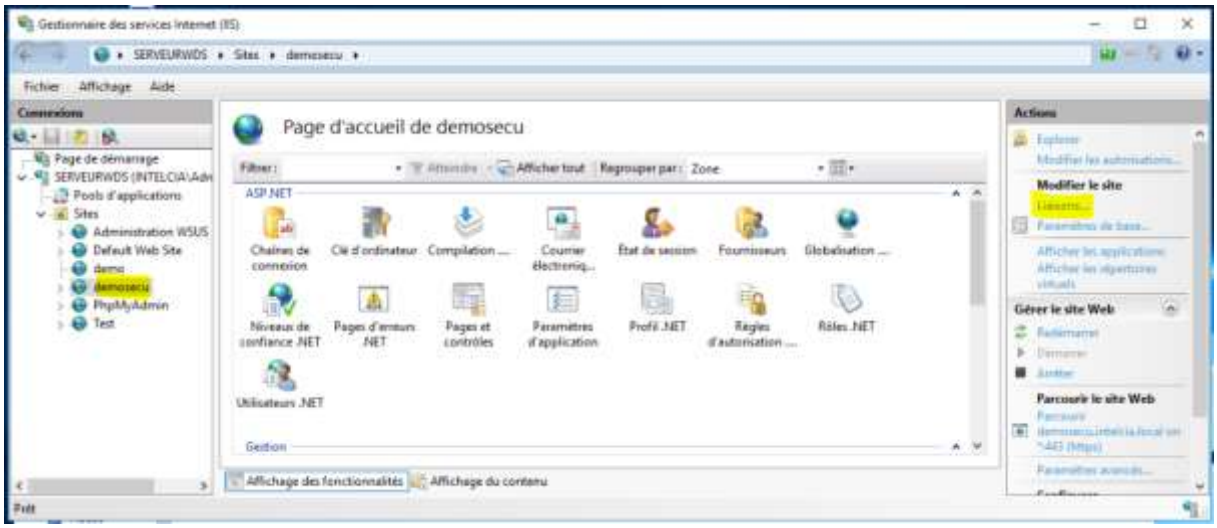

Figure 2.48 : Liaison de notre site Web avec le certificat

Sélectionner le numéro de port et le certificat a associé au site web

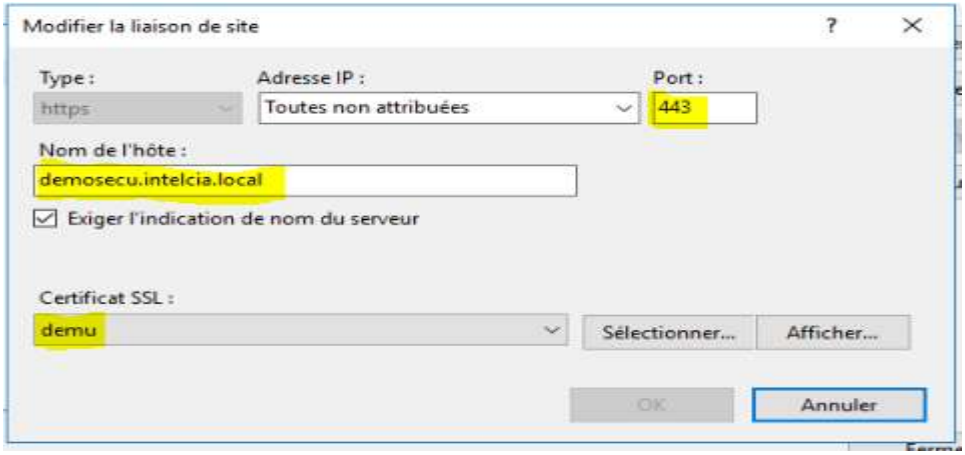

Figure 2.49 : Configurer notre site Web en HTTPS

En essayant de nous connecter à notre site web en HTTPS sur notre navigateur nous voyons clairement un cadenas fermé a cote du nom du site web. Comme l'illustre la figure suivante :

En regardant les details du certificat on peut voir les differentes informations comme le nom de domaine , le nom de l'autorite de certification.

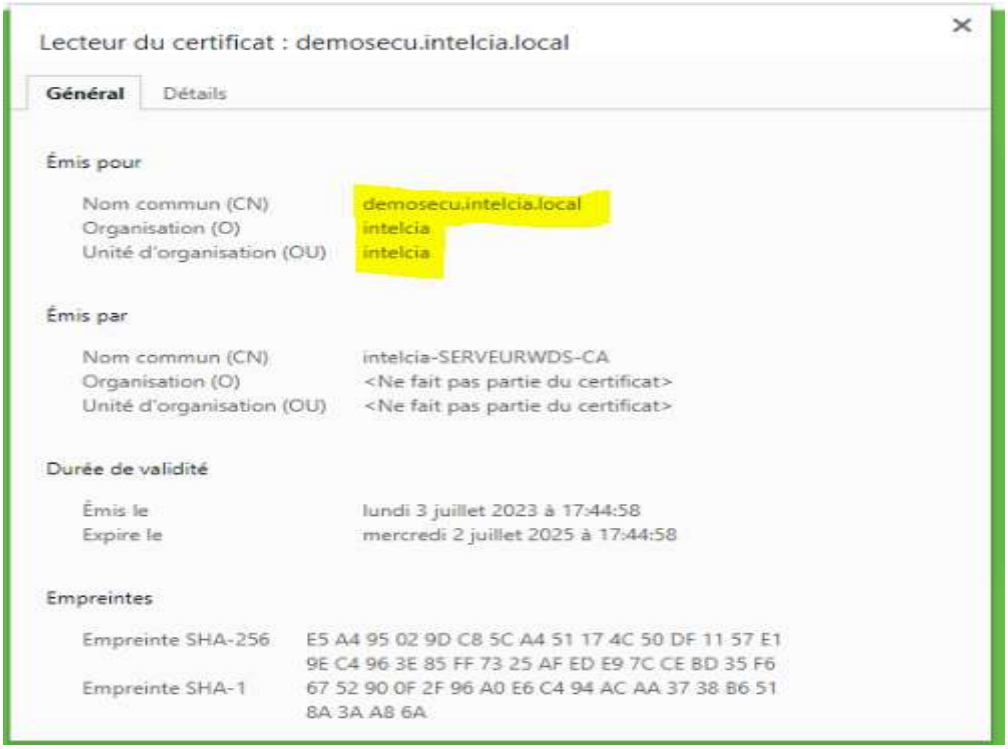

Figure 2.50 : Certificat généré par notre AC

CONCLUSION

Dans ce chapitre nous avons mis en place notre infrastructure à clé publique en nous appuyant sur les outils proposées par Windows serveur 2016.Ainsi nous avons pu montrer un exemple palpable de PKI. Dans la suite nous allons présenter les résultats obtenus et discuter sur les limites et les possibilistes d'amélioration de notre projet.

CHAPITRE 3 : RESULTATS ET DISCUSSION

INTRODUCTION

En se basant sur les études réalisées, ce chapitre a pour but de présenter la plus-value de notre travail dans un réseau informatique. Ici, nous allons faire une présentation des résultats obtenus, les interpréter et discuter des insuffisances ainsi que des possibles améliorations de notre projet.[15]

3.1 Présentation des résultats et interprétations

3.1.1 Test de sécurité avec wireshark

Pour effectuer notre test nous allons connecter un utilisateur à deux sites web lié à une base de données et pour étudier les résultats le premier site sera en http (non sécurisé) et le deuxième site sera en HTTPS (sécurisé).

Dans les deux cas nous allons capturer les paquets entre le serveur et le client avec Wireshark puis faire une interprétation.[18]

Allons dans whireshark au niveau de notre serveur et sélectionnons la carte réseau à capturer

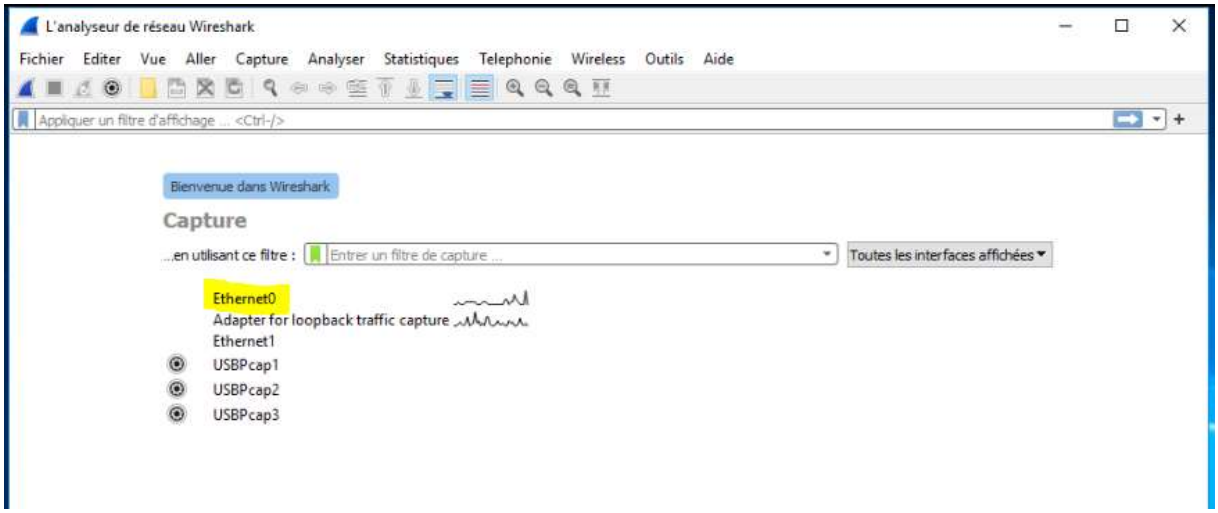

Figure 3.1 : Choix de l'interface à analyser

Puis accedons au site web depuis un machine du domaine et connectons a l'utilisateur root [19]

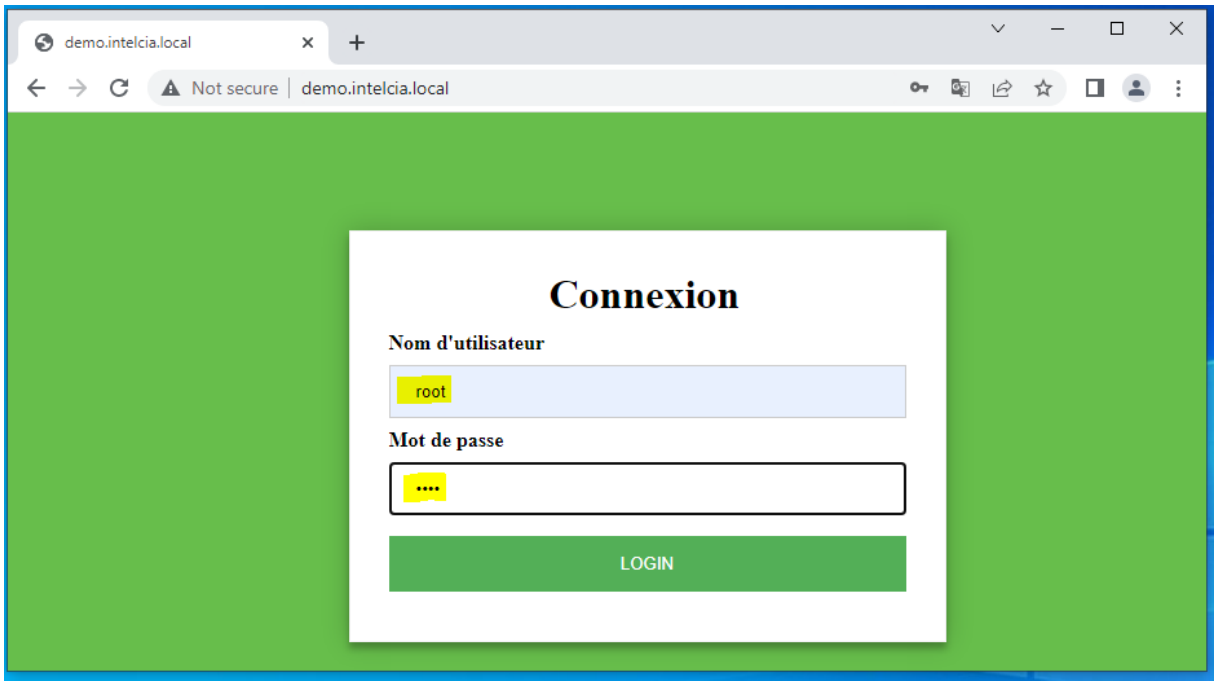

Figure 3.2 : Connexion au site http (non sécurisé)

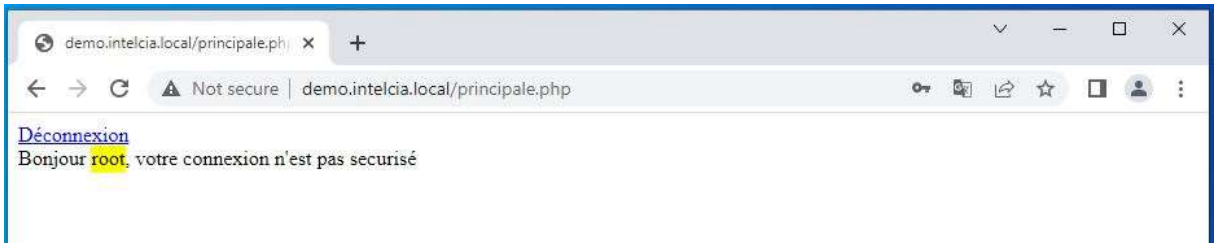

Figure 3.3 : Fenêtre de connexion au site non sécurisé

Dans ce cas notre capture whireshark nous renvoie les informations suivantes :

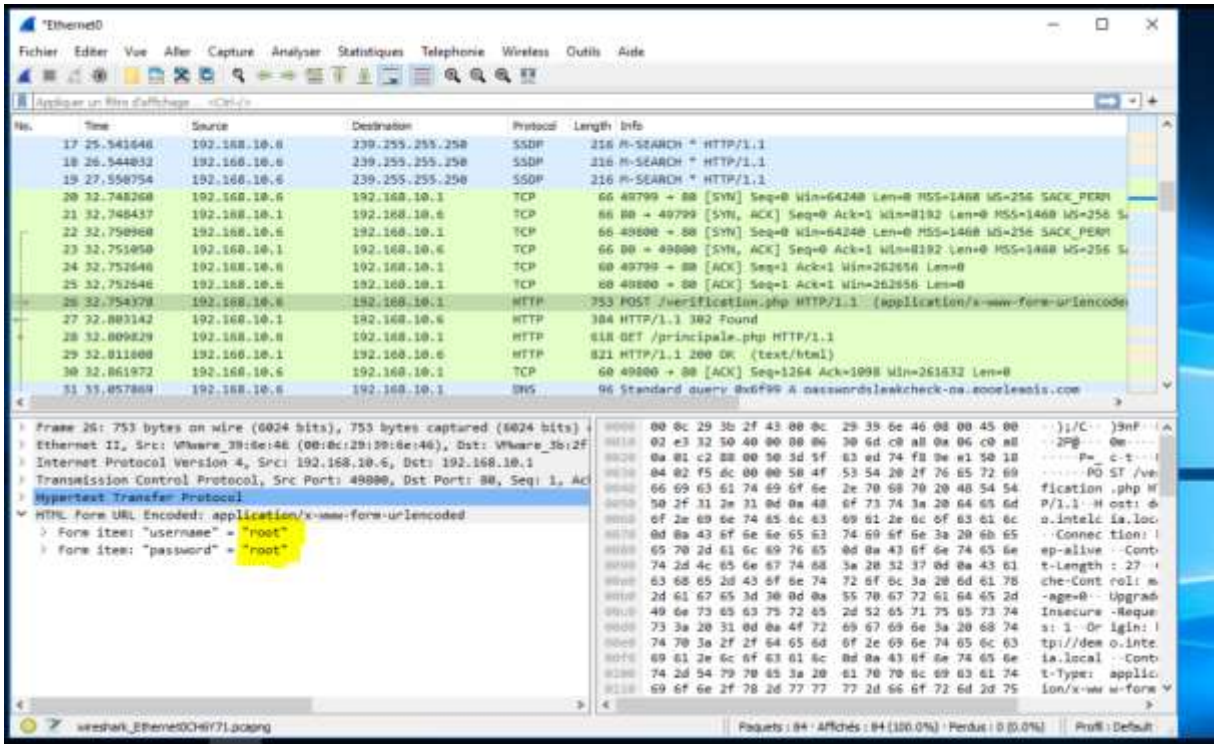

Figure 3.4 : Résultats de la capture Wireshark

Maintenant connectons a notre site web en HTTPS et identifions à nouveau en tant que root.[20]

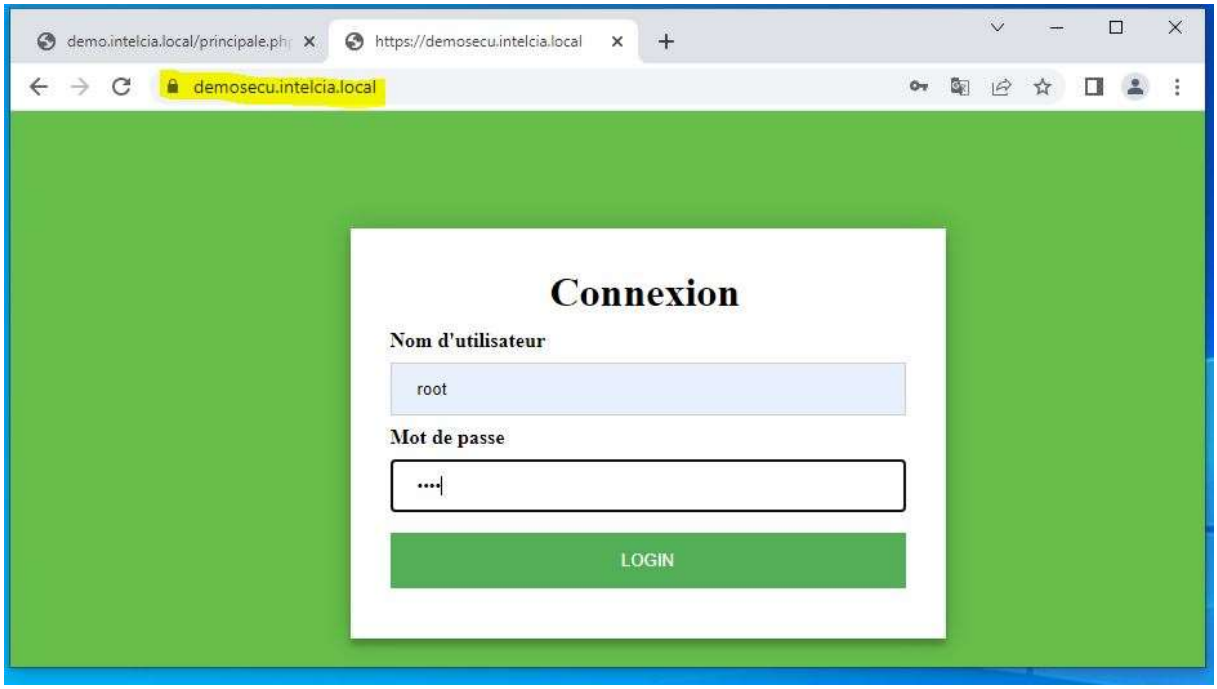

Figure 3.5 : Connexion au site HTTPS (sécurisé)

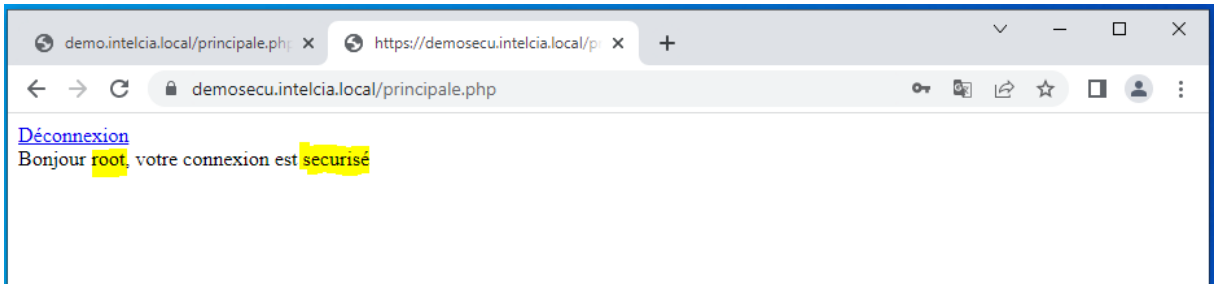

Figure 3.6 : Fenêtre de connexion au site sécurisé

La Capture whireshark nous ressort les paquets suivants :

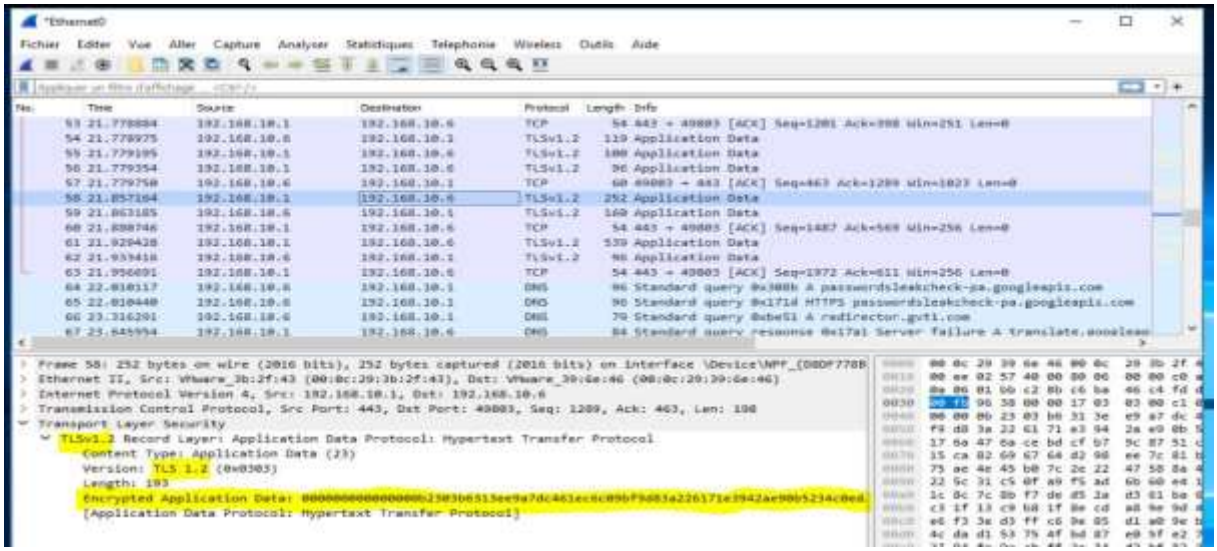

Figure 3.7 : Résultats de la capture de la connexion sur le site sécurisé

3.1.2 Interprétations

Il s'agit d'interpréter les deux tests fait plus haut :

Tableau 3.1 : Interprétations des résultats

Cas	Interprétations
Interception des données sur le site HTTP	Lorsqu'on étudie la capture Wireshark quand l'utilisateur entre ses informations sur la page de connexion, ses informations sont clairement visibles sur le réseau. Là on voit clairement : - Le mot de passe : root - Le nom d'utilisateur : root
Interception des données sur le site HTTPS	Lorsqu'on étudie la capture Wireshark quand l'utilisateur entre ses informations sur la page de connexion, ses informations sont tous crypter en utilisant le protocole TLS v3. Dans ce cas impossible de lire les données.

3.2 Estimation financière

Dans cette section, nous allons essentiellement donner le coût estimatif du projet qui est constitué du coût des équipements nécessaires pour sa réalisation, du coût des licences et de la main d'œuvre. Le tableau 3.2 représente le coût des équipements :

Tableau 3.2 : Cout des équipements et des logiciels

Nom de l'équipement	Quantité	Prix unitaire (PU)	Prix total en FCFA
Serveur HPE ProLiant DL380 gen 9	1	4 000 000	4 000 000
Licence Windows serveur 2016	1	560 000	560 000
Licence VMware Workstation 17 pro	1	130 000	130 000
Total			4 690 000

CONCLUSION

Ici, nous avons présenté et interprété les résultats de notre projet. Après avoir étudié les résultats de la mise en place de notre infrastructure, nous avons discuté de leurs impacts. L'utilisation des PKI est aujourd'hui un facteur incontournable pour assurer un environnement informatique sécurisé.

CONCLUSION GENERALE ET PERSPECTIVES

Durant notre projet, nous avons pu mettre en œuvre une infrastructure de gestion de clés publiques avec le service AD CS de Windows serveur. Ainsi nous avons eu une idée sur le fonctionnement de la PKI et son importance dans le cadre du réseau d'Intelcia. La mise en place d'une PKI au sein du centre de calcul a permis de faciliter la gestion des clés publiques et la sécurisation des sites web et autre applications par le moyen des certificats numériques. Dans ce travail, une description des différents éléments qui entrent dans la conception et la mise en service d'une infrastructure PKI s'est vue indispensable. Pour parvenir à rendre le système de sécurité optimal, nous avons réalisé une étude afin de comprendre les différents concepts lies à la mise en place d'une infrastructure à clé publique. À travers ses différents ensembles nous avons pu ressortir toute la terminologie qui entre en jeu dans la mise en place des PKI. Par la suite, une étude du projet a été établie afin de ressortir les différents services à mettre en place. Une fois le choix des services et des outils fait, nous les avons déployées au sein du réseau d'Intelcia tout en présentant les méthodes utilisées concernant les différentes installations et de configurations effectuées. Enfin nous avons discutés sur les résultats du projet implémenté et le coût du projet.

Pour améliorer notre système de gestion des clés et des certificats, nous pouvons créer plusieurs autorités de certification (une par site) sur chaque site Intelcia et les liées de manière hiérarchique comme ça tous les sites pourront reconnaitre les certificats valides sans ajouter d'autres configuration.

Toujours dans le souci de faire évoluer notre solution nous pouvons acheter des certificats en ligne a des autorités de certifications de confiance et les utilisés dans notre réseau par exemple ceci permettrait de rendre les sites intranet sécuriser même dans le réseau externe.

REFERENCES BIBIOGRAPHIQUES

[1] A. Belkaaloul, « Développement d'une infrastructure à clés publiques pour les réseaux V2G », PhD Thesis, Université du Québec à Trois-Rivières, 2021.

[2] M. Abadi, *La sécurité informatique*. Collège de France, 2013.

[3] P. Barthélemy, R. Rolland, P. Véron, et R. Rolland, *Cryptographie: Principes et Mises en øeuvre*. Hermès Science Publications, 2005.

[4] J.-L. Archimbaud, « Les IGC, infrastructures de gestion de clés », *Cah. Numér.*, vol. 4, nº 3, p. 111–134, 2003.

[5] L. Hilmi, « Mise en place d'une solution PKI: infrastructure à clé publique », 2016.

[6] « SSL Digital Certificate Authority | Encryption & Authentication | DigiCert.com ». https://www.digicert.com/ (consulté le 13 juillet 2023).

[7] « Fonctionnement des certificats TLS/SSL | DigiCert ». https://www.digicert.com/fr/how-tls-ssl-certificates-work (consulté le 23 juin 2023).

[8] « PKI : Qu'est-ce qu'une PKI ou Infrastructure à clés publiques ? » https://www.certeurope.fr/blog/quest-ce-quune-pki-ou-infrastructure-a-cles-publiques/ (consulté le 13 juillet 2023).

[9] « Accueil | Intelcia ». https://www.intelcia.com/fr (consulté le 13 Mars 2023).

[10] « Presentation de openSSL ». https://www.fil.univ-lille.fr/~wegrzyno/portail/PAC/Doc/TP-Certificats/tp-certif001.html (consulté le 05 juin 2023).

[11] « Que sont les services de certification Active Directory ». https://www.globalsign.com/fr/blog/services-certifications-active-directory (consulté le 01 juillet 2023).

[12] « Créer et configurer un serveur DNS, ainsi que déléguer des sous-domaines sous Windows Server 2012 / 2012 R2 - Windows Server - Tutoriels - InformatiWeb Pro ». https://www.informatiweb-pro.net/admin-systeme/win-server/ws-2012-2012-r2-creer-un-serveur-dns-et-deleguer-des-sous-domaines.html (consulté le 15 mai 2023).

[13] « configuration du DNS et du dhcp sur windows server pdf - Recherche Google ». https://www.google.com/search?q=configuration+du+DNS+et+du+dhcp+sur+windows+server+pdf&sxsrf=AB5stBhbzuOfZCI354C0yjtOUJv5n2hXsA%3A1689213240473& (consulté le 12 mai 2023).

[14] « Autorité de certification (AD CS) - Tutoriels - InformatiWeb Pro ». https://www.informatiweb-pro.net/admin-systeme/win-server/sujets/autorite-certification-ad-cs (consulté le 05 juin 2023).

[15] « Autorité de certification d'entreprise : installation et configuration avec Windows Server - Page 2 à 11 ». https://rdr-it.com/autorite-certification-entreprise-installation-configuration-windows-server/2/ (consulté le 21 Mai 2023).

[16] P. A. LAKHOUAJA, « Administration Réseaux ».

[17] Deland-Han, « Add SAN to secure Lightweight Directory Access Protocol (LDAP) certificate - Windows Server », 23 février 2023. https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/add-san-to-secure-ldap-certificate (consulté le 13 juin 2023).

[18] « Comment utiliser Wireshark: tutoriel complet + astuces | Varonis ». https://www.varonis.com/fr/blog/comment-utiliser-wireshark (consulté le 08 juin 2023).

[19] « Formulaire de login avec HTML/CSS, PHP et MySQL ». https://www.codeurjava.com/2016/12/formulaire-de-login-avec-html-css-php-et-mysql.html (consulté le 16 juin 2023).
[20] « MySQL :: Download MySQL Installer ». https://dev.mysql.com/downloads/windows/installer/8.0.html (consulté le 10 juin 2023).