Table des matières

Sigles

DES	Data Encryption Standard
AES	Advanced Encryption Standard
RSA	Rivest–Shamir–Adleman
DH	Diffie-Hellman
MD5	Message Digest 5
SHA-1	Secure Hash Algorithm 1
OTP	One-Time Password
PKI	Public Key Infrastructure
CA	Certificate Authority
RA	Registration Authority
LDAP	Lightweight Directory Access Protocol
AD CS	Active Directory Certificate Services.
AD DS	Active Directory Domain Services.
SSL	Secure Sockets Layer
TOTP	Time-based One-Time Password

Introduction Générale

La sécurité est un enjeu majeur des technologies numériques modernes. Avec le développement de l'Internet, les besoins de sécurité sont de plus en plus importants. En effet, les besoins tels que, l'identification et l'authentification des entités communicantes, l'intégrité des messages échangés, la confidentialité des transactions, etc., liées à la sécurité des communications sont à satisfaire.

La cryptographie moderne permet la mise en œuvre de ces services de sécurité grâce à différents mécanismes tels que le chiffrement et la signature électronique. Plusieurs de ces mécanismes sont basés sur des algorithmes cryptographiques asymétriques dits « à clé publique ». Bien que très efficace, la cryptographie à clé publique comporte cependant un enjeu majeur ; qui consiste à la gestion des clés publiques. En effet, l'efficacité de ce mécanisme de sécurité dépend du niveau de certitude que détient l'utilisateur d'une clé publique concernant l'identité de son propriétaire légitime..

La problématique que rencontrent plusieurs grandes entreprises, c'est comment assurer la sécurité des transactions entre les différentes entités, filières et partenaires à travers le réseau interne ou externe ? Et Comment assurer une authentification et un accès sûr aux ressources de l'entreprise ? Et comment assurer l'intégrité, et la non-répudiation des échanges établis ?.

Dans ce contexte l'objectif de ce memoire est de faire l'étude et le déploiement d'un système de gestion d'une authentification forte : Cas de LaPoste , afin de renforcer la politique de contrôle d'accès de la direction générale de LaPoste. il s'agit de mettre en place un système de gestion d'une authentification forte basée sur OTP(One-Time Password)(mot de passe à usage unique) et déployer le SSL(https) avec certificat, pour assurer l'identification et l'authentification forte des utilisateurs du système d'information de LaPoste, et protéger l'accès aux services métiers de l'entreprise à travers des certificats numériques.

Ce memoire est structuré en deux parties : l'approche théorique et l'approche pratique.
L'approche théorique est organisée en trois chapitres comme suit :

Chapitre 1 : Le chapitre 1 est consacré au Cadre de référence et méthodologie.Dans ce chapitre on décrit le Contexte, la Problématique, la Proposition des solutions et la Solution préconisée.

Chapitre 2 : Le chapitre 2 est réservé à la Présentation du thème et des notions fondamentales. Il est destiné à la Justification du champ d'étude, à l'Objectif général du thème, aux Objectifs spécifiques, aux Définitions et notions fondamentales enfin à l'Avantage de la solution.

Chapitre 3 : Le chapitre 3 est consacré à L'authentification forte basée sur un certificat.Ici on aborde le Fonctionnement de l'authentification forte, les Différentes composantes et les Cas d'utilisation.

L'approche pratique est constituée en deux chapitres comme suit :

Chapitre 4 : Le chapitre 4 est réservé au Déploiement d'une authentification forte basée sur OTP(One-Time Password) et du SSL(https) avec certificat.Dans cette partie nous allons aborder l'Architecture applicative, le Déploiement de l'autorité de certification, l'Administration de l'autorité de certification, le Déploiement de la solution d'authentification forte par mot de passe à usage unique et du SSL(https) avec certificat et le Test de fonctionnement .

Chapitre 5 : Le chapitre 5 est consacré à l'Evaluation financière de la solution. Dans cette partie on parle du Budgétisation de la solution.

Ce mémoire s'achève par une conclusion générale où nous présentons le bilan et les perspectives de notre travail.

Première partie

Approche théorique

Chapitre 1

Cadre de référence et méthodologie

Introduction

Les sociétés modernes comme LaPoste sont aujourd'hui fortement dépendantes des technologies de l'information et des communications.
Dans un environnement ouvert, les interlocuteurs sont parfois inconnus et toujours dématérialisés. Les concepts et technologies de la confiance numérique et de la sécurité informatique vont se compléter pour permettre de réaliser un contrôle d'accès en environnement ouvert. Dans ces travaux, nous nous proposons d'étudier les concepts majeurs de cette problématique, puis de concevoir et enfin de développer un système fonctionnel d'authentification forte , basée sur OTP(One-Time Password)(mot de passe à usage unique) et déployer le SSL(https) avec certificat, pour un environnement ouvert et appliqué à l'Internet.

1.1 Contexte

Dans le contexte de sécurité actuel, le mot de passe est devenu en quelques années un élément incontournable de notre vie quotidienne. Nous les utilisons pour protéger nos appareils (ordinateurs, tablettes, smartphones, etc. . .), nos données, ou encore pour restreindre l'accès aux services que nous utilisons (comptes mail, applications bancaires, etc. . .). Mais le mot de passe est loin d'être un moyen d'authentification totalement fiable, et constitue de ce fait un risque pour les utilisateurs.

En effet, nous devons faire face à une multitude de comptes à créer, et donc à retenir. Il est alors très courant pour un utilisateur d'utiliser toujours le même mot de passe ou de choisir un mot de passe simple, facile à retenir et à saisir. Ensuite, il est relativement simple pour un malware de " capturer " un mot de passe. Les keyloggers par exemple, surveillent les touches du clavier et transmettent les mots de passe saisis à l'attaquant.

L'actualité, et notamment les nombreuses attaques massives visant à compromettre des mots de passe (1 milliard de comptes Yahoo piratés, 145 millions de comptes eBay ou encore 117 millions de comptes LinkedIn, et plus récemment le géant mondial du

VTC Uber avec plus 57 millions de victimes, dont au moins 600 000 chauffeurs nous le démontrent : Un simple mot de passe ne suffit plus à nous protéger.

Les réglementations se sont donc durcies afin de mieux protéger les utilisateurs. Par exemple la directive sur les services de paiement (DSP2) entrée en vigueur le 13 janvier 2018, impose aux établissement bancaires une authentification forte des clients lorsque ceux-ci accèdent à leur compte de paiement en ligne, initient une opération de paiement, ou exécutent une action susceptible de comporter un risque de fraude.

1.2 Problématique

en raison de la vulnérabilité des systèmes protégés par la seule utilisation de mots de passe. Concrètement, entre la négligence des utilisateurs et les techniques ultra sophistiquées des hackers, les mots de passe ne sont désormais plus suffisants pour assurer la sécurité des informations et des ressources des entreprises. Un utilisateur inconnu du fournisseur de service obtient un accès au travers de la confiance du fournisseur de service envers des organisations attestant d'informations sur l'utilisateur. Avec l'évolution de la technologie de l'information et de la communication, et principalement du « cloud computing », nous nous sommes posés la question de comment la confiance numérique entre organisations sera utilisée dans l'avenir pour permettre à des usagers d'accéder à des services en ligne offerts par des organisations desquelles ils sont inconnus ?

1.3 Proposition des solutions

L'authentification forte est une méthode permettant à un utilisateur de s'identifier/authentifier auprès d'un fournisseur de services en demandant une combinaison de deux méthodes d'authentification différentes parmi :

— Ce que l'on sait (exemple : un mot de passe)
— Ce que l'on possède (exemple : le téléphone qui reçoit un mot de passe)
— Ce que l'on est (exemple : une caractéristique biométrique)

Il existe également des mécanismes d'authentification émergents qui s'appuient sur :

— L'emplacement où vous êtes (exemple : géolocalisation)
— Les personnes que vous connaissez (exemple : réseaux sociaux)
— Ce que vous êtes en train de faire (exemple : analyse comportementale)

L'authentification forte permet donc de renforcer le niveau de sécurité lors de la connexion des utilisateurs à l'accès aux services.

Aujourd'hui, les mécanismes d'authentification forte les plus utilisés sont :

1. **Les OTP (One-Time Password) par SMS** :
   Ce mécanisme consiste à recevoir par SMS un mot de passe à usage unique (utilisable pour une durée déterminée) qui sera renseigné lors du processus d'authentification. Ce mécanisme est utilisé par de très nombreux établissements bancaires, notamment lors de la réalisation d'achats sur internet.

   La figure.1.1 résume toutes les étapes des OTP (One-Time Password) par SMS.

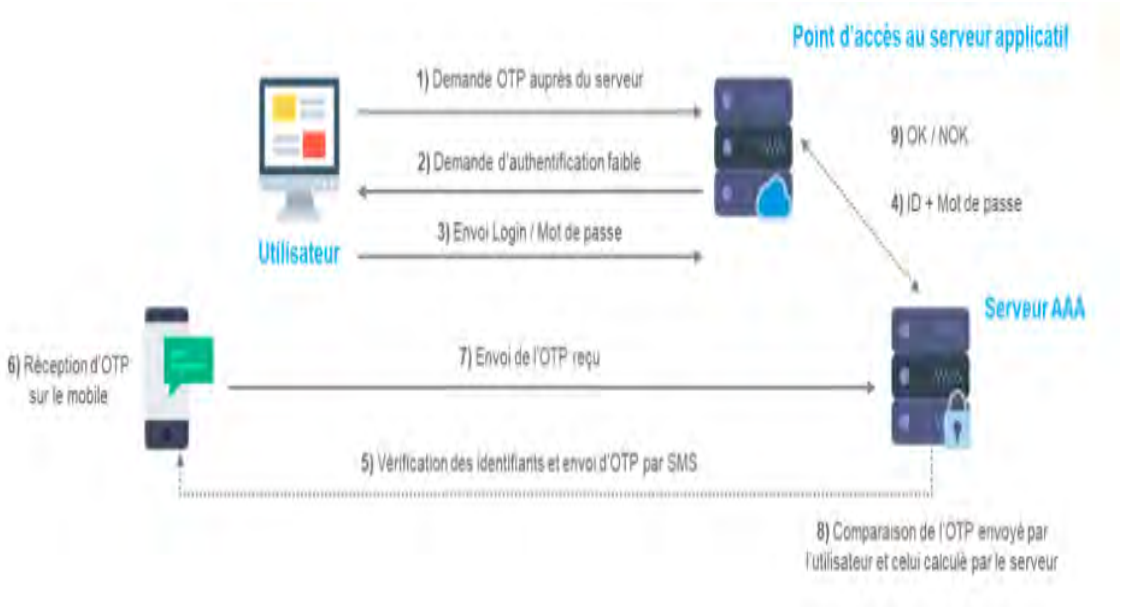


Figure.1.1.étapes des OTP (One-Time Password) par SMS source :[11]

2. **Les OTP (One-Time Password) par soft token** :
   Ce mécanisme consiste à générer un mot de passe unique via une application sur son smartphone. Il nécessite donc que l'utilisateur installe sur son smartphone l'application contenant le soft token (il peut s'agir directement de l'application de la banque en question).

   La figure.1.2 résume le processus des OTP (One-Time Password) par soft token.

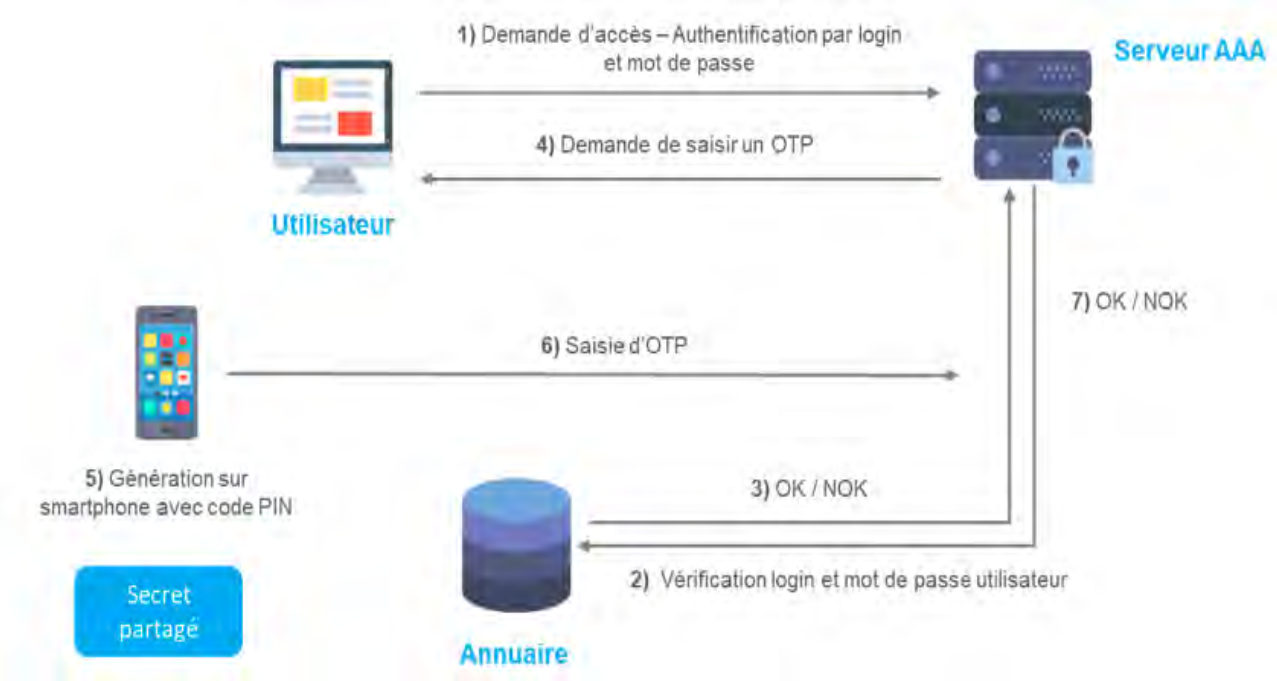


Figure.1.2.processus des OTP (One-Time Password) par soft token source :[11]

3. **Les OTP (One-Time Password) par hard token** :
   Ce mécanisme consiste à générer un mot de passe unique via un " token physique ". Le token RSA est un exemple célèbre de hard token. Le hard token génère un mot de passe aléatoire, valable pour une durée déterminée, qui est demandé lors de l'authentification de l'utilisateur.
   La figure.1.3 résume le processus des OTP (One-Time Password) par hard token.

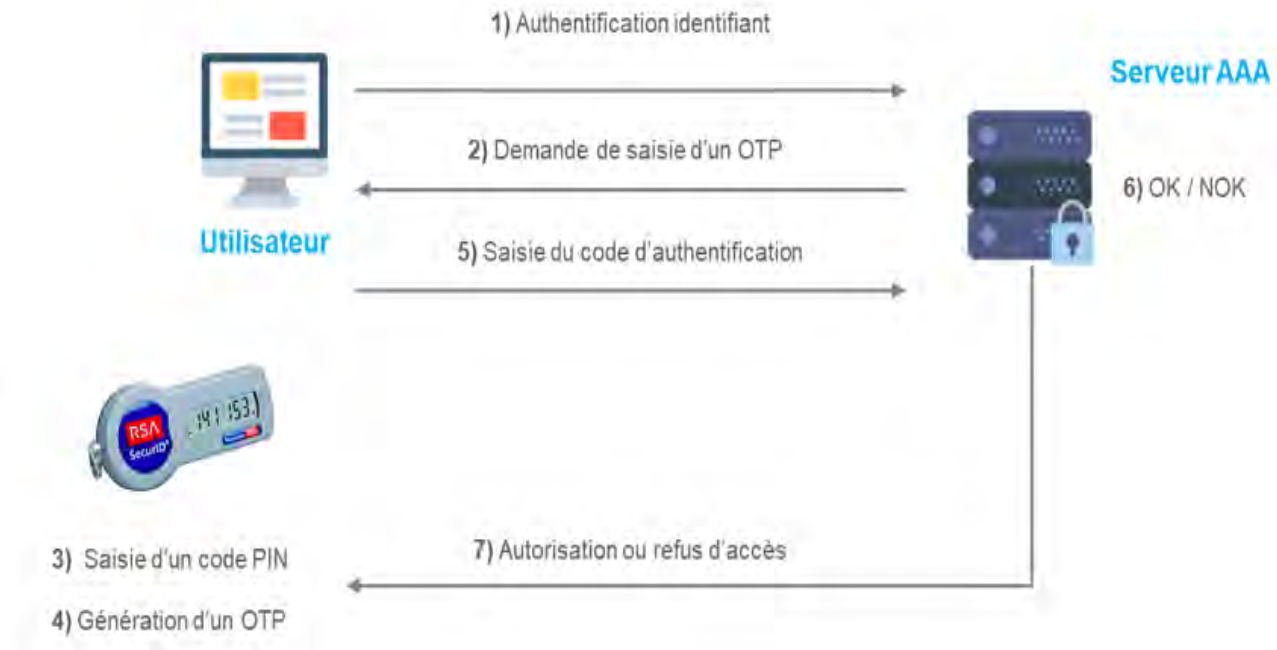


Figure.1.3.processus des OTP (One-Time Password) par hard token source :[11]

4. **La biométrie** :
   Considérée comme une des méthodes les plus prometteuses, la biométrie est de plus en plus utilisée dans le processus d'authentification forte. On distingue quatre cas d'utilisation de la biométrie :

   — La reconnaissance digitale
   — La reconnaissance vocale
   — La reconnaissance d'iris
   — La reconnaissance faciale

   La figure.1.4 résume les differentes etapes d'authentification forte par biométrie.

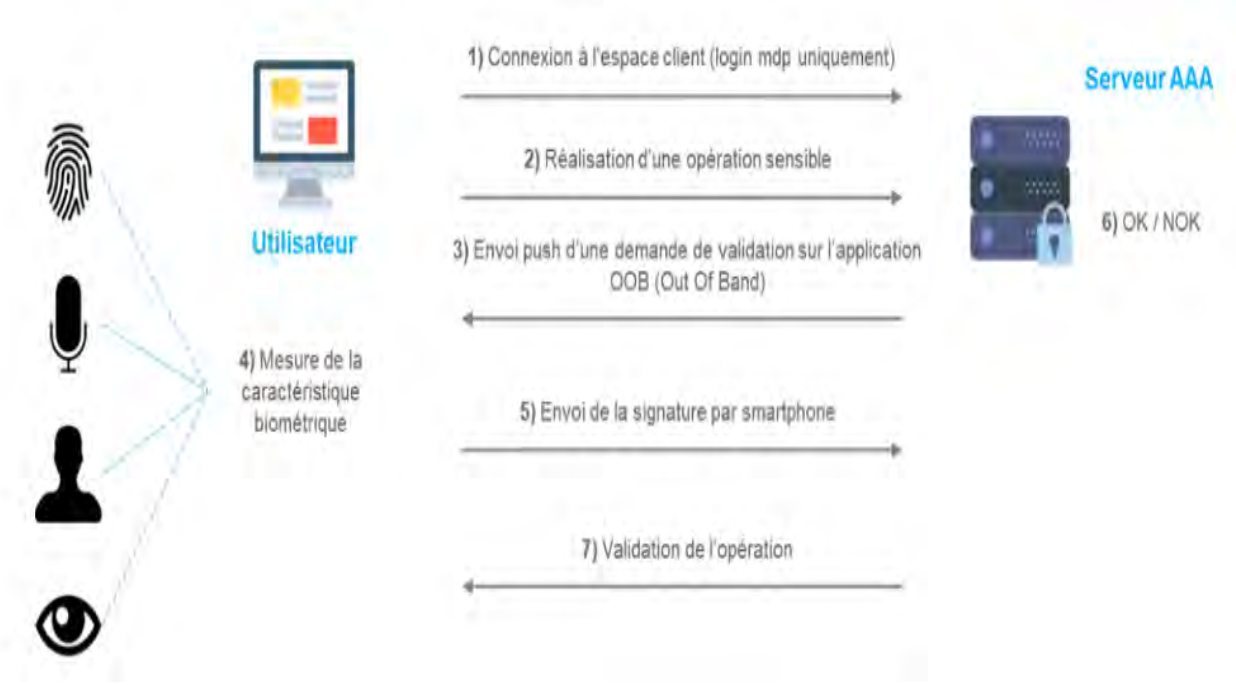


Figure.1.4.etapes d'authentification forte par biométrie source :[11]

5. **Les certificats numériques** :
   Un certificat numérique est l'équivalent virtuel d'une carte d'identité : il garantit que l'identité de l'utilisateur a été vérifiée et qu'il a l'autorisation d'accéder aux ressources concernées. L'authentification par certificats repose sur une technologie de chiffrement qui permet de chiffrer (ou signer) un message sans avoir à partager de " secret ". L'identifiant est un certificat public signé par une autorité de certification reconnue.

La figure.1.5 résume les differentes etapes d'authentification forte par certificats numériques.

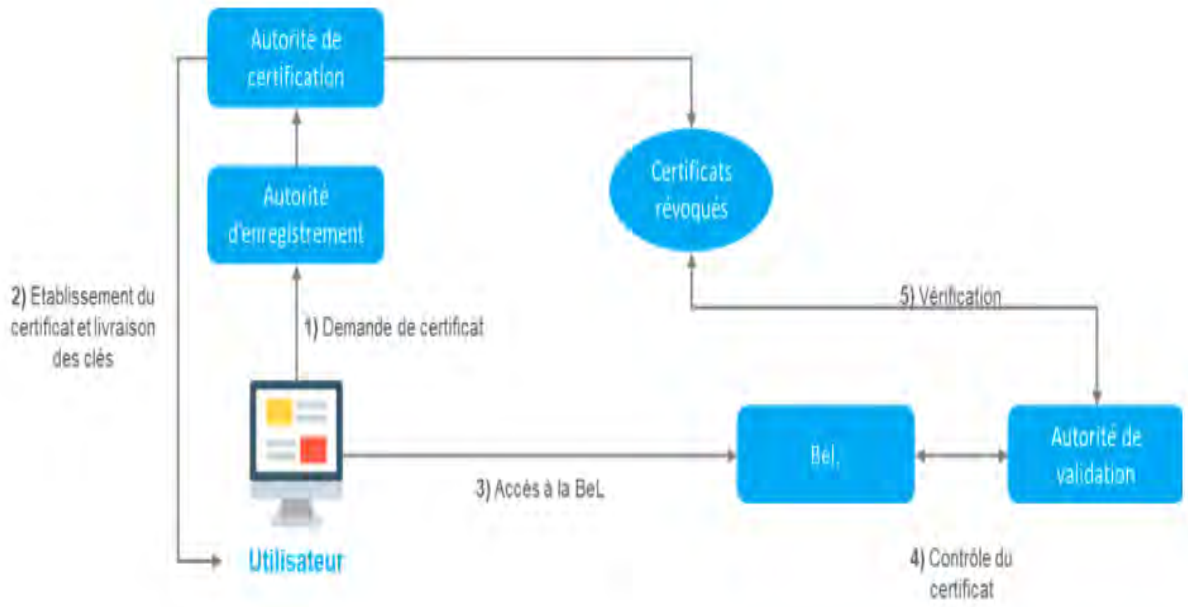


Figure.1.4.etapes d'authentification forte par certificats numériques source :[11]

Toutes ces solutions garantissent une sécurité et un contrôle des accès bien plus efficaces que l'utilisation seule de mots de passe.

1.4 Solution préconisée

Le choix de la solution d'authentification forte repose sur trois principaux critères :

— Le niveau de sécurité
— L'expérience utilisateur
— Le coût

Il est recommandé d'adopter une approche souple, en implémentant une méthode d'authentification basée sur le niveau de risque, et de choisir une solution qui permettra de s'adapter en cas de besoins. Cette approche offre généralement le meilleur compromis entre un niveau de sécurité élevé et une bonne expérience utilisateur. Compte tenu de la multitude de solutions d'authentification forte, il est également recommandé d'évaluer soigneusement chacune des solutions disponibles en se posant les questions suivantes :

— Quel est le niveau de sensibilité de mes données métier ?
— Mes utilisateurs doivent-ils accéder à de nombreuses applications protégées par un mot de passe ?
— Mes utilisateurs doivent-ils se connecter à distance ?

A l'inverse des autres solutions d'authentification forte , y compris la biométrie, Les certificats numériques ont des caracteristiques importantes :

— Processus d'intégration et de formation minimal
— Nombre réduit de demandes d'assistance technique
— Aucun équipement supplémentaire nécessaire
— Aucun jeton d'authentification à distribuer ou gérer
— Aucun plan de secours à mettre en place si oubli ou perte du jeton
— Les utilisateurs peuvent travailler sur plusieurs appareils sans interruptions
— Fonctionne avec très peu de ressources internes
— Identifiants faciles à émettre ou révoquer selon le renouvellement du personnel

En effet aucun équipement supplémentaire n'est nécessaire pour utiliser un certicat numérique. Le certicat est conservé sur l'ordinateur de l'utilisateur, il n'y a donc aucun risque d'oubli ou de perte du jeton d'authentification indispensable pour la création d'un mot de passe unique. Les certificats numériques peuvent être exportés sur d'autres appareils
Remarque : dans les situations à haut risque, la copie et l'installation des clés doivent être gérées avec prudence.

Voici donc quelques-unes des nombreuses raisons pour lesquelles on envisage de choisir comme type d'authentification forte OTP(One-Time Password)(mot de passe à usage unique) et déployer le SSL(https) avec certificat pour authentifier les utilisateurs internes , externes et les partenaires utilisants les differentes ressources de l'entreprise LaPoste.

Conclusion

Les mécanismes d'authentification forte sont nombreux. Cependant le choix du mécanismes d'authentification forte fait appel à plusieurs criteres comme : Le niveau de sécurité, L'expérience utilisateur et le coût. Ainsi il est necessaire d'étudier de plus prés toutes les notions fondamentales des mécanismes d'authentification forte.

Chapitre 2

Présentation du thème et les notions fondamentales

Introduction

Le monde numérique qui est reposé sur le concept de sécurité des systèmes d'informations recouvre un ensemble de méthodes, techniques et outils chargés de protéger les ressources et les échanges. Dans ce chapitre, nous allons découvrir les differentes méthodes utilisées pour améliorer la sécurité en particulier les PKI, aussi nous allons présenter une définition sur la PKI, les différentes méthodes qui assurent la transaction des données d'une manière confidentielle et authentique, et les certificats qui garantissent leur sécurité.

2.1 Justification du champ d'étude

Le schéma d'authentification des utilisateurs le plus couramment utilisé pour la connexion à des services numériques de toutes sortes est toujours une combinaison de nom d'utilisateur et de mot de passe. Si un attaquant devine ou vole le mot de passe de l'utilisateur, il peut effectivement voler l'identité numérique de l'utilisateur, accéder aux informations personnelles ou professionnelles de l'utilisateur et de l'entreprise et effectuer des actions par formulaire dans le nom de l'utilisateur. Le mot de passe est souvent le lien le plus faible . Pour de nombreuses applications, ce niveau de sécurité peut être suffisant. Mais les informations sensibles où la capacité à effectuer des actions critiques nécessitent des niveaux de sécurité supplémentaires. L'authentification multifacteur (MFA) est une méthodologie qui introduit des facteurs d'authentification supplémentaires et indépendants qui doivent tous être validés lors de l'authentification d'un utilisateur. Dans certains domaines d'application, comme l'e-banking, l'authentification multifacteur est déjà un mécanisme établi. De nombreux fournisseurs de services bien connus ont également adopté la 2FA (authentification à deux facteurs, souvent appelée «vérification en 2 étapes»), notamment Apple, Google, Microsoft et même Steam. C'est ce qui nous pousse à faire l'étude et le déploiement d'un système de gestion d'une authentification forte pour le cas du Groupe LaPoste.

2.2 Objectif général du thème

1. **Généralités sur la sécurité des réseaux informatiques**

   Définition 2.2.1. ***(Cryptologie)***
   La cryptologie est une science de chiffrement, englobant la cryptographie et la cryptanalyse. Elle a pour objet les écrits secrets et leur étude. Elle permet de cacher des informations, d'assurer la confidentialité des messages et de garantir leur authenticité.

a-) **Cryptographie** : c'est une discipline incluant les principes, les moyens et des méthodes de transformation des données, afin de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale.

b-) **Cryptanalyse** : c'est l'étude des faiblesses des outils de sécurité (algorithmes) produits par la cryptographie dans le but de les corriger ou nuire au système de communication .

c-) **Chiffrement** : Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.

d-) **Déchiffrement** : C'est la fonction permettant de retrouver le texte clair à partir du texte chiffré.

e-) **Texte chiffré** : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

f-) **Clé** : Il s'agit du paramètre impliqué et autorisant des opérations de **chiffrement** et/ou **déchiffrement**.

g-) **Cryptosystème** : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un **algorithme** donné.

2. **Objectif de la cryptographie**
   Pour assurer la sécurité dans le transfert de données, la cryptographie dans les applications téléinformatiques doit garantir la sécurité à quatre niveaux :

   Confidentialité : La confidentialité des données garantit que seul le destinataire peut lire le message.

   Authentification : L'authentification a pour objectif de vérifier l'identité des processus communicants, et garantit que le message vient bien de la personne de qui il déclare venir.

   Intégrité : L'intégrité des données garantit que les messages ne sont pas modifiés durant le transfert, et le récepteur peut vérifier que le message reçu est identique au message envoyé et qu'aucune manipulation ne s'est produite.

   Non-répudiation : La non-répudiation des données est un service similaire qui permet à l'expéditeur d'un message d'être identifié de façon unique.

3. **Modélisation des systèmes de chiffrement**

   Un système de cryptographie est composé d'un quintuplet $(P, C, C_k, D_{k'}, K)$ où :

   — P est un ensemble appelé espace des textes clairs

   — C est un ensemble appelé espace des textes chiffrés

   — C est un ensemble appelé espace des clés

   — $C_k : P \longrightarrow C$ est une fonction inversible à gauche appelée fonction de chiffrement et qui dépend d'un parametre k appelé clé.

   — $D_{k'} : C \longrightarrow P$ est la fonction inverse à gauche de C_k (i.e $D_{k'} \circ C_k(m) = m, \forall m \in P$) et est appelée fonction de déchiffrement (dépendant de la clé k').

   A partir de ce modèle, il existe deux systèmes de cryptographie : le système symétrique ou cryptographie à clés secrètes et le système asymétriqu ou non-symétrique ou cryptographie à clés publiques.

4. **Cryptographie a clés symétriques et asymétriques**

   Nous distinguons deux types de cryptographie symétrique et asymétrique.

a-) **Cryptographie à clé symétrique (clé secrète) :**

Le principe de la cryptographie symétrique repose sur l'utilisation d'une seule clé secrète appelée clé privée pour chiffrer et déchiffrer, elle permet d'assurer la confidentialité des données ainsi que leur authentification du faite que seules les personnes possédant la clé peuvent chiffrer et déchiffrer un message. Cependant son plus grand avantage repose sur sa rapidité et la facilité dans sa mise en œuvre sur les circuits (bon marché).
D'autre part, si une personne malicieuse prend part de cette clé alors tout devient à découvert, il devient possible pour cette personne de déchiffrer le message et de le modifier. Par ailleurs le plus grand inconvénient est d'avoir toujours des problèmes dans la gestion des clés quand on a un nombre d'utilisateurs élargi, en effet, il faudrait au moins une clé privée pour chaque couple d'utilisateurs, ainsi on se retrouve dans le problème de partage et de distribution des clés.

Caractéristiques :

— Les clés de chiffrement (K_E) et de déchiffrement (K_D) sont identiques : $K_E = K_D = K$.

— La clé doit rester secrète.

— Au niveau de la génération des clés, elle est choisie aléatoirement dans l'espace des clés ;

— Ces algorithmes sont basés sur des opérations de transposition(diffision) et de substitution des bits du texte clair en fonction de la clé ;

— Les algorithmes les plus répandus sont le DES, AES, 3DES, ...

— La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256,

— L'avantage principal de ce mode de chiffrement est sa rapidité,

Limites :

— Le principal désavantage réside dans la distribution des clés : pour une meilleure sécurité, on préfèrera l'échange manuel. Malheureusement, pour de grands systèmes, le nombre de clés peut devenir conséquent. C'est pourquoi on utilisera souvent des échanges sécurisés pour transmettre les clés. En effet, pour un système à N utilisateurs, il y aura $N(N-1)/2$ paires de clés.

Les algorithmes les plus répandus sont :

DES (Data Encryption Standard) : est un algorithme de chiffrements par bloc de 64 bits (clé : 56 bits + redondance : 8bits) ce qui nous donne 256 possibilités. C'est un algorithme robuste et bien conçu, il a résisté à toutes les attaques

3DES : utilisé 3clés, ce qui nous donne une clé effective de 168 bits (56*3). Ce système est suffisamment robuste pour la plupart des transactions bancaire. Mais vu le nombre de traitement, il nécessite des ressource système important, une grande capacité mémoire, son exécution ralentirais la communication. Il est généralement utilisé serveurs et les stations de travail.

AES (Advanced Encryption Standard) : « standard de chiffrement avancé », il s'agit d'un algorithme de chiffrement symétrique, il prend en entrée un bloc de 128 bits (16 octet), la clé fait 128, 192 ou 256 bits.

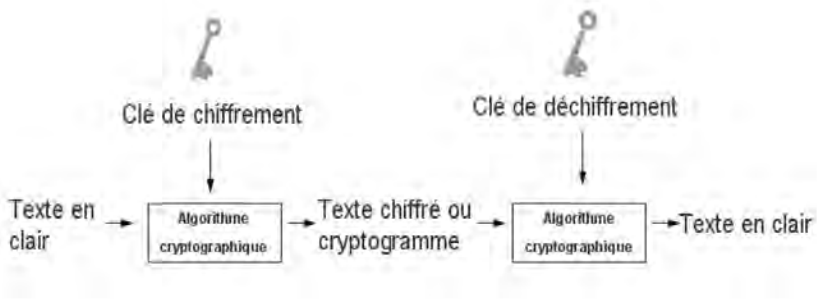


Figure.2.1.Chiffrement symétrique source :[2]

b-) **Cryptographie à clé asymétrique (à clé publique) :**
Afin de résoudre les principaux inconvénients de cryptographie symétrique qui consiste dans la gestion des clés, une nouvelle technique cryptographique a été mise en place c'est la Cryptographie Asymétrique à base de clé publique. Le principe de cryptographie asymétrique repose sur l'utilisation de deux clés déférentes, l'une est publique et l'autre est privée. La clé publique est utilisée pour le chiffrement et peut être publiée librement, tandis que la clé privée est destinée pour le déchiffrement, elle doit être impérativement secrète et cachée. La figure 2.2 montre le fonctionnement de chiffrement à clés asymétrique.

Fonction à sens unique :

Soit M et C deux ensembles et $f : M \longrightarrow C$ et $f(M)$ image de M par f. f est à **sens unique** si

(a) $\forall x \in M, f(x)$ facile à calculer (temps polynomial) et

(b) Trouver, pour la plupart des $y \in f(M)$ un $x \in M$ tel que $f(x) = y$ doit être difficile

$f : M \longrightarrow C$ à sens unique est à **trappe** si le calcul dans le sens inverse est efficace en disposant d'une information secrète la trappe qui permet de construire g tel que $g \circ f = Id$.

Facile de calculer l'image par f mais calculatoirement difficile d'inverser f sans connaître g.
Construire des couples (f, g) doit être facile. Publier f ne doit rien révéler sur g.

Idée : algos (2 clés) $\neq$, f pour chiffrer (clé publique) et g pour déchiffrer (clé privée) .

Problèmes mathématiques :
Les algorithmes se basent sur des concepts mathématiques tels que :

— l'exponentiation de grands nombres premiers (RSA)
— le problème des logarithmes discrets (ElGamal) ;
— le problème du sac à dos (Merkle-Hellman) ;
— le problème sur les réseaux arithmétiques (NTRU) ;
— le problème sur les polynôme mutivariés ;
— problème d'isogénie supersingulière décisionnelle (SIDH)
— problème d'isogénie supersingulaire computationnelle ;
— problème de calcul supersingular computational Diffie-Hellman ;

Caractéristiques :

— Une clé publique K_{pub} (pour chiffrer ou vérifier une signature),
— Une clé privée K_{priv} (pour déchiffrer ou signer) ;
— Propriété : La connaissance de K_{pub} ne permet pas de déduire K_{priv} ;
— $D_{K_{priv}}(E_{K_{pub}}(M)) = M$;
— Cependant, à l'inverse du chiffrement symétrique où le nombre de clés est le problème majeur, ici, seules n paires sont nécessaires. En effet, chaque utilisateur possède une paire (K_{priv}, K_{pub}) et tous les transferts de message ont lieu avec ces clés.
— La distribution des clés est grandement facilitée car l'échange de clés secrètes n'est plus nécessaire. Chaque utilisateur conserve sa clé secrète sans jamais la divulguer. Seule la clé publique devra être distribuée.

— Les algorithmes se basent sur des concepts mathématiques tels que l'exponentiation de grands nombres premiers (RSA), le problème des logarithmes discrets (ElGamal), ou encore le problème du sac à dos (Merkle-Hellman).

— L'algorithme de cryptographie asymétrique le plus connu est le RSA,

— Le principe de ce genre d'algorithme est qu'il s'agit d'une fonction unidirectionnelle à trappe. Une telle fonction à la particularité d'être facile à calculer dans un sens, mais difficile voire impossible dans le sens inverse. La seule manière de pouvoir réaliser le calcul inverse est de connaître une trappe. Une trappe pourrait par exemple être une faille dans le générateur de clés. Cette faille peut être soit intentionnelle de la part du concepteur (définition stricte d'une trappe) ou accidentelle.

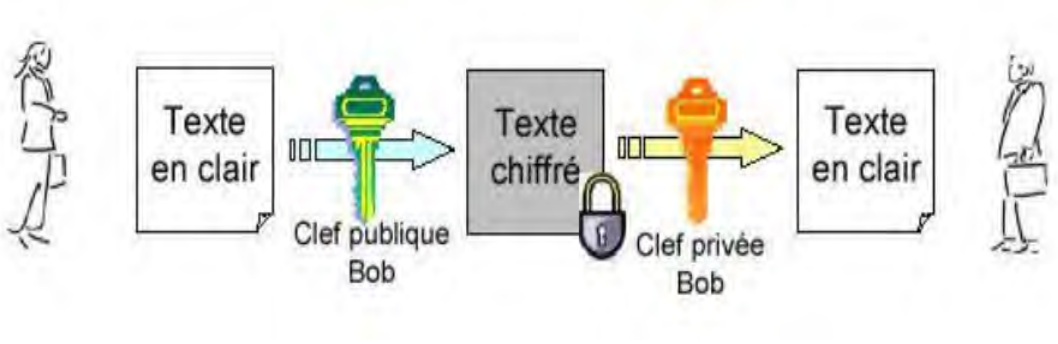


Figure.2.2.Chiffrement asymétrique source :[13]

Puisque la clé publique sert au chiffrement, alors tous les utilisateurs peuvent chiffrer un message que seul le propriétaire de la clé privée pourra déchiffrer, on assure ainsi la confidentialité, puisque les clés de chiffrement et de déchiffrement sont distinctes et ne peuvent se déduire l'une de l'autre.
Les algorithmes les plus répandus sont :

RSA (Algorithme de Cryptographie Asymétrique) : Pour générer les deux clés, il s'agit de choisir deux nombres premiers p et q. et un nombre e n'ayant pas de facteur commun avec q-1 et p-1, n=p*q est partagé et l'expéditeur calcule (M : message). Cet algorithme assurer la sécurité des transactions sensibles. Il est recommandé d'avoir recours à des clés de 1024 bits pour les applications normales et 2048 bits pour les applications les plus critiques.

DH (Diffie-Hellman) : est un protocole de cryptographie asymétrique qui permet à deux parties qui n'ont aucune connaissance préalable de l'autre d'établir conjointement une clé secrète partagée sur un canal de communication non-sécurisé qui utilise un chiffrement des clés de 512, 1024 ou 2048 bits

Inconvénient de la cryptographie asymétrique :
En contrepartie de leurs propriétés spécifiques, les chiffrements asymétriques sont globalement moins performants que leurs équivalents symétriques ; les temps de traitement sont plus longs, et pour un niveau de sécurité équivalent ; les clés doivent être beaucoup plus longues. Ils tendent à être environ 1000 fois plus

lents. Autrement dit, il va falloir plus de 1000 fois plus de temps de CPU (Central Processing Unit) pour traiter un cryptage ou décryptage asymétrique que symétrique. Si le chiffrement asymétrique permet de se prémunir des écoutes passives, la transmission initiale de la clé publique sur un canal non sécurisé exposé à des attaques de l'homme du milieu. Pour se prémunir contre ce risque on fait généralement appel à une infrastructure à clés publiques.

c-) **Système hybride**

Le système hybride est un système qui combine les deux branches de chiffrement symétrique et asymétrique, cela en utilisant le chiffrement à la clé publique du destinataire pour Chiffrer la clé de session (privée). La méthode de cet échange consiste à établir une communication entre deux individus Alice et Bob. Alice génère une clé de session privée pour chiffrer le message envoyé, cette clé de session sera chiffrée par la clé publique de Bob. Bob déchiffre le message à l'aide de sa clé privée, et connaît ainsi la clé de session commune. Alice chiffre ensuite le message avec la clé de session connue par Bob qui pourra aisément le déchiffrer. La figure.2.4 montre le fonctionnement de chiffrement hybride.

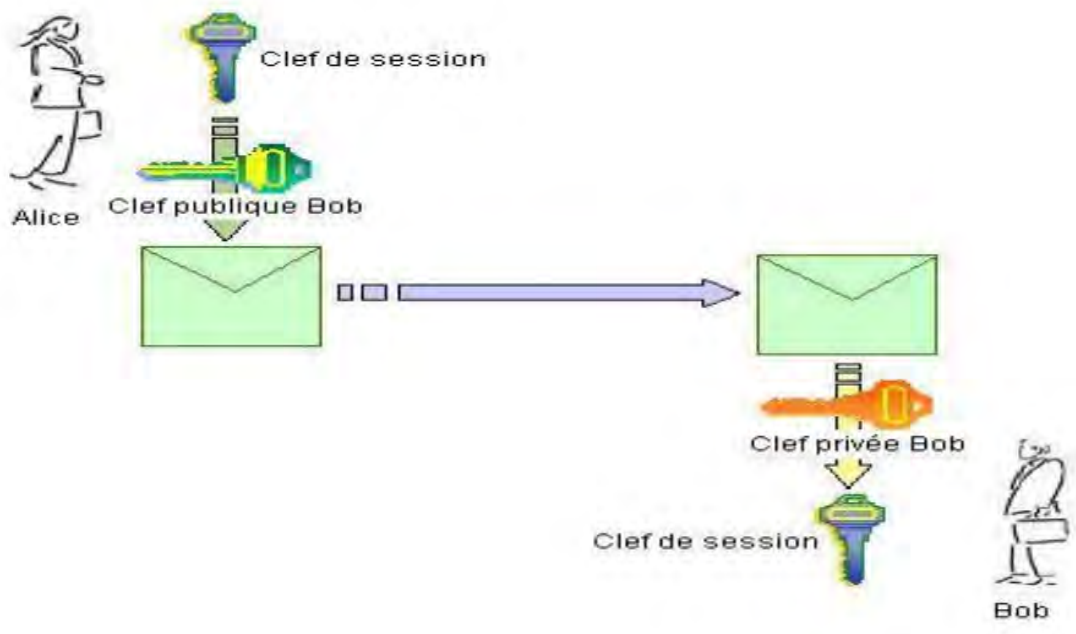


Figure.2.4.Chiffrement hybride source :[13]

Fonctions de hachage (empreinte)

Une fonction à sens unique est une fonction facile à calculer mais difficile à inverser. La Cryptographie à clé publique repose sur l'utilisation de fonctions à sens unique à brèche secrète celui qui connait le secret, la fonction devient facile à inverser. Le hachage est l'une des fonctions qui utilise le chiffrement à sens unique qui convertit une chaine de caractères à une chaine de caractère à longueur fixe

souvent taille inferieur, le résultat d'une fonction de hachage est appelé une empreinte, cette empreinte est unique et pas redondante, car il est rare de trouver deux empreintes similaires. Les fonctions de hachages sont souvent utilisées pour assurer l'intégralité et l'authentification de l'origine des documents envoyés . Une fonction de hachage verifie les propriétés suivantes :

$$h : \{0,1\}^* \longrightarrow \{0,1\}^n$$

a-) h permet de calculer à partir de tout message de longueur arbitraire appartenant à $\{0,1\}^*$ (Ensemble des messages) une valeur de longueur fixe appelé « empreinte » du message appartenant à $\{0,1\}^n$;

b-) La description du calcul $h(x)$, pour tout $x \in \{0,1\}^*$ doit être connu du public ;

c-) h est une fonction à sens unique ;

d-) Étant donné x et $h(x)$, il doit être "difficile" de trouver un message $x' \neq x$ tel que $h(x') = h(x)$, (**faible** résistance aux collisions)

e-) Il doit être impossible de trouver x, x' tels que $h(x') = h(x)$ (résistance **forte** de collision)

La figure.2.3 illustre le fonctionnement de hachage.

Figure.2.3.Fonction de hachage source :[13]

Il existe plusieurs algorithmes de hachage :

(a) **MD5 :**
C'est l'un des algorithmes de hachage les plus utilisés. Il divise un texte en plusieurs mots de 512 bits chacun pour en déduire un mot de 128bits. Ces 128bits sont calculés en blocs de 32bits par des permutations et des fonctions logiques. Malgré quelques failles découvertes dans le MD5 (Message Digest 5) mais il reste sécurisé et très performant.

(b) **SHA-1 :**
Comme le MD5, il exécute une série d'itérations et de fonction logique pour en déduire un mot de 160bits qui est l'ensemble de cinq mots de 32 bits.

5. **Signature**

Un système de signature est composé d'un quintuplet $(P, S, S_{s_k}, V_{p_k}, K)$ où :

(a) P est un ensemble appelé espace des textes à signer ;

(b) S est un ensemble appelé espace des signatures ;

(c) H une fonction de hachage ;

(d) K ensemble des paires de clés ;

(e) $S_{s_k} : P \longrightarrow S : m \longrightarrow S_{s_k}(H(m)) = \sigma_K$ la signature,

(f) $V_{p_k} : P \times P \longrightarrow \{0, 1\} = \{V, F\} : (m, \sigma) \longrightarrow V_{p_k}(m)$ qui vaut 1 si la signature est valide et 0 sinon.

Pour assurer cette demande, trois méthodes sont possibles :

— chiffrer le message

— utiliser une fonction de hachage

— utiliser un code d'authentification de message (MAC - Message authentication code)

Dangers à contrer

Plusieurs problèmes peuvent survenir lors de la transmission de messages, aussi bien entre les parties, que face à un pirate. En voici quelques-uns :

— mascarade : insertion des messages d'une source frauduleuse dans le réseau.

— modification du contenu : changements du contenu d'un message, y compris l'insertion, la suppression, la transposition, et la modification.

— modification de séquence (ou d'ordre) : toute modification à un ordre des messages entre les parties, y compris l'insertion, la suppression, et commander à nouveau.

— modification de la synchronisation : retarde ou rejoue des messages.

— répudiation de la source : démenti de transmission de message par source.

— répudiation de la destination : démenti de la réception du message par la destination.

2.3 Objectifs spécifiques

L'authentification forte a de multiples objectifs spécifiques, comme expliqué ci-dessous :

— **Amélioration de la sécurité des données**
En ayant recours à l'authentification forte, vous renforcez la difficulté pour accéder à vos comptes et vos données personnelles. Si vous optez pour deux facteurs de catégories distinctes, par exemple une information mémorisée comme la question secrète et un élément matériel, comme OTP ou l'appairage sur mobile, vous n'ajoutez pas seulement une protection au processus de connexion, mais vous passez bien à un niveau supérieur, plus complexe à atteindre pour un hacker.

— **Facilité d'utilisation dans la majorité des cas**
La majorité des procédés proposés pour l'authentification à double facteur sont faciles d'utilisation et accessibles à tous. En effet, ils ne nécessitent que très peu de matériel, à savoir un téléphone mobile, une clé cryptographique ou encore une connexion Internet. Particulièrement intuitifs, les étapes à suivre sont généralement bien expliquées pour permettre au plus grand nombre de les suivre sans difficulté majeure.

— **Accessibilité sur tous types de supports**
Que vous vous connectiez sur ordinateur, téléphone mobile ou encore tablette, l'authentification double facteur est accessible sur l'ensemble des supports numériques. Ainsi, vos données sont protégées quel que soit le canal que vous utilisez. Vous pouvez donc en changer selon vos envies et vos besoins, sans pour autant mettre en péril la sécurité de vos comptes.

2.4 Définitions et notions fondamentales

1. **Définition de la PKI(Public Key Infrastructure)**

   Une infrastructure à clés publiques PKI est un ensemble de technologies, organisations, procédures et pratiques qui supportent l'implémentation et l'exploitation des certificats basés sur la cryptographie à clés publiques. La PKI est une structure à la fois technique et administrative qui a pour but d'établir la confiance dans les échanges entre des entités morales, physiques et/ou logiques. Ainsi elle assure la création et la distribution des certificats.
   Techniquement la PKI est un système de gestion des clés publiques qui permet de gérer des listes importantes de clés publiques et d'en assurer la fiabilité pour des entités, généralement dans un réseau. Elle offre un cadre global permettant d'installer des éléments de sécurité tels que la confidentialité, l'authentification, l'intégrité et la non-répudiation tant au sein de l'entreprise que lors de l'échange d'information avec les différentes entités.

2. **Composants du PKI**

   Les PKI se compose de (04) quatre entités distinctes :

   — **AC (Autorité de Certification)** qui a pour mission de signer les demandes de certificat CSR (Certificate Signing Request) et de signer les listes de révocation CRL (Certificate Revocation List).

   — **L'Autorité d'Enregistrement RA (Registration Authority)** qui a pour mission de générer les certificats, et d'effectuer les vérifications d'usage sur l'identité de l'utilisateur final.

   — **L'Autorité de Dépôt (Repository)** qui a pour mission de stocker les certificats numériques ainsi que les listes de révocation.

   — **L'Entité Finale EE (Entité d'Extrémité)** :L'utilisateur ou le système qui est le sujet d'un certificat.

La figure 2.5 illustre l'architecture d'une PKI.

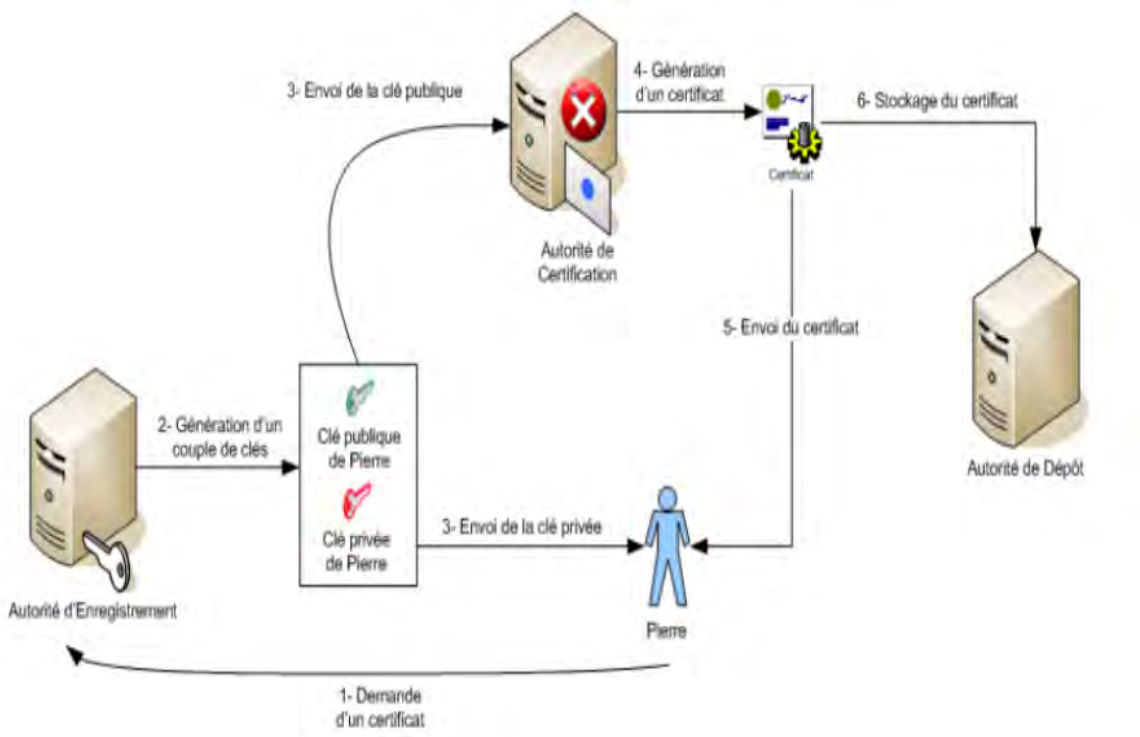


Figure.2.5.Architecture d'une PKI source :[13]

(a) **Autorité de Certification**
Une Autorité de Certification est une organisation qui délivre des certificats électroniques à une population. Elle possède elle-même un certificat (auto signé ou délivré par une autre AC) et utilise sa clé privée pour créer les certificats qu'elle délivre, une AC joue le rôle de tiers de confiance.
Les services des autorités de certification sont principalement utilisés dans le cadre de la sécurisation des documents ou des communications numériques via Internet ou Intranet. Lorsqu'une personne souhaite transmettre des données en utilisant par exemple une communication HTTPS (Hypertext Transfer Protocol Secure), elle génère une clé publique et une clé privée puis envoie à l'une des autorités de certification une demande de signature de certificat contenant sa clé publique ainsi que des informations sur son identité (coordonnées postales, téléphoniques, email...).
Après vérification de l'identité du demandeur du certificat par une autorité d'enregistrement, l'autorité de certification signe le CSR grâce à sa propre clé privée (et non pas avec la clé privée de la personne) qui devient alors un certificat puis le transmet en retour à la personne qui en a fait la demande.

Architecture logique d'une AC
Dans la vie courante, comme dans le cas de distribution de certificats physiques (permis de conduire, carte d'identité...), il est courant de posséder

plusieurs types de certificats .De la même façon, du point de vue électronique, nous serons amenés à posséder des certificats provenant d'autorités différentes mais pour des usages différents. Mais, même pour un usage identique, il peut être nécessaire de mettre en œuvre plusieurs autorités de certification. En effet, il est difficile de pouvoir tout gérer, surtout au niveau mondial, par un serveur de certification unique.

— **Le modèle hiérarchique**
Une autorité centralisée pourra déléguer ses pouvoirs de certification à des serveurs intermédiaires qui, eux-mêmes, les céderont à d'autres autorités jusqu'à un serveur de certification terminal qui délivrera les certificats aux particuliers. Ainsi, se crée, une hiérarchie de certification dans laquelle chaque niveau accrédite un niveau inférieur. Dans ce cas en parle de Co-certification. Le point central est le serveur racine (AC racine) qui doit distribuer sa clé publique à tous. Cette racine est le point de convergence de toutes les vérifications de certificats, c'est l'ancre de confiance. La figure 2.6 montre le modèle hiérarchique.

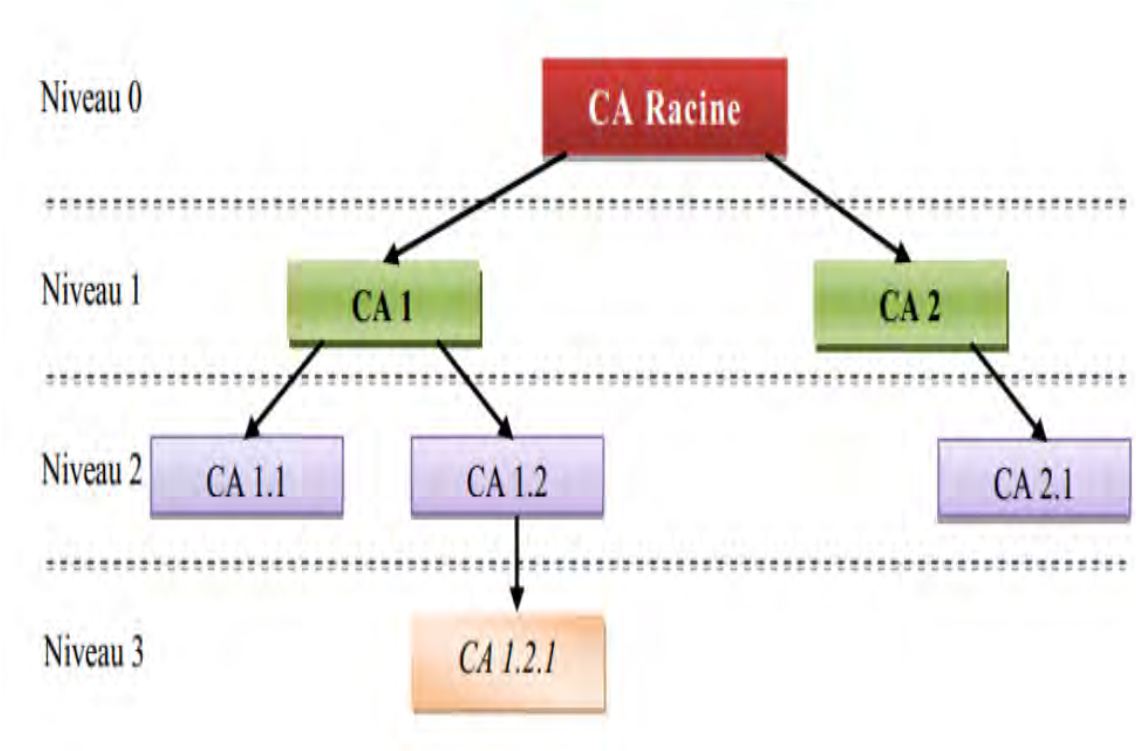


Figure.2.6.Modèle hiérarchique source :[13]

Une chaîne de certification est l'ensemble des Certificats nécessaires pour valider la généalogie d'un certificat d'un porteur de certificat. Ainsi la valeur pathlen du champ Basic doit être égal au nombre d'AC, dans ce cas il doit contenir la valeur 3. Il y a aussi plusieurs types du modèle comme le modèle trust list, le modèle maillé.

Opérations effectuées par l'Autorité de Certification

a-) **Délivrance des certificats**
Une AC crée un certificat en le signant par sa propre signature numérique. Généralement, une paire de clés (publiques, privées) est générée par le client, puis celui- ci dépose une demande de délivrance de certificat pour l'AC. La demande doit contenir au moins la clé publique du client et quelques autres informations (nom, adresse email,...). Quand une RA est fondé l'AC n'a plus besoin de faire le processus de vérification ou les autres fonctions de gestion car ils deviennent parmi les responsabilités de la RA. Après la vérification de la demande, l'AC crée le certificat numérique et le signe.

b-) **Renouvellement des certificats**
Chaque certificat a une période de validité et donc une date d'expiration bien connue. Quand un certificat expire, un processus de renouvellement est éventuellement initialisé et donc après l'approbation positive, un nouveau certificat va être publié pour l'EE considérée.

c-) **Révocation des certificats**
L'AC envoie le certificat pour le CRL (liste de certificats annulés) quand la durée de vie maximale pour un certificat est expiré.
Il y a plusieurs raisons peuvent amener une autorité à annuler des certificats :

— il est supposé que la clé privée du détenteur du certificat a été révélée ou subtilisée de façon frauduleuse ;
— l'utilisateur a perdu le rôle attaché à la possession de son certificat ;
— la clé privée de l'autorité de certification a été compromise ou subtilisée.

d-) **Publication des certificats et des CRLs**
Une fois le certificat est délivré ou qu'il est révoqué, l'information doit être publiée dans un annuaire public (conforme aux normes X.500 dans la majorité des cas). Les répondeurs OCSP (Online Certificate Status Protocol) qui offrent des avantages considérables par rapport aux CRL sont utilisés aussi pour répondre à cette fonction de révocation.

(b) **Autorité d'enregistrement RA**
L'autorité d'enregistrement est responsable des tâches administratives associées aux requêtes effectuées par l'entité d'extrémité EE. C'est une entité optionnelle dans la PKI. Si l'autorité d'enregistrement n'est pas présente dans la PKI, l'AC assume les mêmes tâches que celles associées à l'autorité d'enregistrement. Les fonctions qu'une autorité d'enregistrement doit mettre en application varient selon les fonctions que l'on souhaite mettre en œuvre sur la PKI, mais elle doit au minimum gérer les fonctions de vérification de l'identité du demandeur.
L'autorité d'enregistrement est généralement constituée des fonctions suivantes :

— Authentification personnelle (physique) du sujet demandant un certificat ;

- Vérification de la validité des informations indiquées par le demandeur ;
- Valider le droit pour un sujet de demander un certificat ;
- Vérification que le sujet possède la clé privée relative à la demande de certificat. On se réfère généralement au POP (Preuve de Possession) ;
- Reporter une compromission de clé quand une révocation est nécessaire ;
- Attribution des noms à des fins d'identification ;
- Génération des secrets partagés à utiliser pendant les phases d'initialisation et les phases de collecte de demande de certificat ;
- Déclenchement du procédé d'enregistrement avec l'autorité de certification de la part de l'entité d'extrémité ;
- Archivage des clés privées ;
- Initiation du processus de recouvrement de clé ;
- Distribution des clés privées (cartes à puce, Token USB (Universal Serial Bus),...).

(c) **Autorité de Dépôt (Repository)**
Le dépôt est généralement un annuaire LDAP(Lightweight Directory Access Protocol) qui est utilisé pour le stockage public des certificats et des CRL. PKI supporte essentiellement les annuaires LDAP via les protocoles opérationnels. Bien que les opérations avec un protocole de gestion puissent fournir un support de requête pour obtenir certains certificats ou des CRL, LDAP peut être employé directement comme protocole de consultation pour le même type d'information.

- **LDAP**
  Le LDAP est un protocole d'accès aux services annuaire qui propose une grande flexibilité pour la gestion des certificats d'une organisation. Les administrateurs systèmes peuvent stocker la plupart des informations requises par la gestion des certificats dans un annuaire compatible LDAP. Les informations stockées dans l'annuaire peuvent également être utilisées en association avec les certificats pour contrôler l'accès aux différentes ressources disponibles sur un réseau en fonction des utilisateurs ou des groupes d'utilisateurs.

3. **Certificat électronique**

Un certificat est un document électronique émis par un tiers de confiance ou AC, il est utilisé principalement pour identifier une entité physique ou morale, mais aussi pour chiffrer des échanges. Il assure un environnement de confiance aux utilisateurs pour échanger des informations numériques et confidentielles. Un certificat spécifie le nom d'une personne, serveur ou entité. Il certifie que la clé publique incluse dans le certificat, lui appartient.
Les certificats donc sont des petits fichiers divisés en deux parties :

- Une partie contenant des informations,
- Une partie contenant la signature de l'AC.

Son intérêt est de garantir l'intégrité du contenu du message, s'assurer que les instructions originales sont respectées et qu'elles ne seront pas modifiées lors de leur transmission. La structure des certificats est normalisée par le standard X.509 de l'UIT(Union International des Télécommunications) qui définit les informations contenues dans le certificat :

- Nom de l'autorité de certification ;
- Nom du propriétaire du certificat ;
- Date de validité du certificat ;
- Algorithme de chiffrement utilisé ;
- La clé publique du propriétaire.

(a) **Types de certificats**
Il existe quatre types de certificats électroniques :

- **Certificats de personne** : Destiné aux personnes est semblable à une carte d'identité nationale. Ce certificat peut être utilisé pour signer les messages électroniques et l'authentifier lors d'une session sécurisée.
- **Certificats serveur** : Propre à un serveur (web, courrier...). Il assure la sécurité des échanges entre le serveur et ses clients lors de l'établissement d'une session sécurisée.
- **Certificat VPN** : Permet à des informations dans certains nœuds du réseau (routeurs, Pare- feu...) d'être associées à une clé publique. Ce certificat est utilisé pour garantir la sécurité des échanges effectués entre une organisation et ses branches sécurisées dans le réseau de communication.
- **Certificat de signature de code** : Cela permet à un programme, un script ou un logiciel d'être signé pour garantir son authenticité par la signature de son développeur. Ce type de certificat permet la protection contre les risques de piratage.

(b) **Supports de certificat**
Un certificat électronique utilise un procédé cryptographique pour sécuriser et soutenir des documents. Le certificat électronique est un fichier de type PKCS12(Public Key Cryptography Standard), il peut se présenter soit sous sa forme logicielle ou il peut être stocké dans un support cryptographique :

- Solution logicielle : le certificat est téléchargé et stocké sur le disque dur de l'ordinateur.
- Solution matérielle : Sur une carte à puce ou une clé USB (le certificat est enregistré sur la clé dédiée qui se connecte directement sur le port USB du PC).

Les avantages d'un certificat stocké dans un support matériel sont plus sûrs et plus pratiques, vu qu'on ne peut pas le copier.

(c) **Cycle de vie d'un certificat**

- **Généré (valide) :** Cette étape consiste à gérer techniquement un fichier électronique à partir des informations personnelles du demandeur.
- **Expiré :** Au-delà d'une certaine date le certificat n'est plus valide car la validité temporelle a été dépassée.
- **Renouvelé :** Le certificat régénère un nouveau certificat moyennant les mêmes informations contenues dans le certificat expiré.
- **Révoqué :** Tout certificat est sujet à la révocation pour des raisons multiples. Il peut être volé soit physiquement, soit suite à une attaque informatique. Pour cette raison, chaque AC possède une CRL qui comporte les certificats dont les propriétaires ont exprimé leur demande de révocation.
- **Suspendu :** Dans le cas où l'utilisateur a un problème temporaire avec son certificat, il demande la suspension de son certificat, par la suite celui-ci est placé dans la CRL jusqu'à nouvel ordre.

La figure.2.7 résume toutes les étapes d'un cycle de vie de certificat.

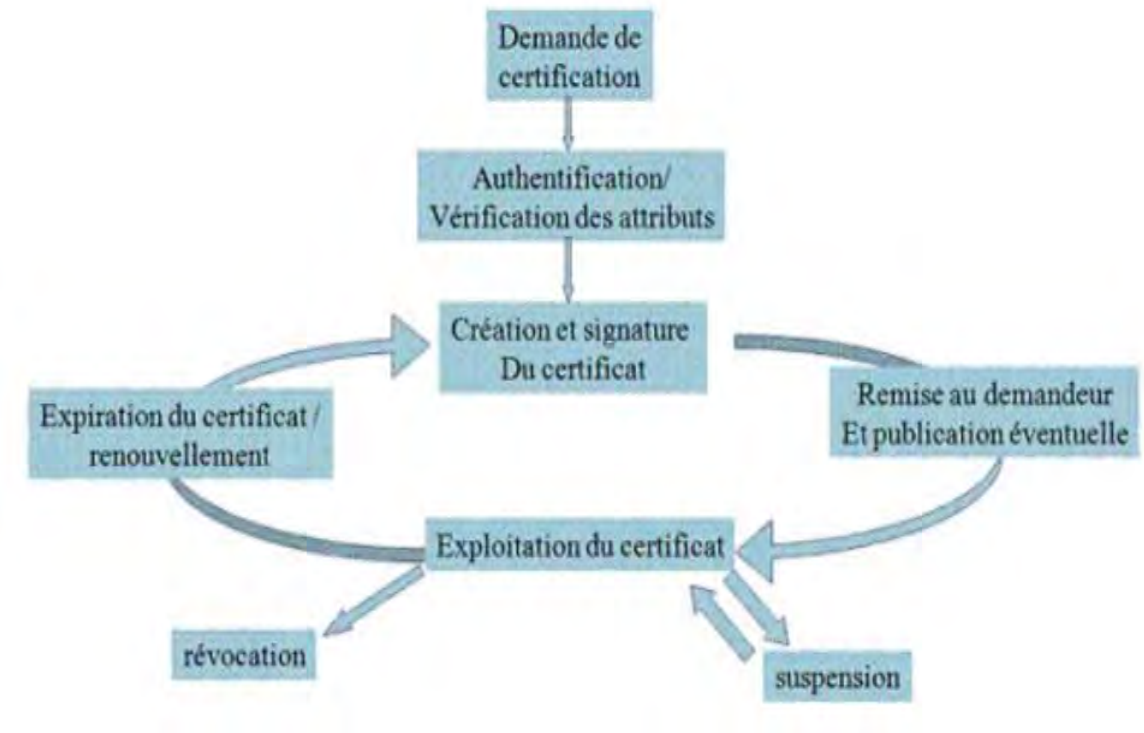


Figure.2.7.Cycle de vie d'un certificat source :[13]

(d) **Caractéristiques d'un certificat**
Le standard de certificat X.509 est lancé en association avec la norme X.500.

Il représente un système d'autorité de certification pour la délivrance des certificats et la vérification des signatures.

Version	Ce champ identifie à quelle version de X.509 correspond ce certificat.
Serial number	Numéro de série du certificat (propre à chaque AC).
Signature Algorithm ID	Désigne l'algorithme utilisé par l'AC pour signer le certificat, ainsi que tous les paramètres de l'algorithme.
Issuer Name	Permet d'identifier la AC qui a délivré le certificat. Il existe un formalisme bien déni pour attribuer un nom à chaque entité sans ambigüité.
Validity period	C'est une paire de date durant laquelle le certificat est valide.
Subject Name	Identifie le détenteur de la clé publique.
Subject public key info	Le nom de l'algorithme à clé publique (ex RSA), ainsi que tous les paramètres concernent cette clé, et la clé proprement dite.
Issuer Unique ID/Subject Unique Id	Extensions optionnelles introduites avec la version 2 de X.509.
Extensions	Extensions génériques optionnelles, introduites avec la version 3de X.509, Il permet aux autorités de certification de rajouter leurs propres informations aux certificats qu'elles délivrent.
Signature	Signatures numériques de l'AC sur l'ensemble des champs précédents

Tableau.2.1.Caractéristiques d'un certificat X.509 source :[13]

2.5 Avantage de la solution d'authentification forte

Selon les partisans, l'authentification multifacteur réduit considérablement l'incidence du vol d'identité en ligne et d'autres fraudes en ligne , car le mot de passe de la victime ne serait plus suffisant pour donner au voleur un accès permanent à ses informations.

Différentes composantes

Il existe plusieurs systèmes d'authentification forte dans le domaine de la sécurité informatique :

1. **OTP**
   C'est un système d'authentification forte permettant de sécuriser l'utilisation du mot de passe sur le réseau. En effet avec un système OTP, l'utilisateur possède un token(calculateur spécialisé) qui lui fournit à la demande un code(mot de passe) . Ce code est valide pendant une durée limitée seulement, et pour une seule utilisation.

la figure.3.1 montre le principe d'OTP :

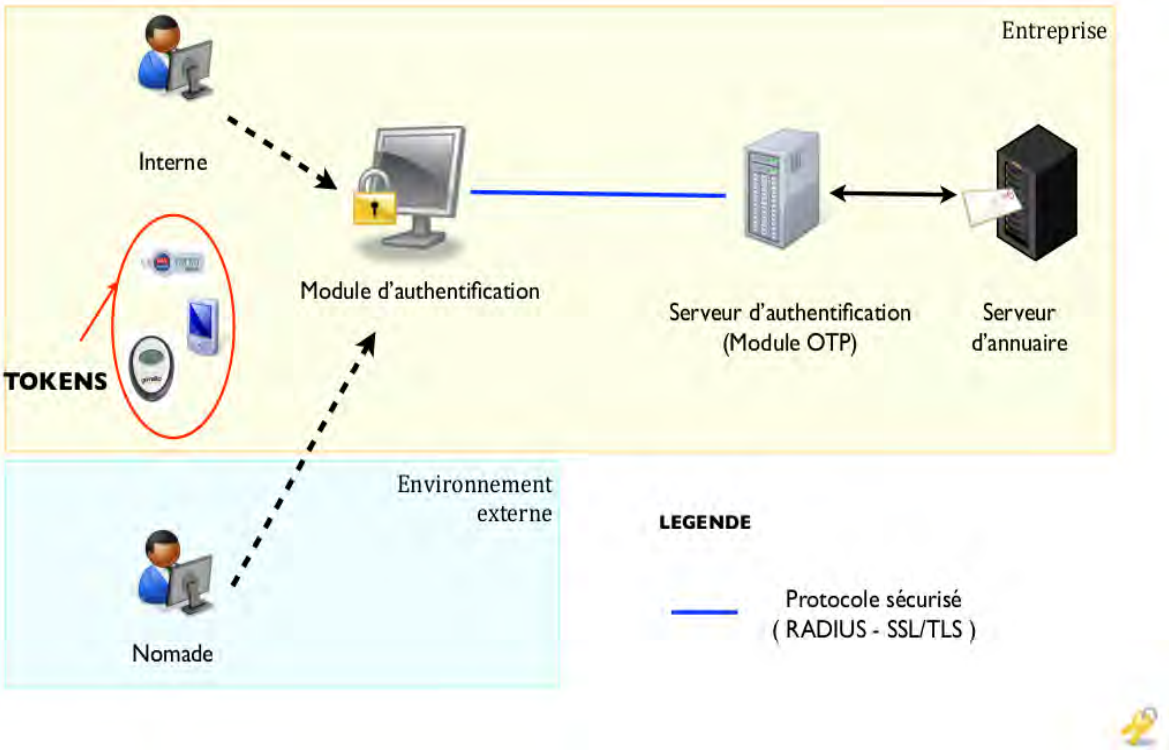


Figure.3.1 Mécanisme de l'OTP source :[4]

Cependant il existe plusieurs outils open source qui permettent de faire l'authentification forte par OTP.

outils open source :

a) **Google Authenticator**

L'application d'authentification à deux facteurs de Google est probablement la plus populaire et la plus connue des évangélistes 2FA. Elle est gratuite, pratique et proposée par défaut sur de nombreux sites Web. Jetons un coup d'œil à ses fonctionnalités :

— **Convivialité :** Google Authenticator a une interface utilisateur claire, facile à utiliser et décisive que même un enfant trouverait informative. En outre, il convient de noter que le logiciel fonctionne sur presque toutes les versions d'Android et iOS et ne prend pas plus de 2 Mo, ce qui est important pour les propriétaires de téléphones avec une petite quantité de RAM.

— **Algorithmes TOTP :**L'application Google Authenticator prend en charge les algorithmes de génération OTP de mot de passe à usage unique basé sur l'heure (TOTP) , ce qui permet de l'utiliser avec plus de ressources. TOTP est plus répandu et plus fiable, il s'agit d'un algorithme dans lequel le temps est utilisé comme l'un des paramètres pour la génération de mots de passe

à usage unique. La durée de vie de tous les mots de passe OTP générés selon les algorithmes TOTP est de 30 secondes, c'est-à-dire que chaque 30 secondes, un nouveau mot de passe est créé.

— **Pas besoin de connexion réseau :**L'utilisation de tels algorithmes de génération OTP permet à Google Authenticator de fonctionner sans connexion réseau. Les mêmes mots de passe à usage unique seraient générés sur votre smartphone sans accès à Internet ou au réseau cellulaire et sur le serveur d'authentification (dans le paradigme client-serveur), si les mots de passe à usage unique correspondent, vous avez accès à votre compte.

— **De nombreux comptes en un seul endroit :**Vous pouvez utiliser une application pour tous vos comptes sur différents sites Web ainsi que pour vos multiples comptes sur un site Web. C'est très pratique par rapport à l'authentification par SMS, mais sachez que vous pouvez avoir beaucoup de problèmes lors de la perte ou de l'effacement d'un téléphone si vous ne vous occupez pas de la sauvegarde de Google Authenticator

b) **FreeOTP Authenticator**
il existe une application intéressante et, surtout, simple et en même temps fonctionnelle FreeOTP Authenticator. Ce dernier a plusieurs caracteristiques :

— **Fonctionne pour de nombreux services :**Le programme fonctionne avec de nombreux services populaires : Google, Facebook, GitHub ; il est également disponible pour iOS et Android. Bien que nous puissions le dire à propos de presque toutes les applications de cette liste.

— **Faible Taille :** FreeOTP Authenticator n'occupe qu'une quantité de RAM égale à 500 Ko, ce qui est l'un de ses principaux avantages. Certains de ses concurrents nécessitent jusqu'à 6 Mo de RAM pour smartphone.

c) **Authy 2-Factor Authentication**
Basé sur un principe de fonctionnement similaire, Authy se distingue par des fonctionnalités intéressantes et extrêmement utiles :

— **Version Desktop :** Peu importe que vous ayez un smartphone ou que vous souhaitiez simplement utiliser l'application sur votre ordinateur, vous avez le choix. Les développeurs ont veillé à la commodité des utilisateurs de bureau.

— **Sauvegarde sur le cloud :**L'application permet à l'utilisateur de sauvegarder les données et de les stocker dans un cloud protégé. Ainsi, en cas de perte de votre smartphone ou de suppression accidentelle (ou non) de toutes les données de celui-ci, l'application vous aidera à restaurer l'accès aux comptes précédemment liés en quelques clics.

En se basant sur les fonctionnalités de ces software token(logiciels de génération de mot de passe à usage unique) open source , Google Authenticator reste le meilleur choix pour le déploiement de notre solution d'authentification forte au sein de LaPoste car étant gratuit, pratique, proposé par défaut sur de nombreux sites Web, son interface utilisateur est claire, facile à utiliser et en plus n'a pas besoin de connexion réseau.

Il existe aussi des outils d'authentication forte par OTP qui sont **payants** comme l'exemple de **RSA SecurID** ayant des ses prpopres fonctionnalités.

2. **Authentification biométrique**

L'authentification biométrique est la vérification automatique de l'identité ou l'identification basée sur les caractéristiques biologiques uniques de l'utilisateur, c'est-à-dire sur ses attributs biométriques, les solutions biométriques proposées sont les reconnaissances de l'empreinte, du visage, de la forme de la main, et beaucoup d'autres :

— **Empreinte digitale (finger-scan)**
L'authentification de l'empreinte digitale est la mesure biométrique la plus employée dans le monde, la donnée de base est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu.

La figure 3.2 montre l'authentification par l'empreinte digitale.

Figure.3.2 Authentification par l'empreinte digitale source :[13]

— **visage (facial-scan)**

Il s'agit ici de faire une photographie plus ou moins évoluée pour en extraire un ensemble de facteurs qui se veulent propres à chaque individu. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage tel que le haut des joues, les coins de la bouche, etc... On évitera d'autre part les types de coiffures, les zones occupées par des cheveux, en général ou toute zone sujette à modification durant la vie de la personne. La figure 3.3 représente l'authentification par visage.

Figure.3.3 Authentification par visage source :[13]

— **Biométrie vocale**

La biométrie vocale permet d'authentifier vos clients à l'aide de leur empreinte vocale, leur évitant ainsi toutes les contraintes liées aux codes confidentiels, mots de passe et autres questions de sécurité. Elle garantit un niveau de sécurité optimal, tout en offrant aux appelants une expérience inédite reposant sur le pouvoir de la parole [w4]. La figure 3.4 montre l'authentification par la voix.

Figure.3.4.Authentification par la voix source :[13]

Conclusion

Ce n'est un secret pour personne : les méthodes d'authentification par mots de passe ne sont plus fiables. Face à ce problème, auquel s'ajoutent l'omniprésence des risques inhérents au BYOD (Bring Your Own Device) et la menace grandissante des machines malveillantes, de nombreux professionnels informatiques s'interrogent sur la manière de s'assurer que seuls les utilisateurs et appareils autorisés pourront accéder [aux ressources, réseaux et applications souhaitées. Les certificats numériques sont heureusement adaptés aux deux cas d'utilisation : utilisateurs et machines. Étudions de plus près l'authentification basée sur des certificats. Pour quelles raisons choisir cette méthode ? Et comment l'utiliser ?

Chapitre 3

L'authentification forte basée sur un certificat

Introduction

L'authentification forte par certificats repose sur une technologie de chiffrement qui permet de chiffrer (ou signer) un message sans avoir à partager de " secret ". L'identifiant est un certificat public signé par une autorité de certification reconnue.

3.1 Qu'est-ce que l'authentification basée sur des certificats ?

L'authentification basée sur les certificats désigne l'utilisation d'un certificat numérique pour identifier un utilisateur, une machine ou un périphérique avant de lui octroyer l'accès à une ressource, un réseau, une application, etc. Pour authentifier un utilisateur, cette méthode est souvent déployée conjointement à d'autres méthodes classiques comme l'authentification basée sur un nom d'utilisateur et un mot de passe.

3.2 Qu'est-ce qui distingue l'authentification basée sur des certificats des autres méthodes ?

Contrairement à certaines solutions qui ne fonctionnent que pour les utilisateurs (biométrie ...etc), la même solution peut être utilisée pour tous les points de terminaison utilisateurs, machines, périphériques et même pour l'Internet des Objets (IoT) en plein essor.

A l'inverse des autres solutions, y compris la biométrie, aucun équipement supplémentaire n'est nécessaire pour utiliser un certificat numérique. Le certificat est conservé sur l'ordinateur de l'utilisateur, il n'y a donc aucun risque d'oubli ou de perte du jeton d'authentification indispensable pour la création d'un mot de passe unique. Les certificats numériques peuvent être exportés sur d'autres appareils. (remarque : dans

les situations à haut risque, la copie et l'installation des clés doivent être gérées avec prudence).

3.3 Pourquoi utiliser l'authentification basée sur des certificats ?

— **Facilité de déploiement et gestion continue**

Aujourd'hui, la plupart des solutions basées sur des certificats sont fournies avec une plateforme de gestion sur le cloud qui facilite les émissions de certificats pour les nouveaux employés. Cette solution séduit les administrateurs chargés en prime du renouvellement et de la révocation des certificats après le départ des collaborateurs. Grâce à l'automatisation des commandes et l'activation de l'installation en mode silencieux, les solutions qui s'intègrent à Active Directory simplifient encore davantage les processus de commande et d'émission.

— **Convivialité**

Entre renforcer la sécurité, ou réduire les coûts et la pénibilité pour les utilisateurs finaux, c'est toujours une affaire de compromis. On omet bien souvent ce critère, mais les certificats sont extrêmement simples à manier pour les utilisateurs finaux. Une fois le certificat installé (dans certains cas, l'opération s'effectue même automatiquement), il n'y a rien d'autre à faire. De plus, la plupart des solutions d'entreprise prennent déjà en charge l'authentification basée sur les certificats.

— **Exploitation des règles de contrôle d'accès existantes**

Vous pouvez également exploiter facilement les règles de groupes et les autorisations existantes pour contrôler les utilisateurs et les machines autorisés à accéder aux différents réseaux et applications. Ainsi, seuls les utilisateurs qui possèdent les privilèges correspondants peuvent accéder aux opérations sensibles ou stratégiques.

— **Authentification mutuelle**

Autre avantage : l'utilisation des certificats permet une authentification mutuelle. En clair, les deux parties engagées dans une communication s'identifient elles-mêmes, qu'il s'agisse d'une communication entre deux utilisateurs, entre un utilisateur et une machine ou entre deux machines. Ainsi, avant qu'une connexion puisse être établie, un client doit prouver son identité pour accéder à l'intranet de l'entreprise et l'intranet doit prouver son identité au client.

— **Extension aux utilisateurs externes**

Les certificats sont également faciles à déployer pour les utilisateurs en dehors de votre organisation (partenaires, sous-traitants et prestataires indépendants) qui sont susceptibles d'avoir besoin d'accéder à vos réseaux. Pas besoin pour eux d'installer de logiciel supplémentaire sur leur machine locale ou de se former longuement : les certificats sont simples à utiliser.

3.4 Cas d'utilisation

Le protocole SSL

Le protocole Secure Sockets Layer (SSL) est un ensemble de règles gouvernant l'authentification serveur, l'authentification client et les communications encryptées entre des serveurs et des clients. SSL est largement utilisé sur Internet, particulièrement pour les interactions mettant en œuvre l'échange d'informations confidentielles telles que les numéros de cartes de crédit.

SSL requiert un certificat SSL serveur, au minimum. Comme partie du processus de négociation, le serveur présente son certificat au client afin d'authentifier son identité. Le processus d'authentification utilise le chiffrement par clef privée et les signatures numériques pour confirmer que ce serveur est bien celui-ci qu'il prétend être. Une fois le serveur authentifié, le client et le serveur utilisent des techniques de chiffrement à clefs symétriques, ce qui est rapide, pour chiffrer toutes les informations qu'ils échangent pour le reste de la session et pour détecter toutes tentatives d'altération des données qui peuvent arriver.

Les serveurs peuvent éventuellement être configurés pour demander l'authentification client aussi bien que l'authentification serveur. Dans ce cas, après le succès de l'authentification serveur, le client doit à son tour présenter son certificat au serveur afin d'authentifier son identité avant qu'une connexion SSL ne puisse s'établir.

Etude d'un cas d'authentification SSL/TLS

L'objectif des certificats est de permettre l'identification des accès aux systèmes d'information de l'entreprise, aux sites internet, intranet. Parade au phishing, sécurisant les accès et les opérations sensibles pour les populations nomades, le certificat permet d'éviter les usurpations d'identité. Lors d'une négociation SSL (Secure Socket Layer), il faut s'assurer de l'identité de la personne avec qui on communique (risque d'une attaque de type « Man In the Middle »). Voici dans la figure.3.5 le fonctionnement d'une authentification SSL mutuelle lors de la création d'une connexion sécurisée entre un client et un serveur avec certificats (utilisateur et serveur).

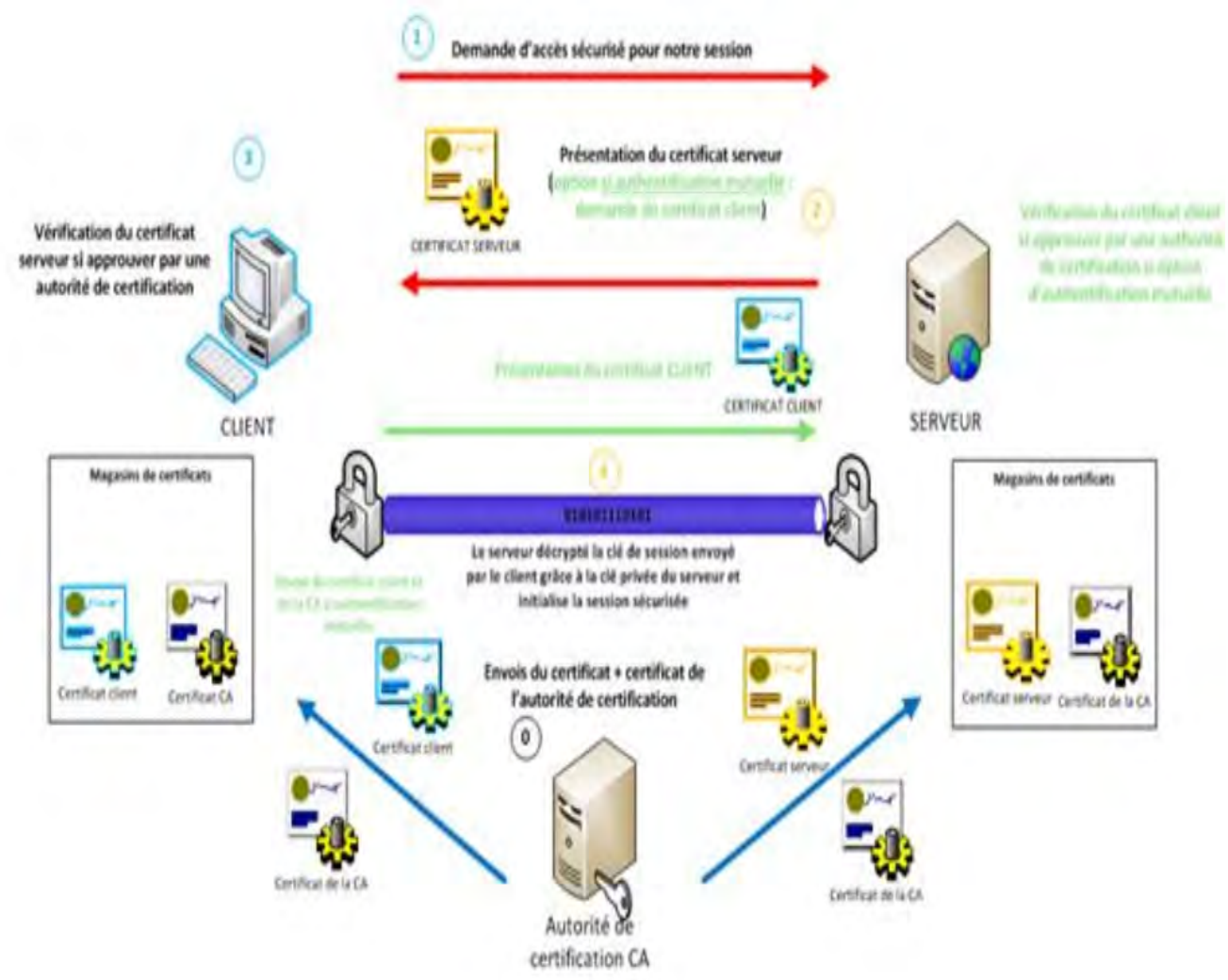


Figure.3.5.Authentification avec certificat x.509 source :[13]

Cette technique permet d'avoir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.

Les échanges définis par le protocole SSL se déroulent en deux phases :

1. **Première phase : authentification du serveur (en rouge)**
   - requête d'un client, le serveur envoie son certificat au client et lui liste les algorithmes cryptographiques, qu'il souhaite négocier.
   - Le client vérifie la validité du certificat en interrogeant la liste CLR.
   - Le client génère ensuite une empreinte chiffré avec la clé publique du serveur puis transmis à ce dernier.
   - Les données échangées par la suite entre le client et le serveur sont chiffrées et authentifiées à l'aide de clés dérivées de celle-ci.
2. **Deuxième phase : authentification (optionnelle) du client (en vert)**

— Le serveur (et seulement lui) peut demander au client de s'authentifier en lui demandant tout d'abord son certificat.

— Le client réplique en envoyant ce certificat puis en signant un message avec sa clé privée (ce message contient des informations sur la session et le contenu de tous les échanges précédents).

L'utilisation d'une authentification bidirectionnelle (mutuelle) permet d'assurer l'intégrité, la confidentialité et grâce à la Deuxième phase, la non répudiation, permettant de garantir qu'une transaction ne peut être niée par aucune des deux parties (client ou serveur).

Ainsi les méthodes d'authentification forte ont des caracteristiques particulieres .Voyons tout ça dans le tableau comparatif ci-dessous des différentes méthodes d'authentification forte.

Méthode d'authentification	Requiert un objet additionnel	Requiert le téléphone portable de l'utilisateur	Étape additionnelle pour l'utilisateur
Authentification réseau via certificat	Non	Non	Non
Login et mot de passe	Non	Non	Non
One Time Password	Oui	Parfois	Oui
SMS	Non	Oui	Oui
Smart card / USB Token	Oui	Non	Oui
Biométrie	Parfois	Non	Parfois

Figure.3.6. Tableau comparatif des méthodes d'authentification forte [16]

De ce fait notre choix porte sur l'authentification forte basée sur OTP(One-Time Password) et le déploiement du SSL(https) avec l'aide des certificats.

En effet nous allons mettre en pratique dans le chapitre suivant le déploiement d'authentification forte basé sur OTP(One-Time Password) et du SSL(https) avec certificat dans l'entreprise LaPoste.

Conclusion

Dans ce chapitre nous avons vu l'importance de l'authentification forte par certificat.Le choix de l'authentification forte repose sur trois principaux critères : le niveau de sécurité, l'expérience utilisateur et le coût. Cependant nous allons déployer la solution d'authentification forte basée sur OTP(One-Time Password) et du SSL(https) avec certificat dans l'entreprise LaPoste où nous expliquons toutes les étapes en pratique dans le chapitre suivant.

Deuxième partie

Approche pratique

Chapitre 4

Déploiement d'une authentification forte basée sur OTP(One-Time Password) et du SSL(https) avec certificat

Introduction

Cette partie nous amene à faire la pratique de la solution d'authentification forte à mettre en place dans l'entreprise LaPoste.Ainsi nous allons dabord déployer le SSL(https) dans l'application DigitalPost avec des certificats client-serveur. Ensuite déployer la solution d'authentification forte basée sur OTP(One-Time Password) mot de passe à usage unique avec le software token(logiciel de génération de mot de passe à usage unique) Google Authenticator et enfin faire les tests de fonctionnements.

4.1 Architecture applicative

— **Architecture Generale de LaPoste**

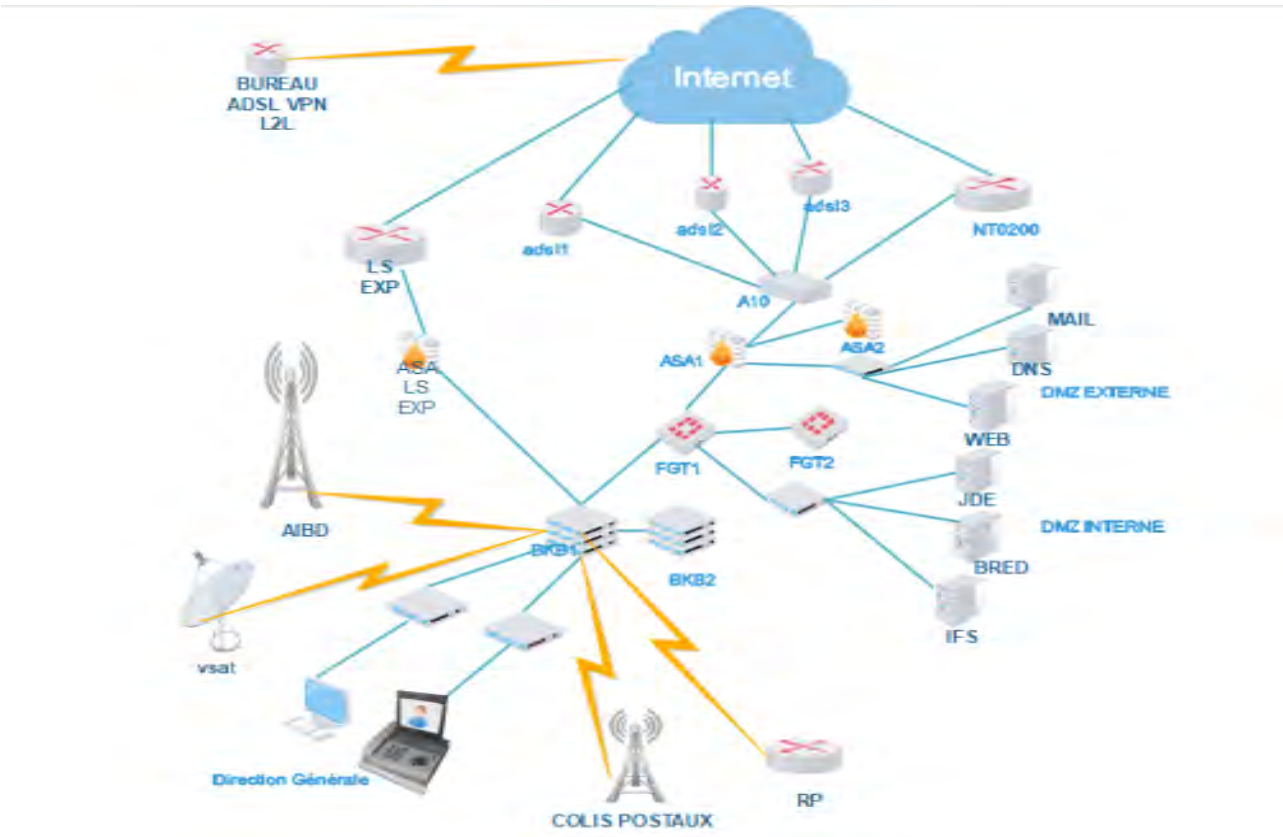


Figure.4.1.1 Architecture Generale de LaPoste

— **Architectures applicatives de la solution d'authentification forte par OTP(One-Time Password) et du SSL(https) avec certificat de LaPoste**

a) **Architecture de communication client-serveur via SSL(https) avec certificat**

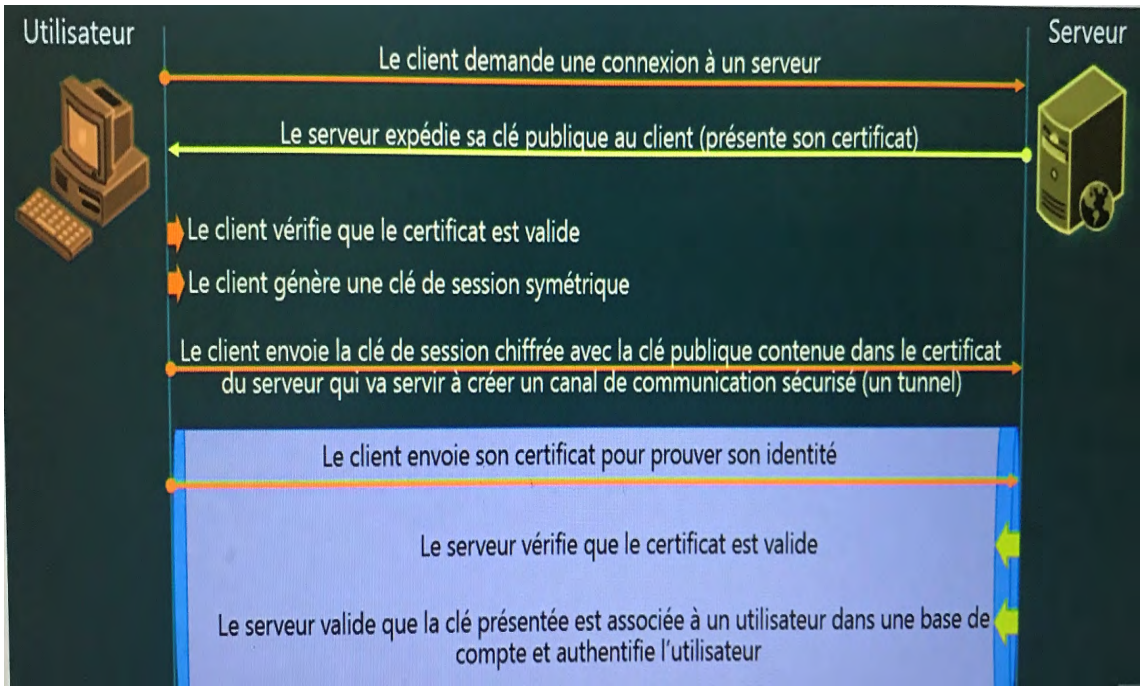


Figure.4.1.2 Architecture de communication Client-Serveur [16]

b) **Architecture de communication d'un agent de LaPoste avec le serveur d'application de LaPoste via SSL(https) avec certificat**

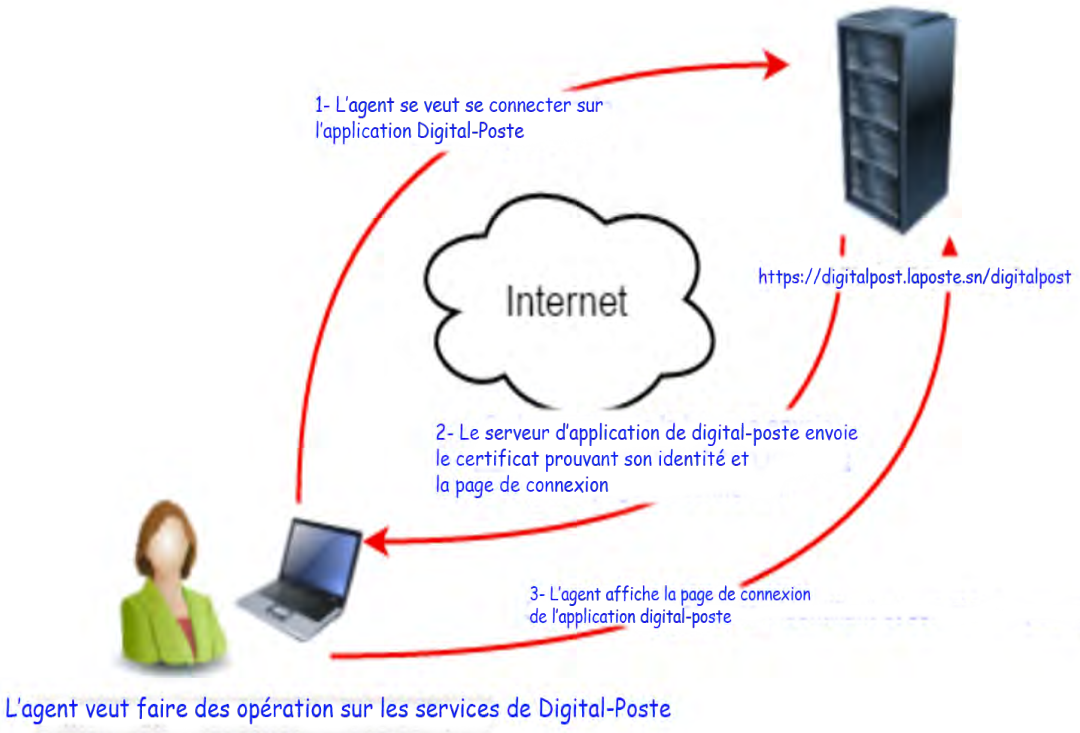


Figure.4.1.3 Architecture communication agent et serveur d'application de LaPoste

c) **Principe de fonctionnement de l'authentication forte par OTP en utilisant Google Authenticator**

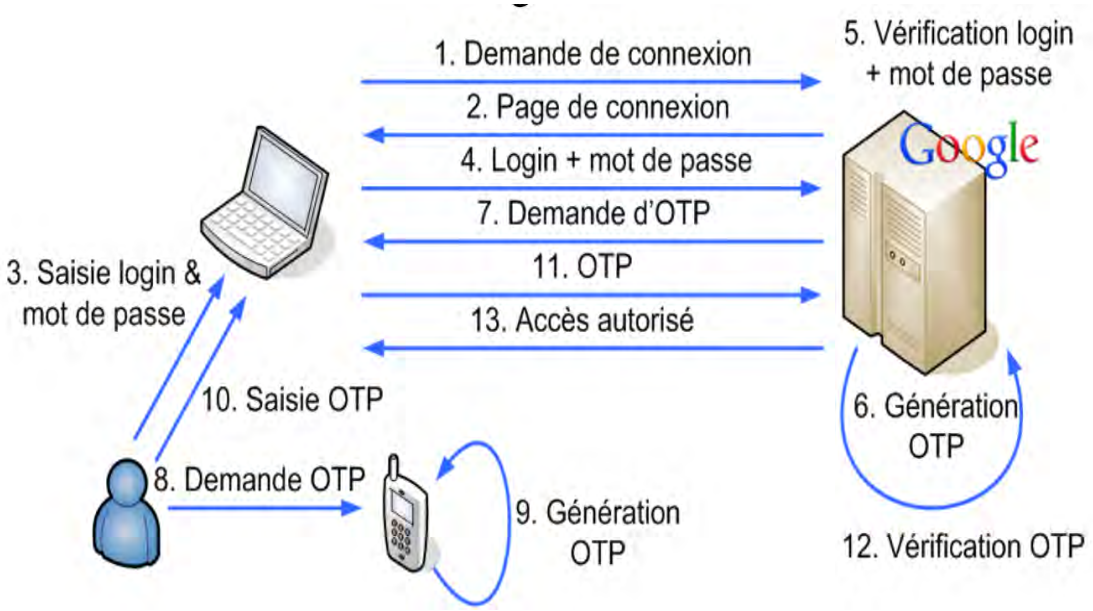


Figure.4.1.4 Architecture authentication forte par OTP avec Google Authenticator

4.2 Déploiement de l'autorité de certification

1. **Outils utilisés**

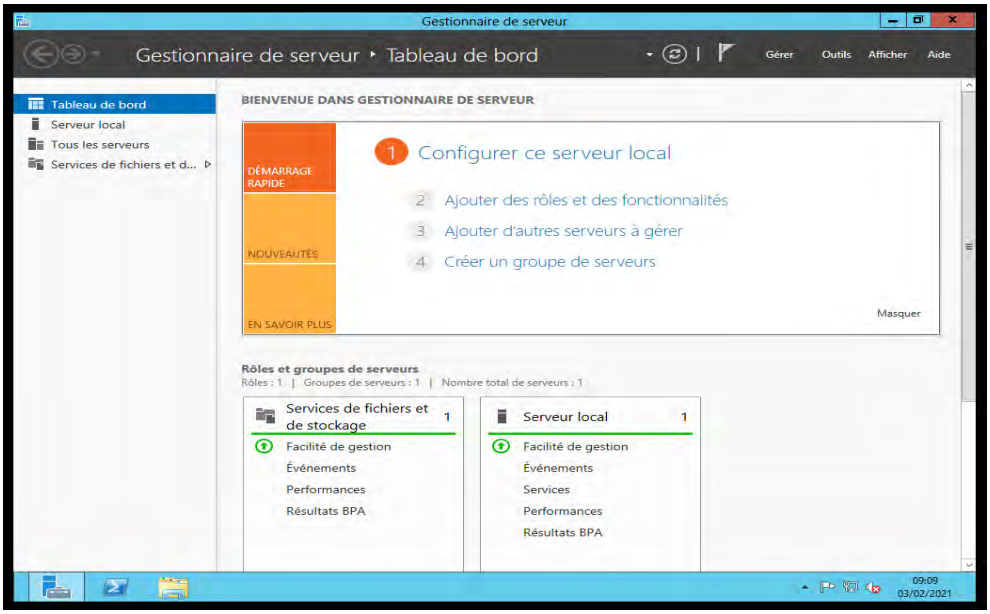
   — Windows Serveur 2012 R2 .

   — Windows 7 client .

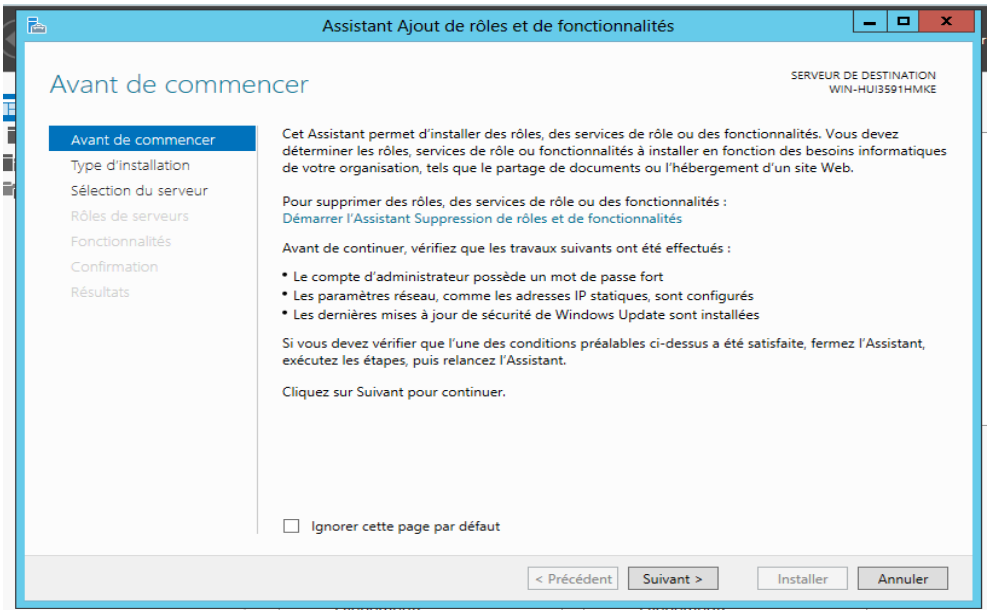
   — Ubuntu 18.04 serveur d'Application .

2. **Installation et Configuration du service Active Directory(AD DS)**

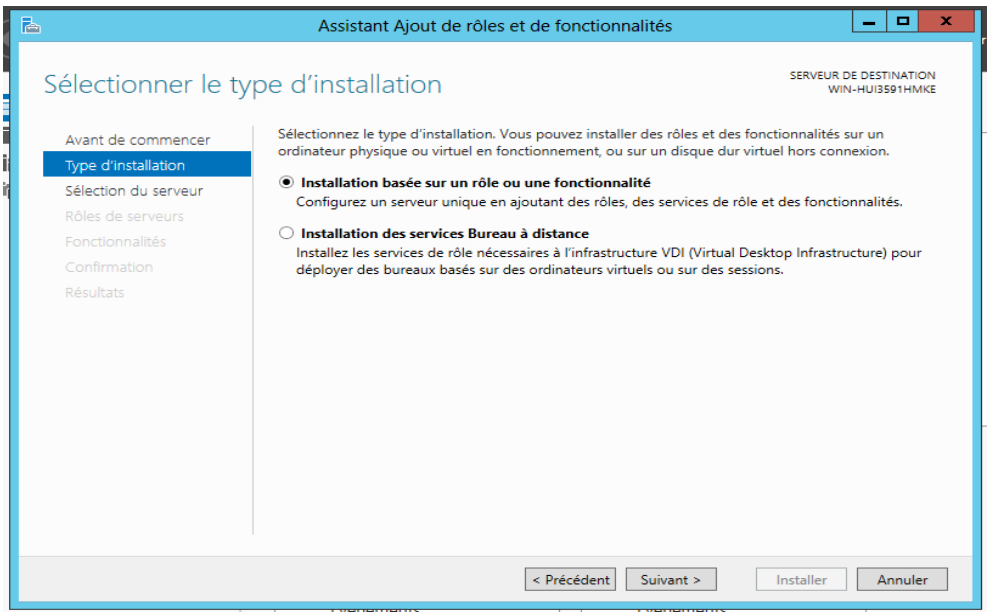
   a) Ouvrez le « Gestionnaire de serveur » et cliquer sur « Ajouter des rôles et des fonctionnalités » juste en face.



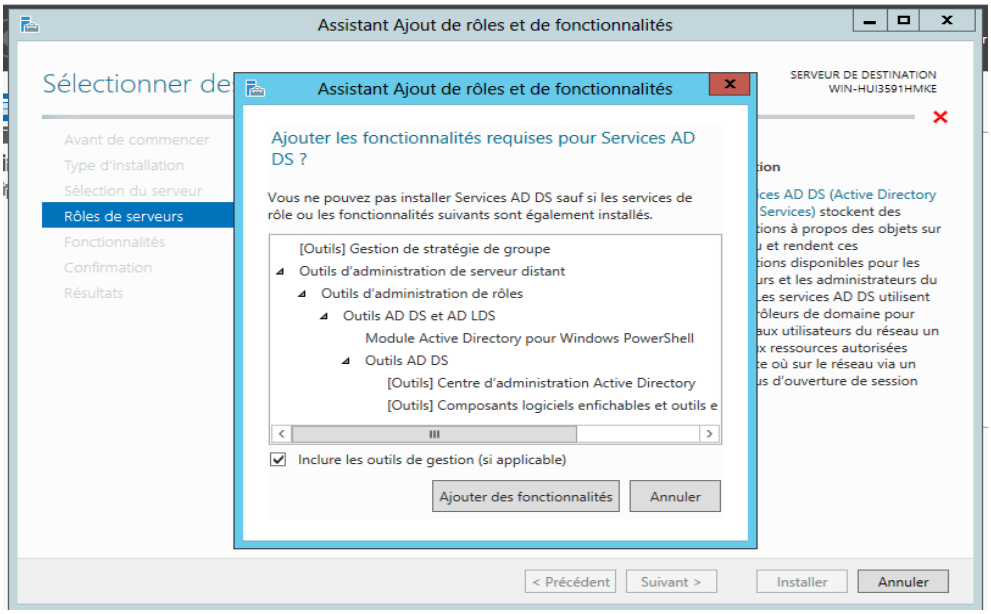
b) L'assistant s'exécute et vous demande de vous assurer que le compte Administrateur possède un mot de passe fort, que la configuration réseau est en adresse statique et que votre serveur est à jour au niveau des mises à jour de sécurité. Cliquez sur «Suivant».



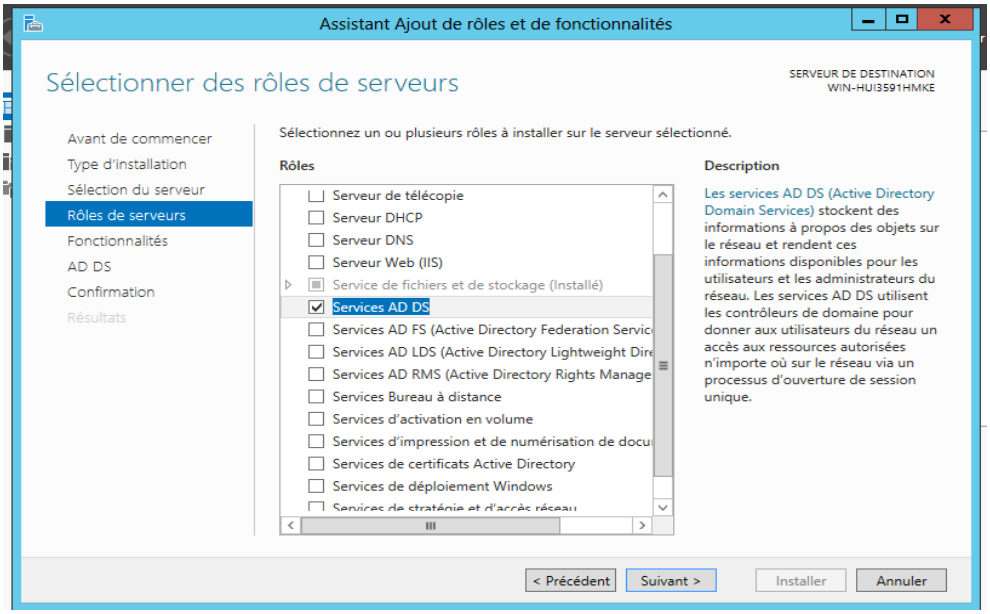
c) Laissez le choix par défaut puisque nous souhaitons ajouter un nouveau rôle à notre serveur et non installer des services de Bureau à distance comme le propose le second choix. Cliquez sur « Suivant ».



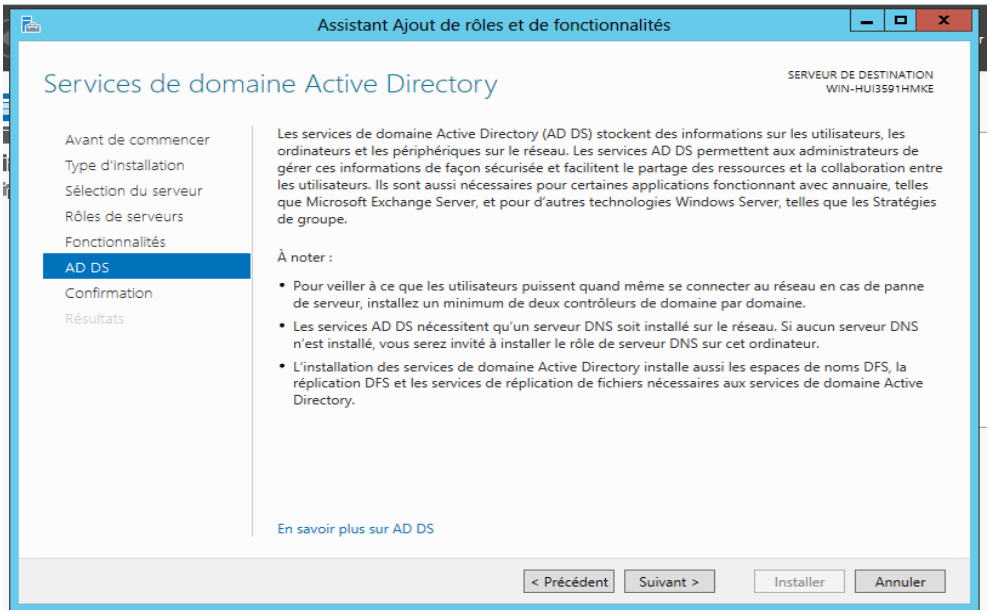
d) Au niveau des rôles, sélectionnez « Service AD DS » qui correspond au service de domaine Active Directory en cochant la case. Une fenêtre va apparaître pour vous indiquer que d'autres éléments requis par AD DS doivent être installés, cliquez sur « Ajouter des fonctionnalités ». Ensuite, cliquez sur « Suivant ».



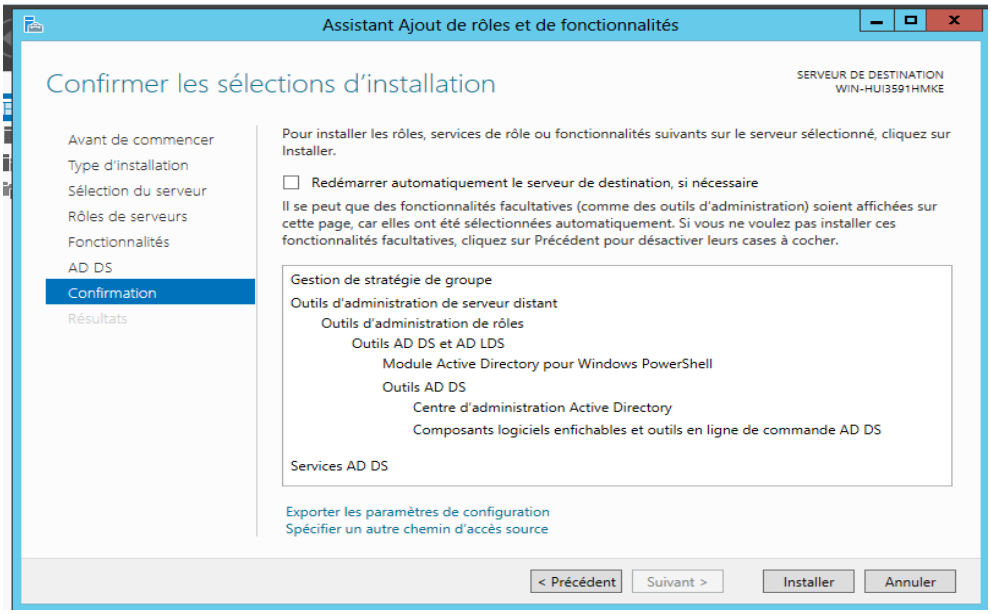
e) Cliquez sur « Suivant ».



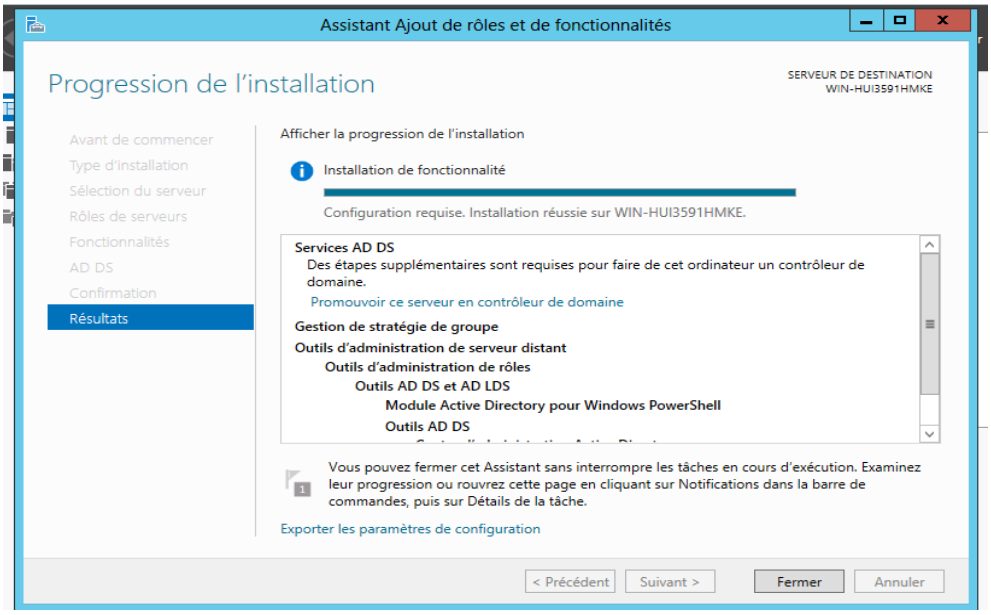
f) Lisez les informations qui s'affiche avant installation et cliquez sur « Suivant ».



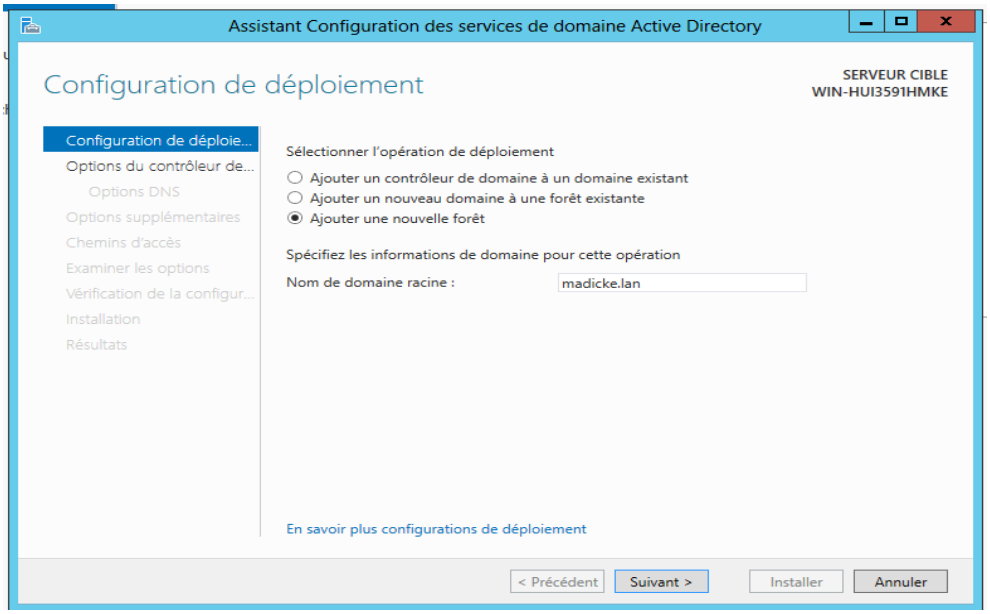
g) Cochez la case « Redémarrer automatiquement le serveur de destination, si nécessaire » et dans la fenêtre qui s'affichera cliquez sur « Oui » puis sur » Installer ».



h) Après que l'installation s'achève avec succès, cliquez sur « Promouvoir ce serveur en contrôleur de domaine ».



i) Choisissez l'option « Ajouter une nouvelle forêt » et puis taper le « Nom de domaine racine » dans mon cas (Nom de domaine racine : madicke.lan). Vu que nous souhaitons créer un nouveau domaine appelé « madicke.lan », nous devons déployer une nouvelle forêt (une forêt étant un ensemble de domaines, ce qui permet d'ajouter d'autres domaines dans cette forêt par la suite). Cochez « Ajouter une nouvelle forêt » et indiquez « madicke.lan ».

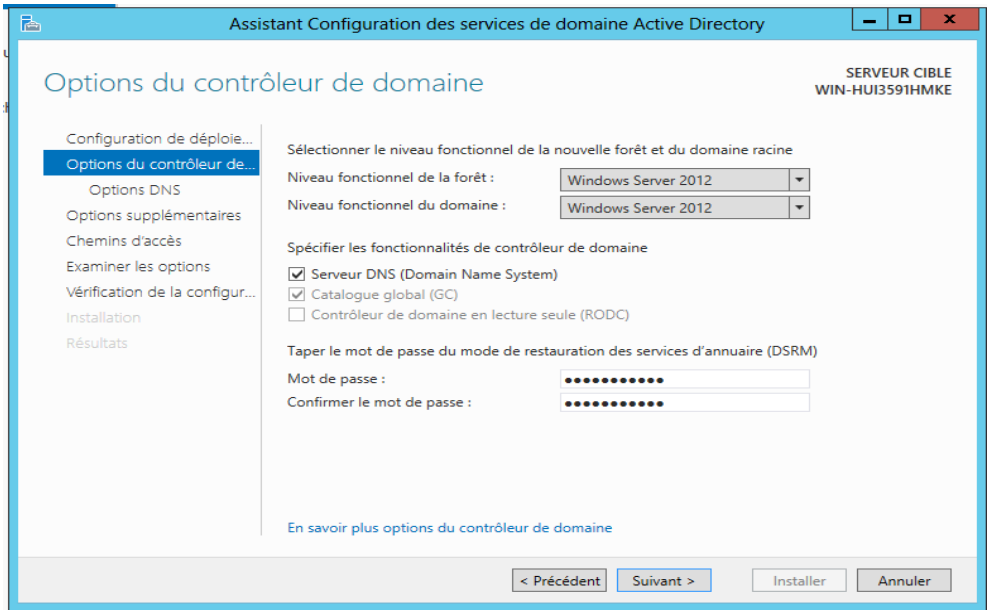


Choisissez le niveau fonctionnel qui vous convient le mieux pour la forêt. Cela dépend de ce que vous prévoyez à l'avenir, dans le cas où vous créez d'autres domaines dans cette forêt vous allez devoir adaptez le système d'exploitation embarqué par vos serveurs par rapport au niveau fonctionnel sélectionné.

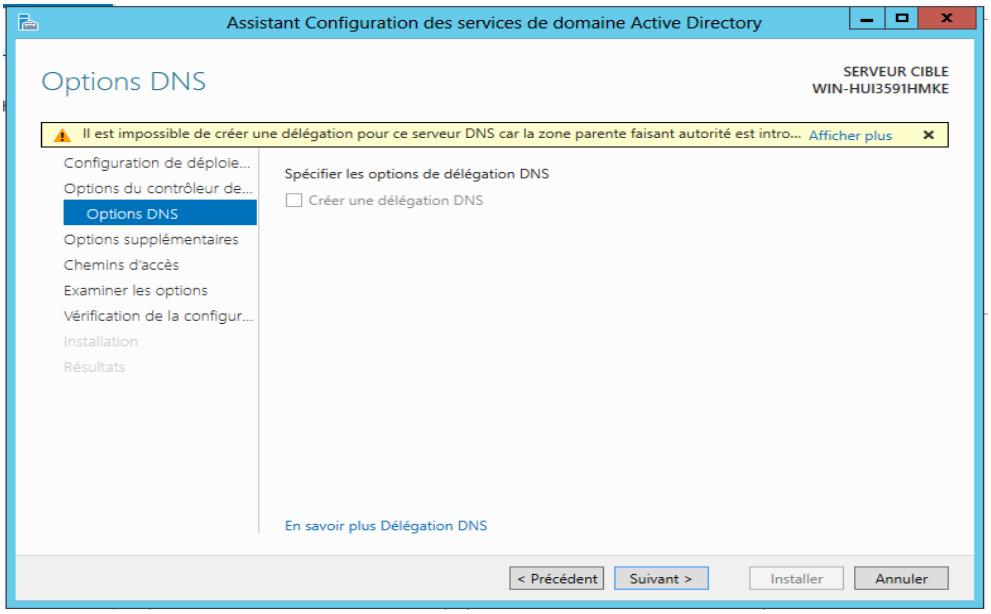
Pour information, on peut augmenter le niveau fonctionnel, mais en aucun cas le diminuer.

Pour ma part, je sélectionne « Windows Server 2012 » pour les deux niveaux fonctionnels. Laissez coché « Serveur DNS » puisque ce serveur servira également de serveur DNS sur le domaine.

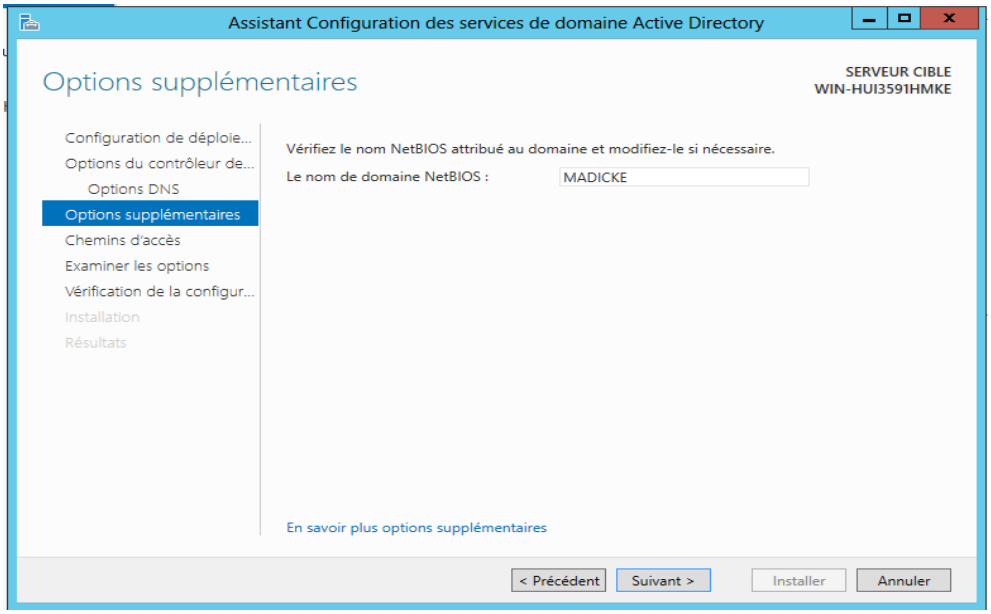
j) Sélectionnez le « Niveau fonctionnel de la forêt et celui de domaine » selon vos besoin et écrire le mot de passe de restauration des services d'annuaire en cas de panne puis cliquer sur « Suivant ».



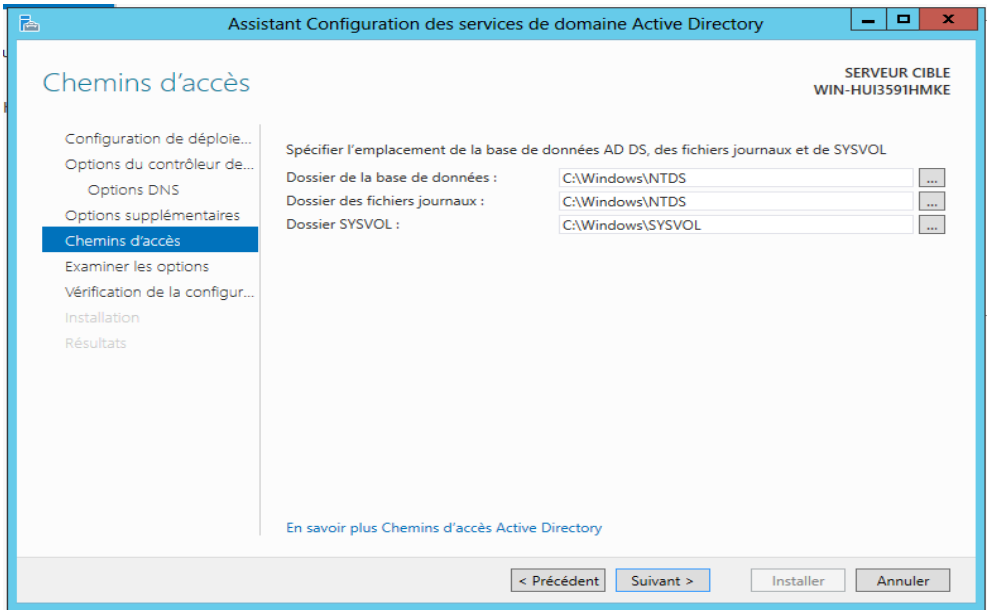
k) Cliquez sur « Suivant ».



l) Vérifiez le nom NetBIOS et cliquer sur « Suivant ».

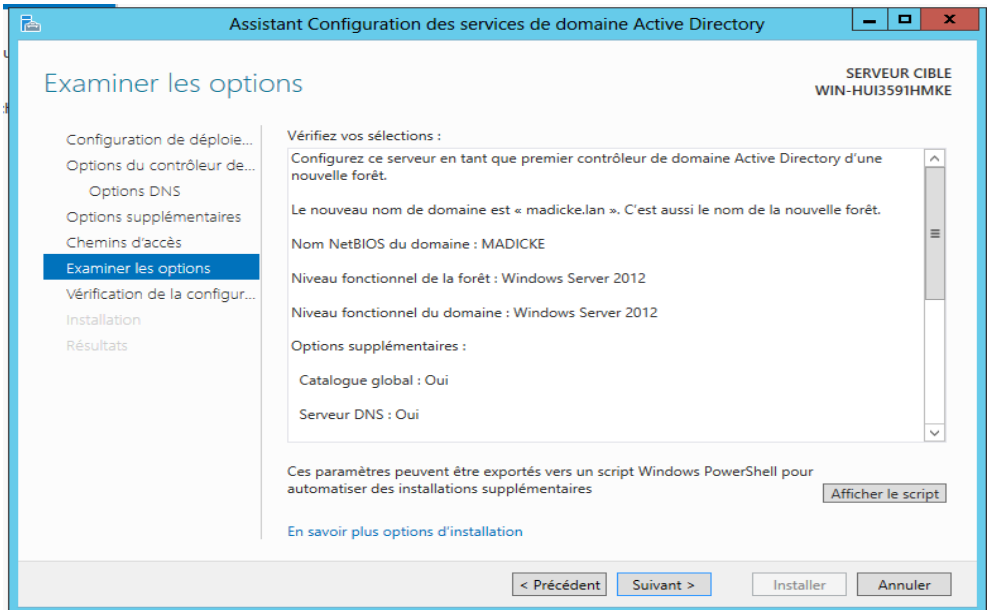


m) Vérifiez l'emplacement des fichiers des bases de données du service AD DS et cliquer sur « Suivant ».

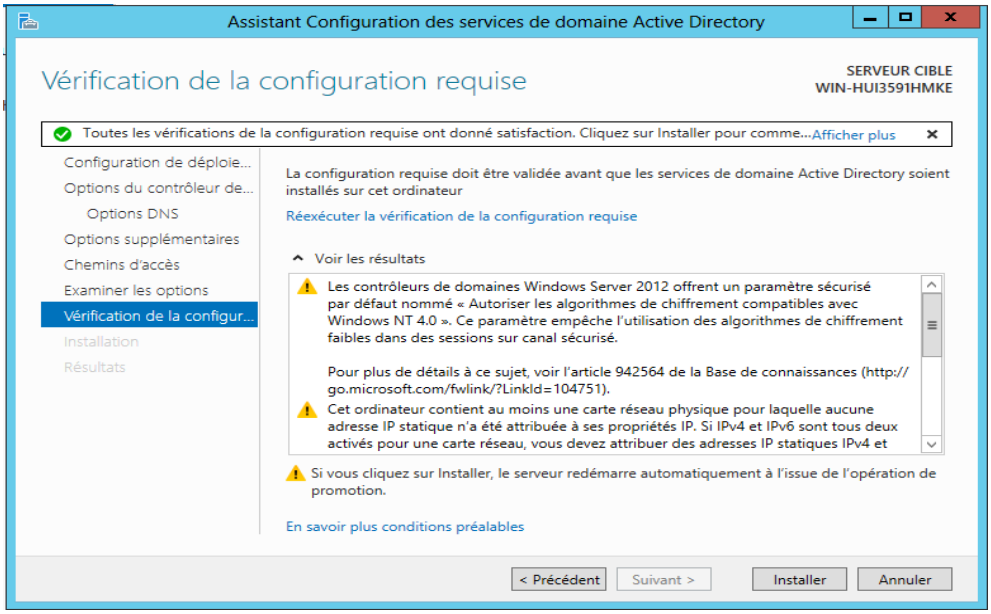


n) Cliquez sur « Suivant », puis examinez une dernière fois les options que vous avez définies dans la page récapitulative. Une fois que le tour est fait, cliquez une seconde fois sur « Suivant ».

Enfin, vérifiez qu'il n'y a pas d'erreur(s) critique(s) et cliquez sur « Installer ». Le serveur redémarrera automatiquement une fois le déploiement terminé..



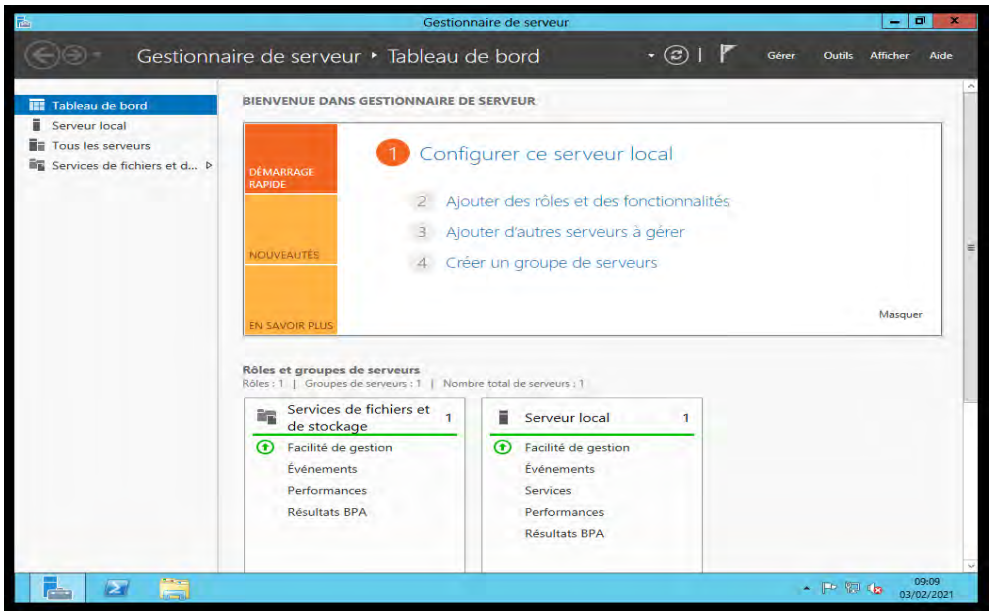
o) Cliquez sur « Suivant » puis sur « Installer ».



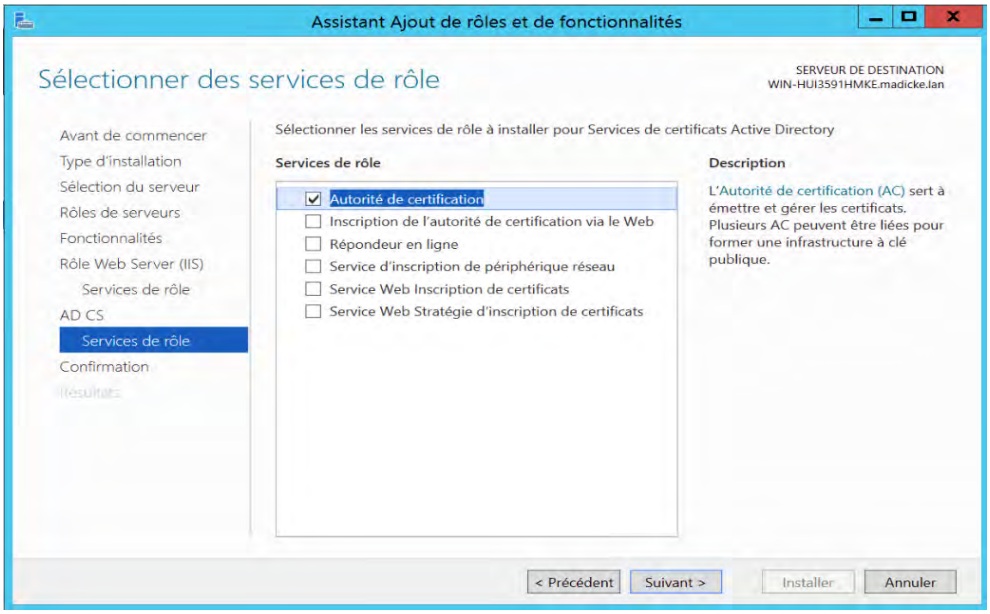
3. **Installation et Configuration du service de l'Autorité de Certification(AD CS)**

— **Installation du service de l'Autorité de Certification(AD CS)**

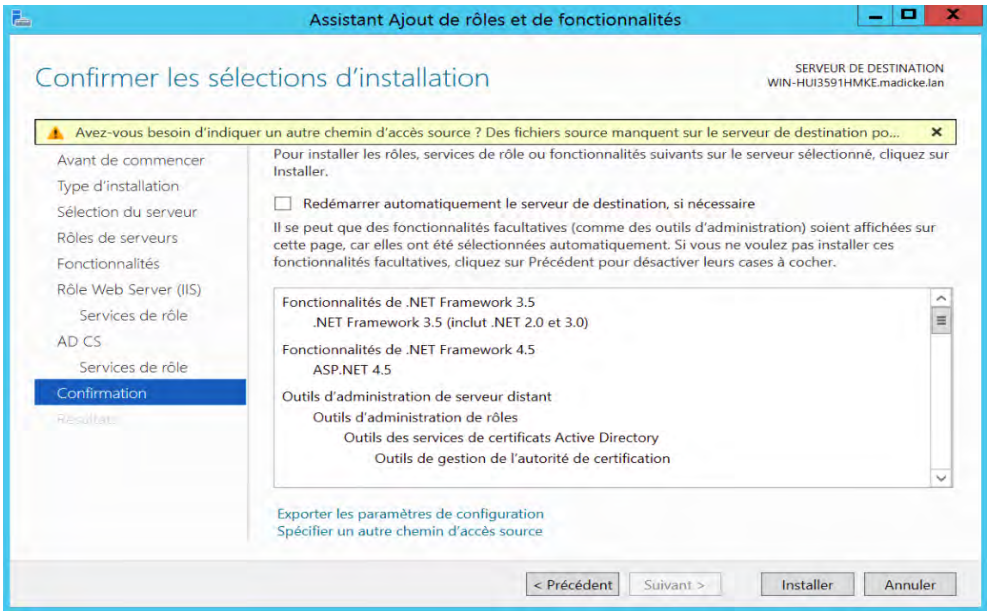
a) Sélectionner « Ajouter des rôles et des fonctionnalités ».

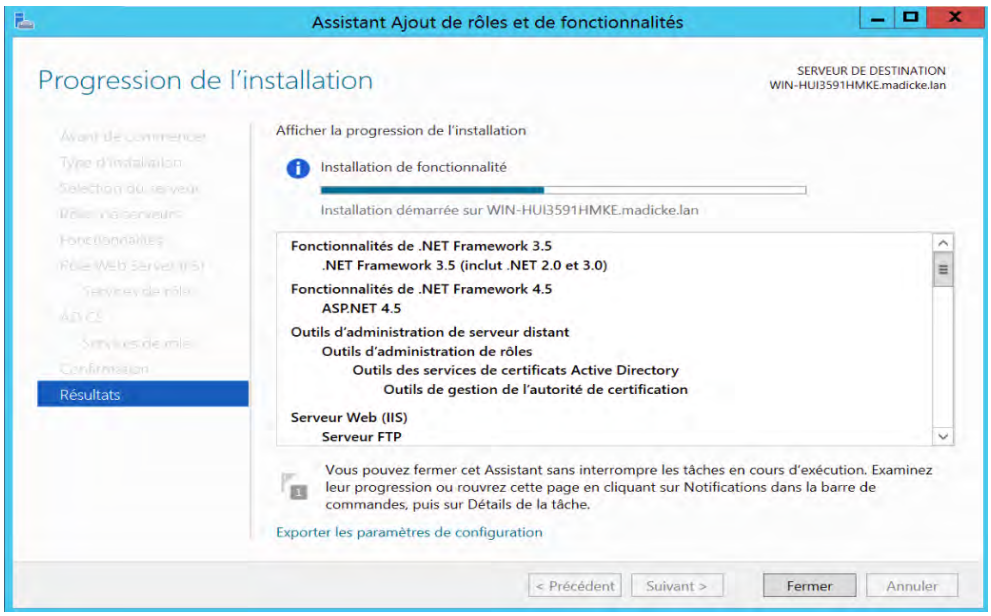


b) Cochez la case «Autorité de certification ". (Le rôle que nous souhaitons installer à AD CS (Active Directory Certificate Service)).



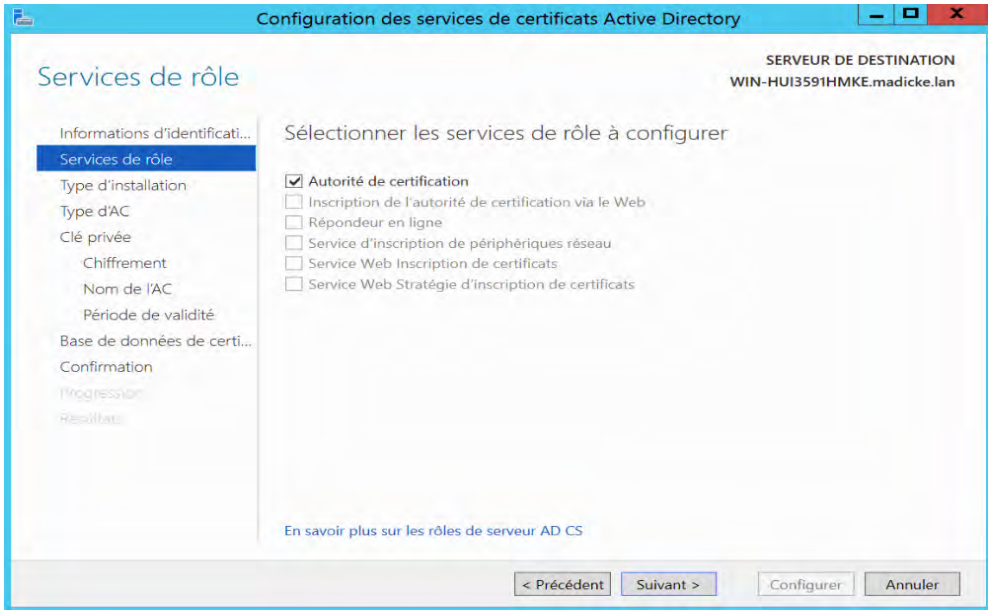
c) Et enfin cliquer sur installer.



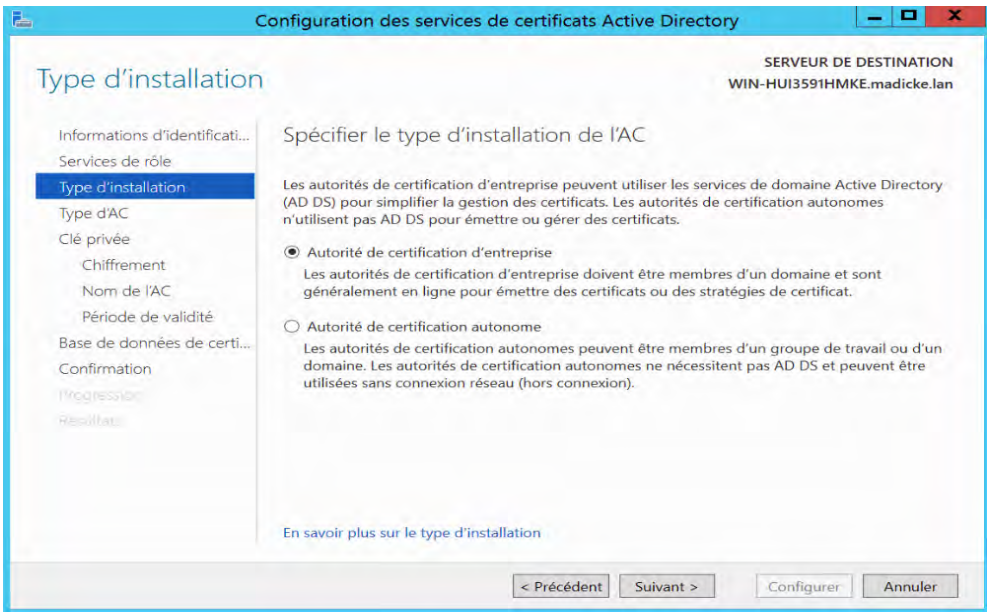


— **Configuration du service de l'Autorité de Certification(AD CS)**

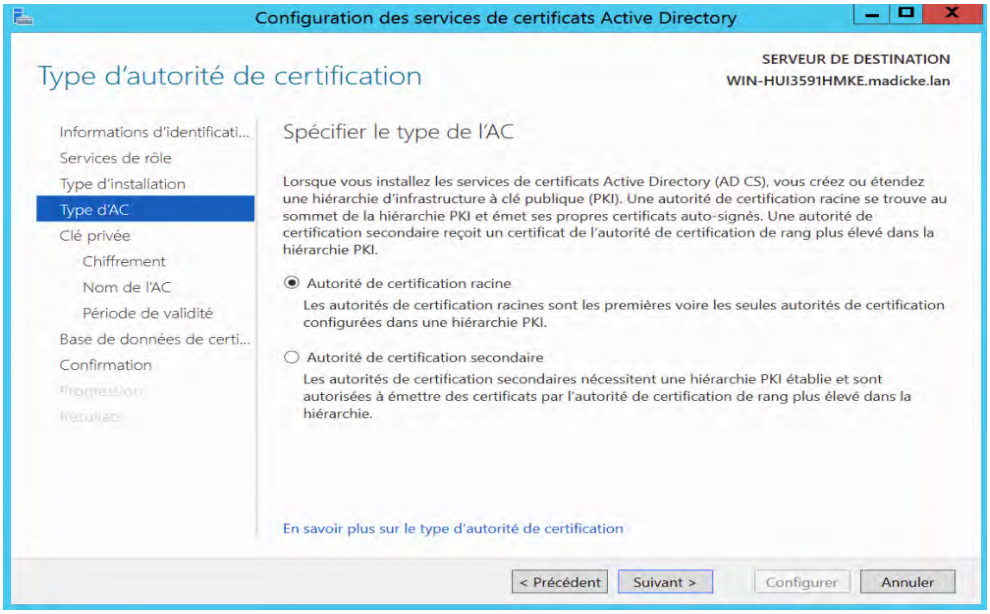
a) Sélectionner le service de role Autorité de Certification et l'installer.



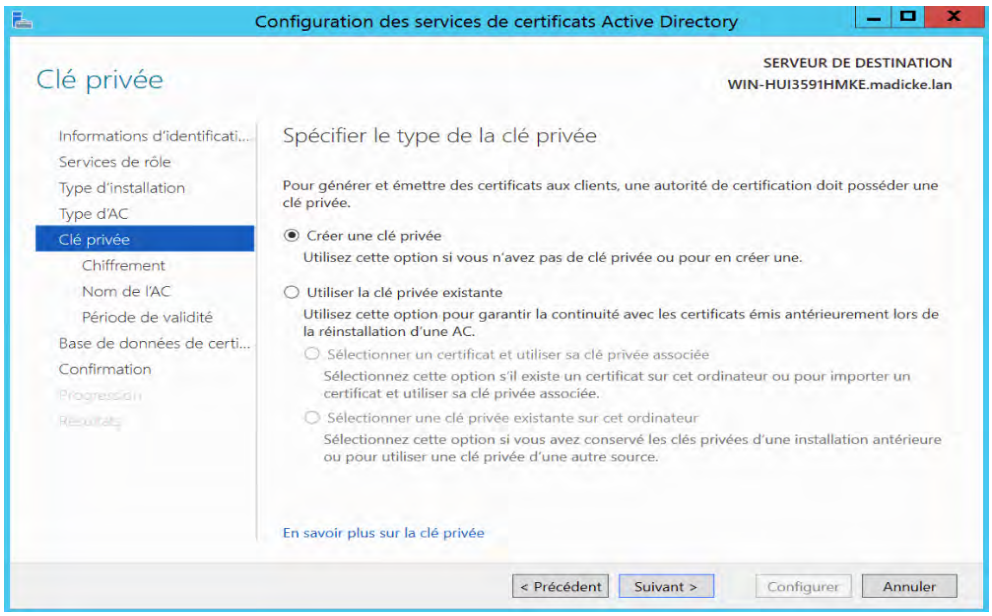
b) Spécifier le type d'installation de l'AC



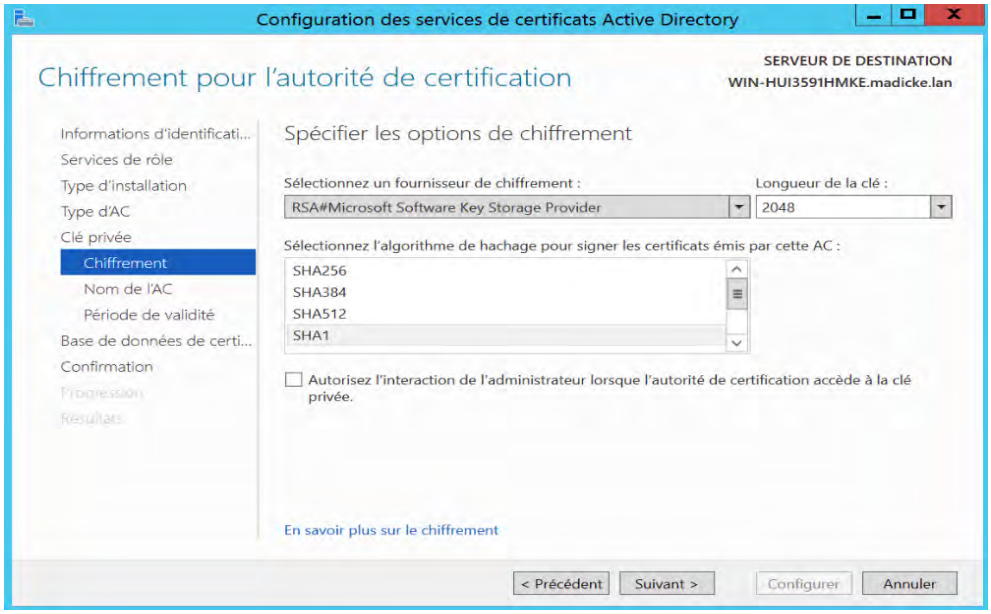
c) Spécifier le type de l'AC.



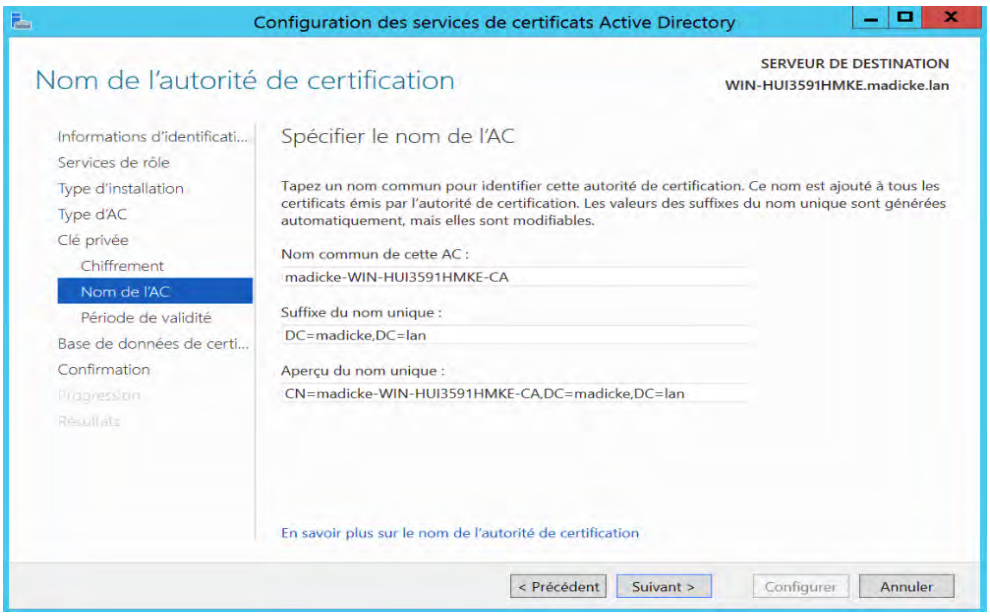
d) Spécifier le type de de la clé privée



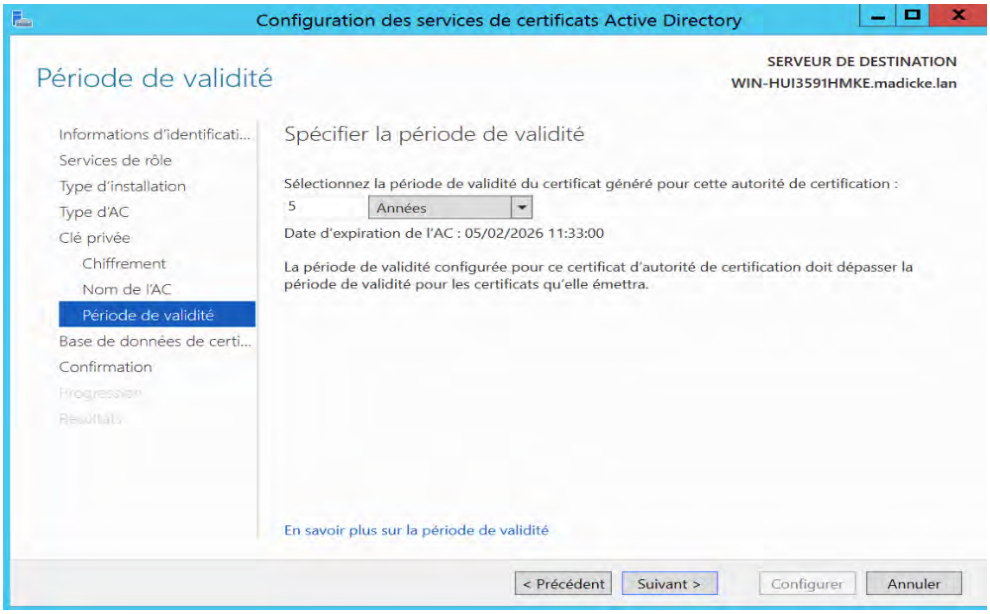
e) Spécifier les options de chiffrement



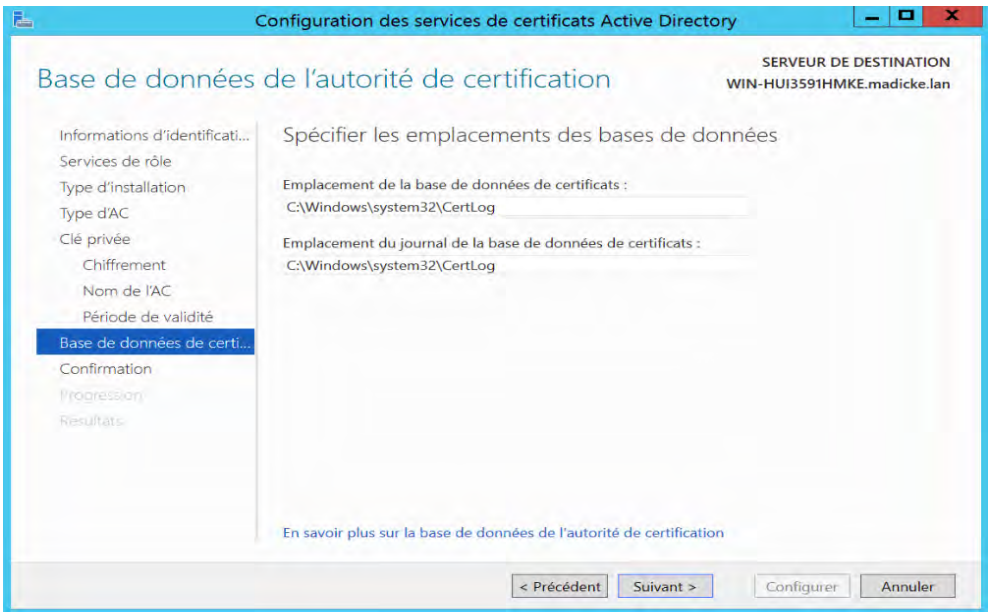
f) Spécifier le nom de l'AC



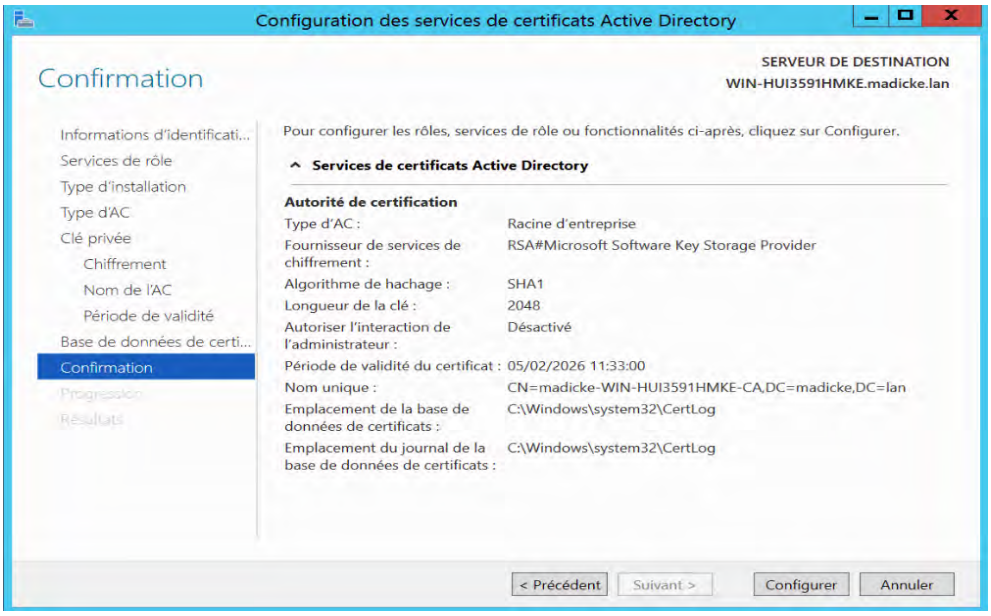
g) Spécifier la période de la validité de l'AC



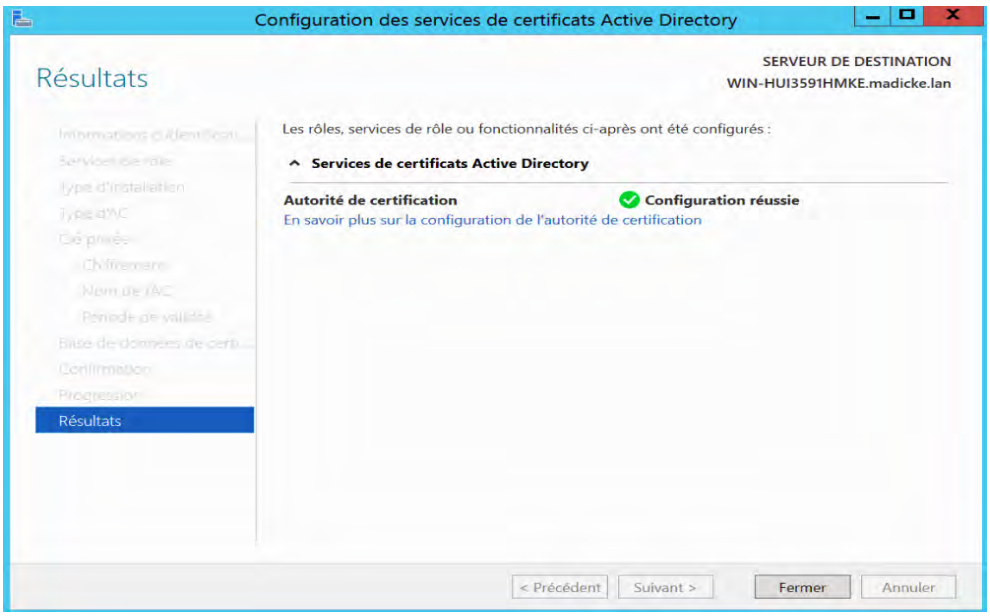
g) Spécifier les emplacements de base de données



g) Vérifier que les informations de configuration de votre autorité de certification racine sont justes, puis nous cliquons sur **Configurer**.

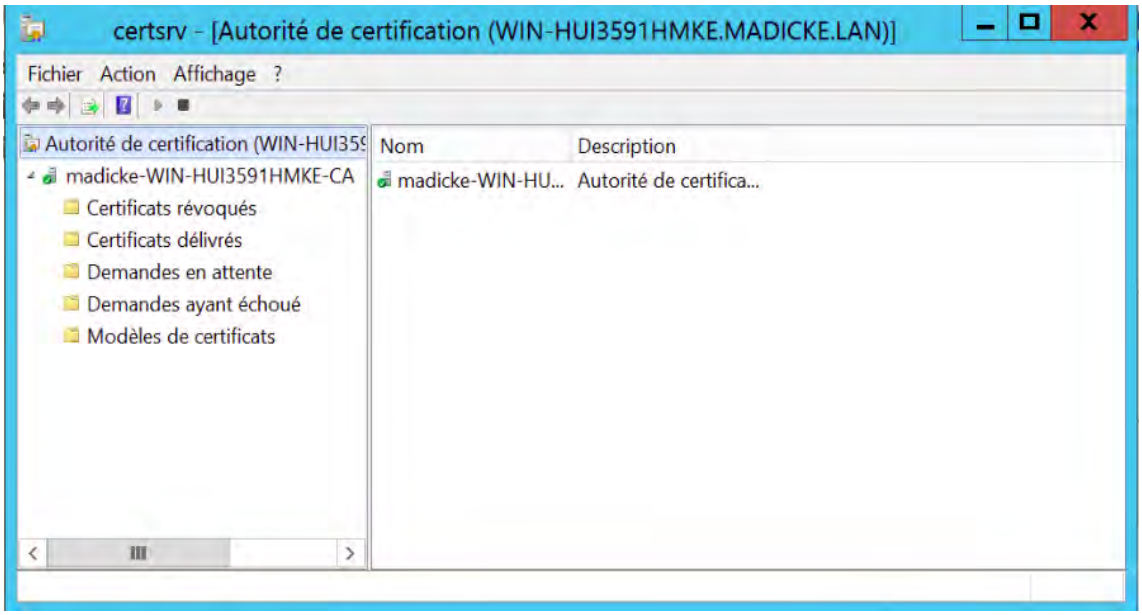


h) Assurer que notre autorité de certification affiche un état **Configuration réussie**, pour pouvoir **fermer**.



i) Administration de l'autorité de certification .

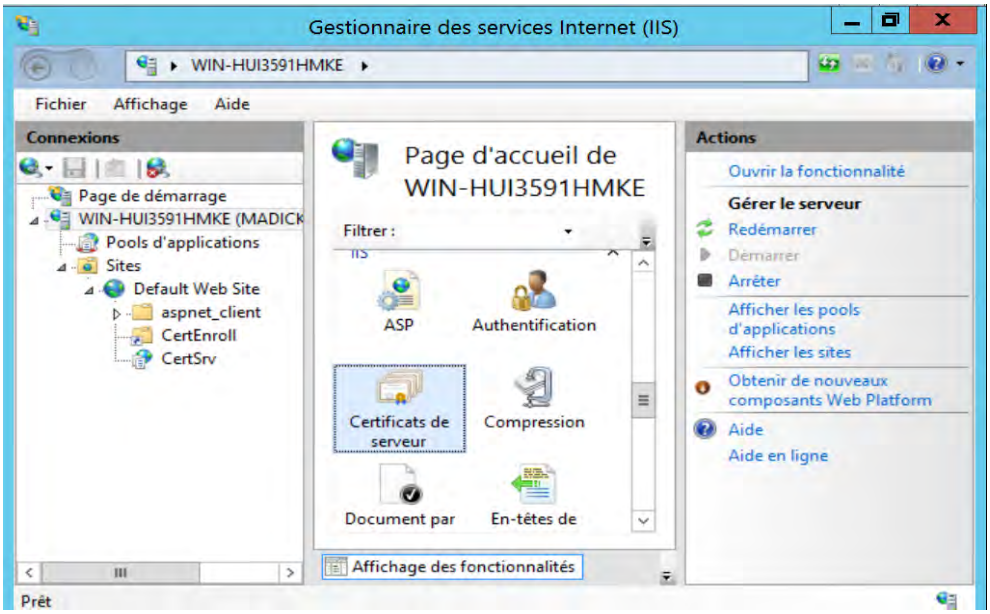
Structure de l'Autorité de Certification



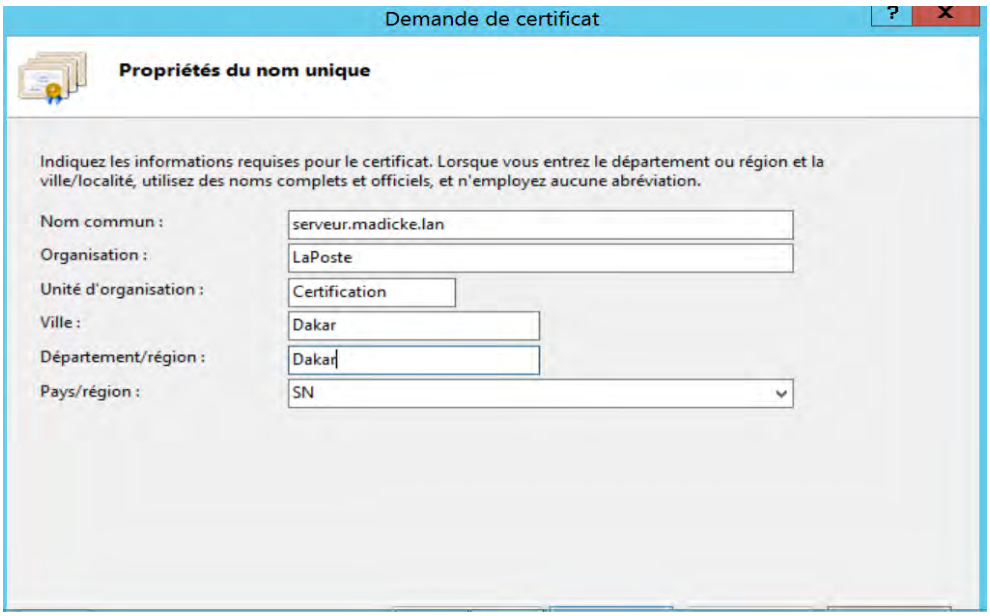
4.3 Déploiement du SSL(https) avec certificat client-serveur

1. **Création d'un certificat serveur**

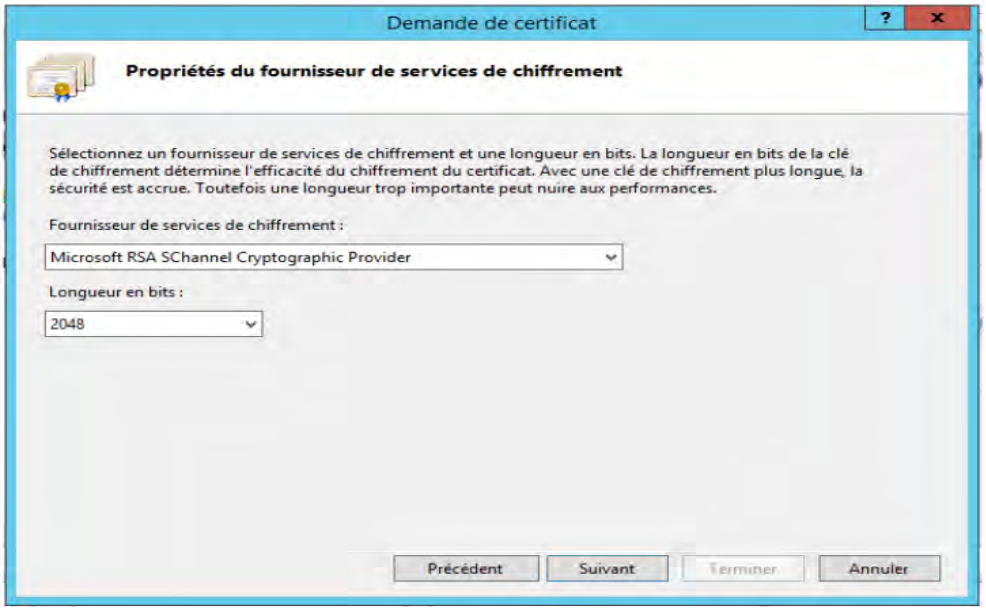
a) Cliquer sur **Certificats de serveur**.



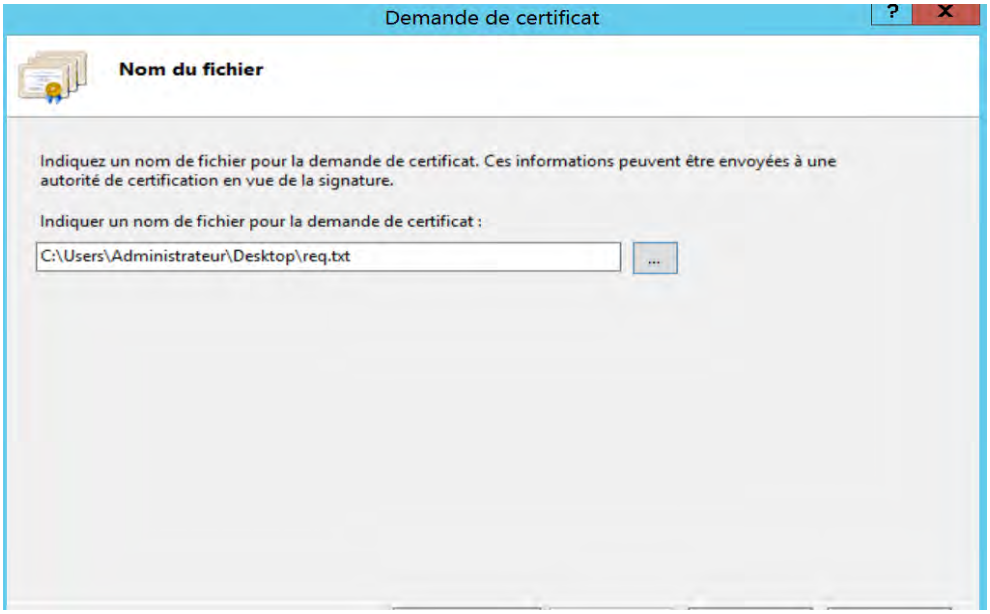
b) Entrer les informations requises pour le certificat serveur.



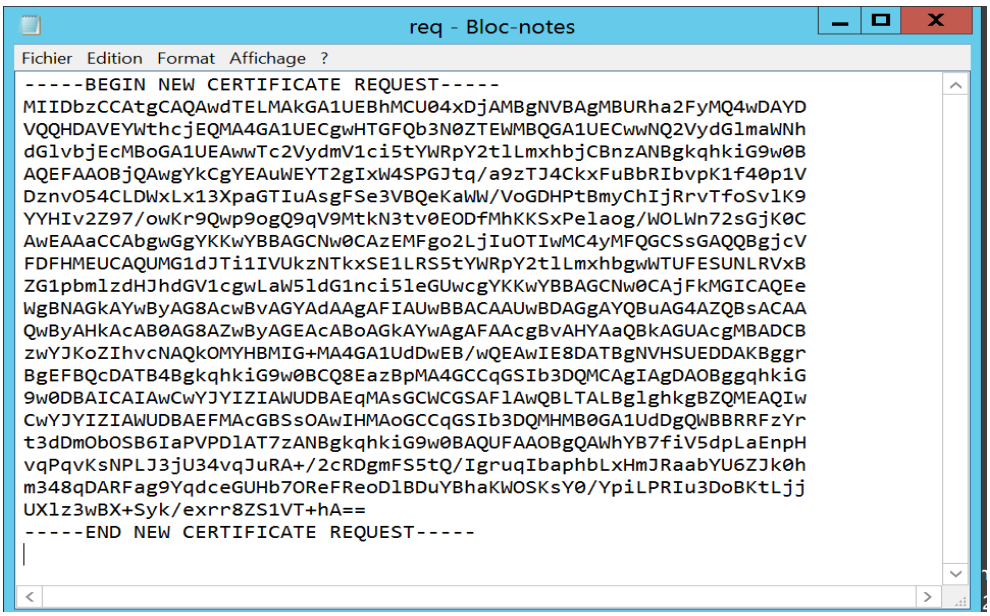
c) Sélectionner un fournisseur de services de chiffrement et la taille de la clé de chiffrement.



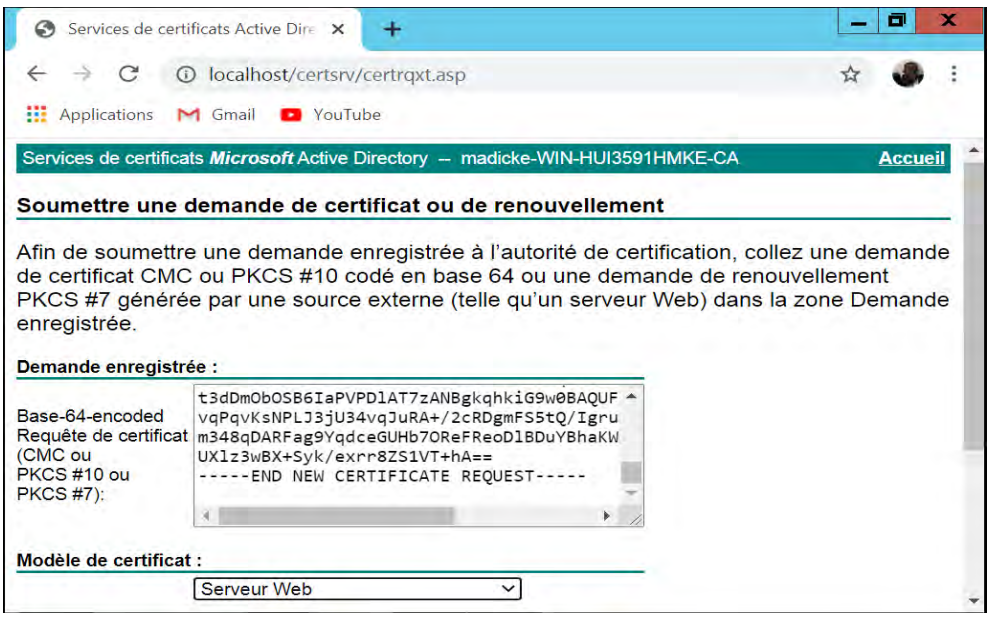
d) Indiquer un nom de fichier pour la demande de certificat.



d) Affichage de la requete de la demande.

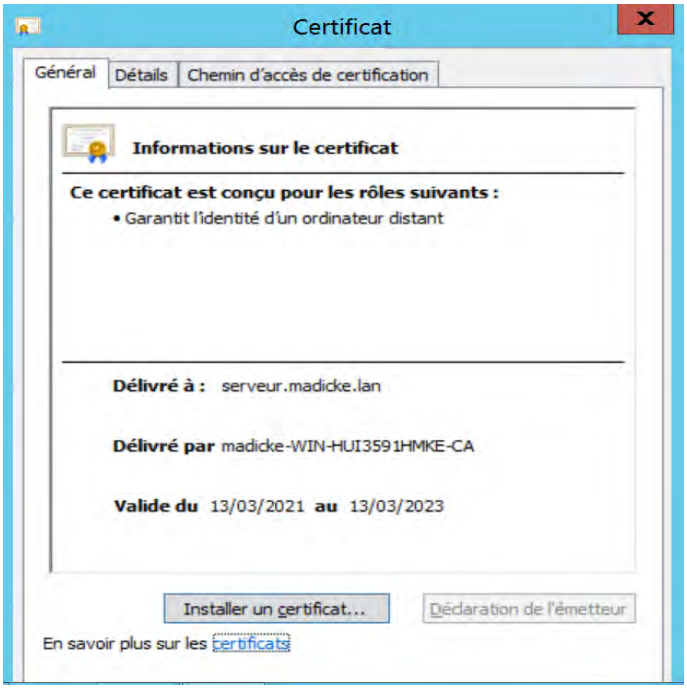


e) Soumettre la demande.

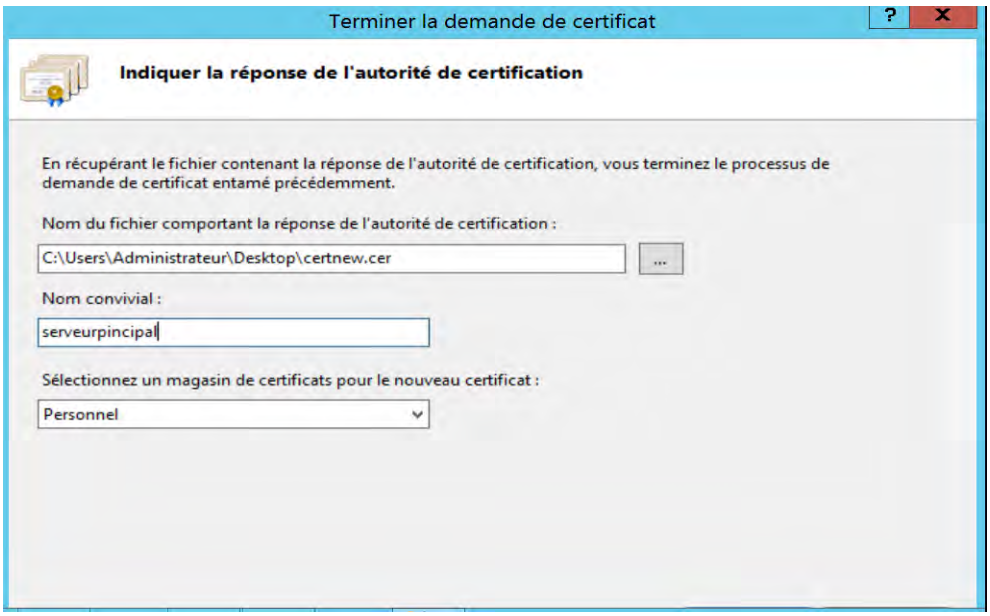


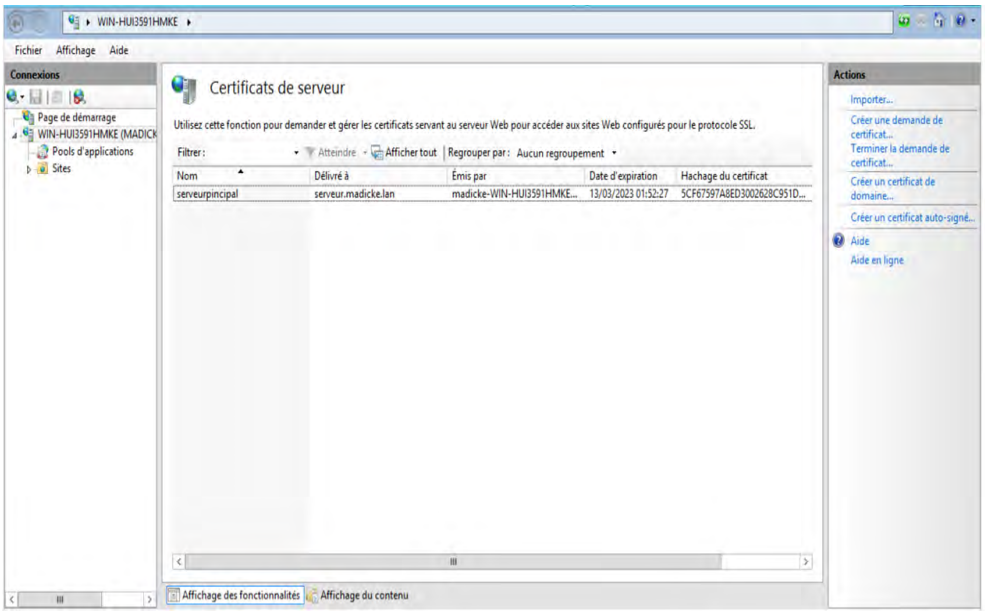
f) le certificat serveur demandé est emis.

g) Affichage du certificat serveur sans clé privé correspondant .

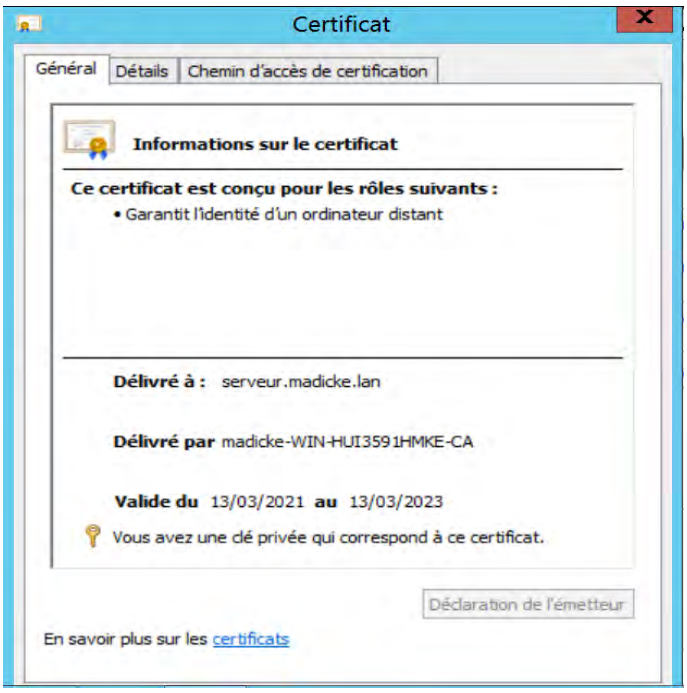


h) Termininer le processus de demande de certificat serveur .





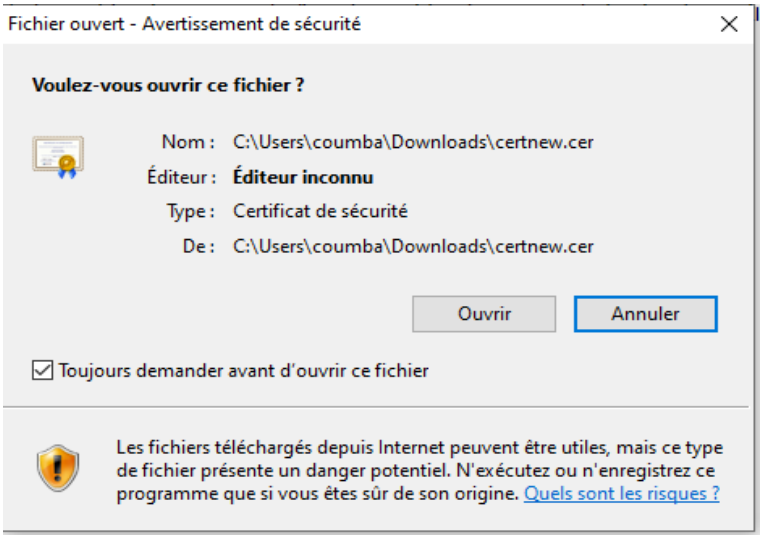
i) Affichage du certificat serveur avec clé privé correspondant et signature numérique .



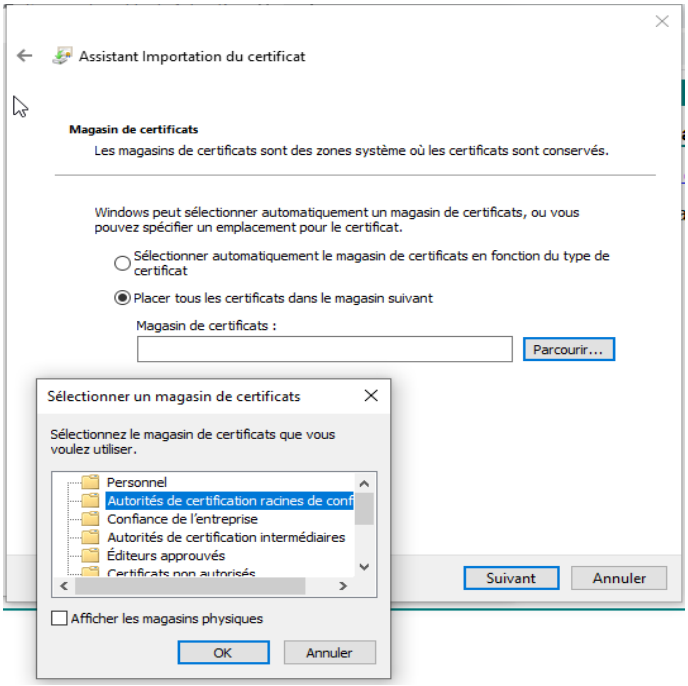
2. **Demande de certificat client au prés l'Autorité de Certification(AC) du serveur serveur**

a) Télécharger le certificat de l'Autorité de Certification(AC) du serveur.

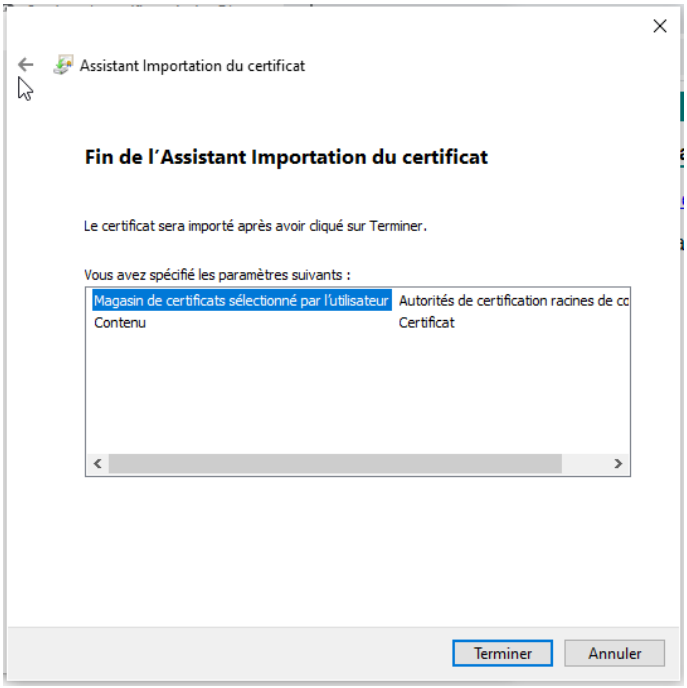
b) Ouvrir le fichier de certificat de l'Autorité de Certification(AC) du serveur.

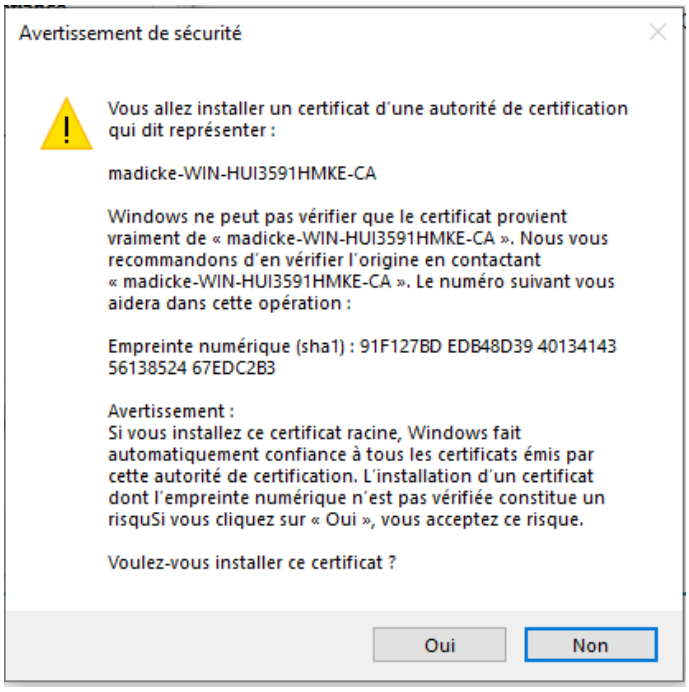


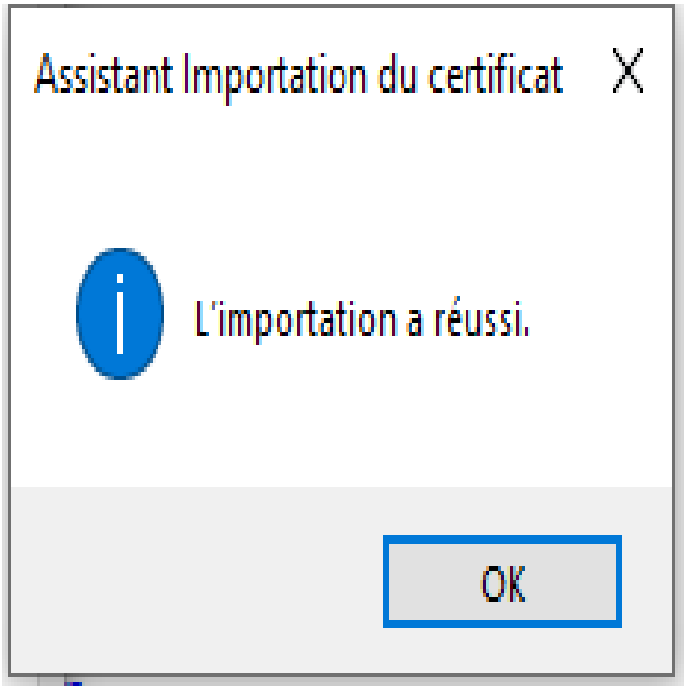
c) Ajouter le certificat de l'AC du serveur dans le magasin de l'AC racines de confiance du client.



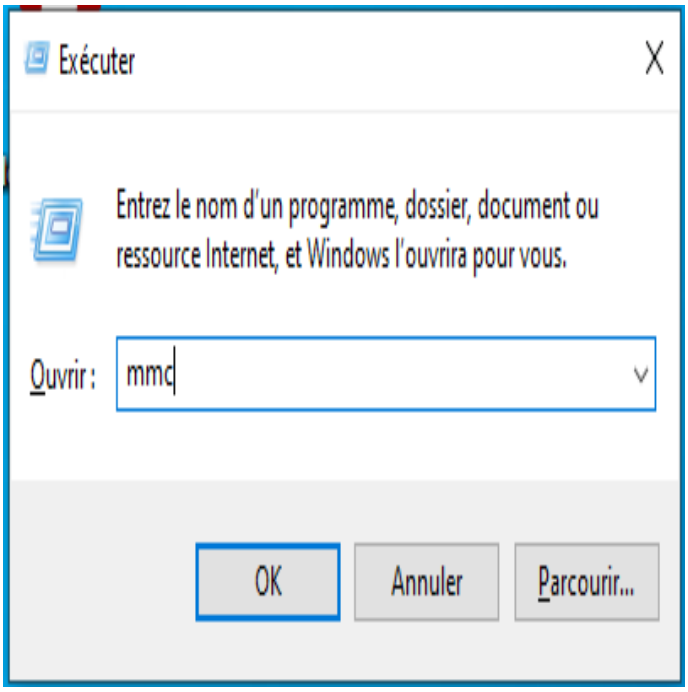
d) Fin de l'assistant d'importation du certificat serveur

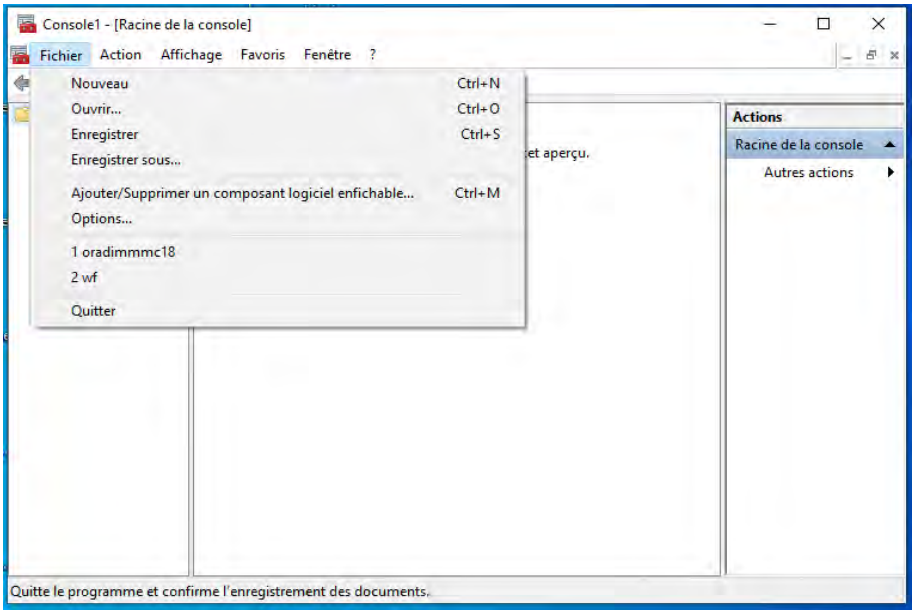

Assistant Importation du certificat
Fin de l'Assistant Importation du certificat
Le certificat sera importé après avoir cliqué sur Terminer.
Vous avez spécifié les paramètres suivants :
Magasin de certificats sélectionné par l'utilisateur
Autorités de certification racines de cc
Contenu
Certificat
Terminer
Annuler

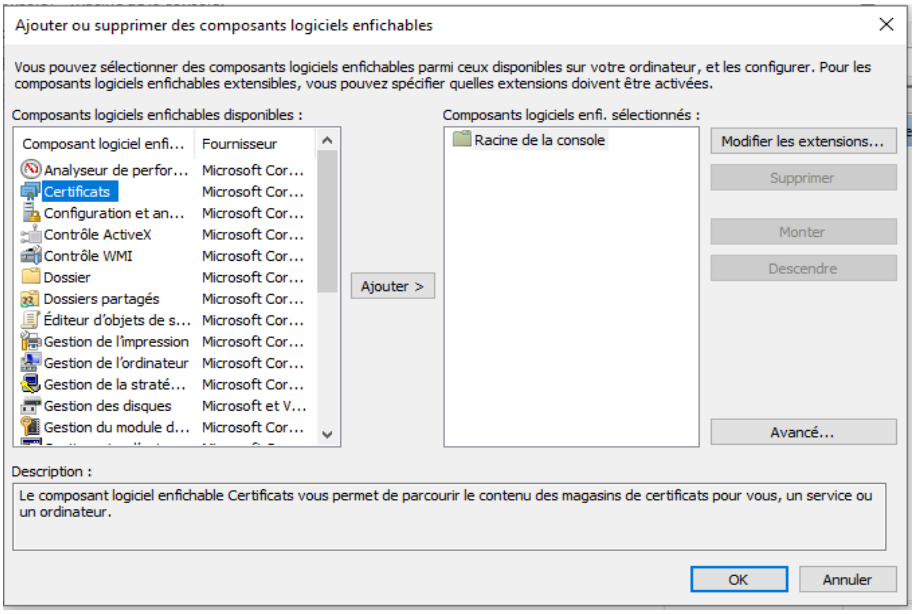

Avertissement de sécurité
Vous allez installer un certificat d'une autorité de certification qui dit représenter :
madicke-WIN-HUI3591HMKE-CA
Windows ne peut pas vérifier que le certificat provient vraiment de « madicke-WIN-HUI3591HMKE-CA ». Nous vous recommandons d'en vérifier l'origine en contactant « madicke-WIN-HUI3591HMKE-CA ». Le numéro suivant vous aidera dans cette opération :
Empreinte numérique (sha1) : 91F127BD EDB48D39 40134143 56138524 67EDC2B3
Avertissement :
Si vous installez ce certificat racine, Windows fait automatiquement confiance à tous les certificats émis par cette autorité de certification. L'installation d'un certificat dont l'empreinte numérique n'est pas vérifiée constitue un risquSi vous cliquez sur « Oui », vous acceptez ce risque.
Voulez-vous installer ce certificat ?
Oui
Non



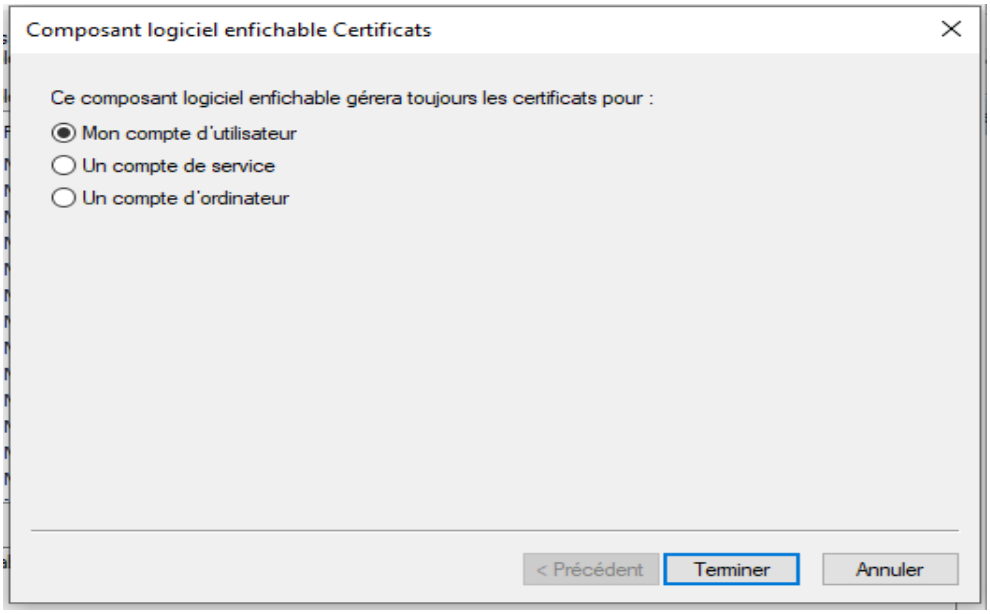
d) Installation du certficat client dans la machine du client



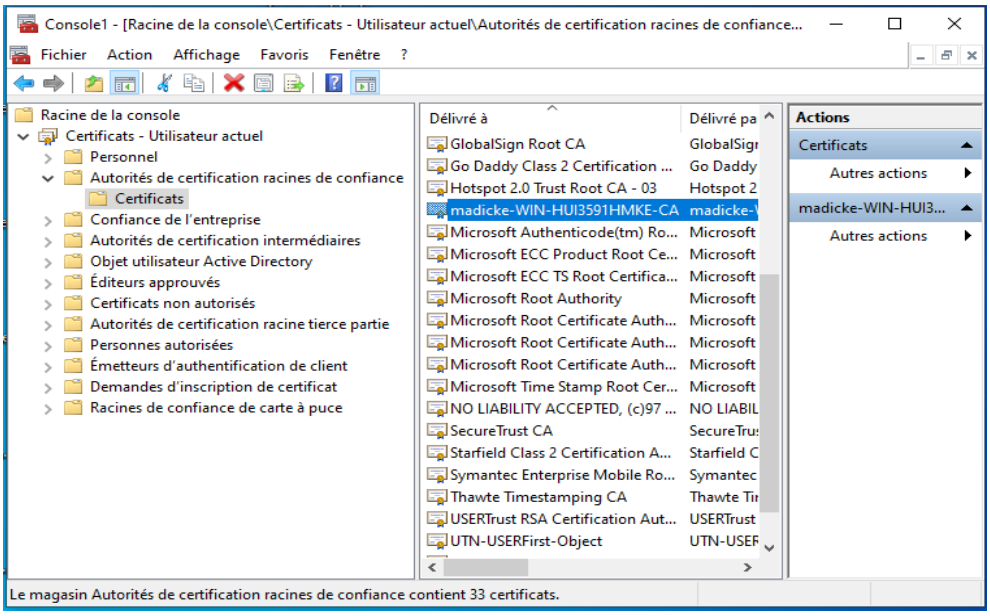




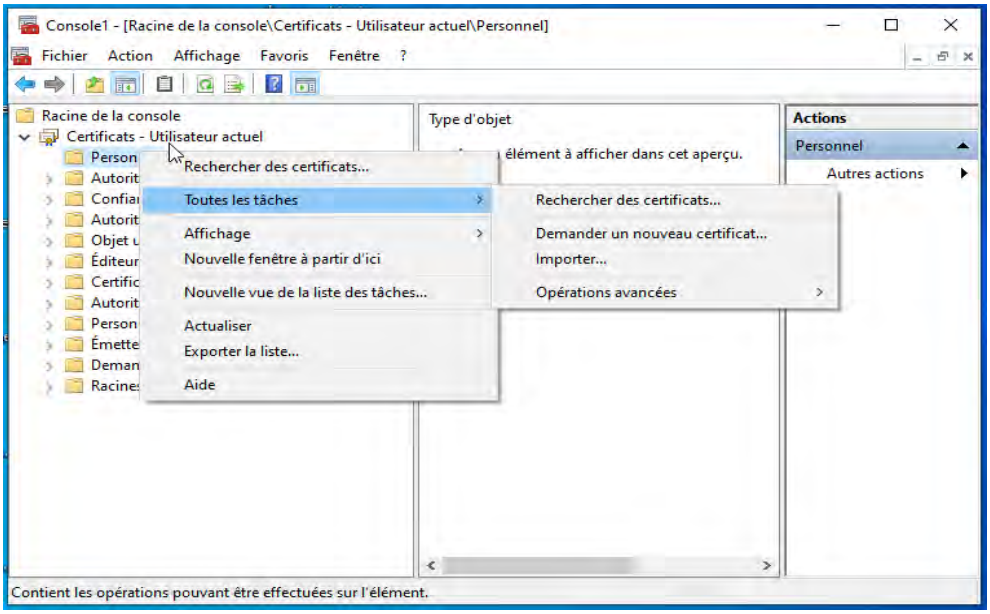
e) Choisir le type de compte pour le certficat client

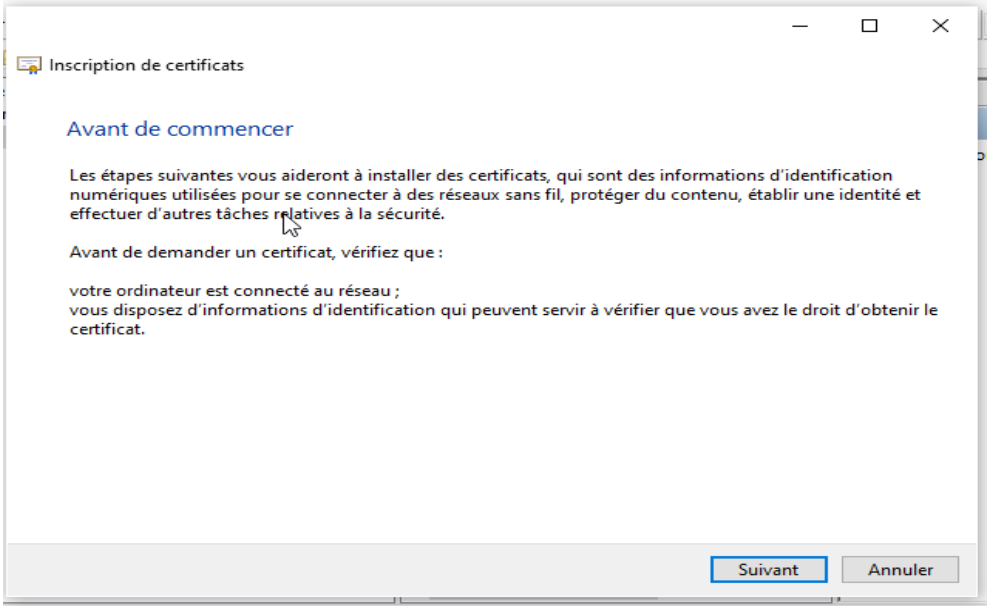


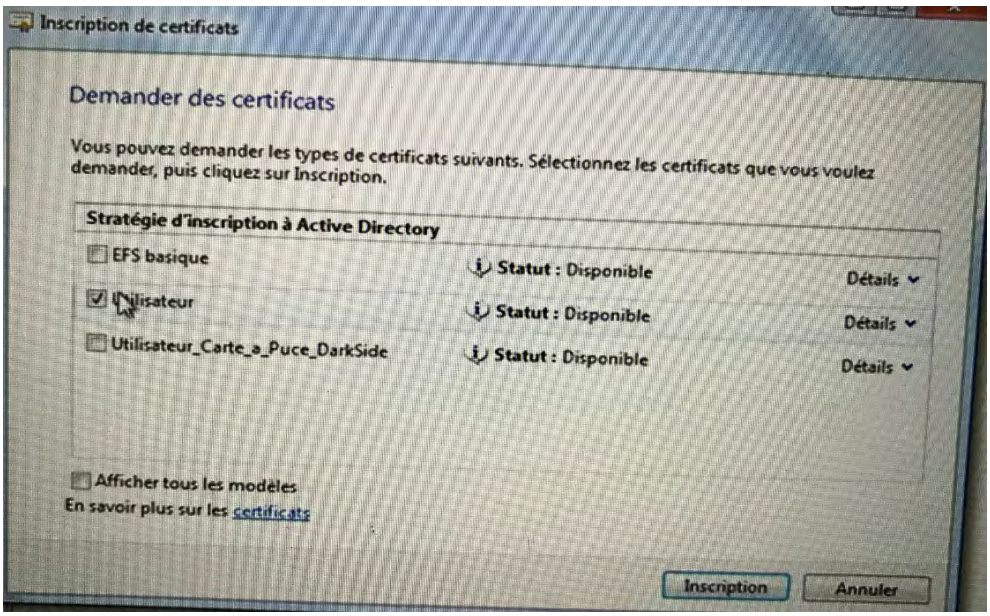
f) Verification de la présence l'AC du serveur dans le magasin de l'AC racines de confiance du client.



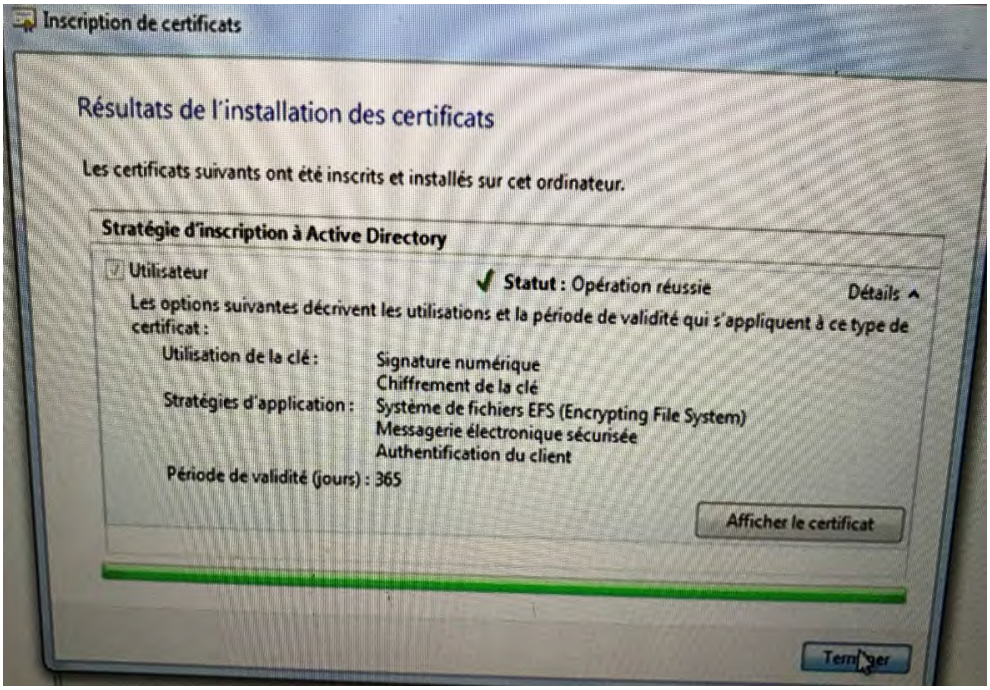
g) Etapes de l'installation du certficat client dans la machine cliente


Console1 - [Racine de la console\Certificats - Utilisateur actuel\Personnel]
Fichier Action Affichage Favoris Fenêtre ?
Racine de la console
Certificats - Utilisateur actuel
Type d'objet
Actions
Personnel
Autres actions
Rechercher des certificats...
Toutes les tâches
Affichage
Nouvelle fenêtre à partir d'ici
Nouvelle vue de la liste des tâches...
Actualiser
Exporter la liste...
Aide
Rechercher des certificats...
Demander un nouveau certificat...
Importer...
Opérations avancées
Contient les opérations pouvant être effectuées sur l'élément.


Inscription de certificats
Avant de commencer
Les étapes suivantes vous aideront à installer des certificats, qui sont des informations d'identification numériques utilisées pour se connecter à des réseaux sans fil, protéger du contenu, établir une identité et effectuer d'autres tâches relatives à la sécurité.
Avant de demander un certificat, vérifiez que :
votre ordinateur est connecté au réseau ;
vous disposez d'informations d'identification qui peuvent servir à vérifier que vous avez le droit d'obtenir le certificat.
Suivant
Annuler

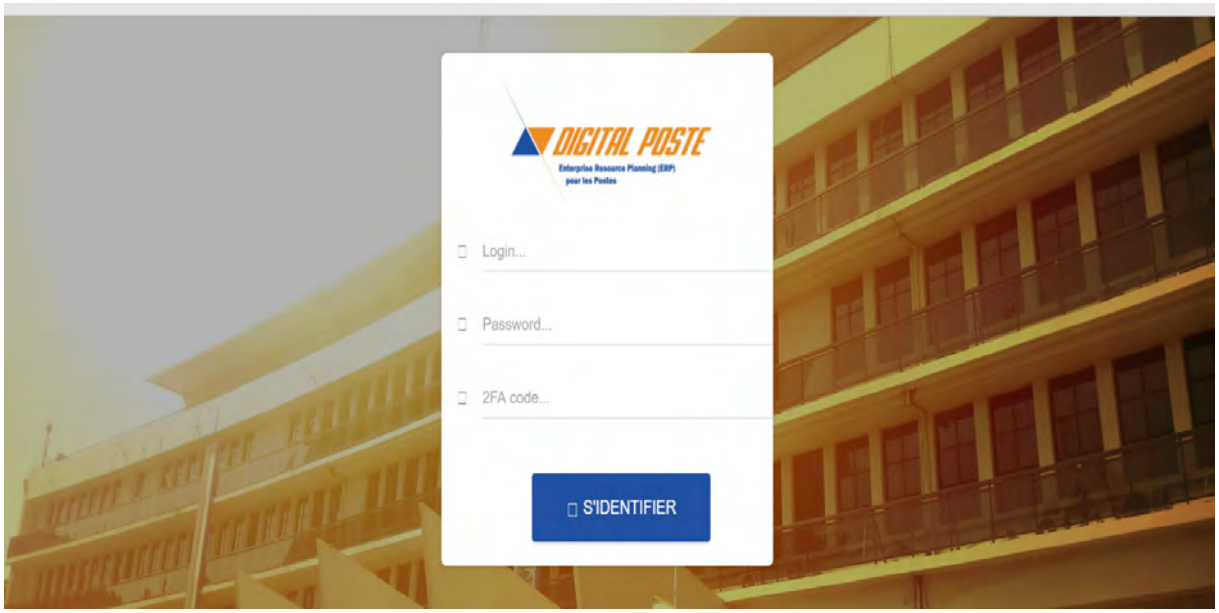


g) Fin et resultat de l'installation du certficat client dans la machine cliente



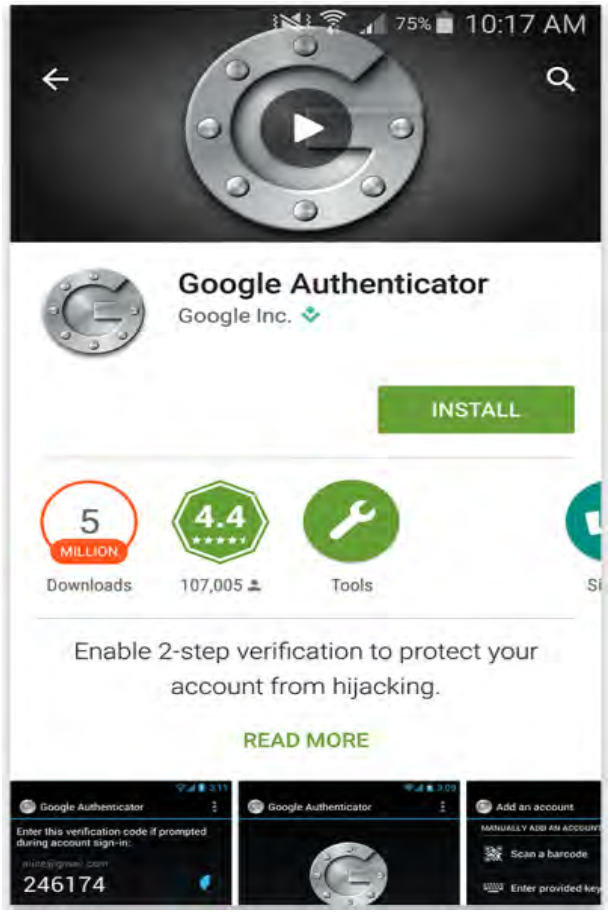
3. **Déploiement de l'authentification forte OTP(One-Time Password) sur l'application DigitalPost**

a) Ajout du second facteur d'authentification **2FA code** dans la page d'Authentication de l'application DigitalPost



b) Génération d'un second facteur d'authentification basé sur le temps à partir du software token(logiciel de génération de mot de passe à usage unique) Google Authenticator installé sur notre téléphone portable.

D'abord chaque agent de l'entreprise LaPoste ayant un compte sur l'application DigitalPost installe sur son téléphone portable le software token Google Authenticator ci-dessous :

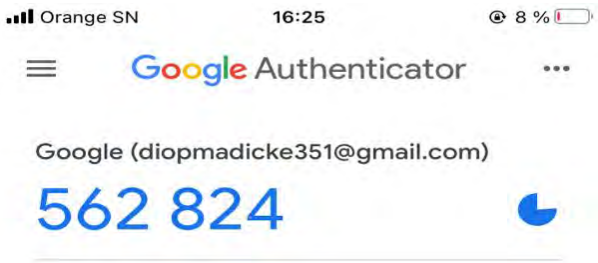


Software token Google Authenticator source :[17]

Ensuite on synchronise ces comptes stockés dans l'appication DigitalPost avec Google Authenticator. Cette synchronisation se faite à travers des algorithmes appliqués sur l'application DigitalPost et des OTP générés par Google Authenticator.

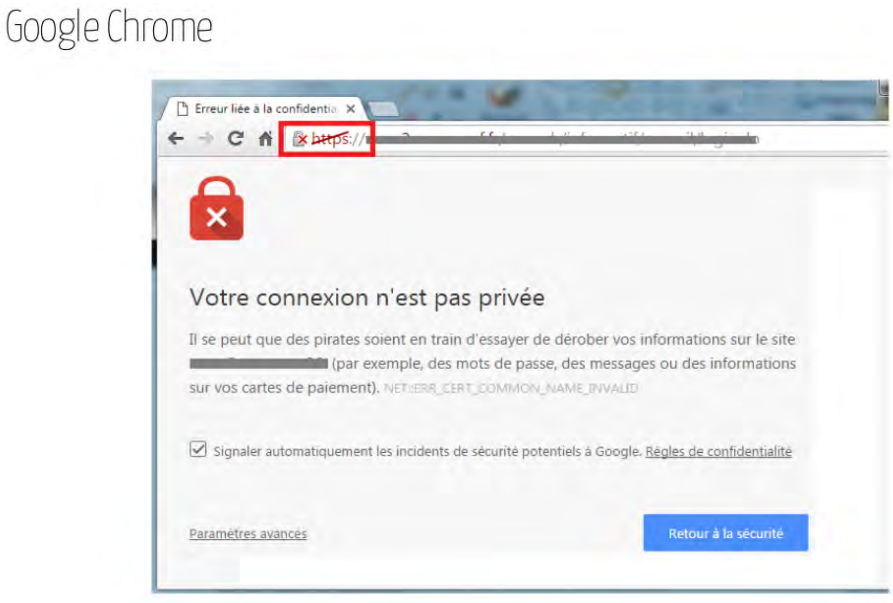
Après la synchronisation des deux applications, chaque agent voulant acceder aux ressources ou services de l'appication DigitalPost ouvre Google Authenticator et génére un OTP(mot de passe à usage unique) à 6 chiffres, aprés avoir indiquer ses identifiants(login + password).

Ce OTP a une durée de vie de 30 secondes. Donc un nouveau OTP sera généré toutes les 30 secondes comme le montre la figure ci-dessous :

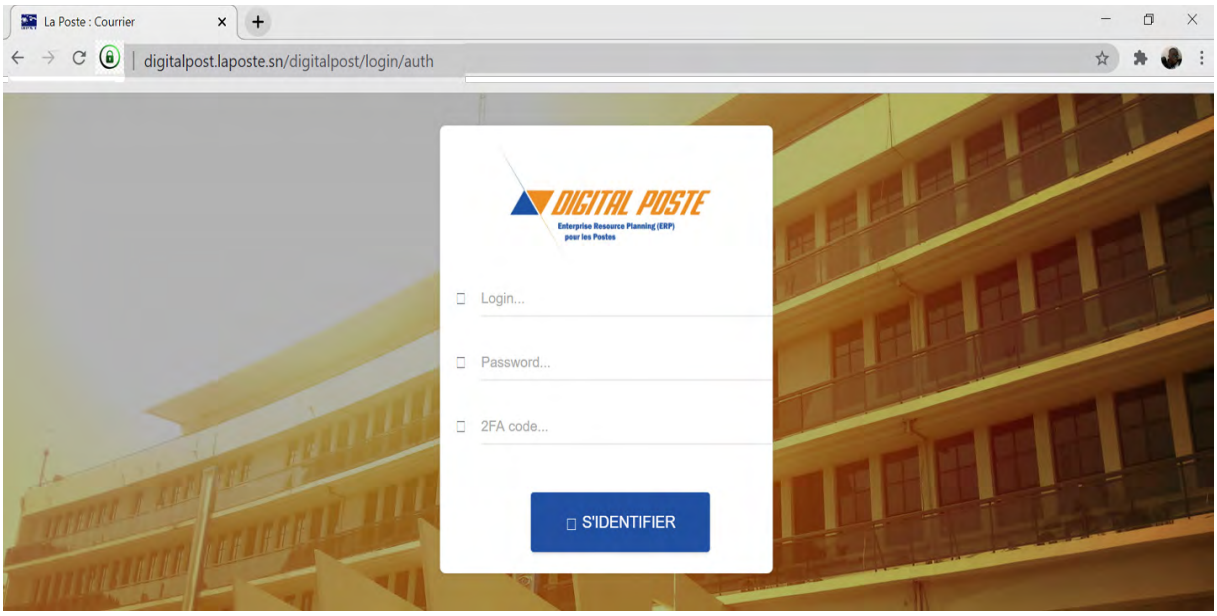


4.4 Test de fonctionnement

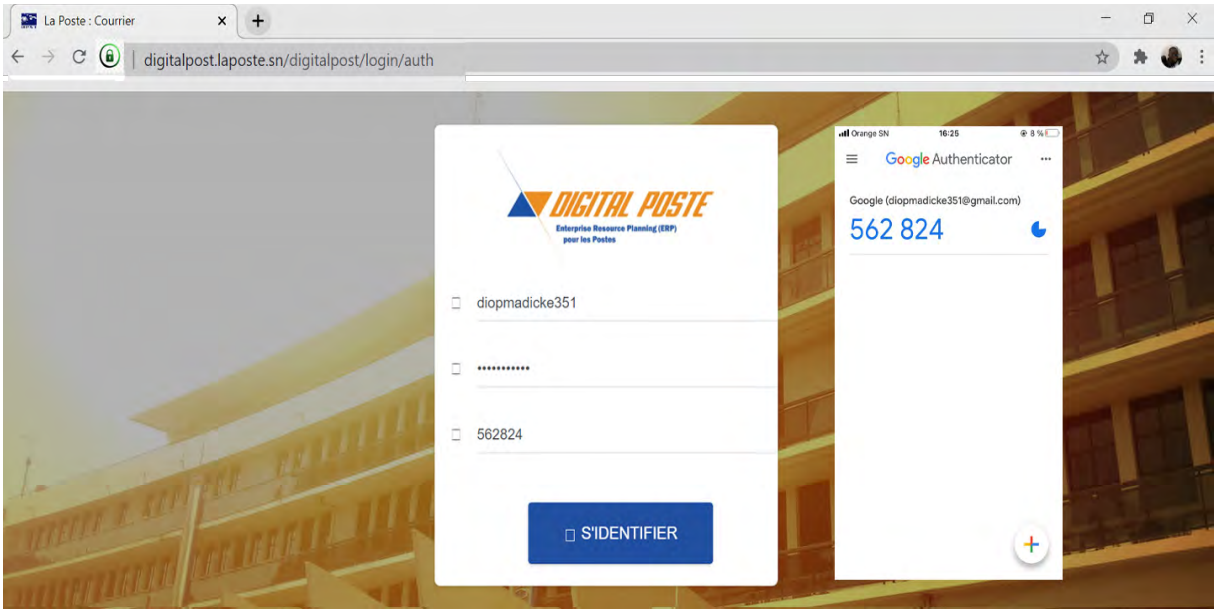
1. **Acceder sur l'application DigitalPost avant déploiement de SSL(https)**



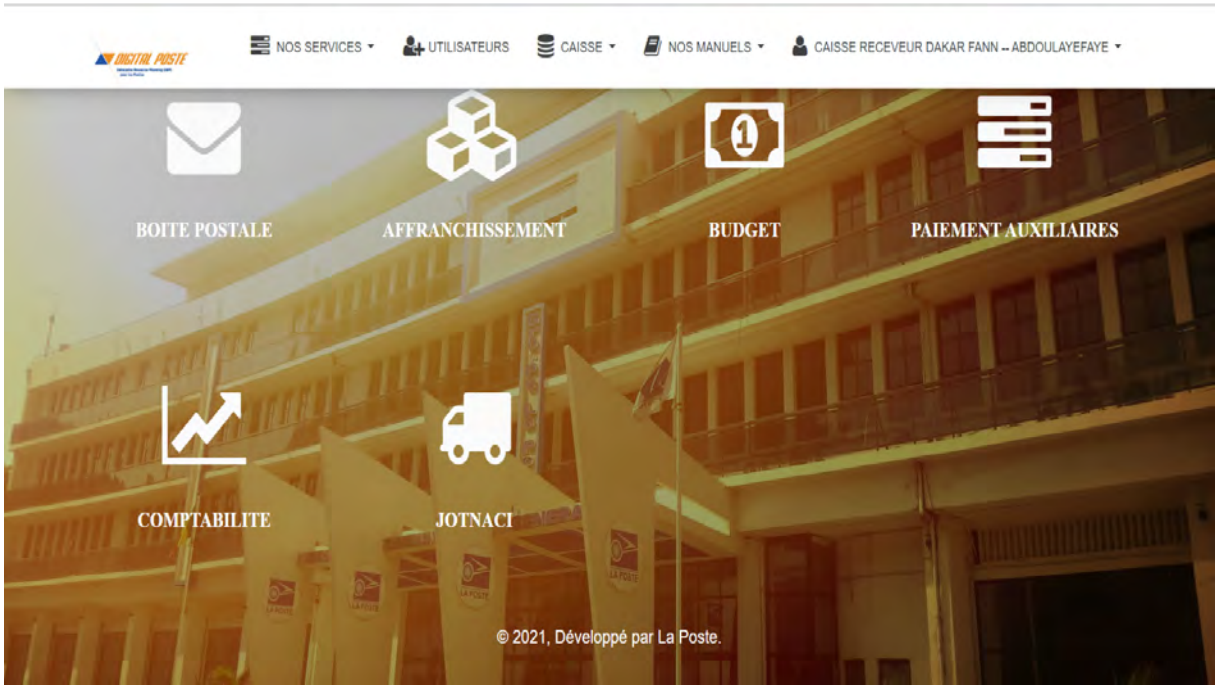
2. **Acceder sur l'application DigitalPost apres déploiement de SSL(https) et de l'authentification forte OTP(One-Time Password)**



3. **Saisie du premier et du second facteur d'auhentification forte**



4. **Acces aux ressources ou services de l'application DigitalPost**



Conclusion

Notre travail comprend un cas précis de déploiement de la solution d'authentification forte, où nous avons adhéré les normes internationales et les bonnes pratiques. Dans la première phase nous avons montré comment implémenter l'AC racine qui va être utilisé pour la création de certificat client-serveur afin d'assurer le déploiement du SSL(https). Ensuite nous avons déploiement la solution d'authentification forte basée sur OTP(One-Time Password) sur l'application DigitalPost à travers le software token Google Authenticator et en finir avec les tests de fonctionnements.

Chapitre 5

Evaluation financière de la solution

Introduction

En confiant un nombre croissant de projets de sécurité aux experts, les entreprises délèguent à leurs fournisseurs informatiques la création de leur infrastructure à clés publiques (PKI) afin de déployer le SSL(https) avec certificat et sa maintenance opérationnelle. Présumant souvent à tort de la « gratuité » des Autorités de certification (AC) internes, les intégrateurs de systèmes s'engagent dans cette voie ignorant les conséquences financières et bonnes pratiques .

Budgétisation de la solution

La réalité d'une AC interne est plus complexe qu'il n'y paraît. Outre les trois à quatre mois de préparation nécessaires, un projet quinquennal requiert, d'après nos estimations, 800 000 F de budget de déploiement et de maintenance. Ces chiffres peuvent exploser pour les projets PKI de grande envergure lorsque, par exemple, si la confiance publique est également requise. Avant d'établir votre devis, prenez bien en compte l'ensemble des éléments suivants :

— **Coûts logiciels et matériels**
Si l'émission des certificats est gratuite, il n'en va pas de même pour les systèmes d'exploitation, les environnements de virtualisation, les serveurs d'AC, les serveurs de listes de révocation des certificats et de protocole de vérification en ligne des certificats (CRL/OCSP), les modules matériels de sécurité et les répartiteurs de charge.

— **Documentations**
Pour toute mise en production, plusieurs documents doivent être rédigés, approuvés et maintenus à jour durant le cycle de vie du projet. Une simple demande de changement doit faire l'objet d'une vérification complète.

— **Conformité**
La connaissance des réglementations sectorielles étant essentielle, les déclarations des pratiques de certification (DPC) et les processus correspondants doivent être mis en œuvre, et couvrent tous les aspects allant de la sécurité des bâtiments à

la formation du personnel.

— **Ressources internes**
Plusieurs équipes devront faire fonctionner l'AC (pas uniquement pour la préparation, mais également pour la maintenance et les mises à jour). Pensez à budgétiser toutes les ressources (en heures-hommes), à savoir l'équipe d'infrastructure, les experts en cybersécurité et l'assistance technique pour maintenir les niveaux de services souhaités...

Conclusion

Dans ce chapitre nous avons vu l'ensemble des criteres indispensables pour pouvoir estimer le budget du déploiement du SSL(https) avec les certificats numeriques.Ces criteres nous ont permi aussi de savoir à peu pres le coût de notre solution d'authentication forte basée sur OTP(One-Time Password) et le déploiement du SSL(https) avec les certificats numeriques.

Conclusion Générale et Perspectives

Ce projet nous a permis d'approfondir les connaissances théoriques et pratiques que nous avons acquises tout au long de notre formation, cela nous a permis de faire l'étude et le déploiement d'un système de gestion d'une authentification forte en utilisant le mot de passe à usage unique (OTP) et du SSL(https) avec l'appui des certificats électroniques pour le cas de LaPoste. Ces déploiements ont assuré l'authentification forte des utilisateurs et ordinateurs sur l'application DigitalPost de l'entreprise LaPoste, la signature électronique des certificats et la sécurité des sites web ainsi que le trafic entre différentes entités... etc.

Il nous a été confié durant ce projet la mission de réaliser une solution d'authentification forte basée sur le mot de passe à usage unique (OTP) et le déploiement du SSL(https) avec l'appui des certificats électroniques basée sur les infrastructures à clé publique.

Ce projet a de nombreux avantages tels que la facilité et la gestion des problèmes d'administration, résoudre la notion de confiance et d'authentification forte et assurer la sécurité des informations... etc. L'élaboration de ce travail nous a permis de rentrer dans un monde de sécurité informatique tellement vaste, et d'apprendre la façon d'appliquer les outils informatiques pour une bonne gestion d'authentification forte et de confiance, et d'élever le niveau de protection des données de tous les agents de l'entreprise LaPoste.

Ce projet nous a permis de s'intégrer dans le milieu de la recherche et professionnel, de bénéficier une expérience. Cependant, le développement d'un tel projet n'est jamais totalement achevé et certaines idées seront développées dans nos perspectives. C'est dans ce sens et afin d'améliorer ce présent travail que nous proposons de créer pour l'entreprise LaPoste sa propre software token(application de génération de mot de passe à usage unique) afin qu'elle soit indépendante de certaines solutions de génération d'OTP(One-Time Password).

Enfin, nous souhaiterons que ce travail puisse servir d'accompagnement pour les futurs projets innovants de l'entreprise LaPoste dans le domaine de l'authentification multifacteur sur les Infrastructure à clé publique.

Bibliographie

[1] Demba SOW,
Courbes elliptiques, Cryptographie à clés publiques et Protocolesd'échange de clés,
le 06/07/2013 ,
Université Cheikh Anta Diop de Dakar(UCAD),
Thèse de doctorat,
Consultée le 10/01/2021, disponible sur :
https://www.scribd.com/document/405825954/122-DembaSow-courbeselliptiquescryptogra

[2] Cours cryptographie de Docteur Demba SOW
Enseignant chercheur au Département de Mathématiques/Informatique Email :
demba1.sow@ucad.edu.sn, sowdembis@yahoo.fr
Consulté le 15/01/2021

[3] A et B - Newsletter Confiance Numérique
N 2 - L'authentification forte
Consulté le 19/02/2021 , disponible sur :
ab-newsletterconfiancenumrique-n2lauthentificationforte-141015042955-conversion-ga
pdf

[4] Authentification Forte
Concept et Technologies
Consulté le 20/02/2021 , disponible sur :
xposir3af-13322411791483-phpapp01-120320060219-phpapp01.pdf

[5] LIVRE BLANC GLOBALSIGN
John B Harris,
Expert en sécurité
Pour GMO GlobalSign Ltd.
Consulté le 18/02/2021

[6] Houda FERRAD
Initiation à la cryptographie : théorie et pratique
Consulté le 02/02/2021 , disponible sur :
https://www.di.ens.fr/~ferradi/cours.pdf

[7] Cryptographie et Sécurité informatique
Université de Liège
Faculté des Sciences Appliquées

Consulté le 01/02/2021 , disponible sur :
http://www.montefiore.ulg.ac.be/~dumont/pdf/crypto.pdf

[8] Luca De Feo
Mathematics of Isogeny Based Cryptography
Université de Versailles et Inria Saclay
Consulté le 27/02/2021 , disponible sur :
http://defeo.lu/

Webographie

[9] Authentification à deux facteurs avec Google Authenticator.
Consulté le 24/02/2021 , disponible sur :
https://support.clio.com/hc/en-us/articles/203184210-Two-Factor-Authentication-with-Google-Authenticator

[10] Traveaux master sécurité des systemes d'informations
authentification à double facteurs
Consulté le 20/02/2021 , disponible sur :
https://www.clubdsi.ci/Publications/CDSI_ESATIC_AUTHENTIFICATION_2_FACTEURS.pdf

[11] Authentification forte par opérateur de réseau mobile à l"usage
des utilisateurs de services web
Consulté le 10/02/2021 , disponible sur :
https://www.researchgate.net/publication/268503949

[12] L'authentification double facteur expliquée à tous
Consulté le 21/02/2021 , disponible sur :
https://www.clubic.com/antivirus-securite-informatique/actualite-853735-authentification-double-facteur-expliquee.html

[13] Conception et implémentation
d'une solution d'authentification forte « PKI »
Consulté le 18/02/2021 , disponible sur :
https://www.slideshare.net/hossam-10/pki-77008678

[14] IOT et Cyber
CYBERSÉCURITÉ : QUELS SONT LES MOYENS D'AUTHENTIFICATION ?
Consulté le 01/03/2021 , disponible sur :
https://weave.eu/cybersecurite-sommes-moyens-dauthentification/

[15] Wikipédia Authentification forte
Consulté le 02/03/2021 , disponible sur :
https://fr.wikipedia.org/wiki/Authentification_forte

[16] Architecture de communication client-serveur via SSL(https) avec certificat
Consulté le 04/02/2021 , disponible sur :
https://www.linkedin.com/learning/les-fondements-des-reseaux-la-securite/comprendre-l-authentification-par-certificat

[17] Installation de l'application Google Authenticator
Consulté le 08/02/2021 , disponible sur :

https://support.clio.com/hc/en-us/categories/
200961717-Account-Administration-Settings