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).

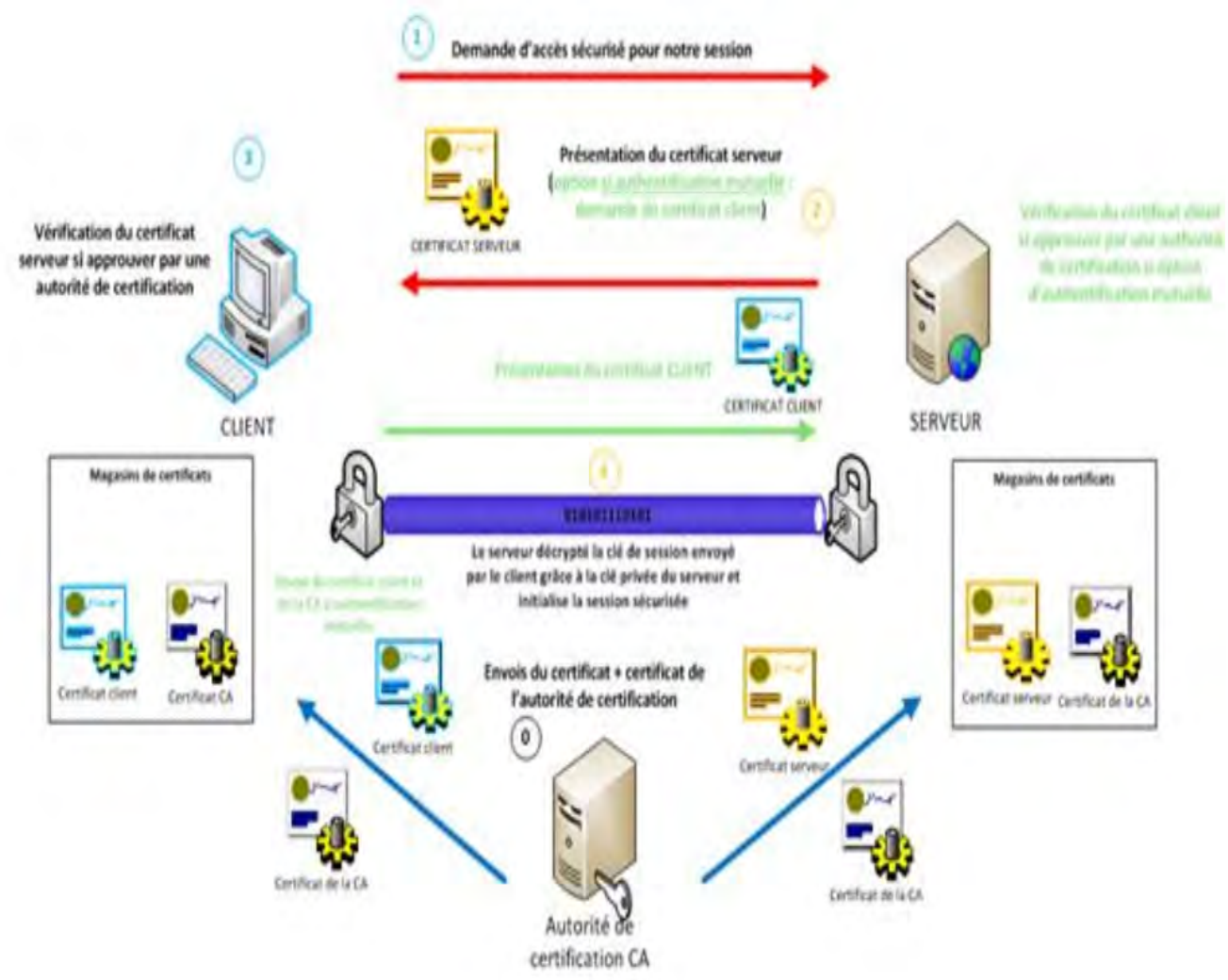

Figure.3.5.Authentification avec certificat x.509 source :[13]

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.