Sécurité - PKI et Certificats

Difficulté : Intermédiaire

Notions : certificats, identité, https, chiffrement.

I. Introduction

Lors d'échanges sur des protocoles standards non sécurisés, il est facile d'intercepter les données. Afin de sécuriser ces échanges, celles-ci doivent être chiffrées à l'aide d'algorithmes adaptés.

Cependant, même si les données sont chiffrées, il reste essentiel de s'assurer que l'on communique avec un partenaire de confiance. Il devient donc nécessaire de pouvoir valider l'identité de ce partenaire.

Il faut également garantir que les données transmises n'ont pas été altérées pendant l'échange.

Pour répondre à ces trois besoins (confidentialité, authentification et intégrité) a été créée l'infrastructure à clés publiques, ou Public Key Infrastructure (PKI).

Une PKI est un ensemble de composants matériels, logiciels et de procédures permettant de gérer les clés publiques des utilisateurs et des systèmes, afin de garantir la fiabilité de leurs identités. Elle renforce ainsi la confiance dans les systèmes numériques.

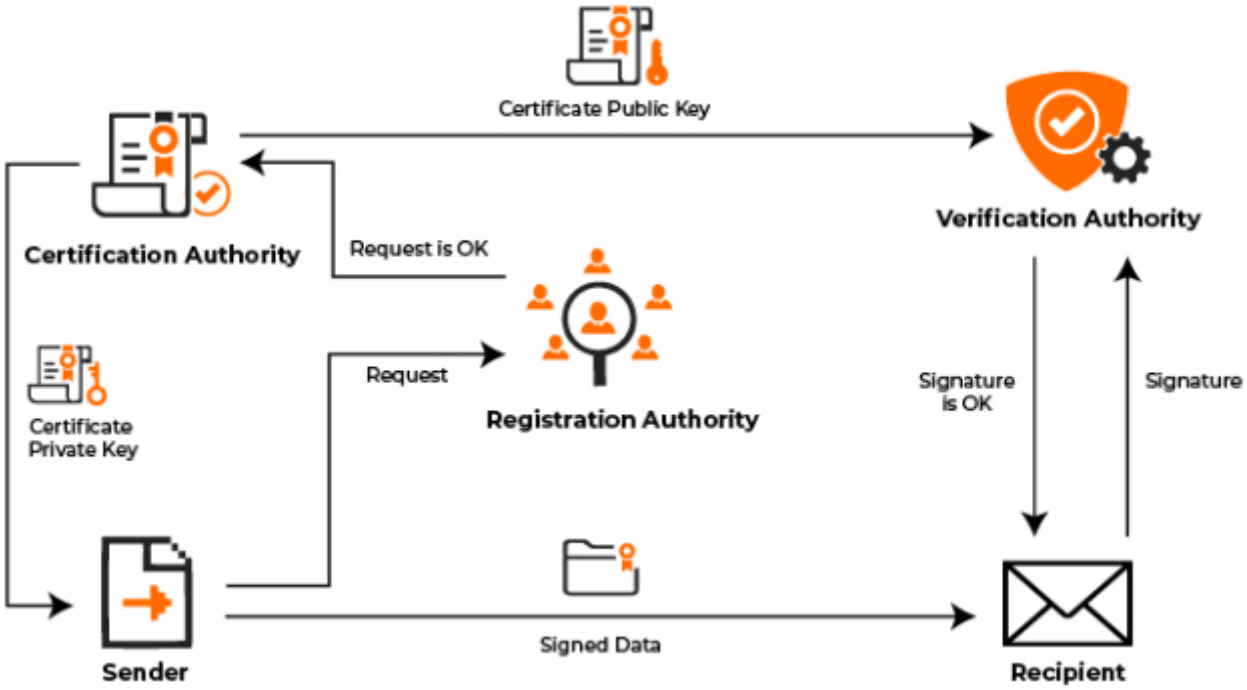
Bien qu'il existe plusieurs modèles de PKI, ce cours se concentrera sur un modèle reposant sur trois composants principaux :

- **Autorité de certification (CA)**
- **Autorité d'enregistrement (RA)**

- **Service ou autorité de validation (VA)**

Le principe de fonctionnement est le suivant :

1. Un utilisateur ou une machine génère une clé privée.
2. À partir de cette clé, une requête de certificat (CSR) est créée.
3. Cette requête est soumise à une autorité d'enregistrement.
4. L'autorité d'enregistrement vérifie l'identité du demandeur et transmet la requête à l'autorité de certification.
5. Une fois validée, l'autorité de certification signe la requête et génère le certificat, qui sera fourni à l'utilisateur ou à la machine.
6. Lors des échanges entre deux tiers, le destinataire peut vérifier la validité du certificat et son état (non-révocation) via un service de validation



Source : appViewx

II. Le protocole SSL/TLS

> **Info** : Le protocole SSL/TLS intervient entre les couches transport (4) et application (7).

2.1 Qu'est ce que SSL/TLS

Pour chiffrer les communications, notamment web, il existe deux protocoles principalement utilisés :

- **SSL (Secure Sockets Layer)**: Le SSL est une technologie standard de chiffrement qui permet d'établir une communication à travers un socket chiffré entre un navigateur et un serveur web.

> **Attention** : l'usage de SSL est déprécié et remplacé par TLS.

- **TLS (Transport Layer Security)**: Le protocole TLS est le successeur de SSL. Celui-ci permet une sécurité accrue avec des validations plus poussées et un meilleur chiffrement. Il est plus souvent appelé SSL/TLS.
  - Les versions majoritairement utilisées sont TLS 1.2 et 1.3

Ceux-ci s'appuieront sur des certificats et des clés de chiffrement.

Plus les algorithmes de chiffrements utilisés sont performants, plus il sera difficile de déchiffrer la communication.

2.2 Le but des certificats SSL

L'utilisation des certificats poursuit un but triple :

- **Chiffrement** : Le certificat contient la clé publique utilisée pour établir un secret partagé, qui servira ensuite à chiffrer la communication.
- **Authentification** : Il garantit que l'identité du pair est vérifiée et qu'il s'agit bien de la machine/personne avec qui l'on souhaite communiquer.
- **Intégrité de la donnée** : L’intégrité des données est assurée par les mécanismes cryptographiques de TLS (MAC ou AEAD), pas par le certificat lui-même.

III. Le fonctionnement de SSL/TLS

3.1 Application de Public Key Infrastructure (PKI)

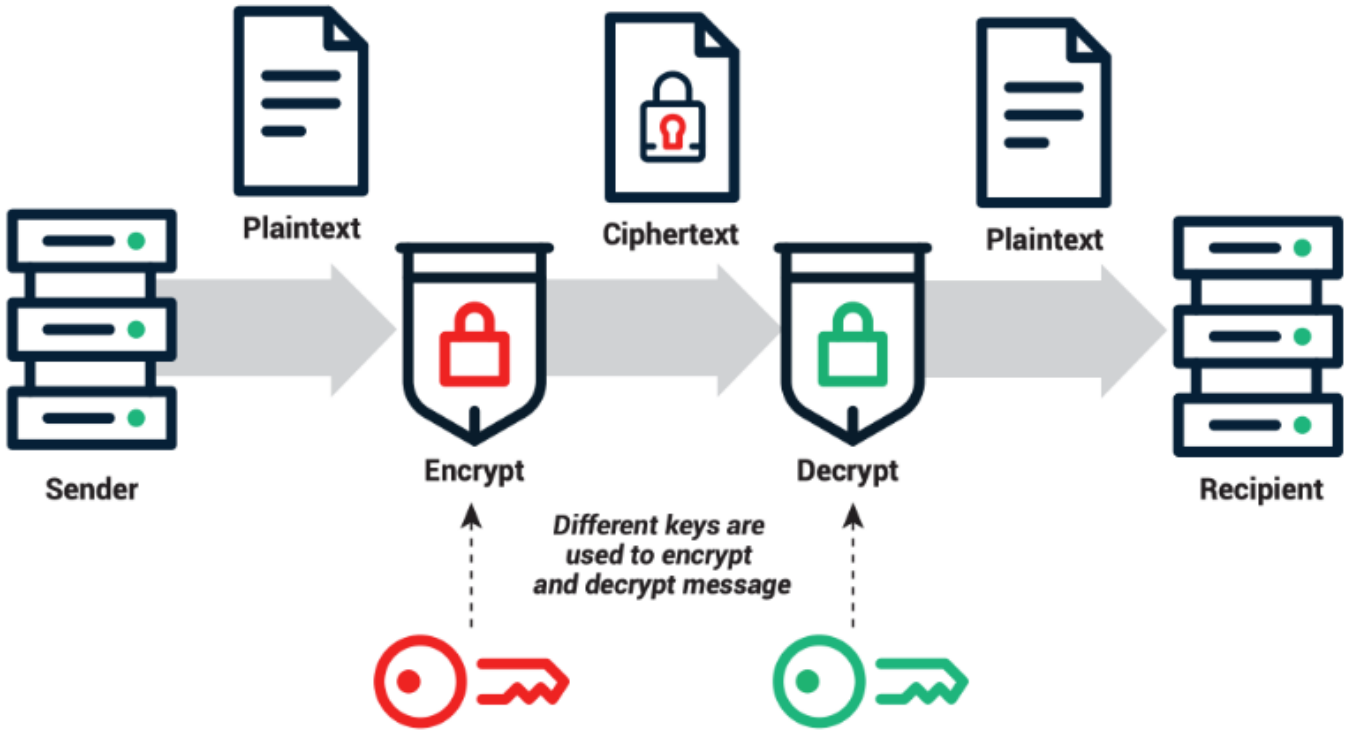
Lors d'un échange d'informations utilisant SSL/TLS, le serveur possède une paire de clés composée d'une clé privée et d'une clé publique. La clé publique est intégrée dans un certificat numérique signé par une autorité de certification (CA).

Le client, quant à lui, ne possède généralement pas de clé privée : il utilise simplement les certificats des autorités de certification de confiance installés dans son système pour vérifier l'authenticité du certificat du serveur.

Lors de la connexion, le client peut :

- vérifier la signature du certificat du serveur grâce au certificat de la CA,
- vérifier que le certificat est valide (dates, nom de domaine),
- vérifier que le certificat n'a pas été révoqué (via CRL ou OCSP).

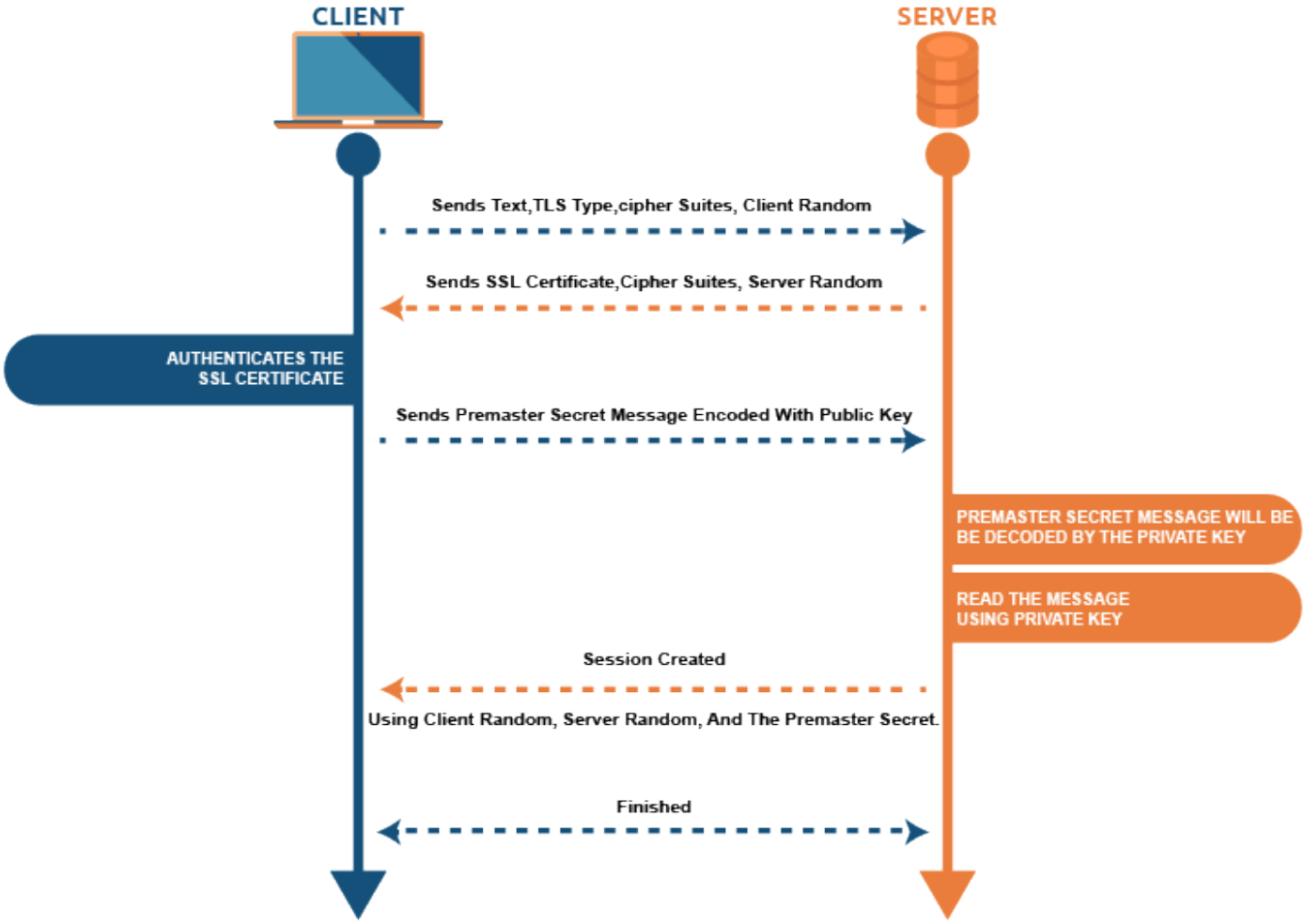
Une fois ces vérifications effectuées, le client peut établir une connexion TLS sécurisée avec le serveur.



Source : Sectigo

3.2 Le processus du "Handshake" SSL

Une étape clé du fonctionnement de SSL/TLS est le '***handshake***'. Cette phase permet au client et au serveur de négocier les paramètres de sécurité, d'authentifier le serveur et d'établir un secret partagé qui servira à chiffrer la session.



1. **Client Hello**: Le client envoie un message contenant la version de TLS qu'il supporte, la liste des suites cryptographiques disponibles et des paramètres aléatoires.
2. **Server Hello**: Le serveur répond en choisissant une version TLS et une suite de chiffrement parmi celles proposées. Il envoie également son certificat SSL/TLS.
3. **Certificate Verification**: Le client vérifie le certificat du serveur à l'aide des autorités de certification de confiance (CA) et des mécanismes de révocation (CRL/OCSP).
4. **Pre-Master Secret**: Le client génère un pré-secret (Pre-Master Secret), le chiffre avec la clé publique du serveur (présente dans le certificat) et l'envoie au serveur.
5. **Session Keys**: Le client et le serveur dérivent indépendamment les clés de session à partir du Pre-Master Secret et des valeurs aléatoires échangées.
6. **Secure Connection** : Une fois les clés établies, la communication est chiffrée et l'échange sécurisé peut commencer.

> **Info** : Dans la version 1.3 de TLS, le processus de handshake à été simplifié afin d'être plus rapide et sécurisé (suppression du Pré-master secret et utilisation obligatoire de ECDHE (Perfect Forward Security)).

IV. Les autorités de certifications

Comme vu plus haut, les autorité de certifications jouent un rôle déterminant dans une PKI. Elles sont responsables de la création, de la signature et de la gestion des certificats numériques.

4.1 Portée des autorités de certification

On les divise en deux groupes :

- **Les CA publiques.**
  - Elles sont publiées et accessible sur internet.
  - Elles ont fait l'objet de validations par des organismes spécialisés et disposent ainsi d'un haut degré de confiance.
  - Les certificats des autorités publiques sont installés dans tous les navigateurs et les OS et mis à jours avec ceux-ci.
  - Ainsi ils permettent une ***confiance Universelle***.

Par exemple : let's encrypt, Sectigo, Digicert, ...

- **Les CA privées ou organisationnelles.**
  - Ce sont les CA mises en place au sein d'une organisation.
  - Elles ne sont validée qu'en interne par l'organisation et la portée de leur confiance se limite donc à celle-ci.
  - Les certificats ne sont pas installés dans les navigateurs ou les systèmes et doivent donc être déployés.
  - Elles permettent donc d'avoir une ***confiance en interne*** envers les composants de l'organisation.

Utilisés par exemple pour : VPN, interfaces web, applications, DNSsec, messagerie chiffrée, LDAPs, ...

4.2 Type des autorités de certification

Une chaîne de certificat est généralement construite comme suit et repose sur :

- **Une autorité racine de confiance (ROOT CA)**
  - C'est l'autorité la plus haute dans la hiérarchie PKI.
  - Son certificat est ***autosigné*** (elle se signe elle-même).
  - Elle est ***extrêmement protégée*** : souvent hors ligne, stockée dans des modules matériels sécurisés (HSM).
  - Elle ne signe généralement ***pas directement*** les certificats des serveurs.
  - Son rôle principal est de signer les certificats des autorités intermédiaires.

La confiance dans toute la PKI repose sur la sécurité de la Root CA.

- **Les autorités intermédiaires (Intermediate CA)**
  - Située entre la Root CA et les certificats finaux (serveurs, utilisateurs).
  - Son certificat est signé par la Root CA ou par une autre CA intermédiaire.
  - Elle signe les certificats des serveurs ou des utilisateurs.
  - Permet de limiter les risques : si une CA intermédiaire est compromise, la Root CA peut la révoquer sans détruire toute la PKI.

La plupart des certificats SSL/TLS sont signés par une ***CA intermédiaire***, pas par la racine.

4.3 Les certificats auto-signés

Un certificat autosigné est un certificat dont la clé publique appartient au même acteur que la clé privée et qui est ***signé par lui-même***.

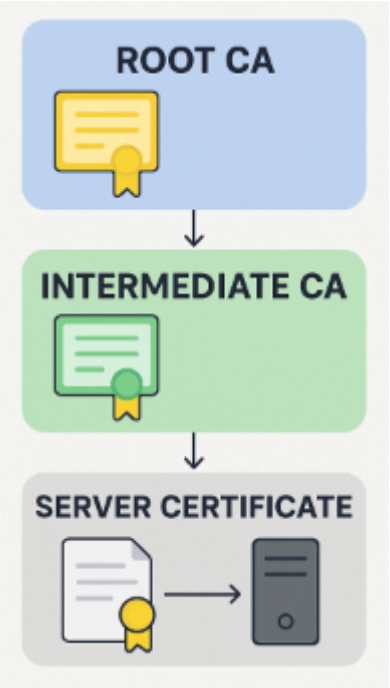
Il existe deux cas :

1. Certificat autosigné légitime

- C'est le cas des **certificats racine**.
- Ils doivent être autosignés, car ils sont au sommet de la chaîne de confiance.

2. Certificat autosigné non reconnu

- Généré par un serveur ou un administrateur sans passer par une CA.
- Utilisé parfois pour des tests ou des environnements internes.
- Les navigateurs affichent une alerte car **aucune autorité de confiance ne l'a validé**.



V. Les types de certificats

	Validation	Cas d'usage
Validation de domaine (**DV**)	L’autorité de certification vérifie que le demandeur contrôle bien le nom de domaine concerné. Cela peut se faire par e-mail, en ajoutant un enregistrement DNS, ou via un fichier placé sur le serveur.	*Sites web simples, blogs, pages d’information, environnements de test...* Ce type de certificat ne garantit pas l’identité de l’organisation derrière le site
Validation d'organisations (**OV**)	En plus de la vérification du domaine, l’autorité de certification vérifie l’existence légale de l’organisation, son adresse, son numéro d’enregistrement, etc.	*Sites professionnels, plateformes e-commerce, services publics.* Le certificat affiche le nom de l’organisation, ce qui renforce la confiance des utilisateurs.

Validation étendue (**EV**)	Vérification approfondie de l'organisation (existence légale, physique et opérationnelle). L'autorité de certification suit un processus strict et documenté.	*Sites à haute sensibilité : banques, services financiers, plateformes de paiement, administrations.* Dans certains navigateurs, le nom de l'organisation apparaît en vert ou dans la barre d'adresse.

VI. Considérations de sécurité

L'utilisation de certificats SSL/TLS renforce la sécurité des échanges, mais elle n'est pas infaillible. En effet, une mauvaise configuration expose à des risques. Il est essentiel de connaître les principales vulnérabilités et d'adopter des bonnes pratiques pour garantir une protection efficace.

6.1 Faiblesses et attaques

- **Man-in-the-Middle (MitM) :**Un attaquant intercepte la communication entre le client et le serveur, pouvant ainsi lire, modifier ou injecter des données.

Cette attaque est possible si le certificat n'est pas correctement vérifié ou si la connexion n'est pas chiffrée.

- **Usurpation de certificat (Certificate Spoofing) :** Des certificats falsifiés ou compromis peuvent être utilisés pour faire croire à l'utilisateur qu'il communique avec un site légitime.

Cela peut survenir si une autorité de certification est compromise ou si l'utilisateur ignore les avertissements du navigateur.

6.2 Bonnes pratiques

- **Mises à jour régulières :** Maintenir à jour les logiciels serveurs, bibliothèques SSL/TLS et certificats permet de corriger les vulnérabilités connues et d’éviter les failles exploitées par les attaquants.
- **Chiffrement fort :** Utiliser des algorithmes modernes et robustes (ex : AES-256, ECDHE) et désactiver les suites de chiffrement obsolètes (ex : RC4, MD5, SSLv3).
- **Surveillance et audit :** Vérifier régulièrement la configuration SSL/TLS du serveur, la validité des certificats, et surveiller les journaux pour détecter toute tentative d’accès non autorisé ou anomalie.

6.3 Erreurs courantes

Les erreurs les plus courantes lors de l'utilisation des certificats qui peuvent empêcher l'affichage correcte d'un site sont :

- Certificat expiré
- Nom de domaine incorrect
- Chaîne incomplète
- Utilisation de suites de chiffrement faibles

Conclusion

Les certificats SSL/TLS et l’infrastructure à clés publiques (PKI) constituent la base de la confiance numérique moderne. Ils permettent de garantir la confidentialité des échanges, d’authentifier les acteurs et d’assurer l’intégrité des données. Leur efficacité repose autant sur la robustesse des algorithmes que sur la bonne gestion des autorités de certification, des chaînes de confiance et des mécanismes de validation.

Dans un contexte où les attaques deviennent plus sophistiquées, il est essentiel de maintenir des configurations TLS à jour, de surveiller l’état des certificats et d’adopter des pratiques de sécurité rigoureuses. Une PKI bien conçue et correctement administrée reste l’un des piliers les plus fiables pour sécuriser les communications et renforcer la confiance dans les systèmes d’information.

Revision #2
Created 2026-07-17 20:41:29 UTC by Olivier
Updated 2026-07-17 20:42:20 UTC by Olivier