# Défense

**ISI**

4 - Defense


## Résumé du document

Cette note parle de la sécurité informatique, abordant le protocole TLS pour sécuriser les communications web, l'utilisation de HTTPS, la sécurisation des emails avec PGP, la protection des réseaux via les pare-feu et la défense contre les attaques par le biais des équipements avec EDR


## Table des matières

# 1. SLS/TLS

- SLS: Security Level Specification
- TLS: Target Level of Security

Leur **objectif** est d'offrir une boîte à outils pour établir des communications sécurisées. Le protocole a été développé par Netscape et avait pour objectif de sécuriser les échanges sur le web. Il est basé sur SSL (Secure Socket Layer) et a été renommé TLS (Transport Layer Security) par l'IETF.

Ce protocole s'applique à la couche **application** du modèle OSI.

## 1.1. Propositions

- négociation de la version SSL/TLS et des algorithmes utilisés
- authentification des entités
- authentification/intégrité des données
- confidentialité des données
- compression des données

## 1.2. Utilisation

### 1.2.1. Création nouveau protocol

- HTTP (port 80) devient HTTPS (port 443)
  - Avantage: assure que la communication est sécurisée
  - Inconvénient: seuls les clients supportants TLS peuvent se connecter

### 1.2.2. Extension protocol existant

- ESMTP avec STARTTLS, le client **peut** demander du TLS
  - Avantage: le client n'a pas besoin de supporter TLS mais peut le demander si souhaité
  - Inconvénient: les communications peuvent ne pas être sécurisées

## 1.3. HTTPS

- L'utilisation de TLS est imposée (non négociable)
- Le serveur doit avoir un certificat
- Garantie de l'authenticité du serveur
- Garantie de la confidentialité des communications
- Le client peut avoir un certificat (optionnel)

## 1.4. SMTP, POP3, IMAP

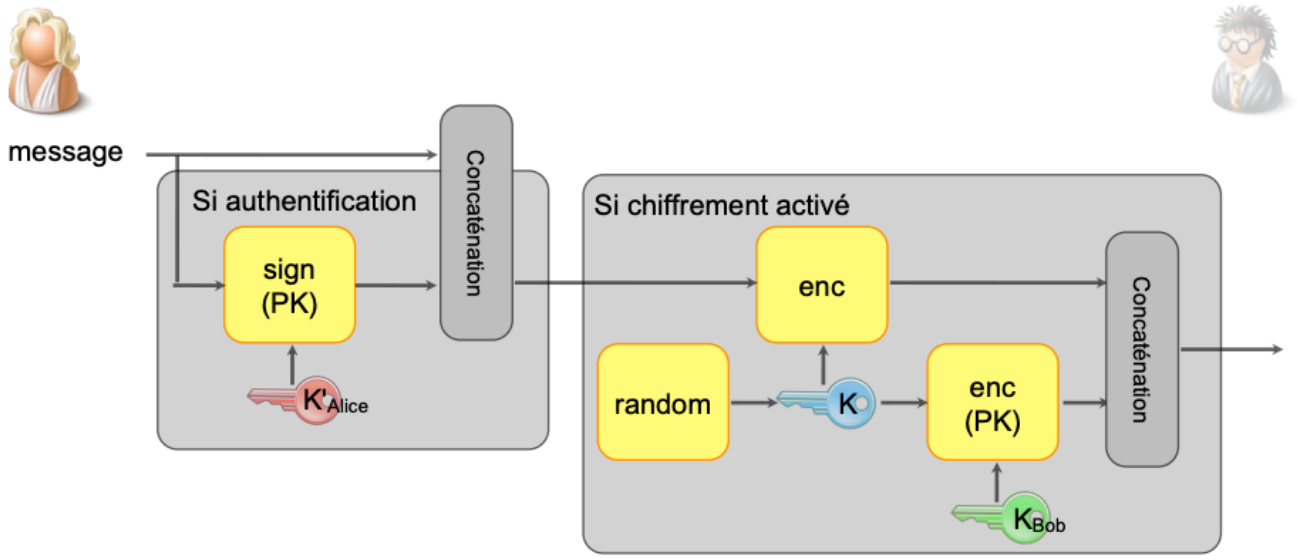
- ESMTP (envoi d'emails)
- POP3 (récupération d'emails)
- IMAP (gestion d'une boîte email)
- Faiblesses du protocole de base :
  - Par défaut, les mots de passe sont envoyés en clair.
  - Par défaut, le contenu des emails est envoyé en clair.
- **TLS** permet de protéger l'ensemble des communications :
  - TLS est une **extension** du protocole
  - TLS est **optionnelle** (configuration)

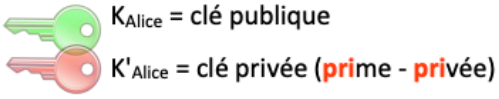
# 2. PGP

PGP signifie Pretty Good Privacy. C'est un logiciel permettant de sécuriser du texte, des emails, des fichiers, des répertoires, etc.. Il utilise la **cryptographie hybride** (symétrique et asymétrique).

Il garantit :
- la confidentialité des données (chiffrement)
- l'authentification/intégrité des données (signature)

## 2.1. Principe




## 2.2. Algorithme utilisés

- Fonctions de hachage :
  - MD5, SHA-1,…
- Chiffrement symétrique :
  - 3DES, IDEA, AES, …
- Algorithmes asymétriques :
  - RSA, DSA, ElGamal
  - Types de clés :
  - RSA et RSA
  - DSA et ElGamal
  - DSA (signature uniquement)
  - RSA (signature uniquement)

## 2.3. PGP vs X.509

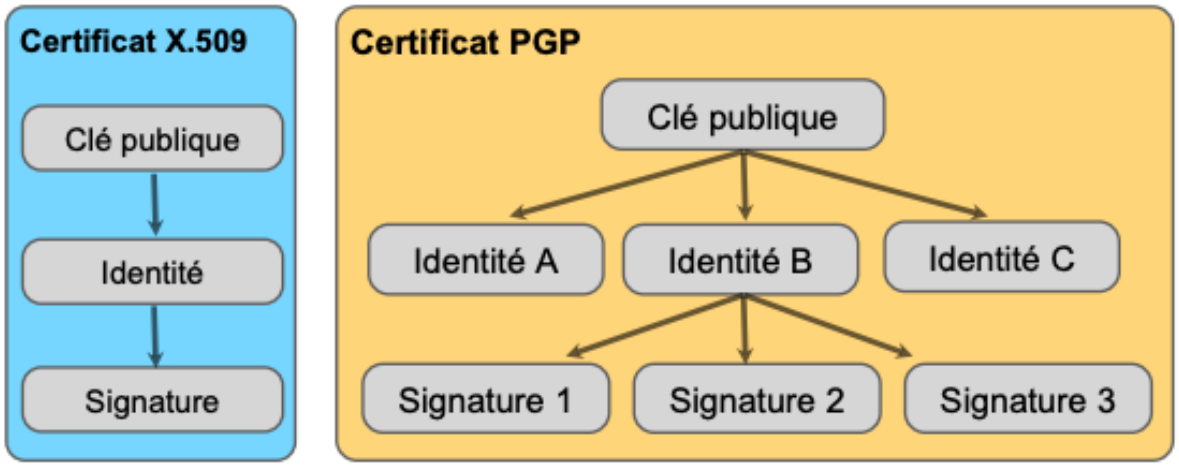
Clé signée = certificat, c'est un lien entre une clé publique et une identité.

X.509 ne permet qu'une **seule identité** alors que PGP permet **plusieurs identités**.

X.509, l'auteur est l'autorité de certification (**une seule** signature) alors que PGP, les auteurs sont ad-hoc (**plusieurs signatures** possibles)

Un certificat PGP comprend :
- une/plusieurs identité(s)
- une/plusieurs signature(s) par identité
- photo (option)

- un révocateur désigné (option)
- une «Additional Decryption Key» (option)



# 3. Pare-feu

Un pare-feu est un dispositif de sécurité qui a pour objectif de protéger un réseau informatique des attaques extérieures. Il est placé entre le réseau local et le réseau externe (Internet).

## 3.1. Contrôles d'accès

- Filtrage statique (obsolète) :
  - inspection de chaque paquet indépendamment les uns des autres (rarement utilisé)
  - Pare-feu sans mémoire
  - Pare-feu sans état
- Filtrage dynamique :
  - décision en fonction du rôle du paquet dans les flux de communication (client-serveur essentiellement)
  - Pare-feu avec mémoire
  - Pare-feu à état

## 3.2. Types de pare-feu

- Pare-feu réseau
  - équipement réseau
  - filtrage des paquets entre deux réseaux
  - critères de base : source (IP), destination (IP), service (ports), …
- Pare-feu personnel
  - logiciel installé sur un ordinateur
  - filtrage des paquets entre l'ordinateur et le réseau
  - critères de base : application, source (IP), destination (IP), service (ports), …

# 4. EDR

•Un attaquant peut pénétrer dans réseau privé en s’en prenant a un équipement (“endpoint”) disposant d’un accès privilégié

- Réseau: VPN obligatoire (totalité du traffic sauf la connexion au VPN)
- Gestion à distance via un agent
  - Anti-virus
  - Collecte centralisée des logs vers un SIEM