

Présentation : une histoire de clés et de capsules

Protection des échanges au-delà du réseau local

La mise en place d'un **firewall** ou **pare-feu** permet de protéger le contenu présent à l'intérieur d'un réseau et d'empêcher la fuite de données vers l'extérieur.

Mais pour les échanges autorisés à sortir, l'information est diffusée au delà de notre sphère de contrôle et il faut ajouter une *capsule* de protection autour de l'information que l'on transfère (on parle d'encapsulation) si l'on souhaite en empêcher la lecture par des personnes extérieures à l'échange.

Clé(s) de cryptage

Pour partager des messages de manière confidentielle, deux extrémités d'une communication doivent disposer d'un secret (**une ou des clés**) qui permettra

- de **coder** un message (on parle aussi de **chiffrement**) à l'émission,
- de le **décoder** (ou **déchiffrer** ou encore **décrypter**) à la réception.

Si c'est la même clé qui permet le cryptage/décryptage, on dira qu'il s'agit d'une clé symétrique.

Si on veut un niveau de sécurité accru, on réalisera l'encryptage par le biais d'une clé distribuée à tous les émetteurs potentiels (cette clé est publique, généralement contenue dans un certificat), et seul le destinataire possèdera la clé capable de réaliser le déchiffrement (la clé est donc privée).

Dans ce cas d'une clé privée de décodage et publique de codage, on parle d'un cryptage asymétrique.

Cryptage, clé publique, clé privée

La **clé publique** peut être vue comme un **cadenas ouvert** dont la serrure est basée sur l'empreinte de la **clé privée**.

1. On distribue des cadenas (**clé publique**) à des interlocuteurs qui demandent à entrer en communication.
2. Les interlocuteurs enferment leur message dans des boîtes qu'ils cadenaient avec cette **clé publique (cryptage)**.
3. La **clé privée** est la seule à même d'ouvrir les cadenas (**décryptage**) et de donner accès au contenu de la boîte.



Certificat

Dans le cas d'un accès à un serveur public sécurisé (par exemple pour gérer ses comptes ou payer en ligne), il est difficile de distribuer la clé publique à l'avance. 

Le principe est alors de déposer, sur le serveur, un **objet** qui remplira les objectifs suivants :

- crypter l'information envoyée vers le serveur avec la *clé publique* contenue dans le *certificat*
- garantir l'intégrité des données transférées grâce à des techniques de **hachage**
- garantir l'identité du serveur en précisant toutes les coordonnées de l'entreprise qui le met à disposition et, éventuellement, de l'organisme qui en *garantit la validité* (**tiers de confiance**, indispensable pour le paiement en ligne par exemple)
- préciser tous les algorithmes de cryptage et de hachage supportés par le serveur

Cet **objet** est un fichier textuel nommé certificat. Divers formats existent, dont le standard de l'*Union Internationale des Télécoms* (Certificat X.509).

From:

<https://wiki.sio.bts/> - **WIKI SIO : DEPUIS 2017**

Permanent link:

<https://wiki.sio.bts/doku.php?id=secuapplis>

Last update: **2020/07/26 16:27**

