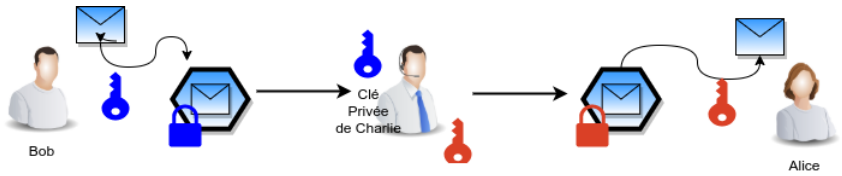
6 Les certificats électroniques

Attaque de l'homme du milieu

— Imaginons qu' Alice souhaite communiquer à Bob sa clé publique.
— L'attaquant Charlie parvient, par un moyen ou un autre, à intercepter les communications entre Alice et Bob.
— Il intercepte la diffusion de la clé publique ;
— Il envoie à Bob sa propre clé publique en se faisant passer pour Alice ;

Attaque :

— L'usurpation fonctionne alors dans les deux sens :
— lorsque Alice signe un message, il le signe avec sa propre clé privée
— lorsque Bob envoie un message chiffré à Alice, il utilise la clé de Charlie.



Les certificats

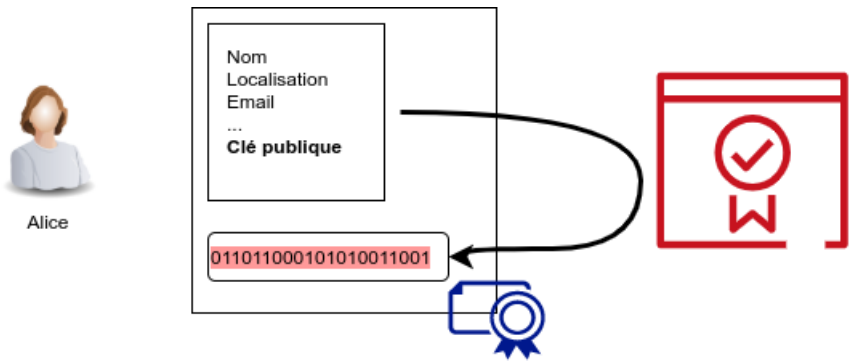
Les certificats électroniques sont une réponse à ce problème de diffusion non sécurisée de la clé publique.
Il y a deux modèles :
— modèle hiérarchique : basé sur des autorités de certification
— modèle réseau : pgp, mail

Autorité de certification

Un certificat met en jeu une autre entité : l'autorité de certification.
Il s'agit d'organismes dûments enregistrés et certifiés auprès des autorités publiques.
Les systèmes d'exploitation et navigateurs web incluent nativement les listes des clés publiques de ces autorités de certification.
Un certificat électronique est un ensemble de données contenant :
— des informations d ?identification (nom, email, ?)
— une clé publique
— une signature des données précédentes obtenue avec la clé privée d'une autorité de certification.

Création du certificat

Lorsque Alice veut diffuser sa clé publique, elle effectue une demande auprès d'une autorité de certification. Celle ci reçoit la clé publique et l'identité d'Alice.
Après avoir vérifié la clé publique et l'identité d'Alice par des moyens conventionnels, elle crée un certificat contenant les données et la signature calculée avec sa clé privée.



Bob souhaite communiquer avec Alice. Celle-ci lui envoie son certificat.
Bob peut alors vérifier l'intégrité du certificat en utilisant la clé publique de l'autorité de certification.
S'il authentifie le certificat, alors il peut utiliser la clé publique qu'il contient pour échanger avec Alice.

Utilisation du certificat

Bob souhaite communiquer avec Alice. Celle-ci lui envoie son certificat.
Bob peut alors vérifier l'intégrité du certificat en utilisant la clé publique de l'autorité de certification.
S'il authentifie le certificat, alors il peut utiliser la clé publique qu'il contient pour échanger avec Alice.