10 – Certificats, gestion de clefs, protocoles sécurisés

Motivation

- en cryptographie symétrique, les échanges de clefs secrètes ne sont pas aisés
- le principe des centres distributeurs de clefs (KDC pour *Key Distribution Center*) a ses limites (*e.g.* Kerberos)
- la cryptographie à clef publique a justement été introduite pour éviter de devoir partager une clef secrète avec son interlocuteur

Mais comment rattacher sûrement une clef publique à son propriétaire ?

- il faut prévenir l'attaque dite de l'homme du milieu (MITM) sans quoi il peut y avoir usurpation d'identité
- chaque participant doit pouvoir vérifier l'authenticité de la clef publique des autres

  à noter que le protocole de Diffie-Hellman, qui vise au partage d'un secret (d'une clef secrète) est lui-même vulnérable à cette attaque

- on a besoin d'un équivalent de la carte d'identité qui elle fait le lien entre la personne et la signature
- c'est le rôle joué par les certificats numériques qui reposent *in fine* sur un tiers de confiance

L'attaque de l'homme du milieu (rappel cours n°6)

Elle porte sur la communication des clefs :

- Bob demande sa clef publique (n,e) à Alice pour lui envoyer sûrement le message M
- Alice envoie (n,e) à Bob
- Melchior intercepte (n,e) et envoie à la place (n',e') à Bob
- Bob chiffre en utilisant à son insu la clef factice (n',e') de Melchior et envoie le message ainsi chiffré C à Alice
- Melchior intercepte à nouveau le message chiffré C et le déchiffre aisément en M …

Melchior pourrait arrêter là les nuisances, mais non :

- Melchior rechiffre M avec (n,e) et le transmet à Alice …

Elle débouche sur les problèmes d'authentification pour éviter l'usurpation d'identité. Les certificats et les chaînes de certification en sont la parade.

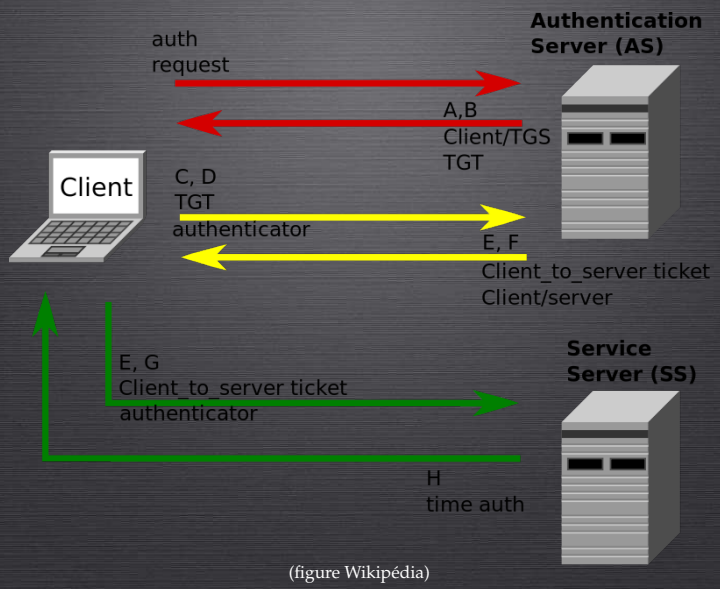
Kerberos, un distributeur de clefs secrètes

- du nom grec de Cerbère (*κέρβεροσ*), gardien des Enfers
- c'est un protocole d'authentification réseau TCP/IP inventé au MIT
- il est basé sur le chiffrement symétrique pour éviter l'attaque MITM
- c'est un système d'authentification sécurisée à tierce personne (TA pour *Trusted Authority*)
- le système partage avec chaque entité utilisateur U une clef secrète K_U
- le tiers de confiance est le KDC (*Key Distributor Center*)
- le fonctionnement est fondé sur un échange de tickets et aucun mot de passe ne transite en clair

Faiblesses :

- attaques par répétition
- attaque des services de datation
- paris pour retrouver les mots de passe
- BD des clefs vulnérable.

KERBEROS : ILLUSTRATION



(figure Wikipédia)

KERBEROS : ÉBAUCHE DU FONCTIONNEMENT

Connexion d'un utilisateur

1. l'utilisateur entre son identifiant et son mot de passe sur sa machine-client
2. le client transforme ce mot de passe en une clef secrète $K_{U/C}$ (chiffrement symétrique)

Authentification du client

3. le client envoie les informations sur l'identité de l'utilisateur au serveur d'authentification (AS) en demandant l'accès à un service
4. l'AS vérifie que le client est dans la BD et si oui, génère une clef secrète par hachage des informations de l'utilisateur et envoie 2 messages au client :
   A. une clef de session $K_{C/TGS}$ avec le TGS (*Ticket-Granting-Service*) chiffrée avec la clef secrète $K_{U/C}$
   B. un ticket TGT (*Ticket-Granting-Ticket*) incluant identifiant client, période de validité du ticket et la clef de session $K_{C/TGS}$ chiffrée avec la clef secrète du TGS
5. à réception le client déchiffre le premier envoi avec la clef secrète $K_{U/C}$ pour obtenir la clef de session $K_{C/TGS}$ pour accès ultérieur au TGS
   (le second message est destiné à être déchiffré par le TGS).
   à présent, le client peut s'authentifier auprès du TGS.

Autorisation du service client (...)

Demande de service du client (...)

ANNUAIRES DE CONFIANCE TRUSTED DIRECTORY SERVICE

Le rôle d'une telle organisation dirigée par Dirk serait de garantir le lien entre le nom d'une personne et sa clef publique :

- Alice demande à Dirk de lui envoyer la clef publique de Bob
- Alice doit faire confiance à Dirk et penser qu'il ne ment pas
- Dirk n'a pas lui-même été abusé par des imposteurs se faisant passer pour Bob
- pour éviter de déplacer le problème, la clef publique de Dirk doit être connue des applications d'Alice devant se procurer des clefs publiques

Mais les failles d'un tel système sont nombreuses :

- confiance : tout le système ne repose que sur l'entière honnêteté de Dirk
- facteur d'échelle : le service d'annuaires risque l'engorgement
- fiabilité : ce service centralisé peut être vulnérable aux attaques d'atteinte à la disponibilité (*denial-of-service*)
- *on line* : impossible d'utiliser un tel service déconnecté
- sécurité : ce service constamment *on-line* doit se prémunir des attaques à distance

Bref, il faut une meilleure idée !

CERTIFICATS

- un certificat numérique certifie une association entre un nom de personne (ou une entreprise, un serveur *etc*) et une clef publique
- il est délivré et signé par une autorité de certification (CA)
- cette autorité use de sa clef privée pour signer un certificat
- on utilise donc sa clef publique pour vérifier la validité du certificat

  Mais qui garantit l'authenticité de la clef publique de l'autorité de certification en question ?

  Réponse : une (autre) autorité de certification ...

  - cela donne lieu au concept de chaîne de certification
  - et aussi à celui de certificat auto-signé
- ainsi, Alice n'aura plus qu'à produire son certificat en cours de validité à toute personne voulant lui écrire ou susceptible de vouloir vérifier sa signature.

Exemples de CA

VERISIGN, CERTISIGN, TERENA, AVAST ... : il en existe beaucoup (des centaines ?)

Certificats : contenu

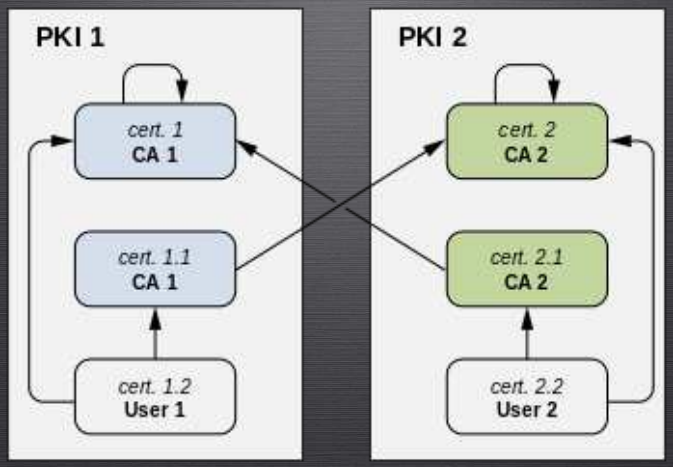
Voici le contenu minimal d'un certificat numérique :

- une clef publique
- l'identité du dépositaire de la clef privée associée
- des dates de validité
- le contexte d'emploi (chiffrement ou signature) associé à la clef publique
- l'identifiant de l'autorité de certification
- la signature du certificat et la description de l'algorithme utilisé

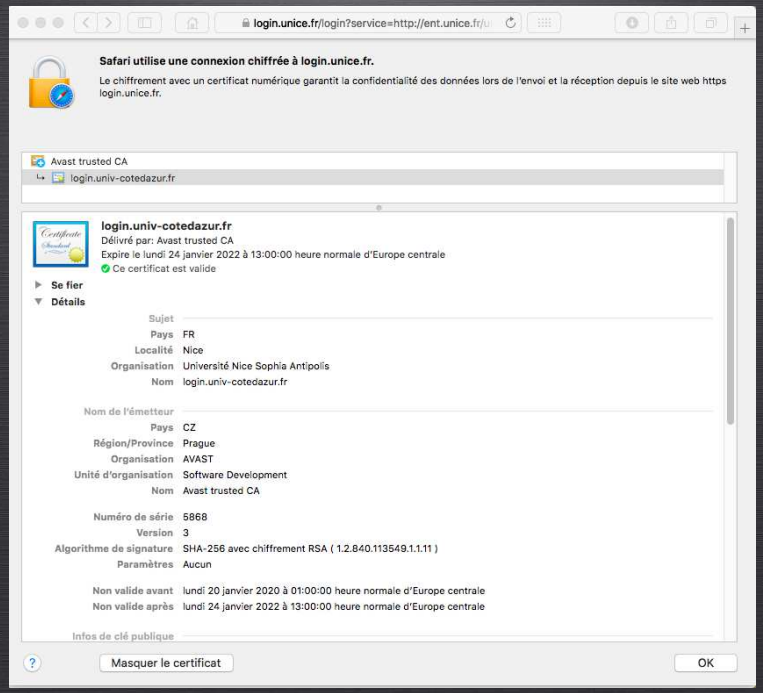
Chaque certificat résulte d'une véritable chaîne de certification :

- un certificat est signé par une CA dont le certificat est signé par une CA ... et ainsi de suite jusqu'à tomber sur un certificat auto-signé
- une autorité de certification qui signe son propre certificat est dite autorité de certification « racine »
- pour augmenter la confiance, ces certificats-racine pourront faire l'objet de certifications croisées

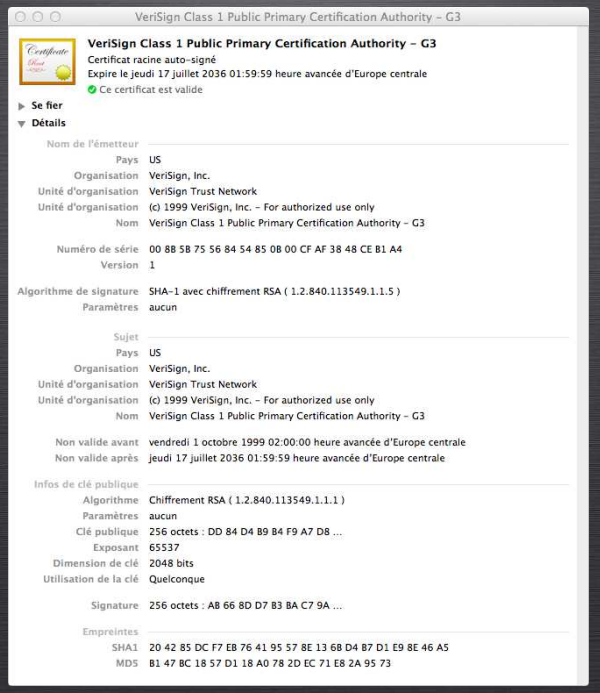
Certifications croisées



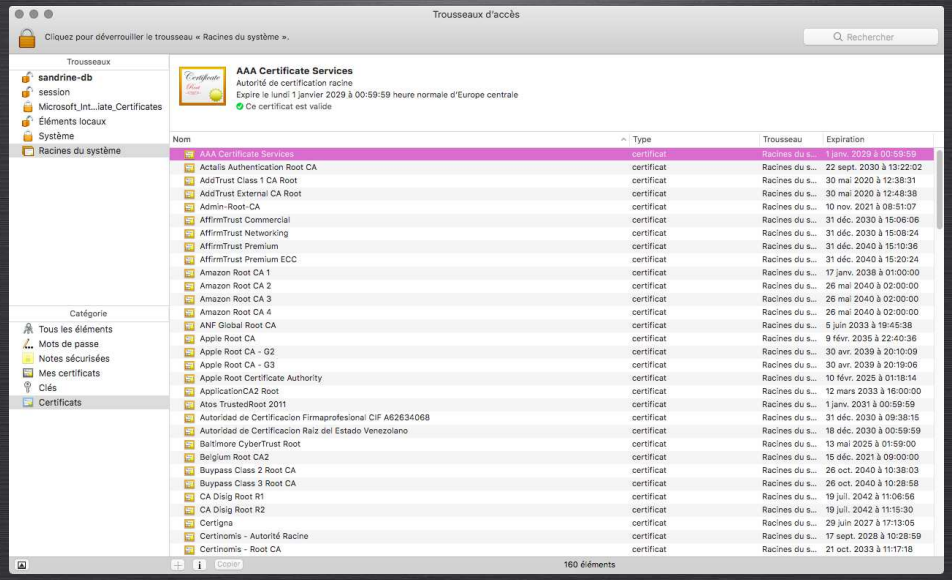
Certificat : exemple d'utilisation par HTTPS



Certificat-racine : exemple



Certificats-racine du système : aperçu



Public-Key Infrastructure (PKI)

- francisé en Infrastructure de Gestion de Clefs (IGC)
- elles permettent de réaliser des échanges sécurisés
- c'est un ensemble de technologies, organisations, procédures et pratiques qui garantissent le bon fonctionnement de la cryptographie - à clef publique -
- le problème de l'authentification entre différentes entités est ainsi résolu

Rôle de la CA dans les PKI :

- émission de certificats à des entités authentifiées
- maintenance, révocation de certificats
- veiller à créer un espace de confiance
- publier par le biais de service d'annuaires
- gestion des clefs, mise en commun, transport des clefs

Emission d'un certificat (*cf.* TP n° 10)

- une entité, Alice, dépose une requête de certificat auprès d'une Autorité d'Enregistrement (*Registration Authority*, RA)
- une entité peut aussi bien être un serveur WEB, un client-messagerie, un équipement réseau *etc*
- cette RA étudie puis transmet la requête de certificat auprès d'une Autorité de Certification (*Certifying Authority*, CA)
- la CA est l'entité juridique et morale d'une PKI
- le certificat qu'elle émet est publié sur un Annuaire (Repository) et éventuellement fourni à Alice
- l'annuaire contient aussi une Liste de Révocation de Certificats (*Certification Revocation List*, CRL)
- l'annuaire est connu par son adresse et son protocole d'accès

Différentes normes existent (en cours d'évolution), chacune définissant son propre format de certificat :

- PKIX pour *Public Key Infrastructure X.509* (`https://en.wikipedia.org/wiki/X.509`)
- SPKI pour *Simple Public Key Infrastructure*
- SDSI pour *Simple Distributed Security Structure*

Messagerie sécurisée

- les messages transitent en clair sur les réseaux, leur confidentialité nécessite un chiffrement
- il existe 2 niveaux de protection : le niveau protocolaire et le chiffrement du contenu des messages
- les protocoles mis en jeu, `smtp`, `pop` et `imap` sont encapsulés par SSL ce qui a pour but de chiffrer les connexions

  le message ne pourra pas être lu pendant l'envoi ou lors de la réception mais le message sera stocké en clair dans la boîte du destinataire et sur les zones de stockage temporaire de tous les serveurs de messagerie impliqués dans son transport

- pour assurer une complète confidentialité, il faut chiffrer le contenu du message lui-même
- c'est le rôle par exemple de S/MIME et de PGP basés sur la cryptographie asymétrique (*cf.* TP n° 11)

Pretty Good Privacy (PGP)

- PGP a été conçu en 1991 pour permettre la messagerie sécurisée
- avant l'avènement des CA, PGP a résolu le problème de la fiabilité sans la hiérarchie inhérente aux PKI
- dans PGP, chaque utilisateur est un peu sa propre CA sans qu'il y ait tout de même autant de CA que d'utilisateurs ...
- PGP propose une notion de fiabilité complète et de fiabilité marginale
- un utilisateur peut signer le certificat d'un autre s'il l'estime de confiance, il n'y a pas de limitation au nombre de signatures d'un certificat
- de fait, les personnes les plus fiables émergent comme gestionnaire en chef de la sécurité ou correspondant fiable : il s'agit donc d'un modèle de fiabilité cumulatif
- ce système est donc basé sur la réputation : certaines personnes sont réputées donner des signatures correctes et les autres utilisateurs leur font confiance lorsqu'elles valident d'autres clefs
- cela dit, le réseau de confiance est assez vulnérable aux tiers indélicats

PGP : certificat

Un certificat PGP comprend, entre autres, les informations suivantes :

- le numéro de version de PGP, celle utilisée pour créer la clef associée au certificat
- la clef publique du détenteur, associée à l'algorithme (RSA, DSA, ...)
- les informations du détenteur
- la signature numérique du détenteur, appelée auto-signature
- la période de validité du certificat
- l'algorithme de chiffrement symétrique préféré pour la clef (CAST, IDEA ou TRIPLE-DES)
- un certificat peut contenir plusieurs identités pour un même détenteur de la clef publique
- les certificats peuvent être signés par des tiers sans que le nombre de signatures ne soit limité
- on évalue aussi la confiance portée aux signatures

Les certificats `X-509` sont également reconnus par PGP.

PGP : chiffrement

- PGP combine le meilleur de la cryptographie à clef publique et à clef privée : c'est un système hybride
- PGP crée une clef de session à usage unique, elle provient d'un nombre aléatoire
- on applique un chiffrement symétrique au message (compressé) à chiffrer avec cette clef de session
- à présent, on chiffre la clef de session avec la clef publique du destinataire
- le tout (message chiffré + clef de session chiffrée) est transmis au destinataire
- le déchiffrement coule de source ...
- les clefs sont stockées chiffrées sur le disque dur de l'utilisateur dans 2 fichiers : l'un est destiné aux clefs publiques, l'autre aux clefs privées
- ces fichiers s'appellent des trousseaux de clefs

L'utilitaire de sécurisation de canal SSH est lui aussi basé sur de la cryptographie hybride. L'authentification est dite TOFU pour *Trust On First Use* (*cf.* TP n° 10).

A suivre ...