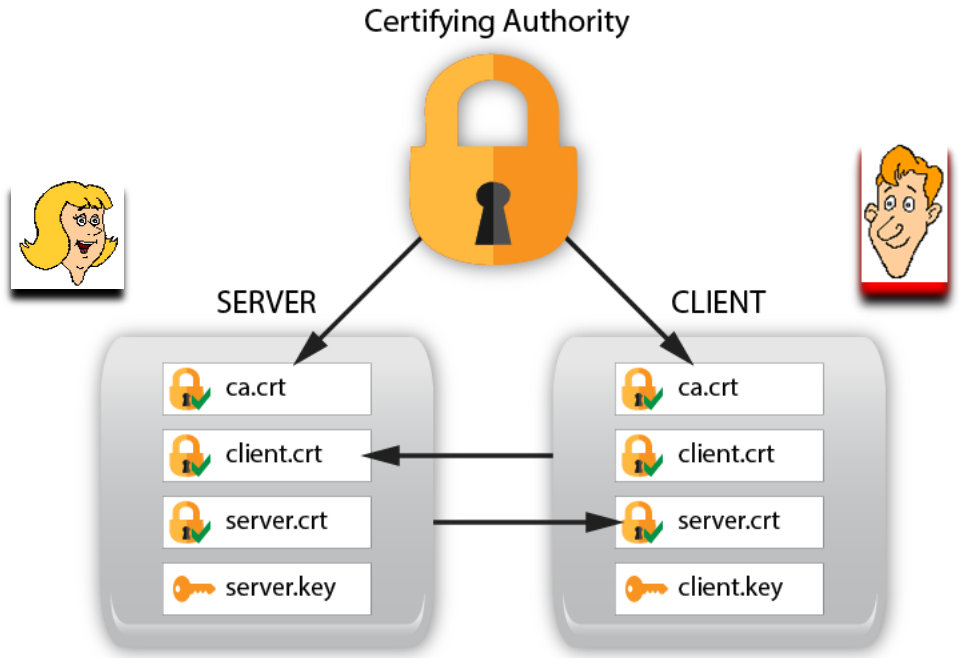
Travaux dirigés –TD
PKI et services de sécurité

Exercice 1 : Génération d'un certificat x509.

On suppose qu'Alice veut obtenir un certificat (**server.crt**) pour son serveur auprès d'une autorité de confiance (AC). On suppose que le client Bob veut aussi obtenir un certificat (**client.crt**) auprès de la même autorité de confiance (AC) pour l'utiliser quand il se connecte au serveur d'Alice. L'autorité de confiance a généralement un certificat appelé auto-signé (**ca.crt**) qui doit être utilisé par les clients pour la vérification des certificats serveurs et par ces derniers pour vérifier les certificats des clients.



Le problème, avec la cryptographie à clef publique est de s'assurer qu'on a bien les bonnes clefs publiques. L'une des solutions consiste à utiliser des certificats. Un certificat contient :

- Une identité (adresse email, URL d'un serveur, adresse IP d'une machine, . . .).
- Une clef publique associée à cette identité.
- Une signature des deux éléments ci-dessus par une autorité de certification

Dans cet exercice nous voulons modéliser les différents échanges entre les demandeurs de certificats et l'autorité de confiance. Pour ce faire, nous supposons que le serveur, le client et l'AC peuvent potentiellement utiliser un certain nombre de méthodes cryptographiques, qui sont décrites dans le tableau suivant :

M	Message contenant : nom, clé publique, adresse, email
K_c K^{-1}_c	Clé publique du client Clé privée du client
K_S K^{-1}_S	Clé publique du serveur Clé privée du serveur
K_{AC} K^{-1}_{AC}	Clé publique de l'autorité de confiance Clé privée de l'autorité de confiance
SHA	Fonction de hachage SHA-256
Sign	Signature numérique avec RSA
Vérif	Vérification de la signature numérique avec RSA

1. Expliquer comment peut-on obtenir un certificat pour sa clé publique sans divulguer sa clé privée ?
2. Pour obtenir un certificat le serveur commence par envoyer une requête de certification signée à l'autorité de confiance. Modéliser cette requête.
3. Pour obtenir un certificat le client envoie une requête de certification signée à l'autorité de confiance. Modéliser cette requête.
4. L'autorité de confiance doit, après vérification des informations dans les requêtes, signer les requêtes de certifications. Modéliser la signature des deux requêtes (serveur et client).
5. Expliquer comment le client peut vérifier la validation du certificat du serveur. Modéliser le processus.
6. Expliquer comment le serveur peut vérifier la validation du certificat du client. Modéliser le processus.
7. Quel protocole déployé à grande échelle de nos jours utilise le système d'autorités de confiance ?

Exemple d'un message échangé :

Si Alice souhaite signer le hash de son message avec sa clé privée, elle transmettra par exemple : Sign $_K{}^{-1}$[SHA(M)].

Application numérique

La clé publique RSA du serveur (n_s=221,e_s=5) et sa clé privée est d_s=77.
La clé publique RSA du client est (n_c=91,e_c=5) et sa clé privée est d_c=29.
La clé publique RSA de l'autorité est (n_{ac}=299, e_{ac}=5) et sa clé privée est d_{ac}=53.

Nous supposons que le contenu de la requête de certification envoyée par le serveur est M1=s||221||date => M1= 115 221 17102019 avec 115 est le code ascii de la lettre « s »

Nous supposons que le contenu de la requête de certification envoyée par le client est M2=c||91||date => M2= 99 91 17102019 avec 99 est le code ascii de la lettre « c »

L'algorithme de hachage appliqué sur les données numériques fonctionne de la manière suivante : on divise les éléments de données en groupes de deux chiffres. Ensuite, on calcule la somme des groupes. Exemple: si le message est 4432, la somme résultante sera 76 car 44+32=76). La valeur de hachage du message complet M1 est calculée en additionnant les valeurs de hachage de chaque élément de données et en appliquant l'opération de modulo 91.

Calculer les valeurs des opérations cryptographiques (signature et vérification) dans les questions 2 à 6.

Exercice 2 : Chaînes de certification

Alice reçoit le certificat de Bob signé par l'autorité de certification TrustSign. Malheureusement Alice ne connaît pas la clef publique de TrustSign. Il se trouve que cette clef (i.e., clef publique de TrustSign) est certifiée par l'autorité de certification VeriSign (dite racine) dont Alice a entièrement confiance.

a) Dessinez le graphe hiérarchique des différents certificats, en indiquant à chaque fois les clés authentifiées.
b) Dessinez le graphe de la chaîne de confiance qui en résulte. Comment Alice pourra-elle vérifier le certificat de Bob ?
c) Que pouvez-vous dire de la validité de la clef contenu dans le certificat de Bob ?