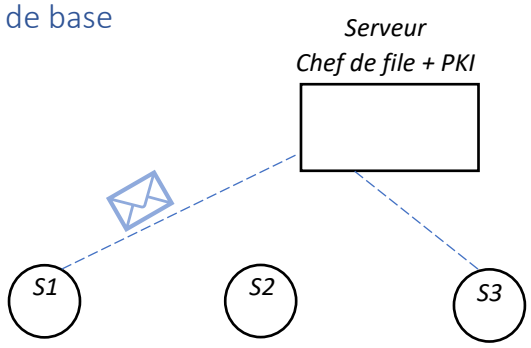
Projet

Principe de base



Le nombre de station est connu d'avance. Il faut être capable de générer *n* stations. (Les identifiants des stations sont des entiers).
Chaque station aura à communiquer avec d'autres stations.

Chaque station sait communiquer directement seulement avec le serveur. Le serveur est un médium de communication. *Exemple :* la station 1 envoie un message au serveur pour communiquer avec la station 3. Le serveur sert donc de relai.

Une station a deux threads :

- Thread envoi
- Thread réception

Mais il est également possible d'utiliser une file MQTT/AMQP.

Serveur de distribution de certificats

Tous les certificats ont eu racine. La racine est le certificat auto-signé généré par le serveur. La première instruction est donc l'envoi à toutes les stations de ce certificat autosigné.

Le certificat racine est mis en dur dans les stations. Il est possible de générer le certificat racine en dur sur chaque station (par un copier/coller).

Propriétés : *(DEMANDER PLUS DE DETAILS)*

- Certificats de type X509
- ECDSA 248
- Asymétrique : ECDS
- Symétrique : AES128

Communication entre les différentes stations

Le chef de file rend service aux stations et renvoie les messages sans les déchiffrer. Les en-têtes ne sont pas chiffrées.

Une station qui démarre :

- A les moyens de communication avec le serveur.

- Génère un certificat qu'elle demande à la racine de signer. Chaque station demande un certificat à la PKI avec retour à la station. Cet échange ne se fait pas en clair. Attention, la station doit générer sa clef, le serveur ne doit pas tout générer.

INFO

Les échanges chiffrés : les échanges symétriques sont plus légers que les échanges asymétriques. Il faut donc éviter d'utiliser les échanges asymétriques. Il est cependant parfois nécessaire d'avoir des échanges asymétriques. *Exemple* : Quand on établit un secret obligation d'utiliser de l'asymétrique.

Les premiers messages sont en clair quand une station souhaite commencer à parler à une deuxième station. Le certificat n'est échangé qu'au besoin. La deuxième station lui renvoie son certificat. Le chiffrement se fait par la suite.

Dead line

Le projet est à faire à deux. Rendre le projet la semaine de cours en avril. Les soutenances seront cette semaine-là également.