Projet RT802

2022-2023

On considère une PKI constitué d'un serveur génère une paire de clés privée/publique. Avec la clé publique, il produit un certificat X509 (qui sera le certificat racine) autosigné. Ensuite ce certificat est embarqué d'office chez tous les équipements qui vont é changer dans l'éco-système.

On considère un ensemble d'équipements (nœuds) qui vont échanger des informations d'une façon sécurisée.
Tout nœud (qui appartient au réseau) doit générer une paire de clés (publique et privée). Il envoie la clé publique au serveur PKI pour obtenir un certificat signé par la PKI. L'échange entre la PKI et le nœud est chiffré en asymétrique.

On s'intéresse à la communication entre deux nœuds A et B à l'initiative de A. A demande le certificat de B à B qui le lui envoie. A vérifie que le certificat est bien signé par la PKI. Ensuite A génère un secret qu'il va partager avec B. Ce secret servira de clé symétrique aux échanges entre A et B en utilisant AES-128.

Quand un nœud A envoie une chaine de caractère à un autre nœud B, il fait avec un chiffrement symétrique et au retour B lui renvoie son message (chiffré également en chiffrement symétrique).

Du point de vue pratique, le serveur PKI est un serveur qui centralisera les échanges entre tous les nœuds. Chaque nœud va ouvrir une socket avec le serveur et quand il a besoin de communiquer avec un autre nœud il enverra son message au serveur qui relayera à la destination. Le serveur fera office de relais sans déchiffrer le message de l'émetteur.

Ecrire un code avec 3 noeuds et un serveur PKI.