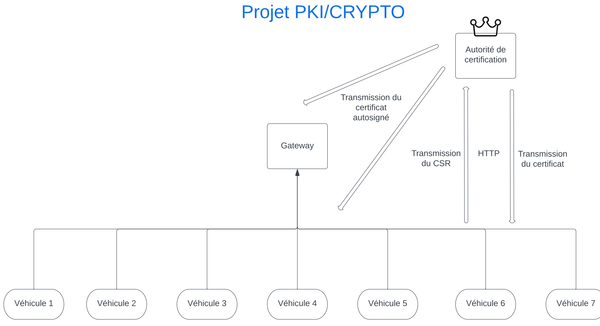
Projet PKI/CRYPTO



A - Opérations de génération des paires de clés

1

Autorité de certification

1- l'autorité de certification génère une paire de clé (Privé et Publique)

2 - L'autorité de certification génère une demande de signature de sa clé publique et envoie sa demande à lui même

3 - L'autorité de certification signe la clé publique présentée dans la demande avec sa clé privée

4 - Le certificat autosigné X509 de l'autorité de certification est généré

5 - La clé privée de l'autorité de certification est gardée en interne et la clé publique sous forme de certificat X509 est distribuée à toutes les autres entités

2

Objets

1- L'objet génère une paire de clé (Privé et Publique)

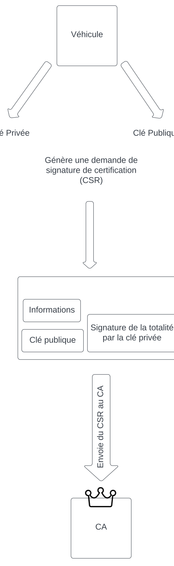
2 - La clé privée de l'objet est gardée en interne

3 - L'objet génère une demande de signature de sa clé publique et envoie sa demande à l'autorité de certification

4 - L'autorité de certification signe la clé publique de l'objet présentée dans la demande avec sa propre clé privée et le retourne à l'objet sous forme de certificat X509

B - Opérations sur les objets

1



C - Opérations du CA

2

3

Attends de recevoir une demande de signature de certificat (CSR) de la part d'un objet

D - Opérations de la gateway