TP4 : Un petit devoir sur l'IoT

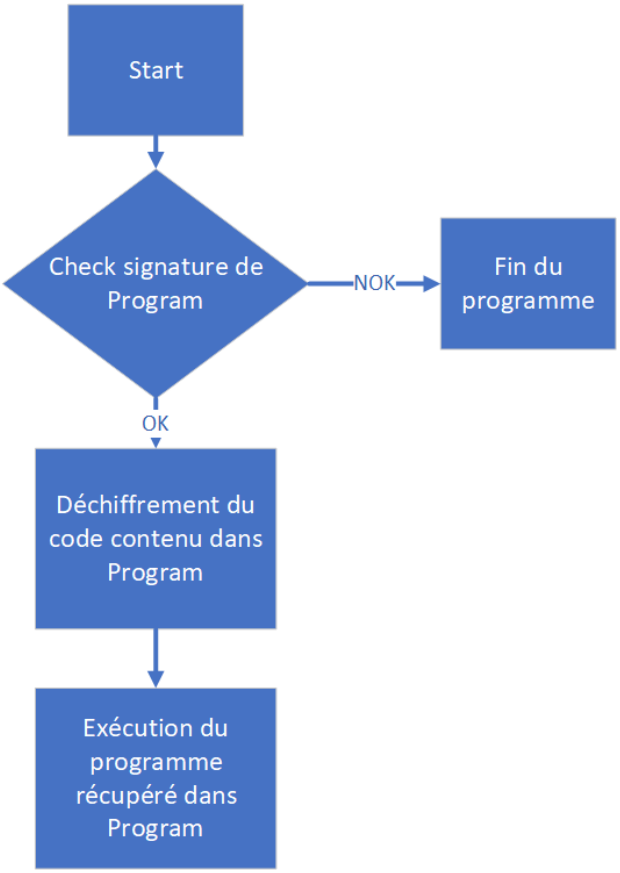
Ce devoir très simple est là pour vous permettre de mieux comprendre, en pratique, la sécurité dans le monde de l'IoT et vous montrer que ce domaine n'est pas si différent de la sécurité que nous avons déjà vue ensemble. Le C++ est le langage le plus utilisé dans l'IoT (embarqué oblige) néanmoins je vous laisse le choix du langage parmi la liste habituelle (JAVA, Golang, NodeJS (Typescript), Python, C#).

Vous devez me rendre ce petit travail pour le **Lundi 11 Décembre à 12H15** via la GitHub qui sera créé pour cela.

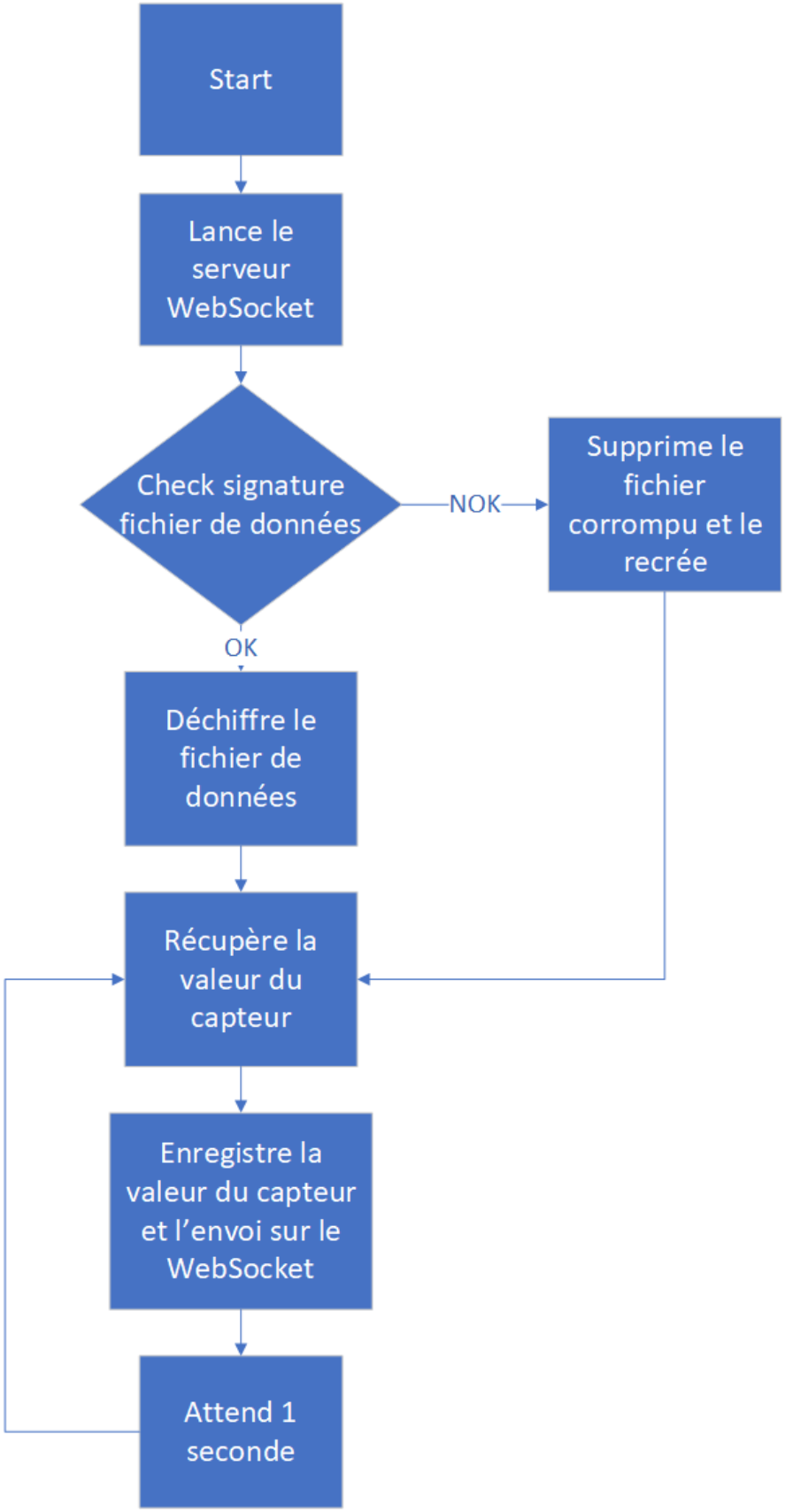
Vous allez me réaliser un petit prototype de dispositif IoT comme si votre PC en était un. Vous simulerez uniquement les stockages et la communication. Pour les besoins de la simulation, vous aurez à créer trois fichiers/programmes :

- Startup : un simple programme qui va jouer le rôle du boot de votre dispositif
- Program : un fichier chiffré et signé simulant le stockage du code principal de l'application
- Data : le fichier simulant le stockage d'enregistrement des données

Voici le diagramme expliquant précisément ce que fait le fichier Statup quand il est lancé :



Voici le diagramme expliquant précisément ce que fait le script contenu dans Program quand celui-ci est lancé par le programme Startup :



Consignes

Évidemment vous devez utiliser les algorithmes de chiffrement AES-128 bits et Elliptic-Curve (il existe plein de librairies pour cela).

Vous devez rechiffrer le fichier de données et le fichier du programme avant l'extinction de celui-ci (pensez à intercepter le Ctrl+C).

Pour générer la signature du programme principale vous pouvez générer son hash (SHA-256) et chiffrer votre hash avec votre clé privée Elliptic-Curve.