

Sécurisation des communications 4G LTE par renouvellement distant des certificats

- **Nom de l'Encadrant** : Durand Gabriel
- **Établissement** : Socotec Monitoring

I. Introduction

• Contexte :

Notre société utilise des modules 4G LTE pour envoyer des données.
Ces modules utilisent des certificats pour chiffrer leurs communications.
Aujourd'hui les certificats ne sont pas changés ce qui pose un problème de sécurité.

• Objectif :

Les étudiants devront développer un système de mise à jour de certificats à distance.
Les modules n'étant pas accessibles une fois installés, les certificats doivent être mis à jour de manière automatique et autonome.
L'environnement embarqué très basse consommation oblige à avoir un microcontrôleur (μ C) qui a une très petite RAM, plus petite que la taille d'un certificat. Il faudra donc développer une sauvegarde automatique dans le module 4G sans passer par le μ C.
La génération de certificat a déjà été réalisée cependant il faudra développer le système d'envoi au module.

• Technologies Utilisées :

C++, python, Js, serveur AWS, μ C ARM Cortex M0, module BG96.

II. Résultats Attendus

• Livraisons :

Les étudiants devront fournir un programme pour le module BG96 avec détection de péremption de certificat, requête de récupération d'un nouveau ainsi que la sauvegarde en FLASH.
La partie serveur devra aussi être implémenté pour générer le nouveau certificat pour le module et l'envoyer.

• Impact :

Ce projet est une brique d'un projet plus grand qui est développé en interne. Les étudiants pourront découvrir l'entièreté du projet et comprendre où il se situe dedans.

Contacts

Durand Gabriel → gabriel.durand@socotec.com