Création d'une infrastructure à clé publique (PKI) pour cybervigile OT

Auteurs : Redouane BENABDALLAH – Elie WILHEM – Hugo MAIORANA

CONTEXTE ET OBJECTIF

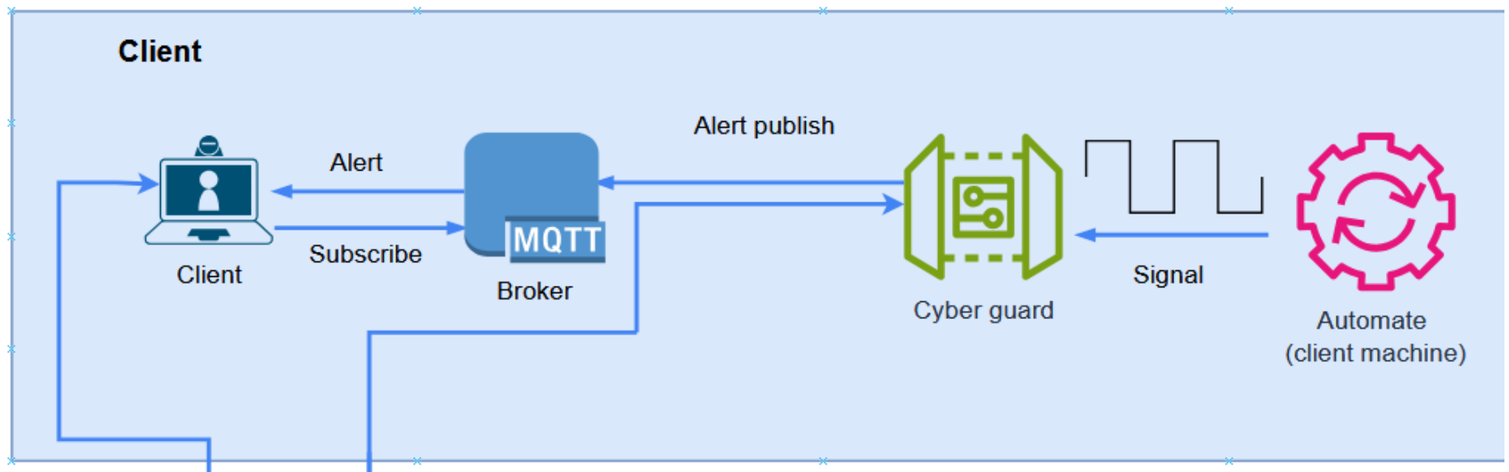
AIoTrust est une start-up française spécialisée en cybersécurité pour les systèmes industriels (OT). Elle conçoit des solutions de supervision sécurisée, destinées à protéger les installations critiques des Opérateurs d'Importance Vitale (OIV). Ses dispositifs embarqués, appelés *cybervigiles*, sont capables de collecter des données sur le terrain et d'agir en réponse à des anomalies ou menaces détectées.

Dans le cadre de la pré-industrialisation des cybervigiles, AIoTrust souhaite renforcer leur sécurité en les intégrant dans une infrastructure cloud robuste, en vue d'obtenir la Certification de Sécurité de Premier Niveau (CSPN) délivrée par l'ANSSI.

Cette infrastructure doit permettre :

- Le provisioning et l'enrôlement sécurisé des cybervigiles
- La mise à jour logicielle Over-The-Air (OTA)
- La signature des configurations
- La gestion des secure boots
- Le stockage des métadonnées critiques (clés publiques, identifiants).

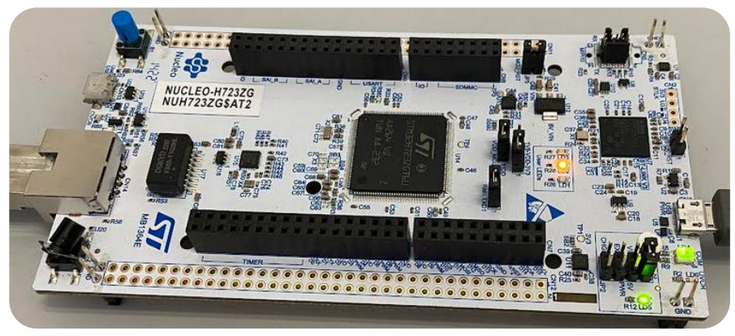
MÉTHODES ET DÉVELOPPEMENTS



Le projet s'est articulé en plusieurs étapes. Il a débuté par une étude comparative des solutions PKI et cloud, selon des critères tels que la souveraineté, l'adaptabilité et les fonctionnalités offertes. Cette analyse a permis de dresser un tableau comparatif et de dégager plusieurs podiums en fonctions des critères considérés comme les plus importants.

La solution retenue, EJBCA, a ensuite été déployée pour mettre en place l'infrastructure PKI. En parallèle, une API de gestion des cybervigiles a été spécifiée puis implémentée. Un service d'authentification basé sur Keycloak a été intégré afin de sécuriser les accès à l'infrastructure. Enfin, un développement côté embarqué a permis d'implémenter un client HTTP et un client MQTT sur une carte STM32, facilitant la communication avec l'infrastructure cloud.

RÉSULTATS ET CONCLUSION



Les composants prévus ont été développés et intégrés avec succès : la PKI (EJBCA), l'API de gestion, le service d'authentification (Keycloak), ainsi que le stockage des métadonnées. L'infrastructure a été entièrement automatisée à l'aide de Docker, répartie sur six conteneurs, ce qui facilite le déploiement et la maintenance.

Un client HTTP a été implémenté sur la carte STM32, assurant la communication avec l'API. Le client MQTT, initialement non prévu dans le périmètre du projet, n'a pas pu être finalisé par manque de temps, sans que cela nuise aux objectifs fixés.

MOTS-CLÉS : PKI – Provisioning – Enrolment – API REST – Infrastructure – Oauth 2.0