**Projets communs aux cours de l’UE7**

Ce document décrit les sujets proposés dans le cadre des cours de l’UE7, à savoir

* Internet des objets et plateformes à large échelle
* Web services
* Plateformes d’objets communicants

L’objectif est de développer un ou plusieurs projets dans lesquels vous utiliserez les compétences acquises dans les différents modules de la licence.   
En particulier chaque projet doit mettre en œuvre des technologies enseignées dans les modules de vos trois enseignants mais pas uniquement.

Les développements que vous réaliserez devront concerner les cours de :

- objets et protocoles de Mme Belleudy

- architecture et web service de M. Ferry

- protocoles IoT, standards er sécurité de Mme Peraldi

La gestion de projet devra suivre les préconisations du cours gestion de projet de Mme Barisic et les outils étudiés dans le cours de M. Cremoni.

**Organisation**

- Il y aura 3 groupes de 3 étudiants donc 3 projets menés en parallèle.

- Chaque étudiant doit contribuer au moins à deux des cours concernés par les projets.

- la gestion du projet devra être conforme aux préconisations données lors du cours gestion de projet et utilisera les outils de gestion de projet.

Etudiants : Saxemard, Pillar, Pascucci

Sujet 3 - - **Contrôle d'accès de bâtiments** :

Objectif s’assurer de l’identité des personnes présentes sur le site. Utilisation des technologies RFID active ou Bluetooth Low Energy, pour faire du comptage et du contrôle d’accès à la volée, sans qu'aucune action ne soit requise. Les badges ou téléphones sont automatiquement détectés dans un périmètre. Le but est de gérer les autorisations d’accès, d'avoir un état d'occupation des lieux et d’alerter en cas de tentative d’intrusion.

Cela suppose

- l'utilisation de différentes technologies telles que RFID, BTLE, Wifi pour la collecte des capteurs,

- De mettre en place une infrastructure de collecte et de gestion des données collectées

- De développer des services pour la configuration et la gestion du mécanisme de contrôle d’accès ainsi que des actions particulières.

Matériel identifié disponible à l’IUT :

* TV pour affichage
* Carte rfid
* Téléphone
* Serrure connectée (voir si lecteur rfid intégré)
* RPI
* Lecteur RFID
* Caméra de vidéo surveillance
* M5Stick-C

**Résultat et livrables attendus**

Des scénarios d’usages clairement identifiés

* Une architecture logicielle matérielle claire
* Des POC qui démontrent ces scénarios,
* Un dépôt git qui contient tous les éléments permettant la reproductibilité de ces scénarios
* Un suivi de projet permettant d’identifier le travail de chacun

Définition du scénario : Banque

Scénario 1 : pour la tentative d’intrusion :

Fixation d’heure d’entrée et/ou sortie du bâtiments (exp : 7h30 – 20h), si quelqu’un essaie de s’introduire dans la banque en dehors de ces horaires prédéfinis, l’alarme sonne et prévient la sécurité directement via l’alarme préconfigurée.

Scénario 2 :

Si une personne arrive devant la porte avec le badge de quelqu’un d’autre et qu’il se trompe à 2 reprises de code au niveau de la serrure, l’alarme sonne…

Scénario 3 ? : Utilisation d’une caméra de vidéosurveillance destinée à la sécurité qui va permettre de visualiser en temps réel ce qu’il se passe dans la banque.

Utilisation d’une base de données qui va collecter les informations des tag rfid (code du tag et leur appartenance) et les informations de la personne (nom, prénom, fonction, code du tag auquel il appartient), les codes d’ouverture de la serrure de chaque employé de la banque.

Scénario 4 :

Service calcul visage

Service agenda

Service configuration agenda

Service détection personne de type message

Doc pour les messages