**Contexte, Présentation et Critique du Projet PRJ1401**

**Contexte**

Dans une ère menée par la technologie, les établissements se tourne vers des ressources de sortes à optimiser l’expérience des étudiants et des professeurs. Dans ce cadre, l’Université Bretagne Sud, dans sa démarche pour la réalisation d’un campus connecté (“***campusco***”), souhaite mettre en place des casiers connectés qui “permettront aux usagers du campus de faire du « click and collect » entres usagers ou simplement de la consigne.”

**Présentation**

C’est dans ce contexte que le projet de mettre en place un système de **casiers intelligents** permettant aux étudiants et aux enseignants de déposer et de récupérer des objets de manière simple, rapide et sécurisée.

L’objectif est de proposer une **solution automatisée et connectée** qui facilite l’échange de matériel entre les usagers du campus, tout en garantissant un accès contrôlé et une gestion efficace des espaces de stockage. Ce dispositif offrira une **expérience fluide et intuitive**, où chaque utilisateur pourra accéder à un casier via un système d’identification sécurisé.

Ce projet s’inscrit dans une démarche d’**innovation technologique et d’optimisation des infrastructures universitaires**. En plus de moderniser la logistique sur le campus, il apporte une solution fiable et ergonomique qui répond aux besoins des étudiants et du personnel universitaire. Son intégration au sein de l’établissement marque une avancée significative vers un environnement plus **intelligent, sécurisé et connecté**.

Critique du projet

**Analyse des projets similaires**

Plusieurs initiatives de casiers intelligents ont déjà été mises en place dans différents contextes. Ces projets, bien qu’innovants, présentent certaines limitations qui nous permettent d’identifier les améliorations et les adaptations nécessaires pour notre propre système.

**1. Amazon Locker**

Ces casiers sont conçus pour les livraisons e-commerce d’Amazon. Ils permettent aux clients de récupérer leurs commandes en saisissant un code reçu par email ou via l’application Amazon. Ce modèle est optimisé pour le commerce en ligne et fonctionne de manière entièrement automatisée.

* **Points positifs**
* Solution robuste et éprouvée, utilisée à grande échelle.
* Interface intuitive et simple pour l’utilisateur.
* Sécurisation efficace des colis grâce à une gestion automatisée.
* **Limites**
* **Solution propriétaire** exclusivement dédiée aux services Amazon, ne pouvant être adaptée à d’autres usages.
* **Absence de flexibilité** pour une utilisation académique ou communautaire.
* **Accès restreint** aux seuls clients Amazon, ce qui en fait un système fermé.

**2. Smart Lockers de l’Université de Californie (UC Davis)**

Ce projet universitaire propose des casiers connectés permettant aux étudiants d’emprunter ou de retourner du matériel (ordinateurs, outils de laboratoire, livres, etc.). L’accès aux casiers se fait via un code ou une carte d’étudiant, ce qui permet une gestion semi-automatisée du matériel.

* **Points positifs**
* **Adapté au milieu universitaire**, facilitant le prêt et le retour d’équipements.
* **Accès contrôlé** via une carte étudiante, renforçant la sécurité.
* **Simplicité d’utilisation** pour les étudiants et le personnel universitaire.
* **Limites**
* **Fonctionnalités limitées** : le système ne permet que le stockage et la récupération de matériel sans intégration avancée avec d’autres services numériques.
* **Manque d’interopérabilité** : ne propose pas d’intégration avec des services externes pour une gestion plus centralisée des ressources universitaires.

**3. Casiers connectés de l’Université de Lille**

L’Université de Lille a introduit un système de casiers intelligents financé par la Contribution Vie Étudiante et Campus (CVEC). Ces casiers sont destinés au prêt de matériel sportif, permettant aux étudiants d’accéder aux équipements via un système automatisé.

* **Points positifs**
* **Projet universitaire en France**, prouvant la faisabilité du concept dans un contexte académique national.
* **Solution pratique** pour la gestion du prêt de matériel sportif.
* **Financement institutionnel**, favorisant l’adoption et l’accessibilité.
* **Limites**
* **Capacité limitée** : le nombre de casiers ne permet pas de répondre à une forte demande.
* **Utilisation restreinte** uniquement pour le matériel sportif, alors que d’autres usages pourraient être envisagés (prêt de matériel informatique, stockage temporaire, etc.).
* **Absence de gestion avancée des accès** pour permettre une plus grande flexibilité d’utilisation.

**Ce que notre projet apporte en plus**

En analysant ces initiatives, notre projet vise à combler les lacunes observées et à offrir une solution plus polyvalente et adaptée aux besoins des usagers du campus.

* **Flexibilité d’usage** : Notre solution ne se limite pas à un domaine spécifique (sport, matériel informatique, commerce), mais permet une utilisation variée (consigne, échanges entre étudiants, dépôt sécurisé).
* **Interopérabilité avec d’autres systèmes** : Grâce à une connexion à une base de données centralisée, notre système peut s’intégrer avec d’autres services numériques du campus (gestion des étudiants, accès aux bâtiments, etc.).
* **Meilleure gestion des accès** : L’utilisation de l’authentification par carte NFC permet un accès rapide et sécurisé, évitant les contraintes des codes ou des applications tierces.
* **Optimisation des ressources** : Contrairement aux projets existants qui peuvent être limités par leur nombre de casiers, notre approche prévoit une gestion intelligente des disponibilités et un modèle évolutif pouvant s’adapter aux besoins réels du campus.

**Analyse des besoins**

***Analyse***

* **Système de verrouillage et de déverrouillage automatique des portes** :

La porte du casier doit s’ouvrir automatiquement grâce à un système de **loquets électriques discret** qui offre une sécurité et une ouverture rapide.

* **Ecran LCD** :

Il permet d’afficher des informations concernant l’ouverture et la fermeture de la porte (verrouillage et déverrouillage).

* **Système d’authentification** (**NFC**) :

Ce système permet de sécuriser les casiers. Avec celui-ci l’utilisateur pourra s’authentifier grâce à un **badge magnétique** afin de récupérer ou de déposer son colis ce qui garantit ainsi le fait que seuls les utilisateurs autorisés puissent accéder au casier afin d’éviter les vols.

* **Connexion** **au réseau de l’UBS** :

La connexion au réseau de l’Université Bretagne Sud (UBS) permettra au casier d'être connecté à Internet et aux serveurs locaux.

***Exemples de scénario d’utilisation : Prêt d’un PC par la DSI à un étudiant***

*Contexte* : Un étudiant a besoin d’un PC portable pour un projet, et demande à la DSI de lui en prêter un via un casier intelligent.

***Déroulement*** :

* **Demande de l’étudiant (indépendant de notre projet)**
  + L’étudiant effectue une demande de prêt sur la plateforme universitaire.
  + La DSI valide la demande et attribue un PC à l’étudiant.
* **Dépôt du PC par la DSI**
  + Un agent de la DSI place le PC dans un casier disponible.
  + Il associe ce casier au badge NFC de l’étudiant via l’interface de gestion.
  + L’étudiant reçoit une notification l’informant que son PC est prêt à être récupéré. (Indépendant de notre projet)
* **Récupération du PC par l’étudiant**
  + L’étudiant se rend au casier et **scanne son badge NFC** sur le lecteur.
  + Le casier s’ouvre automatiquement.
  + Il prend le PC et referme la porte.
  + La DSI supprime l’accès au casier à l’étudiant.
* **Retour du PC**
  + Une fois l’utilisation terminée, la DSI lui attribue un casier
  + L’étudiant retourne le PC en allant au casier qui lui est attribué.
  + Il **scanne à nouveau son badge NFC**, ouvre le casier et replace l’ordinateur.
  + L’agent de la DSI peut ensuite récupérer le matériel ou le réattribuer à un autre étudiant si nécessaire.

**Spécifications Techniques**

1. ***Composants Matériels***

* **Microcontrôleur** : ESP32 Devkit v4
* **Système de verrouillage** : Loquet électromagnétique
* **Module NFC** : Lecteur NFC DFRobot
* **Interface utilisateur** : Écran LCD + adaptateur I2C
* **Alimentation** : 5V/12V selon les composants

1. ***Fonctionnalités***

* Identification des utilisateurs via **badge NFC**.
* Contrôle d’accès aux casiers via **une connexion entre le lecteur et l’ESP32 pour vérifier l’identité de l’utilisateur**.
* Affichage **dynamique** des informations sur **écran LCD**.
* Connexion au réseau de l'UBS via **Wi-Fi ou Ethernet.**

**Schéma d’Architecture**

L’architecture comprendra une **interface externe** qui définit **la partie visible par l’utilisateur** et une **interface interne**, plus important qui montrera les **connexions entre les différents composants.**

***Interface externe***

L’interface défini ci-contre correspond à l’apparence visible du casier intelligent pour les utilisateurs. Voici une explication des éléments présents :



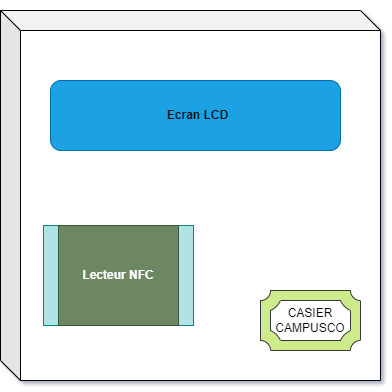
Interface externe du casier



Interface

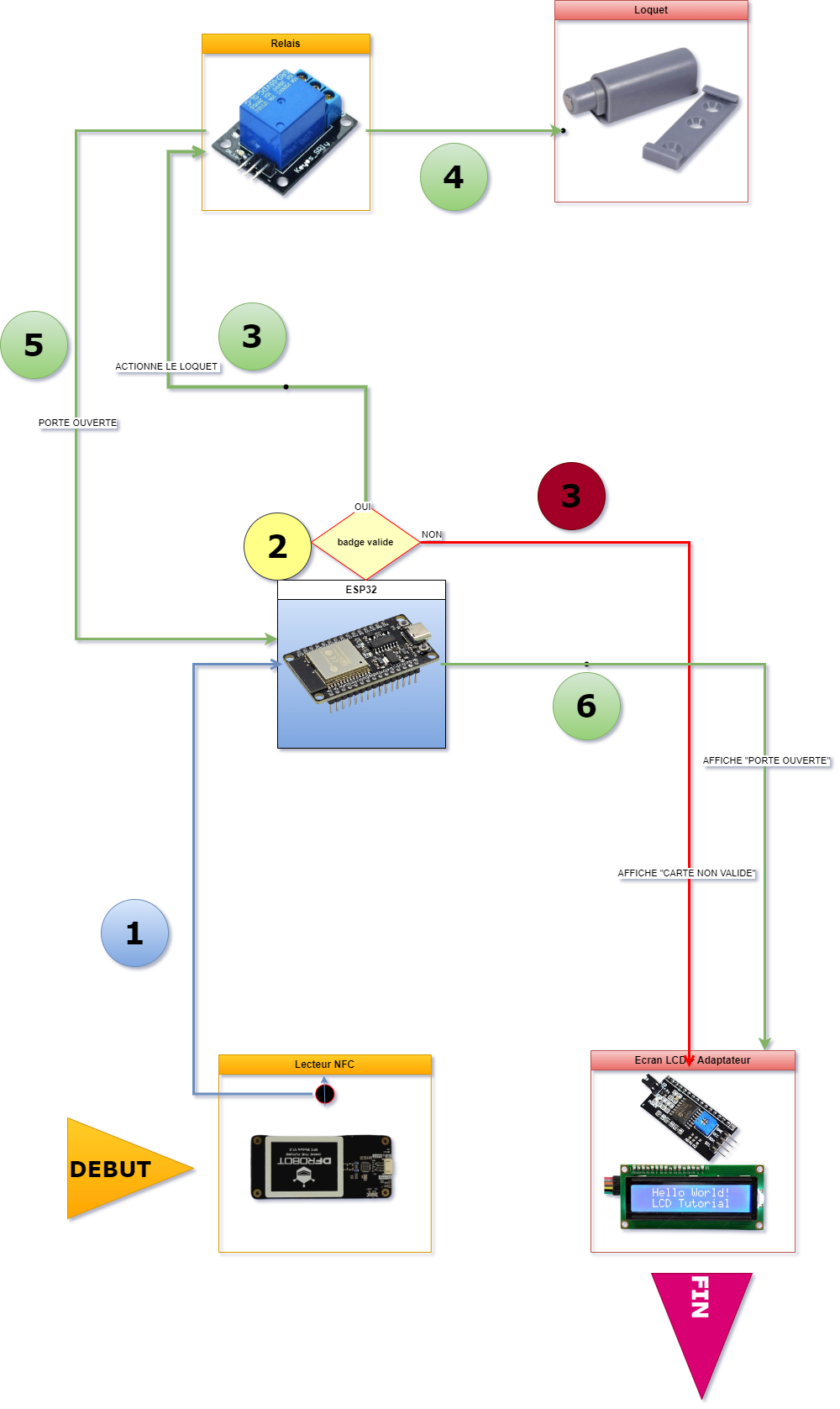
externe

du casier



* **Écran LCD** (en bleu)
  + - Permet d’afficher des instructions et des messages aux utilisateurs (ex : "Scannez votre badge", "Accès autorisé", "Erreur, badge inconnu").
  + Peut afficher des informations sur l’état du casier (libre/occupé).
* **Lecteur NFC** (en vert)
  + Permet aux utilisateurs de scanner leur badge pour s’identifier.
  + Communique avec l’ESP32 pour valider l’accès au casier.
* **Casier Campusco** (en Jaune et noir)
  + Indique le nom du casier.

***Interface Interne***



Interface

interne

du casier

**Analyse de l'interface interne**

* **Identification du badge NFC**
  + L'utilisateur scanne son badge sur le **lecteur NFC (Début)**.
  + Le lecteur envoie l’information à **l’ESP32** pour vérification (Etape 1)
* **Vérification du badge**
  + L’ESP32 (Étape 2) compare l’ID du badge avec la base de données intégrée.
  + Si le badge est valide, on passe à l’étape 3 (vert)
  + Si le badge est invalide, un message "Carte non valide" s’affiche sur l’écran LCD (Etape 3 rouge)
* **Activation du mécanisme d’ouverture**
  + Si le badge est valide, l’ESP32 active le **relais** (Étape 3 - vert).
  + Le relais actionne le **loquet** (Étape 4), permettant l’ouverture du casier.
* **Confirmation de l’ouverture**
  + Le casier est ouvert (Étape 5), et l’écran LCD affiche "Porte ouverte" (Étape 6).
  + L’utilisateur peut récupérer ou déposer son matériel (Fin).

**Erreurs et Sécurité**

La gestion des erreurs est tout aussi important pour ce projet. En effet, notre système pourra bien subir des désagréments et des solutions devront donc être envisagées.

De plus, la **protection des données** via un système de chiffrement des informations stockées devient une obligation au vu de l’importance que cela représente.

**Contraintes du projet de PRJ1401**

**1. Lecteur NFC**

**Rôle :** Permet l’authentification de l’utilisateur en scannant une carte NFC.

**Contraintes :**

* **Alimentation** : Généralement 3,3V ou 5V, compatible avec l’ESP32.
* **Latence** : Le temps de lecture doit être rapide (<1 seconde).
* **Compatibilité** : Doit fonctionner avec les cartes NFC autorisées.
* **Sécurité** : Les données doivent être transmises de manière sécurisée pour éviter le clonage de cartes.

**2. Microcontrôleur ESP32**

**Rôle :** Cerveau du système, il reçoit les données du lecteur NFC, contrôle le loquet et affiche les informations sur l’écran.

**Contraintes :**

* **Alimentation** : 3,3V (nécessite un régulateur si alimenté par 5V ou plus).
* **Nombre de ports GPIO limité** : Doit gérer plusieurs périphériques sans conflit.
* **Latence** : Doit traiter les données en temps réel et envoyer rapidement les commandes.
* **Consommation électrique** : Modérée (~100-250 mA), doit être optimisée si le système est alimenté sur batterie.
* **Sécurité** : Connexions Wi-Fi/Bluetooth doivent être protégées contre les cyberattaques.

**3. Relais**

**Rôle :** Active et désactive l’alimentation du loquet magnétique en fonction des commandes de l’ESP32.

**Contraintes :**

* **Alimentation** : Nécessite du 5V pour fonctionner, compatible avec l’ESP32 via un transistor ou un circuit d’adaptation de tension.
* **Charge supportée** : Doit être capable de commuter la tension et l’intensité du loquet (souvent 12V ou 24V).
* **Temps de réponse** : <100 ms pour éviter tout retard dans l’ouverture.
* **Durée de vie** : Doit supporter plusieurs cycles d’activation/désactivation sans s’user rapidement.

**4. Loquet Magnétique**

**Rôle :** Verrouille et déverrouille le casier selon les instructions du relais.

**Contraintes :**

* **Alimentation** : Fonctionne souvent en 12V ou 24V → nécessite une alimentation adaptée.
* **Consommation électrique** : Peut consommer plusieurs ampères lorsqu’il est activé.
* **Sécurité physique** : Doit être robuste pour résister aux tentatives d’effraction.
* **Mode de verrouillage** : Certains modèles restent verrouillés même sans courant (fail-secure), d’autres se déverrouillent en cas de coupure de courant (fail-safe).
* **Temps de réaction** : Doit s’ouvrir instantanément après activation pour éviter un décalage perceptible par l’utilisateur.

**5. Écran LCD (avec adaptateur I2C)**

**Rôle :** Affiche les instructions et les statuts du casier (ex : "Casier ouvert", "Carte invalide", etc.).

**Contraintes :**

* **Alimentation** : Fonctionne généralement en 5V, nécessite une compatibilité avec l’ESP32 (3,3V).
* **Interface de communication** : Utilise l’I2C (moins de fils, mais nécessite des adresses spécifiques pour éviter les conflits avec d’autres périphériques).
* **Lisibilité** : Doit être visible même en conditions de faible luminosité (rétroéclairage requis).
* **Taille d’affichage** : Généralement limité à 16x2 ou 20x4 caractères → nécessite une gestion efficace des messages affichés.
* 6.Serveur
* **Rôle :** L’**ESP32** doit être connecté à un **serveur** contenant la **base de données** des cartes NFC autorisées. Cela ajoute des **contraintes supplémentaires** à prendre en compte :
* **Contraintes :**
* **Connexion Wi-Fi de l’ESP32 :** Permet la communication avec le serveur **-->** Nécessite une connexion réseau stable et sécurisée (peut être limité en cas de coupure du Wi-Fi)
* **Base de données (MySQL, Firebase, etc.) :** Stocke les identifiants NFC autorisés **-->** Doit être rapide pour valider les cartes NFC en temps réel (latence minimale)
* **Sécurité des échanges :** Protège contre les accès non autorisés **-->** Doit utiliser le chiffrement des données (HTTPS, authentification sécurisée)
* **Synchronisation :** Mise à jour en temps réel des accès **-->** Assurer que la base de données reste à jour sans latence excessive
* **Serveur hébergé (local ou cloud) :** Gère les requêtes et les accès aux casiers **-->** Si en cloud, dépend d'Internet ; si local, doit être robuste et accessible en interne

## **Impact des Contraintes sur le Projet**

* **Optimisation des échanges serveur-ESP32** pour limiter la latence (utilisation d’un protocole léger comme MQTT).
* **Sécurisation des communications** pour éviter les failles de sécurité.
* **Prévoir un mode de secours** en cas de panne réseau (ex: cache local des cartes NFC).
* **Assurer une alimentation stable** pour les composants énergivores comme le loquet magnétique.

### Justification du choix des composantes du projet de PRJ1401

Le projet repose sur plusieurs composantes essentielles, chacune ayant été sélectionnée pour répondre à des besoins précis en matière de sécurité, d’automatisation et d’accessibilité. Voici une justification détaillée du choix de chaque élément du système.

### 1. Lecteur NFC

**Pourquoi ?**

* Il permet une **authentification rapide et sécurisée** des utilisateurs.
* La technologie NFC est **simple d’utilisation** : il suffit de passer une carte devant le lecteur.
* Elle est **largement utilisée** dans les systèmes d’accès et compatible avec les cartes étudiantes.
* Le NFC offre un **temps de réponse rapide** et réduit le risque d’erreurs d’authentification.

**Alternatives possibles :**

* Un clavier pour entrer un code → moins sécurisé et plus lent.
* Un QR code → nécessite un smartphone

### 2. ESP32 Devkit V4

**Pourquoi ?**

* Ce microcontrôleur est **puissant** et **polyvalent**.
* Il intègre une **connexion Wi-Fi et Bluetooth**, essentielle pour la communication avec un serveur et la base de données.
* Il offre **une grande capacité de traitement** pour gérer les accès et contrôler les autres composants.
* Il est **économique et largement documenté**, facilitant son intégration et son développement.

**Alternatives possibles :**

* Arduino Uno → Pas de Wi-Fi natif, nécessiterait un module additionnel.
* Raspberry Pi → Plus puissant, mais aussi plus coûteux et surdimensionné pour cette application.

### 3. Relais

**Pourquoi ?**

* Nécessaire pour **contrôler l’ouverture et la fermeture des loquets** via le microcontrôleur.
* Fonctionne comme un **interrupteur électronique** permettant de gérer des tensions plus élevées.
* Compatible avec l’ESP32 et **facile à piloter via un signal numérique**.

**Alternatives possibles :**

* Un MOSFET → Trop complexe pour cette application.
* Un relais statique → Plus coûteux, sans réel avantage pour ce projet.

### 4. Loquets magnétiques

**Pourquoi ?**

* Ils assurent **une fermeture sécurisée** des casiers et peuvent être activés électroniquement.
* Ils sont **robustes et fiables**, évitant les ouvertures accidentelles.
* Fonctionnent bien avec un relais et offrent **une réponse rapide** à la commande d’ouverture.

**Alternatives possibles :**

* Un verrou motorisé → Plus complexe et plus énergivore.

### 5. Écran LCD + Adaptateur I2C

**Pourquoi ?**

* Permet d’afficher des **instructions claires** à l’utilisateur (exemple : “Présentez votre carte”, “Casier ouvert”, “Accès refusé”).
* L’adaptateur I2C simplifie la connexion avec l’ESP32, réduisant le nombre de fils nécessaires.
* Il consomme **peu d’énergie** et reste **lisible même en plein jour**.

**Alternatives possibles :**

* Un écran OLED → Plus compact mais coûteux, et moins utile pour des affichages simples.
* Un écran tactile → Trop complexe et pas nécessaire pour cette application.

### 6. Connexion au serveur et base de données

**Pourquoi ?**

* Permet de **stocker et gérer les numéros de cartes NFC autorisées** en temps réel.
* Facilite **l’ajout et la suppression d’utilisateurs** sans modifier le code du microcontrôleur.
* Garantit une **sécurité renforcée** en limitant l’accès uniquement aux personnes autorisées.
* Assure une **traçabilité des ouvertures**, utile pour la gestion et la maintenance.

**Alternatives possibles :**

* Stockage local sur l’ESP32 → Limité en mémoire et plus difficile à mettre à jour.
* Utilisation d’une API externe → Peut poser des problèmes de latence ou de confidentialité.

### Pistes d’amélioration et perspectives

Dans le cadre de l’évolution du projet des casiers intelligents, plusieurs axes d’amélioration et de développement peuvent être envisagés afin d'enrichir les fonctionnalités, de renforcer la sécurité, et de favoriser un déploiement à plus large échelle.

### Implémentation d’une Double Authentification (2FA)

Afin de renforcer significativement la sécurité d’accès aux casiers connectés, nous proposons la mise en place d’une **authentification à deux facteurs (2FA)**. Ce mécanisme oblige l’utilisateur à prouver son identité à l’aide de deux éléments distincts, rendant les accès beaucoup plus difficiles à usurper.

Le processus envisagé est le suivant :

* **Premier facteur : authentification physique via badge NFC**  
  L’utilisateur s’identifie dans un premier temps en scannant son badge NFC personnel sur le lecteur du casier. Ce badge doit être préalablement enregistré dans la base de données centrale.
* **Deuxième facteur : validation via code temporaire (OTP)**  
  Une fois le badge reconnu, un **code temporaire** (One-Time Password, OTP) est généré automatiquement par le serveur et envoyé à l’utilisateur :
  + Soit par notification via une application mobile dédiée,
  + Soit par mail vers l’adresse institutionnelle de l’utilisateur (par exemple adresse universitaire).

L’utilisateur devra ensuite entrer ce code sur une **interface mobile ou web** reliée au système pour valider définitivement l’ouverture du casier.

### Interface mobile/web

Le développement d’une **interface utilisateur mobile ou web** offrirait une meilleure ergonomie et plus de flexibilité. Elle permettrait notamment aux usagers de :

* Réserver un casier à distance,
* Suivre l’état de disponibilité en temps réel,
* Recevoir des notifications lors de la mise à disposition ou du retrait d’un objet.

Une telle interface contribuera à une expérience utilisateur plus fluide et connectée.

### Déploiement élargi

Enfin, le système de casiers intelligents a le potentiel d’être **déployé en dehors du cadre universitaire**, par exemple :

* Dans d’autres établissements d’enseignement supérieur (écoles, universités),
* Dans des entreprises pour la gestion de matériel partagé ou de consignes sécurisées,
* Dans des espaces publics (gares, bibliothèques, coworkings, etc.).

L’adaptation du prototype à des environnements variés nécessiterait une modularité accrue (nombre de casiers, types d’authentification, configuration logicielle) mais représenterait une excellente opportunité de valorisation du projet.

**Mise en veille automatique pour limiter la consommation énergétique**

Afin d’optimiser la consommation d’énergie du système de casiers intelligents, une **fonction de mise en veille automatique** peut être intégrée :

* Lorsque **aucune activité utilisateur** (pas de scan NFC, pas d'interaction réseau) n'est détectée pendant une période donnée (par exemple 5 minutes), l’ESP32 bascule automatiquement l'ensemble du système en **mode veille profonde**.
* Pendant ce mode, la majorité des composants (écran LCD, lecteur NFC, relais) seraient désactivés ou mis en mode faible consommation.
* Le système se **réactive automatiquement** dès qu'un événement externe est détecté, comme :
  + Une détection de badge NFC
  + La touche de l’interface utilisateur