KEYLESS ACCESS

A85 Analyse de projet

Analyse Préliminaire

A picture containing graphics, map, graphic design, design

Description automatically generated

Tremblay Philippe

Latulippe Delfik

# Table des matières

[Table des matières 1](#_Toc137451141)

[Introduction 2](#_Toc137451142)

[Persones Ressources 2](#_Toc137451143)

[Steeve Tremblay 2](#_Toc137451144)

[Lancement du projet 2](#_Toc137451145)

[Présentation de Steeve Tremblay et SERVICE VIP 2](#_Toc137451146)

[Problématiques et Besoins 3](#_Toc137451147)

[Présentation du mandat 3](#_Toc137451148)

[Cas d’utilisation – Système actuel 4](#_Toc137451149)

[Introduction : 4](#_Toc137451150)

[Description du cas : « Gestion des propriétés/acces(serrures) » 4](#_Toc137451151)

[Description du cas : « Gestion des clés » 5](#_Toc137451152)

[Description du cas : « Accéder à la propriété » 6](#_Toc137451153)

[Cas d’utilisation – Nouveau système 7](#_Toc137451154)

[Introduction : 7](#_Toc137451155)

[Description du cas : « Gestion des propriétés/acces(serrures) » 8](#_Toc137451156)

[Description du cas : « Gestion des clés - propriétaire » 9](#_Toc137451157)

[Description du cas : « Gestion des clés - Locataire » 10](#_Toc137451158)

[Description du cas : « Accéder à la propriété » 11](#_Toc137451159)

[Les phases 12](#_Toc137451160)

[Phase #1 – BD | Site web | application mobile 12](#_Toc137451161)

[Phase #2 – Microcontroleur et résautique 13](#_Toc137451162)

[Phase #3 – sécurité et fonctionalité supplémentaires 14](#_Toc137451163)

[Conclusion 15](#_Toc137451164)

[Annexe A : Lettre d’entente 16](#_Toc137451165)

[Annexe B : Calendrier d’analyse 17](#_Toc137451166)

# Introduction

L’analyse qui suit expliquera notre choix tant qu’au projet final de fin d’études. Un projet stimulant qui saura nous présenter son lot de défis.

Quelques idées nous sont venues en tête : Un système de booking en ligne pour une salle de spectacle, un gestionnaire de projet et un système de gestion d’accès de serrures électroniques à distance.

L’une de celle-ci nous ferait sortir des sentiers battus; Le choix pour nous était évident.

## Persones Ressources

### Steeve Tremblay

Propriétaire de Service VIP Inc.

Une dizaine d’années dans le monde des serrures électroniques on permit à Steeve d’identifier des problématiques, à la tête de l’idée, il nous apporte un projet intriguent. Une nouvelle idéologie pour une serrure adapté aux besoins du jour, avec la technologie du jour.

## Lancement du projet

L’idée est claire. Créer une créer une serrure donc l’accès serait géré complètement à distance, ou la clé du client serait… Son téléphone !

C’est un projet motivant pour nous, intriguent, qui, si mené à terme, saura satisfaire nos exigences envers nous-même face à ce projet final et nous en apprendre sur des sujets de l’informatiques moins travaillés pendant les cours, soit la réseautique et le hardware.

# Présentation de Steeve Tremblay et SERVICE VIP

L’expérience de Steeve Tremblay dans le monde des serrures électroniques lui ont amené à se poser bien des questions … Gestion d’accès, complètement à distance, pour des serrures d’unités de location (Airbnb, Motel, Chalet, etc.) ou la clé serait l’appareil mobile du client, tout en priorisant les principes de simplicité et facilité d’utilisation, c’est possible ? Nous le croyons maintenant. C’est d’ici que décolle l’idée d’une clé mobile (entrée via NFC).

# Problématiques et Besoins

#### Problématiques :

* Les serrures existantes n’utilisent pas le NFC.
* Les locataires doivent mémoriser un PIN.
* Les locataires ne peuvent pas gérer ou créer des accès temporaires.
* L’envoie des clés aux clients n’est pas automatisée.

#### besoins :

* Serrure qui emmagasine des clés en mémoire.
* Serrure qui prend en compte la datte et l’heure.
* Serrure qui ne permet l’accès que si le contact NFC ou le PIN entré correspond à l’une des clés valides.
* Contient un moyen d’entrée d’urgence (PIN).
* Gestion des clés autorisées par le propriétaire.
* Gestion de clés invitées par le locataire.
* Gestions de clés spéciales (Ex : Femme de ménage, entretien).
* Synchronisation de la mémoire serrure avec la BD.

# Présentation du mandat

Nous voulons créer une serrure électronique, contenant des clés en mémoire, qui gère son accès et autorise l’accès seulement si une clé valide et autorisée est présentée.

Le microcontrôleur de notre serrure devra être en mesure de faire un appel vers le web API, contenant la liste de clés autorisé et s’actualiser à une fréquence à déterminer. Le microcontrôleur devra également être en mesure de recevoir des données NFC et les comparer à notre liste de clé.

Il sera possible pour le propriétaire des serrures d’ajuster la liste des clés autorisées ainsi qu’affecter une plage horaire à ces dites clés. Il sera également possible pour un usager de partager son accès et gérer les plages horaires de ces invitations à son tour, tout en gardant une interface simple et intuitive, ou le programme fait la plus grande partie du travail.

# Cas d’utilisation – Système actuel

## Introduction :

Le système actuel n’offre la clé que par NIP. L’utilisateur n’a donc pas accès à une application mobile et à la gestion des clés de son côté. Le système actuel est fort simple et géré uniquement par le propriétaire. Les cas d’utilisations présentés ci-dessous décrivent l’expérience d’un propriétaire pour la gestion de ses serrures électroniques des modèles les plus courants.

## Description du cas : « Gestion des propriétés/acces(serrures) »

A picture containing text, diagram, screenshot, font

Description automatically generated

#### Identification*:*

But: Faire la gestion des différents établissements d’un propriétaire ainsi que leurs points d’accès.

Acteur principal: Le propriétaire.

Acteur secondaire: Le système contenant l’informations des établissements et accès (BD).

#### *Séquencement :*

Après son inscription, le propriétaire peut s’authentifier, lui donnant accès à la création d’établissements et permettant maintenant l’utilisation des fonctionnalités suivantes. Modifier son établissement, lui assigner une/des serrures, lister ces différentes serrures ainsi que les modifier au besoin à leur tour.

#### *post-utilisation :*

À chaque fin de branche la validée des items est vérifiée et l’information est mise à jour dans la base de données.

## Description du cas : « Gestion des clés »

A picture containing text, diagram, screenshot, font

Description automatically generated

#### Identification*:*

But : Faire la gestion de clés, soit consulter, ajouter, retirer, ou modifier la validité de clés et leur affecter différentes plages horaires selon les besoins du client ou de la location.

Acteur principal : Le propriétaire des unités de location

Acteur secondaire : Le système contenant l’informations des clés et des serrures (BD)

#### *Séquencement :*

Après s’être inscrit, le propriétaire peut s’identifier. Il peut ensuite consulter ses différents accès (poignées), et gagne donc vue aux différentes clés valides pour cet accès. Il peut bien entendu ajouter une clé, modifier la validité de celle-ci, lui affecter différentes plages horaires ou faire les modifications voulues.

#### *Enchainement :*

1. Le locataire loue l’unité.
2. Le propriétaire s’inscrit et puis s’authentifie.
3. Il navigue ses accès, consulte les clés associées.
4. Il peut effectuer les changements voulus. (Créer, modifier, désactiver)
5. Les changements sont envoyés au système contenant l’information des clés (BD).
6. Le propriétaire envoie le NIP d’accès au client manuellement.

#### *post-utilisation :*

À chaque fin de branche la validée des items est vérifiée et l’information est mise à jour dans la base de données.

## Description du cas : « Accéder à la propriété »

*A picture containing line, diagram, text, plot

Description automatically generated*

#### *Identification :*

But : Autoriser l’accès à une propriété pour un client

Acteur principal : Le client

Acteur secondaire : Le système contenant l’informations des clés et des serrures (BD)

#### *Séquencement :*

En arrivant sur place, le locataire entre le PIN d’accès préalablement reçu par le propriétaire. La serrure compare avec sa banque de donnée, elle autorise l’accès au locataire s’il a un match, dans le cas où s’est refusé, un compteur s’active, une alarme peut être déclenché si le compteur excède un nombre de tentatives prédéterminé.

#### *Enchainement :*

1. Le locataire reçoit la clé d’accès.
2. Le locataire entre la clé d’accès sur le paver numérique.
3. La serrure compare avec sa banque de données.
4. L’accès est autorisé ou refusé.
5. Optionnel : Une alarme est sonnée.

#### *post-utilisation :*

À chaque fin de branche, si l’accès a été refusé (NIP erroné), un compteur s’incrémente. Une alarme peut être sonnée au bout de X tentatives.

# Cas d’utilisation – Nouveau système

## Introduction :

Notre nouveau système offre un nouvel air de pensé en ce qui concerne la méthode d’authentification. En effet, notre poignée prototype saura se débarrer au simple contact d’un téléphone cellulaire (ou n’importe quel émetteur NFC/RFID).

Notre approche simplifiera l’expérience usager, une fois l’application téléchargée et l’inscription terminée, l’usager n’aura qu’à accepter une invitation (via son téléphone) pour être admis dans ladite serrure. La serrure saura prendre compte de la date et du temps afin de gérer la validité des clés selon des plages horaires définies préalablement.

De plus, notre nouveau système offrira une nouvelle fonctionnalité: La possibilité pour le locataire de de partager l’accès à quelqu’un d’autre. Il pourra envoyer une invitation via l’application mobile et gérer à son tour les plages horaires de ces mêmes invitations. Bref, il devient en quelque sorte ‘master’ de la serrure, ceci pour le temps de sa location.

Avec pour but: Faciliter la gestion de clés pour les propriétaires, permettre la gestion de clés invités au locataire & simplifier l’expérience au niveau applicatif.

## Description du cas : « Gestion des propriétés/acces(serrures) »

À noter que aucun changement n’est apporté pour ce cas. Il reste pratiquement identique au système antérieur.

A picture containing text, diagram, screenshot, font

Description automatically generated

#### Identification*:*

But: Faire la gestion des différents établissements d’un propriétaire ainsi que leurs points d’accès.

Acteur principal: Le propriétaire.

Acteur secondaire: Le système contenant l’informations des établissements et accès (BD).

#### *Séquencement :*

Après son inscription, le propriétaire peut s’authentifier, lui donnant accès à la création d’établissements et permettant maintenant l’utilisation des fonctionnalités suivantes. Modifier son établissement, lui assigner une/des serrures, lister ces différentes serrures ainsi que les modifier au besoin à leur tour.

#### *post-utilisation :*

À chaque fin de branche la validée des items est vérifiée et l’information est mise à jour dans la base de données.

## Description du cas : « Gestion des clés - propriétaire »

A picture containing text, diagram, font, line

Description automatically generated

#### *Identification :*

But : Faire la gestion de clés, soit ajouter, retirer, ou modifier la validité d’une clé mobile ou clé par PIN et l’envoyer au client.

Acteur principal : Le propriétaire de la serrure.

Acteur secondaire : Le système contenant l’informations des clés et des serrures (BD).

#### *Séquencement :*

Après s’être inscrit et authentifié le propriétaire peut naviguer ses accès (portes). Représenté ici, deux chemins s’offrent à lui. Le premier permet l’ajout d’une clé mobile (invitation par application), lui permettant ensuite les changements ou modifications associées, et l’envoie l’invitation automatisé à l’usager à la fin du processus. Le deuxième chemin propose la création d’une clé par PIN, encore une fois, permettant les modifications associées par la suite, petite différence, cette fois l’envoie au client est optionnel.

#### *Enchainement :*

1. Le propriétaire s’authentifie.
2. Il parcoure ses accès (portes) et consulte un accès
3. Il peut effectuer les changements voulus, ajouter, modifier ou désactiver une clé mobile ou PIN.
4. Il détermine la plage horaire et les permissions au besoin.
5. OPT : À la sauvegarde, l’invitation mobile est envoyée au client (automatiquement) par le système.
6. OPT : Pour une invitation par PIN, le propriétaire choisi ou non de la lier à un client & envoyer l’invitation.

#### *post-utilisation :*

À chaque fin de branche la validée des items est vérifiée et l’information est mise à jour dans la base de données.

## Description du cas : « Gestion des clés - Locataire »

*A picture containing text, diagram, font, line

Description automatically generated*

#### *Identification :*

But : Faire la gestion de ses clés (accès autorisés) et la gestion des invités ainsi que de leur plage de permissions.

Acteur principal : Le locataire de la serrure

Acteur secondaire : Le système contenant l’informations des clés et des serrures (BD).

#### *Séquencement :*

Le locataire s’authentifie sur l’application, il peut ensuite recevoir et accepter des invitations, lui autorisant l’accès à une porte ou un lot de portes. Dans le cas où le locataire est ‘master’ de la location, il gagne l’accès aux fonctionnalités supplémentaires : Soit, l’invitation et la gestion de gens additionnels. Il peut donc à son tour modifier les plages horaires de permissions des usagers qu’il invite.

#### *Enchainement :*

1. Le locataire loue l’unité.
2. Le locataire s’authentifie sur l’application.
3. Le locataire reçoit et accepte l’invitation (du propriétaire ou un locataire ‘master’).
4. OPT : Il est initié en tant que ‘master’ de la location, gagne l’accès aux fonctionnalités supplémentaires.
   1. Il peut inviter d’autres utilisateurs et en faire la gestion.

#### *post-utilisation :*

À chaque fin de branche la validée des items est vérifiée et l’information est mise à jour dans la base de données.

## Description du cas : « Accéder à la propriété »

*A picture containing text, diagram, screenshot, line

Description automatically generated*

#### *Identification :*

But : Gagner l’accès à une serrure pour un locataire ou un invité.

Acteur principal : Client (locataire ou invité)

Acteur secondaire : Le système contenant l’informations des clés et des serrures (BD)

#### *Séquencement :*

Ici, deux scénarios sont possibles, dans le premier, ou l’utilisateur est inscrit puis authentifié, il peut accepter une invitation sur l’application mobile et utiliser son téléphone en tant que ‘clé’. Dans le deuxième cas, l’utilisateur n’est pas requis d’être enregistré et authentifié sur l’application mobile, il peut simplement entrer le NIP de passage. Pour les deux situations, la validité de la clé (NIP ou NFC) est validée, l’accès est autorisé en cas de succès, et en cas d’erreur, un compteur s’incrémente. À un nombre d’erreurs déterminable, le propriétaire est notifié et l’alarme peut être sonnée.

#### *Enchainement :*

1. CAS 1 : Le locataire reçoit et accepte l’invitation.
2. Le locataire approche son téléphone du lecteur NFC ou entre le PIN d’accès.
3. La serrure compare la clé avec sa banque de données.
4. L’accès est autorisé ou refusé.
5. Si l’accès est refusé, le compteur d’erreurs s’incrémente
6. OPT : Une alarme et alerte peuvent être sonnées.

#### *post-utilisation :*

À chaque fin de branche, si l’accès a été refusé (NIP erroné), un compteur s’incrémente. Les entrés sont gardés en mémoire par la serrure et à une certaine fréquence, la poignée transfert les registres vers la data base et enregistre à nouveau dans sa mémoire les clés valides. (OverWrite)

# Les phases

Les phases séparent notre travaille en 3 grands blocs. En ordre de priorité d’importance quant au succès de notre projet final. C’est ici que nous exprimerons nos objectifs, idéologies et visions futures par rapport à notre projet.

## Phase #1 – BD | Site web | application mobile

#### *Présentation :*

La phase 1 consiste pour nous, à créer un site web, qui nous propose les fonctionnalités complètes permettant la gestion d’utilisateurs, d’édifices, de serrures et de clés. En plus de terminer l’application mobile, permettant donc aux usagers de s’authentifier et de gérer les clés secondaires associées à leurs locations.

#### *Étapes :*

1. Analyser le format des données des poignées similaires existantes.
2. Créer et imager le schéma de nos données. (Clés, accès, point d’accès).
3. Mise en place et création de la base de données.
4. Développement du site web :
   1. Gestion des utilisateurs.
   2. Gestion des différents points d’accès et leurs clés pour les propriétaires. (CRUD complet)
   3. Gestion des clés secondaires pour les locataires.
5. Développement de l’application mobile :
   1. Gestion des utilisateurs.
   2. Gestion des clés secondaires pour les locataires.
   3. Interface simple et intuitive

#### *Processus :*

Cette étape est la plus grande et la plus importante de notre projet. C’est ici le cœur de notre idée et le fonctionnement du reste dépend ardument de cette phase. Nous allons commencer par analyser le schéma des données des systèmes actuels et étudier les principes importants de ces systèmes. Nous allons ensuite schématiser et concevoir notre BD en prenant compte des analyses précédentes et des nouveaux besoins que comporte notre produit. Ensuite, nous allons développer le site web, en gardant un but en tête : une interface simple, une navigation intuitive. Le site fera la gestion sécuritaire des usagers ainsi que leurs données. Il permettra, pour les propriétaires, de faire la gestion de leurs établissements, des serrures que ceux-ci comportent ainsi la gestion des clés associés à ces mêmes serrures. La gestion de clés permettra d’affecter différentes plages horaires de validité et automatisera l’invitation envoyée aux locataires. Ensuite, une fois le CRUD complet et fonctionnel, nous commenceront le développement de l’application mobile et y ajouteront les fonctionnalités pour s’authentifier, ainsi la possibilité aux locataires de gérer leurs accès et envoyer des invitations à d’autre usagers. Donc, une fois complétée, notre première phase devrait déjà comporter tous les éléments et relations nécessaires pour gérer les différents points d’accès.

## Phase #2 – Microcontroleur et résautique

#### *Présentation :*

La phase deux consiste à rendre notre projet plus vivant. Nous voulons en effet, réussir à incorporer notre programme dans un microcontrôleur, qu’il appelle notre API et conserve en mémoire une liste de clés valides (NFC user or PIN key).En addition, le microcontrôleur saura garder un registre des entrés et l’envoyer vers l’api en pour finalement se libérer de sa mémoire. Nous simulerons ensuite les états de la serrure (Verrouillé or déverrouillé) via un servomoteur. À ce point, nous serons en mesure d’avoir une bonne vue d’ensemble du fonctionnement de notre système.

#### *Étapes :*

1. Analyser les différences entre les microcontrôleurs existants et choisir le bon pour nous.
   1. Batteries
   2. Consommation d’énergie
   3. Mémoire
   4. Puissance/Besoin
2. Ajouter les modules nécessaires au microcontrôleur
   1. Batteries
   2. Réseau
   3. Lecteur NFC
   4. Servomoteur
3. Incorporer notre programme au microcontrôleur
4. Tester les différentes fonctionnalités de notre serrure
   1. Entrée NFC/NIP
   2. Rapidité/Fiabilité
   3. Changement des clés permises
   4. Invitation supplémentaire (pour les locataires)

#### *Processus :*

Bien entendu, nous commenceront par faire le choix de nos composants. Nous analyserons les différences majeures entre différents microcontrôleurs présents sur le marché (Arduino, Raspberry Pi Pico, etc.). Nous devrons nous assurer que le microcontrôleur choisi possède assez de mémoire pour contenir notre programme, une architecture semi complexe de plages de validité de clés, saura prendre compte de la datte et l’heure, tout ceci en étant rapide mais aussi peu couteux en énergie ; La poignée doit être auto-suffisante pour un minimum de temps. Une fois le choix fait, les pièces reçues, on s’attaque à l’assemblage physique de notre système, à la programmation du microcontrôleur et aux tests finals une fois la simulation de notre serrure terminée.

## Phase #3 – sécurité et fonctionalité supplémentaires

#### *Présentation :*

La phase trois est la cerise sur le gâteau. Blague à part, nous voulons apporter notre système dans une réelle serrure, pour le contraindre aux besoins physiques du vrai monde. Cette étape fera de notre projet quelque chose de complet en soit, quelque chose de complètement indépendant et fonctionnel. Dans cette phase, nous toucherons à l’aspect sécurité de l’envois des données (encryptions), l’implémentation de notre microcontrôleur dans une serrure physique et sauront l’ouvrir à même notre téléphone cellulaire.

#### *Étapes :*

1. Implémentation du microcontrôleur dans une serrure existante.
2. Ajustement et connexion des différents modules nécessaires, en prenant compte des dimensions et restrictions physique d’une poignée.
   1. Batteries
   2. Réseau
   3. Lecteur NFC
   4. Servomoteur
3. Recherche sur l’aspect sécurité du partages des données.
4. Implémentation de l’aspect sécurité dans notre microcontrôleur.
5. Test finaux de notre produit terminé.

#### *Processus :*

Pour cette étape, à l’aide d’une vraie serrure dans le type, modifiée à nos besoins nous implémenterons notre lecteur NFC ainsi que notre microcontrôleur. Nous ajusterons les modules nécessaires afin de se plier aux contraintes d’un boîtier en métal (placement de l’antenne, placement du lecteur NFC, batteries, filage, etc.). Cette étape nous apportera sans un doutes quelques surprises, nous devrons nous adapter en fonction de ce qu’on travaille et tester plusieurs différents setups, pour un maximum de performance par rapport à l’énergie consommée par notre serrure.

# Conclusion

Notre objectif final est de modifier une poignée de porte existante et y implémenter notre microcontrôleur, faire la gestion de ses états via une plage de validité pour les clés autorisées (NFC et PIN). Nous apporterons quelques changements aux modèles traditionnels existent sur le marché, en y apportant notre lecteur NFC et en ajoutant au locataire la possibilité d’inviter d’autre utilisateurs et de gérer la validité de leur clé à leur tour. Le but est de rendre de partage d’accès simple, tout en restant sécuritaire et en tenant comptes des besoins réels d’une serrure dans les domaines fessant usage courant de serrures électroniques : soit l’hôtellerie, les unités de locations, les condominiums et bien plus !

# Annexe A : Lettre d’entente

A close-up of a letter

Description automatically generated with medium confidence

# Annexe B : Calendrier d’analyse

A screenshot of a computer

Description automatically generated with medium confidence