Département des Technologie de l'information et de la communication (TIC)
Filière Télécommunications
Orientation Sécurité de l'information

Travail de Bachelor

Gestionnaires de mots de passe : quelle sécurité ?

Étudiante **Noémie Plancherel**
Enseignant responsable Prof. Sylvain Pasini
Année académique 2022-2023

Yverdon-les-Bains, le 30 septembre 2022

Département des Technologie de l'information et de la communication (TIC)
Filière Télécommunications
Orientation Sécurité de l'information
Étudiante : Noémie Plancherel
Enseignant responsable : Prof. Sylvain Pasini

Travail de Bachelor 2022-2023

Gestionnaires de mots de passe : quelle sécurité ?

Résumé publiable

Dans ce travail... Ceci est le résumé publiable...

Étudiant :	Date et lieu :	Signature :
Noémie Plancherel	.....	.....
Enseignant responsable :	Date et lieu :	Signature :
Prof. Sylvain Pasini	.....	.....

Préambule

Ce travail de Bachelor (ci-après TB) est réalisé en fin de cursus d'études, en vue de l'obtention du titre de Bachelor of Science HES-SO en Ingénierie.

En tant que travail académique, son contenu, sans préjuger de sa valeur, n'engage ni la responsabilité de l'auteur, ni celles du jury du travail de Bachelor et de l'Ecole.

Toute utilisation, même partielle, de ce TB doit être faite dans le respect du droit d'auteur.

HEIG-VD

Vincent Peiris
Chef de département TIC

Yverdon-les-Bains, le 30 septembre 2022

Authentification

La soussignée, Noémie Plancherel, atteste par la présente avoir réalisé ce travail et n'avoir utilisé aucune autre source que celles expressément mentionnées.

Yverdon-les-bains, le 30 septembre 2022

Noémie Plancherel

Cahier des charges

Résumé du problème

De nos jours, les gestionnaires de mots de passe sont des outils très fréquemment utilisés. En effet, une bonne pratique est d'utiliser un mot de passe par service. De cette manière, si un service est compromis et le mot de passe divulgué, cela n'impacte pas les autres services. Il est également très important de choisir un mot de passe fort qui ne contient pas d'éléments facilement prévisibles et qui pourrait être brute-forcé rapidement.

Les gestionnaires de mots de passe permettent principalement de faciliter le stockage des mots de passe qui demandent d'être de plus en plus longs et complexes, de manière à ne pas les réutiliser. Ils permettent également d'ajouter une couche sécuritaire aux mots de passe en les stockant de manière sécurisée et en offrant la possibilité de générer des mots de passe forts.

Ces applications offrent plusieurs fonctionnalités sous la forme de différents types ; elles permettent, entre autres, l'utilisation du cloud afin de stocker les mots de passe sur les serveurs du fournisseur pour faciliter la synchronisation des données entre plusieurs devices (mobile, montre, navigateur, etc.). Certains gestionnaires de mots de passe sont également fréquemment utilisés au sein d'entreprises pour permettre le partage de données. Les entreprises vont généralement utiliser une solution self-hosted où elles auront leur propre infrastructure et stockage. Il existe des extensions de navigateur qui proposent le remplissage automatique de mots de passe dans les formulaires de connexion. Enfin, il y a également des applications en local qui vont limiter leur utilisation à un seul appareil.

Étant donné que les utilisateurs se reposent grandement sur les gestionnaires de mots de passe, il est important de s'assurer que ces logiciels satisfassent un certain nombre de principes de sécurité ainsi qu'une implémentation robuste afin d'éviter tout vol ou perte de données.

Objectifs

Ce travail de Bachelor vise à comprendre les menaces d'un gestionnaire de mots de passe, premièrement de manière générique, puis sur des produits spécifiques, sélectionnés à la suite d'une étude complète, en analysant la sécurité sous différents angles (stockage, mémoire, réseau, cryptographie, etc.).

Le travail est réalisé en deux parties distinctes ; une première partie qui est une étude approfondie et complète sur les gestionnaires de mots de passe. Elle permet d'analyser les menaces des différents type de gestionnaires de mots de passe et de présenter les exigences sécuritaires qu'il serait nécessaire de garantir. Elle va également se concentrer sur une étude de marché avec une comparaison de plusieurs gestionnaires de mots de passe existants sous différents aspects.

La deuxième partie du travail se concentrera tout d'abord sur la sélection de quelques candidats (environ 4) en fonction de critères établis au préalable. Ensuite, le but est d'évaluer la sécurité de manière complète de chaque gestionnaire de mot de passe sélectionné ; chaque élément choisi est analysé et évalué en fonction de différents critères comme les choix cryptographiques utilisés, le stockage, ou encore l'architecture de l'application.

Livrables

Les délivrables seront les suivants :

1. Une documentation contenant :
   - Présentation des différents types de gestionnaires de mots de passe
   - Étude de marché
   - Une analyse de menaces de différents types de gestionnaires de mots de passe
   - Spécification des exigences sécuritaires à garantir

   (a) Analyse sécuritaire des quelques candidats représentatifs (environ 4) :
   - Sélection de candidats pour la suite du travail

   chaque analyse se décomposera ainsi :
   - Sélection de critères d'analyse
   - Analyse complète de chaque aspect
   - Rapport des faiblesses trouvées au fabricant

   (b) Synthèse des résultats
2. Comparaison entre chaque candidat

Déroulement

En se référant aux dates validées par M.Donini, le travail de Bachelor débute le 20 septembre 2022 et se termine au plus tard le 10 février 2023. Il y a 3 dates clés incluant des rendus :

- **14 octobre 2022** - rendu du rapport intermédiaire
- **14 décembre 2022** - rendu du rapport final
- **23 janvier au 10 février 2023** - soutenance du travail de bachelor

Etant donné, que la soutenance du travail implique l'intervention d'un expert, la date doit être définie entre tous les intervenants.

Le volume du travail de bachelor est de 15 crédit ECTS, soit 450 heures. Le rapport intermédiaire représente 150 heures de travail.

Au niveau de la répartition de la charge de travail, cela représente environ 45h/semaine jusqu'au rendu, soit le 14 décembre, car le travail se fait à 100%.

Planning

Le travail de bachelor sera séparé en plusieurs tâches et sous-tâches différentes qui permettront de répartir plus facilement le travail sur des périodes de plusieurs semaines. Ci-dessous, le planning détaillé avec toutes les tâches :

1. Préparation
    - Rédaction du cahier des charges
    - Planification
    - Recherches initiales et introduction
2. Étude de marché
    - Recherche et explication des différents types de gestionnaires de mots de passe
    - Comparaison des fonctionnalités, du prix et des plateformes disponibles
    - Analyse du marché actuel et de la demande
    - Récapitulatif
3. Étude sécuritaire
    - Présentation de la sécurité implémentée dans les gestionnaires de mots de passe
    - Identification et analyse des menaces potentielles
    - Rédaction des exigences sécuritaires
4. Sélection
    - Mise en place des critères de sélection des candidats
    - Sélection des candidats
5. Analyse sécuritaire (pour chaque candidat)
    - Identification et rédaction des critères d'analyse
    - Analyse sécuritaire de chaque aspect
6. Synthèse (pour chaque candidat)
    - Synthèse des résultats
    - Rapport des faiblesses au fabricant

7. Synthèse générale
    - Comparaison de tous les résultats
    - Conclusion du travail
8. Documentation
    - Rédaction du rapport
    - Lecture / visualisation de documents
    - Tenue d'un journal de travail

Un diagramme de Gantt a également été effectué afin de pouvoir visualiser le planning et ajouter des périodes de temps :

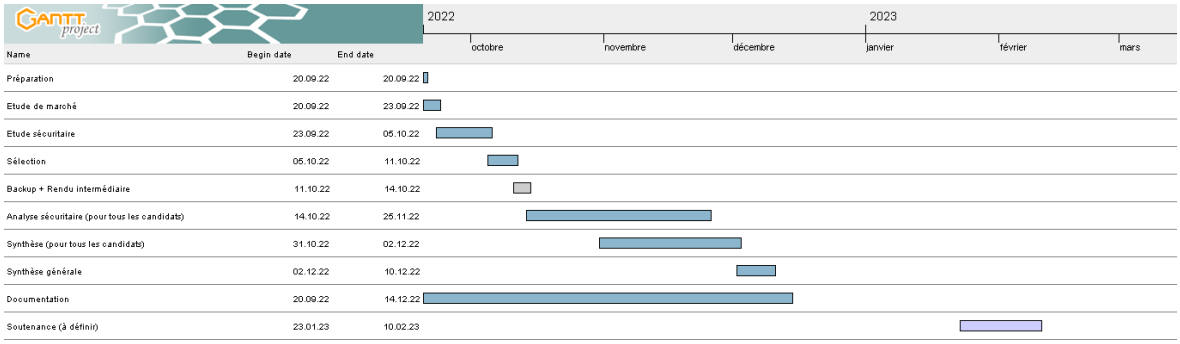

FIGURE 1 – Planning du travail de Bachelor

Table des matières

Chapitre 1

Introduction

Pour un utilisateur lambda, il peut être difficile de se souvenir de tous ses mots de passe tout en s'assurant d'en utiliser un différent pour chaque service afin d'éviter tout vol de données. Typiquement dans ces situations, nous allons naturellement utiliser des mots de passe simples, qui sont facilement mémorisables. Comme, par exemple, utiliser son prénom et sa date de naissance, "123456" ou encore "qwerty". De plus, il est plus simple d'utiliser le même mot de passe pour chacun de ses comptes, afin d'en mémoriser uniquement un seul.

Cependant, même si l'unique mot de passe qu'on utilise est fort et aléatoire, il n'est pas garanti à 100% qu'on soit la cible d'aucun attaquant et si une attaque est réalisée, toutes nos données personnelles sont exposées.

Ainsi, dans ce genre de cas, les gestionnaires de mots de passe interviennent et peuvent faciliter le quotidien de la plupart des utilisateurs.

1.1 Fonctionnement général

Les gestionnaires de mots de passe sont des applications multi-plateformes qui vont permettre de stocker des informations sensibles telles que des mots de passe, numéros de carte de crédit ou encore des fichiers confidentiels. On peut les comparer à des coffres forts.

Ces derniers proposent un *master password* ou une *master key* qui va permettre d'accéder à l'ensemble des données secrètes. En conséquence, la sécurité repose sur un seul mot de passe principal, ce qui est très bénéfique pour les utilisateurs car ils n'ont qu'un mot de passe à retenir. Une fois l'accès à l'application, l'utilisateur a la possibilité de stocker des données, générer des mots de passe ainsi que se connecter à des services en ligne (remplissage de formulaire d'identification automatique).

Les gestionnaires de mots de passe sont disponibles en plusieurs types différents en fonction

du besoin de l'utilisateur et des fonctionnalités proposées.

1.2 Types

1.2.1 Cloud

Les gestionnaires de mots de passe dans le cloud sont proposés pour un usage personnel ainsi qu'un usage professionnel. Les mots de passe entrés dans le coffre fort vont directement être stockés sur les serveurs du constructeur et ils seront également chiffrés sur ces derniers. Aucun stockage n'est effectué en local.

Le cloud va permettre aux utilisateurs d'avoir accès à leurs données sur n'importe quel device (ordinateur, mobile, montre) et à tout moment. De plus, toutes les données vont être synchronisées sur tous les devices connectés.

À propos de la sécurité, elle repose entièrement sur le provider de l'application car toutes les informations sont stockées sur leurs propres serveurs.

1.2.2 Local

Les applications en local s'installent sur le desktop ou sur le mobile de l'utilisateur. Ces gestionnaires de mots de passe fonctionnent indépendamment et sont offline. Ces produits peuvent donc être utilisés sur une seule machine, par conséquence la synchronisation n'est pas proposée pour ce type de password manager.

Toutes les données sensibles sont directement stockées et chiffrées sur le device. La sécurité est plutôt bonne comparé à la solution cloud car c'est du hors-ligne, cependant si on récupère / vole le device, la sécurité devient plus faible car il y aurait la possibilité d'avoir accès aux informations sensibles du gestionnaire de mots de passe, via notamment une gestion de mémoire mal gérée.

Il y a également une solution *on-premise* (ou *self-host*) qui permet d'utiliser sa propre infrastructure locale pour héberger toutes les données du gestionnaire de mots de passe. Les fonctionnalités offertes sont les mêmes que pour les solutions cloud mais le prix est en général plus cher et l'application plus orientée professionnelle.

1.2.3 Navigateur

Le dernier type de gestionnaire de mots de passe sont ceux qui sont basés sur le navigateur (*browser-based*). Les navigateurs les plus populaires, tels que Firefox, Safari ou Chrome offrent ce gestionnaire de mots de passe qui est directement inclu dans ces derniers. Ils vont faciliter la gestion et la sauvegarde de mots de passe de comptes de sites web. Il y a également

la possibilité de synchroniser toutes les données stockées entre tous les devices qui supportent le navigateur en question (Chrome, Firefox, Safari, etc.).

Pour certains navigateurs, les informations sont stockées et chiffrées en local sur le device de l'utilisateur. Si la synchronisation est activée, les données seront également stockées dans le cloud sur les serveurs du constructeur. Un problème de sécurité importante, et la disponibilité des mots de passe sur le navigateur, si aucun master password n'est configuré et qu'on a accès à la machine, les mots de passe sont accessibles en clair sur le navigateur.

Chapitre 2

Étude de marché

Ce chapitre vise à étudier les différentes fonctionnalités offertes par les gestionnaires de mots de passe en les comparant entre plusieurs produits sélectionnés et en établissant un tableau afin d'avoir une meilleure vue d'ensemble.

Nous allons également analyser les différents prix des applications ainsi que présenter où en est le marché actuel afin d'étudier la popularité de ces dernières.

Pour l'étude de marché, les gestionnaires de mots de passe sélectionnés seront : *LastPass*[1], *Dashlane*[2], *1Password*[3], *KeePass*[4], *Bitwarden*[5], *NordPass*[6], *Padloc*[7], *Keeper*[8], *Firefox*[9].

Ils ont été sélectionnés en se basant sur leur popularité sur le marché ainsi qu'à la suite de lecture d'articles concernant les meilleurs gestionnaires de mots de passe [5][8][17][14]. Les applications open-source ont été avantagées lors de leurs sélections.

2.1 Fonctionnalités

Ci-après, une liste des fonctionnalités disponibles dans les gestionnaires de mots de passe. Cette énumération se base sur toutes les fonctionnalités citées sur les websites des différents *password manager*.

1. https://www.lastpass.com/
2. https://www.dashlane.com/
3. https://1password.com/
4. https://keepass.info/
5. https://bitwarden.com/
6. https://nordpass.com/
7. https://padloc.app/
8. https://www.keepersecurity.com/
9. https://www.mozilla.org/fr/firefox/features/password-manager/

1. Stockage d'informations personnelles (cartes de crédit, passeport, contrats, etc.)
2. Remplissage automatique des formulaires en ligne (auto-complétion)
3. Partage de données entre plusieurs utilisateurs (par exemple, partage d'informations d'identifications entre une famille)
4. Générateur de mots de passe forts
5. Surveillance de la fuite de données ou données compromises
6. Alerte en cas de données compromises
7. Synchronisation de données entre devices (cloud)
8. Authentification à double facteurs
9. Self-hosting
10. Support prioritaire
11. Connexion à l'aide de facteurs biométriques (*fingerprint* ou *facial recognition*) ou d'un pin
12. *Backup & Restore*, possibilité de récupérer une ancienne sauvegarde

Ci-dessous un tableau récapitulatif qui indique quels gestionnaires de mots de passe offre quelles fonctionnalités.

Application	1	2	3	4	5	6	7	8	9	10	11	12
LastPass	×	×	×!	×*	×*	×*	×	×		×*	×*	
Dashlane	×*	×	×!	×	×*	×	×*	×!				×
1Password [10]	×*	×*	×*	×*		×*	×*	×*		×*		×
KeePass [11]	×	×		×	×			×	×		×	×
Bitwarden		×	×!	×	×*	×*	×	×!	×*	×*	×!	×
NordPass	×	×	×*	×	×*		×	×	×*	×*	×	
Padloc	×	×	×*	×	×*		×	×*	×	×*	×	
Keeper [12]	×*	×* [13]	×*	×*	×*	×*	×*	×*	×*	×*	×*	×*
Firefox		×		×	×	×	×	×				

TABLE 2.1 – Fonctionnalités proposées par les candidats

× : L'application propose cette fonctionnalité
***** : Fonctionnalité proposée mais avec un version premium (payante)
! : Limitations avec une version gratuite

10. L'application est totalement payante et différents abonnements sont proposés
11. En général, nécessite l'installation de plugins supplémentaires afin de profiter de toutes les fonctionnalités
12. Se référer à la note de bas de page 10
13. Extension *KeeperFill*

Sur tous les candidats sélectionnés, nous remarquons que la plupart offre la majorité des fonctionnalités énumérées plus haut. Nous constatons que l'offre des constructeurs de gestionnaires de mots de passe est assez variée et répond à la demande des particuliers et des entreprises.

Par rapport aux restaurations de sauvegarde, les gestionnaires cloud-based vont automatiquement créer des backups toutes les nuits, donc la restauration se fait directement dans le gestionnaire. Pour bitwarden, lorsque le gestionnaire est hébergé on-premise, il est nécessaire de créer ses propres procédures de sauvegardes. Etant donné que KeePass est uniquement en local, les sauvegardes doivent être faites manuellement et peuvent être importées sur l'application. Toutes ces solutions nécessitent le master password. Si ce dernier est oublié, il existe plusieurs solutions différentes en fonction des constructeurs (fonctionnalité pas disponible sur KeePass).

La "sauvegarde" qui ne nécessite pas d'avoir son master password est l'exportation des données en fichier CSV, mais à moins de chiffrer le fichier, les données sont en claires ce qui n'est évidemment pas sécurisé et pas très recommandé.

2.2 Plateformes

Cette partie va permettre de visualiser sur quelles plateformes les gestionnaires de mots de passe sélectionnés sont supportés.

Application	Windows	MacOS	Linux	Android	iOS	Navigateur
LastPass	×	×	×	×	×	×
Dashlane						×
1Password	×	×	×	×	×	
KeePass	×	×*	×*	×*	×*	×*
Bitwarden	×	×	×	×	×	×
NordPass	×	×	×	×	×	
Padloc	×	×	×	×	×	×
Keeper	×	×	×	×	×	×
Firefox						×

TABLE 2.2 – Plateformes supportées par les différentes applications

× : L'application est supportée sur ces plateformes
* : Des applications (ou des paquets) compatibles avec KeePass Password Safe non-officielles mais contribuées existent

Même si un gestionnaire supporte toutes les plateformes indiquées, il est nécessaire d'aller vérifier les conditions d'utilisation du système, c'est-à-dire les versions des plateformes afin de s'assurer que l'application fonctionnera quand même.

Cependant, nous constatons que la majorité des applications sont disponibles sur les plateformes les plus courantes, et même si elles ne le sont pas, il y a souvent une solution non-officielle (notamment pour KeePass) ou via le navigateur qui existe.

2.3 Prix

Nous allons passer brièvement en revue les prix proposés par les gestionnaires de mots de passe. Chaque application propose leurs propres gammes de prix avec également des abonnements possibles pour les particuliers, familles ou entreprises.

2.3.1 Particuliers

Pour la plupart des applications, nous pouvons retrouver 3 gammes de prix ; Gratuit, Premium, Famille. L'offre familiale va être plus chère car les gestionnaires de mots de passe sont conçus pour pouvoir avoir plusieurs gestionnaires chiffrés individuels.

Les tarifs ci-dessous sont exprimés en mensualités et en USD.

Application	Gratuit	Premium	Famille
LastPass	$0	$3	$4
Dashlane	$0	$3.99	$5.99
1Password	non	$2.99	$4.99
KeePass [14]	$0	non	non
Bitwarden	$0	<$1	$3.33
NordPass	$0	$1.84	$4.99
Padloc	$0	$3.49	$5.95
Keeper	non	$2.92	$6.25
Firefox	non	non	non

TABLE 2.3 – Tarifs pour particuliers

14. Gratuit et open-source

2.3.2 Entreprises

Les entreprises ont quant à elle des prix différents dû à leurs besoins spécifiques où ils pourraient avoir besoin d'un devis personnel afin de choisir l'abonnement qui convient au mieux à leur infrastructure. Il existe plusieurs catégories qui sont en fonction du nombre d'employés et également par rapport aux fonctionnalités souhaitées.

Chaque prix est indiqué en mensualités, en USD et par employé.

Application	Team	Business
LastPass	$4	$6
Dashlane	$5	$8
1Password		$7.99
KeePass [15]	non	non
Bitwarden	$3	$5
NordPass		$3.50*
Padloc	$3.49	$6.99*
Keeper		$3.75*
Firefox	non	non

TABLE 2.4 – Tarifs pour les entreprises

* : Il y a la possibilité d'établir un devis en fonction des besoins spécifiques de l'entreprise

2.4 Marché actuel

Afin d'effectuer une étude un peu plus approfondie et afin d'établir un constat de la demande actuelle sur le marché et de leur popularité, nous allons analyser les différentes statistiques des gestionnaires de mots de passe.

Malgré les multiples fonctionnalités proposées par les *password managers*, les particuliers restent plutôt réticents à l'idée d'en utiliser un régulièrement ; d'après un sondage lancé par PasswordManager[19] aux Etats-Unis avec des personnes âgées de 18-55+, seulement 22.5% utilisent des gestionnaires de mots de passe. Une autre étude de Security.org[21] de novembre 2021, également lancée aux Etats-Unis, ressort les mêmes statistiques ; 20% des utilisateurs utilisent ces derniers. Les autres solutions communes pour stocker ses identifiants sont la mémorisation, le papier, la réutilisation, etc. Nous pouvons sans aucun doute déclarer que ces méthodes ne sont pas très sécurisées.

15. Voir 14

Néanmoins, nous pouvons expliquer cette réticence à l'aide des études citées ci-dessus qui déclarent qu'au niveau des utilisateurs qui n'utilisent pas de gestionnaires de mots de passe, 70% ne font pas confiance à la sécurité qu'elles fournissent, ils pensent que leur application pourrait être hackée. Certains, ne font également pas confiance aux constructeurs de ces dernières en pensant qu'ils volent leurs données.

En contradiction à ces avis populaires, en se basant sur un sondage de 2022 de bitwarden[4], globalement, 35% des utilisateurs sont plus inquiets des cyberattaques par rapport à l'année 2020. Nous pouvons justifier ces inquiétudes avec le fait que le nombre de cyberattaques effectuées en 2021 a augmenté (en partie dû au COVID-19 et au *home office*). Le DBIR de 2022 (Data Breach Investigations Report)[22] indique qu'il y a eu une augmentation de 13% des vols de données (dont 85% font partie de vulnérabilités humaines).

Avec toutes ces statistiques, nous pouvons constater que malgré une utilisation encore trop basse des gestionnaires de mots de passe, les particuliers s'y intéressent progressivement dû aux attaques et vols de données en progression constante. Cependant, il y a un manque de confiance général sur ces derniers, surtout envers les constructeurs. C'est pourquoi, la sécurité parfaite au sein des gestionnaires est un sujet très important si l'on souhaite augmenter la protection des données et éviter des vulnérabilités humaines (notamment l'utilisation de mots de passe trop de simple, comme "123456"). La sécurité "presque" parfaite des applications pourraient également baisser les vols de données par des personnes malveillantes.

2.5 Récapitualtif de l'étude

Nous allons résumer toutes les informations que nous avons recueillies dans ce chapitre-ci ; au final, nous constatons que les gestionnaires de mots de passe qui sont actuellement sur le marché (ici les plus populaires), sont assez complets au niveau des fonctionnalités proposées et ils sont adaptées pour tout type d'utilisation (personnelle, familiale ou professionnelle). Pour les gestionnaires payants, leurs prix sont assez abordables pour l'offre qu'ils proposent. Toutefois, même les gestionnaires en version gratuite, convient tout à fait à une utilisation quotidienne.

Au niveau des applications comparées, toutes ont leurs points positifs et leurs points négatifs (l'aspect sécuritaire et les failles connues seront discutées dans le chapitre *étude sécuritaire*).

LastPass propose une version gratuite avec les fonctionnalités classiques que l'on attend d'un gestionnaire de mot de passe. La limite est que l'application n'est accessible que depuis un seul type d'appareil, ils font la différence entre ordinateur (fixe et portable) et appareil mobile (téléphone, montre, tablette). La version payante offre le MFA ainsi qu'un dashboard (avec les alertes de sécurité et la surveillance sur les données compromises), ce qui est une fonctionnalité intéressante.

La version gratuite de DashLane propose un stockage jusqu'à 50 mots de passe, ce qui est au

final assez limtité mais il offre le 2FA ainsi que le partage sécurisé (jusqu'à 5 comptes). La version premium, permet l'utilisation d'un VPN ainsi qu'une synchronisation sur plusieurs appareils.

1Password est totalement payant mais est l'un des gestionnaires de mots de passe le plus populaire sur le marché.

KeePass est une application gratuite et open-source. Il propose une grande sélection de plugins assez utiles et variés, ce qui permet une grande offre, en plus d'être complètement gratuite.

bitwarden propose une version gratuite étonnement très complète avec un stockage illimité de mots de passe et un nombre illimité d'appareils. La version premium offre un 2FA avancé (notamment la connexion à l'aide d'une Yubikey) ainsi que des rapports de sécurité.

NordPass propose également une version gratuite complète qui permet le MFA ou encore la synchronisation entre plusieurs appareils, ce qui est très utile. Le premium propose l'aspect sécuritaire en plus. Cependant, c'est la solution gratuite la meilleure de tous les candidats sélectionnés.

Padloc n'est pas un gestionnaire très populaire mais il l'avantage d'être open-source et d'être disponible sur Github [16]. La version gratuite n'offre pas beaucoup de fonctionnalités mais il y a la possibilité de stocker un nombre illimité de secrets et d'y connecter un nombre illimité d'appareils. De plus, il est multi-plateformes.

Keeper est complètement payant mais a une offre très complète et est particulièrement bien adapté pour les entreprises.

Finalement, le gestionnaire de mots de passe proposé par Firefox est directement inclus avec le navigateur, ainsi ses fonctionnalités proposées sont assez basiques et pas très poussées, mais il propose les fonctionnalités attendues d'un gestionnaire, c'est-à-dire enregistrement, génération et synchronisation de mots de passe.

16. https://github.com/padloc/padloc

Chapitre 3

Étude sécuritaire

Ce chapitre est dédié à toute l'analyse sécuritaire des gestionnaires de mots de passes en général. Nous allons dans un premier temps décrire comment ces applications sont sécurisées en fonction de leur type, puis justifier l'importance d'une forte sécurité suite à l'augmentation de la demande des entreprises et des particuliers.

Dans un second temps, nous allons identifier et analyser toutes les menaces existantes et / ou potentielles des *password manager* en mettant en avant les failles actuellement connues des constructeurs et les conséquences de ces dernières ou des faiblesses qui pourraient survenir à tout moment (par exemple des cyberattaques).

Finalement, nous allons rédiger toutes les exigences sécuritaires que doivent respecter les gestionnaires de mots de passe afin que ces dernières garantissent une utilisation sûre qui évite des pertes ou vol de données.

3.1 Implémentation de la sécurité dans les gestionnaires de mots de passe

Dans cette section, afin de se baser sur des gestionnaires de mots de passe déjà existants et de pouvoir comparer les différentes sécurités implémentées, nous allons reprendre les 9 candidats sélectionnés dans la partie *étude de marché*, c'est-à-dire ; *LastPass*, *Dashlane*, *1Password*, *KeePass*, *Bitwarden*, *NordPass*, *Padloc*, *Keeper* et *Firefox*. Toutes les informations citées sont basées sur les *security whitepapers* des constructeurs[15][6][1][12][3][18][13].

Les gestionnaires de mots de passe sélectionnés fonctionnent tous de la même manière, au final cette méthode est plutôt classique dans les architectures des applications. Un *master password* (qui est seulement connu par l'utilisateur) est généré ou entré par l'utilisateur et va permettre le déverrouillage de l'application et le chiffrement / déchiffrement en local de

toutes les données stockées.

À part pour les gestionnaires en local qui gèrent la sécurité différemment, ils mettent en avant le *Zero-knowledge encryption*. C'est une méthode qui va permettre un chiffrement *end-to-end* et qui va sécuriser au mieux les données personnelles et sensibles des utilisateurs, des serveurs du constructeur. En sachant que toutes les données sont stockées dans le cloud du provider, afin d'éviter que n'importe qui puisse y avoir accès, toutes les données sont chiffrées avant d'être envoyées au serveur. Ainsi, les données sont uniquement déchiffrées sur le device de l'utilisateur et la clé de chiffrement reste également en local.

Nous allons décrire dans les sous-sections suivantes comment la sécurité est implémentée dans les gestionnaires de mots de passe en fonction de leur type afin d'aller un peu plus en détail.

3.1.1 Les gestionnaires browser-based

Les gestionnaires de mots de passe *browser-based* proposent des fonctionnalités classiques et ne sont pas très poussés. Ce sont des applications légères qui sont pensées pour faciliter au mieux les utilisateurs.[23]

Par défaut, ces applications n'activent pas de *master password* et certaines n'en proposent même pas pour ajouter un chiffrement supplémentaire. Toutefois, ils proposent la fonctionnalité de 2FA.

Firefox fonctionne localement ou avec la synchronisation qui demande l'utilisation du cloud. Si la synchronisation n'est pas activée, les mots de passes stockés sont directement chiffrés sur l'appareil et sont ajoutés à un fichier *logins.json* qui se trouve dans le répertoire de l'utilisateur.

Il propose également la fonctionnalité d'ajouter un master password afin d'avoir une couche sécuritaire supplémentaire (par défaut, cette fonction est désactivée), ainsi, sans un mot de passe principal et sans l'activation du 2FA, les mots de passe sont accessibles en clair sur le navigateur dès le moment où on a accès à l'appareil et que l'utilisateur est connecté à son compte (ce qui est fortement probable, car le compte reste connecté, même après une fin de session). Toutefois, lors de l'ajout d'un master password, ce dernier est uniquement défini en local et n'est pas synchronisé entre profils ou appareils, mais il chiffrera toutes les données en local.

Au niveau du fonctionnement[2] (sans master password), les identifiants sont chiffrés à l'aide de 3DES-CBC et sont directement stockés dans un fichier JSON *logins.json* encodés en ASN.1 puis en Base64. La clé de chiffrement est stockée dans une base de donnée *key4.db*. Il existe actuellement des outils pour déchiffrer les mots de passe du gestionnaire.

Si l'option de synchronisation (*Firefox Sync*) est activée[20], les données stockées sur les serveurs Mozilla seront chiffrés. Nous pouvons se baser sur le schéma suivant qui explique le

processus de synchronisation des données avec les serveurs Mozilla :

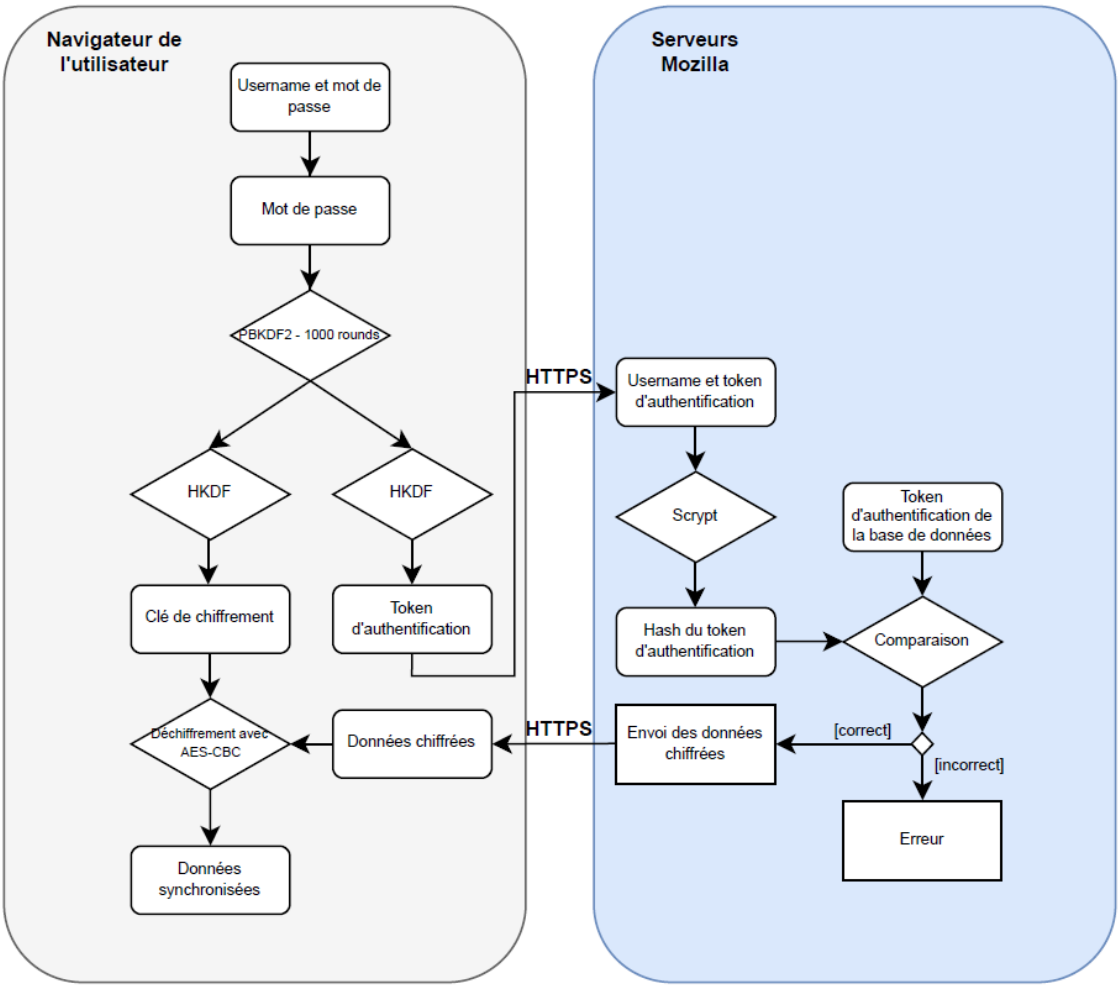

FIGURE 3.1 – Schéma de synchronisation de données sur Firefox

Les données chiffrées sont protégées avec HMAC-SHA256 afin de pouvoir authentifier les données avant de les déchiffrer. La méthode utilisée est Encrypt-then-MAC. Cela permet de protéger l'intégrité des données en clair et chiffrées.

Comme cité précédemment, lors d'un ajout de master password afin de protéger les données localement, Firefox va tout d'abord chiffrer les données localement (le stockage se fait comme expliqué plus haut) et va les rechiffrer lors de la synchronisation avec le processus expliqué à l'aide du schéma.

Au final, ce design cryptographique est plutôt classique au sein des gestionnaires de mots de

passe qui utilisent les serveurs du constructeur pour stocker les données.

Les autres gestionnaires de mots de passe browser-based fonctionnent en général de la même manière avec les données synchronisées. Chrome stocke également les identifiants dans un fichier local protégé avec DPAPI (Microsoft's Data Protection API).

3.1.2 Les gestionnaires en local

Pour les gestionnaires qui fonctionnent uniquement en local, nous allons nous baser sur l'implémentation sécuritaire de KeePass, qui est open-source, ce qui peut faciliter à comprendre tout le concept. Dans cette section, nous n'allons pas détailler toute l'architecture mais rester plutôt en surface. D'autres gestionnaires de mots de passe fonctionnent également en *offline* avec un stockage local, cependant lors de la première connexion, il y a quand même des informations envoyées aux serveurs du constructeur (comme 1Password par exemple), ce qui n'est pas le cas pour l'application de base KeePass.

Etant donné que KeePass ne fonctionne qu'en local, il est important de bien gérer la mémoire et le stockage de données sensibles.

Toutes les données se trouvent dans un fichier de base de données spécial *.kdbx*. Ce fichier contient toutes les données du gestionnaire (mots de passe, usernames, etc.) et est chiffré (également compressé en GZIP si on le souhaite). Dans la version de KeePass 2.x, les chiffrements supportés sont AES256-CBC et ChaCha20.

La base de données est stockée où l'utilisateur le souhaite (avec une possibilité de la stocker dans un cloud), c'est pourquoi la sécurité repose sur la complexité du mot de passe. Elle est structurée avec un header et un contenu[16][10].Dans le header, sont stockées différentes informations ; un UUID indiquant le cipher, une indication si le fichier est compressé, différentes seed (voir 3.2), l'IV pour le chiffrement et des bytes pour l'authentification (générés aléatoirement lors de la sauvegarde de la base de données). Le corps du fichier contient des blocs hachés avec HMAC-SHA256 et des blocs de données qui ont un format XML lorsqu'ils sont déchiffrés.

Tous les deux sont authentifiés avec le schéma Encrypt-then-Mac avec HMAC-SHA256.

Au niveau de l'utilisation de la mémoire du processus, lors de l'ouverture de la base de données chiffrée, elle est chargée en mémoire. La protection de la mémoire s'applique aux données sensibles telles que la Master key et des mots de passe. Dès que la base de donnée est sauvegardée, les données chiffrées sont envoyées sur le disque.

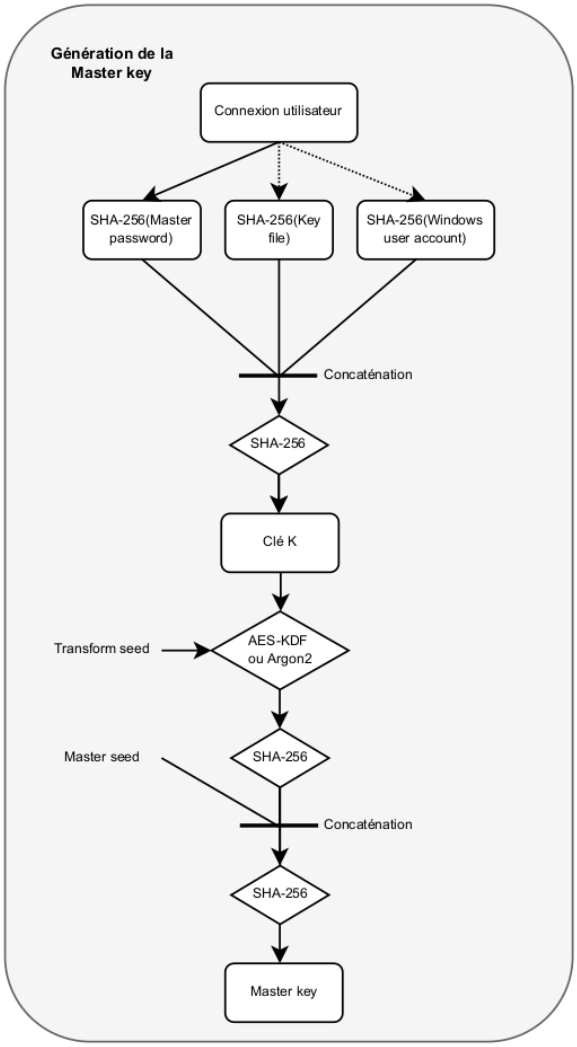

FIGURE 3.2 – Génération de la Master key sur Keepass

La Master key sur KeePass prend plusieurs arguments différents et est générée d'une manière assez complexe. L'utilisateur doit obligatoirement fournir un master password, et peut également utiliser un key file et / ou le compte utilisateur Windows.

Chaque composant est haché avec SHA-256 et sont concaténés et hachés ensemble. En output, on a une clé composite K qui va être dérivée à l'aide de AES-KDF ou Argon2. Les paramètres de ces deux algorithmes peuvent être configurés dans les paramètres de la base de données.

Chaque output est haché avec SHA-256 et au final, on obtient la Master key qui permettra de déchiffrer la base de données.

Les deux différentes seeds utilisées dans la génération de la clé sont stockées dans le header de la base de données *.kdbx*.

Cette architecture permet de se protéger contre les attaques par dictionnaires et le brute-force de la Master key.

3.1.3 Les gestionnaires cloud-based

Les gestionnaires de mots de passes cloud-based ont tous une architecture similaire dû au fait que toutes les données sont stockées sur les serveurs du constructeur. Il y a des différences avec l'authentification de l'utilisateur et des algorithmes cryptographiques choisis, mais le design sécuritaire a la même base au niveau de la connexion de l'utilisateur et du chiffrement du gestionnaire.

Ainsi, afin d'expliquer un peu plus en détail le fonctionnement d'un gestionnaire cloud-based, nous allons prendre l'exemple de LastPass. Nous allons nous basé sur le schéma ci-dessous afin d'appuyer nos propos.

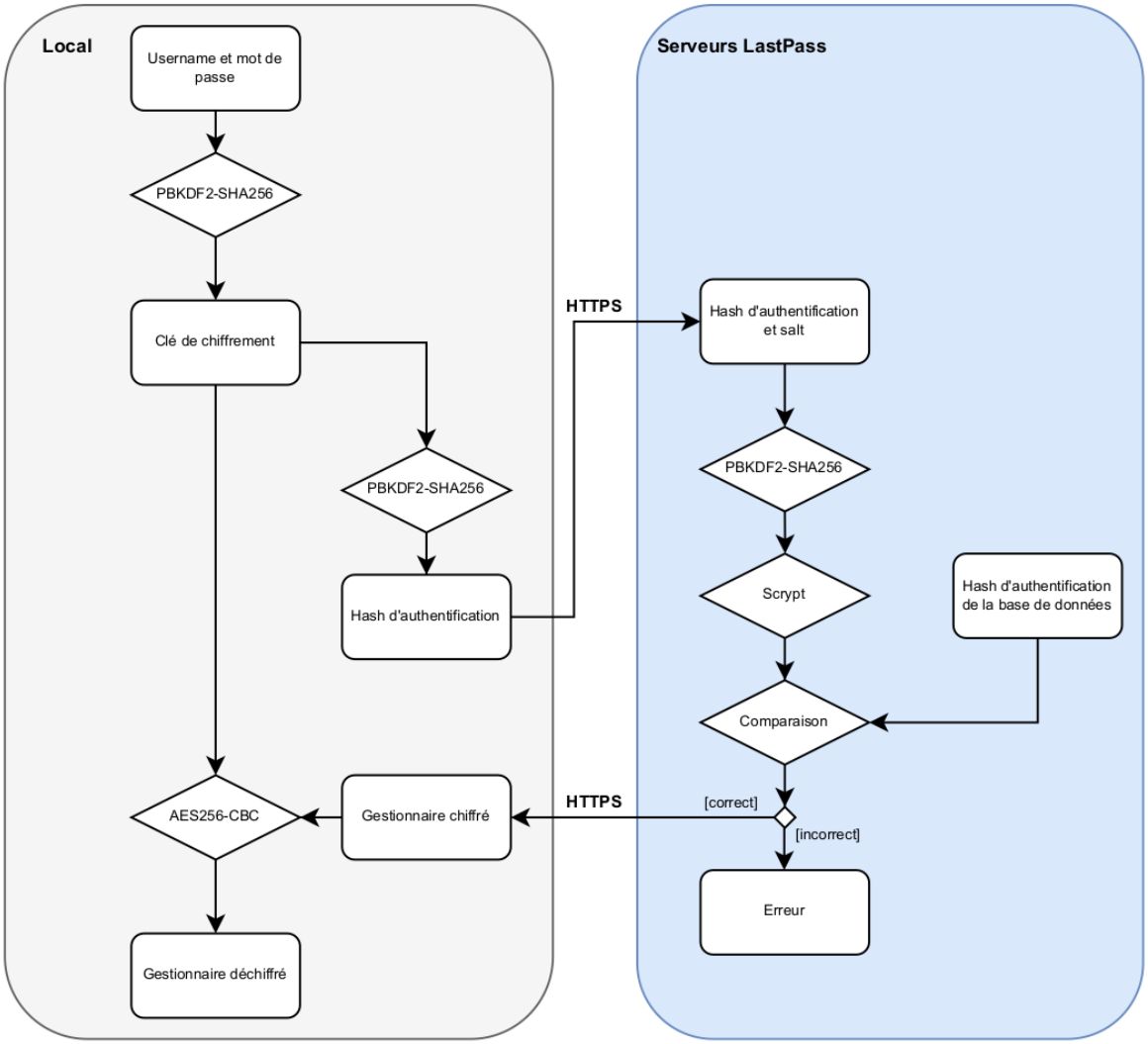

FIGURE 3.3 – Schéma de déchiffrement de LastPass

Afin de générer la clé de chiffrement, ce dernier dérive le master password en utilisant le nom d'utilisateur comme sel. Il utilise l'algorithme PBKDF2-SHA256 avec 100'100 rounds.

3.1.4 Partage d'informations

3.1.5 Perte du master password

3.1.6 3 états du gestionnaire de mot de passe

Les gestionnaires de mots de passe ont généralement 3 états différents, *Not Running*, *Unlocked State* et *Locked State*. Nous allons expliquer plus en détails comment ils fonctionnent lorsqu'ils sont dans les différents états. Nous nous basons sur un article qui analyse le management des secrets[11].

3.1.6.1 Etat *Not Running*

C'est l'état du password manager lorsqu'il n'a jamais été utilisé et configuré après son installation. On définit également cet état s'il n'a pas été lancé depuis le dernier redémarrage du système ou a été arrêté par un utilisateur. Dans cet état, le gestionnaire doit garantir qu'il n'y a aucune donnée sensible stockée sur le disque, comme une clé de chiffrement ou le master password.

3.1.6.2 Etat *Unlocked State*

Cet état indique que le gestionnaire fonctionne et donc, l'utilisateur a entré son master password afin de déchiffrer toutes les données afin d'avoir accès aux informations stockées. Le gestionnaire doit garantir qu'il n'est pas possible d'extraire aucune information sensible de la mémoire.

3.1.6.3 Etat *Locked State*

Nous considérons cet état lorsque l'utilisateur a lancé le gestionnaire (déjà configuré) sans avoir encore entré le master password ou qu'il a lui même verrouiller son gestionnaire. À ce moment, il ne devrait pas y avoir de données sensibles stockées sur le disque afin d'éviter toute extraction.

3.1.7 Algorithmes cryptographiques

- les algos utilisés pour le chiffrement et auth des données

3.1.8 L'importance d'une forte sécurité

à voir si utile

3.2 Analyse des menaces

3.2.1 Failles connues des constructeurs

à voir si je devrais pas les ajouter dans le chapitre de l'analyse de chaque gestionnaire sélectionné

3.2.2 Conséquences d'une quelconque faiblesse

à voir si utile, mais les conséquences seront sûrement soulignées lorsque je ferai l'analyse de menaces de toute manière -
remember me du master password HAA

3.3 Exigences sécuritaires à respecter

Chapitre 4

Sélection des candidats

4.1 Critères de sélection

Chapitre 5

Conclusion

Bibliographie

[1] 1Password. 1password security design, 2021.

[2] Apr4h. Decrypting browser credentials for fun (but not profit), 2019.

[3] bitwarden. Bitwarden security whitepaper, 2022.

[4] bitwarden. World password day global survey full report, 2022.

[5] Clifford Colby, Rae Hodge, and Attila Tomaschek. Best password manager to use for 2022, 2022.

[6] Dashlane. Security white paper, 2022.

[7] ECRYPT-CSA. Algorithms, key size and protocols report, 2018.

[8] Elizabeth A. Gallagher. Choosing the right password manager. *Serials Review*, 45 :1–2, 84–87, 2019.

[9] Eric Griffith. How to master google password manager, 2022.

[10] Jingxin Hong Hengwei Zhang and Jun Hu. Analysis of encryption mechanism in keepass password safe 2.30. *2016 10th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, pages 43–46, 2016.

[11] ISE. Password managers : Under the hood of secrets management, 2019.

[12] KeePass. Security, 2022.

[13] Keeper. Keeper encryption model, 2022.

[14] Michael Kurko. Best password managers, 2022.

[15] LastPass. Technical whitepaper.

[16] lgg. Keepass file format explained, 2017.

[17] Paulius Masiliauskas. Most secure password managers in 2022, 2022.

[18] Padloc. Security whitepaper, 2022.

[19] PasswordManager. Password manager trust survey, 2020.

[20] Tom Ritter. Private by design : How we built firefox sync, 2018.

[21] Security.org Team. Password manager and vault 2021 annual report : Usage, awareness, and market size, 2021.

[22] Verizon. 2022 data breach investigations report, 2022.

[23] Liz Wegerer. Is your browser's password manager safe ?, 2022.

Table des figures

Liste des tableaux

Liste des listings

Annexe A

Outils utilisés pour la compilation

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Annexe B

Journal de travail

TABLE B.1 – Journal de travail

Date	Description	Rech. [h]	Dev. [h]	Rapport [h]	Admin [h]
> 20.09.22	Discussion avec le professeur responsable, établissement du cahier des charges, introduction	7	0	10	4
20.09.2022	Update + organisation du TB, planing, relire le début du TB déjà commencé, avancement de l'étude du marché (fonctionnalités, plateformes, prix), lecture d'articles	2	0	5	1
21.09.2022	Recherches sur les statistiques des gestionnaires de mots de passe sur le marché, rédaction du chapitre étude de marché (terminé ce jour-ci)	3	0	3	0
22.09.2022	Introduction et organisation du chapitre étude sécuritaire, recherche et lecture sur les différentes implémentations sécuritaire des gestionnaires de mots de passe	3	0	1	1
23.09.2022	Recherche et lecture sur les différentes implémentations sécuritaire des gestionnaires de mots de passe et organisation du rapport	1	0	1	0
26.09.2022	Recherche et lecture sur les gestionnaires de mots de passe browser-based, rédaction dans le rapport à ce propos	4	0	1	0
27.09.2022	Recherche et lecture sur les gestionnaires de mots de passe browser-based et local-based, et rédaction dans le rapport	3	0	2	0
28.09.2022	Recherche et lecture sur les gestionnaires de mots de passe browser-based et local-based, et rédaction dans le rapport	4	0	1	0
29.09.2022	Recherche et lecture sur les gestionnaires de mots de passe local-based, et rédaction dans le rapport	5	0	3	0
30.09.2022	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0

Le journal de travail continue à la page suivante.

Date	Description	Rech. [h]	Dev. [h]	Rapport [h]	Admin [h]
xx.xx.2020	Test	0	0	4	0
xx.xx.2020	Test	0	0	4	0