

Sommaire

I. Descriptif général de l'application	2
1. Problème et solution proposée	2
2. Question de sécurité	2
3. Fonctionnalités supplémentaires.....	3
4. Note importante	3
II. Graphisme	4
1. Droits des ressources	4
2. Quelques précisions	4
3. La maquette	5
III. Détails sur les fonctionnalités.....	9
1. Première utilisation.....	9
2. Fenêtre principale	9
3. Ajout ou modification d'un mot de passe	11
4. Ajout ou modification d'une catégorie.....	11
5. Connexion/Déconnexion	11

I. Descriptif général de l'application

1. Problème et solution proposée

Avec la banalisation d'Internet et l'explosion du nombre de services proposés sur la Toile ou ailleurs, nous avons tous à retenir une quantité importante de mots de passe : pour sa/ses messagerie(s), son compte bancaire etc. C'est inévitable, on en oublie certains, et il n'est pas rare de devoir aller jusqu'à la demande d'un nouveau mot de passe que l'on risque bien de reperdre.

C'est précisément à ce problème que l'application "Gestionnaire de Mots de Passe" veut apporter une solution, et son principe pourrait se résumer en une image très simple : un coffre-fort contenant des dizaines de mots de passe différents, tous protégés par un autre, unique.

Plus besoin de retenir tous ses mots de passe, le Gestionnaire le fait pour nous. Il suffit simplement de choisir et mémoriser un unique mot de passe pour protéger tous les autres, et avoir enfin l'esprit tranquille !

2. Question de sécurité

Tout naturellement, une énorme importance doit être accordée à la sécurité : les mots de passes stockés doivent être parfaitement sécurisés. C'est pourquoi un certain nombre de précautions sont prises :

- Le mot de passe unique est stocké sous la forme d'une clé cryptée de 256bits, obtenue par l'utilisation de l'algorithme de hachage SHA-256. Cet algorithme est à sens unique : disposer de la clé hachée ne permet pas de retrouver le mot de passe.
- Les autres mots de passe, quant à eux, sont destinés à être affichés en clair à un moment. Il est donc nécessaire de les crypter à l'aide d'algorithmes dits symétriques. Ceux utilisés sont AES et TwoFish qui sont réputés pour être les plus sûrs.
- La technique du "sel" (*chaîne aléatoire rajoutée à la fin des mots de passe*) est utilisée pour empêcher une éventuelle attaque par dictionnaire

L'utilisation de l'ensemble de ces algorithmes et techniques garantissent la sécurité des mots de passe.

Par ailleurs, certaines précautions sont prises pour éviter des erreurs dommageables :

- lorsque l'on rentre un mot de passe au clavier, les caractères sont affichés par des étoiles
- tout mot de passe rentré dans l'application doit être tapé une deuxième fois pour s'assurer de sa validité

3. Fonctionnalités supplémentaires

L'application permet d'aller encore plus loin en proposant les fonctionnalités suivantes :

- générateur de mot de passe : l'application propose à l'utilisateur un mot de passe généré automatiquement. Ce mot de passe se veut sécurisé et facile à retenir (*composition de 3 mots, combinés à des chiffres*)
- évaluation de la qualité d'un mot de passe : en se basant sur certains critères (*taille du mot de passe, nombre de mots, utilisation de caractères autre qu'une lettre et combien...*), l'application évalue sur une échelle de 1(*faible*) à 4(*parfait*) la force d'un mot de passe.
- possibilité de classer ses mots de passe par catégorie (*web, banque etc.*) et d'associer à chacun certaines informations (*nom, description, url*). Par défaut, l'application proposera certaines catégories (*à définir*).

4. Note importante

Malheureusement, au prix de la sécurité des mots de passe, si le mot de passe unique est perdu, tous les autres le sont aussi. Par ailleurs le seul moyen de réutiliser l'application serait de la désinstaller puis de la réinstaller.

II. Graphisme

1. Droits des ressources

Tous les éléments graphiques qui composent cette application sont libres de droits et/ou réalisés pour les besoins du programme. La police de caractère utilisée à titre d'exemple (*susceptible de changement*) est Arial.

Sont citées ci-après les différentes sources d'où ont été extraites certaines ressources :

- deviantart.com, utilisateur iTweek (<http://itweek.deviantart.com/art/Knob-Buttons-Toolbar-icons-73463960>)
- icône cadenas du Crystal Project (<http://www.everaldo.com/crystal/?action=downloads>)

2. Quelques précisions

Plusieurs icônes spécifiques sont utilisées pour cette application :

- un petit cadenas qui est en quelque sorte le logo de l'application (*qui sert de "launcher" à l'application*)
- le cadenas grand format utilisé dans la page de démarrage de l'application (*voir "3. La maquette"*)
- 4 icônes en forme de boule (*couleur verte, bleue, orange et rouge*) qui indiquent la force d'un mot de passe

Le fond est de couleur unie (*blanc*) avec un simple dégradé noir sur le haut de l'écran.

Le reste des éléments graphiques sont ceux par défaut de l'appareil.

3. La maquette

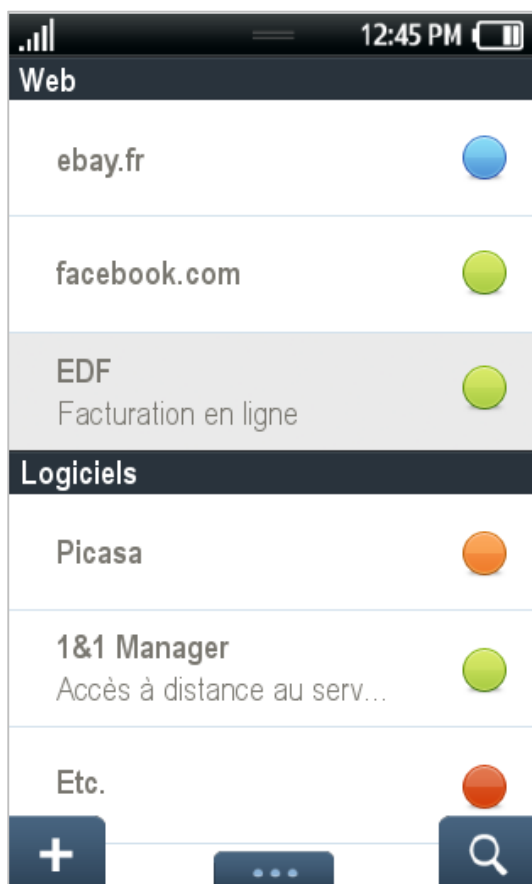
Ce qui suit ne constitue qu'une maquette et **la disposition des éléments, ainsi que les couleurs, peuvent-être sujettes à certains changements.**



Page de démarrage de l'application (*quand la personne n'est pas encore authentifiée*)



Formulaire d'authentification



Page de démarrage de l'application (*quand la personne est authentifiée*).

Ici, "Web" et "Logiciels" sont des catégories créées par l'utilisateur.

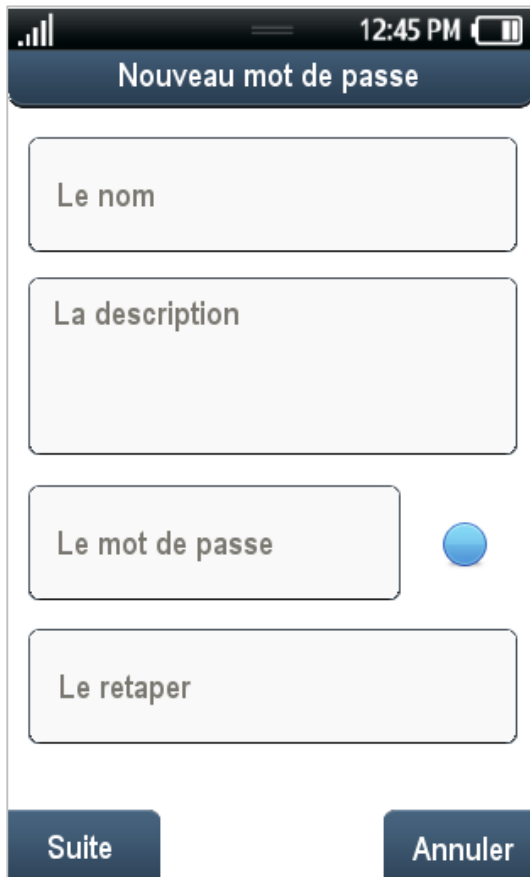
"ebay.fr", "facebook.com" etc. sont des noms de mot de passe et les icônes en face indiquent la force du mot de passe (*vert pour "parfait" et rouge pour "faible"*)

"Facturation en ligne" est une description

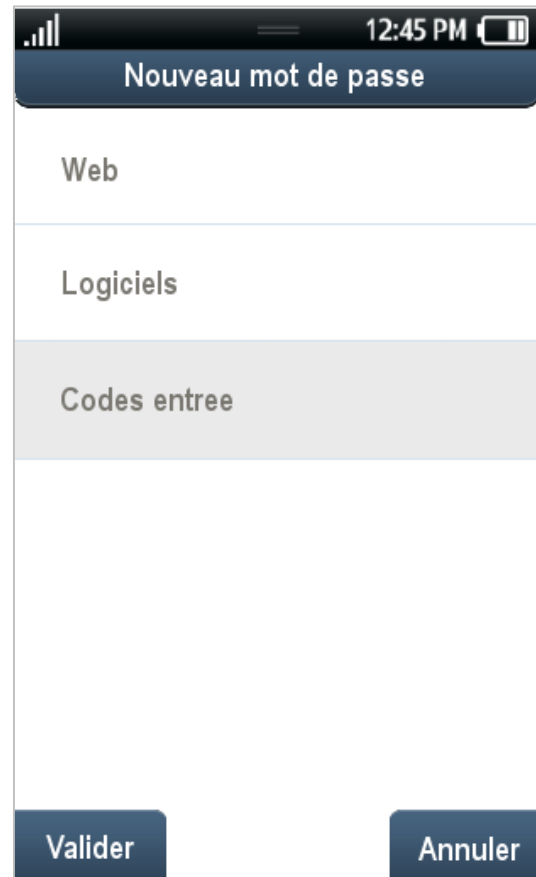
Note : cette maquette correspond également au résultat d'une recherche



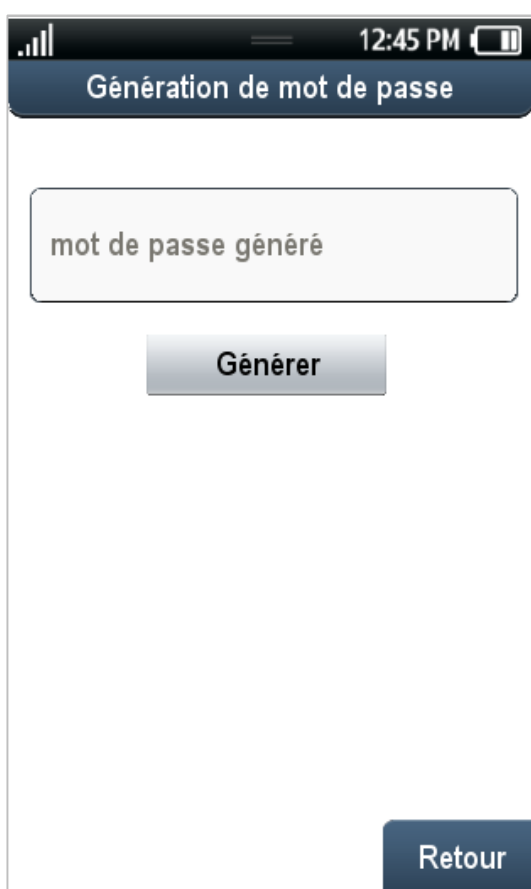
Sélection d'une catégorie



Ajout d'un mot de passe (étape 1/2)
L'icone indique en temps réel la force du
mot de passe tapé



Ajout d'un mot de passe (étape 2/2) {choix
d'une catégorie}



Génération d'un mot de passe aléatoire



Recherche d'un mot de passe (*la page des résultats est la même que la page de démarrage présentée plus haut*)

III. Détails sur les fonctionnalités

Cette partie recense les éléments fonctionnels et certains comportements qui n'apparaissent pas dans la maquette.

1. Première utilisation

Lors de la première utilisation de l'application, l'utilisateur ne dispose pas encore de mot de passe unique. Une boîte de dialogue va donc s'ouvrir et lui proposer d'entrer deux fois le mot de passe de son choix.

Chose importante, ce mot de passe unique ne sera pas accepté si il n'a pas une force d'au moins 3/4 (si l'on considère l'échelle définie précédemment dans ce document).

Il pourra alors accéder à l'ensemble des fonctions comme vu dans la maquette.

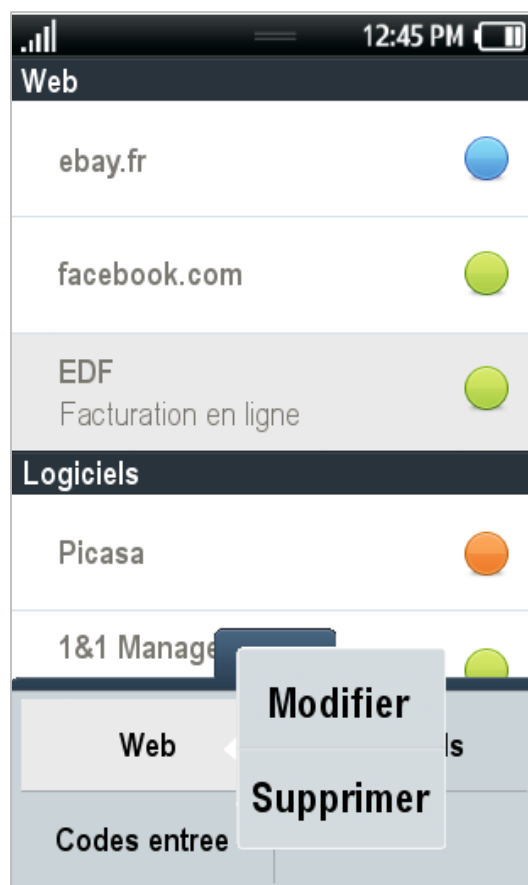
2. Fenêtre principale



Comme cela se voit dans la maquette, l'application est composée d'une fenêtre principale qui liste l'ensemble des mots de passe (leur nom, leur description et leur force symbolisée par une icône en forme de boule), triés par catégorie.

Le menu des catégories permet d'afficher la liste des catégories. Depuis cette liste, deux actions sont possibles :

- un appui rapide sélectionne la catégorie et ne laisse à l'écran que les mots de passe appartenant à cette catégorie
- un appui long affiche un sous-menu permettant de modifier et/ou supprimer cette catégorie



La suppression d'une catégorie n'entraîne pas la suppression des mots de passe associés : ils sont placés dans une supercatégorie (*sur laquelle l'utilisateur n'a pas la main*) "Indéfini".

Note: la modification ou suppression d'un mot de passe se fait de la même manière qu'une catégorie, à l'aide d'un appui long qui affiche un sous-menu.

Le menu principal affiche la liste des actions possibles déjà vus dans la maquette :

- Ajouter un mot de passe
- Ajouter une catégorie

- Tester la force d'un mot de passe
- Générer un mot de passe

Enfin, le dernier bouton mène à la page de recherche déjà présentée dans la maquette.

3. Ajout ou modification d'un mot de passe

Comme vu sur la maquette, l'ajout ou la modification se fait en deux temps : on rentre d'abord les informations concernant le mot de passe, puis on sélectionne une catégorie avant de valider.

4. Ajout ou modification d'une catégorie

La maquette et le comportement sont similaires à ce qui a été présenté pour le mot de passe, c'est pourquoi cette partie ne sera pas détaillée.

5. Connexion/Déconnexion

L'utilisateur est automatiquement désauthentié dès l'instant où il quitte l'application, et ce par question de sécurité.