

# Spécification technique des besoins

|            |                  |
|------------|------------------|
| Version    | 1.3              |
| Date       | 28 février 2013  |
| Rédigé par | Florian GUILBERT |
| Relu par   | Baptiste DOLBEAU |

## MISES À JOUR

| Version | Date       | Modifications réalisées   |
|---------|------------|---|
| 0.1     | 07/01/2013 | Création  |
| 1.0     | 29/01/2013 | Relecture par Baptiste DOLBEAU  |
| 1.1     | 22/02/2013 | Ajout d'un cas d'utilisation (initialisation) et changement de la priorité (chiffrement document/commentaire) |
| 1.2     | 26/02/2013 | Ajout d'un cas d'utilisation (génération d'un nouveau mot de passe)   |
| 1.3     | 28/02/2013 | Modifications de listes d'amis et du cas concernant le déchiffrement de mot de passe                          |
|         |            |   |

## Table des matières

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Objet</b>   | <b>4</b>  |
| <b>2</b> | <b>Documents applicables et de référence</b>             | <b>4</b>  |
| <b>3</b> | <b>Terminologie et sigles utilisés</b>                   | <b>4</b>  |
| <b>4</b> | <b>Exigences fonctionnelles</b>                          | <b>4</b>  |
| 4.1      | Présentation de la mission du produit logiciel . . . . . | 4         |
| 4.2      | Initialisation . . . . .                                 | 4         |
| 4.3      | Chiffrer/déchiffrer un statut . . . . .                  | 5         |
| 4.4      | Chiffrer/déchiffrer un document . . . . .                | 6         |
| 4.5      | Gérer les liens d'amitiés . . . . .                      | 8         |
| 4.6      | Chiffrer/déchiffrer un commentaire . . . . .             | 10        |
| 4.7      | Exigences fonctionnelles détaillées . . . . .            | 11        |
| <b>5</b> | <b>Exigences opérationnelles</b>                         | <b>12</b> |
| <b>6</b> | <b>Exigences d'interface</b>                             | <b>12</b> |
| <b>7</b> | <b>Exigences de qualité</b>                              | <b>12</b> |
| <b>8</b> | <b>Exigences de réalisation</b>                          | <b>12</b> |

## 1 Objet

Proposer des solutions cryptographiques garantissant la protection de la vie privée des utilisateurs vis-à-vis d'un réseau social. Cette protection pourra être effective par le chiffrement systématique des données sensibles. Et le déchiffrement de ces données ne sera possible que par des personnes considérées explicitement par l'utilisateur.

Le projet prendra la forme d'une extension pour le navigateur *Mozilla Firefox* s'interfaçant avec une carte à puce pour effectuer certaines tâches de chiffrement.

Il ne sera pas nécessaire de créer un compte, notre projet pourra fonctionner comme patch sur un compte déjà existant.

Le réseau social étudié sera *Facebook* à moins que des problèmes spécifiques à ce réseau social soient rencontrés lors du développement du projet. Par conséquent, la terminologie utilisée correspondra à celle de *Facebook* (statut, mur, ...).

## 2 Documents applicables et de référence

- Manuel d'utilisation.
- proxy-encryption.pdf, le sujet du projet.

## 3 Terminologie et sigles utilisés

**SN** : Social Network, représente le réseau social que nous avons choisi comme support pour ce projet.

**FaceCrypt** : Application Java gérant les traitements lourds (chiffrement/déchiffrement) de l'extension et étant en relation avec la carte à puce.

**Extension** : Programme incorporé dans le navigateur permettant de manipuler les pages de *Facebook*.

**SoftCard** : Application effectuant le relais entre la carte et FaceCrypt.

## 4 Exigences fonctionnelles

### 4.1 Présentation de la mission du produit logiciel

| Référence | Fonctionnalité Globale                             | Acteur      | Priorité      |
|-----------|--|-------------|---------------|
| F-Gl-10   | Chiffrer/déchiffrer un statut                      | Utilisateur | Indispensable |
| F-Gl-20   | Chiffrer/déchiffrer un document                    | Utilisateur | Secondaire    |
| F-Gl-30   | Gérer les liens d'amitiés                          | Utilisateur | Important     |
| F-Gl-40   | Chiffrer/déchiffrer un commentaire                 | Utilisateur | Indispensable |
| F-Gl-50   | Déploiement du système sur un compte déjà existant | Utilisateur | Indispensable |

### 4.2 Initialisation

Le système doit pouvoir être adapté sur un compte déjà existant, pour se conformer aux principes de la plupart des réseaux sociaux obligeant un utilisateur à posséder un unique compte correspondant à son identité réel.

Le cas d'utilisation concernant l'initialisation du système correspond au cas C10 de la STB *SmartCard* de même le cas d'utilisation pour la génération d'un nouveau mot de passe correspond au cas d'utilisation C11.

Pour tous les cas d'utilisation décrits ci-dessous, nous supposons que l'utilisateur est déjà authentifié sur le réseau social (Facebook). Il a donc déjà inséré sa carte dans le lecteur. Par conséquent que le cas ci-dessus a déjà été fait et s'est bien déroulé.

### 4.3 Chiffrer/déchiffrer un statut

Un utilisateur peut, lorsqu'il le souhaite, écrire un message sur son mur et le chiffrer. Il choisit dans ce cas les amis qui peuvent déchiffrer ce message.

Inversement, lorsqu'un de ses amis poste (sur son mur) un message chiffré, l'utilisateur peut tenter de le déchiffrer. Si l'utilisateur fait partie des personnes autorisées, il pourra lire le message. Les éventuels commentaires du messages sont aussi déchiffrés.

|  |  |
|--|--|
| Nom : C1   | Chiffrement d'un message sur son mur   |
| Acteurs concernés  | Utilisateur  |
| Description  | L'utilisateur chiffre un message qui sera affiché sur le mur   |
| Préconditions  |  |
| Evénements déclenchants  | L'utilisateur souhaite poster un message sur son mur   |
| Conditions d'arrêt   | L'utilisateur a posté un message chiffré sur son mur, lisible uniquement par les personnes autorisées  |
| Description du flot d'événements principal :   |  |
| Acteur(s)  | Système  |
| 1. L'utilisateur saisi un message et choisit de le chiffrer, il spécifie les personnes autorisées.<br>3. L'utilisateur précise des listes d'amis ou des amis, qui pourront lire son message. | 2. L'extension demande à l'utilisateur quels amis vont être autorisés à déchiffrer le message.<br>4. L'extension récupère le message avant son envoi sur le serveur de Facebook et l'envoie à FaceCrypt qui va le chiffrer avec une clef de chiffrement, récupérer les clefs publiques des personnes autorisées et chiffrer la clef de chiffrement avec ces clefs.<br>5. FaceCrypt envoie ensuite une concaténation de ce message et des clefs chiffrées à l'extension qui enverra le tout, chiffré, sur les serveurs de Facebook. |
| Flots secondaires :  |  |
| Flots d'exceptions :   | 2. Si une des personnes choisie n'a pas de clef publique, elle ne pourra pas déchiffrer le message.  |

| Nom : C2  |  | Déchiffrement d'un message sur un mur   |  |
|---|--|---|--|
| Acteurs concernés   |  | Utilisateur   |  |
| Description   |  | L'utilisateur déchiffre un message du mur d'un de ses amis  |  |
| Préconditions   |  |   |  |
| Evénements déclenchants   |  | L'utilisateur souhaite déchiffrer un message  |  |
| Conditions d'arrêt  |  | L'utilisateur a déchiffré un message, ou pas  |  |
| Description du flot d'événements principal :                      |  |   |  |
| Acteur(s)   |  | Système   |  |
| 1. L'utilisateur appuie sur le bouton pour déchiffrer le message. |  | 2. L'extension récupère le message ainsi que les commentaires et envoie le tout à FaceCrypt.<br>3. FaceCrypt déchiffre tout le message et les commentaires avec la clef de chiffrement et envoie le message à l'extension.<br>4. L'extension affiche le résultat. |  |
| Flots secondaires :   |  |   |  |
| Flots d'exceptions :  |  | 1. Si l'utilisateur ne fait pas partie des personnes autorisées, il ne pourra pas déchiffrer le message.  |  |

#### 4.4 Chiffrer/déchiffrer un document

Un utilisateur peut choisir d'utiliser l'option de téléversement d'image du réseau social pour téléverser un document (image, fichier texte, ...) chiffré. Celui-ci sera considéré comme une image par le réseau social.

| Nom : C3  |  | Chiffrement d'un document  |  |
|---|--|--|--|
| Acteurs concernés   |  | Utilisateur  |  |
| Description   |  | L'utilisateur chiffre un document qui sera interprété comme une image par Facebook   |  |
| Préconditions   |  |  |  |
| Evénements déclenchants   |  | L'utilisateur souhaite téléverser un document  |  |
| Conditions d'arrêt  |  | L'utilisateur a téléversé un document, lisible uniquement par les personnes autorisées   |  |
| Description du flot d'événements principal :  |  |  |  |
| Acteur(s)   |  | Système  |  |
| 1. L'utilisateur téléverse un document et choisit de le chiffrer.<br><br>3. L'utilisateur précise des listes d'amis ou des amis, qui pourront lire son message. |  | 2. FaceCrypt chiffre le document avec une clef de chiffrement, récupère les clefs publiques des personnes autorisées et chiffre la clef de chiffrement avec ces clefs.<br><br>4. L'extension récupère le commentaire avant son envoi sur le serveur de Facebook et l'envoi à FaceCrypt qui va chiffrer le document avec une clef de chiffrement, récupérer les clefs publiques des personnes autorisées et chiffrer la clef de chiffrement avec ces clefs.<br><br>5. FaceCrypt envoie ensuite une concaténation de ce message et des clefs chiffrées à l'extension qui enverra le tout, chiffré, aux serveurs de Facebook. |  |
| Flots secondaires :   |  | 1. Si l'utilisateur spécifie un document qui n'est pas une image et choisit de ne pas le chiffrer, cela sera refusé par Facebook.<br><br>2. Si une des personnes choisie n'a pas de clef publique, elle ne pourra pas déchiffrer le message.   |  |
| Flots d'exceptions :  |  |  |  |

| Nom : C4  |  | Déchiffrement d'un document  |  |
|---|--|--|--|
| Acteurs concernés   |  | Utilisateur  |  |
| Description   |  | L'utilisateur déchiffre un document d'un de ses amis   |  |
| Préconditions   |  |  |  |
| Evénements déclenchants   |  | L'utilisateur souhaite déchiffrer un message   |  |
| Conditions d'arrêt  |  | L'utilisateur a déchiffré un message   |  |
| Description du flot d'événements principal :                      |  |  |  |
| Acteur(s)   |  | Système  |  |
| 1. L'utilisateur appuie sur le bouton pour déchiffrer le document |  | 2. L'extension récupère le message et l'envoi à FaceCrypt.<br>3. FaceCrypt déchiffre tout le document avec la clef de chiffrement, le télécharge dans le cas ou ce n'est pas une image, sinon le renvoie à l'extension.<br>4. L'extension reçoit l'image et l'affiche. |  |
| Flots secondaires :   |  |  |  |
| Flots d'exceptions :  |  | 1. Si l'utilisateur ne fait pas partie des personnes autorisées, il ne pourra pas déchiffrer le document.  |  |

#### 4.5 Gérer les liens d'amitiés

Afin d'améliorer l'ergonomie des opérations de chiffrement, l'utilisateur aura la possibilité d'organiser ses amis en différents groupes.

| Nom : C5  | Création d'une liste d'amis  |
|---|--|
| Acteurs concernés   | Utilisateur  |
| Description   | L'utilisateur crée une liste d'amis  |
| Préconditions   |  |
| Evénements déclenchants   | L'utilisateur souhaite créer une liste d'amis  |
| Conditions d'arrêt  | L'utilisateur a créé une liste d'amis  |
| Description du flot d'événements principal :  |  |
| Acteur(s)   | Système  |
| 1. L'utilisateur appuie sur le bouton "Gestion des listes".<br>3. L'utilisateur appuie sur le bouton "Ajouter une liste".<br>6. L'utilisateur entre le nom de sa liste et valide. | 2. L'extension ouvre la fenêtre de gestion de liste.<br>4. L'extension ouvre une popup pour inviter l'utilisateur à choisir un nom pour sa liste.<br>5. L'extension envoie une requête à FaceCrypt de création de liste et actualise ses listes.<br>7. FaceCrypt crée la liste dans sa base. |



|                             |  |
|-----------------------------|--|
| <b>Flots secondaires :</b>  | 1. Si l'utilisateur met un nom trop long (> 128) à sa liste. |
| <b>Flots d'exceptions :</b> |  |

| Nom : C6   | Suppression d'une liste d'amis   |
|--|--|
| Acteurs concernés  | Utilisateur  |
| Description  | L'utilisateur supprime une liste existante d'amis  |
| Préconditions  |  |
| Evénements déclenchants  | L'utilisateur souhaite supprimer une liste d'amis  |
| Conditions d'arrêt   | L'utilisateur a supprimé une liste d'amis  |
| Description du flot d'événements principal :   |  |
| Acteur(s)  | Système  |
| 1. L'utilisateur appuie sur le bouton "Gestion des listes".<br>3. L'utilisateur sélectionne une liste et appuie sur le bouton "Supprimer". | 2. L'extension ouvre la fenêtre de gestion de liste.<br>4. L'extension envoie la requête de suppression à FaceCrypt et réactualise les listes.<br>5. FaceCrypt supprime la liste de sa base. |
| Flots secondaires :  |  |
| Flots d'exceptions :   |  |

| Nom : C7   | Modifications d'une liste                        |  |
|--|--|--|
| Acteurs concernés  | Utilisateur                                      |  |
| Description  | L'utilisateur modifie une liste                  |  |
| Préconditions  | La liste d'amis doit déjà exister                |  |
| Evénements déclenchants  | L'utilisateur souhaite modifier une liste d'amis |  |
| Conditions d'arrêt   | L'utilisateur a modifier une liste d'amis        |  |
| Description du flot d'événements principal :   |  |  |
| Acteur(s)  |  | Système  |
| 1. L'utilisateur appuie sur le bouton "Modifier";<br>3. L'utilisateur coche ou décoche les amis qu'il souhaite avoir ou non dans sa liste et valide; |  | 2. L'extension ouvre une popup contenant tous les amis de l'utilisateur, ceux déjà présent dans la liste sont cochés;<br>5. L'extension synchronise la liste avec sa base de données (partagé avec FaceCrypt); |
| Flots secondaires :  |  |  |
| Flots d'exceptions :   |  |  |

| Nom : C8  | Suppression d'un ami dans une liste                               |  |
|---|---|--|
| Acteurs concernés   | Utilisateur   |  |
| Description   | L'utilisateur supprime un ami d'une de ses listes                 |  |
| Préconditions   | La liste d'amis doit déjà exister, et l'ami doit y être présent   |  |
| Evénements déclenchants   | L'utilisateur souhaite supprimer un ami dans une des liste d'amis |  |
| Conditions d'arrêt  | L'utilisateur a supprimé un ami d'une de ses liste d'amis         |  |
| Description du flot d'événements principal :  |   |  |
| Acteur(s)   |   | Système  |
| 1. L'utilisateur appuie sur le bouton "Gestion des listes".<br>3. L'utilisateur sélectionne une liste et clique sur le bouton "Gérer les amis".<br>5 L'utilisateur décoche l'ami voulu et valide. |   | 2. L'extension ouvre la fenêtre de gestion de liste.<br>4. L'extension ouvre une popup contenant tous les amis de l'utilisateur.<br>6. L'extension envoie une requête d'actualisation de la liste à FaceCrypt et actualise la liste.<br>7. FaceCrypt supprime un lien entre le(s) ami(s) et la liste dans sa base. |
| Flots secondaires :   |   |  |
| Flots d'exceptions :  |   |  |

#### 4.6 Chiffrer/déchiffrer un commentaire

De même que pour les messages de statut (de mur), l'utilisateur peut chiffrer ses commentaires ou au contraire en déchiffrer ( s'il fait partie des personnes autorisées), le déchiffrement d'un commentaire étant automatique, pas de cas.

| Nom : C9   |  | Chiffrement d'un commentaire  |  |
|--|--|---|--|
| Acteurs concernés  |  | Utilisateur   |  |
| Description  |  | L'utilisateur chiffre un commentaire  |  |
| Préconditions  |  |   |  |
| Evénements déclenchants  |  | L'utilisateur souhaite chiffrer un commentaire  |  |
| Conditions d'arrêt   |  | L'utilisateur a chiffré un commentaire, lisible uniquement par les personnes autorisées   |  |
| Description du flot d'événements principal :   |  |   |  |
| Acteur(s)  |  | Système   |  |
| 1. L'utilisateur saisit un commentaire et choisit de le chiffrer ;<br>4. L'utilisateur peut appuyer sur entrée pour poster le commentaire. |  | 2. L'extension récupère le commentaire avant son envoi sur le serveur de Facebook et l'envoie à FaceCrypt qui va chiffrer le commentaire avec la même clef de chiffrement que celle utilisée pour le message ;<br>3. FaceCrypt envoie le chiffré à l'extension qui remplace le contenu du message originel par son chiffré. |  |

|                      |  |
|----------------------|--|
| Flots secondaires :  |  |
| Flots d'exceptions : |  |

#### 4.7 Exigences fonctionnelles détaillées

| Référence | Fonctionnalité  | Priorité      |
|-----------|---|---------------|
| F-FN-10   | L'utilisateur peut chiffrer un message sur son mur  | Indispensable |
| F-FN-20   | L'utilisateur peut tenter de déchiffrer un message du mur d'un de ses amis, en appuyant sur un bouton | Indispensable |
| F-FN-30   | L'utilisateur peut chiffrer un document   | Indispensable |
| F-FN-40   | L'utilisateur peut tenter de déchiffrer un document, en appuyant sur un bouton                        | Indispensable |
| F-FN-50   | L'utilisateur peut chiffrer un commentaire  | Secondaire    |
| F-FN-60   | L'utilisateur peut déchiffrer un commentaire, en appuyant sur un bouton                               | Secondaire    |
| F-FN-70   | L'utilisateur peut créer une liste d'amis   | Indispensable |
| F-FN-80   | L'utilisateur peut effacer une liste d'amis   | Indispensable |
| F-FN-90   | L'utilisateur peut ajouter un ami dans une liste  | Indispensable |
| F-FN-100  | L'utilisateur peut retirer un ami d'une liste   | Indispensable |

## 5 Exigences opérationnelles

| Référence | Fonctionnalité                     | Priorité      |
|-----------|------------------------------------|---------------|
| F-FO-10   | Le chiffrement n'est pas trop long | Indispensable |

## 6 Exigences d'interface

| Référence | Fonctionnalité  | Priorité      |
|-----------|---|---------------|
| F-FI-10   | Notre système s'interface avec <i>Mozilla Firefox</i>   | Indispensable |
| F-FI-20   | Notre système s'utilisera comme un <i>patch</i> : il pourra fonctionner sur un compte déjà existant | Indispensable |
| F-FI-30   | Un bouton permet à l'utilisateur de déchiffrer un message qui lui apparaît chiffré                  | Indispensable |

## 7 Exigences de qualité

| Référence | Fonctionnalité   | Priorité      |
|-----------|--|---------------|
| F-FQ-10   | La système sera livré pour le 01 mars 2013   | Indispensable |
| F-FQ-20   | Un manuel d'utilisation sera livré avec le système   | Indispensable |
| F-FQ-30   | Les mots de passes utilisés par l'utilisateurs doivent avoir une taille conséquente pour améliorer leur sécurité | Indispensable |

## 8 Exigences de réalisation

| Référence | Fonctionnalité   | Priorité      |
|-----------|--|---------------|
| F-FR-10   | Seul le mot de passe nécessite de ne jamais être transmis en clair | Indispensable |