

# Spécification technique des besoins

Version	0.1
Date	21 janvier 2013
Rédigé par	Florian GUILBERT
Relu par	

## MISES À JOUR

Version	Date	Modifications réalisées
0.1	07/01/2013	Création

## 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	Chiffrer/déchiffrer un statut . . . . .	4
4.3	Chiffrer/déchiffrer un document . . . . .	6
4.4	Gérer les liens d'amitiés . . . . .	7
4.5	Chiffrer/déchiffrer un commentaire . . . . .	8
4.6	Exigences fonctionnelles détaillées . . . . .	10
<b>5</b>	<b>Exigences opérationnelles</b>	<b>11</b>
<b>6</b>	<b>Exigences d'interface</b>	<b>11</b>
<b>7</b>	<b>Exigences de qualité</b>	<b>11</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 serait 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 un patch sur un compte déjà existant.

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

## 4 Exigences fonctionnelles

### 4.1 Présentation de la mission du produit logiciel

Reference	Fonctionnalité Globale	Acteur	Priorité
F-Gl-10	Chiffrer/déchiffrer un statut	Utilisateur	Indispensable
F-Gl-20	Chiffrer/déchiffrer un document	Utilisateur	Indispensable
F-Gl-30	Gérer les liens d'amitiés	Utilisateur	Important
F-Gl-40	Chiffrer/déchiffrer un commentaire	Utilisateur	Secondaire

### 4.2 Chiffrer/déchiffrer un statut

Un utilisateur peut lorsqu'il souhaite écrire un message sur son mur 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 peut lire le message.

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 que des personnes autorisées	
Description du flot d'événements principal :			
Acteur(s)		Système	
1. L'utilisateur saisie un message et choisi de le chiffrer, il spécifie les personnes autorisées ;		2. FaceCrypt chiffre le message avec une clef de chiffrement, récupère les clefs publiques des personnes autorisées et chiffre la clef de chiffrement avec ces clefs ; 3. FaceCrypt envoi ensuite une concaténation de ce message et des clefs chiffrées aux 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 est arrivé sur une page contenant un message chiffré	
Conditions d'arrêt	L'utilisateur a déchiffré un message	
Description du flot d'événements principal :		
Acteur(s)		Système
		<div>1. FaceCrypt tente de déchiffrer la clef de chiffrement du message avec la clef publique de l'utilisateur ;</div> <div>2. FaceCrypt déchiffre tout le message avec la clef de chiffrement.</div>
Flots secondaires :		
Flots d'exceptions :		<div>1. Si l'utilisateur ne fait pas partie des personnes autorisées, il ne pourra pas déchiffrer le message.</div>

### 4.3 Chiffrer/déchiffrer un document

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

Nom : C3		Chiffrement d'un document
Acteurs concernés		Utilisateur
Description		L'utilisateur chiffre un document qui sera interpréter comme une image par Facebook
Préconditions		
Evénements déclenchants		L'utilisateur souhaite téléverser un document
Conditions d'arrêt		L'utilisateur a téléverser un document, lisible que des personnes autorisées
Description du flot d'événements principal :		
Acteur(s)		Système
1. L'utilisateur téléverse un document et choisi de le chiffrer, il spécifie les personnes autorisées ;		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 ; 3. FaceCrypt envoi ensuite une concaténation de du document chiffré et des clefs chiffrées aux serveurs de Facebook.
Flots secondaires :		1. Si l'utilisateur spécifie un document qui n'est pas une image et choisi de ne pas le chiffrer, cela sera refusé par Facebook ; 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 est arrivé sur une page contenant un document chiffré	
Conditions d'arrêt	L'utilisateur a déchiffré un message	
Description du flot d'événements principal :		
Acteur(s)		Système
		<div>1. FaceCrypt tente de déchiffrer la clef de chiffrement du document avec la clef publique de l'utilisateur ;</div> <div>2. FaceCrypt déchiffre tout le document avec la clef de chiffrement, la télécharge dans le cas ou ce n'est pas une image.</div>
Flots secondaires :		
Flots d'exceptions :		<div>1. Si l'utilisateur ne fait pas partie des personnes autorisées, il ne pourra pas déchiffrer le document.</div>

#### 4.4 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.

(Cas d'utilisation encore à déterminer)

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" création d'une liste ; 3. L'utilisateur entre le nom de sa liste et valide ;		2. FaceCrypt ouvre une popup pour inviter l'utilisateur à choisir un nom pour sa liste ; du document avec la clef publique de l'utilisateur ; 4. FaceCrypt créé une liste d'amis vide ;

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

#### 4.5 Chiffrer/déchiffrer un commentaire

De même que pour les messages de statut (de mur), l'utilisateur peut chiffrer un commentaire ou au contraire en déchiffrer, s'il fait partie des personnes autorisées.

Nom : C6	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 que des personnes autorisées
Description du flot d'événements principal :	
Acteur(s)	Système
1. L'utilisateur saisie un commentaire et choisi de le chiffrer, il spécifie les personnes autorisées à le déchiffrer ;	2. FaceCrypt chiffre le commentaire avec une clef de chiffrement, récupère les clefs publiques des personnes autorisées et chiffre la clef de chiffrement avec ces clefs ; 3. FaceCrypt envoi ensuite une concaténation de du commentaire chiffré et des clefs chiffrées aux serveurs de Facebook.
Flots secondaires :	2. Si une des personnes choisie n'a pas de clef publique, elle ne pourra pas déchiffrer le message ;
Flots d'exceptions :	



Nom : C7		Déchiffrement d'un commentaire	
Acteurs concernés		Utilisateur	
Description		L'utilisateur déchiffre un commentaire d'un de ses amis, présent sur la page	
Préconditions			
Evénements déclenchants		L'utilisateur est arrivé sur une page contenant un commentaire chiffré	
Conditions d'arrêt		L'utilisateur a déchiffré un commentaire	
Description du flot d'événements principal :			
Acteur(s)		Système	
		1. FaceCrypt tente de déchiffrer la clef de chiffrement du commentaire avec la clef publique de l'utilisateur ; 2. FaceCrypt déchiffre le commentaire avec la clef de chiffrement 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 commentaire.	

#### 4.6 Exigences fonctionnelles détaillées

Reference	Fonctionnalité	Priorité
F-FN-10	L'utilisateur peut chiffrer un message sur son mur	Indispensable
F-FN-20	L'utilisateur peut déchiffrer un message d'un mur de ses amis, s'il a été autorisé à le faire	Indispensable
F-FN-30	L'utilisateur peut chiffrer un document	Indispensable
F-FN-40	L'utilisateur peut déchiffrer un document, s'il a été autorisé à le faire	Indispensable
F-FN-50	L'utilisateur peut chiffrer un commentaire	Secondaire
F-FN-60	L'utilisateur peut déchiffrer un commentaire, s'il a été autorisé à le faire	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

Reference	Fonctionnalité	Priorité
F-FO-10	Le chiffrement n'est pas trop long ( $> 2s$ )	Indispensable

## 6 Exigences d'interface

Reference	Fonctionnalité	Priorité
F-FI-10	Notre système s'interface avec <i>Mozilla Firefox</i>	Indispensable
F-FI-20	Notre système fonctionnera comme un <i>patch</i> : il pourra fonctionner sur d'un compte déjà existant	Indispensable

## 7 Exigences de qualité

Reference	Fonctionnalité	Priorité
F-FQ-10	La système sera livré pour le 04 mars 2013	Indispensable
F-FQ-20	Un manuel d'utilisation sera livré avec le système	Indispensable