Spécification Technique de Besoin

Version	0.1
Date	2 janvier 2013
Rédigé par	Baptiste Dolbeau, Florian Guilbert
Relu par	
Approuvé par	
Signature	

MISES À JOUR

Version	Date	Modifications réalisées
0.1	02/01/2013	Création

Table des matières

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 ;

4 Exigences fonctionnelles

4.1 Présentation de la mission du produit logiciel

Reference	Fonctionalité 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. Le "proxy" 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. le "proxy" envoi ensuite une concaténation de ce message 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 : 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**
	1. Le "proxy" tente de déchiffrer la clef de chiffrement du message avec la clef publique de l'utilisateur ; 2. le "proxy" déchiffre tout le message avec la clef de chiffrement.

Flots secondaires :	
Flots d'exceptions :	1. Si l'utilisateur ne fait pas partie des personnes autorisées, il ne pourra pas déchiffrer le message.

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. Le "proxy" 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. le "proxy" 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**
	1. Le "proxy" tente de déchiffrer la clef de chiffrement du document avec la clef publique de l'utilisateur ; 2. le "proxy" déchiffre tout le document avec la clef de chiffrement, la télécharge dans le cas ou ce n'est pas une image.

Flots secondaires :	
Flots d'exceptions :	1. Si l'utilisateur ne fait pas partie des personnes autorisées, il ne pourra pas déchiffrer le document.

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.

Nom : C5	
Acteurs concernés	
Description	
Préconditions	
Evénements déclenchants	
Conditions d'arrêt	
Description du flot d'événements principal :	
Acteur(s)	**Système**
1. toto	2. tutu
Flots secondaires :	
Flots d'exceptions :	

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. Le "proxy" 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. le "proxy" 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. Le "proxy" tente de déchiffrer la clef de chiffrement du commentaire avec la clef publique de l'utilisateur ; 2. le "proxy" 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

TODO

Reference	Fonctionalité	Priorité
F-FN-10	L'utilisateur ne donne son mot de passe qu'au SAUD	Indispensable
F-FN-20	L'authentification sur un service externe ne peut se faire qu'à partir d'un emplacement donnée	Secondaire
F-FN-30	Plusieurs authenfication simultanées sont impossible, le SAUD déconnecte la session en cours en cas d'une autre demande d'authenfication	Indispensable
F-FN-40	À chaque tentative de connexion d'un client sur un service externe, celui-ci vérifie l'authenticité du SAUD associé au client	Indispensable
F-FN-50	Les échanges et dialogues entre service externe, SAUD et utilisateur sont sécurisés	Indispensable

Reference	Fonctionalité	Priorité
F-FN-60	Le SAUD est accessible au travers d'une page web	Indispensable
F-FN-70	La page d'accueil du site propose un formulaire d'authentification ainsi que le lien/bouton "Creer un compte"	Indispensable
F-FN-80	Un visiteur peut créer un compte utilisateur	Indispensable
F-FN-90	Un login unique, un mot de passe, une question secrête ainsi que sa réponse et une adresse mail valide est essentiel pour créer un compte utilisateur	Indispensable
F-FN-100	Quand un visiteur créé un compte d'utilisateur, un mail lui est envoyé et sans accusé de reception, le compte n'est pas créé	Indispensable
F-FN-110	Si un utilisateur veut suprimer son compte, il doit entrer son mot de passe	Secondaire
F-FN-120	Un utilisateur peut se déconnecter du SAUD en cliquant sur un lien	Important
F-FN-130	Un utilisateur peut modifier son mot de passe	Secondaire
F-FN-140	Un utilisateur peut changer sa question secrête (intitulé et réponse)	Secondaire
F-FN-150	Un utilisateur peut modifier son adresse mail	Indispensable
F-FN-160	Un utilisateur peut se connecter à un site quelconque en donnant son adresse SAUD dans le champs "identifiant" du site	Indispensable
F-FN-170	Un utilisateur peut créer un compte sur un site quelconque en utilisant l'authentification externe	Indispensable
F-FN-180	Lorsqu'un utilisateur se connecte depuis une autre adresse IP pour la première fois, il doit répondre à sa question secrête et rentrer son adresse mail	Indispensable
F-FN-190	L'utilisateur peut modifier son mot de passe peut entrer un nouveau en suivant la procédure adéquate	Indispensable
F-FN-200	L'administrateur peut supprimer le compte de n'importe quel utilisateur	Secondaire
F-FN-210	L'administrateur n'aura jamais accès aux mot de passes des utilisateurs	Secondaire
F-FN-220	Il est possible de télécharger un paquetage d'installation d'un SAUD peronnel	Secondaire

Reference	Fonctionalité	Priorité
F-FN-230	Log de la dernière connexion à chaque nouvelle connexion	Secondaire

5 Exigences opérationnelles

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

6 Exigences d'interface

Reference	Fonctionalité	Priorité
F-FI-10	Notre système d'interface avec *Mozilla Firefox*	Indispensable

7 Exigences de qualité

Reference	Fonctionalité	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

8 Exigences de réalisation

Reference	Fonctionalité	Priorité
F-FR-10	TODO	Indispensable