

Sp cification technique des besoins

Version	0.1
Date	29 janvier 2013
Rédigé par	Florian GUILBERT
Relu par	Baptiste DOLBEAU

MISES JOUR

Version	Date	Modifications r alis es
0.1	07/01/2013	Cr ation

Table des matières

1	Objet	4
2	Documents applicables et de r frence	4
3	Terminologie et sigles utilis s	4
4	Exigences fonctionnelles	4
4.1	Pr sentation de la mission du produit logiciel	4
4.2	Pr conditions	4
4.3	Chiffrer/d chiffrer un statut	5
4.4	Chiffrer/d chiffrer un document	6
4.5	G rer les liens d'amiti s	8
4.6	Chiffrer/d chiffrer un commentaire	10
4.7	Exigences fonctionnelles d taill es	13
5	Exigences op rationnelles	14
6	Exigences d'interface	14
7	Exigences de qualit	14
8	Exigences de r alisation	14

1 Objet

Proposer des solutions cryptographiques garantissant la protection de la vie priv e des utilisateurs vis- -vis d'un r seau social. Cette protection pourra tre effective par le chiffrement syst matique des donn es sensibles. Et le d chiffrement de ces donn es ne sera possible que par des personnes consid r es explicitement par l'utilisateur.

Le projet prendra la forme d'une extension pour le navigateur *Mozilla Firefox* s'interfa ant avec une carte puce pour effectuer certaines t ches de chiffrement.

Il ne sera pas n cessaire de cr er un compte, notre projet pourra fonctionner comme patch sur un compte d j existant.

Le r seau social tudi sera *Facebook* moins que des probl mes sp cifiques ce r seau social soient rencontr s lors du d veloppement du projet. Par cons quent, la terminologie utilis e correspondra celle de *Facebook* (statut, mur, ...).

2 Documents applicables et de r f rence

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

3 Terminologie et sigles utilis s

SN : Social Network, repr sente le r seau social que nous avons choisi comme support pour ce projet.

FaceCrypt : Application Java g rant les traitements lourds (chiffrement/d chiffrement) de l'extension et tant en relation avec la carte puce.

Extension : Programme incorpor 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 Pr sentation de la mission du produit logiciel

Reference	Fonctionalit Globale	Acteur	Priorit
F-Gl-10	Chiffrer/d chiffrer un statut	Utilisateur	Indispensable
F-Gl-20	Chiffrer/d chiffrer un document	Utilisateur	Indispensable
F-Gl-30	G rer les liens d'amiti s	Utilisateur	Important
F-Gl-40	Chiffrer/d chiffrer un commentaire	Utilisateur	Secondaire

4.2 Pr conditions

Pour tous les cas d'utilisation d crits ci-dessous, nous supposons que l'utilisateur est d j authentifi sur le r seau social (Facebook). Il a donc d j ins r sa carte dans le lecteur.

4.3 Chiffrer/d chiffrer un statut

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

Inversement, lorsqu'un de ses amis poste (sur son mur) un message chiffr , l'utilisateur peut tenter de le d chiffrer. Si l'utilisateur fait partie des personnes autoris es, il pourra lire le message.

Nom: C1		Chiffrement d'un message sur son mur	
Acteurs concernés		Utilisateur	
Description		L'utilisateur chiffre un message qui sera affich sur le mur	
Préconditions			
Evénements déclenchants		L'utilisateur souhaite poster un message sur son mur	
Conditions d'arrêt		L'utilisateur a post un message chiffr sur son mur, lisible uniquement par les personnes autoris es	
Description du flot d'événements principal :			
Acteur(s)		Système	
1. L'utilisateur saisi un message et choisit de le chiffrer, il sp cifie les personnes autoris es. 3. L'utilisateur pr cise des listes d'amis ou des amis, qui pourront lire son message.		2. L'extension demande l'utilisateur quels amis vont tre autoris s d chiffrer le message. 4. L'extension recup re le message avant son envoi sur le serveur de Facebook et l'envoi FaceCrypt qui va le chiffrer avec une clef de chiffrement, recup rer les clefs publiques des personnes autoris es et chiffrer la clef de chiffrement avec ces clefs. 5. FaceCrypt envoie ensuite une concat nation de ce message et des clefs chiffr es l'extension qui enverra le tout, chiffr , 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 d chiffrer le message.	

Nom: C2		D chiffrement d'un message sur un mur	
Acteurs concernés		Utilisateur	
Description		L'utilisateur d chiffre un message du mur d'un de ses amis	
Préconditions			
Evénements déclenchants		L'utilisateur souhaite d chiffrer un message	
Conditions d'arrêt		L'utilisateur a d chiffr un message, ou pas	
Description du flot d'événements principal :			
Acteur(s)		Système	
1. L'utilisateur appuie sur le bouton pour d chiffrer le message.		2. L'extension recupere le message et l'envoie FaceCrypt. 3. FaceCrypt d chiffre tout le message avec la clef de chiffrement et envoie le message l'extension. 4. L'extension affiche le resultat.	
Flots secondaires:			
Flots d'exceptions:		1. Si l'utilisateur ne fait pas partie des personnes autorisées, il ne pourra pas d chiffrer le message.	

4.4 Chiffrer/d chiffrer un document

Un utilisateur peut choisir d'utiliser l'option de t l versement d'image du r seau social pour t l verser un document (image, fichier texte, ...) chiffr . Celui-ci sera consid r comme une image par le r seau 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			
Événements déclenchants		L'utilisateur souhaite télécharger un document	
Conditions d'arrêt		L'utilisateur a téléchargé 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. 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. 4. L'extension récupère le commentaire avant son envoi sur le serveur de Facebook et l'envoie 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. 5. FaceCrypt envoie ensuite une concaténation de ce message et des clefs chiffrées 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. 2. Si une des personnes choisie n'a pas de clef publique, elle ne pourra pas déchiffrer le message.	
Flots d'exceptions:			

Nom: C4		D chiffrement d'un document	
Acteurs concernés		Utilisateur	
Description		L'utilisateur d chiffre un document d'un de ses amis	
Préconditions			
Evénements déclenchants		L'utilisateur souhaite d chiffrer un message	
Conditions d'arrêt		L'utilisateur a d chiffré un message	
Description du flot d'événements principal :			
Acteur(s)		Système	
1. L'utilisateur appuie sur le bouton pour d chiffrer le document		2. L'extension récupère le message et l'envoi FaceCrypt. 3. FaceCrypt d chiffre tout le document avec la clef de chiffrement, le t l charge dans le cas ou ce n'est pas une image, sinon le renvoie l'extension. 4. L'extension reçoit l'image et l'affiche.	
Flots secondaires:			
Flots d'exceptions:		1. Si l'utilisateur ne fait pas partie des personnes autoris es, il ne pourra pas d chiffrer 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	Cr ation d'une liste d'amis
Acteurs concernés	Utilisateur
Description	L'utilisateur cr e une liste d'amis
Préconditions	
Evénements déclenchants	L'utilisateur souhaite cr er une liste d'amis
Conditions d'arrêt	L'utilisateur a cr une liste d'amis
Description du flot d'événements principal :	
Acteur(s)	Système
1. L'utilisateur appuie sur le bouton "Gestion des listes". 3. L'utilisateur appuie sur le bouton "Ajouter une liste". 3. L'utilisateur entre le nom de sa liste et valide.	2. L'extension ouvre la fen tre de gestion de liste. 4. L'extension ouvre une popup pour inviter l'utilisateur choisir un nom pour sa liste. 5. L'extension envoie une requ te FaceCrypt de cr ation de liste et actualise ses listes. 6. FaceCrypt cr e la liste dans sa base.

Flots secondaires:	1. Si l'utilisateur met un nom trop long (> 128) sa liste.
Flots d'exceptions:	

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". 3. L'utilisateur sélectionne une liste et appuie sur le bouton "Supprimer".		2. L'extension ouvre la fenêtre de gestion de liste. 4. L'extension envoie la requête de suppression FaceCrypt et actualise les listes. 5. FaceCrypt supprime la liste de sa base.
Flots secondaires:		
Flots d'exceptions:		

Nom: C7		Ajout d'un ami dans une liste
Acteurs concernés		Utilisateur
Description		L'utilisateur ajoute un ami dans une de ses listes
Préconditions		La liste d'amis doit déjà exister
Evénements déclenchants		L'utilisateur souhaite ajouter un ami dans une des liste d'amis
Conditions d'arrêt		L'utilisateur a ajouté un ami dans 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". 3. L'utilisateur sélectionne une liste et clique sur le bouton "Gérer les amis". 5 L'utilisateur coche l'ami voulu et valide.		2. L'extension ouvre la fenêtre de gestion de liste. 4. L'extension ouvre une popup contenant tous les amis de l'utilisateur. 6. L'extension envoie une requête d'actualisation de liste FaceCrypt et actualise sa liste. 7. FaceCrypt ajoute un lien entre le(s) ami(s) et la liste dans sa base.
Flots secondaires:		1. Si l'utilisateur choisit un ami qui ne dispose pas de notre système, celui ne peut pas être ajouté.
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 d j exister, et l'ami doit y tre pr sent	
Evénements déclenchants		L'utilisateur souhaite supprimer un ami dans une des liste d'amis	
Conditions d'arrêt		L'utilisateur a supprim 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". 3. L'utilisateur s lectionne une liste et clique sur le bouton "G rer les amis". 5 L'utilisateur d coche l'ami voulu et valide.		2. L'extension ouvre la fen tre de gestion de liste. 4. L'extension ouvre une popup contenant tous les amis de l'utilisateur. 6. L'extension envoie une requ te d'actualisation de la liste FaceCrypt et actualise la liste. 7. FaceCrypt supprime un lien entre le(s) ami(s) et la liste dans sa base.	
Flots secondaires:			
Flots d'exceptions:			

4.6 Chiffrer/d chiffrer un commentaire

De m me que pour les messages de statut (de mur), l'utilisateur peut chiffrer ses commentaires ou au contraire en d chiffrer (s'il fait partie des personnes autoris es).

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. 3. L'utilisateur précise les listes d'amis, ou les amis, qui pourront lire son message.		2. L'extension demande à l'utilisateur quels amis vont-ils être autorisés à chiffrer le message. 4. L'extension récupère le commentaire avant son envoi sur le serveur de Facebook et l'envoie FaceCrypt qui va chiffrer le commentaire avec une clef de chiffrement, récupérer les clefs publiques des personnes autorisées et chiffrer la clef de chiffrement avec ces clefs. 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:		2. Si une des personnes choisies n'a pas de clef publique, elle ne pourra pas chiffrer le message.	
Flots d'exceptions:			

Nom: C10		D chiffrement d'un commentaire	
Acteurs concernés		Utilisateur	
Description		L'utilisateur d chiffre un commentaire d'un de ses amis, pr sent sur la page	
Préconditions			
Evénements déclenchants		L'utilisateur souhaite d chiffrer un commentaire	
Conditions d'arrêt		L'utilisateur a d chiffr un commentaire	
Description du flot d'événements principal :			
Acteur(s)		Système	
1. L'utilisateur appuie sur le bouton pour d chiffrer un commentaire.		2. L'extension r cup re le commentaire et l'envoi FaceCrypt. 3. FaceCrypt d chiffre tout le commentaire avec la clef de chiffrement et envoie le message l'extension. 4. L'extension affiche le r sultat.	
Flots secondaires:			
Flots d'exceptions:		1. Si l'utilisateur ne fait pas partie des personnes autoris es, il ne pourra pas d chiffrer le commentaire.	

4.7 Exigences fonctionnelles d taill es

R f rence	Fonctionalit	Priorit
F-FN-10	L'utilisateur peut chiffrer un message sur son mur	Indispensable
F-FN-20	L'utilisateur peut tenter de d chiffrer 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 d chiffrer un document, en appuyant sur un bouton	Indispensable
F-FN-50	L'utilisateur peut chiffrer un commentaire	Secondaire
F-FN-60	L'utilisateur peut d chiffrer un commentaire, en appuyant sur un bouton	Secondaire
F-FN-70	L'utilisateur peut cr er 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 op rationnelles

R f rence	Fonctionalit	Priorit
F-FO-10	Le chiffrement n'est pas trop long	Indispensable

6 Exigences d'interface

R f rence	Fonctionalit	Priorit
F-FI-10	Notre syst me s'interface avec <i>Mozilla Firefox</i>	Indispensable
F-FI-20	Notre syst me s'utilisera comme un <i>patch</i> : il pourra fonctionner sur un compte d j existant	Indispensable
F-FI-30	Un bouton permet l'utilisateur de d chiffrer un message qui lui appara t chiffr	Indispensable

7 Exigences de qualit

R f rence	Fonctionalit	Priorit
F-FQ-10	La syst me sera livr pour le 04 mars 2013	Indispensable
F-FQ-20	Un manuel d'utilisation sera livr avec le syst me	Indispensable
F-FQ-30	Les mots de passes utilis s par l'utilisateurs doivent avoir une taille cons quente pour am liorer leur s curit	Indispensable

8 Exigences de r alisation

R f rence	Fonctionalit	Priorit
F-FR-10	Seul le mot de passe n cessite de ne jamais tre transmis en clair	Indispensable