

Cahier de recettes

| | |
|-------------------|---------------------------|
| Version | 1.0 |
| Date | 1 ^{er} mars 2013 |
| Rédigé par | Baptiste DOLBEAU |
| Relu par | Zakaria ADDI |

MISES À JOUR

| Version | Date | Modifications réalisées |
|---------|------------|-------------------------|
| 0.1 | 24/02/2013 | Création |
| 1.0 | 28/02/2013 | Finalisation |

Table des matières

| | | |
|---|--|----|
| 1 | Introduction | 4 |
| 2 | Documents applicables et de références | 5 |
| 3 | Terminologie et sigles utilisés | 5 |
| 4 | Environnement de tests | 5 |
| 5 | Responsabilité | 5 |
| 6 | Stratégie de tests | 6 |
| 7 | Gestion des anomalies | 6 |
| 8 | Procédures de tests | 6 |
| 9 | Couverture de tests | 12 |

1 Introduction

Ce document est un support pour la validation du logiciel lors de la recette auprès du client. Il est consacré à la définition des moyens et des procédures utilisés pour assurer la recette du produit développé. La recette est un procédé permettant d'assurer la conformité du logiciel à la spécification déjà définie. Nous allons recenser dans ce document les objectifs de tests de validation et les moyens nécessaires pour les atteindre en précisant :

- Les pré-conditions à satisfaire ;
- Les moyens matériels requis (plate-forme de tests) ;
- La logique de leur déroulement (étapes successives).

Notre logiciel peut être divisé en une liste de constituants qui seront testés à tour de rôle. L'ensemble des opérations devra être transparent vis à vis de l'utilisateur. Les différents cas d'utilisation prélevés de la spécification technique de besoin sont les suivants (par ordre de priorité) :

Chiffrement et déchiffrement d'un statut

Notre application doit pouvoir chiffrer et déchiffrer le statut d'un utilisateur du réseau social "Facebook". S'il choisit de chiffrer, il doit spécifier les utilisateurs qui seront autorisés à le déchiffrer.

Chiffrement et déchiffrement d'un commentaire

Notre application doit pouvoir chiffrer et déchiffrer un commentaire d'un utilisateur du réseau social "Facebook". S'il choisit de chiffrer, il doit spécifier les utilisateurs qui seront autorisés à le déchiffrer.

Déploiement du système sur un compte déjà existant

Notre application finale doit pouvoir être applicable à un compte d'un utilisateur de "Facebook" déjà existant. Les opérations offertes par notre système à cet utilisateur ne seront disponibles que pour les futurs messages qu'il écrira.

Gestion des liens d'amitiés

Afin d'améliorer l'ergonomie de notre projet, nous proposons de gérer les liens d'amitiés de l'utilisateur de "Facebook". Il pourra ainsi organiser ses amis en listes. Ces listes seront utiles lors d'opérations telles que le chiffrement d'un message ou d'un commentaire.

Chiffrement et déchiffrement d'un document

Notre application doit pouvoir chiffrer et déchiffrer un document d'un utilisateur du réseau social "Facebook". S'il choisi de chiffrer, il doit spécifier les utilisateurs qui seront autorisés à le déchiffrer.

Génération et changement d'un mot de passe

Notre application doit pouvoir gérer la génération d'un nouveau mot de passe ainsi que son enregistrement.

2 Documents applicables et de références

- SSN_STB : Le document renfermant les spécifications techniques de Besoin ;
- SSN_DAL : Le document contenant l'architecture logicielle ;
- Les comptes rendu de réunion du projet ;
- Le sujet du projet : "proxy-encryption.pdf".

3 Terminologie et sigles utilisés

CdR : Cahier de Recettes ;

AdR : Analyse des Risques ;

DAL : Document d'Architecture Logicielle ;

STB : Spécification Technique de Besoin ;

SC : *SmartCard*, relatif au sous-projet sur les cartes à puce ;

SSN : *Secure Social Network*, relatif au sous-projet sur les réseaux sociaux ;

PIN : *Personal Identification Number* - Code servant à authentifier l'utilisateur ;

4 Environnement de tests

L'ensemble des tests se sont effectués sur des machines ayant les caractéristiques suivantes :

- Système d'exploitation : Ubuntu 12.04 ;
- Processeur : Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz ;
- Mémoire : 2Go RAM ;
- Logiciel : Eclipse Platform Version : 3.8.0, Java 1.6 (Client) et Firefox 18.0.2.

Nous utilisons également des cartes Java Card J3A (marque NXP) avec 40K d'EEPROM et des lecteurs Omnikey 3121. Les cartes sont conformes aux standards Java Card 2.2.2 et Global Platform 2.1.1.

5 Responsabilité

Afin de mener les tests dans les meilleurs conditions, une organisation au sein du groupe a été mise en place :

La conception et la définition des données de tests ont été réalisées par Baptiste DOLBEAU. Après avoir exécuté les différents tests, les responsables de ce module transmettront aux développeurs un compte rendu contenant les résultats afin d'améliorer la version actuelle du logiciel et d'en fournir une nouvelle à évaluer. Chaque version fournie doit être testée et validée.

6 Stratégie de tests

La démarche utilisée pour effectuer les tests est la suivante :

- Mettre à la disposition de l'équipe testeur les modules développés.
- Réalisation des tests à travers une procédure, celle ci comportera un jeu de tests ainsi que la modalité de leur exécution.
- Élaboration d'un compte rendu des résultats des tests qui sera transmis aux développeurs.
- Correction des anomalies par l'équipe développeur.
- Des tests secondaires seront effectués pour s'assurer que toutes les anomalies ont été corrigées.

Les tests seront réalisés par ordre de priorité. Les modules ayant une priorité indispensable seront pris en compte dès que possible. La condition d'arrêt des tests sera le succès de ces derniers après correction des anomalies.

7 Gestion des anomalies

A chaque modification apportée (correction), nous devons réaliser un nombre de tests permettant de détecter les anomalies persistantes. Toute anomalie détectée sera notée dans un rapport et ce dernier sera envoyé aux développeurs afin qu'ils apportent les modifications nécessaires.

8 Procédures de tests

Pour chaque cas d'utilisation, nous décrivons une procédure de test détaillée. Chaque procédure dispose d'un jeu de tests basé sur des données réelles.

| | | | | |
|---|--|--|---------------|--------|
| Objet testé : Chiffrement et déchiffrement d'un statut facebook. | | | Version : 1.0 | |
| Objectif de test : Vérifier le comportement d'une demande de chiffrement ou déchiffrement d'un statut facebook. | | | | |
| Procédure n°1 : Chiffrer un statut en mode anonyme. | | | | |
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 2 | Après entrée du texte, Appuyer sur le bouton "chiffrer". | Une "pop-up" apparait pour la selection des listes et du mode. | F-GI-10 | OK |
| 3 | Sélectionner une liste d'amis et le mode anonyme. | Les cases sélectionnées sont cochées. | F-GI-10 | OK |
| 4 | Appuyer sur le bouton "chiffrer". | Obtention d'un chiffré, ne contenant pas les noms des amis de la liste spécifiée, à la place de notre message. | F-GI-10 | OK |

| Procédure n°2 : Déchiffrer un statut en mode anonyme. | | | | |
|---|--|--|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Sélectionner un message chiffré et appuyer sur le bouton Déchiffrer. | Obtention du message déchiffré si il lui était destiné, ou sinon d'un message "Ce message ne vous concerne pas.", à la place de notre message chiffré. | F-GI-10 | OK |

| Procédure n°3 : Chiffrer un statut en mode non anonyme. | | | | |
|---|---|--|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Écrire un message dans la zone réservée. | Le bouton "chiffrer" apparait. | F-GI-10 | OK |
| 2 | Appuyer sur le bouton "chiffrer". | Une "pop-up" apparait pour la selection des listes et du mode. | F-GI-10 | OK |
| 3 | Sélectionner une liste d'amis et le mode non-anonyme. | Les cases sélectionnées sont cochées. | F-GI-10 | OK |
| 4 | Appuyer sur le bouton "chiffrer". | Un chiffré, contenant les noms des amis de la liste spécifiée, apparait à la place de notre message. | F-GI-10 | OK |

| Procédure n°4 : Déchiffrer un statut en mode non anonyme. | | | | |
|---|---------------------------|--|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Aucune action nécessaire. | Obtention du message déchiffré si il lui était destiné ou du message "Ce message ne vous concerne pas", à la place de notre message chiffré. | F-GI-10 | OK |

| Objet testé : Chiffrement et déchiffrement d'un document. | | | | Version : 1.0 |
|---|--|-------------------------------|----------|---------------|
| Objectif de test : Vérifier le comportement d'une demande de chiffrement ou déchiffrement d'un document sur facebook. | | | | |
| Procédure n°5 : Chiffrer un document sur facebook. | | | | |
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Chiffrer un document telle qu'une image sur facebook | Non implémenté sur ce projet. | F-GI-20 | OK |

| Procédure n°6 : Déchiffrer un document sur facebook. | | | | |
|--|--|-------------------------------|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Déchiffrer un document telle qu'une image sur facebook | Non implémenté sur ce projet. | F-GI-20 | OK |

| Objet testé : Gestion des liens d'amitiés. | | | | Version : 1.0 |
|--|---|---|----------|---------------|
| Objectif de test : Vérifier la manipulation des listes d'amis. | | | | |
| Procédure n°7 : Création d'une liste d'amis. | | | | |
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Appuyer sur le bouton "Créer" dans la partie gauche de la page. | Une "pop-up" vous demande un nom de liste. | F-GI-30 | OK |
| 2 | Entrer un nom de liste. | Création d'une liste d'amis vide visible en dessous du bouton "créer" et dans la base de données. | F-GI-30 | OK |

| Procédure n°8 : Modification d'une liste. | | | | |
|---|--|---|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Appuyer sur le bouton "modifier" à droite d'un nom de liste. | Une "pop-up" s'ouvre et affiche la liste de vos amis. Les amis appartenant à la liste sont déjà cochés | F-GI-30 | OK |
| 2 | Cocher ou décocher un ami dans la liste. | Cet ami est respectivement ajouté ou supprimé de la liste sélectionnée. Un lien est créé ou supprimé dans la base de données. | F-GI-30 | OK |

| Procédure n°9 : Suppression d'une liste d'amis. | | | | |
|---|---|---|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Appuyer sur le bouton "supprimer" à droite d'un nom de liste. | La liste est supprimée de la page et de la base de données. | F-GI-30 | OK |

| | | | | |
|--|---|--|---------------|--------|
| Objet testé : Chiffrement et déchiffrement d'un commentaire. | | | Version : 1.0 | |
| Objectif de test : Vérifier le comportement d'une demande de chiffrement ou déchiffrement d'un commentaire attaché à un statut facebook. | | | | |
| Procédure n°10 : Chiffrement d'un commentaire lié à un statut facebook que l'on peut déchiffrer. | | | | |
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Utiliser la procédure 3 ou 4 pour déchiffrer un statut. | Obtention du message déchiffré à la place de notre message chiffré. | F-GI-40 | OK |
| 2 | Ajouter un commentaire lié au statut déchiffré | Un bouton "chiffrer" apparait | F-GI-40 | OK |
| 3 | Appuyer sur le bouton "chiffrer". | Le commentaire chiffré apparait à la place de notre commentaire, prêt à l'envoi. | F-GI-40 | OK |

| Procédure n°11 : Chiffrement d'un commentaire lié à un statut chiffré facebook que l'on ne peut pas déchiffrer. | | | | |
|---|---|--|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Utiliser la procédure 3 ou 4 pour déchiffrer un statut. | Obtention du message "Ce message ne vous concerne pas", à la place de notre message chiffré. | F-GI-40 | OK |
| 2 | Écrire un commentaire | Aucun bouton "chiffrer" n'est disponible. L'action n'est donc pas possible. | F-GI-40 | OK |

| Procédure n°12 : Post d'un commentaire non chiffré lié à un statut chiffré. | | | | |
|---|---|---|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Insertion d'un commentaire relié à un message chiffré sans le déchiffrer. | Le commentaire non chiffré apparait rattaché au statut. | F-GI-40 | OK |

| Procédure n°13 : Déchiffrement d'un (ou plusieurs) commentaire(s) lié(s) à un statut chiffré. | | | | |
|---|---|--|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Appuyer sur le bouton "déchiffrer" d'un message chiffré contenant des commentaires chiffrés ou non. | Obtention du statut déchiffré et de la liste des commentaires déchiffrés ou laissés tels quels s'ils ne sont pas chiffrés. | F-GI-40 | OK |

| | | | | |
|--|--------------------------------|--------------------------------------|---------------|--------|
| Objet testé : Déploiement du système sur un compte facebook déjà existant. | | | Version : 1.0 | |
| Objectif de test : Vérifier l'intégration du système sur un compte pré-existant. | | | | |
| Procédure n°14 : Chiffrement possible. | | | | |
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Création d'un statut facebook. | Le bouton "chiffrer" est disponible. | F-GI-50 | OK |

| Procédure n°15 : Déchiffrement possible. | | | | |
|--|---------------------------|---|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Aucune action nécessaire. | Le bouton "déchiffrer" apparaît à suite à un message chiffré. | F-GI-50 | OK |

| Procédure n°16 : Identification possible via la carte à puce (carte vierge). | | | | |
|--|---------------------------------------|---|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Aller sur la page "facebook.com". | Une demande de code PIN apparaît dans le terminal. | F-GI-50 | OK |
| 2 | Rentrer le code PIN dans le terminal. | Une "pop-up" apparaît et nous demande de rentrer les identifiants | F-GI-50 | OK |
| 3 | Rentrer les identifiants | Connexion au site, la carte contient maintenant les données. | F-GI-50 | OK |

| Procédure n°17 : Identification possible via la carte à puce (carte pré-remplie). | | | | |
|---|---------------------------------------|--|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Aller sur la page "facebook.com". | Une demande de code PIN apparaît dans le terminal. | F-GI-50 | OK |
| 2 | Rentrer le code PIN dans le terminal. | Connexion au site, la carte contient maintenant les données. | F-GI-50 | OK |

| Procédure n°18 : Possibilité de changer de mot de passe. | | | | |
|--|---|--|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Aller sur dans l'onglet "compte" de l'icone outils (roue crantée) | Une liste de paramètres modifiables apparaît. | F-GI-50 | OK |
| 2 | Appuyer sur le bouton "modifier" lié au paramètre "mot de passe" | Une liste apparaît avec les champs pré-remplis. | F-GI-50 | OK |
| 3 | Appuyer sur le bouton "enregistrer les modifications". | Le nouveau mot de passe est pris en compte par la carte et par facebook. | F-GI-50 | OK |

| Procédure n°19 : Insertion de la clef publique. | | | | |
|---|--|---|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Aller sur la page principale. | Un bouton "publier ma clef" | F-GI-50 | OK |
| 2 | Appuyer sur le bouton "publier ma clef". | La clef publique de l'utilisateur est affichée dans le champs "à propos de moi" sur notre profil. | F-GI-50 | OK |

| Procédure n°20 : Récupération des clefs publiques. | | | | |
|--|--|---|----------|--------|
| N° | Actions | Résultats attendus | Exigence | OK/NOK |
| 1 | Aller sur la page principale. | Un bouton "synchroniser les clefs" | F-GI-50 | OK |
| 2 | Appuyer sur le bouton "synchroniser les clef". | La base de donnée est remplie avec le nom des utilisateurs et leur clef publique. | F-GI-50 | OK |

9 Couverture de tests

Ce tableau reprend les exigences de la STB et précise, pour chacune d'entre elles, la méthode de vérification (démonstration / tests) et une description de celle-ci.

| Exigence | Méthode de vérification | Procédure utilisée | Commentaire |
|----------|-------------------------|--------------------|---|
| F-Gl-10 | Test | Procédure 1 | Ce test consiste à chiffrer un statut en mode anonyme. |
| F-Gl-10 | Test | Procédure 2 | Le test consiste à déchiffrer un statut en mode anonyme. |
| F-Gl-10 | Test | Procédure 3 | Le test consiste à chiffrer un statut en mode non anonyme. |
| F-Gl-10 | Test | Procédure 4 | Le test consiste à déchiffrer un statut en mode non anonyme. |
| F-Gl-20 | Test | Procédure 5 | Le test consiste à chiffrer un document sur facebook. |
| F-Gl-20 | Test | Procédure 6 | Ce test consiste à déchiffrer un document sur facebook. |
| F-Gl-30 | Test | Procédure 7 | Le test consiste à créer une liste d'amis. |
| F-Gl-30 | Test | Procédure 8 | Le test consiste à modifier une liste d'amis. |
| F-Gl-30 | Test | Procédure 9 | Le test consiste à supprimer une liste d'amis. |
| F-Gl-40 | Test | Procédure 10 | Le test consiste à chiffrer un commentaire lié à un statut que l'on peut déchiffrer. |
| F-Gl-40 | Test | Procédure 11 | Le test consiste à chiffrer un commentaire lié à un statut que l'on ne peut pas déchiffrer. |
| F-Gl-40 | Test | Procédure 12 | Le test consiste à poster un commentaire non chiffré lié à un statut chiffré. |
| F-Gl-40 | Test | Procédure 13 | Le test consiste à déchiffrer un (ou plusieurs) commentaire(s) lié(s) à un statut chiffré. |
| F-Gl-50 | Démonstration | Procédure 14 | Le test consiste à évaluer le chiffrement. |
| F-Gl-50 | Démonstration | Procédure 15 | Le test consiste à évaluer déchiffrement. |
| F-Gl-50 | Démonstration | Procédure 16 | Le test consiste à évaluer l'identification via la carte à puce (carte vierge). |
| F-Gl-50 | Démonstration | Procédure 17 | Le test consiste à évaluer l'identification via la carte à puce (carte pré-remplie). |
| F-Gl-50 | Démonstration | Procédure 18 | Le test consiste à évaluer le changement de mot de passe. |
| F-Gl-50 | Démonstration | Procédure 19 | Le test consiste à évaluer l'affichage de la clef publique. |
| F-Gl-50 | Démonstration | Procédure 20 | Le test consiste à évaluer la récupération des clefs publiques. |