Plan de Qualité

Version	0.1
Date	1er mars 2013
Rédigé par	Baptiste Dolbeau
Relu par	Yicheng Gao, Romain Pignard

MISES À JOUR

Version	Date	Modifications réalisées
0.1	31/01/2013	Création

Table des matières

1 Objet du Plan de Qualité

1.1 Cadre

Ce plan de qualité a été élaboré pour le projet *Smart Social Network* associant la promotion de master 2 Sécurité des Systèmes Informatiques avec Madame Bardet et Monsieur Otmani.

1.2 Objectif

Il a pour but de mettre en évidence la définition et les mesures à prendre pour le projet *Smart Social Network* afin d'assurer un seuil de qualité défini et atteindre les résultats demandés.

1.3 Utilisation

Le plan de qualité est un outil de suivi et de gestion du projet. De part sa nature, il est amené à être modifié selon les ajouts ou suppressions que l'on apportera au projet.

2 Données

2.1 Contexte

Dans le cadre de notre master 2 Sécurité des Systèmes Informatiques, nous devons réaliser un projet de fin d'année. Ce projet *Smart Social Network* est devenu l'agrégat des deux projets initiaux *Smart Card* et *Secure Social Network*. L'effectif n'étant pas assez suffisant, il a été convenu par les deux clients "Mme Bardet" et "M. Otmani" de réunir ces deux projets en un seul.

Ces projets sont nés d'une part du besoin d'un cas d'utilisation de cartes à puce et d'autre part du besoin de rester propriétaire des données postées sur un réseau social.

2.2 Rappels

2.2.1 Objectifs projet

Notre projet possède deux objectifs principaux :

- Authentification d'une personne via carte à puce.
- Chiffrement des données déposées sur le réseau social "Facebook".

Ainsi, *Smart Social Network* fournit une solution utilisateur en permettant de rendre les informations illisibles pour leur hébergeur, ici Facebook, au moyen d'une carte à puce.

2.2.2 Livrables

- Trois applications permettants respectivement de : générer des nombres pseudo-aléatoires, de chiffrer/déchiffrer des données et d'un add-on communiquant avec le navigateur firefox.
- Stockage de données sur la carte, injection de code sur le site du réseau social grâce à l'extension et stockage permanent d'informations sur la troisième application.
- Les trois applications fonctionnent et peuvent dialoguer entre elles à l'aide de "tunnels" sécurisés
- Projet Fini.

2.2.3 Objectifs produit

Ces deux objectifs s'articulent dans *Smart Social Network* dans le sens où, une fois la personne authentifiée, nous utiliserons la carte à puce pour fournir des éléments utilisés pour le chiffrement et déchiffrement des données utilisateurs de Facebook.

2.2.4 Limites

Ce projet, bien que pensé pour fonctionner avec plusieurs réseaux sociaux, est implanté, dans notre cas, uniquement pour Facebook. De plus, il ne fontionnera que sur un navigateur : *Firefox*.

Un utilisateur de *Smart Social Network* pourra poster des données telles que des images, des messages ou des commentaires, tout ceci de manière chiffrée. Ainsi, ces données ne seront lisibles ni par Facebook ni par les autres personnes non spécifiées. Cependant, la liste de ses amis, les conversations instantanées ainsi que ses données personnelles ne seront pas prises en compte par notre système et pourront donc être lues par Facebook.

2.3 Moyens

Pour la réalisation de ce projet, nous avons mis en place plusieurs concept afin d'améliorer l'efficacité de notre travail :

- Un espace partagé de travail (github)
- Un environnement de developpement (eclipse)
- Un kit de developpement pour firefox (addon-sdk)

De plus, nous avons reçu des lecteurs de cartes à puces ainsi qu'un lot de cartes.

2.4 Organismes, parties prennantes

Les parties prennantes du projet sont la promotion du master 2 SSI en tant que fournisseurs et Mme Bardet ainsi que M Otmani en tant que clients.

3 Organisation

3.1 Structure

Afin de réaliser notre projet, nous avons décidé de garder la même structure présente avant la réunion des deux projets. Il y aura donc une équipe spécialisée pour l'authentification par carte à puce (équipe *Smart card*) et une équipe pour le chiffrement des données sur le réseau social (équipe *Secure Social Network*). Le chef de projet aura pour rôle la coordination de ces deux équipes.

3.2 Acteurs

3.2.1 Organismes participants

Organisme	**Nom**	**Fonctions**	**Rôle**
Université de Rouen	Mme Bardet	Professeur	Client
Université de Rouen	M Otmani	Professeur	Client
Université de Rouen	Promotion M2SSI	Etudiants	Fournisseurs

3.2.2 Liste des acteurs de la promotions

Equipe	Nom	Rôle
	Guilbert Florian	Chef de Projet
Secure Social Network	Addi Zakaria	Developpeur
Secure Social Network	Péchoux Maxence	Developpeur
Secure Social Network	Dolbeau Baptiste	Testeur
Smart Card	Mocquet Emmanuel	Developpeur
Smart Card	Yicheng Gao	Developpeur
Smart Card	Pignard Romain	Testeur
Smart Card	Huet Giovanni	Testeur

3.3 Communications

3.3.1 Documentation

- STB Secure Social Network
- DAL Secure Social Network
- Tutoriel d'utilisation
- Plan de développement
- Manuel d'utilisation
- Analyse des risques
- Cahiers de recette
- Plan de qualité
- STB Smart Card
- DAL Smart Card
- Comptes rendus

Chaque document est soumis à une relecture par une personne tierce. Le document n'est pas présenté au client tant qu'il y a des remarques faites par la personne tierce.

Une fois présenté au client, le document peut être accepté directement ou être à nouveau révisé en fonction des remarques du client.

4 L'assurance qualité

À partir de nos documents "Spécifications Techniques des Besoins", nous avons pu mettre en évidence des exigences de qualité. Celles ci sont les suivantes :

- Le rendu du livrable
- Les opérations cryptographiques de SmartCard
- Les opérations cryptographiques de FaceCrypt
- Les accès à la carte à puce

Cette partie du plan de qualité explique comment chaque exigence est controlée et est appréciée. Nous avons mis en place une échelle de mesure afin de quantifier la qualité de chacune de ces exigences.

4.1 Le rendu du livrable

Celui ci consiste en une application facile d'utilisation répondant aux exigences des clients.

4.1.1 Mise en place de l'exigence

Pour mesurer la qualité du livrable, nous établissons une échelle par rapport aux exigences des clients pour vérifier si celles-ci sont remplies par notre application.

4.1.2 Vérification du fonctionnement

Les critères de vérification sont :

OK : Notre livrable final remplit toutes les exigences tant fonctionnelles qu'opérationnelles.

Partiel : Notre livrable final ne remplit pas toutes les exigences mais implémentera toutes les exigences indispensables.

NOT OK : Notre livrable n'implémente pas une ou plusieurs exigences indispensables.

4.2 Les opérations cryptographiques de SmartCard

La carte à puce *SmartCard* est une des composantes de notre projet. Celle ci va permettre de stocker le biclef (clef publique, clef privée) de l'utilisateur, ainsi qu'effectuer des opérations de cryptographie. Dans notre projet, nous utilisons la carte uniquement pour déchiffrer, signer et générer des données aléatoires.

4.2.1 Mise en place de l'exigence

Pour éprouver la qualité des opérations cryptographiques de la carte à puce (SmartCard), nous avons effectué une série de tests qui consistent à déchiffrer, signer et produire des données arbitraires. Cette qualité est évaluée en fonction du temps nécessaire pour accomplir l'opération.

4.2.2 Vérification du fonctionnement

Les critères de vérifications sont :

OK : Le déchiffrement et la signature se font en moins de 150 ms et la production de données arbitraires en moins de 50 ms.

Partiel : Toutes ces opérations se font entre le seuil minimal et la seconde.

NOT OK : Toutes ces opérations se font au dessus de la secondes.

4.3 Les opérations cryptographiques de FaceCrypt

Notre application java "FaceCrypt" est une autre composante de notre projet. Elle est utilisée pour effectuer des opérations de chiffrement, de déchiffrement et de vérification.

4.3.1 Mise en place de l'exigence

Pour éprouver la qualité des opérations cryptographiques de notre application java (FaceCrypt), nous avons effectué une série de tests qui consistent à chiffrer, déchiffrer et vérifier des données arbitraires. Pour ces tests, nous avons pris un message défini, de X octets. Cette qualité est évaluée en fonction du temps nécessaire pour accomplir l'opération.

4.3.2 Vérification du fonctionnement

Les critères de vérifications sont :

OK : Le chiffrement se fait en moins de X ms, le déchiffrement en moins de X ms et la vérification en moins de X ms.

Partiel : Toutes ces opérations se font entre le seuil minimal et la seconde.

NOT OK : Toutes ces opérations se font au dessus de la secondes.

4.4 Les accès à la carte à puce

Lors de notre projet, un grand nombre de requêtes vont transiter entre les entités SoftCard et SmartCard. Il est donc nécessaire que ces accès soient rapides.

4.4.1 Mise en place de l'exigence

Pour mesurer la qualité de cette exigence, nous avons effectué une série de tests. Ces derniers consistent à effectuer des demandes à la carte (établissement d'un tunnel sécurisé, nombre aléatoire). Une fois encore, notre critère de qualité est le temps requis pour l'opération.

4.4.2 Vérification du fonctionnement

Les critères de vérifications sont :

OK : L'établissement du tunnel se fait en moins de 106ms et le nombre aléatoire demandé transitant par le tunnel sécurisé sera reçu en moins de 160ms.

Partiel : L'établissement du tunnel se fait entre le seuil optimal et 110 ms et le nombre aléatoire demandé transitant par le tunnel sécurisé est reçu entre le seuil optimal et 180 ms.

NOT OK : L'établissement du tunnel se fait en plus de 110 ms et le nombre aléatoire demandé transitant par le tunnel sécurisé est reçu en plus de 180ms.