Cahier de recettes

Version	0.1
Date	18 février 2013
Rédigé par	Giovanni Huet, Romain Pignard
Relu par	Florian Guilbert, Emmanuel Mocquet

MISES À JOUR

Version	Date	Modifications réalisées
0.1	05/02/2013	Création

Table des matières

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 développée. La recette est un procédé permettant d'assurer que le logiciel est conforme à la spécification déjà définie. Nous allons recenser dans ce cahier de recette les objectifs de tests de validation et les moyens nécessaires pour les atteindre en précisant :

- les conditions à satisfaire préalablement à l'exécution des tests ;
- les moyens matériels requis (plate-forme de tests) ;
- la logique de leur déroulement (étapes successives).

Les fonctionnalités de notre logiciel peuvent être divisées en une liste de constituants qui seront testés à tour de rôle. L'ensemble des opérations devront être transparentes vis à vis de l'utilisateur. Nous donnerons par la suite les différents cas d'utilisation prélevé de la spécification technique de besoin :

Génération de nombres aléatoires

La carte à puce doit pouvoir générer des nombres aléatoires de manière sécurisée, c'est à dire non prévisible.

Déblocage de la carte (via authentification par code PIN ou via PUK)

Afin d'utiliser la carte, il nous faut pour cela nous authentifier à l'aide d'un code PIN. Cependant si l'utilisateur échoue à l'authentification par code PIN suite à un certain nombre de tentatives alors la carte sera verrouillée. Pour la déverrouiller on utilisera un code PUK.

Transimission de données

La carte doit pouvoir transmettre des données stockées à SoftCard (login, mot de passe, clef publique,...).

Chiffrement/Déchiffrement de données

Sur la carte est stockée la clef public et la clef privée préalablement générées (Crypto système assymétrique de type RSA). Ces clefs nous permettront de chiffrer et de déchiffrer des données reçu ou à envoyer.

Signature/Vérification de données

Par le biais de la carte, nous serons en mesure de signer des données avec notre clef privée afin d'authentifier des données afin d'appliquer la non répudiation. A contrario, nous devons également pouvoir vérifier l'auteur des données. Pour cela une vérification des données devra être possible via la clef publique.

Administration des cartes

On devra pouvoir également administrer les cartes, telle que la réinitialisation du code PIN, attribution du code PIN,...

2 Documents applicables et de référence

- SC_STB : le document renfermant les spécifications techniques de Besoin ;
- SC_DaL : le document contenant l'architecture du logiciel ;
- Les comptes rendu de réunion du projet ;
- cartes-a-puce.pdf, le sujet du projet.

3 Terminologie et sigles utilisés

CdR : Cahier de Recettes ;

AdR : Analyse des Risques ;

DAL : Document d'Architecture Logicielle ;

PdD : Plan de développement ;

STB : Spécification Technique de Besoins ;

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

SSN : *Secure Social Network* ;

FaceCrypt : Application Java gérant les traitements lourds (chiffrement/déchiffrement) de l'extension et étant en relation avec la carte à puce ;

IHM : Interface Homme-Machine, (interface graphique) ;

Utilisateur : entité (humain ou programme) intéragissant avec ce sous-projet ;

Système : ce sous-projet ;

SoftCard : Application effectuant le relais entre la carte et FaceCrypt ;

Extension : programme incorporé dans le navigateur ;

Aléatoire : indistingable en temps polynomial, distribution de probabilité uniforme ;

PRNG : (Pseudo Random Number Generator) générateur de nombres pseudo-aléatoires ;

PIN : (Personal Identification Number) code servant à authentifier l'utilisateur ;

PUK : (Personal Unlock Key) code servant à débloquer la carte quand trop de codes PIN erronés ont été entrés.

4 Environnemment de tests

L'ensemble des tests ce sont effectués sur des machines ayant ces caractéristiques :
- 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 Java 1.5 (Java card).

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 a été réalisée par Giovanni Huet et Romain Pignard. Après avoir exécuté les différents tests, les responsables de ce module transmettront aux développeurs un compte rendu contenant les résultats de ces tests afin d'améliorer la version courante du logiciel et de fournir une nouvelle version à tester. 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 de tests, cette procédure comportera un jeu de tests et les modalités d'exécution des tests procédure de test.
- 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 (corrigé), nous devons réaliser un nombre de tests permettant de détecter les anomalies persistantes. Toute anomalie détectée sera noté en détails 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 test basé sur des données réelles.

Objet testé : Génération de nombres aléatoire			Version : 1.0	
Objectif de test : vérifier le comportement du générateur aléatoire de la carte à puce.				
Procédure n°1 : générer un nombre aléatoire				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Générer un nombre aléatoire à l'aide des fonctions javacard disponibles.	Obtention d'un nombre aléatoire.	F-Gl-10	OK

Procédure n°2 : évaluer le niveau de l'aléatoire				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Générer plusieurs (millions) nombres aléatoires afin d'établir des stastitiques et vérifier le niveau de l'aléatoire.	Générateur non prévisible (Probabilité uniforme)	F-Gl-10	NC

Procédure n°3 : évaluer le temps d'éxecution				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Etablir une moyenne pour la génération d'un nombre aléatoire.	Pour être transparent à l'utilisateur, nous souhaitons que le temps de génération soit $<$ 300ms.	F-Gl-10	OK

Objet testé : Déblocage de la carte (via authentification par code PIN et PUK)			Version : 1.0	
Objectif de test : vérifier le comportement de la carte lors de plusieurs tentive d'authentification.				
Procédure n°4 : verrouillage/deverouillage de la carte.				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Entrer le code PIN valide.	Déblocage de la carte et authentification de l'utilisateur rendant la carte utilisable.	F-Gl-20	OK

Procédure n°5 : verrouillage de la carte				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Effectuer un certain nombre d'authentification erroné.	Verrouillage de la carte au bout d'un nombre prédéfini de tentative.	F-Gl-20	OK

Procédure n°6 : déverrouillage de la carte				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Entrer le code PUK valide.	Deverrouillage de la carte rendant celle ci de nouveau opérationnelle.	F-Gl-20	OK

Objet testé : transmission de données			Version : 1.0	
Objectif de test : vérifier si les données contenu dans la carte peuvent être transmise.				
Procédure n°7 : transmettre des données.				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Envoyer des données de la carte à SoftCard.	Réception intégrale des données par SoftCard.	F-Gl-30	OK

Objet testé : communication sécurisée lecteur/carte			Version : 1.0	
Objectif de test : vérifier les fonctions de chiffrement, d'authentification et d'intégrité.				
Procédure n°8 : envoie de données chiffrées				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Envoyer des données chiffrées	Données non compréhensibles sans la clef de déchiffrement.	?	OK

Procédure n°9 : envoie de données authentifiées				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Envoyer des données authentifiées sans altérer le contenu.	Validation de la non modification des données reçues.	?	OK

Procédure n°10 : envoie de données authentifiées avec altération				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Envoyer des données authentifiées en altérerant le contenu.	Détection de la non modification des données reçues.	?	OK

Procédure n°11 : déchiffrement de données reçues				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Déchiffrement des données à la sortie du tunnel.	Récupération des données envoyées chiffrées en clair.	?	OK

Objet testé : déchiffrement de données			Version : 1.0	
Objectif de test : vérifier si les données reçues peuvent être déchiffrées.				
Procédure n°12 : déchiffrer avec la clef associée.				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Déchiffrer des données à partir de la carte avec la clef privée correspondante.	Données déchiffrées.	F-Gl-40	OK

Procédure n°13 : déchiffrer avec une clef invalide				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Déchiffrer des données à partir de la carte avec une clef privée non correspondante.	Données non déchiffrées	F-Gl-40	OK

Objet testé : Signature/Vérification de données			Version : 1.0	
Objectif de test : Signer des données et vérifier la signature				
Procédure n°14 : Signer/Vérrifier.				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Signer des données à partir de la carte avec la clef privée.	Données signées.	F-Gl-50	OK

Procédure n°15 : Vérification avec la clef publique associée				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Vérifier des données signées à partir de la carte avec la clef publique correspondante.	Données vérifiées.	F-Gl-50	OK

Procédure n°16 : vérification avec une clef publique invalide				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Vérifier des données signées à partir de la carte avec la clef publique non correspondante.	Données non vérifiées.	F-Gl-50	OK

Objet testé : Administration des cartes			Version : 1.0	
Objectif de test : vérifier si nous pouvons administrer les cartes				
Procédure n°17 : Attribuer un code PIN				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Attribution d'un code PIN à un utilisateur.	L'utilisateur posséde un code PIN qui lui est propre.	F-Gl-60	OK

Procédure n°18 : insertion de données sur la carte				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Insérer des données qui soit propre à l'utilisateur (login, mot de passe,...).	La carte contient les données.	F-Gl-60	OK

Procédure n°19 : modification des données sur la carte				
N°	Actions	Résultats attendus	Exigence	OK/NOK
1	Modification de données préalablement insérer (login, mot de passe, code PIN,...).	Données modifiées.	F-Gl-60	NC

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 celles ci.

Exigence	Méthode de vérification	Procédure utilisée	Commentaire
F-Gl-10	Démonstration	Procédure 1	Ce test consiste à utiliser une fonction disponible via la librairie javacard pour générer un nombre aléatoire.
F-Gl-10	Test	Procédure 2	Le test consiste à générer plusieurs nombres aléatoires (millions) et les soumettre à un test stastistique pour évaluer le niveau de l'aléatoire.
F-Gl-10	Test	Procédure 3	Le test consiste à générer plusieurs nombres aléatoires (10000) et nous faisons la moyenne afin de connaitre le temps d'éxecution moyen pour la génération d'un nombre aléatoire, qu'on considérera valide si inférieur à 300ms.
F-Gl-20	Test	Procédure 4	Le test consiste à débloquer la carte en s'authentifiant auprès de celle ci en entrant le code PIN associé.
F-Gl-20	Test	Procédure 5	Le test consiste à entrer 10 code PIN erronés afin de verrouiller la carte, et entrer ensuite le bon code PIN pour vérifier le verrouillage.
F-Gl-20	Test	Procédure 6	Le test consiste à déverrouiller la carte après avoir entré 10 codes PINs erroné en entrant le code PUK valide.
F-Gl-30	Test	Procédure 7	Le consiste à envoyer des données contenu sur la carte.
?	Test	Procédure 8	Le test consiste à envoyer des données chiffré via une commincation sécurisé par un chiffrement symétrique.
?	Test	Procédure 9	Le test consiste à envoyer des données authentifiées sans altérer le contenu. Nous devons ensuite vérifier que le contenu est bien intégre.
?	Test	Procédure 10	Le test consiste à envoyer des données authentifiées en altérant le contenu. Nous devons ensuite pouvoir voir une détection de modification du contenu.
?	Test	Procédure 11	Le test consiste à recevoir des données au préalable chiffrées, et vérifier si elles ont bien été déchiffrées.
F-Gl-40	Test	Procédure 12	Le test consiste à déchiffrer des données avec la clef privée correspondante, nous devrions alors obtenir le clair associé.
F-Gl-40	Test	Procédure 13	Le test consiste à déchiffrer des données avec la clef non valide, nous devrions alors obtenir une erreur.
F-Gl-50	Test	Procédure 14	Le test consiste à signer des données à partir de la clef privée stockée sur la carte.
F-Gl-50	Test	Procédure 15	Le test consiste à vérifier avec la clef publique correspondante des données au préalable signées. Les données doivent être alors vérifiées.
F-Gl-50	Test	Procédure 16	Le test consiste à vérifier avec une clef publique non correspondante des données au préalable signées. Les données ne sont alors pas vérifiées.
F-Gl-60	Démonstration	Procédure 17	Dans cette procédure, nous affectons à un utilisateur, donc à la carte lui appartenant, un code PIN lui étant propre afin de pouvoir débloquer la carte et l'utiliser.
F-Gl-60	Démonstration	Procédure 18	Dans cette procédure, nous insérons des données dans une carte telles qu'un mot de passe, un login,...
F-Gl-60	Test	Procédure 19	Le test consiste à modifier les données précédemment insérer sur la carte.