Plan de développement

Version	1.1
Date	24 février 2013
Rédigé par	Florian Guilbert
Relu par	Emmanuel Mocquet

MISES À JOUR

Version	Date	Modifications réalisées
0.1	07/01/2013	Création
1.0	08/01/2013	Relecture par Emmanuel MOCQUET
1.1	08/01/2013	Modifications planning (Florian GUILBERT)

Table des matières

1 Contexte du projet

Ce projet propose la mise en place de solutions cryptographiques pour sécuriser les données qu'un utilisateur place sur un réseau social au moyen d'authentifications fortes.

Il s'agirait donc ici de développer une extension pour le logiciel Mozilla Firefox permettant à l'utilisateur de gérer le chiffrement de ses données sur le réseau social Facebook. Cette extension utilisera une application Java pour assurer les traitements lourds. Pour gérer l'authentification forte, cette application dialoguerait avec une carte à puce qui contiendrait les données sensibles de l'utilisateur (login/mot de passe), clef privée, ...

Le dialogue avec cette carte à puce se fera par l'intermédiaire d'un client Java.

Ce projet est une fusion de deux projets :

- Étude et mise en œuvre de solutions d'authentifications et de signatures par cartes à puce, proposé par Magali Bardet ;
- Solutions cryptographiques pour les réseaux sociaux, proposé par Ayoub Otmani ;

Étant un projet universitaire, ce travail a pour but de nous apprendre à gérer un projet, de sa partie analyse jusqu'à sa complète réalisation. Pour cette même raison, le projet devra être impérativement terminé avant le 04 mars 2013.

2 Documents applicables et de références

- Intitulé des sujets du projet ;
- spécification technique de besoin ;
- cahier des recettes ;
- document d'architecture logicielle ;
- analyse des risques ;
- plan qualité ;

3 Terminologie et sigles utilisés

AdR : Analyse des Risques ;

CdR : Cahier de Recettes ;

DAL : Document d'Architecture Logicielle ;

PdD : Plan de développement ;

STB : Spécification Technique de Besoins ;

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

SSN : Secure Social Network, relatif au sous-projet sur la sécurisation d'un réseau social

IHM : Interface homme-machine, (interface graphique) ;

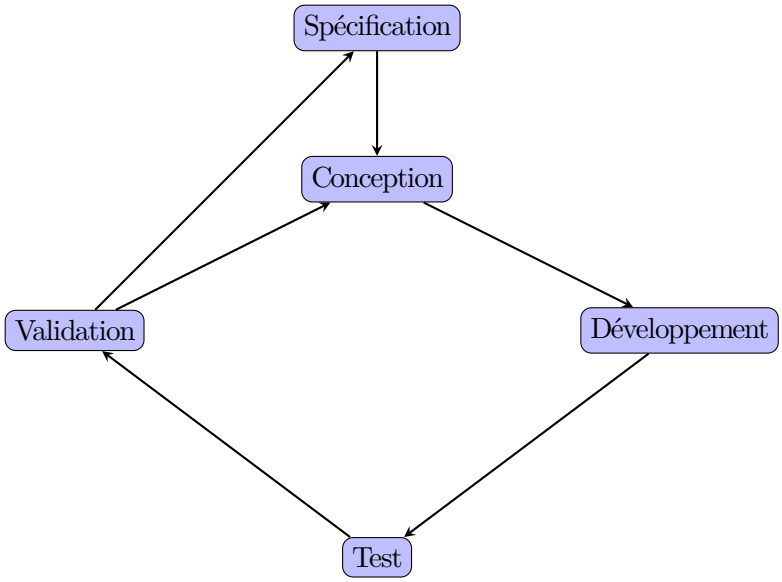
SoftCard : application qui assure un passerelle entre le lecteur de carte et l'ordinateur ;

Extension : programme incorporé dans le navigateur.

FaceCrypt : application Java effectuant les traitements lourds de l'extension.

4 Méthodologie et développement

Le développement du projet suit le schéma suivant :



Spécification
- Déterminer les objectifs ;
- définir les contraintes ;
- évaluer les risques.

Responsabilité : clients, testeurs et programmeurs.

Conception
- Définir les composants à développer.

Responsabilité : testeurs et programmeurs.

Développement
- Développement des composants ;
- tests unitaires sur ces composants.

Responsabilité : programmeurs.

Test
- Tester des scénarii de tests.

Responsabilité : testeurs.

Validation
- L'étape de validation détermine si la version développée propose bien les fonctionnalités attendues et dans ce cas valide la version du logiciel. Le travail pour la prochaine version peut commencer ;
- s'il n'y pas validation de la version, alors c'est aux testeurs de décider s'il faut repasser l'étape de spécification ou s'il faut retourner directement à l'étape de conception ;

– dans le cas d'un succès d'une validation, une version du logiciel peut être livrée.

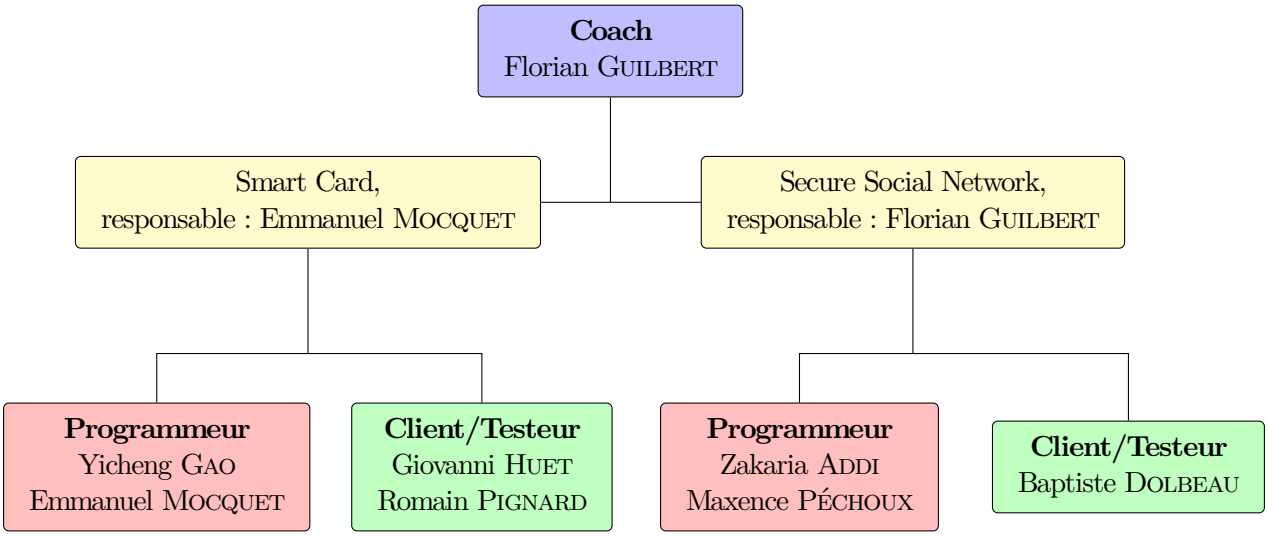
Responsabilité : clients et testeurs.

Cette méthodologie de développement suit la méthode XP (eXtreme Programming). Durant le développement de ce projet, il y aura quatre itérations. Chacune des trois premières itérations est divisée en deux (correspondant aux deux sous-projets) :

1. – établir un dialogue entre le terminal et la carte ;
   – développer une extension et l'application Java (FaceCrypt) implantant le chiffrement et le déchiffrement de données ;
2. – utiliser les fonctions cryptographiques de la carte,
   – développer les systèmes d'injection de code dans l'extension, gérer la persistance de données dans FaceCrypt, étudier le protocole `xpcom` ;
3. – rédaction de documentation et développement de *SoftCard* ;
   – implantation du protocole `xpcom` permettant le dialogue entre FaceCrypt et l'extension
4. fusion des projets : implantation du dialogue entre le *softCard* et FaceCrypt.

Chacune de ces étapes comporte des modules qui seront développés en binôme afin, d'une part, de faire en sorte que le plus de programmeurs possible maitrisent le code source et, d'autre part, qu'une absence ne nuise pas au processus de développement.

5 Organisation et responsabilités



Coach :

– Garant du processus et de la méthodologie ;
– vérifie que chacun joue son rôle ;
– organise et anime les réunions et les séances de planifications ;
– valide les orientations techniques.

Client :
- Spécifie les fonctionnalités du logiciel ;
- communique les informations utiles aux développeurs et reçoit leurs “feedback” ;
- définit les fonctionnalités à partir de scénarii d’utilisations ;
- spécifie les tests de recette.

Programmeur :
- Responsables de la production du code ;
- conçoit pour assurer la pérennité du code ;
- teste pour assurer la qualité du code ;
- émet et révise des estimations de charge.

Testeur :
- Conçoit et réalise les tests de recettes défini par le client ;
- recherche l’automatisation des tests ;
- développe les outils de tests nécessaires et les scripts à exécuter ;
- témoigne de l’avancement du projet.

6 Évaluation du projet et dimensionnement des moyens

Le projet va être organisé en quatre versions (une par itération). À la fin de chaque version, les applications seront testées conformément aux tests décrits dans les cahiers de recettes.

Voici un résumé de chaque version.

Version 0.1 La première version du projet consistera en trois composants, une application permettant de faire générer des nombres pseudo-aléatoire par la carte et d’y stocker des informations, d’une extension incorporée sur le navigateur Mozilla Firefox et une application Java (FaceCrypt) qui permet chiffrer ou de déchiffrer des données.

Version 0.2 Dans la deuxième version, l’application et la carte à puce doivent pouvoir chiffrer/déchiffrer/-signer/vérifier des données. De plus, il devrait être possible de stocker des données, tels que des certificats, sur la partie cachée. Pour la partie *Secure Social Network*, l’extension devrait pouvoir injecter du code dans la page du réseau social tandis qu’en parallèle, FaceCrypt devrait pouvoir stocker des informations de manière permanente.

Version 0.3 La troisième version se résume principalement en la mise en place d’un dialogue entre l’extension et FaceCrypt, un autre entre FaceCrypt et SoftCard et encore un autre entre la carte et SoftCard. Tous ces dialogues devront être sécurisés (dans le sens défini dans les STB).

Version 1.0, finale La version finale correspond à la fusion des deux sous-projets, l’intégration finale des composants et de leurs connexions.

7 Planning général

7.1 Prévisions

	Mode Tâche	Nom de la tâche	Durée	Début	Fin	Préd	Noms ressources
1		Etablir dialogue entre carte et terminal	3 jours	Lun 21/01/13	Mer 23/01/13		Emmanuel Mocquet;Yicheng
2		Stocker des informations sur carte	2 jours	Jeu 24/01/13	Ven 25/01/13	1	Emmanuel Mocquet;Giovanni
3		développement d'une extension	5 jours	Lun 21/01/13	Ven 25/01/13		Maxence Péchoux;Zakaria Addi
4		application Java (chiffrement, déchiffrement)	5 jours	Lun 21/01/13	Ven 25/01/13		Baptiste Dolbeau;Florian Guilbert
5		Utilisation des fonctions cryptographique de carte	10 jours	Lun 28/01/13	Ven 08/02/13	1;2	Emmanuel Mocquet;Yicheng Gao
6		stocker des informations sur partie caché de carte	10 jours	Lun 28/01/13	Ven 08/02/13	1;2	Giovanni Huet;Romain Pignard
7		injection de code par l'extension	10 jours	Lun 28/01/13	Ven 08/02/13	3	Maxence Péchoux;Zakaria Addi
8		persistance des données sur Application Java	5 jours	Lun 28/01/13	Ven 01/02/13	4	Baptiste Dolbeau;Florian Guilbert
9		Etude du protocole xpcom	5 jours	Lun 04/02/13	Ven 08/02/13	8	Baptiste Dolbeau;Florian G
10		Développement du SoftCard	5 jours	Lun 11/02/13	Ven 15/02/13	6;5	Emmanuel Mocquet;Giovar
11		Implantation xpcom entre extension et Application Java	5 jours	Lun 11/02/13	Ven 15/02/13	9;7	Baptiste Dolbeau;Florian Guilbert;Maxence
12		Fusion des sous-projets	10 jours	Lun 18/02/13	Ven 01/03/13	10;11	Baptiste Dolbeau;Emmanu

FIGURE 1 – Diagramme de Gantt, prévision

Sur le graphe ci-dessous, on peut observer trois couleurs, le tâche bleue correspond aux tâches correspondants au sous-projet *smartCards*, le rouge aux tâches du sous-projet *Secure Social Network* et enfin le violet correspond aux tâches ayant trait aux deux sous-projets. Pour les graphes autres ci-dessous, le vert a remplacé le rouge (qui était une couleur mal adaptée car préférée pour les tâches critiques).

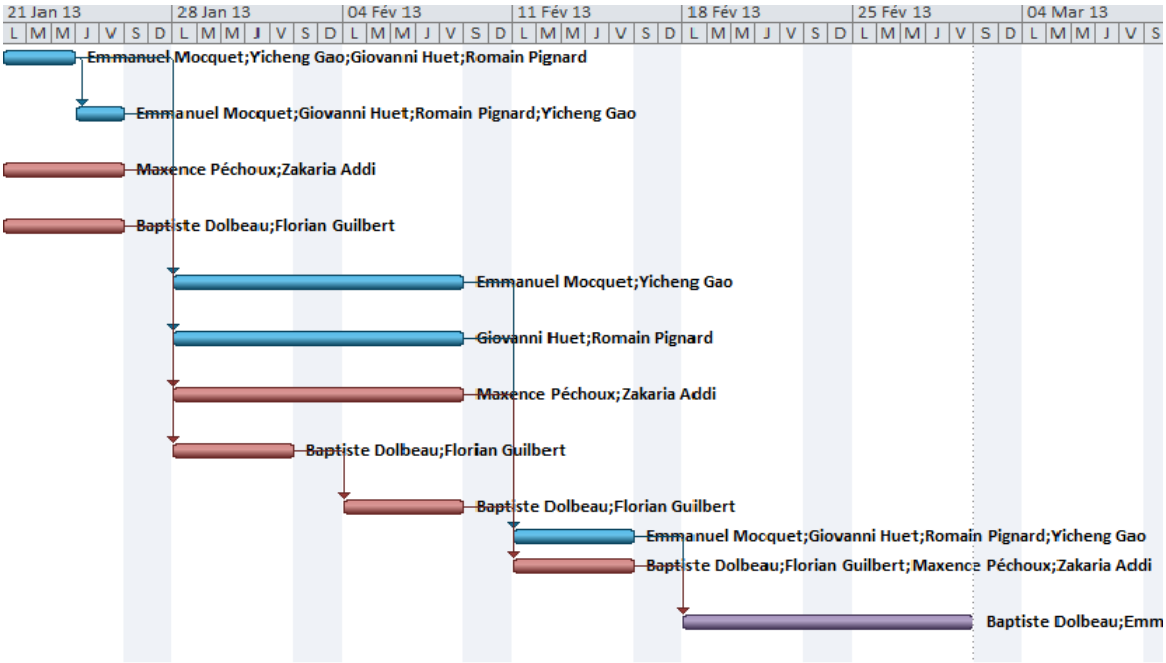


FIGURE 2 – Diagramme de Gantt, graphe, prévision

7.2 Suivi

Mode Tâche	Nom de la tâche	Durée	Début	Fin	Préd	Noms ressources
	Itération 1	**5 jours**	**Lun 21/01/13**	**Ven 25/01/13**		
	Etablir dialogue entre carte et terminal	3 jours	Lun 21/01/13	Mer 23/01/13		Emmanuel Mocquet;Yicheng
	Stocker des informations sur carte	2 jours	Jeu 24/01/13	Ven 25/01/13	2	Emmanuel Mocquet;Giovanni
	développement d'une extension	5 jours	Lun 21/01/13	Ven 25/01/13		Maxence Péchoux;Zakaria Addi
	FaceCrypt (chiffrement, déchiffrement)	5 jours	Lun 21/01/13	Ven 25/01/13		Baptiste Dolbeau;Florian Guilbert

FIGURE 3 – Diagramme de Gantt, itération 1

	Itération 2	**15 jours**	**Lun 28/01/13**	**Ven 15/02/13**		
	Utilisation/tests fonctions cryptographiques de carte	10 jours	Lun 28/01/13	Ven 08/02/13	3	Emmanuel Mocquet;Yicheng
	Tunnel sécurisé entre smartCard et SoftCard	15 jours	Lun 28/01/13	Ven 15/02/13	3	Romain Pignard
	injection de code par l'extension	10 jours	Lun 28/01/13	Ven 08/02/13	4	Maxence Péchoux;Zakaria Addi[50%]
	Etude du protocole XPCom	10 jours	Lun 28/01/13	Ven 08/02/13	4	Zakaria Addi[50%]
	Gestion des listes d'amis	10 jours	Lun 28/01/13	Ven 08/02/13	5	Florian Guilbert
	FaceCrypt, Tunnel SSL	10 jours	Lun 28/01/13	Ven 08/02/13	5	Baptiste Dolbeau

FIGURE 4 – Diagramme de Gantt, itération 2

	Itération 3	**5 jours**	**Lun 11/02/13**	**Ven 15/02/13**		
	Communication FaceCrypt/SoftCard	5 jours	Lun 11/02/13	Ven 15/02/13	12	Baptiste Dolbeau[50%];Emmanuel
	Communication FaceCrypt/Extension	5 jours	Lun 11/02/13	Ven 15/02/13	10	Baptiste Dolbeau[50%];Zakaria
	Tests des composants de smartCard	5 jours	Lun 11/02/13	Ven 15/02/13	7	Giovanni Huet;Yicheng Gao
	IHM extension et étude des images Facebook	5 jours	Lun 11/02/13	Ven 15/02/13		Florian Guilbert
	Intégration de l'extension	5 jours	Lun 11/02/13	Ven 15/02/13	9	Maxence Péchoux

FIGURE 5 – Diagramme de Gantt, itération 3

	Itération 4	10 jours	Lun 18/02/13	Ven 01/03/13		
	OTP	10 jours	Lun 18/02/13	Ven 01/03/13	13	Yicheng Gao
	Adaptations des applets avec le tunnel	10 jours	Lun 18/02/13	Ven 01/03/13	8	Romain Pignard
	Tests et documentations	10 jours	Lun 18/02/13	Ven 01/03/13	16;14	Giovanni Huet
	Administration, test sur le PIN, protocole de communication	10 jours	Lun 18/02/13	Ven 01/03/13	14	Emmanuel Mocquet
	Intégration des listes d'amis, première connexion, modif mot de passe, déconnexion	10 jours	Lun 18/02/13	Ven 01/03/13	17;18	Florian Guilbert;Maxence Péchoux;Zakaria Addi
	Gestion des protocoles de FaceCrypt avec (SoftCard/Extension)	10 jours	Lun 18/02/13	Ven 01/03/13	14;15	Baptiste Dolbeau

FIGURE 6 – Diagramme de Gantt, itération 4

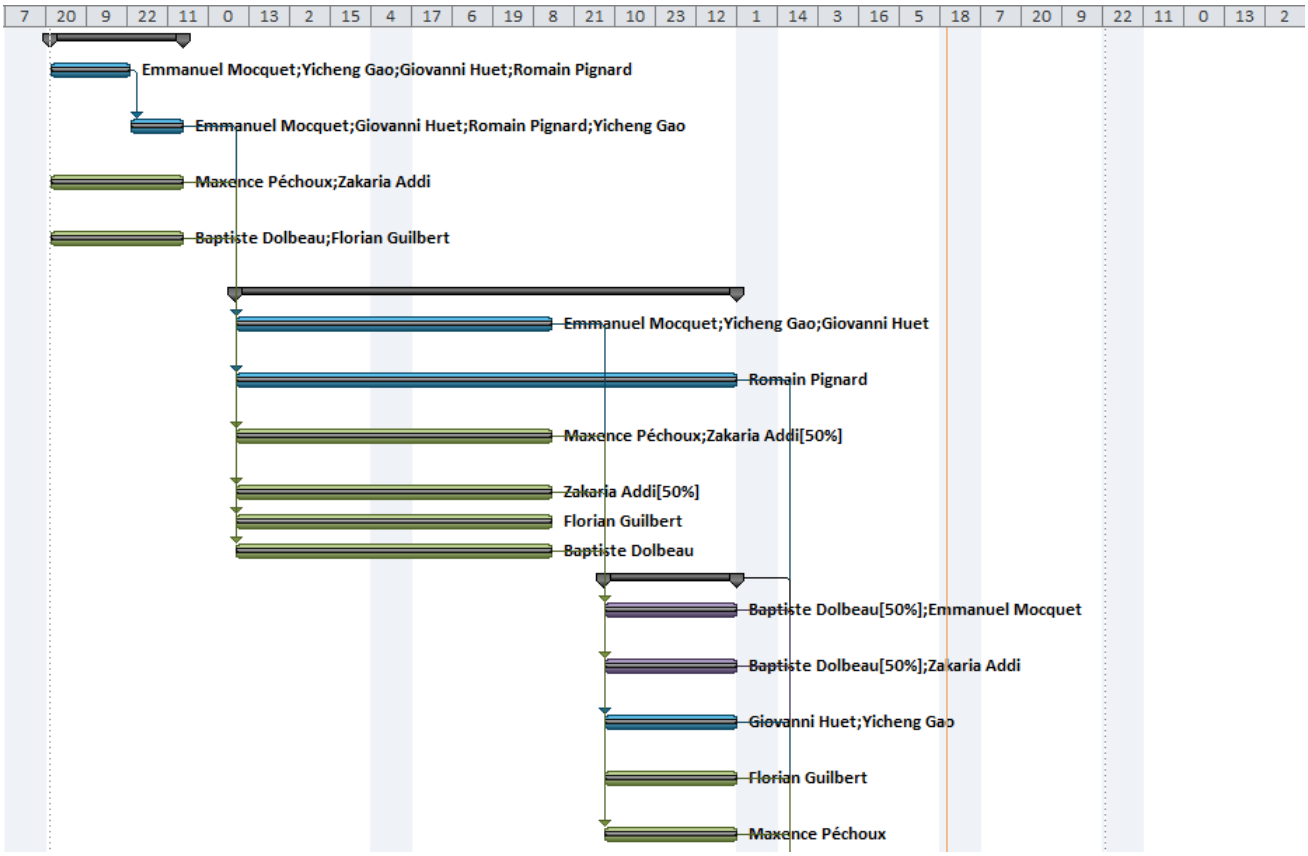


FIGURE 7 – Diagramme de Gantt, graphes

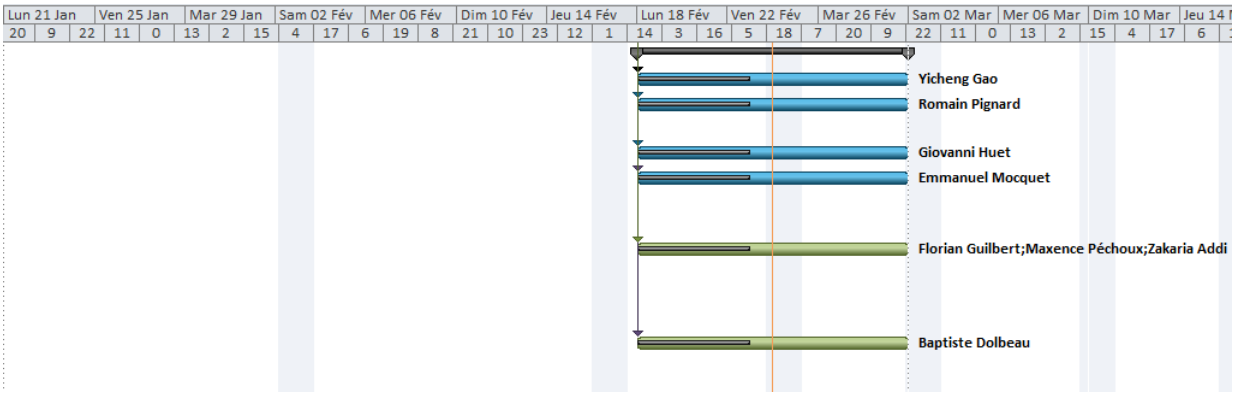


FIGURE 8 – Diagramme de Gantt, graphes

8 Procédés de gestion

8.1 Gestion de la documentation

Il y aura quatre documentations livrables :
- le manuel d'utilisation du *softCard* rédigé par l'équipe testeur, du groupe *smartCards* ;
- le manuel d'utilisation global de l'application rédigé par l'équipe testeur, des deux groupes ;
- un document décrivant comment ont été développées les applications pour la carte à puce et comment sont-elles installés ;
- un document sur les protocoles cryptographiques mis en œuvre dans ce projet.

Les documents utilisées tout au long de la réalisation de ce projet sont : (les relecteurs sont encore à préciser)
- Analyse des risques (AdR) rédigée par Yicheng GAO ;
- Cahier des recettes *smartCard* (CdR) rédigé par Giovanni HUET et Romain PIGNARD ;
- Cahier des recettes *Secure Social Network* (CdR) rédigé par Baptiste DOLBEAU et Florian GUILBERT ;
- Document d'architecture logicielle *smartCard* (DAL) rédigé par Emmanuel MOCQUET ;
- Document d'architecture logicielle *Secure Social Network* (DAL) rédigé par Zakaria ADDI et Maxence PÉCHOUX ;
- Plan de développement (PdD) rédigé par Florian GUILBERT et relu par Emmanuel MOCQUET ;
- Plan de qualité (PdQ) rédigé par Baptiste DOLBEAU et relu par Yicheng GAO ;
- Spécification technique des besoins *smartCard* (CdR) rédigée par Giovanni HUET et Romain PIGNARD, relu par Florian GUILBERT et Emmanuel MOCQUET ;
- Spécification technique des besoins *Secure Social Network* (STB) rédigée Florian GUILBERT et relu par Baptiste DOLBEAU.

8.2 Gestion des configurations

Toutes les versions du programmes seront gérées par le logiciel de versionnage `git`. Toutes les machines servant à développer devront avoir les même configurations du logiciel Java (1.5). De même, mais cela reste à confirmer, les ordinateurs clients devront aussi posséder cette version de Java.

9 Revues et points clefs

Pas de revues officielles de prévues.

10 Procédures de suivi d'avancement

Le suivi d'avancement du projet sera effectué par l'intermédiaire de réunions régulières et de jalons. Ceux-ci permettront de contrôler l'état d'avancement de chaque module et de réagir rapidement à tout écart avec les prévisions en réorganisant le planning.

Il y aura par conséquent une réunion chaque semaine avec les clients respectifs les membres du groupe. À chaque validation, il y aura présentation au client du travail effectué.

Des réunions avec le client pourront aussi être organisées si le client en fait la demande ou bien qu'un membre du groupe souhaite bénéficier de son avis.

Pour chaque réunion, un compte-rendu sera réalisé et placé à disposition du groupe par l'intermédiaire de `git`.