Annexe

❖ Section A

Etape 1 : Suppression du contrat

- Taper #73
- Sélectionner le « nom applicatif » : « CB-PP EMV BIAT »
- Entrer le « numéro application » (No Usager) : ****
- « <-Carte COMM CB<<< »
- Taper « ok ».
- Entrer le « Num Commerçant » : *******
- « Confirmer la destruction du contrat ? »
- Tapez « oui ».

Etape 2 : création du contrat

- Taper #71
- Sélectionner « le nom applicatif » : « CB-PP EMV BIAT »
- « Libelle CB-PP EMV BIAT » (taper « Enter »)
- Taper « Cancel ».

Etape 3 : Télé paramétrage de l'application

- Taper #80
- Sélectionner « la carte » : « CB-PP EMV BIAT »
- « <-Carte COMM CB<<< »
- Taper « ok ».

- Entrer le « Num Commerçant » : *******
- Sélectionner « Gestion Paramètres »
- Entrer le « Num Tel Telepar » : 71 *** ***
- Entrer le « No serveur » : **********
- Dans le menu « raccordement » sélectionner : « EBAM »
- Sélectionner : « Pas d'impression », dans le menu « TR. Non Abouties ».
- Entrer le « Num log system » : ***.
- Saisir le « code de la banque » : *****.
- Sélectionner « non » dans le menu « Chargement Terminal ».
- Sélectionner « Appel » dans le menu « Appel Telepar ».
- Fin du test.

➔ Remarque : pour réaliser un nouveau test lors d'un chargement réussi il faut exécuter les trois étapes. Si le chargement échoue (perte porteuse se qui implique un échec de connexion), il faut refaire uniquement la troisième étape.

Le chargement échoue quand le TPE n'arrive pas à établir une connexion avec le serveur après trois tentatives («Appel Telepar »).

❖ Section B

Etude et choix méthodologique

Il existe maintenant un nombre important de méthodes de la gestion de travail qui se sont développées en suivant l'évolution des langages et des techniques. Mais ces méthodes n'apportent pas la solution à tous les problèmes, elles disposent de certaines qualités propres au traitement de problèmes spécifiques mais ont des lacunes au regard d'autres problèmes. Elles sont en général très limitées lorsque le système visé est hautement interactif, et ont toutes besoin d'améliorations à ce sujet.

Ça sera l'objectif de ce paragraphe qui fait l'affaire de choisir la méthode la plus appropriée et adaptée pour répondre au problématique de cette application.

Comparatif des méthodes agiles vs classiques

Les méthodes de développements proposées comme « Waterfall », « Cycle en V », la « Spiral de Boehm » et « Cleanroom » ne permettent pas d'apporter des pratiques de développement logiciel assurant la maîtrise des coûts et des délais pour un périmètre fonctionnel donné.

La figure ci-dessous montre les avantages des méthodes agiles par rapport aux méthodes traditionnelles en tout ce qui concerne le pourcentage de succès des projets.

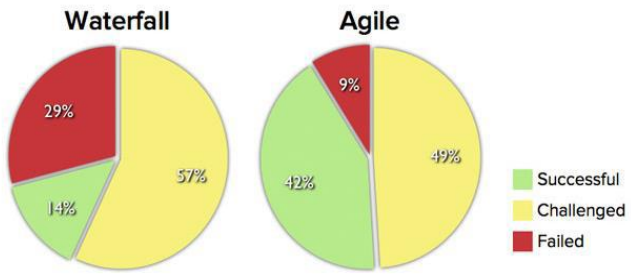

Figure 1 : Pourcentage de succès des projets

En plus que ça les méthodes agiles proposent plusieurs avantages par rapport aux méthodes traditionnelles comme illustré dans le tableau suivant.

Thème	Approche traditionnelle	Approche agile
Cycle de vie	En cascade ou en V, sans rétroaction possible, phases séquentielles.	Itératif et incrémental.
Planification	Prédictive, caractérisée par des plans plus ou moins détaillés sur la base d'un périmètre et d'exigences définies et stables au début du projet.	Adaptative avec plusieurs niveaux de planification (macro- et microplanification) avec ajustements si nécessaires au fil de l'eau en fonction des changements survenus.
Documentation	Produite en quantité importante comme support de communication, de validation et de contractualisation.	Réduite au strict nécessaire au profit d'incréments fonctionnels opérationnels pour obtenir le feedback du client.
Équipe	Une équipe avec des ressources spécialisées, dirigées par un chef de projet.	Une équipe responsabilisée où l'initiative et la communication sont privilégiées, soutenue par le chef de projet.
Qualité	Contrôle qualité à la fin du cycle de développement. Le client découvre le produit fini.	Un contrôle qualité précoce et permanent, au niveau du produit et du processus. Le client visualise les résultats tôt et fréquemment.
Changement	Résistance voire opposition au changement. Processus lourds de gestion des changements acceptés.	Accueil favorable au changement inéluctable, intégré dans le processus.
Suivi de l'avancement	Mesure de la conformité aux plans initiaux. Analyse des écarts.	Un seul indicateur d'avancement : le nombre de fonctionnalités implémentées et le travail restant à faire.
Gestion des risques	Processus distinct, rigoureux, de gestion des risques.	Gestion des risques intégrée dans le processus global, avec responsabilisation de chacun dans l'identification et la résolution des risques. Pilotage par les risques.
Mesure du succès	Respect des engagements initiaux en termes de coûts, de budget et de niveau de qualité.	Satisfaction client par la livraison de valeur ajoutée.

Tableau 1: Avantages des méthodes agiles

Comme on l'a remarqué dans le tableau 1 les méthodes classiques sont rigides ne permettent pas le feedback pour la moindre modification, tout est organisé et planifié auparavant, et la négociation ce fait à travers un document livrable vers la fin de chaque phase.

En analysant le comparatif entre les méthodes classiques et agiles, on déduise que généralement on utilise une méthode agile lorsque :

– Le projet est important et exige des changements au fur et à mesure de son élaboration. C’est bien le cas pour ce travail.

– Les besoins sont évolutifs et le projet apporte, lors de sa mise en œuvre, de nouvelles idées et approches. En effet, il est souvent difficile de déterminer au début de façon définitive les paramètres d’une application. En plus, il est fréquent que la banque décide de rajouter ou supprimer une fonctionnalité au cours de projet.

– Un dialogue doit être établi entre les développeurs de l’application et des clients disponibles pour faire des tests.

Les méthodes agiles

Les méthodes agiles sont des méthodologies essentiellement dédiées à la gestion de projets informatiques. Agile représente un ensemble de “méthodes et pratiques basées sur les valeurs et les principes du Manifeste Agile”, qui repose entre autre sur la collaboration, l’autonomie et des équipes pluridisciplinaires.

Ces méthodes permettent de répondre aux attentes du client en un temps limité grâce à l’utilisation de celui-ci, tout en faisant monter les collaborateurs en compétences. Ces méthodes constituent donc un gain en productivité ainsi qu'un avantage compétitif tant du côté client que du côté du fournisseur.

Les méthodes agiles impliquent le client dans la réalisation du début à la fin du projet. Grâce à la méthode agile le demandeur obtient une meilleure visibilité de la gestion des travaux qu’avec une méthode classique.

L’implication du client dans le processus permet à l’équipe d’obtenir un feedback régulier afin d’appliquer directement les changements nécessaires. [8]

Cette méthode vise à accélérer le développement d’un logiciel. De plus, elle assure la réalisation d’un logiciel fonctionnel tout au long de la durée de sa création.

Ainsi, il est plus adéquat d'opter pour les méthodes agiles qui répondent mieux à nos besoins d'adaptabilité et de flexibilité. Reste aussi à faire le bon choix en ce qui concerne la méthode la plus appropriée pour satisfaire les exigences particulières de notre problématique.

Plusieurs méthodes agiles ont été mises en place, tel que: RUP/ 2TUP / SCRUM/ XP

En se référant au tableau ci-dessous mettant en confrontation trois méthodes agiles, on a conclu qu'il convient de choisir la méthodologie agile SCRUM pour mener à bon port ce projet puisque elle satisfait les conditions suivantes :

- Plus de souplesse et de réactivité
- La grande capacité d'adaptation au changement grâce à des itérations courtes.
- La chose la plus importante, c'est que Scrum rassemble les deux cotés théoriques et pratiques et se rapproche beaucoup de la réalité.

Comparatif des méthodes agiles

Méthodologie	Srum	XP	UP
Description	Méthode agile dédiée à la gestion des projets, méthode itérative qui maitrise une production planifiée des processus incrémentaux.	eXtreme Programming méthode agile orienté sur l'aspect réalisation d'une application pour la gestion des projets.	Unified Process est une méthode de développement logiciels orientés objets Itérative
Points clés	Indépendant, équipes à organisation automatique de développement, cycles de 30 jours	Développement réduit par client, petite équipe, construction quotidienne.	Tâche de rôle conduite par activité.
Caractéristiques	Cette technique est reconnue pour sa flexibilité et son efficacité : Transférer de "défini et répétitif" à la "vue de développement de produits nouveaux de Scrum"	Refectoring – Devoir refaire conception du système de façon continue pour améliorer sa performance et sa capacité de réponse aux changements	Guidée par les besoins des utilisateurs, centrée sur l'architecture logicielle.
Imperfection	Scrum spécifie en détail comment gérer les cycles de 30 jours mais l'intégration et le test d'acceptation ne sont pas détaillées.	Les pratiques individuelles sont bien adaptées dans plusieurs situations mais les pratiques de gestion et de vue général sont moins attentives.	Manque des description comment réduire, comment changer.

Tableau 2 : Comparaison des méthodes agiles

La méthodologie SCRUM

«Scrum » est la méthode agile la plus populaire et la plus utilsée. La méthode scrum s'appuie sur des « sprints » qui sont des espaces temps assez courts pouvant aller de quelques heures jusqu'à un mois. Généralement et de préférence un sprint s'étend sur deux semaines. À la fin de chaque sprint, l'équipe présente ce qu'elle a ajouté au produit

- Sprint

Le sprint est une période d'un mois au maximum, au bout de laquelle l'équipe délivre un incrément du produit, potentiellement livrable. Chaque sprint possède un but et on lui associe une liste d'éléments (fonctionnalités) à réaliser, appelée (backlog du produit).

- Release

Un release correspond à la livraison d'une version. On parle de release pour considérer la période de temps qui va du début du travail sur cette version jusqu'à sa livraison et qui passe par une série de sprints successifs.

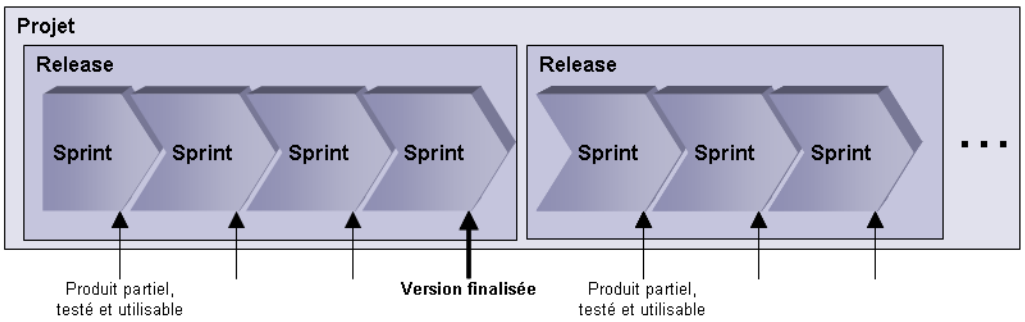

Figure 2: Déroulement d'un release

Scrum s’appuie sur 3 piliers :

- La transparence : permet à tout observateur d'obtenir rapidement une bonne compréhension du projet.
- L'inspection : Scrum propose de faire le point sur les différents artéfacts produits à intervalle régulier, afin de détecter toute variation indésirable.
- L'adaptation : Si une dérive est constatée pendant l'inspection, le processus doit alors être adapté. Scrum fournit des rituels, durant lesquels cette adaptation est possible. Il s'agit de sprint planning, de daily scrum, et de sprint review.

Méthodologie	Scrum
Cycle de développement	Spirale (itératif)
Etapes concernées	Analyse Modélisation Spécification Conception Evaluation à priori Evaluation à posteriori
Approche	Ascendante (Botton-up)
Degré d’implication de l’utilisateur	Beaucoup
Moment d’implication de l’utilisateur	Début Milieu Fin

Tableau 3 : Description du scrum

a) Le processus SCRUM

Le processus présenté dans la figure ci-dessous traduit comment on gère un projet suivant la méthodologie scrum, tout d'abord on décante la liste des tâches à faire, ensuite on associé des priorités et des criticités à chaque tâche et on estime la période de réalisation que dépend chacune, et comme seconde étape, on tient compte de priorité et de l'estimation on décompose les backlogs en des sprint de 2 à 4 semaine et faire le suivi de ces sprint qui finalise par un produit livrable fonctionnelle que le client doit valider.

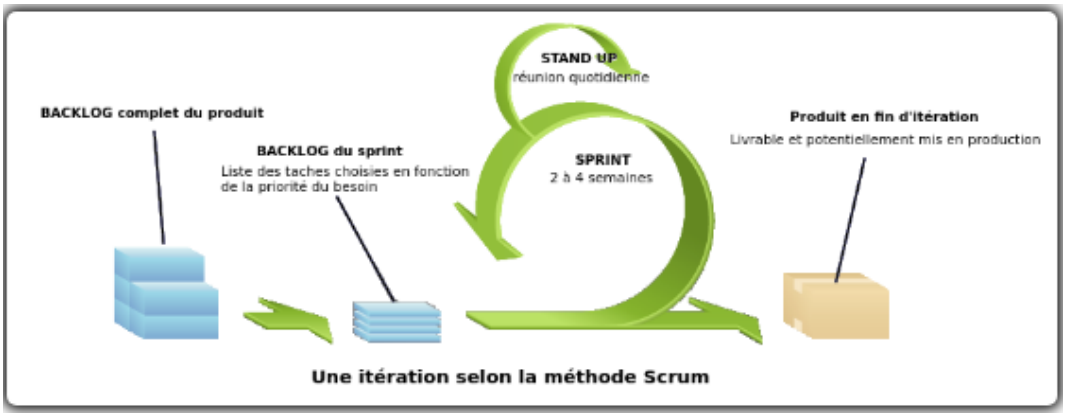

Figure 3 : Le processus SCRUM

b) Les acteurs SCRUM

Product Owner

Le Directeur du Projet: définit les fonctionnalités du produit :

- Choisit la date et le contenu de la release.
- Responsable du retour sur investissement.
- Définit les priorités dans le backlog en fonction de la valeur « métier ».
- Ajuste les fonctionnalités et les priorités à chaque sprint si nécessaire.
- Accepte ou rejette les résultats.
- Etablit la priorité des fonctionnalités à développer ou corriger.

ScrumMaster

- S’assure que les principes et les valeurs de Scrum sont respectés
- Facilite la communication au sein de l’équipe
- Cherche à améliorer la productivité et le savoir-faire de son équipe

L'équipe du projet

- Pas de rôle bien déterminé : architecte, développeur, testeur
- La composition de l'équipe ne change pas pendant un Sprint.
- Tous les membres de l’équipe apportent leur savoir-faire pour accomplir les tâches
- Taille de 6 à 10 personnes en général et pouvant aller jusqu’à 200 personnes.

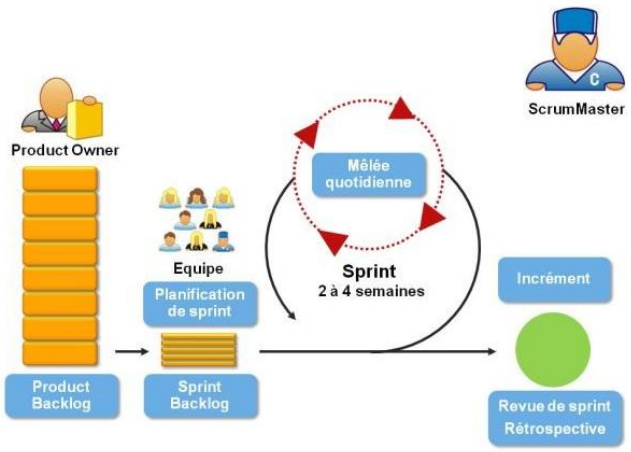

Figure 4 : Les évènements par rapport acteurs SCRUM

Références:

http://ineumann.developpez.com/tutoriels/alm/agile_scrum/

https://www.supinfo.com/articles/single/3093-comparatif-methodes-agiles

❖ Section C

Secure Plain Diffie–Hellman algorithm

Iunput: un point de base P, une clé privée k, une clé privée xAES, une clé privée yHMAC, un identifiant personnel, Timestamp ts

Participants: A, B et Centre d'authentification (AuC)

Output: un secret partagé G

1. A calcule P (A) k,
2. A calcule HMAC (AES (PA (A) k + pidA + ts)) en utilisant xAES (A) et yHMAC (A),
3. → Vérifications AuC (2) (Recalcule HMAC et vérifie que ts est plus récent que répertorié et fiable),
4. AuC déballer HMAC (AES (PA (A) k + pidA + ts)) en utilisant xAES (A) et yHMAC (A),
5. AuC recalcule HMAC (AES (PA (A) k + pidA + ts)) en utilisant xAES (B) et yHMAC (B),
6. → B Vérifications (5) (Recalcule HMAC et vérifie que ts est plus récent que répertorié et fiable),
7. B déballer (6) en utilisant xAES (B) et yHMAC (B),
8. B calcule P (B) k et stocke P (A) k,
9. B calcule HMAC (AES (P (B) k + pidB + ts)) en utilisant xAES (B) et yHMAC (B),
10. → Vérifications AuC (9) (Recalcule HMAC et vérifie que ts est plus récent que répertorié et fiable),

11. AuC décompresser HMAC (AES (P (B) k + pidB + ts)) en utilisant xAES (B) et yHMAC (B),
12. AuC recalcule HMAC (AES (P (B) k + pidB + ts)) en utilisant xAES (A) et yHMAC (A),
13. → A Vérifications (12) (Recalcule HMAC et vérifie que ts est plus récent que répertorié et fiable),
14. Un déballage (13) utilisant xAES (A) et yHMAC (A) et stocke P (B) k,
15. Le secret partagé commun est P (A) kP (B) k.

➔Remarque

La clé k privé est généré par le participant,

Les clés pour A: xAES (A), yHMAC (A) et xAES (B), yHMAC (B) sont délivrées à partir de centre d'authentification (AuC) dans la phase initiale pendant la configuration.

Comme on peut le voir avec cet algorithme, même l'AuC ne peut pas calculer le secret partagé commun P (A) kP (B) k puisque seuls les participants eux-mêmes connaître la clé privée k.

L'échange de clé est sécurisé plus loin. L'algorithme HMAC résout le problème de modification malveillante de l'échange de clés et permettra également d'éviter rejouer les attaques. L'unicité du message est garantie en utilisant Timestamp ts.

❖ HMAC (Hash-based Message Authentication Code)

Le HMAC est publié le 1997 dans le document RFC 2104. Selon ce document l'algorithme HMAC peut être utilisé avec n'importe quelle itérative fonction de hachage cryptographique. À l'heure actuelle, il existe deux standards implémentations: SHA-1 et SHA-2. SHA signifie Secure Hash Standard.

HMAC consiste en un outil de chiffrement fonction de hachage H et une clé secrète K.

Deux chaînes fixes sont également utilisées; ipad (interne) et opad (externe). Ipad contient l'octet 0x36 B fois, où B est la longueur de K. opad contiennent l'octet 0x5C B fois. Le HMAC est maintenant calculé [9, p. 3] sur du texte aText:

H (K XOR opad), H (K XOR ipad, aText)

❖ Spécification de l'algorithme

L'algorithme a d'autres exigences. Ce qui suit est supposé:

1. A et B sont des participants dans le système et la procédure d'authentification entre AuC et les participants sont effectués correctement.
2. Les clés xAES (A), yHMAC (A) et xAES (B), yHMAC (B) sont créées dans une manière challenge-réponse avec AuC.
3. Le point de base de la courbe elliptique est créé avec d'autres paramètres de domaine.
4. Un pid est sélectionné.
5. Une clé privée k pour chaque participant est sélectionnée.
6. L'horodatage ts est créé localement pour les deux participants A et B plus l'AuC.
7. A, B et AuC maintiennent une liste des horodatages utilisés pour vérifier qu'un message est nouveau et n'a jamais été reçu auparavant. L'horodatage est également crypté.