

Plan de développement détaillé

Version	1.3
Date	24 mai 2013
Rédigé par	Ismael Kabore – Julien Legras
Relu par	
Approuvé par	

MISES À JOUR

Version	Date	Modifications réalisées
0.1	07/12/2012	Création
0.2	17/12/2012	Ajout des diagrammes de Gantt
0.3	20/12/2012	Ajout des tableaux de redimensionnement et des réunions client
0.4	29/12/2012	Ajout des réunions de TD et de groupe
1.1	21/02/2013	Correction du document d'après le retour de Karim ABDELLAH GODARD
1.2	26/04/2013	Mise à jour du planning réel de développement et des réunions hebdomadaires
1.3	24/05/2013	Mise à jour du Gantt

Table des matières

1	Objet	4
2	La méthode de développement	4
2.1	Méthodes agiles	4
2.2	Méthode Scrum	4
2.3	Pourquoi ?	5
3	Les livrables	5
4	Organisation	5
5	Dimensionnement	5
5.1	Stratégie	5
5.2	Description des tâches	6
5.3	Évaluation des charges et répartition des tâches	6
6	Suivi	11
6.1	Gestion électronique des documents	11
6.2	Réunions	11
6.2.1	Réunions avec le client	11
6.2.2	Réunions TD	12
6.2.3	Réunions de groupe	13
6.2.4	Réunions pendant le développement	13

1 Objet

Ce document réunit les informations concernant le développement du projet : méthode, livrables, organisation, dimensionnement et le suivi du projet.

2 La méthode de développement

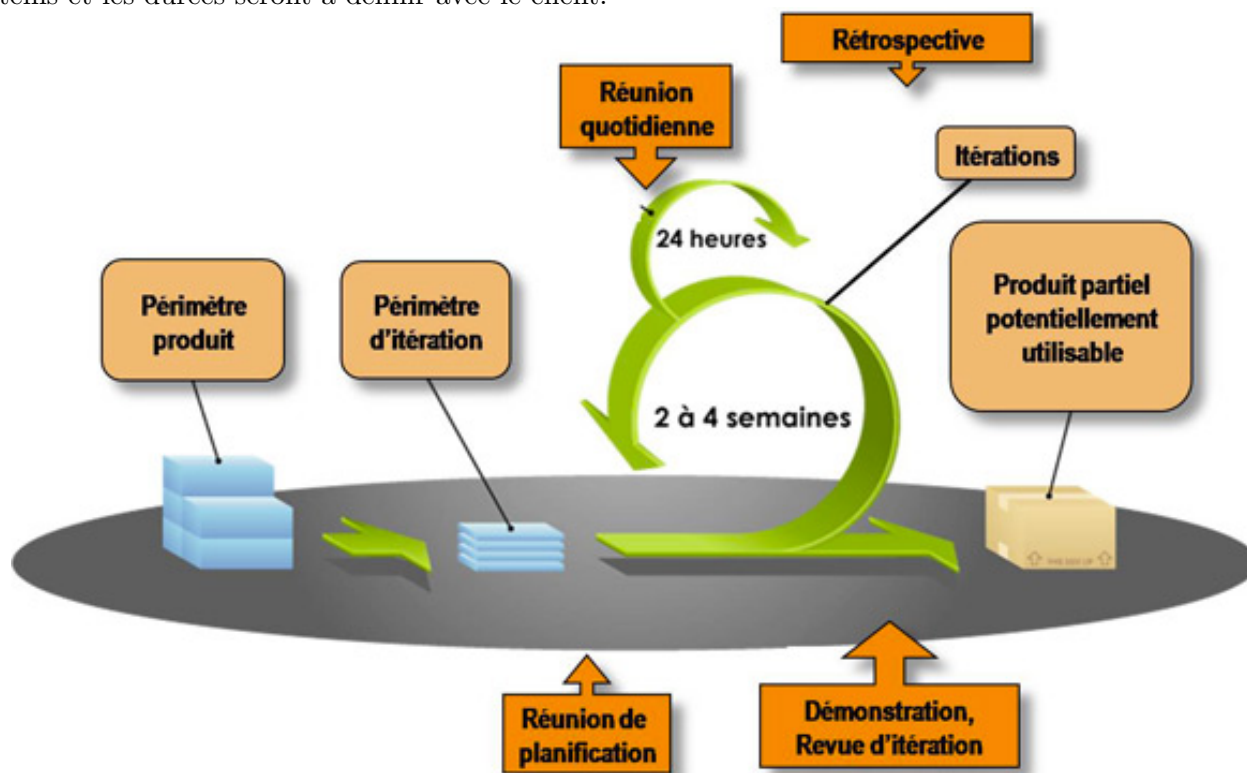
Pour ce projet, la méthode de développement utilisée sera une méthode agile : Scrum.

2.1 Méthodes agiles

Les méthodes agiles sont des groupes de pratiques pouvant s'appliquer à divers types de projets, mais se limitant plutôt actuellement aux projets de développement en informatique, plus particulièrement en conception de logiciel. Les méthodes agiles se veulent plus pragmatiques que les méthodes traditionnelles. Elles impliquent au maximum le demandeur (client) et permettent une grande réactivité à ses demandes. Elles visent la satisfaction réelle du besoin du client et non les termes d'un contrat de développement.

2.2 Méthode Scrum

Scrum est une méthode agile dont l'organisation de l'équipe est autogérée et est protégée par un Scrum Master qui fait partie de l'équipe. Les livraisons seront découpées en sprints dont les listes d'items et les durées seront à définir avec le client.



Sources : http://fr.wikipedia.org/wiki/Méthode_agile et [http://fr.wikipedia.org/wiki/Scrum_\(méthode\)](http://fr.wikipedia.org/wiki/Scrum_(méthode))

2.3 Pourquoi ?

Les méthodes agiles ont fait leur preuve dans leur efficacité et leur qualité de développement. De plus, Scrum permet un suivi et une transparence totale avec le client. Le découpage en sprint, itération assez courte, est adapté à notre projet puisqu'il se déroule sur une période relativement courte.

3 Les livrables

- Spécifications techniques des besoins
- Analyse des risques
- Cahier de recettes
- Document d'architecture logicielle
- Plan de développement détaillé
- Politique de certification
- Déclaration des pratiques de certification

4 Organisation

Rôles	Qui ?
Scrum Master / Chef de projet	Julien Legras
Représentant client	Jean-Baptiste Souchal
Architecte	Yves Nouafo
Testeur	Charles Ango

5 Dimensionnement

5.1 Stratégie

Le développement de ce projet sera découpé en trois itérations (sprints). Chaque sprint durera quatre semaines avec une livraison le dernier jour du sprint. Pour chaque sprint sont prévues une période de correction de problèmes du sprint précédent ainsi qu'une période de tests.

Sprint 1 Ce sprint consiste en le développement de :

- Serveur simple : la gestion des connexions à la base de données, des salons et la transmission de messages aux destinataires.
- Client simple : la connexion et la déconnexion au serveur, l'envoi et la réception d'un message au serveur et l'interfaçage.

Sprint 2 Ce sprint consiste en le développement de :

- PKI : la certification de clef RSA, la vérification, l'envoi, la révocation et le stockage des certificats.
- Client : demande et réception de certificat.
- Cérémonie des clefs pour générer la clef privée de la PKI.

Sprint 3 Ce sprint consiste en le développement de :

- Serveur sécurisé : la gestion des salons privés, des clefs symétriques, l'authentification lors de la connexion et l'enregistrement d'un nouvel utilisateur.
- Client sécurisé : la gestion des clefs, le chiffrement/déchiffrement, la vérification de l'intégrité et de l'authenticité des messages, la création/suppression/administration de salons privés.

5.2 Description des tâches

Pour minimiser le risque de perte de sources, nous avons mis en place un dépôt git avant le début de la phase de développement (<http://github.com/legrajul/bavardage>). De plus, les phases d'apprentissage de nouvelles connaissances techniques sont incluses dans les tâches concernées.

		Tâche	Description	Dépendances
Sprint 1	Serveur	1	Gestion des connexions/déconnexions et BDD	
		2	Salon d'accueil	1, 6
		3	Création/suppression/gestion des salons publics	1,6
		4	Transmission des messages aux destinataires	2
		5	Envoi de messages privés non sécurisés	1, 6
	Client	6	Connexion/déconnexion à un serveur avec pseudo	
		7	Envoi/réception d'un message public/privé	2
		8	Envoi de demande de création de salon au serveur	1, 6
		9	Rejoindre/quitter un salon	3, 8
		10.1	Interface Gtk	
		10.2	Interfaçage de la bibliothèque C en VAPI	10.1
Sprint 2	Client	1.1	Demande de certificat à la PKI	
		1.2	Réception du certificat envoyé par la PKI	1.1, 4
	PKI	2	Certification de clef RSA (AC) pseudo	1.1, 3
		3	Vérification des règles (RA)	
		4	Envoi des certificats (AC)	2
		5	Stockage des certificats (AC)	2
		6	Permettre l'accès en lecture aux certificats (AC)	5
		7	Suppression d'un utilisateur	5
Sprint 3	Serveur S	1	Gestion des salons privés	3, 4
		2	Gestion des clefs de chiffrement symétrique	1, 6
		3	Authentification lors de la connexion	
		4	Enregistrement nouvel utilisateur	
	Client S	5	Chiffrement/déchiffrement des messages et gestion des clefs	2, 8
		6	Demande de suppression de compte	3, 4
		7	Création/suppression/administration de salon privé	3, 4
		8	Rejoindre/quitter un salon privé	1, 7

5.3 Évaluation des charges et répartition des tâches

Tâche	Complexité	Charge	Effectif	Délai	Qui ?	Début	Fin
Sprint 1	1	4	8	2	4	Ismael – Yves	21/01/2013
	2	2	6	2	3	Yves – Jean-Baptiste	25/01/2013
	3	3	6	2	3	Ismael – Julien	26/01/2013
	4	3	3	1	3	Jean-Baptiste	30/01/2013
	5	2	3	1	3	Charles	31/01/2013
	6	2	3	1	3	Jean-Baptiste	21/01/2013
	7	2	3	1	3	Yves	30/01/2013
	8	2	3	1	3	Charles	26/01/2013
	9	2	3	1	3	Ismael	31/01/2013
	10.1	6	10	2	5	Julien – Charles	21/01/2013
10.2	4	8	2	4	4	Julien	04/02/2013
Sprint 2	1.1	2	8	2	4	Ismael – Yves	18/02/2013
	1.2	2	3	1	3	Ismael	04/03/2013
	2	3	6	2	3	Charles – Ismael	22/02/2013
	3	3	8	2	4	Jean-Baptiste – Julien	18/02/2013
	4	3	6	2	3	Charles – Julien	27/02/2013
	5	3	6	2	3	Jean-Baptiste – Yves	27/02/2013
	6	3	6	2	3	Charles – Julien	04/03/2013
	7	2	6	2	3	Jean-Baptiste – Yves	04/03/2013
	1	4	8	2	4	Julien – Jean-Baptiste	22/03/2013
	2	4	6	2	3	Ismael – Yves	27/03/2013
Sprint 3	3	4	8	2	4	Jean-Baptiste – Charles	18/03/2013
	4	4	8	2	4	Ismael – Julien	18/03/2013
	5	2	8	2	4	Jean-Baptiste – Julien	01/04/2013
	6	4	3	1	3	Yves	22/03/2013
	7	2	4	2	2	Charles – Ismael	22/03/2013
	8	4	4	2	2	Charles – Julien	28/03/2013

Sprint 1 : Serveur et client de chat													
21/01	22/01	23/01	24/01	25/01	26/01	27/01	28/01	29/01	30/01	31/01	01/02	02/02	03/02

Sprint 2 : Certificats													
18/02	19/02	20/02	21/02	22/02	23/02	24/02	25/02	26/02	27/02	28/02	01/03	02/03	03/03

Sprint 3 : Serveur et client de chat sécurisés													
18/03	19/03	20/03	21/03	22/03	23/03	24/03	25/03	26/03	27/03	28/03	29/03	30/03	31/03
Apprentissage SSL													
3 (CA, IK)													
4 (YN, JBS)													
Configuration serveur EJBCA (JL)													
01/04	02/04	03/04	04/04	05/04	06/04	07/04	08/04	09/04	10/04	11/04	12/04	13/04	14/04
3 (CA, IK)													
4 (YN, JBS)													
Configuration serveur EJBCA (JL)													
Apprentissage EVP													
9 (JL)													
15/04	16/04	17/04	18/04	19/04	20/04	21/04	22/04	23/04	24/04	25/04	26/04	27/04	28/04
5 (CA)													
1 (JL, JBS)													
7 (C, I)													
2 (IK, YN)													
29/04	30/04	01/05	02/05	03/05	04/05	05/05							
7 (C, I)													
8 (C, J)													
6 (YN, JBS)													
Tests													

6 Suivi

6.1 Gestion électronique des documents

Pour partager les documents, un dépôt git a été mis en place sur Github à l'adresse :
<https://github.com/legrajul/bavardage-doc>

6.2 Réunions

6.2.1 Réunions avec le client

Réunion n°1 – 07/11/2012 Première présentation du projet par le client.

Réunion n°2 – 14/11/2012 Différentes questions ont été posées pour pouvoir réaliser la STB :

1. Lors de la connexion, l'utilisateur se retrouve-t-il dans un salon d'accueil ?
↔ Oui, les messages échangés sur ce salon ne seront pas chiffrés.
2. Il y a-t-il des salons publics ?
↔ Oui, comme pour le salon d'accueil, les messages échangés sur ce salon ne seront pas chiffrés.
↔ Pas besoin de s'enregistrer pour y accéder et y bavarder.
3. Que se passe-t-il lorsque le créateur d'un salon se déconnecte ?
↔ Fermeture du salon avec avertissement.
4. Qui crée un compte sécurisé ?
↔ L'autorité de certification, elle est automatique et applique une politique de certification.
5. Quelles sont les attentes au niveau de l'interface graphique ?
↔ Elle doit rester simple et il doit également être possible d'utiliser le logiciel en lignes de commandes.
6. Quelles sont les qualités attendues ?
 - le niveau de crypto ne doit pas impacter les performances ;
 - l'ajout et la suppression d'un utilisateur doit être rapide pour ne pas perdre de message.
7. Quelles sont les exigences opérationnelles ?
 - création d'un salon privé (avec la liste des personnes autorisées à s'y connecter) ;
 - ajout et suppression d'une nouvelle personne dans un groupe privé ;
 - diffusion des clefs de chiffrement ;
 - communication multi-salons.
8. Quelles sont les exigences de réalisation ?
 - documentation rédigée en \LaTeX ;
 - utilisation d'OpenSSL ;
 - utilisation de tinyca pour créer l'autorité de certification.
9. Quelles sont les exigences au de l'interface de communication ?
↔ Le serveur sécurisé doit pouvoir s'adapter à d'autres protocoles, il doit être indépendant du serveur de bavardage.
10. Autorité de certification

↪ fournit des certificats = une clef publique + identité + date d'expiration + ...

11. Politique de certification

↪ Qui ?

↪ Comment se fait la vérification d'identité ?

↪ Comment se fait la révocation ?

↪ ...

Réunion n°3 – 21/11/2012 Précisions apportées sur des cas d'utilisation :

- Lorsqu'un utilisateur est invité, il y a changement de clef seulement quand il rejoint le salon.
- Paramétrage de compte sécurisé pour choisir s'il peut envoyer/recevoir des messages privés non sécurisés avec un utilisateur non authentifié.
- Comment effectuer une demande de certificat ?
 - ↪ page d'administration accessible par une ou plusieurs personnes pour valider le certificat ;
 - ↪ il faut que l'utilisateur génère sa propre paire de clefs publique/privée puis l'AC certifie cette paire de clefs.
- La révocation d'un certificat est assurée par l'AC et est demandée soit par un administrateur de salon, soit pas le propriétaire du certificat.

Présentation d'une politique de certification (avec la PKI).

Réunion n°4 – 05/12/2012 Réunion après premier retour du client sur la STB

Réunion n°5 – 12/12/2012 Réunion après deuxième retour du client sur la STB et présentation des schémas du DAL.

Réunion n°6 – 19/12/2012 Présentation du DAL version électronique et du CdR. Présentation de EJBCA (Enterprise Java Bean Certificate Authority) par le client.

6.2.2 Réunions TD

TD n°1 – 09/11/2012 Première réunion avec le responsable de gestion de projet, présentation des différents documents à fournir et des différents rôles à attribuer.

TD n°2 – 16/11/2012 Deuxième TD de GDP avec à l'ordre du jour la rédaction de la STB avec l'aide du chargé de TD.

TD n°3 – 23/11/2012 Troisième TD de GDP avec à l'ordre du jour la rédaction du cahier de recette, du document d'architecture du logiciel et de l'analyse des risques avec l'aide du chargé de TD.

TD n°4 – 30/11/2012 Quatrième TD de GDP avec à l'ordre du jour la présentation au chargé de TD du cahier de recette, du document d'architecture du logiciel et de l'analyse des risques qui ont été commencés et présentation du document de planning de développement par le chargé de TD.

TD n°5 – 07/12/2012 Cinquième TD de GDP avec à l'ordre du jour la présentation au chargé de TD de l'avancement des documents et présentation de la méthode pour faire un plan de développement par le chargé de TD.

6.2.3 Réunions de groupe

Il y a eu plusieurs points rapides faits tout au long de l'élaboration des documents mais leur courte durée ne permet pas de les qualifier de réunions.

07/11/2012 Débriefing après la première réunion avec le client.

26/11/2012 Présentation de l'outil Git par Julien Legras.

12/12/2012 Évaluation des charges des tâches.

17/12/2012 Élaboration des diagrammes de Gantt et répartition des tâches.

6.2.4 Réunions pendant le développement

Une réunion avec le client sera faite quelques jours avant la livraison pour lui montrer ce qui sera livré ainsi qu'une autre quelques jours après la livraison pour le client puisse faire un retour sur les éventuels bugs et/ou améliorations à apporter.

Sprint 1 – semaine 1 – 21/01/2013 L'ordre du jour de la réunion était : lancement du projet, coordination des tâches par rapport au plan de développement.

Selon le plan de développement établi lors des séances de travaux pratiques de gestion de projet, le projet de chat sécurisé devait être lancé le 21 Janvier 2013. Les tâches de la semaine : 1, 6, 10.1

Sprint 1 – semaine 2 – 28/01/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement.

Les tâches de la semaine : 2, 3, 4, 5, 7, 8, 9

Sprint 1 – semaine 3 – 04/02/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement

Les tâches de la semaine : 4, 5, 7, 9, 10.2

Sprint 1 – semaine 4 – 11/02/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement

Les tâches de la semaine : tests

Sprint 2 – semaine 1 – 18/02/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement

Les tâches de la semaine : 1.1, 2, 3

Sprint 2 – semaine 2 – 25/02/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement

Les tâches de la semaine : 2, 4, 5

Sprint 2 – semaine 3 – 04/03/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement

Les tâches de la semaine : 1.2, 6, 7

Sprint 2 – semaine 4 – 11/03/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement.

Les tâches de la semaine : tests

Sprint 3 – semaine 1 – 18/03/2013 L'ordre du jour de la réunion était : préparation aux tâches du plan de développement.

Les tâches de la semaine : apprentissage d'OpenSSL (connexions sécurisées SSL).

Sprint 3 – semaine 2 – 25/03/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement.

Les tâches de la semaine : 3, 4, configuration serveur mis à disposition par la fac pour EJBCA.

Sprint 3 – semaine 3 – 01/04/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement.

Les tâches de la semaine : 3, 4

Sprint 3 – semaine 4 – 08/04/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement.

Les tâches de la semaine : interface partie sécurisée, apprentissage d'OpenSSL (chiffrement symétrique)

Sprint 3 – semaine 5 – 23/04/2013 L'ordre du jour de la réunion était : coordination des tâches par rapport au plan de développement.

Les tâches de la semaine : 1, 2, 5, 7, 8