Projet annuel - Chat sécurisé

Charles Ango - Ismaël Kabore - Julien Legras - Yves Nouafo - Jean-Baptiste Souchal

Master 1 Sécurité des Systèmes Informatiques

18/01/2013

Sommaire

Présentation du projet

Sujet proposé par Magali Bardet

Réaliser un logiciel de messagerie instantanée **sécurisée** : client et serveur.
S'inspirer des fonctionnalités d'IRC (Internet Relay Chat).
Fonctionnalités demandées :

- gestion de la création et la suppression d'un compte sécurisé ;
- création par un utilisateur d'une salle de discussion pour un groupe de personnes ;
- ajout/suppression d'un utilisateur autorisé dans une salle ;
- assurance de confidentialité, d'intégrité et d'authentification sur les messages échangés ;
- non-répudiation des messages.

Diagramme de cas d'utilisation I

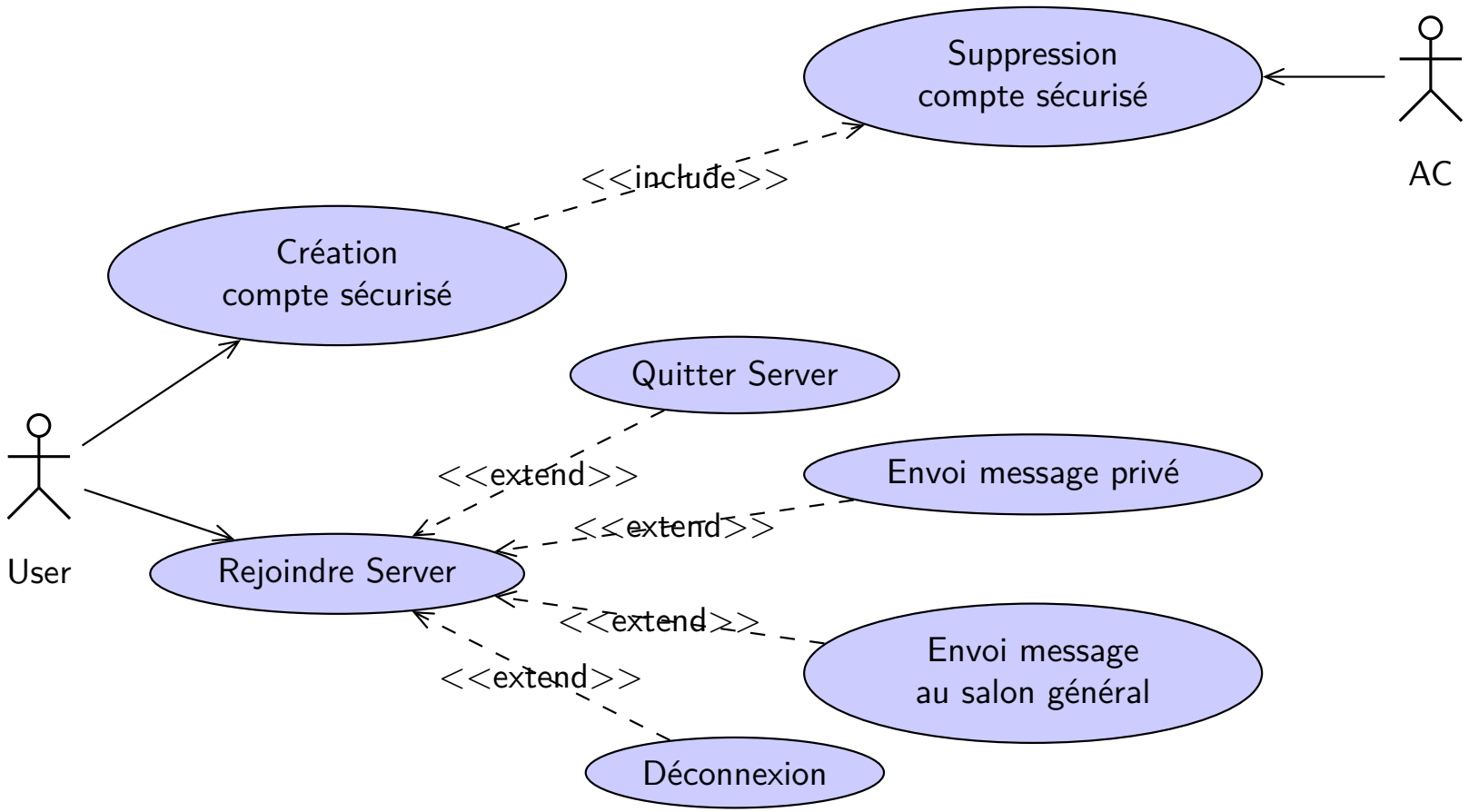


Diagramme de cas d'utilisation II

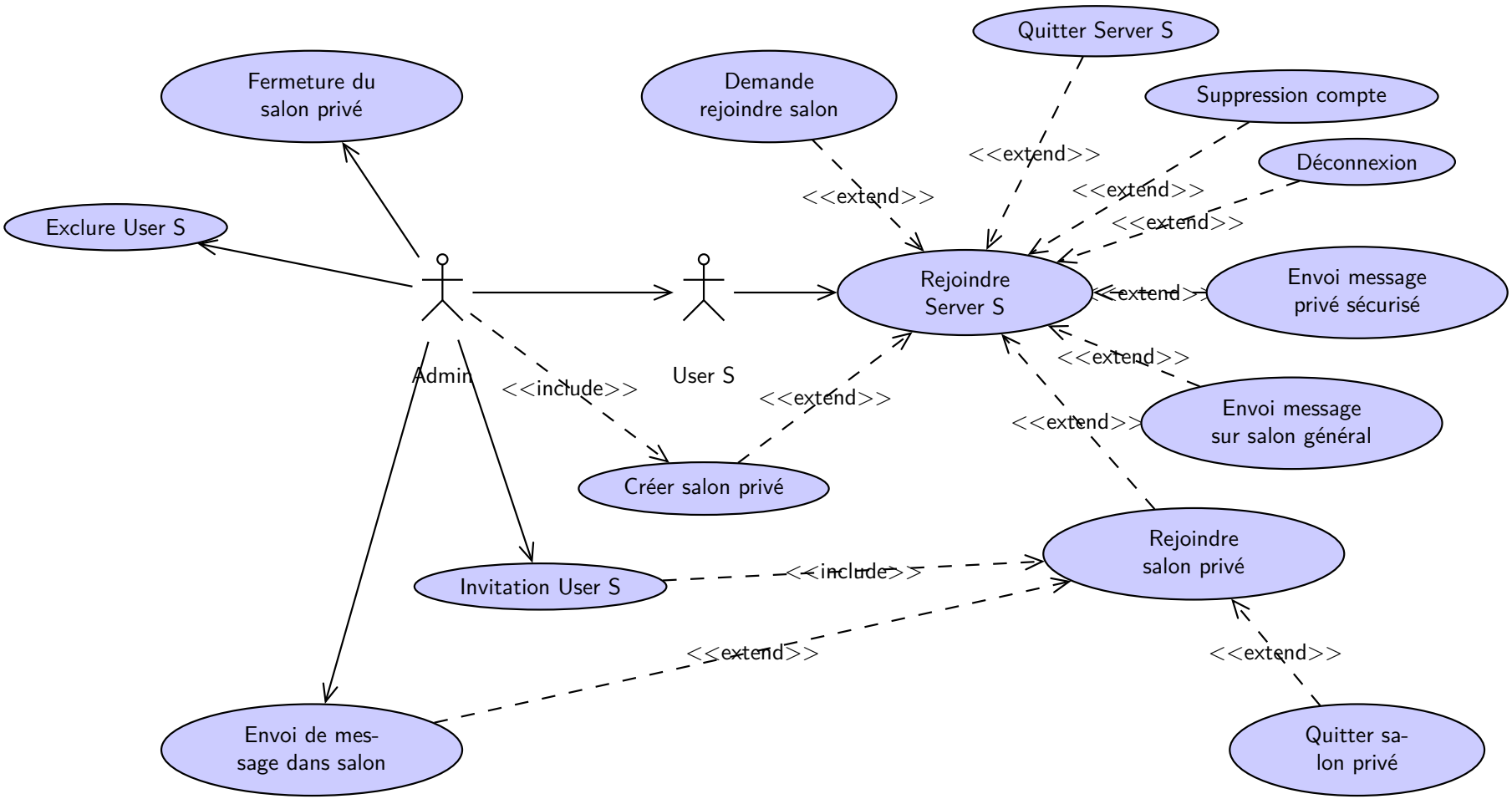
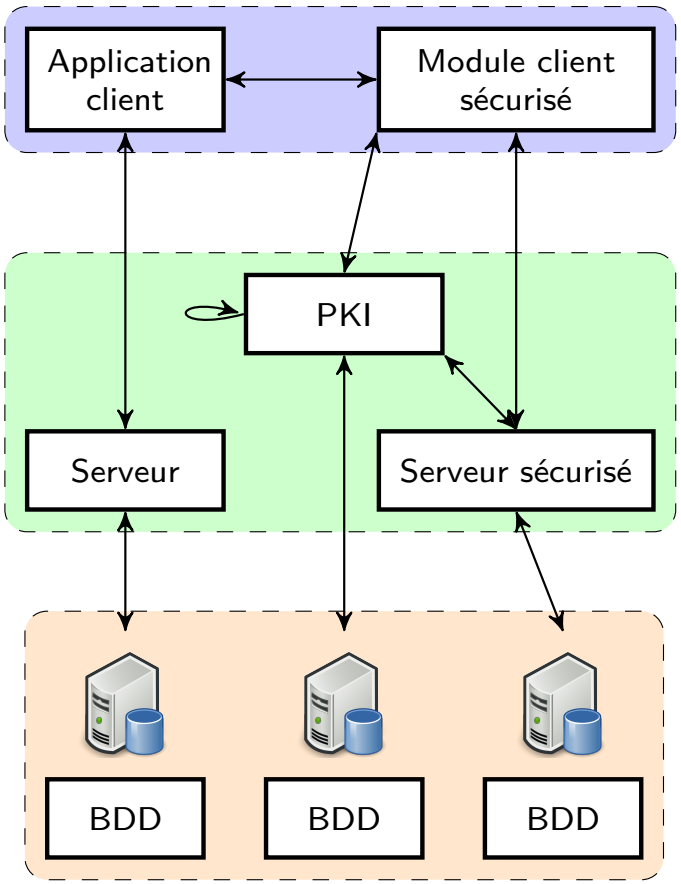


Schéma global et entités



API client :

- sécurisé
- non-sécurisé

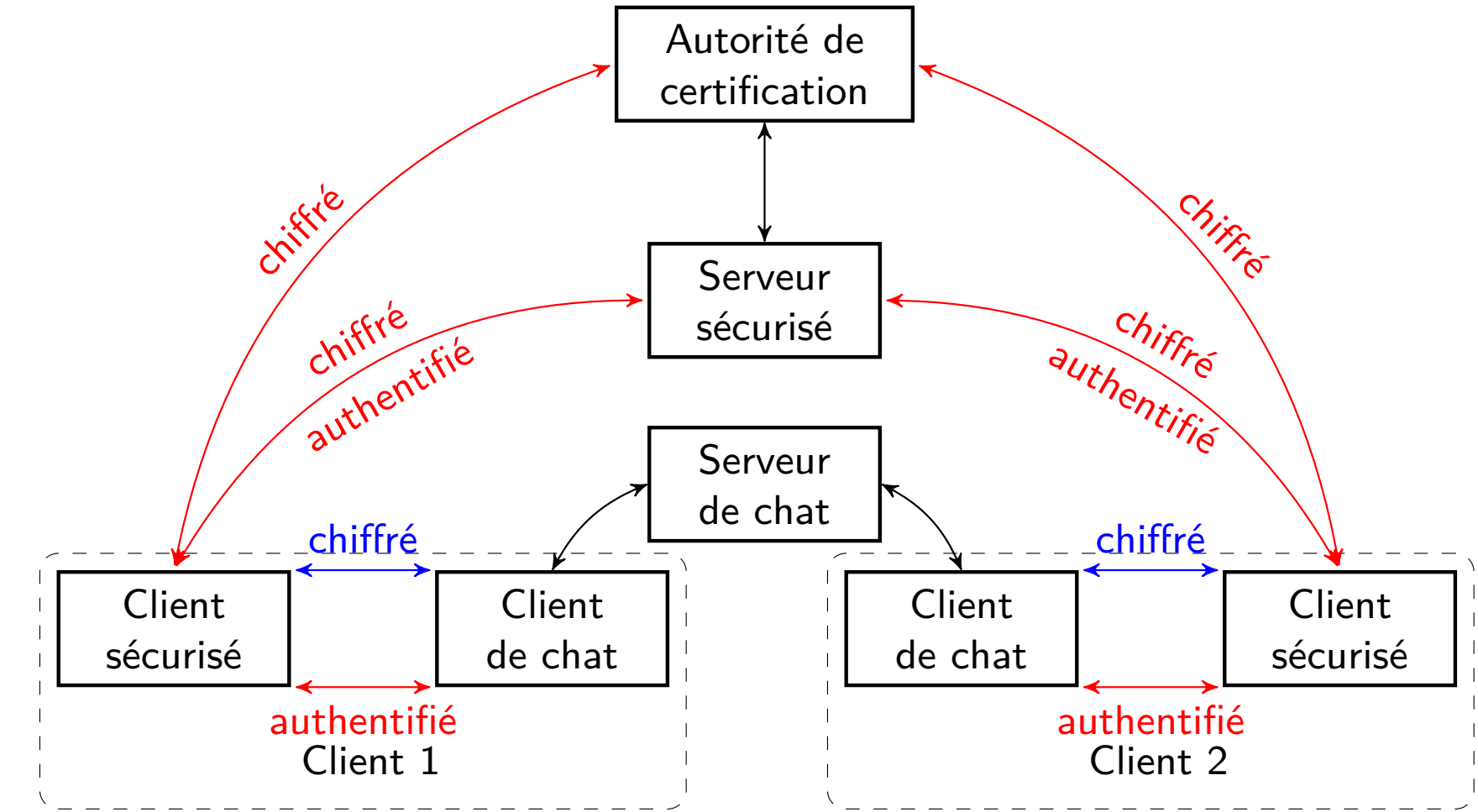
Serveurs :

- sécurisé
- non-sécurisé
- PKI

Données :

- BDD serveur sécurisé
- BDD serveur non-sécurisé
- liste certifications/ révocations

Fonctionnement



Légende : ↔ symétrique ↔ asymétrique

Détails techniques

Langages et bibliothèques

- C → client et serveur
- Vala → interface du client
- GTK+ → interface du client

Sécurité

- OpenSSL → bibliothèque de fonctions cryptographiques
- TinyCA vs EJBCA → EJBCA

Équipe et répartition

Équipe

- Chef de projet : Julien
- Responsable client : Jean-Baptiste
- Testeur : Charles
- Architecte : Yves
- Chargé de certification : Ismaël

Équipe et répartition

Équipe

- Chef de projet : Julien
- Responsable client : Jean-Baptiste
- Testeur : Charles
- Architecte : Yves
- Chargé de certification : Ismaël

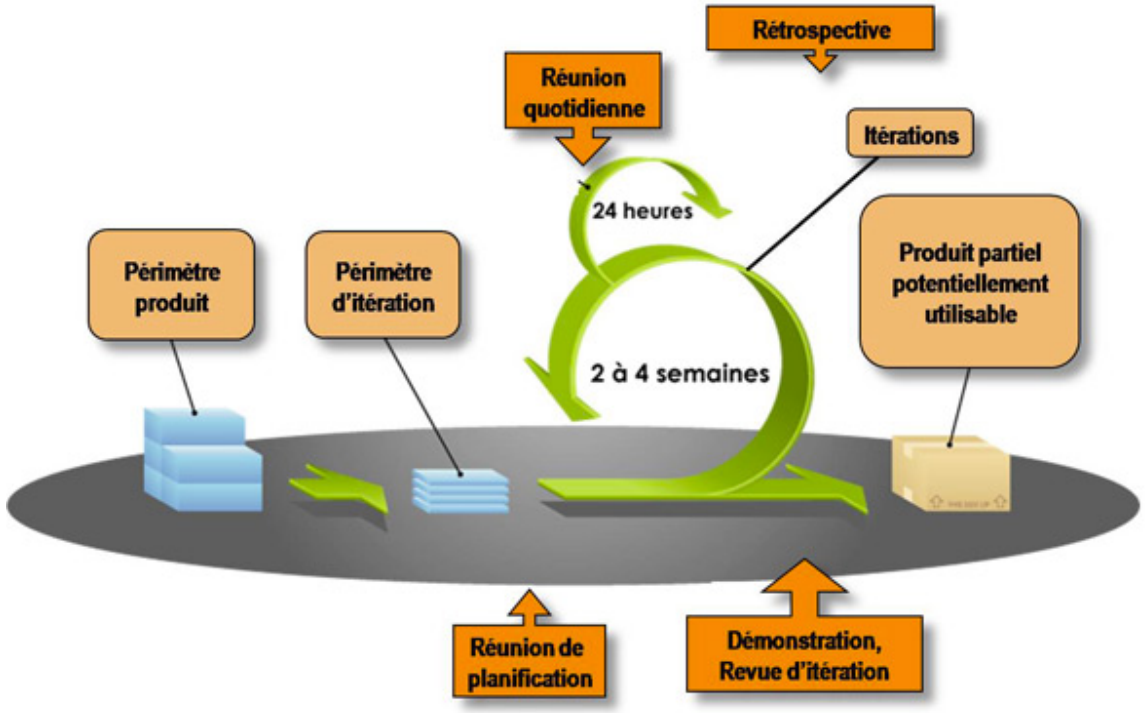
Répartition

- Responsable tâches partie certification → Ismaël
- Responsable tâches partie interface → Julien

Stratégie I

Scrum :

- méthode agile
- découpage en sprints
- chaque sprint est basé sur une fonctionnalité
- fin de sprint → livraison d'un produit partiel fonctionnel



Stratégie II

Participation active du client :

- sur les fonctionnalités de chaque sprint
- le test du livrable à chaque fin de sprint

Adapté a notre projet :

- chaque fonctionnalité est relativement courte
- 3 fonctionnalités principales :
  - Client / Serveur (publics)
  - PKI
  - Client / Serveur (sécurisés)

Planning de développement I

Sprint 1 : Implémentation du client et du serveur simples

- 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.

Planning de développement II

Sprint 2 : Implémentation de la PKI et des échanges entre le client et la PKI

- 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.

Planning de développement III

Sprint 3 : Implémentation du client et du serveur sécurisés

- 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.

Risques

Réf.	Description	Facteurs	Type	Probabilité	Impact	Criticité
R1	Apprentissage long d'OpenSSL, Vala et GTK pouvant entraîner un retard	aucun n'a déjà utilisé OpenSSL, un seul Vala/GTK	Tech	FAIBLE	MAJEUR	10
R2	Charge supplémentaire pouvant entraîner un retard	maladie, emploi du temps chargé	Env	MAJEUR	MINEUR	12
R3	Perte de sources	disque défectueux, machine en panne, vol	Env	FAIBLE	CRITIQUE	12
R4	Client non-impliqué	emploi du temps chargé	RH	FAIBLE	MINEUR	8

Réf.	Action
R1	Tutoriels pour OpenSSL, transmission de connaissances et tutoriels pour Vala/GTK
R2	Répartir la charge ou étaler une tâche.
R3	Perte de sources minimisée grâce à git.

Difficultés rencontrées

⇝ Difficultés pour intégrer la cryptographie dans :

- les cas d'utilisation
- les cas de tests

Conclusion

Application d'une méthode de préparation de projet avec :

- analyse du sujet
- distribution des rôles
- élaboration de documents techniques
- élaboration du planning des tâches