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

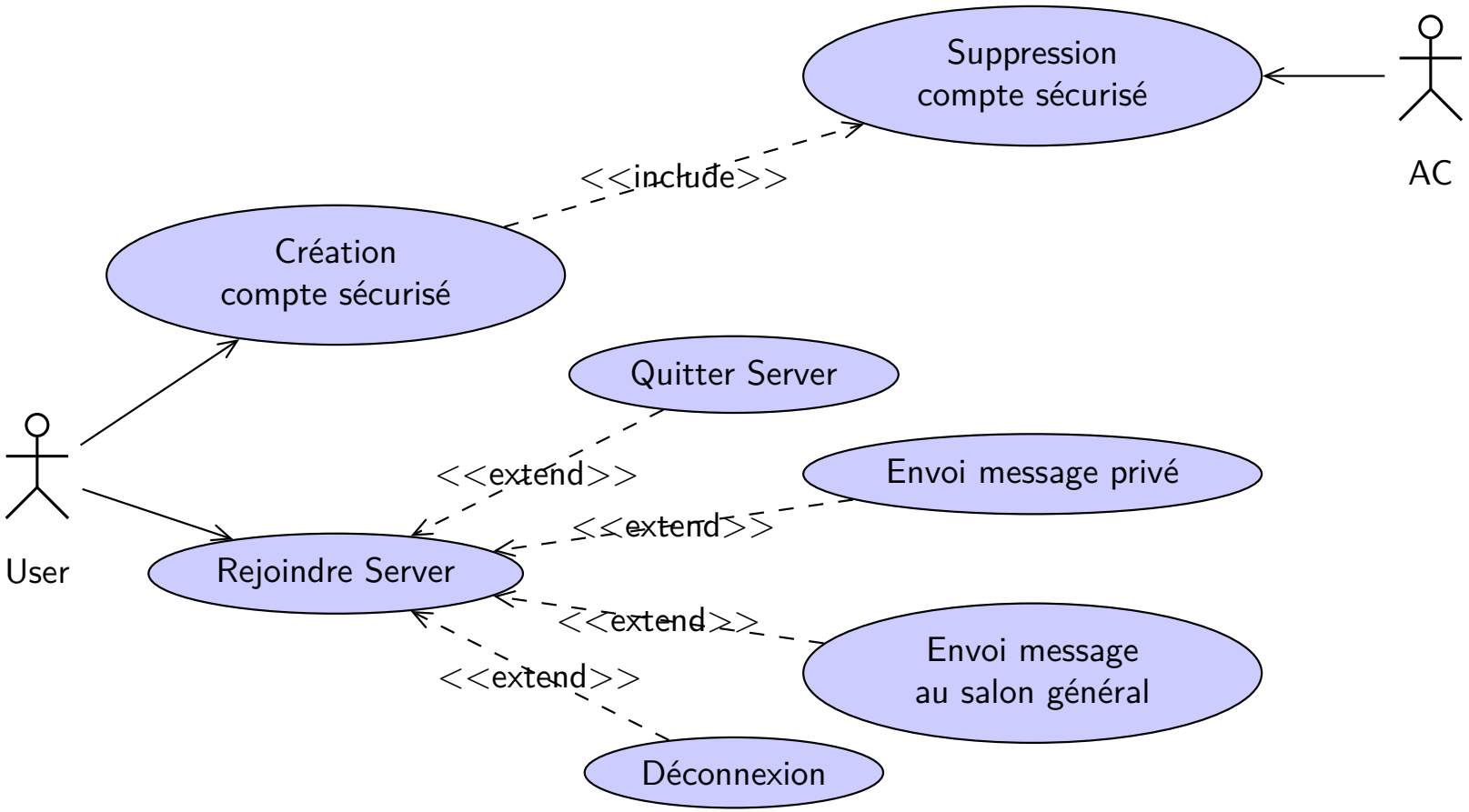
Présentation du projet

Sujet proposé par Maglie 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 confidentialités, d'intégrité et d'authentification sur les messages échangés ;
- non-répudiation des messages.

Digramme de cas d'utilisation I



Digramme de cas d'utilisation II

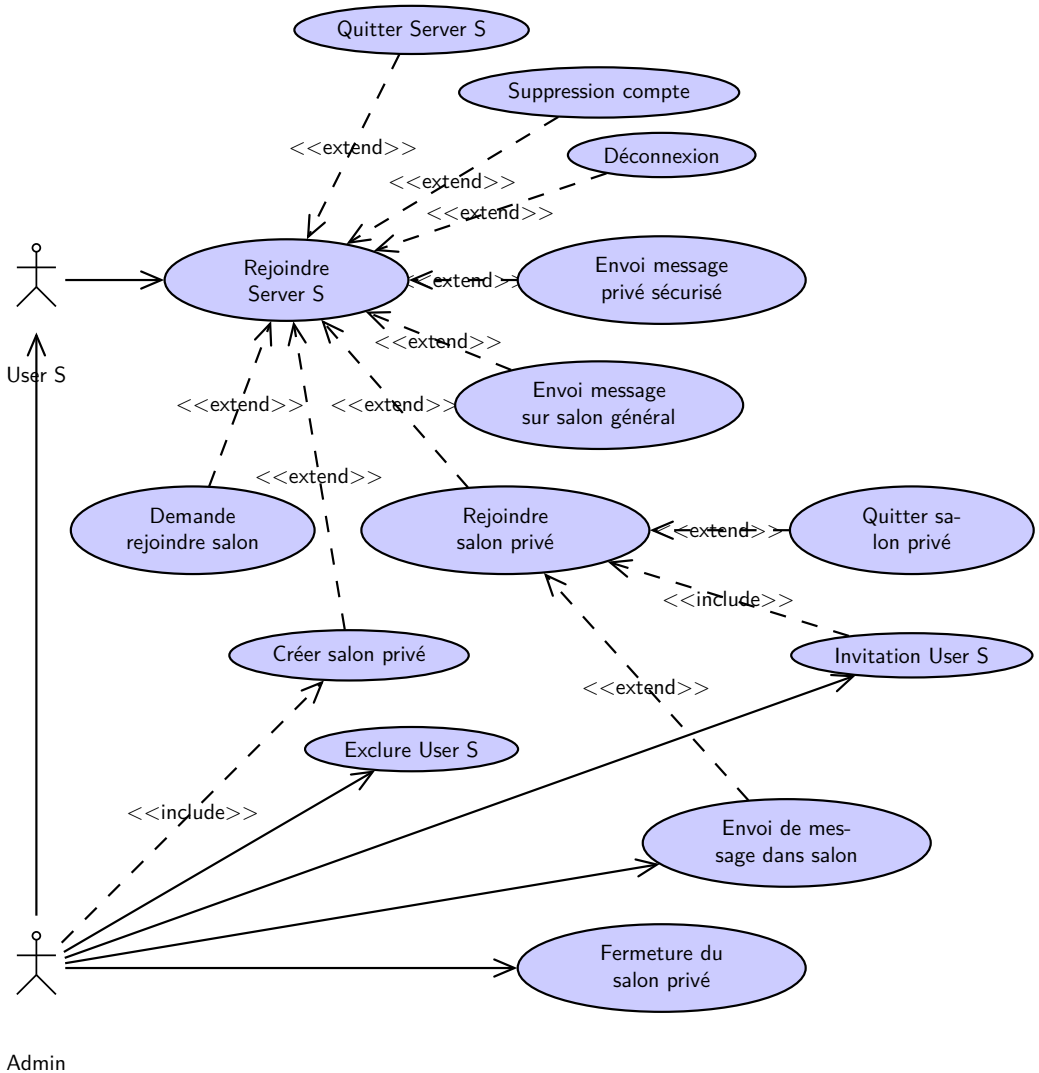
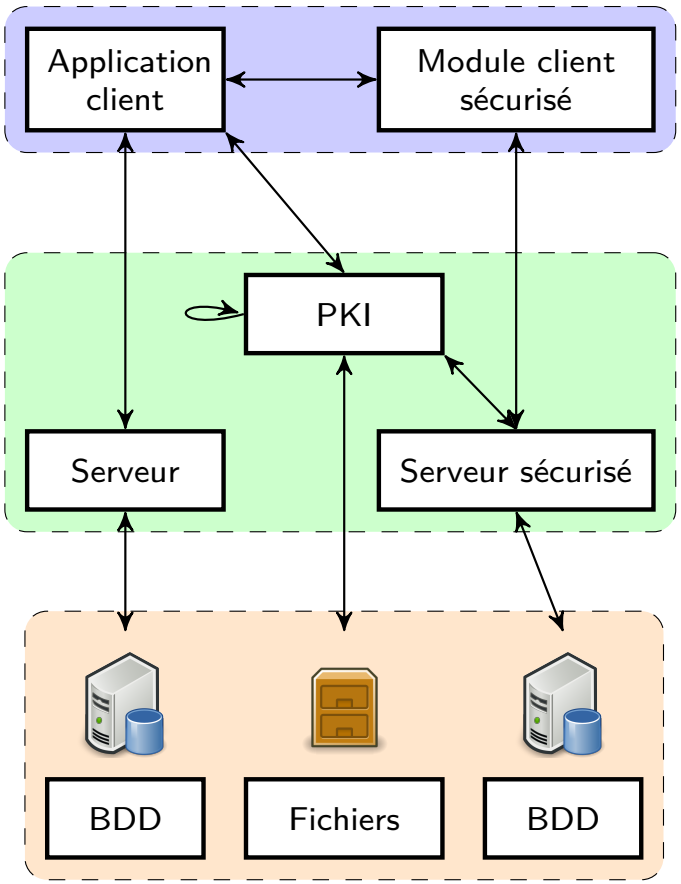


Schéma global et entités



API client :

- sécurisé
- non-sécurisé

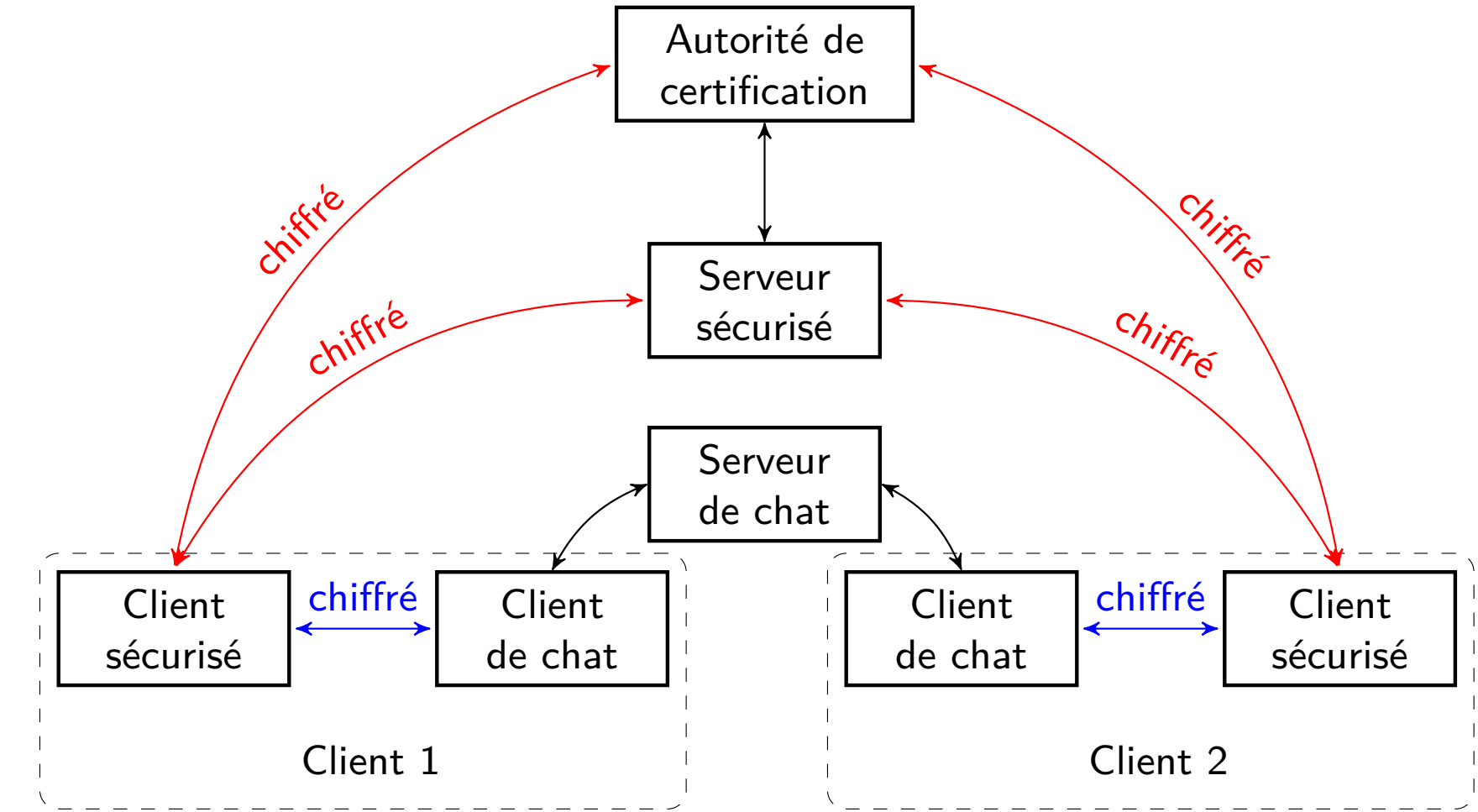
Serveurs :

- sécurisé
- non-sécurisé
- PKI

Données :

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

Fonctionnement



Légende : ↔ symétrique ↔ asymétrique

Détails techniques

Langages et bibliothèques

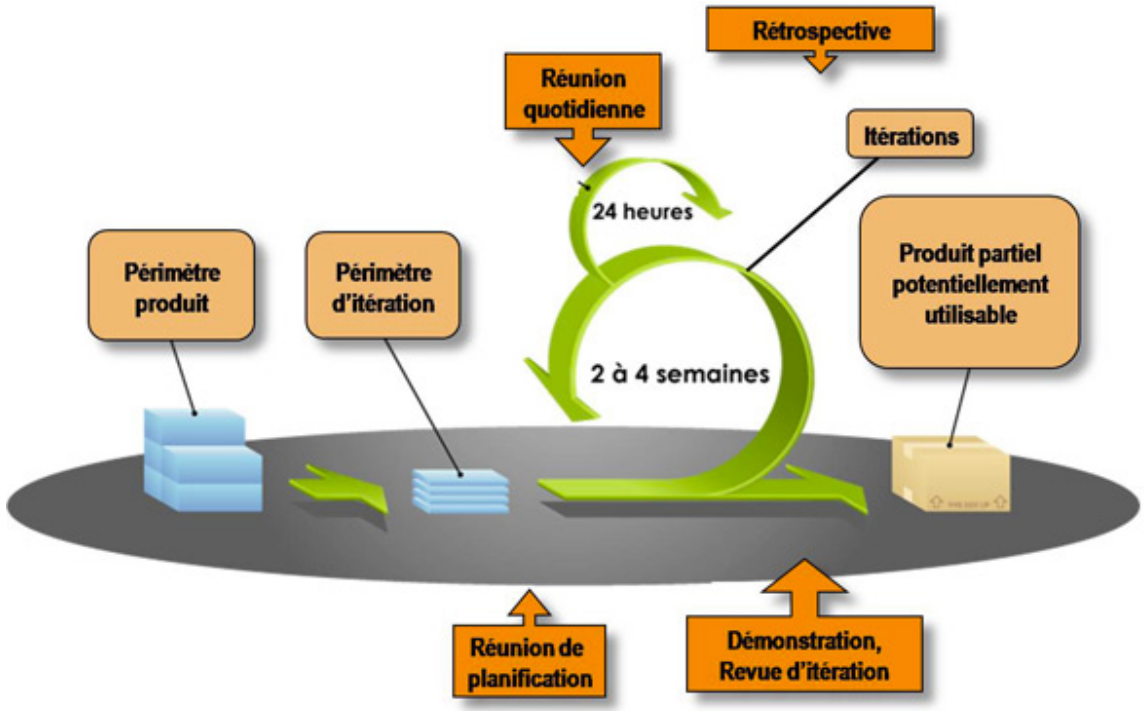
- C → client et serveur
- Vala → interface du client
- GTK+ 3 → interface du client

Sécurité

- OpenSSL → implémentation Open Source de SSL et TLS
- TinyCA vs EJBCA → EJBCA

Organisation I

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



Organisation II

Participation active du client :

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

Trois piliers :

- transparence
- inspection
- adaptation

Organisation III

Les acteurs :

- client
- scrum master
- développeurs

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 et le stockage des certificats.
- Client : demande et de réception de certificat.

Planning de développement III

Sprint 3 : Implémentation du client et du serveur sécurisés

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

Risques

Réf.	Description	Facteurs	Type	Probabilité	Impact	Criticité
R1	Utilisation de Git	Une seule personne sait l'utiliser	Tech	FORT	MAJEUR	20
R2	Apprentissage de Gtk, Vala	3 ont déjà fait du Vala, 1 du Gtk	Tech	MAJEUR	MAJEUR	15
R3	Apprentissage d'OpenSSL	Personne n'a déjà utilisé OpenSSL	Tech	FORT	MAJEUR	20
R4	Membre de l'équipe gravement malade	Environnement	RH	FAIBLE	MAJEUR	10
R5	Vol/Incident matériel		RH	FAIBLE	CRITIQUE	12
R6	Utilisation d'une PKI (tinyca/EJBCA)	Faibles connaissances des PKI	Tech	MAJEUR	MAJEUR	15
R7	Retard dans la livraison	Retard du développement d'une tâche bloquante	RH/Tech	MAJEUR	MAJEUR	15