Spécification technique des besoins

Version	0.7
Date	03 janvier 2013
Rédigé par	Jean-Baptiste Souchal
Relu par	Julien Legras
Approuvé par	

MISES À JOUR

Version	Date	Modifications réalisées
0.1	09/11/2011	Création
0.2	23/11/12	Rédaction des cas d'utilisation
0.3	28/11/12	Modifications après retour client
0.4	09/12/12	Ajout UC 17–18–19 et des règles de gestion
0.5	14/12/12	Modifications après réunion du 12/12/12
0.6	29/12/12	Modifications après réunion du 19/12/12
0.7	03/01/13	Modifications après retour client

Table des matières

1 Objet

Développement d'un système permettant à plusieurs utilisateurs de s'authentifier et de communiquer de manière sécurisée :

- gestion de la création et de la suppression d'un compte utilisateur ;
- création par un utilisateur d'une salle de discussion privée ;
- ajout et suppression d'un utilisateur autorisé dans une salle privée
- confidentialité, intégrité et authentification sur les messages échangés ;
- non répudiation des messages ;
- création d'une autorité de certification ;
- demande de certificat pour l'accès à un salon privé et la communication sécurisée.

2 Documents applicables et de référence

- IRC (RFC 2810 à 2813 d'avril 2000)

3 Terminologie et sigles utilisés

- **IRC (Internet Relay Chat)** ;
- **RFC (Request For Comments)** ;
- **Autorité de Certification (AC)** : gère la délivrance des certificats et des clés publique/privée (EO.4) ;
- **Autorité d'enregistrement (AR)** : Organisme qui génère les certificats et effectue les vérifications d'usage sur les utilisateurs ;
- **Serveur de chat (Server)** : serveur accueillant des utilisateurs ;
- **Serveur de chat sécurisé (Server S.)** : serveur accueillant des utilisateurs sécurisés (EO.5, EO.6, EO.7) ;
- **Client de chat (Client)** : le client de chat permet l'envoi et l'affichage des messages entre utilisateurs (EO.2).
- **Client sécurisé (Client S)** : a pour mission de chiffrer et déchiffrer les messages (EO.1, EO.2, EO.3, EO.5, EO.6).
- **Salon privé (Salon P.)** : salle de chat privée à l'intérieur du serveur de chat permettant à des utilisateurs sécurisés de communiquer ;
- **Utilisateur (User)** : personne étant connectée sur un serveur de chat ;
- **Utilisateur sécurisé (User S.)** : utilisateur ayant un certificat délivré par AC et des clés privée/publique permettant la création de salons privés et l'échange de messages sécurisés ;
- **Administrateur (Admin)** : utilisateur sécurisé ayant créé un salon privé et disposant des droits d'administration sur ce salon privé ;
- **Message privé (MP)** : un MP est un message (sécurisé ou non) à destination d'un unique utilisateur (sécurisé ou non).

4 Exigences fonctionnelles

4.1 Présentation de la mission du produit logiciel

EF.1 : création d'un compte sécurisé ;
EF.2 : suppression compte sécurisé par l'utilisateur ;
EF.3 : suppression compte sécurisé par l'autorité de certification ;
EF.4 : ajout certificat à un utilisateur par l'autorité de certification ;
EF.5 : envoi de message sur salon général ;
EF.6 : envoi de message sur salon privé ;
EF.7 : rejoindre un serveur de chat sans authentification ;
EF.8 : rejoindre un serveur de chat sécurisé avec authentification ;
EF.9 : quitter un serveur de chat ;
EF.10 : quitter un serveur de chat sécurisé ;
EF.11 : quitter un salon privé ;
EF.12 : renouvellement des clefs des salons privés ;
EF.13 : déconnexion technique ;
EF.14 : créer un salon privé ;
EF.15 : rejoindre un salon privé ;
EF.16 : fermeture d'un salon privé ;
EF.17 : exclure utilisateur sécurisé d'un salon privé ;
EF.18 : invitation d'un utilisateur sécurisé dans un salon privé ;
EF.19 : envoi d'un MP non sécurisé ;
EF.20 : envoi d'un MP sécurisé ;
EF.21 : demande pour rejoindre un salon privé ;
EF.22 : un utilisateur génère ses propres clefs ;
EF.23 : mise en place d'une autorité de certification ;
EF.24 : authentification entre les différents acteurs du système entre chaque échange ;
EF.25 : certification du Server S. par AC ;
EF.26 : établir une clef de session entre un utilisateur et un serveur pour l'authentification mutuelle lors des échanges.

Id	Intitulé	Acteur(s)
UC.1	Création d'un compte utilisateur sécurisé	User / AC / AR / Server S
UC.2	Suppression d'un compte sécurisé par utilisateur sécurisé	User S / Server S / AC
UC.3	Révocation d'un certificat par AC	AC
UC.4	Envoi de message sur salon général	User / User S / Client / Server
UC.5	Envoi de message sur salon privé	User S / Admin / Client S / Server S
UC.6	Rejoindre un serveur de chat sécurisé avec authentification	User S / Server S / Client S
UC.7	Rejoindre un serveur de chat sans authentification	User / Server / Client
UC.8	Quitter un serveur de chat	User / Server / Client
UC.9	Quitter un serveur de chat sécurisé	User S / Server S / Client S
UC.10	Quitter un salon privé	User S / Server S / Client S
UC.11	Déconnexion serveurs	User / User S / Server / Server S
UC.12	Créer un salon privé	User S / Server S / Client S
UC.13	Rejoindre un salon privé	User S / Server S / Admin / Client S
UC.14	Fermeture d'un salon privé	Admin / Server S / Client S
UC.15	Exclure utilisateur sécurisé d'un salon privé	Admin / Server S / Client S
UC.16	Invitation d'un utilisateur sécurisé dans un salon privé	Admin / Server / User S / Client S
UC.17	Envoi d'un message privé non sécurisé	User / User S / Client / Server
UC.18	Envoi d'un message privé sécurisé	User S / Client S / Server
UC.19	Demande d'ajout dans un salon privé	User S / Admin / Server S / Client S

RG.1 Le nom d'utilisateur doit être disponible et valide (`[A-Za-z0_9]+`)
RG.2 Le message clair doit respecter la taille maximale d'un message (512 caractères)
RG.3 Le nom du User S doit exister
RG.4 Le certificat du User S doit être valide
RG.5 Le nom du salon doit être disponible et valide (`[A-Za-z0_9]+`)

4.2 UC 1 : Création d'un compte Utilisateur sécurisé

Nom	**Création d'un compte Utilisateur sécurisé**
Acteurs concernés	User / AC / AR / Serveur S
Description	Un utilisateur fait la demande de création d'un compte utilisateur sécurisé auprès de AC
Préconditions	Avoir les prérequis pour obtenir le certificat, prérequis définis par AC
Evénements déclenchants	Envoi de la demande de création du compte sécurisé à AC
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. l'utilisateur génère ces clés 2. l'utilisateur remplit le formulaire de demande de création d'un compte utilisateur sécurisé 3. l'utilisateur envoie le formulaire à AC	4. AC traite la demande de création du compte sécurisé 5. envoi par l'AC du certificat à l'utilisateur

Flots d'exceptions	RG.1

4.3 UC 2 : Suppression d'un compte sécurisé par un Utilisateur

Nom	**Suppression d'un compte sécurisé par un Utilisateur**
Acteurs concernés	User S. / Server S. / AC
Description	Un utilisateur sécurisé supprime son compte du serveur de chat sécurisé
Préconditions	Avoir un compte utilisateur sécurisé sur le serveur de chat sécurisé
Evénements déclenchants	Suppression du compte utilisateur sécurisé dans le registre du serveur de chat sécurisé
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. l'utilisateur sécurisé fait la demande de suppression de son compte 5. l'utilisateur est déconnecté du serveur de chat sécurisé et du client de chat	2. le serveur de chat sécurisé supprime le compte utilisateur sécurisé de ses registres 3. le serveur de chat sécurisé arrête la connexion en cours de l'utilisateur sécurisé 4. suppression des certificats de l'utilisateur par AC
Flots d'exceptions	

4.4 UC 3 : Révocation d'un certificat par AC

Nom	**Révocation d'un certificat par AC**
Acteurs concernés	AC
Description	Suppression d'un compte par AC pour non respect du règlement ou inactivité d'un utilisateur sécurisé
Préconditions	Le compte utilisateur sécurisé ne respecte pas les règles de certification
Evénements déclenchants	Suppression du compte dans le registre du serveur de chat sécurisé
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
	1. AC révoque le certificat de l'utilisateur concerné.
Flots d'exceptions	

4.5 UC 4 : Envoi de message sur salon général

Nom	**Envoi de message sur salon général**
Acteurs concernés	User / User S. / Client / Server
Description	Un utilisateur (sécurisé) envoie un message sur le salon général du serveur de chat et le client affiche le message
Préconditions	Être connecté sur le serveur de chat
Evénements déclenchants	Le client envoie sur le salon général du serveur de chat le message et est lisible par tous les utilisateurs connectés sur ce serveur de chat
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. Un utilisateur envoie un message sur le salon général du serveur de chat	2. le Client envoie le message au Server 3. le serveur de chat reçoit et envoie le message au(x) Client(s) de chat des utilisateurs connectés sur le salon privé 4. le message s'affiche dans le(s) Client(s) de chat de(s) utilisateur(s)

Flots d'exceptions	RG.2

4.6 UC 5 : Envoi de message sur salon privé

Nom	**Envoi de message sur salon privé**	
Acteurs concernés	User S. / Admin / Server / Client S	
Description	Un utilisateur sécurisé envoie un message sur le salon privé	
Préconditions	L'utilisateur sécurisé est connecté sur le serveur de chat sécurisé et est dans le salon privé et être connecté sur le serveur de chat	
Evénements déclenchants	Un message est envoyé dans le salon privé et est lisible par tous les utilisateurs sécurisés connectés sur ce salon privé	
Conditions d'arrêt		
Description du flot d'événements principal		
Acteur(s)		**Système**
1. un User S. envoi un message sur le salon privé		2. le Client S. chiffre le message 3. le Client de chat envoie le message au serveur de chat 4. le serveur de chat envoie le message sur le chat général du salon privé, et est visible par les User S. sécurisé connecté sur le salon privé
Flots d'exceptions	RG.2	

4.7 UC 6 : Rejoindre un serveur de chat sécurisé avec authentification

Nom	**Rejoindre un serveur de chat sécurisé avec authentification**
Acteurs concernés	User / User S. / Client / Server
Description	Un utilisateur sécurisé se connecte sur le serveur de chat sécurisé
Préconditions	Avoir un compte sécurisé sur le serveur de chat sécurisé
Evénements déclenchants	L'utilisateur sécurisé est connecté sur le serveur de chat sécurisé
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. l'utilisateur sécurisé entre son nom d'utilisateur et se connecte au serveur de chat sécurisé	2. le Client envoie la demande aux Server et Server S. 3. le Server S. reçoit la demande de connexion général 4. le Server S. vérifie les certificats du compte utilisateur sécurisé et authentifie l'utilisateur sécurisé 5. le Server S. accepte la connexion de l'utilisateur sécurisé 6. création d'un compte utilisateur temporaire par le Server 7. connexion au Server
8. l'utilisateur sécurisé est connecté aux Server S. et Server	

Flots d'exceptions	RG.3, RG.4

4.8 UC 7 : Rejoindre un serveur de chat sans authentification

Nom	Rejoindre un serveur de chat sans authentification	
Acteurs concernés	User / Server / Client	
Description	Un utilisateur se connecte sur le serveur de chat	
Préconditions	Saisir un nom d'utilisateur valide	
Evénements déclenchants	L'utilisateur est connecté sur le serveur de chat	
Conditions d'arrêt		
Description du flot d'événements principal		
Acteur(s)		**Système**
1. l'utilisateur entre un nom d'utilisateur et ce connecte au serveur de chat		2. le Client envoie la demande au Server 3. le serveur de chat reçoit la demande de connexion 4. le serveur de chat vérifie la validité du nom d'utilisateur 5. le serveur de chat accepte la connexion de l'utilisateur
6. l'utilisateur est connecté au serveur de chat		
Flots d'exceptions	RG.1	

4.9 UC 8 : Quitter un serveur de chat

Nom	Quitter un serveur de chat	
Acteurs concernés	User / Server / Client	
Description	Un utilisateur quitte le serveur de chat	
Préconditions	Être connecté sur le serveur de chat	
Evénements déclenchants	L'utilisateur est déconnecté du serveur de chat	
Conditions d'arrêt		
Description du flot d'événements principal		
Acteur(s)		**Système**
1. l'utilisateur quitte le serveur de chat		2. le Client envoie la demande au Server 3. le serveur de chat déconnecte l'utilisateur et supprime de ses registres l'utilisateur
4. l'utilisateur est déconnecté du Server		
Flots d'exceptions	Les certificats de l'utilisateur sécurisé ne sont pas valides	

4.10 UC 9 : Quitter un serveur de chat sécurisé

Nom	**Quitter un serveur de chat sécurisé**
Acteurs concernés	User S. / Server S. / Client
Description	Un utilisateur sécurisé quitte le serveur de chat sécurisé
Préconditions	Être connecté sur le serveur de chat sécurisé
Evénements déclenchants	L'utilisateur est déconnecté du serveur de chat sécurisé
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. l'utilisateur sécurisé quitte le serveur de chat sécurisé	2. le Client envoie la demande au Server S. 3. le Server reçoit la demande du Client 4. Si User S. connecté a un salon privé => UC.10 5. le serveur de chat sécurisé déconnecte l'utilisateur sécurisé
6. l'utilisateur est déconnecté su Server S (et Server si UC.10)	

Flots d'exceptions	

4.11 UC 10 : Quitter un salon privé

Nom	**Quitter un salon privé**
Acteurs concernés	User S. / Server S. / Client S.
Description	Un utilisateur sécurisé quitte le salon privé
Préconditions	Être dans le salon de discussion privée
Evénements déclenchants	L'utilisateur sort du salon de discussion privée et les clés du salon sont modifiées puis renvoyées à tous les autres utilisateurs présents sur le salon de discussion privée
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. User S. quitte le salon privé	2. le Client S. envoie la demande au Server S. 3. le Server S. reçoit la demande 4. le Server S. déconnecte User S. du salon privé 5. les clés du salon privé sont renouvelées 6. les nouvelles clés sont envoyées à tous les User S. connectés sur le salon privé

Flots d'exceptions	

4.12 UC 11 : Déconnexion Serveurs

Nom	**Déconnexion Serveurs**
Acteurs concernés	Users / User S. / Server / Server S. / Admin
Description	Un utilisateur est déconnecté d'un serveur de chat après un problème technique ou de coupure réseaux
Préconditions	Être connecté sur un des deux serveurs
Evénements déclenchants	L'utilisateur est déconnecté du serveur de chat (privé) : – si l'utilisateur était dans un salon privé, alors il y a un renouvellement des clés du salon privé – si l'utilisateur était l'administrateur d'un salon privé, alors le salon privé se ferme
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. Déconnexion après un problème technique	2. événements système UC.8 ou UC.9 3. si User S. connecté dans un salon privé → évènements système UC.10 4. si Admin → UC.14
Flots d'exceptions	

4.13 UC 12 : Créer un salon privé

Nom	**Créer un salon privé**
Acteurs concernés	User S. / Server S. / Client S / Server
Description	Un utilisateur sécurisé crée un salon privé sur le serveur de chat sécurisé
Préconditions	L'utilisateur sécurisé est connecté sur le serveur de chat sécurisé
Evénements déclenchants	Création d'un salon privé, l'utilisateur sécurisé devient administrateur du salon privé
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. L'utilisateur sécurisé clique sur la création d'un salon privé 3. L'utilisateur saisit le nom du salon privé et la liste éventuelle des utilisateurs sécurisés invités	2. le Client ouvre un formulaire de création d'un salon privé 4. Création du salon privé dans Server et Server S 5. Création des clés du salon privé par Server S. 6. Changement de statut de l'utilisateur sécurisé en administrateur du salon privé et envoi d'une clef d'authentification 7. Avertir les utilisateurs invités dans le salon privé qu'ils peuvent le rejoindre 8. Ouverture du salon privé dans un nouvel onglet, côté administrateur, du salon privé 9. Affichage du nom du salon privé dans la liste des salons privés sur la page d'accueil du serveur
Flots d'exceptions	RG.5

4.14 UC 13 : Rejoindre un salon privé

Nom	**Rejoindre un salon privé**
Acteurs concernés	User S. / Server S.
Description	Un User S. rejoint un salon privé
Préconditions	Être connecté avec un compte utilisateur sécurisé sur le serveur sécurisé. Avoir reçu une invitation de la part d'un Admin à rejoindre le salon privé, ou avoir fait la demande de rejoindre un salon privé auprès d'un Admin
Evénements déclenchants	L'utilisateur rejoint le salon privé, modification des clés du salon et redistribution des clés aux utilisateurs présents dans le salon
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. User S. accepte l'invitation à rejoindre un salon privé 2. User S. rejoint le salon privé	3. Ajout du User S. dans le salon privé 4. Renouvellement des clés du salon privé 5. distribution des nouvelles clés du salon privé aux User S. connectés sur le salon privé 6. Un message s'affiche sur le salon privé pour prévenir qu'un nouvel Utilisateur l'a rejoint

Flots d'exceptions	1. User S. décline l'invitation à rejoindre le salon privé 2. Admin refuse la demande de rejoindre le salon privé du User S.

4.15 UC 14 : Fermeture du salon privé

Nom	**Fermeture du salon privé**	
Acteurs concernés	Admin / Server S. / Client S.	
Description	L'Admin du salon privé ferme le salon privé	
Préconditions	Être Admin du salon privé	
Evénements déclenchants	Fermeture du salon privé	
Conditions d'arrêt		
Description du flot d'événements principal		
Acteur(s)		**Système**
1. l'Admin ferme le salon privé 7. Suppression des privilèges Admin au User S. ancien créateur du salon privé		2. le Client S. envoie la demande au Server S. 3. le Server S. reçoit la demande 4. Les User S. et Admin connectés sur le salon privé sont déconnectés. 5. Suppression du salon privé sur le serveur de chat sécurisé et effacement des clés du salon 6. suppression de la clé délivrée à l'admin lors de la création du salon
Flots d'exceptions	Vérification que celui qui demande la fermeture du salon privé ait la clé (admin) généré lors de la création du salon.	

4.16 UC 15 : Exclure utilisateur sécurisé d'un salon privé

Nom	**Exclure utilisateur sécurisé d'un salon privé**
Acteurs concernés	Admin / Server S. / Client S.
Description	L'Admin du salon privé exclut un User S. connecté sur le salon privé
Préconditions	Le User S. exclu doit être connecté sur le salon privé
Evénements déclenchants	User S. est exclu du salon, renouvellement des clés du salon privé
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. l'Admin exclut le User S. du salon privé	2. le Client S. envoie la demande au Server S. 3. le Server S. reçoit la demande 4. le User S. exclu est déconnecté du salon privé par Server S. 5. renouvellement des clés du salon privé, et distribution des nouvelles clés aux User S. connectés sur le salon privé 6. Un message s'affiche dans le salon privé pour prévenir qu'un utilisateur a été exclu

Flots d'exceptions	

4.17 UC 16 : Invitation utilisateur sécurisé dans un salon privé

Nom	**Invitation utilisateur sécurisé dans un salon privé**
Acteurs concernés	Admin / Server / User S. / Client S.
Description	L'Admin du salon privé invite un User S. à rejoindre le salon privé
Préconditions	L'utilisateur invité doit être un utilisateur avec un compte sécurisé
Evénements déclenchants	User S. reçoit une invitation à rejoindre le salon privé
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. Admin envoie une invitation à un (des) User(s) S. pour rejoindre le salon privé 4. le(s) User(s) S. reçoit(vent) l'invitation à rejoindre le salon privé sous forme d'un message	2. Le Client S. de l'admin envoie l'invitation au Server 3. Le Server envoie l'invitation au Client S. du User S. invité dans le salon privé

Flots d'exceptions	

4.18 UC 17 : Envoi d'un message privé non sécurisé

Nom	**Envoi d'un message privé non sécurisé**
Acteurs concernés	User / User S. / Client / Server
Description	Un User (S.) envoie un MP à un User (S.)
Préconditions	Être connecté sur le même serveur de chat que le destinataire du message.
Evénements déclenchants	User (S.) reçoit un message privé dans un nouvel onglet : – MP User vers User S. – demander à User S si il accepte une communication non sécurisée, sinon fermer le MP. – MP User S vers User – prévenir User S. que la communication ne sera pas sécurisée
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. User (S.) envoie un message privé à un autre User (S.)	2. Le client envoie le message vers le serveur de chat 3. le serveur de chat envoie le message au User (S.) destinataire 4. Le client ouvre un nouvel onglet pour afficher le message privé
5. le User (S.) qui reçoit le message est averti qu'un nouveau MP est reçu.	

Flots d'exceptions	Refus de réception d'un message cas MP User vers User S. Refus d'envoie d'un MP cas User S. vers User

4.19 UC 18 : Envoi d'un message privé sécurisé

Nom	**Invitation utilisateur sécurisé dans un salon privé**
Acteurs concernés	User S. / Client S. / Server
Description	Un User S. envoi un MP à un User S.
Préconditions	Être connecté sur le même serveur de chat que le destinataire du message.
Evénements déclenchants	User S. reçoit un message privé dans un nouvel onglet
Conditions d'arrêt	

Description du flot d'événements principal	
Acteur(s)	**Système**
1. User S. envoie un message privé à un autre User S. 6. le User S. qui reçoit le message est avertis qu'un nouveau MP est reçu.	2. Le Client S. chiffre le message et l'envoie vers le serveur de chat 3. le serveur de chat envoie le message au client du User S. destinataire 4. le Client S. du User S. destinataire déchiffre le message 5. Le Client S. du User S. destinataire ouvre un nouvel onglet pour afficher le message privé

Flots d'exceptions	

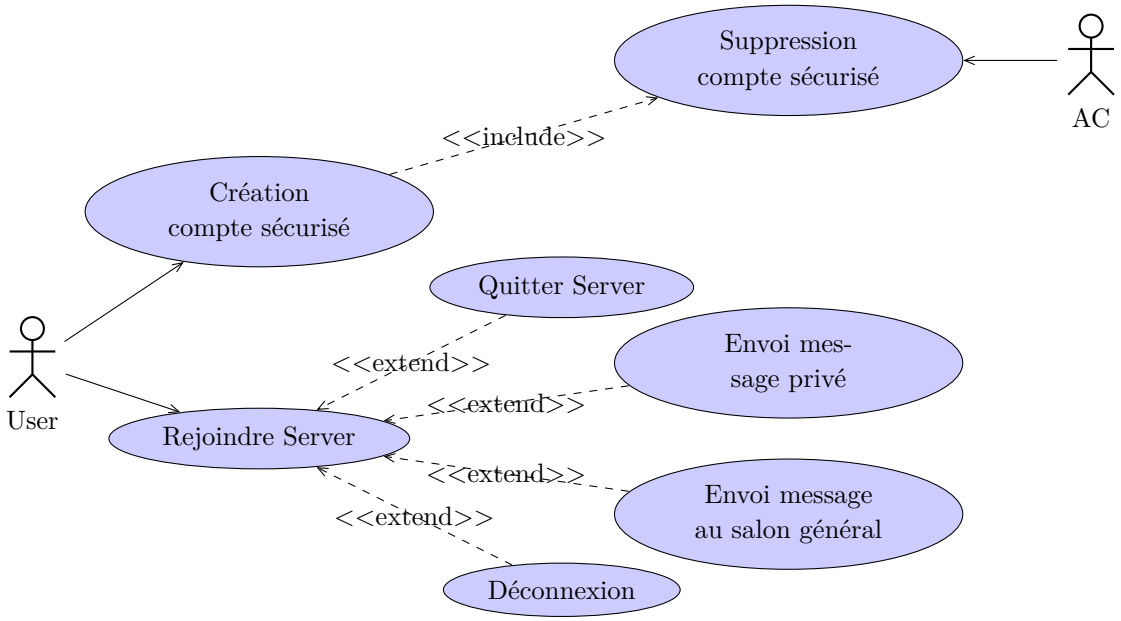
4.20 UC 19 : Demande d'ajout dans un salon privé

Nom	**Demande d'ajout dans un salon privé**
Acteurs concernés	User S. / Admin / Server / Client
Description	Un User S. fait la demande auprès d'un admin pour rejoindre un salon privé
Préconditions	Avoir un compte sécurisé
Evénements déclenchants	L'admin reçoit la demande d'un User S. pour rejoindre le salon privé
Conditions d'arrêt	

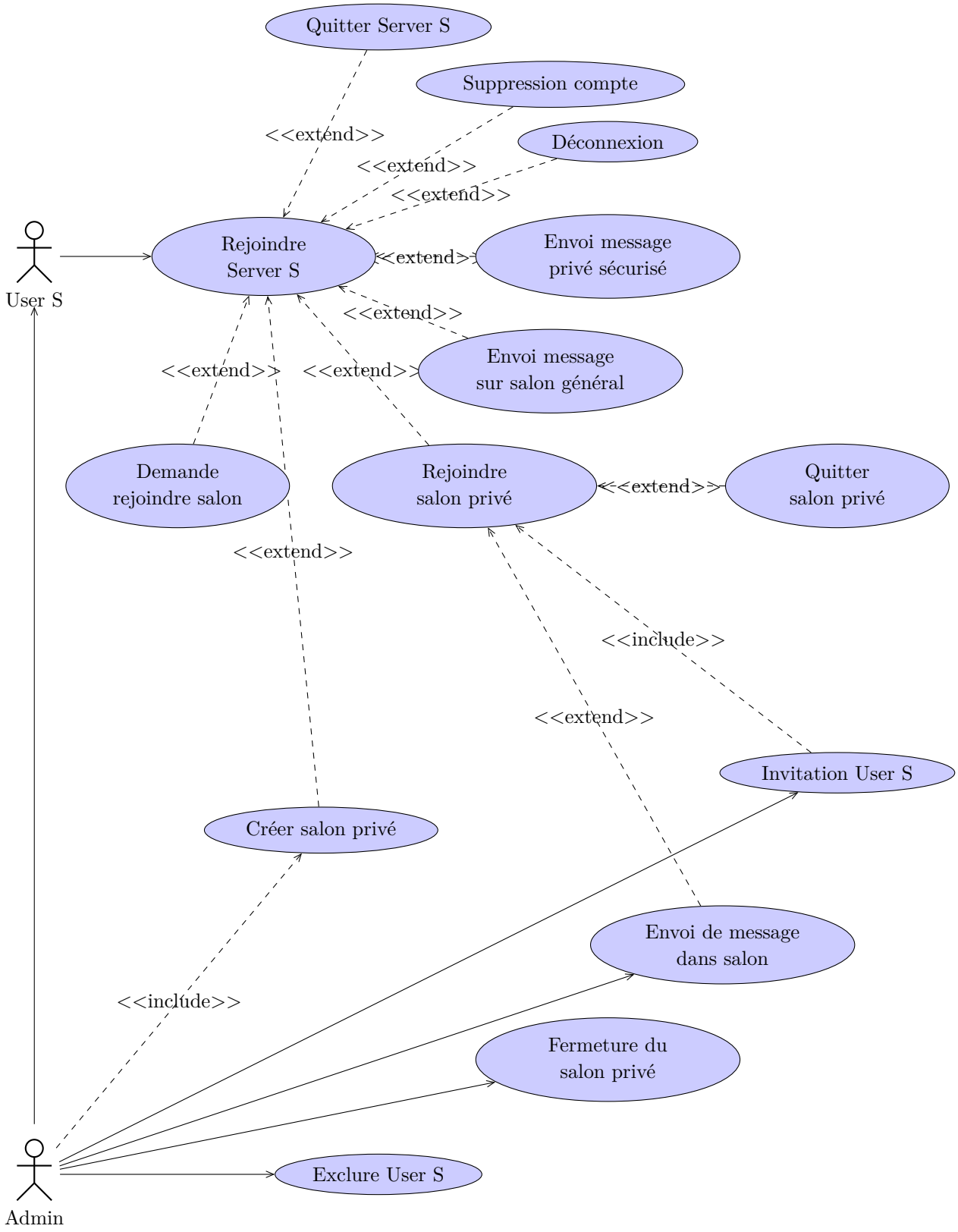
Description du flot d'événements principal	
Acteur(s)	**Système**
1. User S. fait la demande de rejoindre un salon privé auprès d'un Admin	2. Le Client du User S. envoie la demande au Server 3. Le Server envoie la demande au Client de l'admin
4. l'admin reçoit la demande du User S. 5. l'admin accepte la demande et envoie une invitation au User S.	6. Server S. envoie l'invitation au User S.
Flots d'exceptions	Admin refuse la demande de rejoindre un server par User S.

5 Diagrammes de cas d'utilisation

5.1 UC 1



5.2 UC 2


Quitter Server S
Suppression compte
Déconnexion
<<extend>>
<<extend>>
<<extend>>
User S
Rejoindre
Server S
<<extend>>
Envoi message
privé sécurisé
<<extend>>
Envoi message
sur salon général
<<extend>>
<<extend>>
Demande
rejoindre salon
Rejoindre
salon privé
<<extend>>
Quitter
salon privé
<<extend>>
<<include>>
<<extend>>
Invitation User S
Créer salon privé
Envoi de message
dans salon
<<include>>
Fermeture du
salon privé
Admin
Exclure User S

6 Exigences opérationnelles

EO.1 : Confidentialité, intégrité et authentification des messages (seuls les membres du salon peuvent voir les messages et vérifier leur authenticité).

EO.2 : Création d'une interface utilisateur.

EO.3 : Gérer la non répudiation des messages échangés (les certificats doivent pouvoir authentifier l'auteur du message).

EO.4 : Autorité de certification (AC).

EO.5 : Communication multi–salons privés.

EO.6 : Protocoles cryptographiques n'impactant pas sur la rapidité d'échange des messages.

EO.7 : Entrée et sortie d'un utilisateur dans un salon rapides.

7 Exigences d'interface

EI.1 : Création d'un serveur sécurisé « proxy » utilisable sur des protocoles de chat existants.

8 Exigences de qualité

EQ.1 : Assurer la confidentialité, l'intégrité et l'authentification des messages échangés entre les utilisateurs.

9 Exigences de réalisation

ER.1 : Documentation détaillée sur l'utilisation du protocole sécurisé « proxy ».

ER.2 : Documentation détaillée sur l'ensemble de l'application.

ER.3 : Utilisation de openssl dans les algorithmes cryptographiques.

ER.4 : Utilisation de tinyca pour la gestion des certificats.