

Manuel du fonctionnement de Librecord (V1, Août 2023)

Composition du fichier d'un nouvel utilisateur sur le serveur
(pour l'autoriser à se connecter au réseau librerecord)

Hash MDP (qui sert d'identifiant)

Pseudo

Accès salon A = OUI/NON

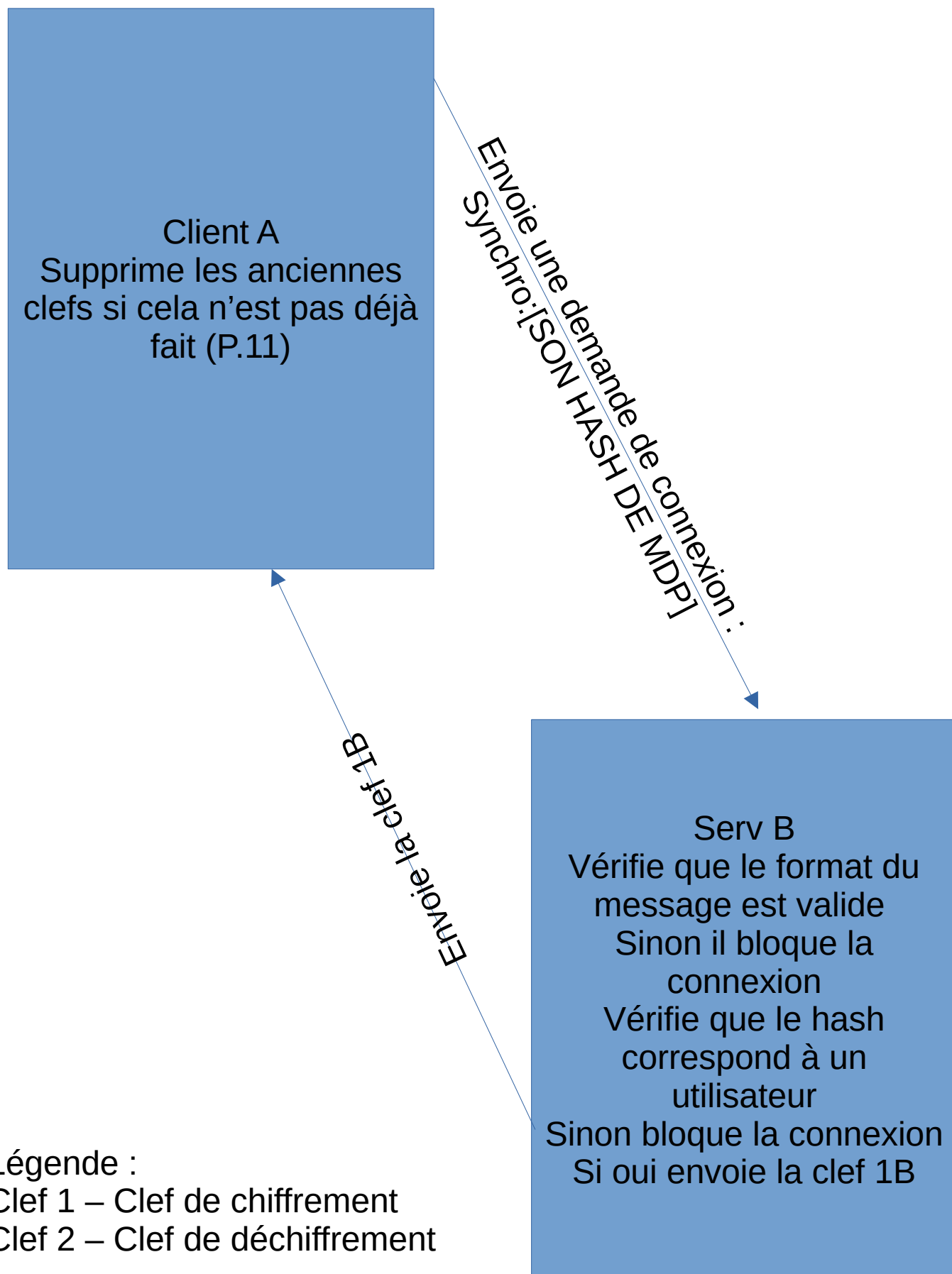
Accès salon B = OUI/NON

Accès salon C = OUI/NON

...

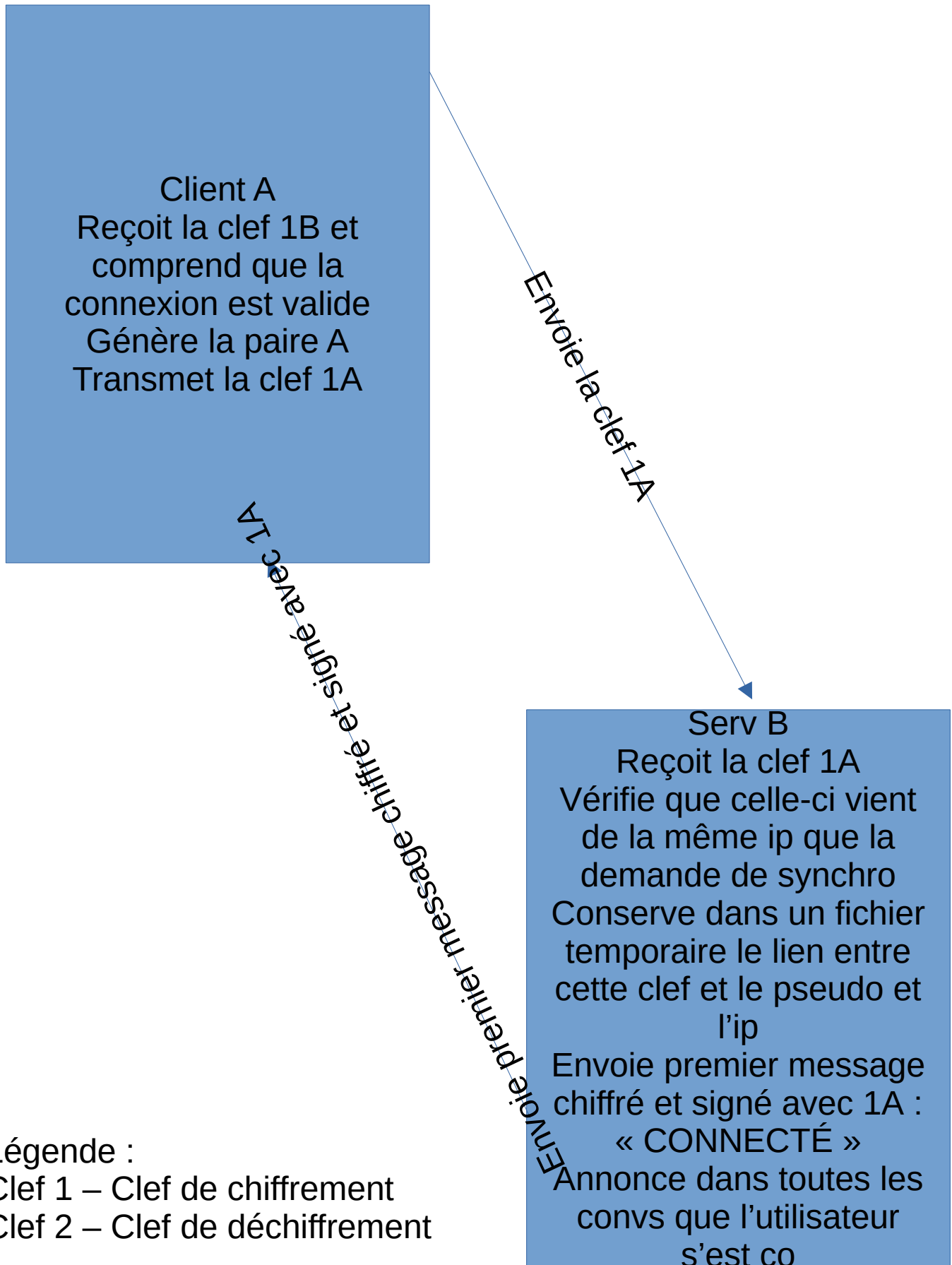
(La création est manuelle, cela permet d'éviter la création de nouveaux outils, qui n'auraient que peu d'utilité car ce système est prévu pour les petites communautés)

Connexion au serveur




Clef A – Pair de clefs générées par le client A
Clef B – Pair de clefs générées par le serv B

Connexion au serveur



Clef A – Pair de clefs générées par le client A
Clef B – Pair de clefs générées par le serv B

Connexion au serveur



Client A
Déchiffre le message
avec 2A
Vérifie la provenance
grâce à la signature
Vérifie que le message
est bien « CONNECTÉ »



Serv B

Légende :

Clef 1 – Clef de chiffrement

Clef 2 – Clef de déchiffrement

Clef A – Pair de clefs générées par le client A

Clef B – Pair de clefs générées par le serv B

Récupération des messages

Client A
Décide le nombre
précédents de messages
qu'il veut télécharger (Par
défaut 10, mais il peut en
demander plus pour
remonter la conversation)

[D]TX/YZ

[D] – Message chiffré et signé

TX – Clef ayant signé

YZ – Clef ayant chiffré

La fonction de récupération est
appelée toutes les 3 secondes

DEMANDE DE 10 MESSAGES

10 MESSAGES

Serv B
Déchiffre avec 2B
Vérifie la signature pour
connaître la provenance
Déchiffre les 10 derniers
message du fichier
général du salon (P.8)
Envoie à l'ip, renseignée
dans le fichier temporaire,
les 10 messages

Légende :

Clef 1 – Clef de chiffrement

Clef 2 – Clef de déchiffrement

Clef A – Pair de clefs générées par le client A

Clef B – Pair de clefs générées par le serv B

Envoi d'un message

Client A
Crée le message signé et chiffré, et le découpe en portions de 256 caractères qui commencent pas MESS1// et finissent par \\MESS1, puis //MESS2 \\MESS2, ... la suite de morceaux se finit par (ENDMESS)

[D]TX/YZ

[D] – Message chiffré et signé

TX – Clef ayant signé

YZ – Clef ayant chiffré

La fonction de récupération des messages entrants par le serv est exécutée toutes les 2 secondes, si celle-ci ne s'exécute pas en continu, je ne m'en souviens plus...

Envoi de tous les morceaux 1 par 1 en 2A/1B

Serv B

Recolle tous les bouts
Vérifie qu'il n'y a pas de trous

Sinon il renvoie une erreur à l'ip de provenance chiffrée et signée au client

Si le message est complet, il enlève mes marqueurs MESS//

Vérifie la signature

Déchiffre avec 2B

Stocke sur le fichier local chiffré

Envoi d'un accusé de réception

1B/2A
MESS1//MESS2\\MESS2\\

Légende :

Clef 1 – Clef de chiffrement

Clef 2 – Clef de déchiffrement

Clef A – Pair de clefs générées par le client A

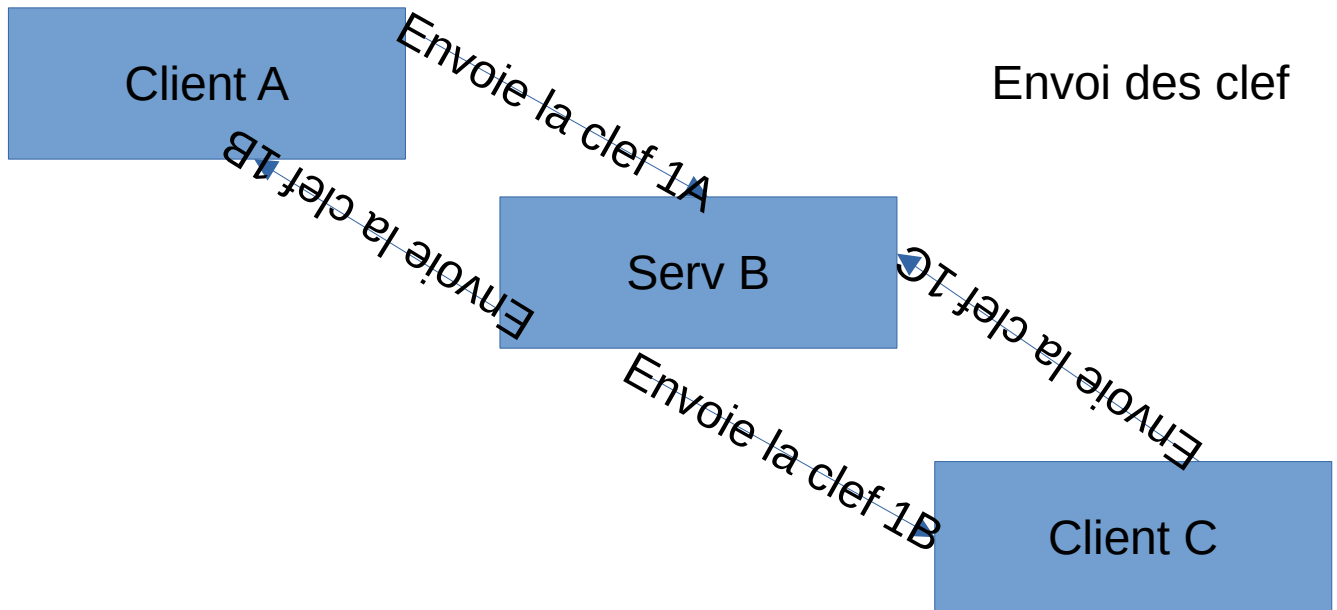
Clef B – Pair de clefs générées par le serv B

Composition du fichier d'un salon

[TOUS LES MESSAGES A LA SUITE AU FORMAT :
PSEUDO : XXXXXXXXXX
MESSAGE : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ;
PSEUDO : XXXXXXXXXX
MESSAGE : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ;
PSEUDO : XXXXXXXXXX
MESSAGE : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ;
PSEUDO : XXXXXXXXXX
MESSAGE : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ;
PSEUDO : XXXXXXXXXX
MESSAGE : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ;
PSEUDO : XXXXXXXXXX
MESSAGE : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ;
PSEUDO : XXXXXXXXXX
MESSAGE : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ;
PSEUDO : XXXXXXXXXX
MESSAGE : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ;
PSEUDO : XXXXXXXXXX
MESSAGE : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ;]
PSEUDO : XXXXXXXXXX

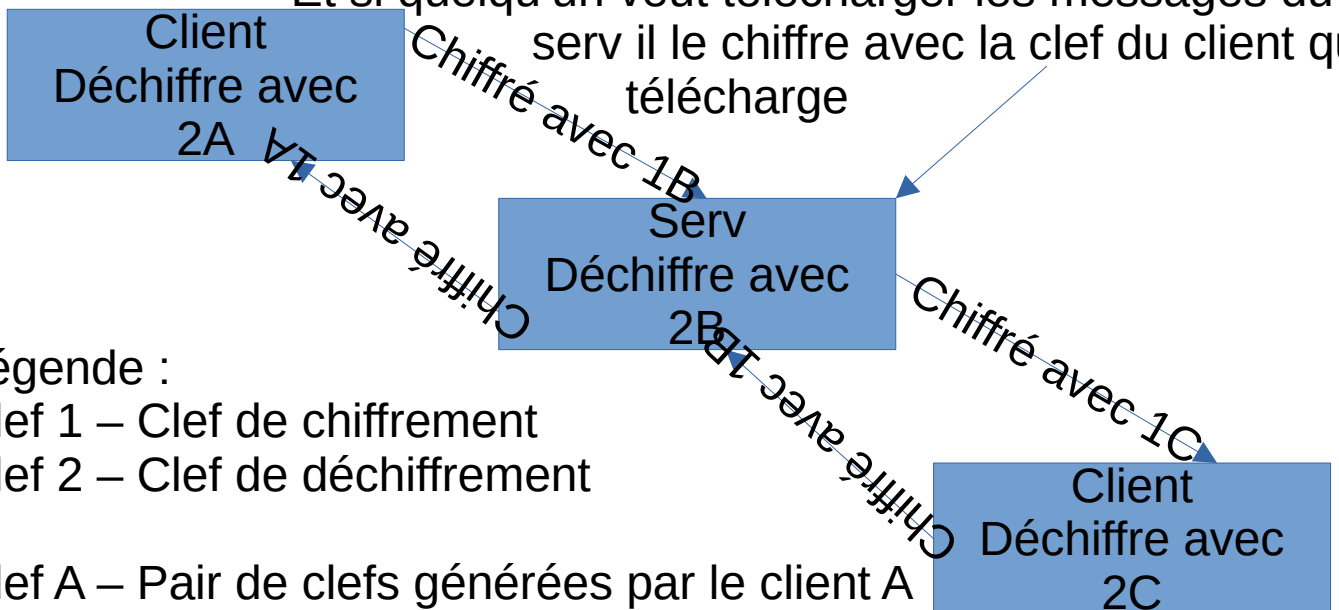
**CHIFFRÉ AVEC LE MDP PERSONNEL QUI
CORRESPOND A UN MOT DE PASSE CHOISIT PAR
L'HÉBERGEUR ET QUI EST FIXE**

Schéma de fonctionnement simplifié avec 2 clients



Envoi des messages

Le serv convertit les messages reçus pour les chiffrer avec sa propre clef de chiffrement Et si quelqu'un veut télécharger les messages du serv il le chiffre avec la clef du client qui télécharge



Légende :

Clef 1 – Clef de chiffrement

Clef 2 – Clef de déchiffrement

Clef A – Pair de clefs générées par le client A

Clef B – Pair de clefs générées par le serv B

Clef C – Pair de clefs générées par le serv C

Fin de communication

[D]TX/YZ

[D] – Message chiffré et signé

TX – Clef ayant signé

YZ – Clef ayant chiffré

Client A
Se ferme
Supprime les clefs

FIN COMM 2A1B

Serv B
Ferme la communication
Supprime le fichier
temporaire de l'utilisateur
Annonce dans la
conversation du dernier
salon actif que l'utilisateur
s'est déco

Légende :

Clef 1 – Clef de chiffrement

Clef 2 – Clef de déchiffrement

Clef A – Pair de clefs générées par le client A

Clef B – Pair de clefs générées par le serv B

Fin de communication brutale
Crash client

[D]TX/YZ
[D] – Message chiffré et signé
TX – Clef ayant signé
YZ – Clef ayant chiffré

Client A
[NE PEUT PAS
SUPPRIMER LA PAIR DE
CLEFS CAR LE
PROCESSUS EST
ARRÊTÉ AVANT] (P.3)

Serv B
Attend un demande de
récupération de
messages
Si timeout de 30 secs
Couper la communication
Supprimer le fichier
temporaire
Annoncer que l'utilisateur
s'est déco

Légende :

Clef 1 – Clef de chiffrement

Clef 2 – Clef de déchiffrement

Clef A – Pair de clefs générées par le client A

Clef B – Pair de clefs générées par le serv B

Fin de communication brutale
Crash connexion

Client A

Décompte de 25
secondes (pour éviter que
le client essaie de se
reco au moment où le
serv le supprime, 30s – 5s
de marge)

Si 25 secondes sans reco
Supprimer la pair de clefs

Revenir à la page de
renseignement du mdp
pour recommencer une
connexion après 7
secondes d'attente pour
être sûr que le serveur
n'attend plus de réponse
de la part du client

[D]TX/YZ

[D] – Message chiffré et signé

TX – Clef ayant signé

YZ – Clef ayant chiffré

Serv B

Attend une demande de
récupération de
messages

Si timeout de 30 secs
Couper la communication
Supprimer le fichier
temporaire

Annoncer que l'utilisateur
s'est déco

Légende :

Clef 1 – Clef de chiffrement

Clef 2 – Clef de déchiffrement

Clef A – Pair de clefs générées par le client A

Clef B – Pair de clefs générées par le serv B