Architecture Client-Serveur comme toute communication sur internet.

Utilisation du module « socket » de Python pour ouvrir des connexions utilisant le protocole TCP/IP.

Le serveur est donc repéré par son adresse IP et le port qu’il dédie à la messagerie.

Mise en place d’une programmation dite « en parallèle » à l’aide du module Thread de Python pour permettre la réception et l’envoi simultané de messages.

Procédure de *Handshake*:

A chaque connexion d’un client sur le serveur, il doit renseigner un pseudo qui permettra aux autres utilisateurs de l’identifier et une clé publique. Le serveur stocke ces informations et les rend accessibles aux autres utilisateurs.

Le serveur est donc bien un canal public puisque tous les utilisateurs peuvent accéder à tous les messages, même ceux qui ne leur sont pas adressés. D’où l’importance du cryptage.

####SCHEMA SERVEUR####

####SCHEMA CLIENT######

####SCRIPT#############