Two user chat

User must be authenticated before it can use chat

Passwords are stored in a separate file with username: hash pair

When creating user, create new keys

I ideal world, file with hashes will be protected, and secret keys stored in a separate location.

When establishing a chat communication public key from the user is sent to the other party and another party will have to accept it. If the key already exists for that user, it is compared and in the case of difference, the warning is displayed to the party. Another participant in the chat and either accept or reject the key if he/she thinks it is a case of a man in the middle attack or identity stealing/forgery.