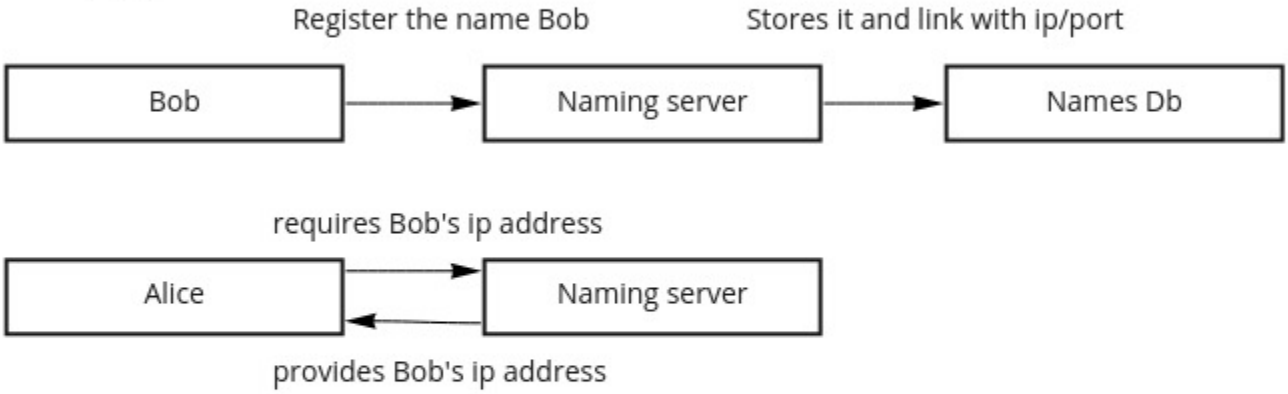
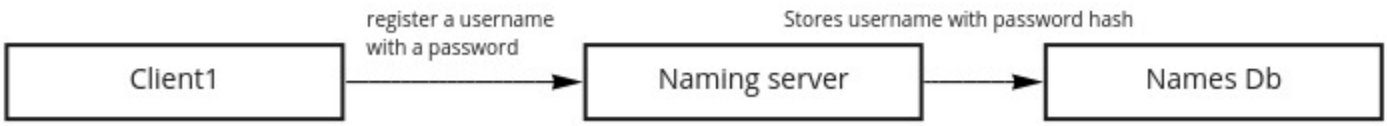
Central naming server

MVP1



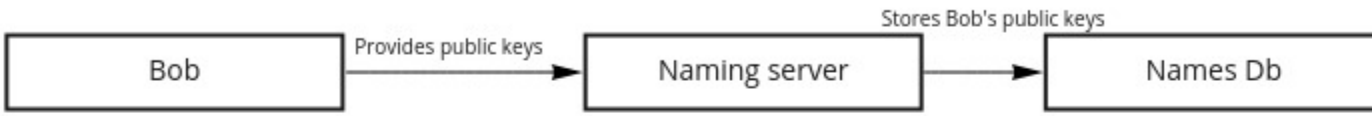
MVP2

Let's see about that register thing, it would be better if somehow we would have some kind of auth to the naming server.



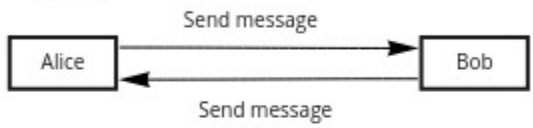
MVP3

The naming db shall also handle the public key storing and being able to give them back
A registered user shall be able to provide it's public keys to the server



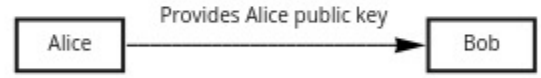
P2P message app

MVP1

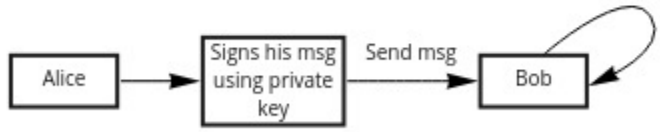


You can choose any languages that may fit and any tech that may fit.
Performances won't be taken into account.
Personnal advice : python3 + websocket and/or rest api

MVP2

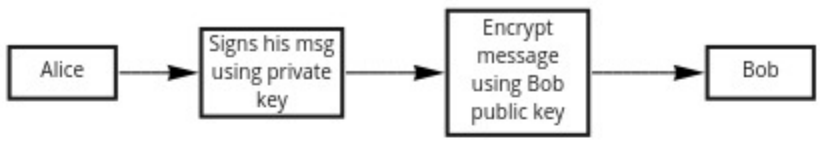


Now that you can send messages to your buddies, we will sign the messages. We want to make sure Alice is who she say she is!



Verifies Alice's signature with Alice's public key

MVP3



Ok so now, I can be sure that Alice is to be trusted, however anyone capturing network could be intercepting our messages.
What we want now is to make sure that the only person able to decrypt Alice's messages to Bob would be Bob.
So what Bob would do is to provide Alice with a public key to encrypt his messages.