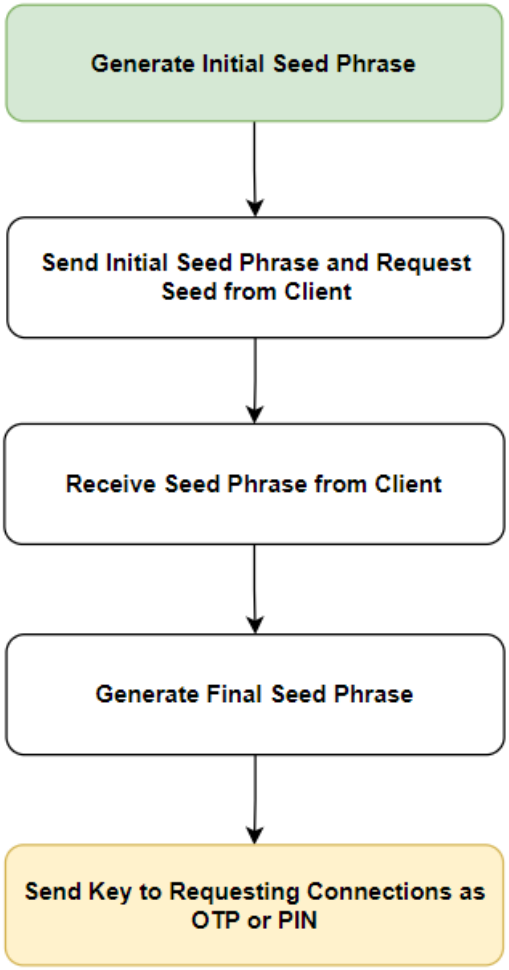
Decentralised Key Generator Using Multi Party Computation

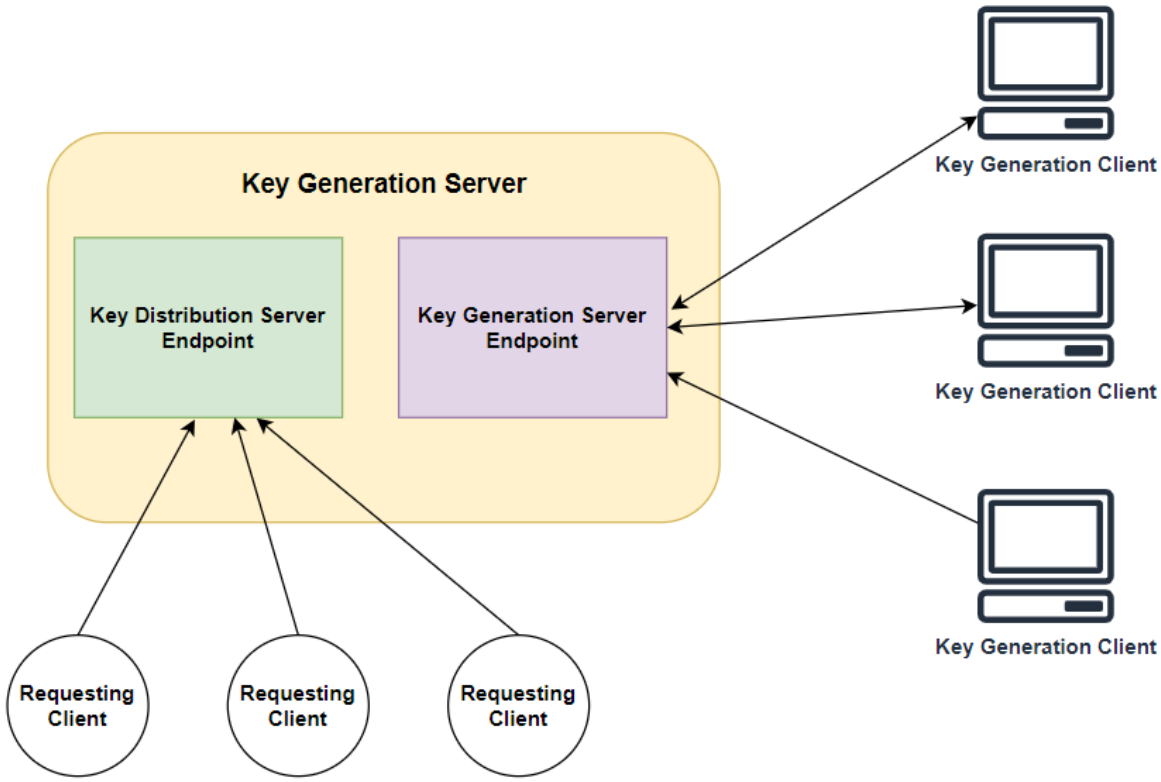
Process Flow:

The server initially generates a seed phrase and then sends it to all the participating clients in the OTP or Key Generation Process. The clients on receiving this seed phrase then initiate a computation that causes the clients to use the received key phrase as the seed phrase for a local computation on their side to generate a secret phrase. THis phrase is then sent to the server as the response. On receiving the seed phrase then the server combines all the received secret phrases from the clients and then pushes them inside a local function in the server that generates the final Key or the OTP which is then stored in the Server Database or File.



Note:

1. Usage of RSA Encryption Algorithm to Generate 2 Keys on the Server side
2. Key need to be passed on to the participating clients
3. All the communication must be encrypted while transmission using the sender keys from the side of the client to the side of the Key Generation Server,
4. Every client should use their own unique function is order to generate the keys



Key Generation at Server

The server immediately creates the key pairs using the RSA algorithm when the server is turned on for the first time.The server then starts listening for the connections from the Key Generation Client.

Key Transportation From Server

While the client server initial connection is being set up, the server sends the **public key of the server** in order to encrypt the data.

Seed Phrase Generation at the Key Generation Client Side

The key generation clients then take a random value from the participating users and then put it inside a **Secret_Phrase_Generator** function that causes the creation of a **secret phrase.**

Seed Encrypt and Transfer:

The secret phrase is then encrypted via using the server's public key and then sent back using the socket object back to the key generation server.

Decryption at the key generation server:
On receiving the secret phrase from the key generation client, the data is decrypted. This decrypted data is then sent to the response secret phrase generation step.

Response Secret Phrase Generation:
Based on the decrypted data a **Response Phrase Generation Function** is initiated that causes the creation of a secret key.

File Storage in Key Server:
The secret key is then stored in the key_store text file.

Key Distribution Server and OTP Requesting Client:
The key distribution server is another endpoint using which the OTP requesting client can **request for the OTP from the key store.** The key distribution server then sends the OTP to the OTP requesting client, which the requesting client can then use.

Application:

1. Can be used as OTP and Two Factor Authentication
2. Use in the RSA algorithm data for the n and the e values **(Key Pair Generation)**
3. Use in ECC for configuration data for the number of point addition in the private key generation phrase (Key Pair Generation)
4. Used in Blockchain for Private and Public Key Generation,
5. Can be used in multiparty computation problems like multi signature wallets etc.
6. Random value in digital signature standards,
7.

Additional Tasks:

1. Put additional client in order to decentralize the process further,
2. The Key Distribution Server should send the data to the OTP requesting client in encrypted format