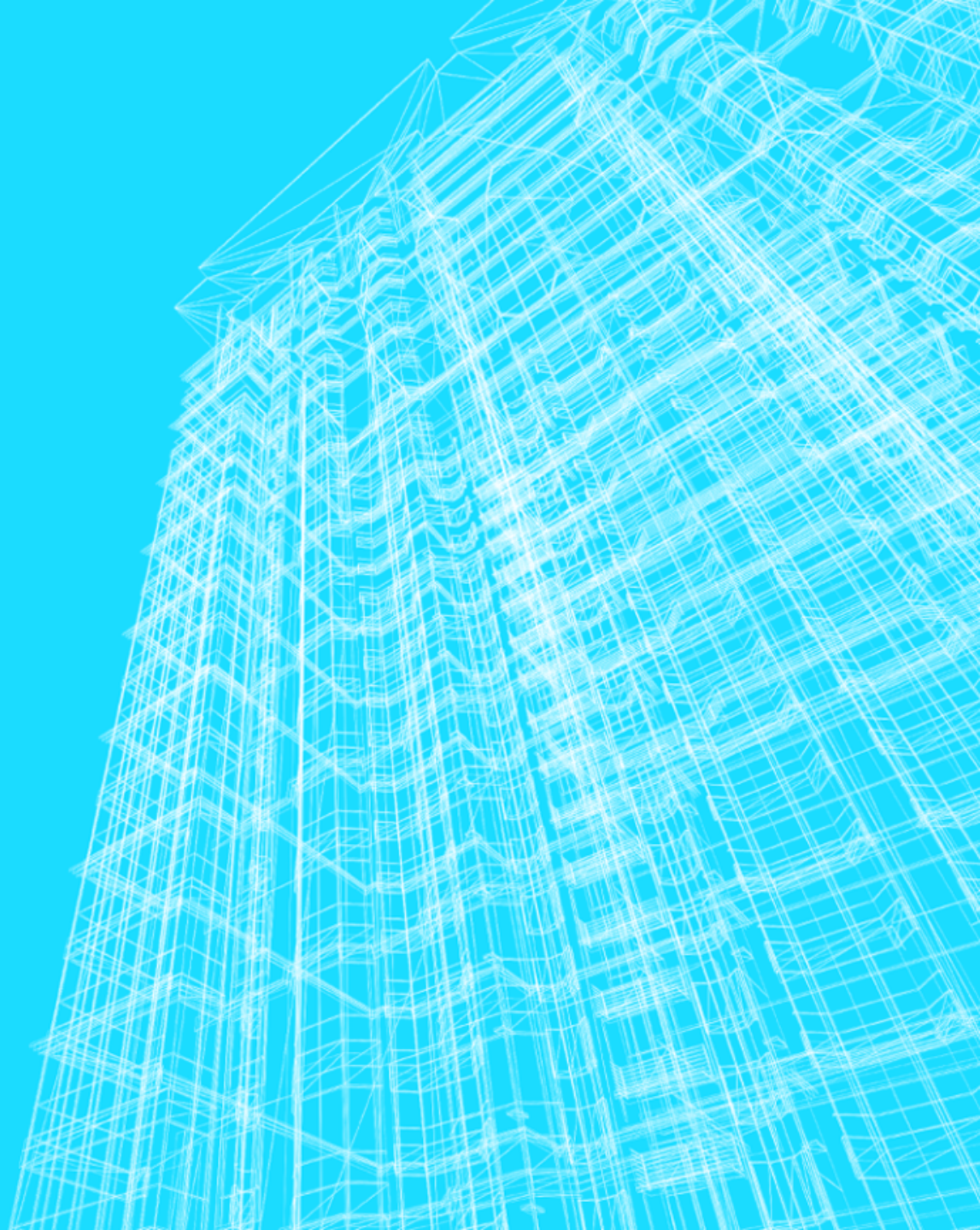
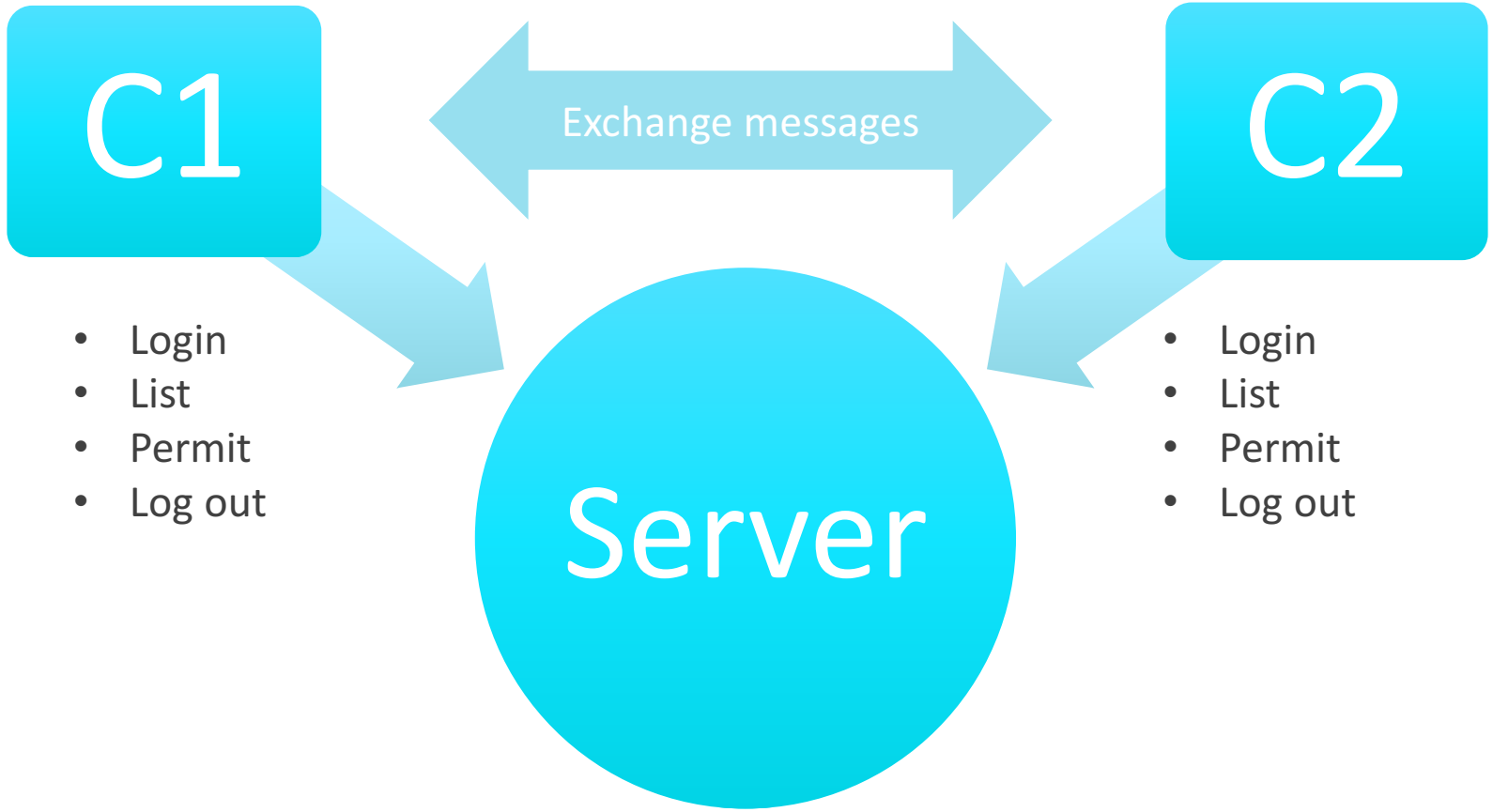
PFS CHAT

Matt Brandman
Ibrahim Aleidan

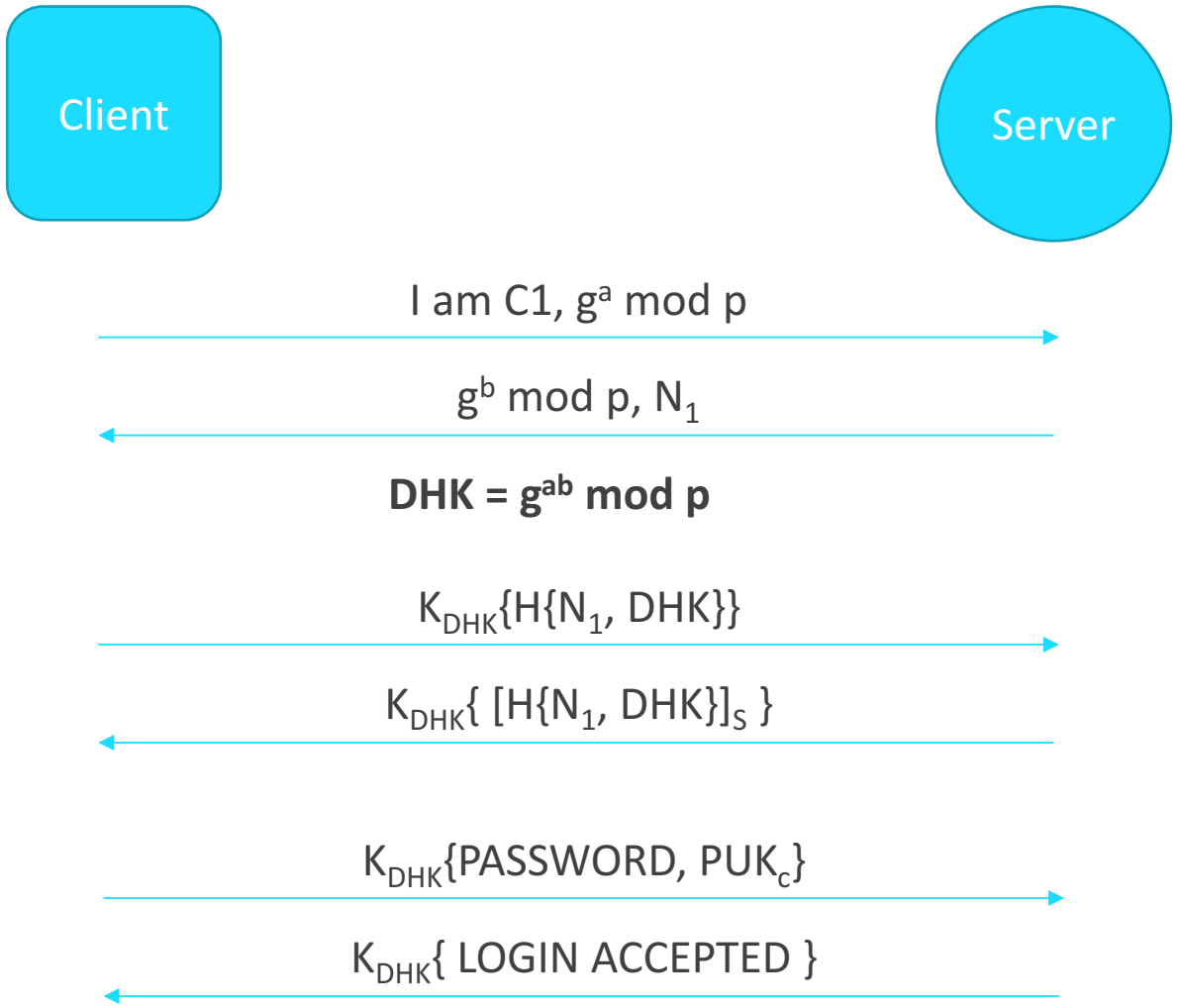


ARCHITECTURE



ASSUMPTIONS

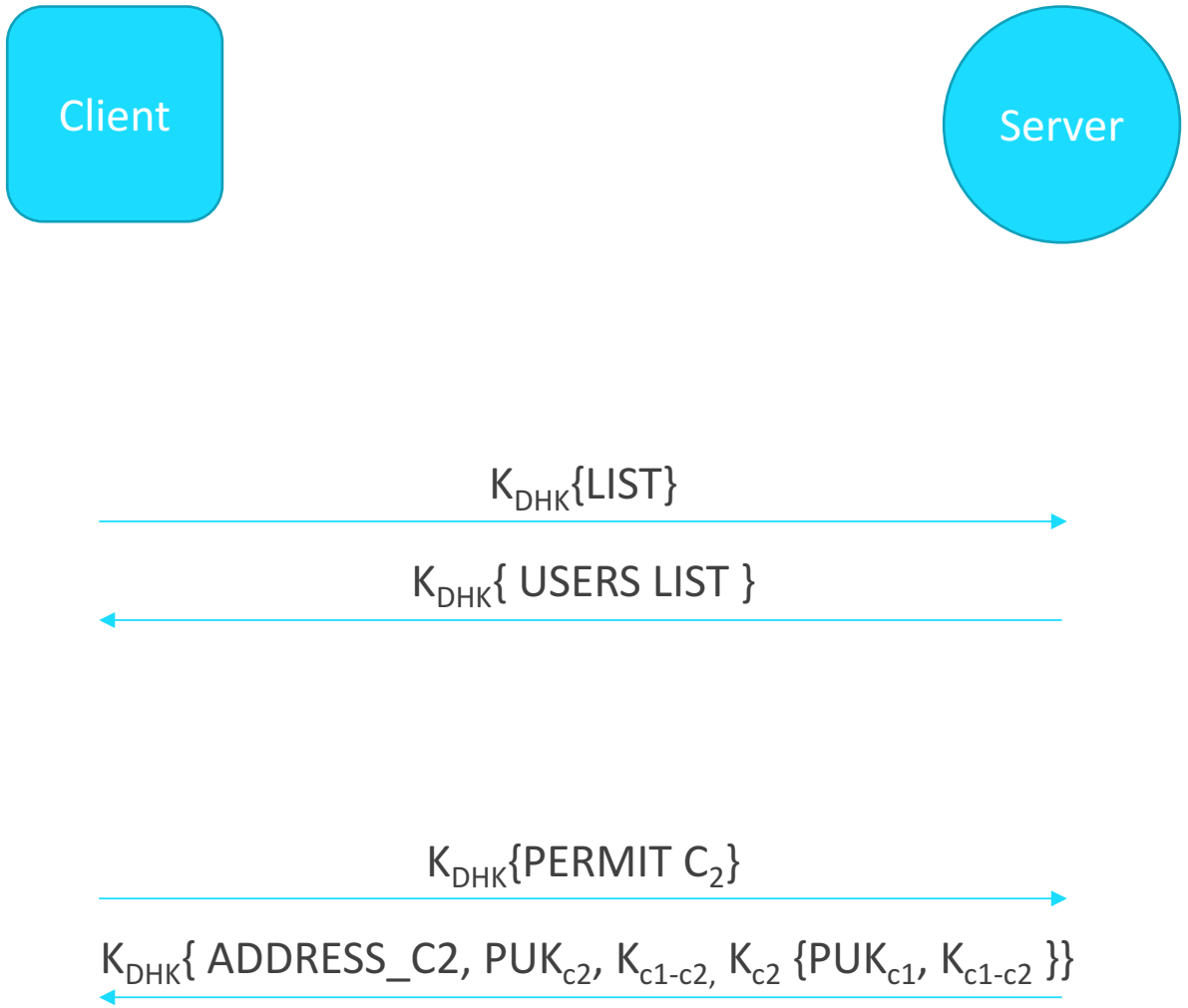
- Client knows the public key of the server
- Server knows the password for the client
- Clients are preregistered with the server and persist through restart
- Shared Secret is used to key a AES-CBC encryption



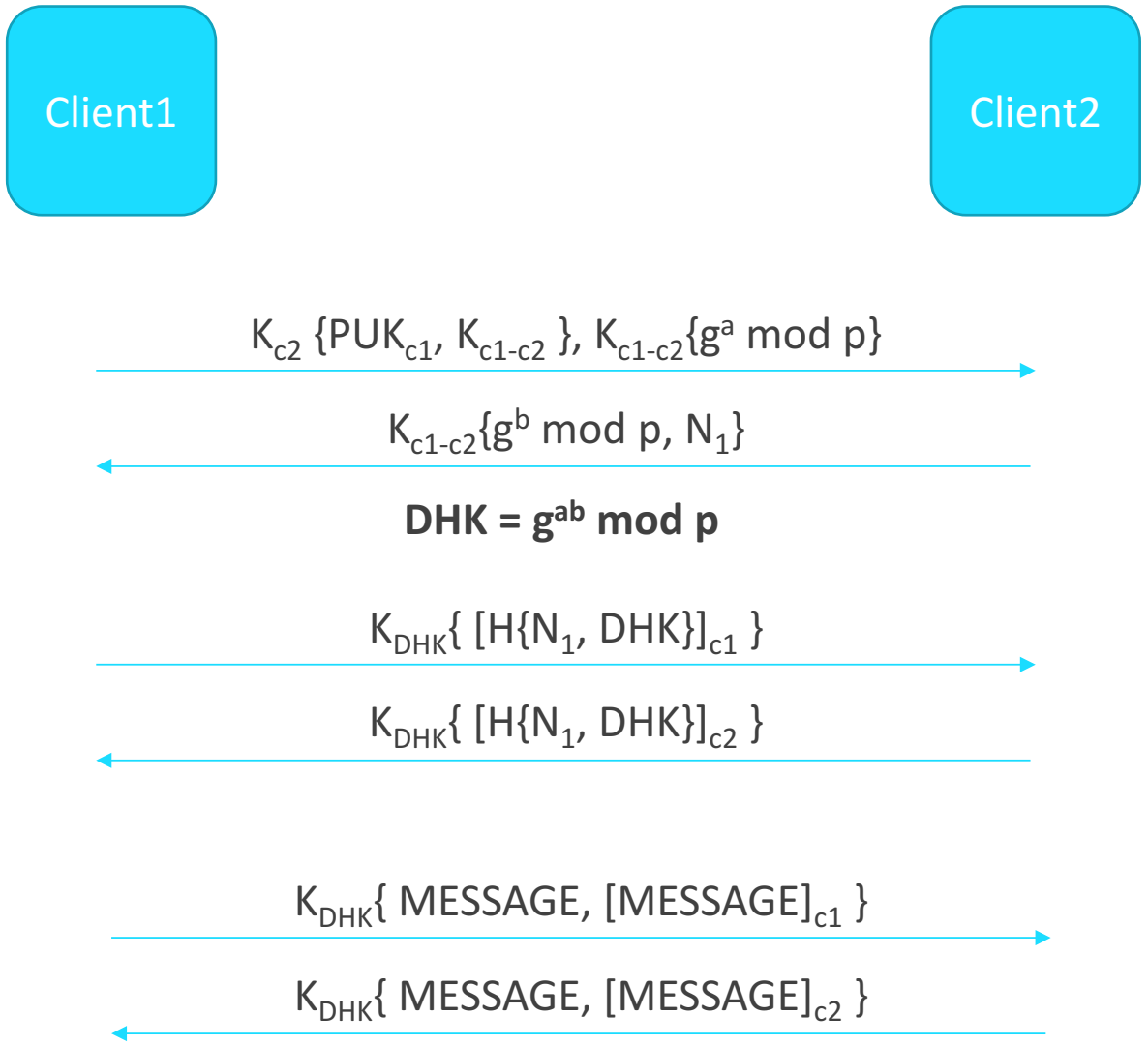
LOGIN PROTOCOL

PUK_x = Public Key of x.

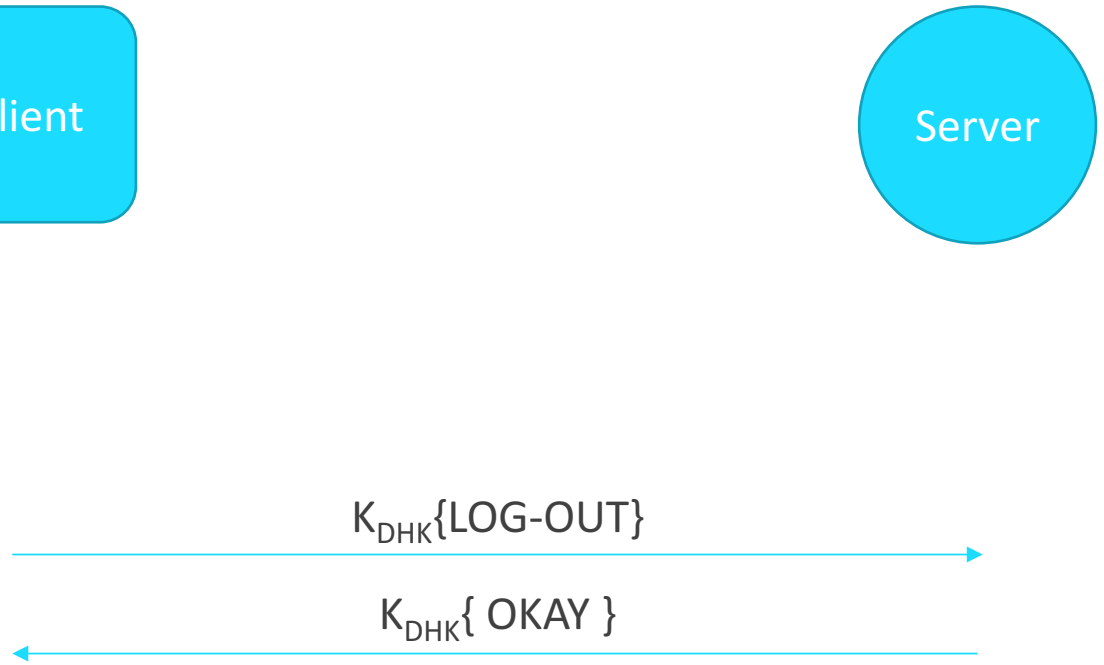
LIST & PERMIT PROTOCOL



CLIENT-CLIENT PROTOCOL



LOGOUT PROTOCOL



DISCUSSION

- The use AES throughout keyed with a DH shared key means that even if the private key of the server is cracked they will never be able to decrypt past messages.
- Shared Secret is used to key a AES-CBC encryption
- SHA-2 is used as hashing algorithm