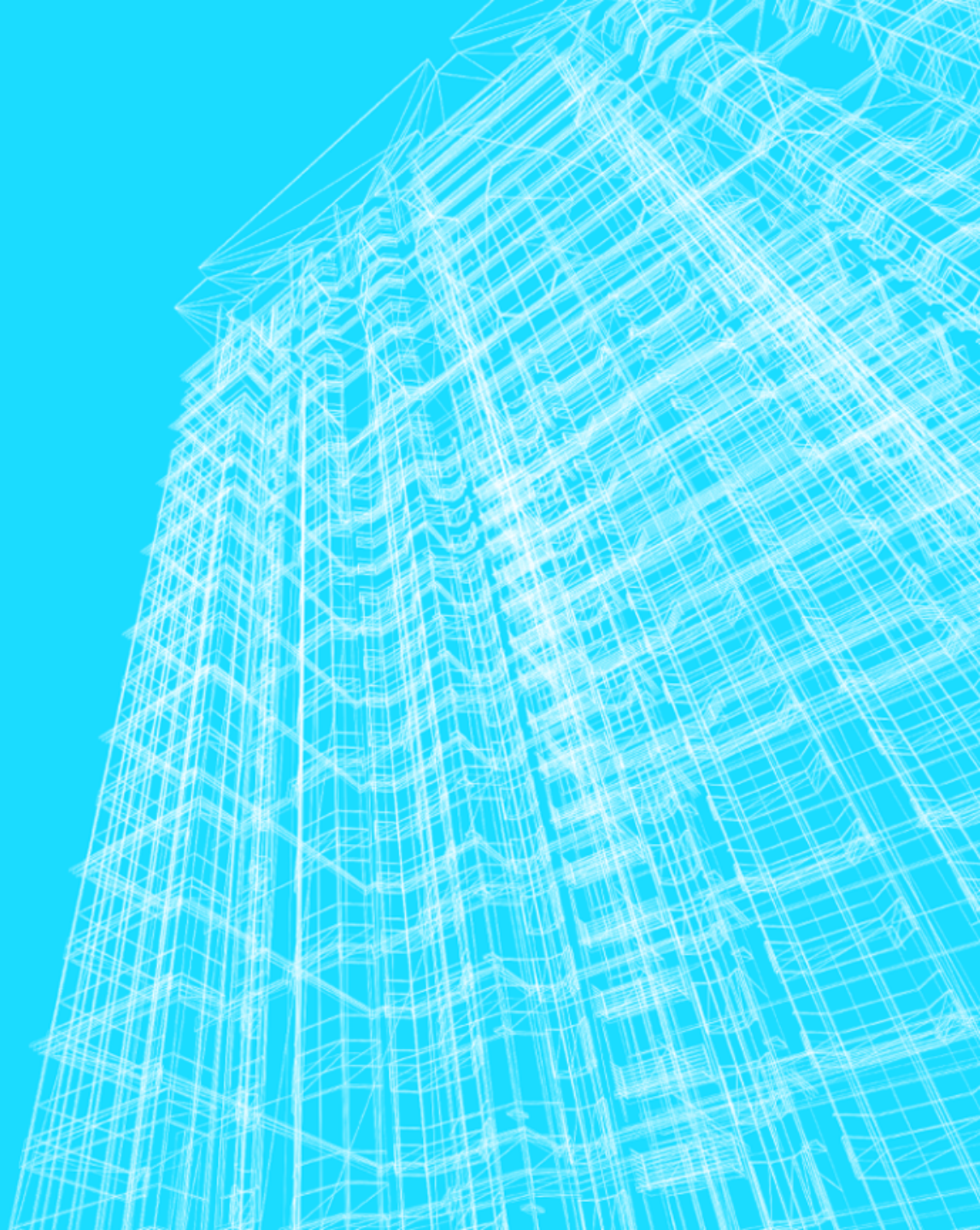
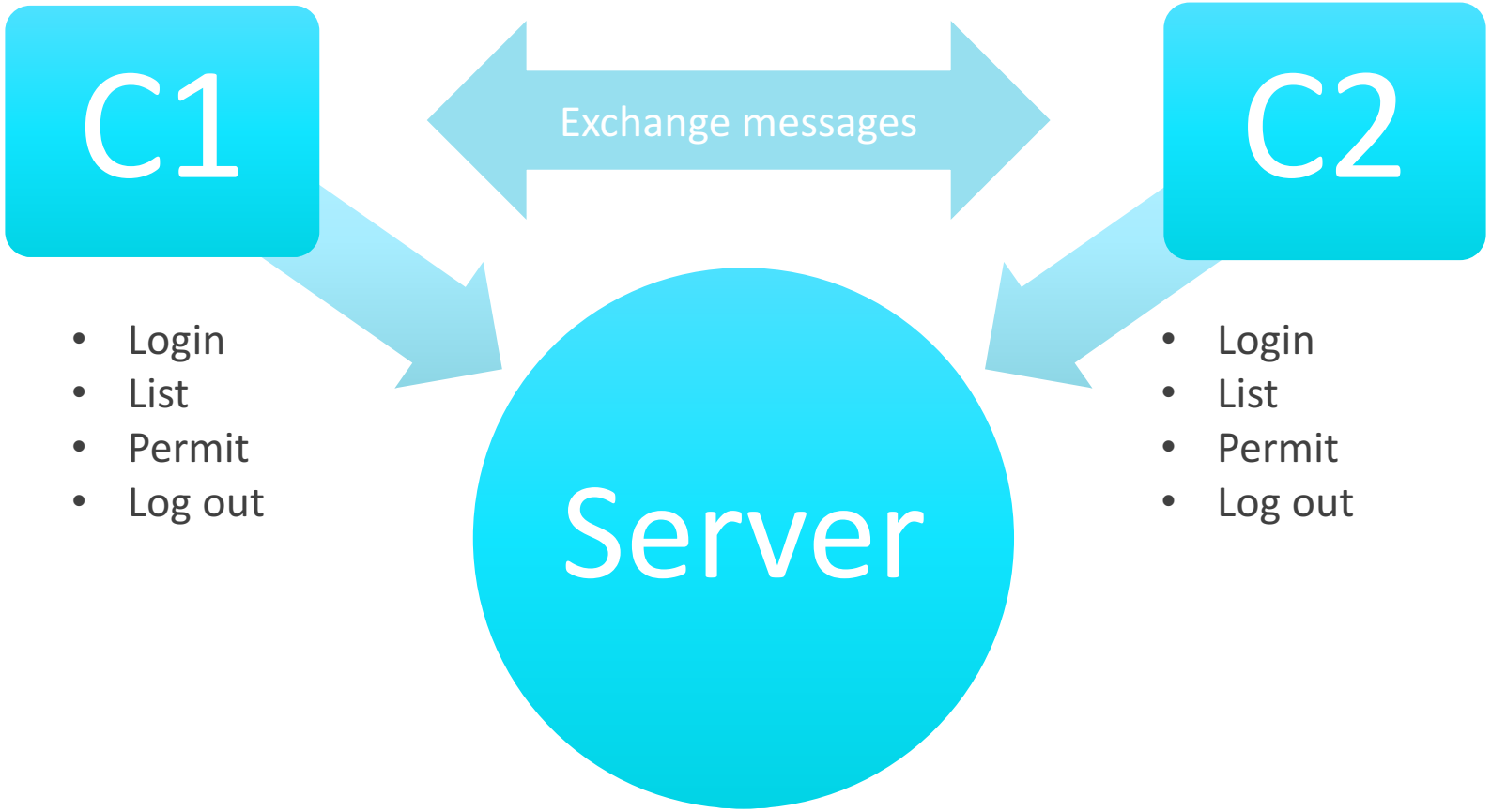
PFS CHAT

Matt Brandman
Ibrahim Aleidan

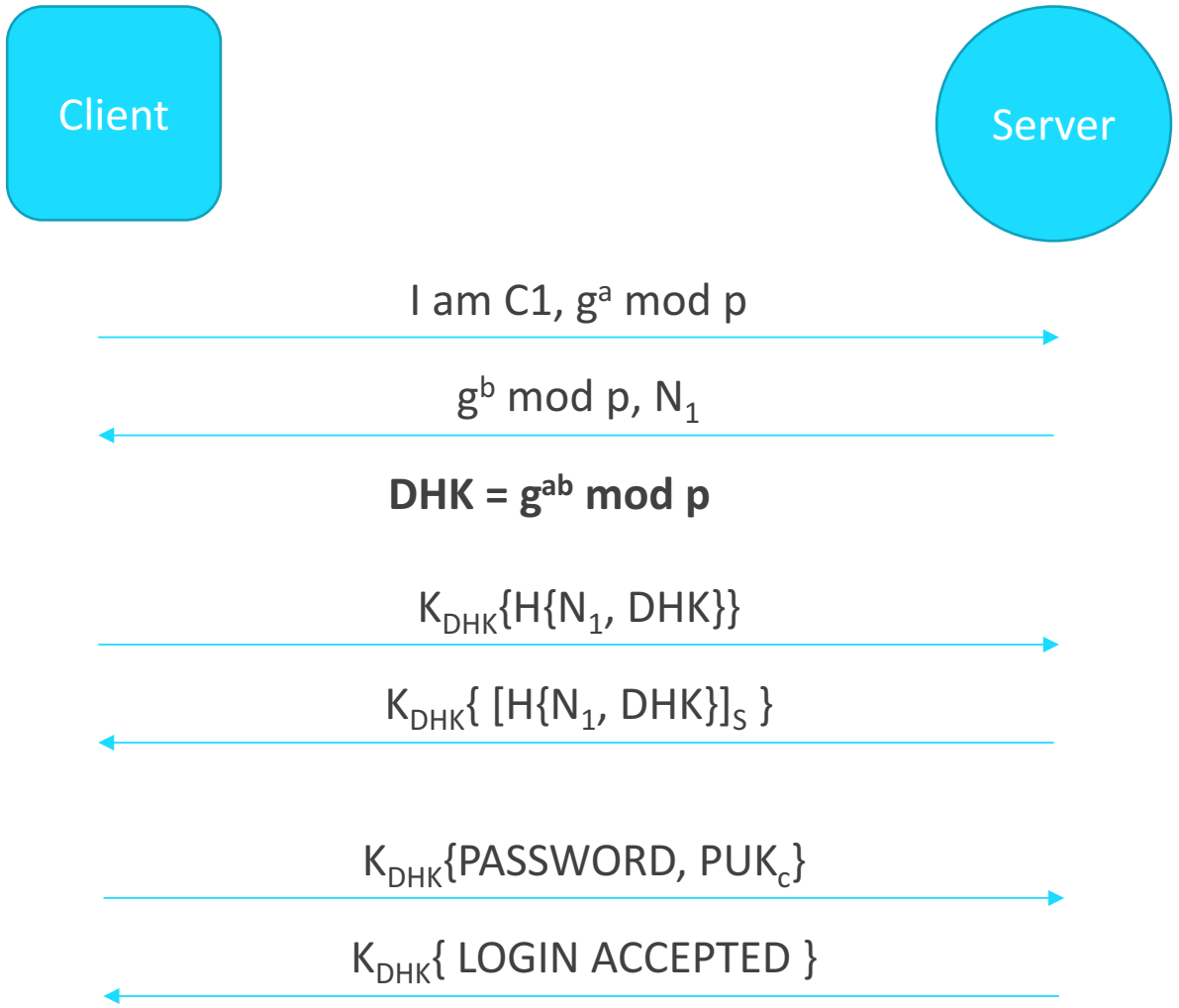


ARCHITECTURE



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-GCM encryption



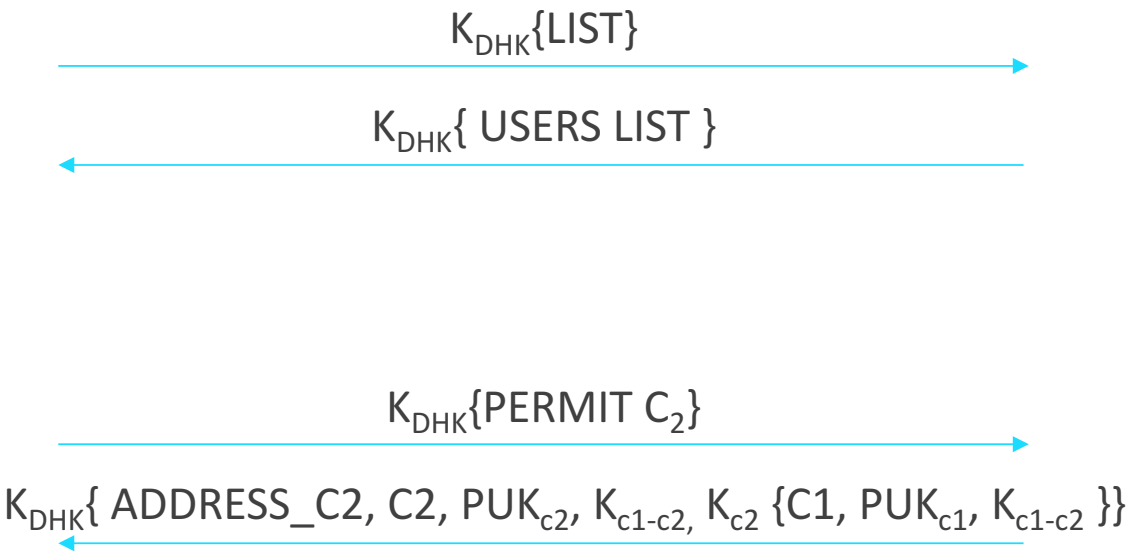
LOGIN PROTOCOL

PUK_x = Public Key of x.

Client

Server

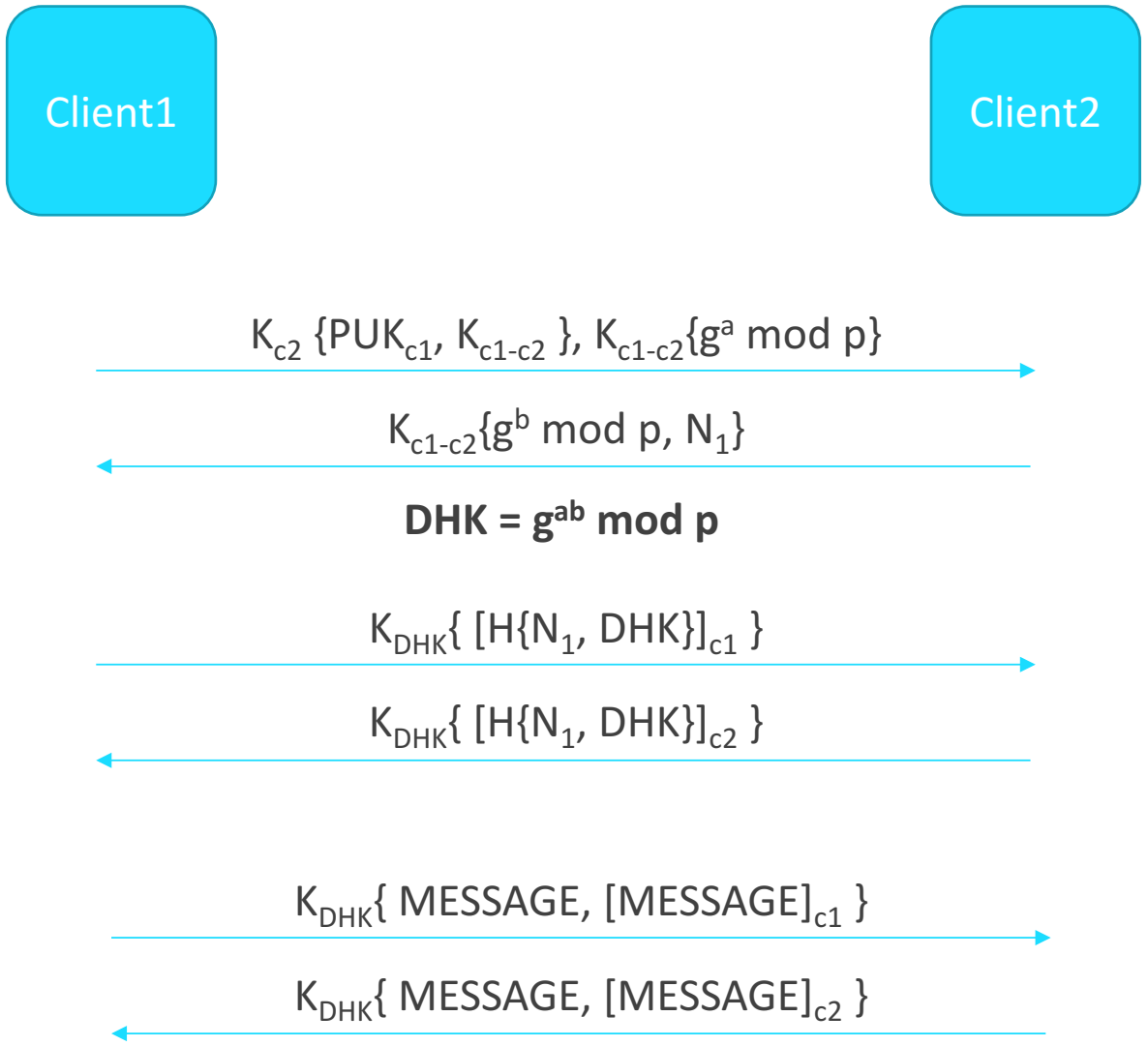
LIST & PERMIT PROTOCOL



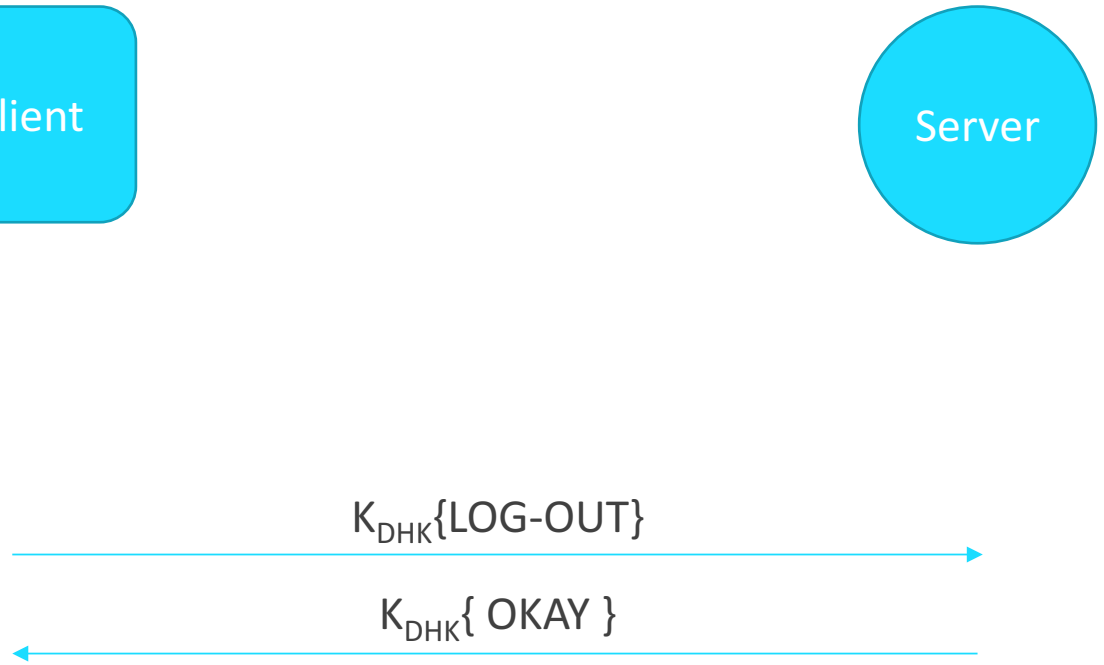
Changed

Added C2 to reply and C1 to ticket.

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

NOT IMPLEMENTED IN CODE

- Delete the key between Client-Server and Client-Client after some time, and ask to start a new key if key expired.

CHANGES FROM PS4

- Used AES-GCM instead of AES-CBC.
- One more change shown in PERMIT Protocol.