**SSH Keys**

SSH-keygen is a standard component of the Secure Shell protocol suite found on Unix, Unix-like and Microsoft Windows computer systems used to establish secure shell sessions between remote computers over insecure networks, using various cryptographic techniques.

There are two types of keys “public key” and Private key, Private is your client ID just like Mac-address, and public key is to verify your connection.

If you want you have secure ssh connection with password authentication, you would need to generate both keys on client using command “ssh-keygen” in will generally create to two files “id\_rsa and id\_rsa.pub” whare id\_rsa is private key and id\_rsa.pub is public key.

Copy the public key and paste in Linux-Server “authorized\_keys” file which is in the directory of “home/user/.ssh” and then ssh form client.

Creating custom keys to share with team use “ssh-keygen -t ed25519“ to access the ssh-server using custom key navigate to directory whare you would save this custom key and type “ssh -i id\_ed2SS19 server-username@server-ip, e.g ssh -i id\_ed2SS19 aqib@192.168.22.61”

Add below to “authorized\_keys” is you want to restrict client to only use keys authentication instead of Password.

“ChallengeResponseAuthentication no

PasswordAuthentication no

PermitRootLogin no”

Prefer to to use multiple public keys on one server instead of using single private key at multiple client. If you have to provide private key to multiple user, then generate custom new public and private key and share that one.