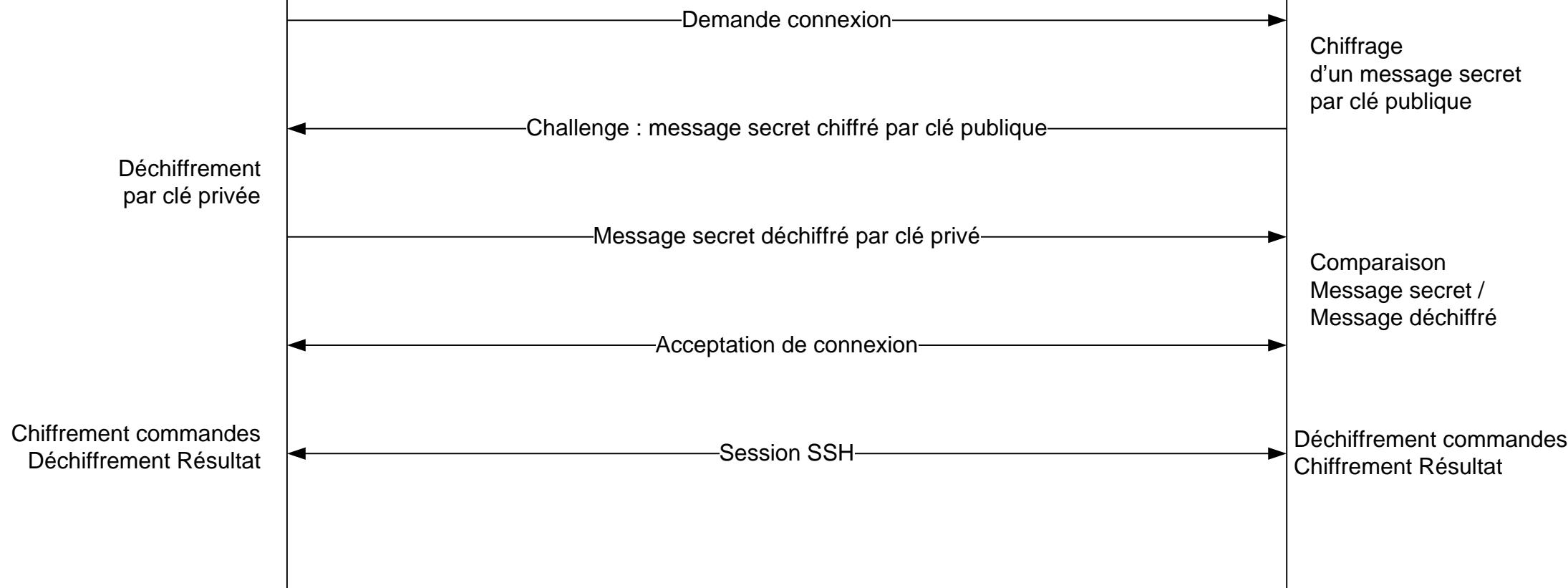
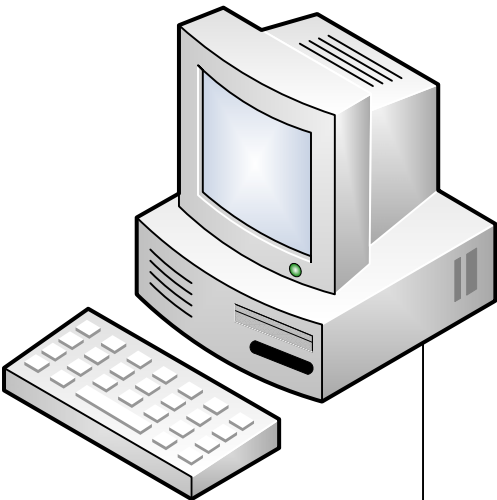


Client SSH
id_rsa (Clé privée)

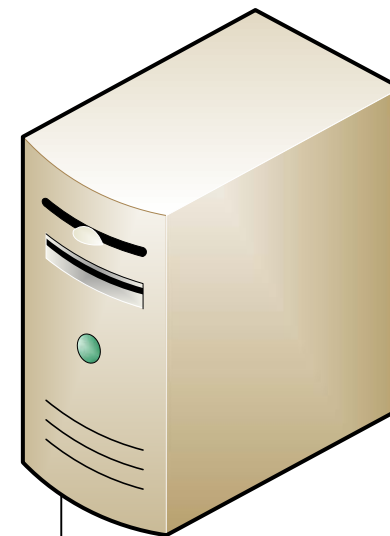


Serveur ssh
Authorized_keys (Clé publique)

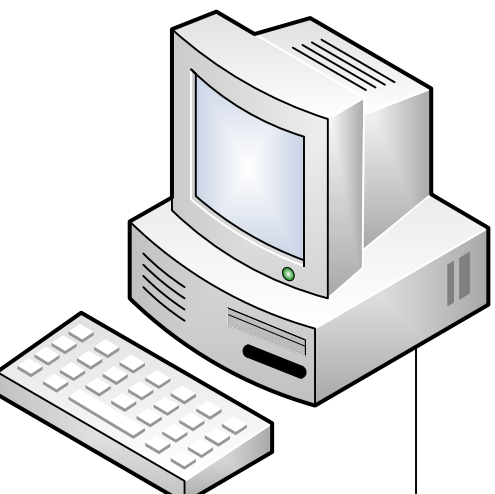




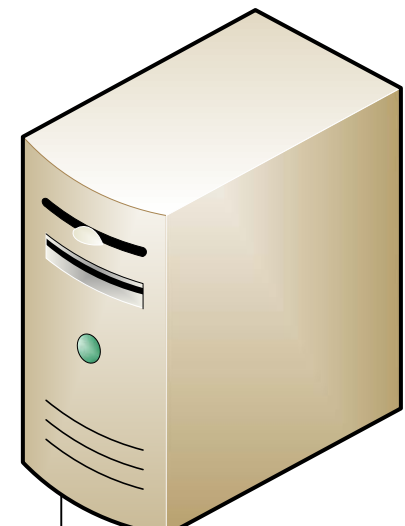
Client SSH
id_rsa (Clé privée)



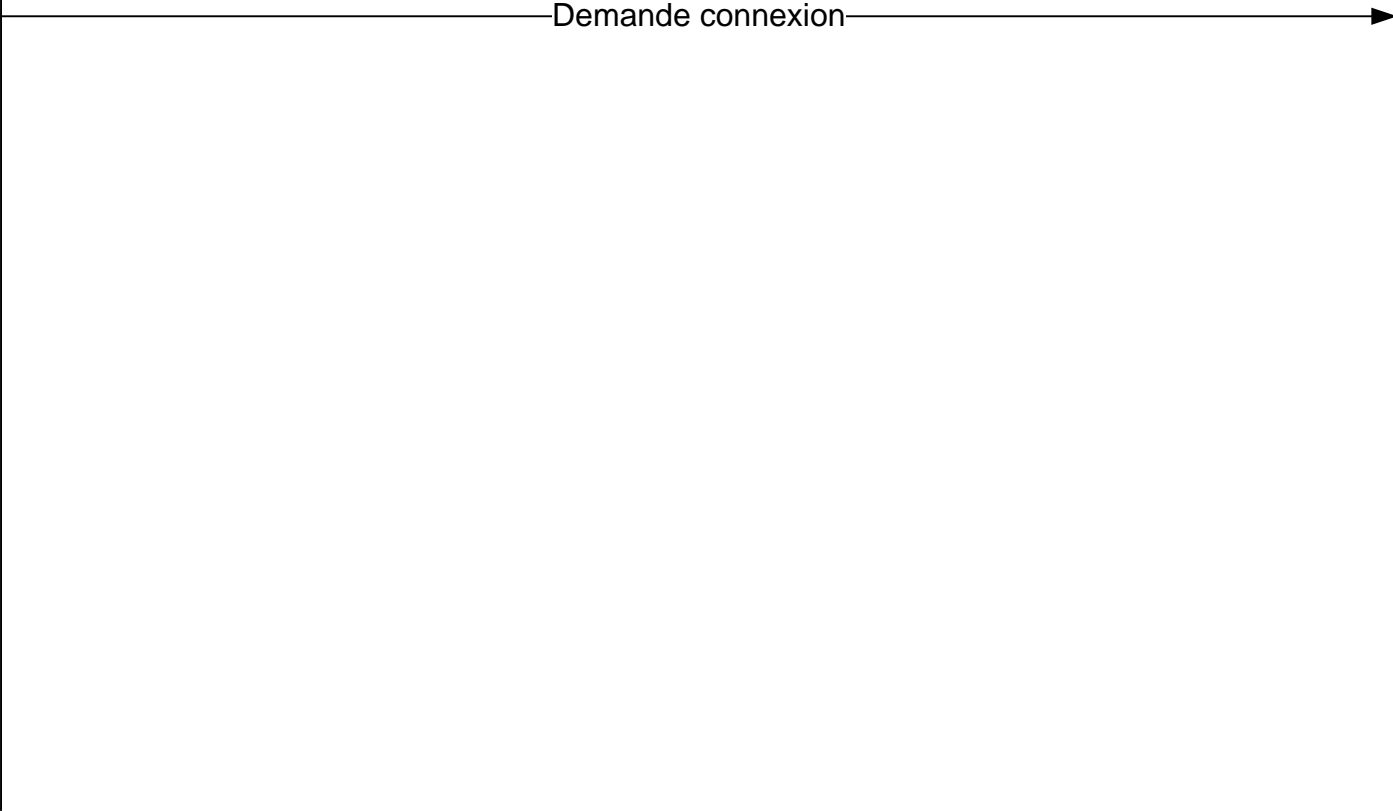
Serveur ssh
Authorized_keys (Clé publique)



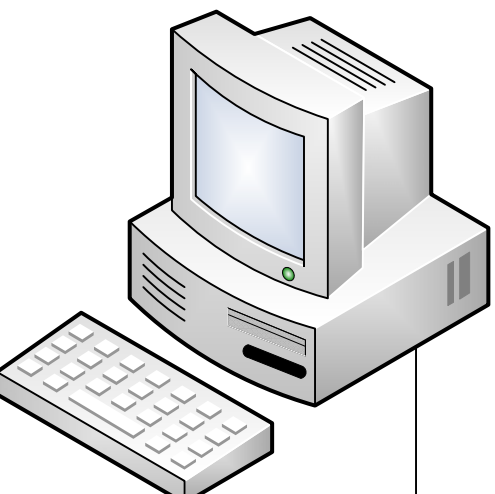
Client SSH
id_rsa (Clé privée)



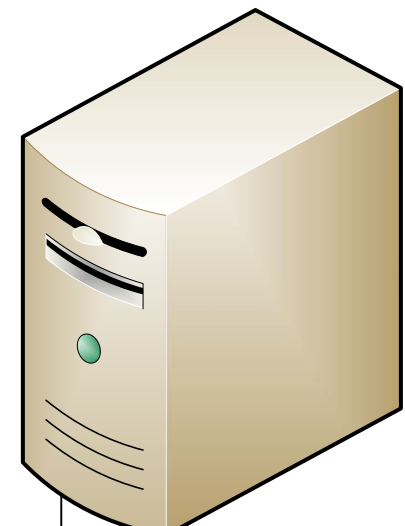
Serveur ssh
Authorized_keys (Clé publique)



Demande connexion



Client SSH
id_rsa (Clé privée)



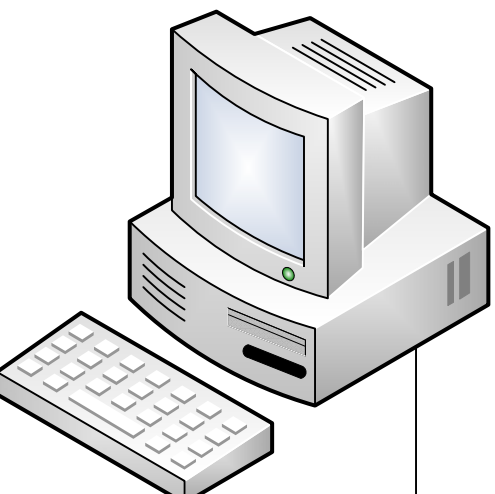
Serveur ssh
Authorized_keys (Clé publique)



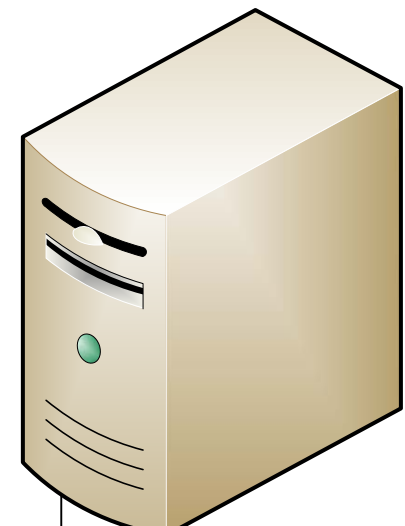
Demande connexion

Challenge : message secret chiffré par clé publique

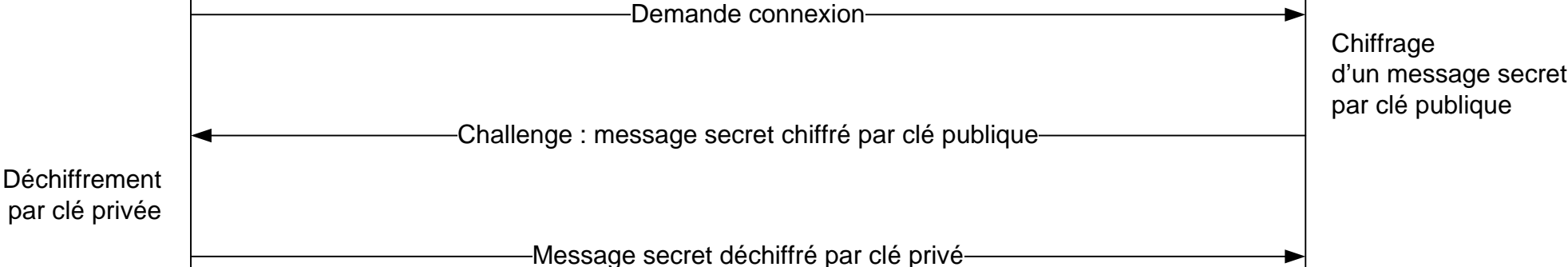
Chiffage
d'un message secret
par clé publique

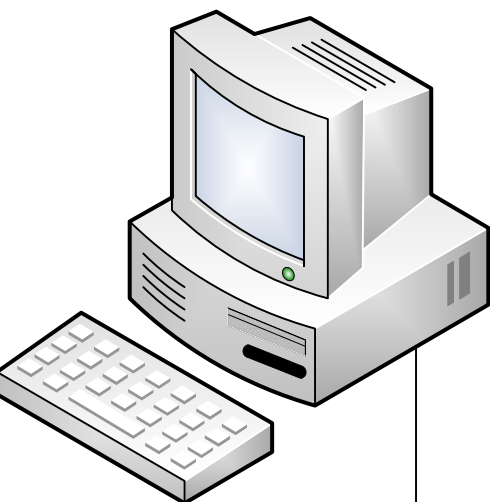


Client SSH
id_rsa (Clé privée)

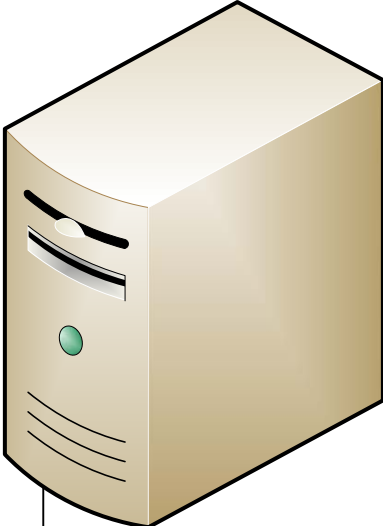


Serveur ssh
Authorized_keys (Clé publique)

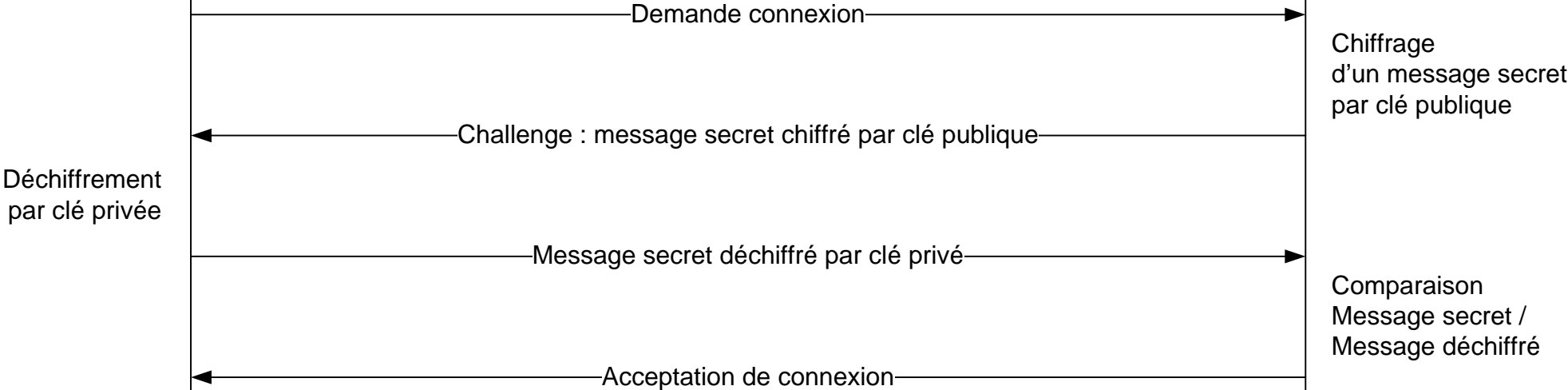


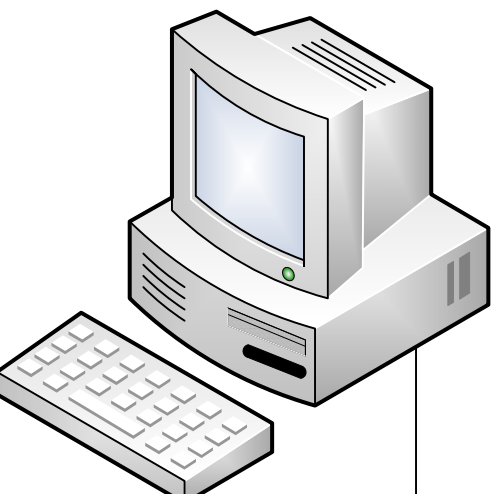


Client SSH
id_rsa (Clé privée)

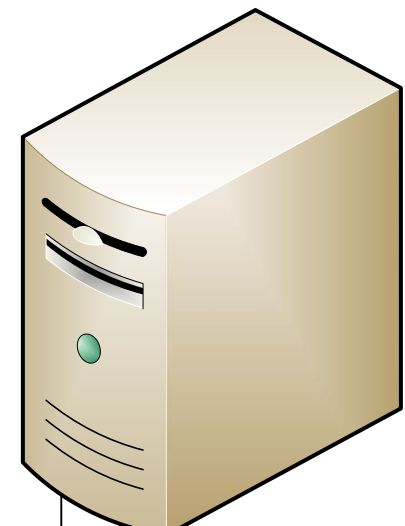


Serveur ssh
Authorized_keys (Clé publique)





Client SSH
id_rsa (Clé privée)



Serveur ssh
Authorized_keys (Clé publique)

