# Diagramme de séquence de l'établissement d'une session SSH

<uml> @startuml group Etablissement d'une session 3-Way Handshake ClientSSH → Serveur : demande session avec paquet SYN (Synchronize) Serveur → ClientSSH : approuve connexion avec paquet SYN-ACK (acknowledgement) ClientSSH → Serveur : confirme avec paquet ACK end group Negociation des algorithmes de chghffrement ClientSSH → ClientSSH : annonce la version de SSH utilisée Serveur → ClientSSH : annonce la version de SSH utilisée ClientSSH → Serveur : Key Exchange Init (liste des algorithmes supportés) Serveur → ClientSSH : Key Exchange Init (liste des algorithmes supportés)

Serveur → ClientSSH : certificat ClientSSH → ClientSSH : vérification certificat & empreinte end group Partage clé secrète ClientSSH → Serveur : liste d'algorithmes de chiffrement Serveur → ClientSSH : liste d'algorithmes de chiffrement ClientSSH → ClientSSH : choix algorithme Serveur → Serveur : choix algorithme ClientSSH → ClientSSH : génèrent des paires de clés \n publiques-privées temporaires ClientSSH → ClientSSH : génére cle de session end @enduml </uml>