SSH et SCP :

SSH généralités :

C'est un protocole qui permet de se connecter à une machine distante. Il remplace le protocole Telnet.

Il est décrit dans plusieurs RFCs.
RFC 4250, RFC 4251, RFC 4252, RFC 4253, RFC 4254.

Il utilise le protocole de transport TCP sur le port 22.
Il utilise des clés public/private pour authentifier le client.
Il est aussi possible de s'authentifier avec un mot de passe mais ceci n'est pas recommandé car moins sécurisé.
Il peut aussi être utilisé pour copier des fichiers depuis/vers une machine distante avec SCP.
SSH est aussi le nom du logiciel qui implemente le protocole SSH. Il est considéré comme standard.

Empreinte digitale de la clé SSH :

L'empreinte digitale de la clé SSH est un hash de la clé publique. Il est utilisé pour identifier une clé publique.

L'empreinte digitale de la clé s'affiche lorsque la clé est générée et lorsque elle est utilisée pour se connecter à une machine distante.

L'empreinte permet de vérifier que la clé publique est la même que la clé utilisée pour se connecter à la machine distante.

Permet d'aider à détecter en attaque Man in the midle.

Les clés publiques sont stockées dans le fichier ~/.ssh/known_hosts, ce fichier contient l'empreinte de la clé et le nom d'hôte de la machine distante.

Génération de clé SSH :

Pour générer un clé utiliser la commande : ssh-keygen
La commande va générer une paire de clés, une publique et une privée.
Par defaut la paire est générée dans le répertoire ~/.ssh la clé privée dans le fichier ~/.ssh/ckeys et la clé publique dans le fichier ~/.ssh/ckeys.pub.
Clé publique → peut être partagée avec tout le monde.
Clé privée → doit absolument rester secrète.
Une phrase secrète peut être utilisée pour chiffrer la clé privée. La phrase doit être utilisée à chaque utilisation de la clé privée.

SCP généralités :

SCP est un protocole qui permet de copier des fichiers depuis/vers une machine distante.
Il remplace le protocole FTP.
Il s'appuie sur le protocole SSH pour l'authentification du client.
Il est une illustration de l'architecture client/serveur utilisant le protocole SSH.