L’empreinte numérique (hash)

Séquence de caractères alphanumériques de longueur fixe, qui représente le contenu d'un message, sans le révéler, dont la valeur unique est produite par un algorithme de hachage, et qu'on utilise pour créer une signature numérique.

Une empreinte numérique est réalisée par une fonction mathématique « à sens unique ». La fonction réalise un condensé (hash) du fichier et la moindre modification du fichier conduira à une grande modification de l’empreinte.

On ne peut pas retrouver le fichier depuis son empreinte.

Plus la taille du condensé est grande, moins il est facile de trouver d’en trouver des identiques (collisions)

Principaux algorithmes de hash :

- SHA1 (160 bits)
- MD5 (128 bits)
- SHA2 (SHA-256, SHA-384 ou SHA-512 bits au choix)

L’empreinte numérique

Utilisations :

- L’empreinte numérique est utilisée pour le stockage des mots de passe.
  - echo "Toto" | md5sum → 08387f861dcfdcbfb01592929b7280cc
  - echo "Toti" | md5sum → f1427db7ae92b32b70d7cef8d0f40438

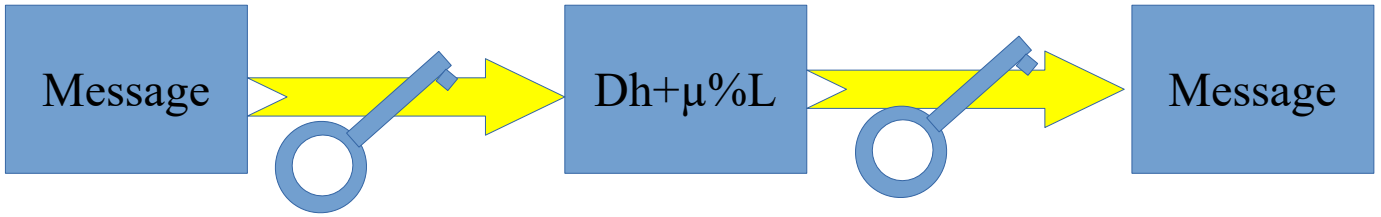
  Le condensat d’un MDP peut être stocké dans une base de comptes. Quand un utilisateur saisit son MDP pour s’authentifier, le condensat de celui-ci est calculé et comparé à celui présent dans la base
- Validation de l’intégrité des fichiers lors des transferts

Le salage :

- Le stockage sous forme de hash est très sensible aux attaques par les « rainbow tables » (base de données de hash pré-calculés). Pour contrer cette attaque une constante connue est ajoutée avant hashage.

Le chiffrement symétrique

Une même « clé » sert à chiffrer et à déchiffrer

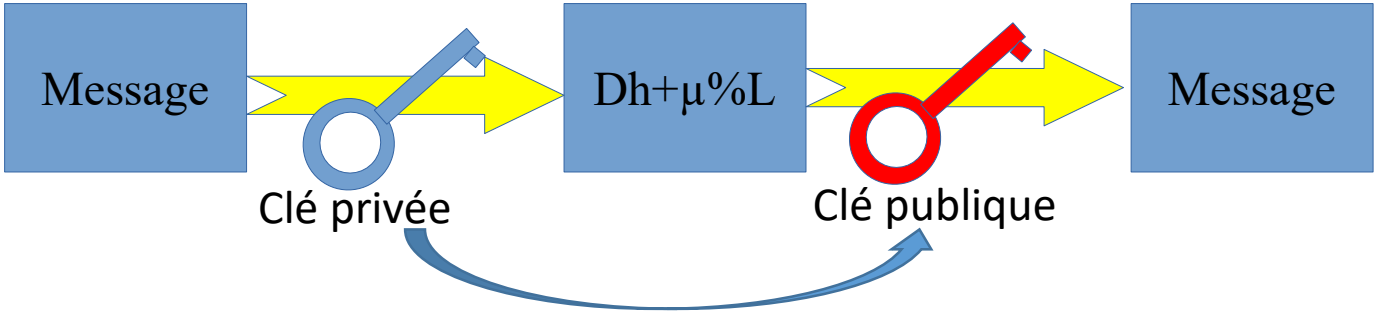


- Le principal avantage est sa rapidité car le chiffrement symétrique est « informatiquement » simple.
- Le principal inconvénient est qu'il faut diffuser la clé unique de façon fiable … sinon le chiffrement n'a aucune valeur
- Plus la clé est longue plus le chiffrement est sûr
- Principaux algorithmes :
  - AES
  - Blowfish
  - DES, Triple DES
  - Twofish

Le chiffrement asymétrique

Un couple de clés liées est généré.

- Une clé est dite « privée » (elle sera gardée secrète)
- Une clé est dite « publique » (elle sera diffusée)



- Le principal avantage est qu'il est maintenant très simple de diffuser la clé (publique).
- Le principal inconvénient est que les calculs mathématiques sont plus lourds donc plus lents.
- Principaux algorithmes :
  - RSA (le plus utilisé)
  - Cryptosystème de ElGamal
  - Cryptosystème de Merkle-Hellman

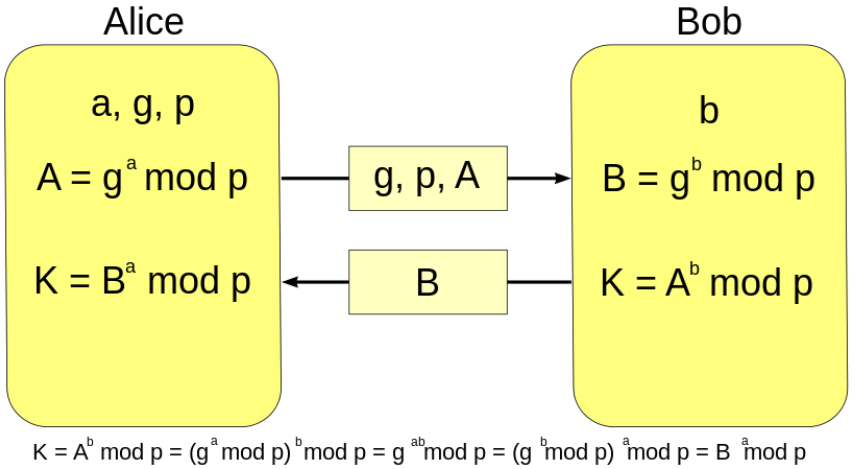
Échange de clés Diffie-Hellman (DH)

La technique, du nom de ses inventeurs, est basée sur l'échange d'informations qui vont permettre de constituer un secret (clé) commun sur un canal non chiffré. Elle est basée sur des propriétés mathématiques qui rendent les calculs réciproques impossibles.

La clé échangée sert ensuite pour du chiffrement symétrique beaucoup plus rapide

- Technique utilisée par TLS et SSH, ...

Exemple pratique :
Alice choisit un nombre premier **p** et une base **g**. Dans notre exemple, ***p=23* et *g=3***
Alice choisit un nombre secret ***a=6***
Elle envoie à Bob la valeur
$A = g^a \text{ [mod p]} = 3^6 \text{ [23]} = \mathbf{16}$
Bob choisit à son tour un nombre secret ***b=15***
Bob envoie à Alice la valeur
$B = g^b \text{ [mod p]} = 3^{15} \text{ [23]} = \mathbf{12}$
Alice peut maintenant calculer la clé secrète :
$(B)a \text{ [mod p]} = 12^6 \text{ [23]} = \mathbf{9 = K}$
Bob fait de même et obtient la même clé qu'Alice :
$(A)b \text{ [mod p]} = 16^{15} \text{ [23]} = \mathbf{9 = K}$



Dans la pratique **p** est un nombre premier de 300 chiffres et **a** et **b** de l'ordre de 100 chiffres.
Le modulo est le reste de la division entière.

Introduction aux certificats

Objectifs :

- la non-répudiation de documents (signature électronique)
- l'intégrité des données
- la confidentialité
- l'authentification forte d'un individu ou d'une identité numérique (URL).

Un certificat électronique est un fichier de données contenant :

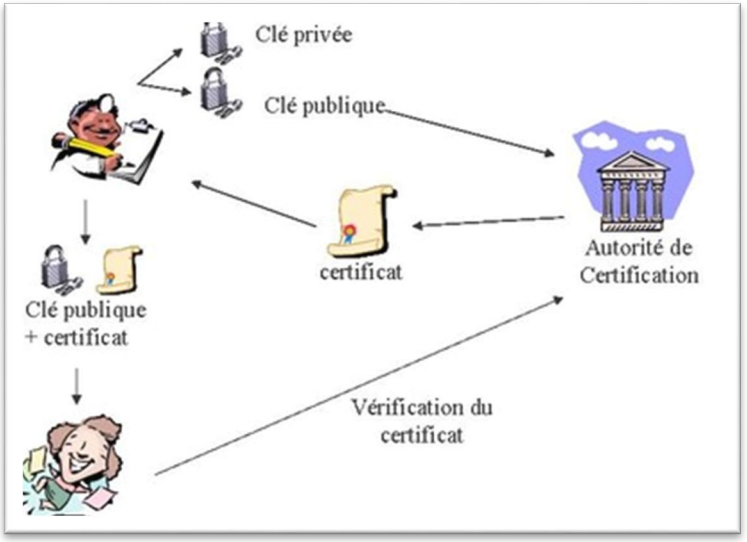
- une clé publique
- des informations d'identification (nom, localisation…)
- des informations complémentaires (mel …)
- le tout est signé par une « racine »

Les certificats électroniques ont un cycle de vie: ils ne sont valides que pour une durée déterminée. La révocation avant la fin est possible.

Introduction aux certificats

Principe :

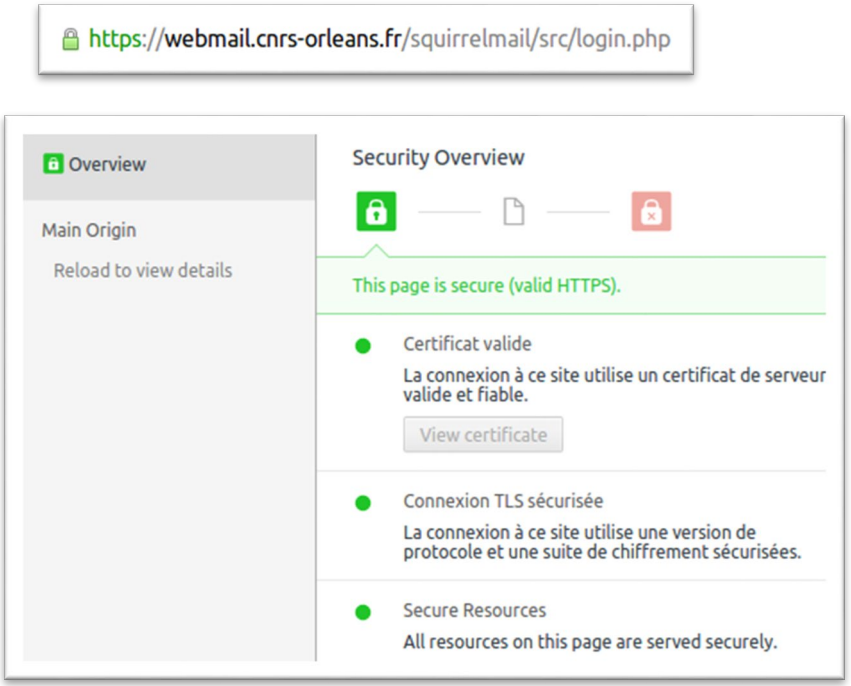
- Le concept de certificat est basé sur une organisation qui atteste que le certificat est valide. Cette organisation est une Infrastructure de Gestion des Clés (IGC ou PKI).
- Cette organisation n'est pas « qu'informatique » : il y a aussi des procédures humaines (par ex. : « *téléphoner au demandeur avant de valider la demande »)*

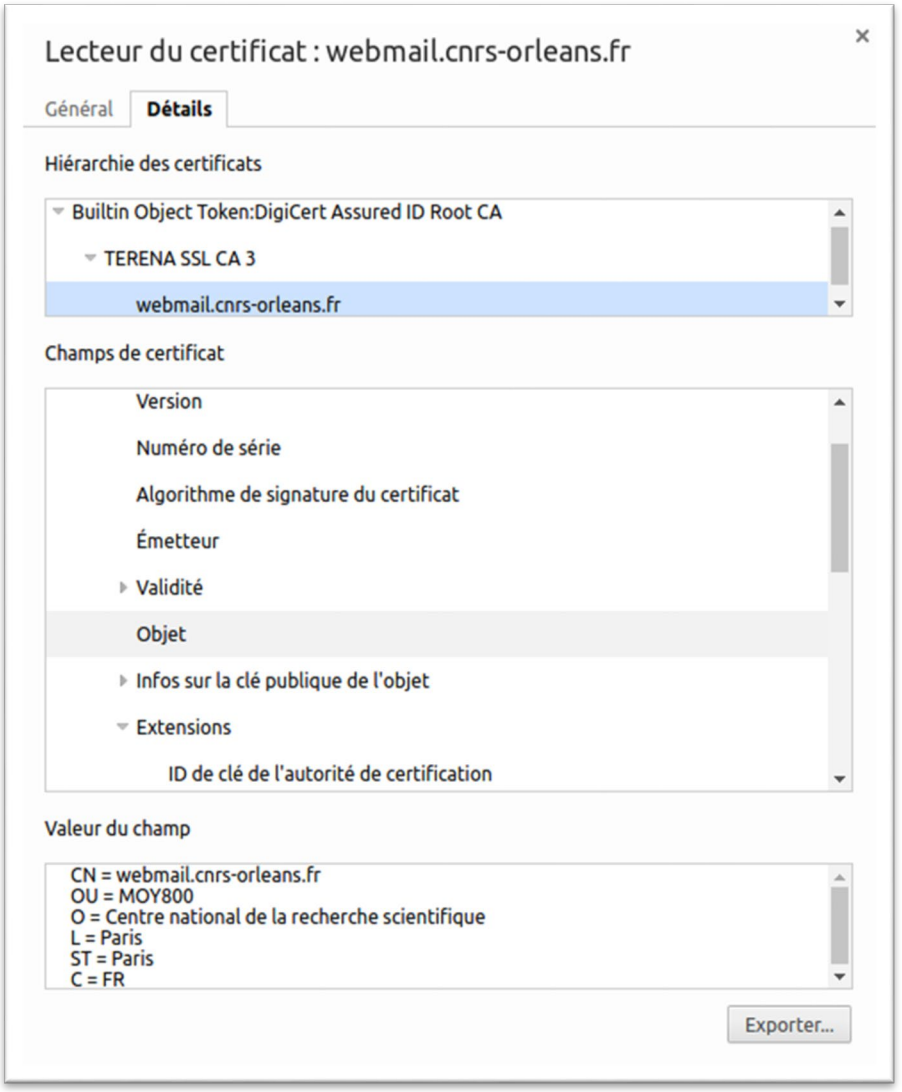


Les certificats auto-signés sont utilisés à des fins de tests ou juste pour assurer le chiffrement mais ils ne peuvent pas authentifier n'ayant aucun garant.

Introduction aux certificats

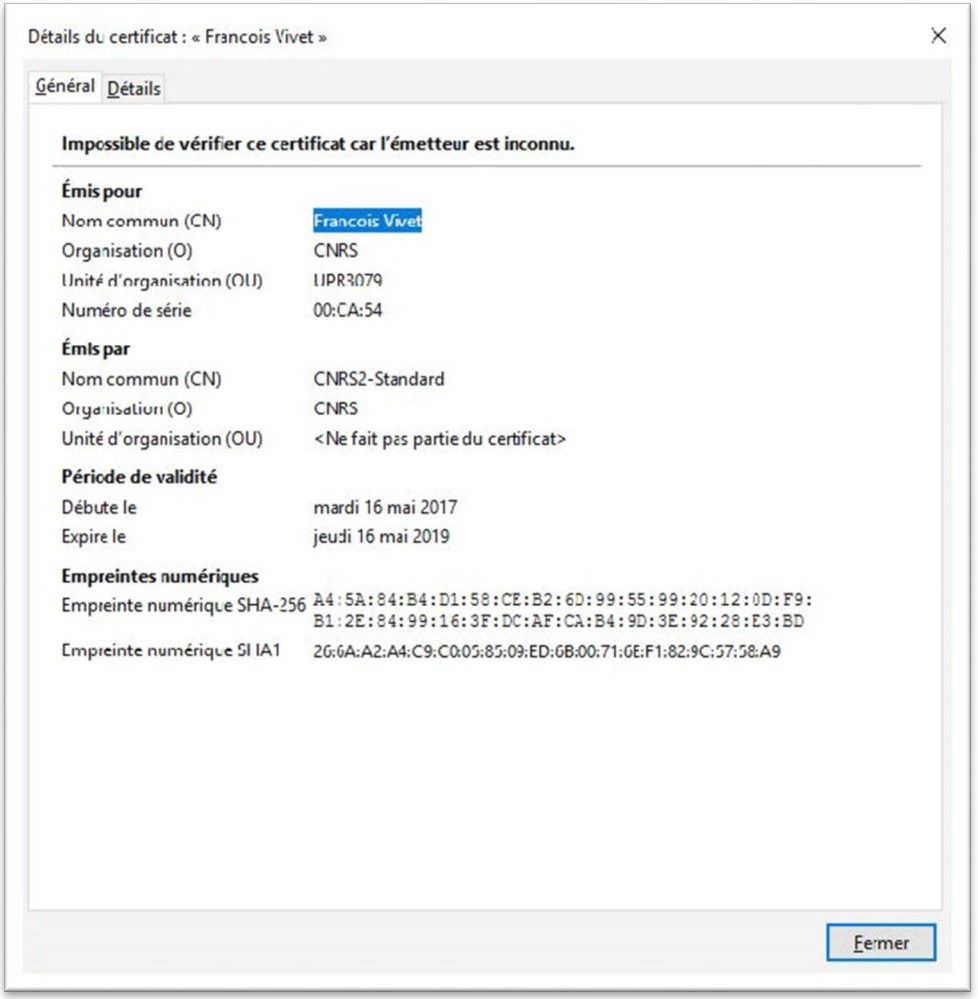
Exemple : Certificat sur une URL

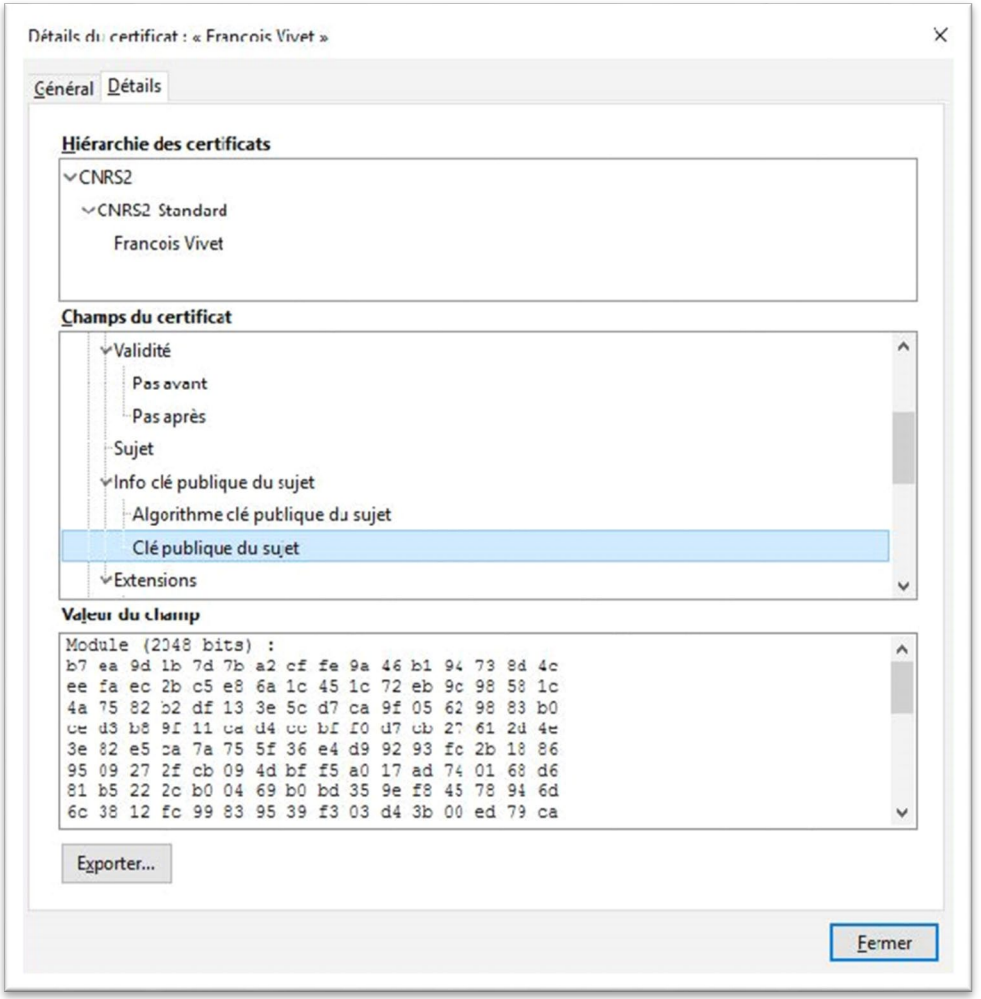




Introduction aux certificats

Exemple : Certificat Utilisateur





SSH - Généralités

SSH (Secure Shell – Ligne de commande sécurisée) est un protocole qui permet de chiffrer les communications entre deux ordinateurs. SSH est aussi le nom de l'offre logicielle qui implémente le protocole.

Le protocole SSH a été conçu avec l'objectif de remplacer les différents protocoles non chiffrés (telnet,rlogin, rshell,…).

SSH-2 a été défini en 2006 par l'IETF (SSH-1 était d'initiative privée). C'est la version aujourd'hui utilisée dans les systèmes modernes.

Une connexion SSH est faite entre un serveur et un client ssh sur le port TCP 22.

Il est principalement pour ouvrir un shell sur une machine distante. Il est possible de « rebondir » vers une autre machine.

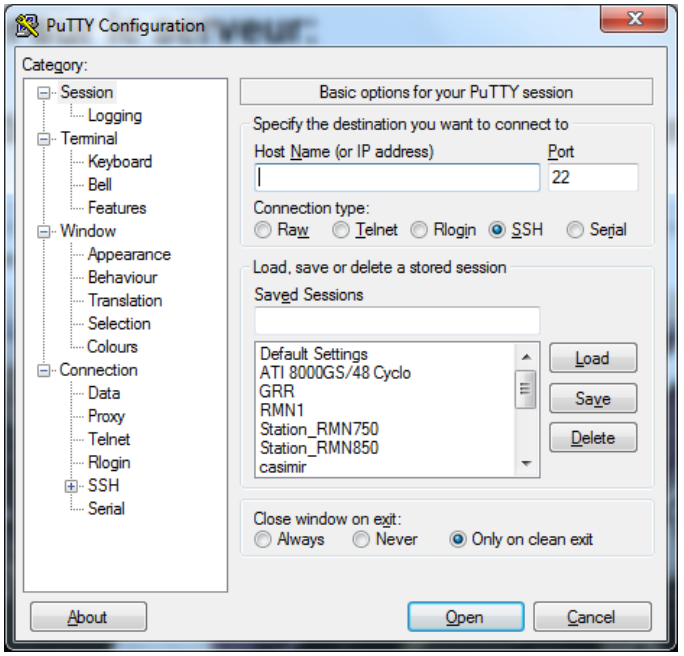
SSH - Connexion

Avec une invite de commande :

#ssh login@machinedistance

puis indiquer le MDP à l'invite

Sous Windows, on pourra utiliser le client PuTTY



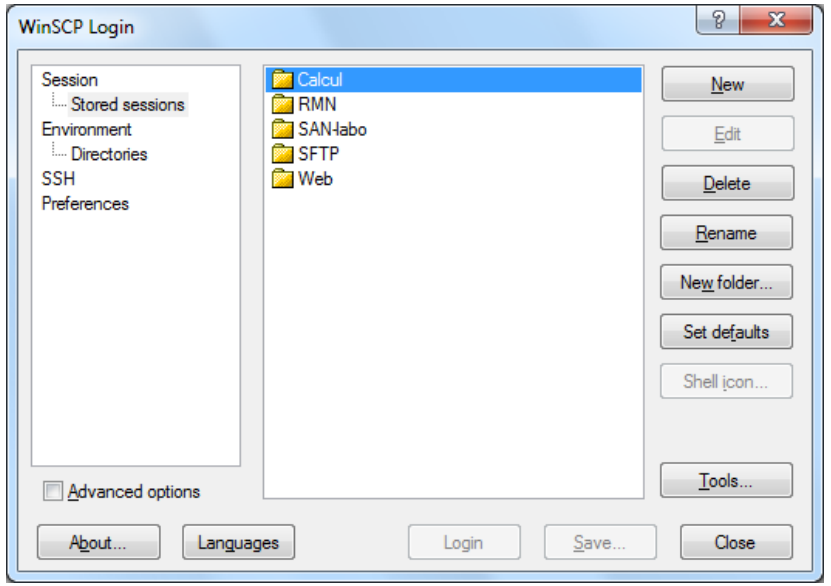
SSH – Copie de fichiers

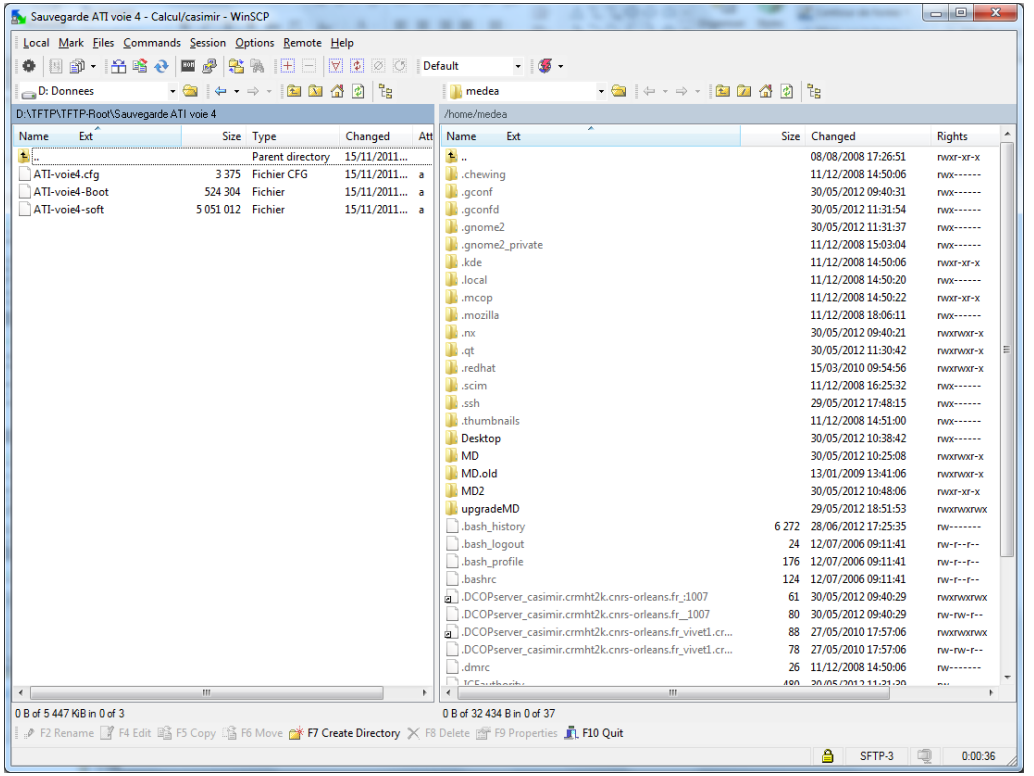
Il existe une fonction de copie de fichier sous SSH : scp (Secure Copy)

#scp fichier1 fichier2 fichier3 serveurdistant

Copie des fichiers à partir de la machine cliente vers le serveur

Sous Windows, on pourra utiliser le logiciel client WinSCP





SSH – Les sécurités

SSH utilise plusieurs mécanismes pour sécuriser la liaison:

- Enregistrement sur le client de la clé publique du serveur pour limiter les risques d'attaque « Man in the middle » : **phase d'ouverture de communication**

  Possibilité de durcir cette méthode avec l'utilisation de certificats serveurs.

- Chiffrement hybride de la connexion :

  Suite au partage d'un secret D.H., un chiffrement symétrique est mis en place

- Validation du login/mot de passe de l'utilisateur : **phase d'authentification**

  Possibilité d'utiliser une clé asymétrique (plus besoin de login/mdp, clé secrète protégée par MDP sur le poste à partir duquel on se connecte)

sshd_config – Le fichier de configuration
exemples de directives de configuration

Pour autoriser l'authentification par mot de passe (l'un ou l'autre)

PasswordAuthentication yes

Pour forcer l'authentification par clés

PasswordAuthentication no

Désactivation de l'accès direct en root

Il est possible d'interdire la connexion avec le compte root.

PermitRootLogin no

Si vous disposez de plusieurs interfaces réseaux sur votre serveur, mais que vous ne voulez qu'on puisse ce connecter en ssh

que d'une seule interface.

ListenAddress 192.168.0.10

Liste des comptes utilisateurs accessibles a distance par le "ssh"

AllowUsers xavier@192.168.1.10, bob

Match est une condition pour la(es) commande(s) suivante(s), ici si le user rambo se connecte depuis l'iP 192.168.1.22 il peut
faire du X11

Match User rambo Address 192.168.1.22
X11Forwarding yes

sshd_config – le fichier de configuration

Une fois le fichier de configuration validé :

#systemctl restart sshd

Puis

#systemctl status sshd

Tous les détails de la configuration dans :

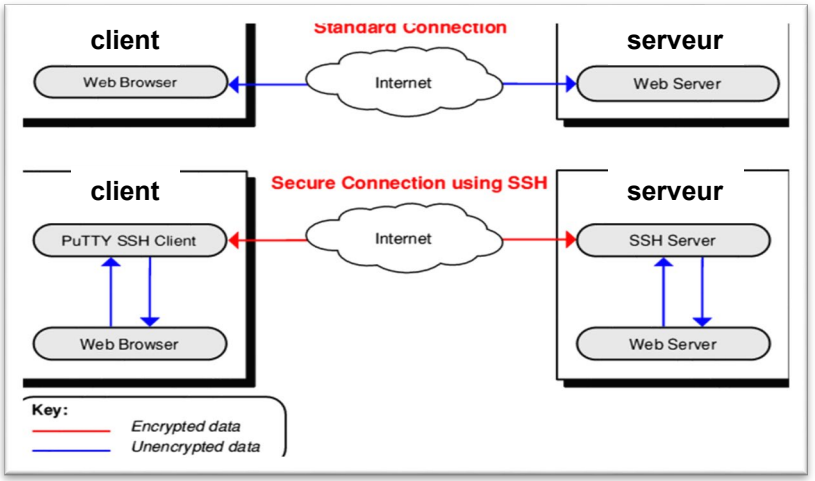
man sshd_config

Ou sur https://www.openssh.com/

sshd – Les tunnels

L'idée est de « transférer » un port distant et un port local dans une session sécurisée par SSH. On obtient alors une encapsulation d'un protocole dans SSH.
On donne l'image d'un tunnel car de l'extérieur on ne sait pas se qui passe dans la session.

Port TCP local 8000



Port TCP distant 80

Dans l'exemple suivant, le port 80 du serveur WEB distant est encapsulé dans SSH et il est accessible au client par le port 8000 local.

Commande exécutée sur le client :

#ssh -L port_machine_A:localhost:port_machine_B machine_B -f -N

#ssh -L 8000:127.0.0.1:80 IP_serveur -f -N

SSL/TLS – Le protocole

Secure Sockets Layer est devenu Transport Layer Security

Protocole défini par les RFC 2246, RFC 4347 et RFC 5246

Fonctionnement :

- Le client se connecte au serveur
- Le serveur renvoie un certificat au client, contenant sa clé publique
- Le client vérifie la validité du certificat (Autorité émettrice connue ?)
- Le client crée une clé secrète aléatoire puis la chiffre avec la clé
- publique du serveur et la lui envoie
- Le serveur déchiffre cette clé secrète avec sa clé privée
- Client et serveur ont alors cette clé secrète (=clé de session) en commun

SSL/TLS – Le protocole

- TLS crée un tunnel de connexion chiffré point à point client – serveur
- TLS est indépendant des autres protocoles (HTTP, FTP, …)
- TLS est une couche supplémentaire qui se situe entre la couche application et la couche transport
- TLS est transparent pour l'utilisateur
- Ce qui est échangé sous TLS est invisible pour un pare-feu, un antivirus…

- SSL n'est plus pris en charge par les navigateurs modernes ainsi que les versions TLS antérieures à 1.2 ➔ Message de connexion non sécurisée

SFTP – SSH+FTP

SFTP permet de transférer des données dès lors que SSH est installé

SFTP est plus ou moins similaire à SCP. Ne pas confondre avec FTPS

Penser à isoler les comptes : Ceux-ci ne peuvent accéder qu'à un répertoire de la machine (le répertoire de dépôt des fichiers du serveur SFTP, par ex.) ➔ On parle de comptes chrootés

Un exemple de client supportant SFTP: Filezilla

FTPS – FTP+SSL/TLS

FTPS : FTP sécurisé avec SSL/TLS

2 modes de chiffrement:

- explicite : connexion en clair (échange login+mdp en clair)
- implicite : chiffrement dès la phase de connexion

Permet d'exiger l'utilisation d'un certificat pour sécuriser la communication

Exemple de serveur FTPS Windows : FileZilla server

Exemple de serveur FTPS Linux : vsftpd (very secure FTP Daemon)

Terminologie

Chiffrement : procédé pour rendre incompréhensible un document à toute personne ne possédant pas la clé de déchiffrement

Déchiffrement : procédé rendant compréhensible à l'aide d'une clé de déchiffrement un document chiffré avec une clé de chiffrement

Décrypter : procédé consistant à essayer de rendre compréhensible un message chiffré sans posséder la clé de déchiffrement

Crypter et cryptage sont des usages abusifs, qui n'existent pas, de même qu'encrypter (du mot anglais « encryption »)