

# JOB 1

La commande permettant d'accéder au manuel d'une commande est : **man nom-de-la-commande**

Ici, c'est donc : **man ls**

```
jerome@LAPTOP-5BDRT0NR:~$ man ls
```

La commande permettant d'afficher les fichiers cachés du home de votre utilisateur est : **ls -a**  
**/home/jerome**

Mais ici je tape juste **ls -a** car je suis déjà sur ce chemin

```
jerome@LAPTOP-5BDRT0NR:~$ ls -a
.      .bashrc  Documents  .mozilla  Public
..     Bureau  Images     Musique   Téléchargements
.bash_history  .cache  .local    .pki      Vidéos
.bash_logout  .config Modèles   .profile
```

La commande permettant d'afficher les fichiers cachés plus les informations sur les droits sous forme de liste est : **ls -la**

```
jerome@LAPTOP-5BDRT0NR:~$ ls -la
total 76
drwxr-xr-x 15 jerome jerome 4096 2 oct. 22:54 .
drwxr-xr-x  3 root  root  4096 2 oct. 22:05 ..
-rw-r----- 1 jerome jerome 1216 2 oct. 23:26 .bash_history
-rw-r--r--  1 jerome jerome  220 2 oct. 22:05 .bash_logout
-rw-r--r--  1 jerome jerome 3526 2 oct. 22:05 .bashrc
drwxr-xr-x  2 jerome jerome 4096 2 oct. 22:25 Bureau
drwx----- 13 jerome jerome 4096 3 oct. 10:13 .cache
drwx----- 12 jerome jerome 4096 3 oct. 09:58 .config
drwxr-xr-x  2 jerome jerome 4096 2 oct. 22:25 Documents
drwxr-xr-x  2 jerome jerome 4096 3 oct. 10:15 Images
drwxr-xr-x  3 jerome jerome 4096 2 oct. 22:25 .local
drwxr-xr-x  2 jerome jerome 4096 2 oct. 22:25 Modèles
drwx-----  4 jerome jerome 4096 2 oct. 22:27 .mozilla
drwxr-xr-x  2 jerome jerome 4096 2 oct. 22:25 Musique
drwx-----  3 jerome jerome 4096 2 oct. 22:54 .pki
-rw-r--r--  1 jerome jerome  807 2 oct. 22:05 .profile
drwxr-xr-x  2 jerome jerome 4096 2 oct. 22:25 Public
drwxr-xr-x  2 jerome jerome 4096 2 oct. 22:32 Téléchargements
drwxr-xr-x  2 jerome jerome 4096 2 oct. 22:25 Vidéos
```

Pour ajouter des options à une commande on doit mettre le nom de la commande; puis : - suivi de l'abréviation de l'option ou -- suivi de l'option tapé cette fois-ci en entier. De plus, on peut compiler les options en tapant les abréviations les une à la suite des autres.

Voici quelques exemples d'options :

- a, --all**  
inclure les entrées débutant par « . »
- l**  
utiliser un format d'affichage long
- s, --size**  
afficher la taille allouée de chaque fichier en nombre de blocs

## JOB 2

La commande qui permet seulement de lire un fichier est : **cat nom\_du\_fichier** ou **cat /chemin/nom\_du\_fichier**

La commande qui permet d’afficher les 10 premières lignes du fichier “.bashrc” est : **head -n 10 .bashrc**

```
jerome@LAPTOP-5BDRT0NR:~$ head -n 10 .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
    *) return;;
esac
```

La commande qui permet d’afficher les 10 dernières lignes du fichier “.bashrc” est : **tail -n 10 .bashrc**

```
jerome@LAPTOP-5BDRT0NR:~$ tail -n 10 .bashrc
# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
    if [ -f /usr/share/bash-completion/bash_completion ]; then
        . /usr/share/bash-completion/bash_completion
    elif [ -f /etc/bash_completion ]; then
        . /etc/bash_completion
    fi
fi
```

La commande qui permet d’afficher les 20 premières lignes du fichier “.bashrc” est : **head -n 20 .bashrc**

```
jerome@LAPTOP-5BDRT0NR:~$ head -n 20 .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
    *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000
```

La commande qui permet d’afficher les 20 dernières lignes du fichier “.bashrc” est : **tail -n 20 .bashrc**

```
jerome@LAPTOP-5BDRT0NR:~$ tail -n 20 .bashrc

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
    if [ -f /usr/share/bash-completion/bash_completion ]; then
        . /usr/share/bash-completion/bash_completion
    elif [ -f /etc/bash_completion ]; then
        . /etc/bash_completion
    fi
fi
```

# JOB 3

La commande pour installer le paquet “cmatrix” est : **sudo apt-get install cmatrix**

```
jerome@LAPTOP-5BDRT0NR:~$ sudo apt-get install cmatrix
[sudo] Mot de passe de jerome :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Paquets suggérés :
  cmatrix-xfont
Les NOUVEAUX paquets suivants seront installés :
  cmatrix
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 17,5 ko dans les archives.
Après cette opération, 53,2 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 cmatrix amd64 2.0-3 [17,5 kB]
17,5 ko réceptionnés en 0s (274 ko/s)
Sélection du paquet cmatrix précédemment désélectionné.
(Lecture de la base de données... 140158 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../cmatrix_2.0-3_amd64.deb ...
Dépaquetage de cmatrix (2.0-3) ...
Paramétrage de cmatrix (2.0-3) ...
Traitement des actions différées (« triggers ») pour mailcap (3.69) ...
Traitement des actions différées (« triggers ») pour desktop-file-utils (0.26-1) ...
Traitement des actions différées (« triggers ») pour gnome-menus (3.36.0-1) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
```

La commande pour lancer le paquet “cmatrix” est : **cmatrix**

Pour quitter cet écran, on tape soit ctrl+c ou q

```

H F      =      R 7      N O e 6 T s s      S N < T x , = %
"      F n G      T 3 [ o l h % 9 z 7 0 ?      V o . m ? % @
F      L Y =      @ n g - I l 4 ] p m I      r U E $ 5 #
T      x & 0 Y      z 4 P V g 9 1 \ 1 ? M      N e L      x =
X      '      l . B q      W ] ] t s [ D @ > r n      @ z      * X
G      2 6 2 D      9 * e j h q F , T k      h      z '
D *      > Y w t      - & f ^ x / I      i M Y      8 D
J x      L z J M u      : g q L t 0 j r S      4 * F      x s
S P      b g \ g l      - t k N G n n A ] / o R      1
X Q      W G .      0 w      ' = @ r B M g 3      7 1 A      8
\ a      T W 4 e      y m s E V - E D k > G m      6      q
h x      I n C ] 4 \ N      : F B W      0 V f      B z N      j      g v H
U ?      p + S : Z H X      + c K      5 9 \      z b R e      Y      1 i 9
0 C      - > N L d      F t I ) T      7 V 3 4 f A 0 A 0      S      d ] J
B \      S * m 0 ] / x v      ^ # 8      5 T      D ' a j S      ^ = i      e 5 b
X      + D X @ i : 0 "      h "      " h m - # Z E l )      0      [ 9 I 3
w      j : ) \      Z n R      \ *      Z f ) * ] T      H J 5      r 7 V =
]      0 v @ 0      l < e      N      \      F p ) 3      .      t ? \      d j e ]
1 ^      K v      a g s N      M 3 g      i g      e u D      > ] Z /
& b      i 2 m      j A o      g ] x @ V 0      4 f      @ \ a s
k      T C      ]      0 @ R      <      r 8      3 t j      t      a 7      . m 3
" S G f      )      K v e      &      : B l )      #      d e      & L ^
l      v      P      i      1 2 l      0 3      0 3      H      i      /      5 b      H C
```

La commande permettant de mettre à jour son gestionnaire de paquets est : **sudo apt-get upgrade**

```
jerome@LAPTOP-5BDRT0NR:~$ sudo apt-get upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

La commande permettant de mettre à jour les logiciels est : **sudo apt-get update**

```
jerome@LAPTOP-5BDRT0NR:~$ sudo apt-get update
```

La commande pour redémarrer est : **sudo shutdown -r now**

```
jerome@LAPTOP-5BDRT0NR:~$ sudo shutdown -r now
```

La commande pour éteindre est : **sudo shutdown -h now**

```
jerome@LAPTOP-5BDRT0NR:~$ sudo shutdown -h now
```

# JOB 4

Pour créer un fichier users.txt en ligne de commande c'est : **touch users.txt**

Puis **nano users.txt** et taper User1 et User2 séparé par un retour à la ligne

La commande pour créer un groupe "Plateformeurs" est : **sudo groupadd Plateformeurs**

La commande pour créer un utilisateur appelé "User1" est : **sudo useradd User1**

La commande pour créer un utilisateur appelé "User2" est : **sudo useradd User2**

La commande pour ajouter "User2" au groupe Plateformeurs est : **sudo usermod -aG Plateformeurs User2**

Pour copier "users.txt" dans le fichier "droits.txt", je créer le fichier destinataire grâce à la commande **touch**. Puis je tape la commande : **cp user.txt droits.txt**

Pour copier "users.txt" dans le fichier "groupes.txt", je créer le fichier destinataire grâce à la commande **touch**. Puis je tape la commande : **cp user.txt groupes.txt**

La commande pour changer le propriétaire du fichier "droits.txt" pour mettre "User1" est : **sudo chown User1 droits.txt**

La commande pour changer les droits du fichier "droits.txt" pour que "User2" ai accès seulement en lecture est : **sudo chmod go=r droits.txt**

La commande pour changer les droits du fichier "groupes.txt" pour que les utilisateurs puissent accéder au fichier en lecture uniquement est : **sudo chmod a=r groupes.txt**

La commande pour changer les droits du fichier pour que le groupe "Plateformeurs" puissent y accéder en lecture/écriture. Il faut tout d'abord modifier le propriétaire du fichier grâce à la commande **sudo chown**. Ensuite il faut taper la commande : **sudo chmod g+w groupes.txt**

## JOB 5

Pour créer des alias et qu'il reste dans le temps, la commande est : **sudo nano .bash\_aliases**

Cette dernière permet d'enregistrer les alias dans un fichier

```
alias la='ls -la'
alias update='sudo apt-get update'
alias upgrade='sudo apt-get upgrade'
```

Pour créer un environnement et qu'il reste dans le temps, la commande est : **sudo nano .bashrc**

Cette dernière permet d'enregistrer l'environnement dans un fichier. Ensuite il faut taper **export USER=/home/jerom**

```
tl
export USER=/home/jerome
```

Pour mettre à jour les modifications de votre bashrc dans votre shell actuel, la commande est : **exec bash**

```
jerome@LAPTOP-5BDRT0NR:~$ exec bash
```

La commande pour afficher les variables d'environnement est : **env**

```
jerome@LAPTOP-5BDRT0NR:~$ env
SHELL=/bin/bash
SESSION_MANAGER=local/LAPTOP-5BDRT0NR:@/tmp/.ICE-unix/1352,unix/LAPTOP-5BDRT0NR:/tmp/.ICE-unix/1352
```

## JOB 6

La commande qui permet de télécharger l'archive c'est : **wget**

**<https://drive.google.com/file/d/1s9ZhRhjo0FXcBNRB5khAGK1jVxkZj6Uk/view?usp=sharing>**

La commande qui permet d'extraire la suite du devoir est : **tar -xvf 'Ghost in the Shell.tar.gz'**

# JOB 7

La commande pour créer un fichier “une\_commande.txt” avec le texte : “Je suis votre fichier texte” est : **echo "Je suis votre fichier texte"> une\_commande.txt**

La commande pour compter le nombre de lignes présentes dans le fichier de source apt et pour les enregistrer dans un fichier nommé “nb\_lignes.txt” est : **wc -l /etc/apt/sources.list > nb\_lignes.txt**

Les commandes pour afficher le contenu du fichier source apt et pour l’enregistrer dans un autre fichier appelé “save\_sources” sont : **cat /etc/apt/sources.list** et **cp /etc/apt/sources.list \$USER/save\_sources.txt**

La commande pour faire une recherche des fichiers commençant par “.” tout en cherchant le mot alias est : **grep --include=\* alias --include=\* . -rnw**

```
jerome@LAPTOP-5BDR0NR:~$ echo "Je suis votre fichier texte"> une_commande.txt | wc -l /etc/apt/sources.list > nb_lignes.txt | cat /etc/apt/sources.list | cp /etc/apt/sources.list $USER/save_sources.txt | grep --include=* alias --include=* . -rnw
./bash_history:69:alias la
./bash_history:70:sudo alias la
./bash_history:74:alias la
./bash_history:76:alias
./bash_history:80:alias
./config/google-chrome/ZxcvbnData/1/us_tv_and_film.txt:4797:alias
grep: ./config/google-chrome/OnDeviceHeadSuggestModel/20220906.473124663/cr_fr_2022-09-06_473124663_500000_index.bin: binary file matches
grep: ./config/google-chrome/Default/Favicons: binary file matches
grep: ./config/google-chrome/Default/Sessions/Tabs_13309353335010097: binary file matches
grep: ./config/google-chrome/Default/Sessions/Tabs_13309345557679986: binary file matches
grep: ./config/google-chrome/Default/Service Worker/CacheStorage/579544fd7d044171f082c9eb123588966aa57ac/18354e93-a8d5-400b-b185-c201ca130066/1c2911110d5822a3_0: binary file matches
grep: ./config/google-chrome/Default/Service Worker/CacheStorage/579544fd7d044171f082c9eb123588966aa57ac/18354e93-a8d5-400b-b185-c201ca130066/8ebf3ed2c092a7cb_0: binary file matches
grep: ./config/google-chrome/Default/Service Worker/CacheStorage/579544fd7d044171f082c9eb123588966aa57ac/18354e93-a8d5-400b-b185-c201ca130066/6d0eece089544f811_0: binary file matches
grep: ./config/google-chrome/Default/History: binary file matches
grep: ./config/google-chrome/pnacr/0.57.44.2492/_platform_specific/x86_64/pnacr_public_x86_64_pnacr_llc_nexe: binary file matches
grep: ./config/google-chrome/pnacr/0.57.44.2492/_platform_specific/x86_64/pnacr_public_x86_64_ld_nexe: binary file matches
grep: ./config/google-chrome/pnacr/0.57.44.2492/_platform_specific/x86_64/pnacr_public_x86_64_sz_nexe: binary file matches
./bash_aliases:1:alias la='ls -la'
./bash_aliases:2:alias update='sudo apt-get update'
./bash_aliases:3:alias upgrade='sudo apt-get upgrade'
grep: ./cache/google-chrome/Default/Cache/Cache_Data/b0bafee5e4f66bf3_0: binary file matches
grep: ./cache/google-chrome/Default/Cache/Cache_Data/e8151c3bc7384d1b_0: binary file matches
grep: ./cache/google-chrome/Default/Cache/Cache_Data/ef2d941de9b29291_0: binary file matches
grep: ./cache/google-chrome/Default/Cache/Cache_Data/96eabe04ebe793a7_0: binary file matches
grep: ./cache/google-chrome/Default/Code Cache/js/dc358fe5a48f9dc_0: binary file matches
grep: ./cache/google-chrome/Default/Code Cache/js/93aa4281e87d1d60_0: binary file matches
grep: ./cache/google-chrome/Default/Code Cache/js/b5abbb2833fdd3f_0: binary file matches
grep: ./cache/google-chrome/Default/Code Cache/js/f32dec6c025b6667_0: binary file matches
grep: ./cache/google-chrome/Default/Code Cache/js/e3d2ed7962257b85_0: binary file matches
grep: ./cache/google-chrome/Default/Code Cache/js/8b96a0b48db41ffe_0: binary file matches
grep: ./cache/google-chrome/Default/Code Cache/js/57d12d2e7db8a9e_0: binary file matches
grep: ./cache/mozilla/firefox/mc3dtbdc.default-esr/cache2/entries/2EDE47315BAC28BCF9360B1377B0F0936A0D2620: binary file matches
grep: ./cache/mozilla/firefox/mc3dtbdc.default-esr/cache2/entries/744FE0668DFC311B20712DB448CCB49A2500A3F: binary file matches
grep: ./cache/mozilla/firefox/mc3dtbdc.default-esr/cache2/entries/D82C842421241E654FFCA4C8C585D8DE73E2931D: binary file matches
grep: ./cache/mozilla/firefox/mc3dtbdc.default-esr/startupCache/webext.sc.124: binary file matches
grep: ./cache/gnome-software/appstream/components.xmlb: binary file matches
grep: ./cache/tracker/meta.db: binary file matches
grep: ./cache/tracker/meta.db-wal: binary file matches
./bashrc:78: alias ls='ls -color=auto'
./bashrc:79: #alias dir='dir --color=auto'
./bashrc:80: #alias vdir='vdir --color=auto'
./bashrc:82: #alias grep='grep --color=auto'
./bashrc:83: #alias fgrep='fgrep --color=auto'
./bashrc:84: #alias egrep='egrep --color=auto'
./bashrc:91:alias ll='ls -l'
./bashrc:92:alias la='ls -A'
./bashrc:93:alias l='ls -CF'
```

## Pour aller plus loin ...

La commande pour installer la commande tree est : **sudo apt-get install tree**

La commande pour lancer la commande tree en arrière-plan qui aura pour but d’afficher toute l’arborescence de notre racine en enregistrant le résultat dans un fichier “tree.save” est : **tree / -o tree.save**

Pour lancer une commande pour update nos paquets, si l’update réussit alors, je lance un upgrade de mes paquets. Si l’update échoue, mon upgrade ne se lancera pas. La commande est : **update && upgrade**

```
jerome@LAPTOP-5BDR0NR:~$ sudo apt-get install tree | tree / -o tree.save | update && upgrade
```

# JOB Bonus

La commande pour installer SSH est : **apt-get install openssh-server**

```
jerome@LAPTOP-5BDRT0NR:~$ sudo apt-get install openssh-server
[sudo] Mot de passe de jerome :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  openssh-sftp-server runit-helper
```

La commande pour générer une clé SSH est : **ssh-keygen**

```
jerome@LAPTOP-5BDRT0NR:~$ ssh-keygen
Generating public/private rsa key pair.
```

La commande pour désactiver la connexion de root au SSH est : **nano /etc/ssh/sshd\_config**

Ensuite, il faut remplacer la ligne PermitRootLogin Yes en No.

Toujours dans le même endroit, je peux modifier le port de connexion SSH. Je change le 22 en 3000. Aussi, la connexion sans mot de passe, autrement appelé connexion publique

```
#Port 3000
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin No
#StrictModes yes

#PubkeyAuthentication yes

#PasswordAuthentication no
```

Ensuite j'exécute ces commandes pour faire redémarrer ssh

```
jerome@LAPTOP-5BDRT0NR:~$ sudo service ssh restart
[sudo] Mot de passe de jerome :
jerome@LAPTOP-5BDRT0NR:~$ systemctl restart ssh
```

Pour pouvoir se connecter en ssh, la commande est : **ssh nom\_utilisateur@ip\_serveur**

L'intérêt d'utiliser SSH par rapport aux alternatives est l'utilisation du cryptage. SSH crypte l'ensemble du trafic entre un client et un serveur lors du transfert de données. Une personne effectuant des écoutes du trafic, par exemple en utilisant un programme de détection de paquets, ne pourra pas accéder aux données transmises ou les décrypter.

SSH utilise trois méthodes de cryptage : le cryptage symétrique, le cryptage asymétrique et le hachage.

Le cryptage symétrique nécessite une clé secrète, qui est utilisée pour le cryptage et pour le décryptage sur l'ensemble d'une connexion SSH. La clé symétrique est créée en utilisant un algorithme d'échange de clés agréées.

Le cryptage asymétrique nécessite deux clés différentes - une paire de clés publique-privée - pour le cryptage et le décryptage. Dans une session SSH, le cryptage asymétrique est utilisé pour installer le cryptage symétrique. Pendant la phase de cryptage symétrique, le client et le serveur créent des paires de clés temporaires et échangent la clé publique, afin de créer la clé symétrique. Le cryptage asymétrique est également utilisé pour authentifier l'identité du client pour le serveur.

La méthode de hachage convertit les données transmises en une autre valeur unique. SSH utilise le hachage pour vérifier l'authenticité des messages.

Les clés générées par SSH par défaut sont assez sécurisées, mais on peut augmenter la sécurité en changeant le nombre de bits de la clé. Par défaut elle est de 2048 bits, mais pour le protocole RSA, on peut l'augmenter jusqu'à 4096 bits.

Il existe d'autre protocole de génération de clés :

- ECDSA -> Conseillé par l'ANSSI mais a priori n'a pas la confiance de tout le monde
  - ED25519 -> le dernier arrivé et le meilleur en termes de sécu et de performance. Clés plus petites, du coup plus rapides pour chiffrer/déchiffrer.
- Seul bémol , utilisable uniquement sur des distrib récentes (ex Debian 8 minimum).

Le protocole de transfert de fichiers FTP (File Transfer Protocol), est une méthode de transfert qui existe depuis 1971. FTP échange des données en utilisant deux canaux distincts : le canal de commande pour authentifier l'utilisateur et le canal de données pour transférer les fichiers.

Cependant, ces deux canaux FTP ne sont pas chiffrés, ce qui implique que les données envoyées ont un risque d'être exploitées même s'il nécessite un nom d'utilisateur et un mot de passe pour authentifier l'accès.

Le protocole HTTP (Hyper Text Transfer Protocol) est le pilier de la communication des données. Il définit le format des messages par lesquels les navigateurs et les serveurs web communiquent et détermine comment un navigateur doit répondre à une requête.

HTTP utilise TCP (Transmission Control Protocol) comme protocole secondaire, qui est aussi un protocole apatride. Cela signifie que chaque commande est exécutée indépendamment et qu'aucune information de session n'est conservée par le destinataire.

HTTPS (Hyper Text Transfer Protocol Secure) est la version sécurisée de HTTP où les communications sont chiffrées par TLS ou SSL.



La Transport Layer Security (TLS), et son prédécesseur la Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges par réseau informatique, notamment par Internet. Le protocole SSL a été développé à l'origine par Netscape Communications Corporation pour son navigateur Web. L'organisme de normalisation Internet Engineering Task Force (IETF) en a poursuivi le développement en le rebaptisant Transport Layer Security (TLS). On parle parfois de SSL/TLS pour désigner indifféremment SSL ou TLS.

La TLS (ou SSL) fonctionne suivant un mode client-serveur. Il permet de satisfaire les objectifs de sécurité suivants : l'authentification du serveur, la confidentialité des données échangées (ou session chiffrée), l'intégrité des données échangées.

Les protocoles AS2, AS3 et AS4 sont tous des protocoles utilisés pour envoyer et sécuriser les transferts de fichiers sensibles.

AS2 est utilisé pour transmettre des données confidentielles de manière fiable sur Internet. AS2 utilise des certificats numériques et des normes de chiffrement pour protéger les informations pendant leur transit entre les systèmes et les réseaux. Les messages AS2 peuvent être compressés, signés, chiffrés et envoyés via un tunnel SSL sécurisé.

AS3 est une norme qui peut être utilisée pour transmettre pratiquement tout type de fichier. AS3 fournit un niveau de sécurité supplémentaire lors de la transmission des données grâce aux signatures numériques et au chiffrement des données. Elle a été créée à l'origine pour transférer des fichiers de données de type XML et EDI. Contrairement à AS2, qui est un protocole de transfert défini, AS3 est une norme de message et se concentre sur la manière dont un message doit être formaté lors de sa transmission de serveur à serveur. Une fois qu'un message AS3 a été composé, il peut être transmis via tout autre protocole (FTP, SFTP, HTTPS, etc.) pour autant que les deux parties puissent accéder à l'endroit où le message a été placé.

AS4 permet aux entreprises d'échanger des données en toute sécurité. Il s'appuie sur les bases établies par AS2, mais fonctionne avec des services web et fournit des notifications de livraison. En tant que norme interentreprises, AS4 contribue à rendre l'échange de documents sûr et simple sur internet.