

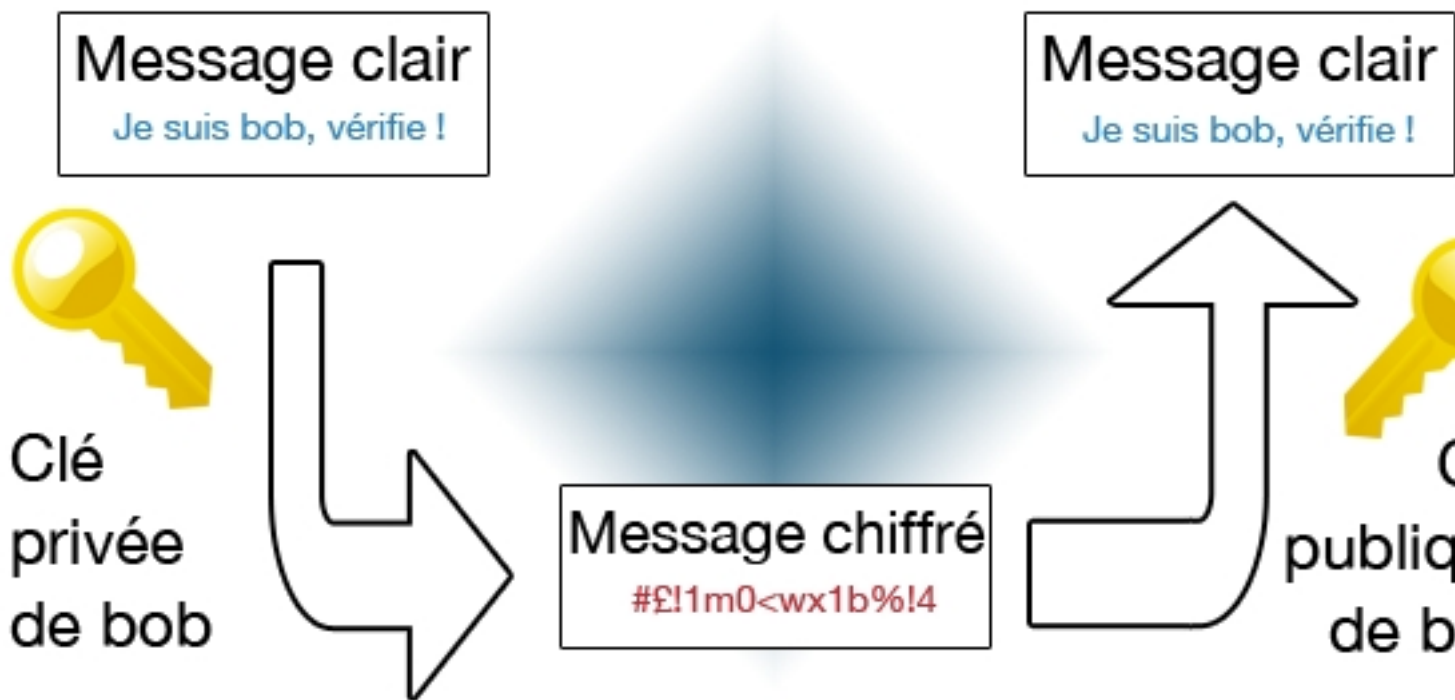
## Authentification par clé SSH

Écrit par Domotics

Mardi, 28 Mai 2013 06:00 - Mis à jour Samedi, 27 Juillet 2013 07:45

---

L'article d'aujourd'hui est un peu technique. Il s'adresse aux utilisateurs de Linux. Si vous scriptez des commandes shell d'un appareil à un autre. Vous en avez peut être assez de passer vos mots de passe sur la ligne de commande. Dans ce cas, il faut utiliser les connexions via SSH et générer une clé privée/publique afin de simplifier la maintenance de vos scripts.



{jumi [\*34]}{jumi [\*34]}

### Mais ça sert à quoi ?

Si par exemple vous avez un routeur qui fonctionne avec un firmware DD-WRT ou OpenWRT, vous avez peut être envie de planifier un script sur votre Raspberry Pi (ou votre PC Linux) pour contrôler l'activation de votre réseau Wifi. Vous pourrez couper le Wifi lorsque les occupants de la maison dorment, ...

## Authentification par clé SSH

Écrit par Domotics

Mardi, 28 Mai 2013 06:00 - Mis à jour Samedi, 27 Juillet 2013 07:45

---

Un autre exemple si vous avez un NAS Synology et que vous souhaitez le rebooter sur demande. Vous pouvez créer un script sur votre Raspberry Pi pour contrôler ce redémarrage.

Par défaut, si j'essaye de me connecter sur mon routeur, ce dernier me demande un mot de passe.

```
ssh root@192.168.1.1
```

```
domotics@wifi-srv-domo1: ~  
/dev/sda1          1946884      635208      1311676      33% /mnt  
domotics@wifi-srv-domo1:~$ ssh root@192.168.1.1 df  
DD-WRT v24-sp2 std (c) 2010 NewMedia-NET GmbH  
Release: 12/24/10 (SVN revision: 15962)  
root@192.168.1.1's password:  
  
domotics@wifi-srv-domo1:~$ ssh  
usage: ssh [-1246AaCfGkKMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]  
        [-D [bind_address:]port] [-e escape_char] [-F configfile]  
        [-I pkcs11] [-i identity_file]  
        [-L [bind_address:]port:host:hostport]  
        [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]  
        [-R [bind_address:]port:host:hostport] [-S ctl_path]  
        [-W host:port] [-w local_tun[:remote_tun]]  
        [user@]hostname [command]  
domotics@wifi-srv-domo1:~$ ssh root@192.168.1.1  
DD-WRT v24-sp2 std (c) 2010 NewMedia-NET GmbH  
Release: 12/24/10 (SVN revision: 15962)  
root@192.168.1.1's password:  
  
domotics@wifi-srv-domo1:~$ ssh root@192.168.1.1
```

Il faut alors générer une clé publique et une clé privé grâce aux commandes SSL de votre distribution Linux. Lancez la commande suivante qui à pour but de générer ces deux clés.

```
ssh-keygen -t rsa
```

## Authentification par clé SSH

Écrit par Domotics

Mardi, 28 Mai 2013 06:00 - Mis à jour Samedi, 27 Juillet 2013 07:45

---

Une phrase vous est demandé pour assurer l'encodage.

```
domotics@wifi-srv-domo1:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/domotics/.ssh/id_rsa)
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/domotics/.ssh/id_rsa
Your public key has been saved in /home/domotics/.ssh/id_rsa.pub
The key fingerprint is:
ce:62:0c:77:77:59:78:0d:4f:1e:fd:0a:09:24:dc:d1 domotics@wifi-srv
The key's randomart image is:
+--[ RSA 2048 ]-----+
|      ..ooo  ..o|
|      ..o E. *o|
|      ...o =|
|      o+  .|
|      . . S . o . .|
|      + + . . .|
|      + o|
|      . .|
+-----+
domotics@wifi-srv-domo1:~$ cat /home/domotics/.ssh/id_rsa
```

Les clés sont générées dans le répertoire `.ssh` de votre utilisateur Linux. Vous pouvez consulter la clé privé avec la commande:

```
cat /home/domotics/.ssh/id_rsa
```

La clé privé reste sur le client qui enverra les commandes. Vous ne devez pas la partager pour garantir une bonne sécurité.

## Authentification par clé SSH

Écrit par Domotics

Mardi, 28 Mai 2013 06:00 - Mis à jour Samedi, 27 Juillet 2013 07:45

```
domotics@wifi-srv-domo1:~$ cat /home/domotics/.ssh/id_r
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC,1D208D901A524F282655DC611665C1C4

mY4qAuFHYp+83JLqnlUqkQHTUqZMnfoQrZJ+kcSpqr6+1iWe44HhXau
4cNZbx+jNQwzYRAOA5EDKnIw+GYvzCL/afSGGokMkhL7VHZJJC7G5EE
snaPb6AY6InaFIIFp+JhI/e9bLDcprKn0a3JVyh1GTx1wORwWx90g66
If5oH09pK10hdhByaJQ7FYDNYTQC+868pj1IuRoU5ZHd9JtJhSe+KI6
Xnt4NsOgDcyoJ7zVNs2ONs7iW7mlw6h+gZDWA06Wi2sBEoMcyj9rP23g
bdVogRCLZEwPIkct3aU41JUSo3wQrIlbhJM6VxyzGoHDaDogVLwolKs
zCktFntCRs7ty16iT3f9FLEdBQnxC95AusK18qy2BXBFAHoH/E+ul0J
+8bVSGtcPnkW5mVjcQB7FuJO4mDjW1RiWLIJQ96RK9dF3amS9cp8nb9
HDKD1XAfQmhL4gizfjGFz4G7YM0+RuyxBTcglaydkAfsplPP3IarOh6
ZvlrRsJVtSdX0RajuYI1dFiXynbjPA9XT2zbiDw/S7ETj4cmY6DL0yn
rd0YO3/MjM4YW5G9rN14Z4z1lqKSK6xdKM5YRSG+J4xX+ATn0mjjL73
7ztbVs9vKByvYgxH/1zVBkl4SQ1OYhJKsS+lzDZOsN6hRZhh5vnxDkz
Jp0rMhpEMLnzILvfz/Ayge/6WA49viGVbChYae0tgBAkblnCLVWQv6h
lb/EpDZoesQSFAzs3sZqs/ZNZ0zTHKhTTNeQQ43WpYSVIQfnDo5H5m/
dUmGCrAJy6317aNz2bzK3aSVz4KbOJaF6WzG2I1prOUDV+BermMzx7c
F1+EEE0iACuvVRr4luqLZfrIGQzqTrBmc7pSTmdGnP4BUcziZFjfuH7
92CBps1MK2yiywyxpszmJU9nFR+x0IfYsCX0TYtVRmwpXGP2Z74i92+
R5p1RKNZL1MGrmCK2YaqhXqWiTOCS40l0YXZOMmIihLWADeRNCV4Bcc
DVmvqlzYty7qnZgRno09raUE1/TLdlNSp3xRa2ssTpiwCI+10Ixjqz9
8dd9gbnu6VWkCnvXS53AxyCUREGdQuHXXNLdg1Xb94Ajzg58xoFrKeb
4Lg4w184SloYKpE15rzS5rYWv3yPGsvSo6WbTpjV2OWeV1ii3fVR10R
bXl4+t7FfoYJtspvtgHnAlpzQGfFJ2ybfexKlSVIz5sjPTKgrogglxM
qQKXVN8QoI28D1zjiODFJKq3WZqd/6dkZevK/szqEzODyEAUheNCQWL
+FkXhKe1P5Coh1KMob1RBsJIMJKqfskxV71dXe5qWW3W96t9/7CqCpP
I6/KJnZImL9x/f26iWlKtBkxotkDq/hCyE2Ro6Uo/V8K+/S1/4dJ0tY
-----END RSA PRIVATE KEY-----
domotics@wifi-srv-domo1:~$
```

Opérer en mode root pour vérifier la clé publique que vous allez interroger via SSH.

## Authentification par clé SSH

Écrit par Domotics

Mardi, 28 Mai 2013 06:00 - Mis à jour Samedi, 27 Juillet 2013 07:45

```
domotics@wifi-srv-domo1:~$ cat .ssh/  
id_rsa      id_rsa.pub  known_hosts  
domotics@wifi-srv-domo1:~$ cat .ssh/id_rsa.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDj5IWjR8rESYRhmXzo4b21tXU+1pnDeCbFh8Ld0iyzE6+5LGMoMdeTal7OKq+p  
7etXd6Pr3CXEXqTwNbPEuS25bVtcE1/JEsfgwJHkKREh70hmo2tAfB076RHyLVcDydjT88yJ4jbytwUkDILaKWYN/MgHaJRjOe40  
URdZ2g9Yoq/6+hg6IO9WiUA+Kz2VG//wgLcpCC9lr2IU0KmfkDeviYapKSeTMq8Rjg73a+Jz5tkeM//qKTIWoWUls9rS66sU1C7/  
YjhYQCYY2Ka975OwB0dp5UPQAakorKSDpq6Gcb domotics@wifi-srv-domo1  
domotics@wifi-srv-domo1:~$
```

Home <https://192.168.1.1/applyuser.cgi>  
erre - E... Full Circle Maga... Seed Studio B... mb.ideas.reposi... Motion - Sensor... ::Sat

dd-wrt.com ... control panel  
Firmware: DD-WRT v2...  
Time: 19:37:32 up 14:34, load average  
WAN

Setup Wireless **Services** Security Access Restrictions NAT / QoS Administration Status

Services PPPoE Server VPN USB NAS Hotspot Milkfish SIP Router My Ad Network

Services Management [Help](#)

DHCP Client

Set Vendorclass   
Request IP

DHCP Server

Use JFFS2 for client lease DB   
Use NVRAM for client lease DB   
Used Domain LAN & WLAN   
LAN Domain touteladomotique.com  
Additional DHCPd Options

Static Leases

MAC Address	Host Name	IP Address	Client Lease Time
00:21:6A:85:E1:D6	wifi-pc-dga	192.168.1.200	<input type="text"/> minutes
A0:0B:BA:B8:50:D0	wifi-note-dga	192.168.1.230	<input type="text"/> minutes

à la fin de la page, vous voyez ou copier votre clé publique. Faites un simple copier/coller, ça

# Authentification par clé SSH

Écrit par Domotics

Mardi, 28 Mai 2013 06:00 - Mis à jour Samedi, 27 Juillet 2013 07:45

**SNMP**  
SNMP  Enable  Disable

**Secure Shell**  
SSHD  Enable  Disable  
SSH TCP Forwarding  Enable  Disable  
Password Login  Enable  Disable  
Port  (Default: 22)  
Authorized Keys  
ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQDcoXSHVnqHhEvuFow0ueLIIUtdp4wOpTXkZmX9tt1P6N9GBXOA9CtzTIIAAbhPAdHKN6  
vUyW6QTDX8iZjvrkk9KsFmyrvQ+wK01CGjBBPNweYzFchkdImXFRZDEomiPC/3glUF1epKBpaysgpf6VRjBjW/j/c6hDXiE9uSCYA00nA  
Hn1U6uqGtsftynTE2SqXhtckBIS/fxC/TGYrPjMnH8A/ZjQjV0hMRQSFwRQB yfqDb5K06x2yUCAJqnLn1EjpxcXE/PvZEK8+Wqh8AE+Yai  
Mr8dNOLIO15BySyDtnYzr/LWqx7kiNcqyVeajMsJJ+LQeEOO0Wy0uDeMx domotics@wifi-srv-domo1

**System Log**  
Syslogd  Enable  Disable

```
domotics@wifi-srv-domo1:~$ ssh root@192.168.1.1 df
DD-WRT v24-sp2 std (c) 2010 NewMedia-NET GmbH
Release: 12/24/10 (SVN revision: 15962)
Filesystem            1K-blocks      Used Available Use%
/dev/root              6272           6272         0 100%
none                   512             0         512   0%
/dev/mtdblock/3       320            196         124  61%
/dev/sda1             1946884        633252     1313632  33%
domotics@wifi-srv-domo1:~$ ssh root@192.168.1.1 df
DD-WRT v24-sp2 std (c) 2010 NewMedia-NET GmbH
Release: 12/24/10 (SVN revision: 15962)
Filesystem            1K-blocks      Used Available Use%
/dev/root              6272           6272         0 100%
none                   512             0         512   0%
/dev/mtdblock/3       320            196         124  61%
/dev/sda1             1946884        633252     1313632  33%
domotics@wifi-srv-domo1:~$ ssh root@192.168.1.1
```