

SSH/SCP/SFTP – Metodologie di autenticazione

1) Password;

2) Chiave Pubblica/Privata:

- ✓ Senza passphrase;
- ✓ Protetta da passphrase.



Autenticazione: 1) Password

```
user_local@local ~ $ ssh user_remote@remote.remotedomain.it
```

```
-----  
  remote.remotedomain.it  
  Unauthorized access is prohibited  
-----
```

```
Password:
```

```
Last login: Fri Oct 13 11:02:34 2006  
user_remote@remote ~ $
```



Autenticazione: 2) Chiave Pubblica/Privata

- Generazione delle chiavi pubblica e privata (ssh-keygen);
- Configurazione della macchina locale (~/.ssh/config);
- Configurazione della/e macchina/e remota/e (~/.ssh/authorized_keys);
- Soluzione ad eventuali problemi.



Autenticazione: 2) Chiave Pubblica/Privata

Generazione delle chiavi pubblica e privata:

```
user_local@local ~ $ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/user_local/.ssh/id_dsa):
/home/user_local/.ssh/id_dsa_mykey
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user_local/.ssh/id_dsa_mykey.
Your public key has been saved in /home/user_local/.ssh/id_dsa_mykey.pub.
The key fingerprint is:
20:4c:8c:7f:32:0e:c4:1d:2d:73:05:1b:43:d8:0d:c5 user_local@local.localdomain.it

user_local@local ~ $ ls -l .ssh/id_dsa_mykey*
-rw----- 1 user_local users 668 Oct 13 14:58 id_dsa_mykey
-rw-r--r-- 1 user_local users 628 Oct 13 14:58 id_dsa_mykey.pub
```



Autenticazione: 2) Chiave Pubblica/Privata

Generazione delle chiavi pubblica e privata:

```
user_local@local ~ $ cat .ssh/id_dsa_mykey
```

```
-----BEGIN DSA PRIVATE KEY-----
```

```
MIIBugIBAABKbgQCtk3YDvCgR3zes7pdsuRFmN7FyEIL6UqqnVNS74Q6JfvnmIJmDmHMT+MsThWLJujqN2X3v2hjA  
vmNIQuqrIsaYY/yNW3r0cqU6srGyr/KuBgjxsWrWycgk1w8CEW1uMVnX1+qrl0s3MZmGZ6jNPBofHTZ5jFBWrWiS4  
Lyr7lwLwIVAMWu+G2GQlrOYZsx1XIZO8P1Nu8pAoGAYf/f6nLQY2no8zKADHO5fjTzBJvcEBsilaK+SfTEKMaCb7iKT  
6bO4UO5Y0i3GkLsMe2fjfcqil6rYNPJsx/rROQRnrwlpUX231wgHKcGTF7aLrDM8OykS2cBPapOUEIX1jGnllZ8lm+jOe  
AGrVc9L5Tvf5Hick1hiMLfaIENN2kCgYBDXGjhUh2lk8a8LEssZrEMH3a7fIG58QuxP1MJgwpg16ToCuqloRHzt9l0HJq  
aDwQc0fvmWrRDu9eQfhi1GqpjdQjdmSi/StR2f0vomQ55iqin6Rz+csTaJKGD7XVAXmco38Ku/SA+NeIRMrloWoUMr  
dinlC2gjoio6fwlZIF54wIUEOaN2QKNvbA+NfE9jGCS/CqsYcl=
```

```
-----END DSA PRIVATE KEY-----
```

```
user_local@local ~ $ cat .ssh/id_dsa_mykey
```

```
-----BEGIN DSA PRIVATE KEY-----
```

```
Proc-Type: 4, ENCRYPTED
```

```
DEK-Info: DES-EDE3-CBC,82699FEB94015871
```

```
podOk1MILIDKp6qzr0XIJQbz8wl62gKwWz1h6VtHnZZ9gihqRqJbHUjYzw924AghN5Dxn9wpP005AAGw20Ywlv86rg  
77umu+bAcNachVGoXuDjBXvz8/loo38XYjv49X2C7B4XJdFVzq21RyrDrce6+piVcfZNfwBi47NIT1A5c1Q/c72eZvJ2  
y8awm9L8RJWujT92BrxqRM0lwl9XsNPxGyi6YFswNN/SNOBr5d8Wmz59dRtnvjxSPtVb1X5vmq1g1TIS+a0nrRmYk  
2NX2iyX+3BNvuYSaKLQlYSehjk6bvzzaygacDPbXY4ioTA8V/lSrFLL6Grk3OBgEqHq2bcNpz6+hKM78NeFeTmlLnO  
G7wU9NuWw1Fer83JBhBng0ErfQPpz1GgyKgYsyQBqtdlm66l3SdrAmaEUhDeqGNSoAMvfz4xIKXY4C7lIPIHro/qfnd  
1rEogCbrE2nBQ8oPYeaOXs215RTtIC5eZ8k2qTBrKcllvG7XyFxDNO7dhetlRPnD601gEFXUDr0l/jEQ+ClwvS+cSjFU  
ggSrg7yr+pcxDe/O8Md00vQt0AA8MRYmkhFy6f1TFXZwuKbsBtOtQ==
```

```
-----END DSA PRIVATE KEY-----
```

Autenticazione: 2) Chiave Pubblica/Privata

Generazione delle chiavi pubblica e privata:

```
user_local@local ~ $ cat .ssh/id_dsa_mykey.pub  
ssh-dss AAAAB3NzaC1kc3MAAACBAK2TdgO8KBHfN6zul2y5EWY3sXIQgvpSqqdU1Lvhdol++e  
aUmYOYcxP4yxOFYsm6Oo3Zfe/aGMC+Y0hC6quWxphj/I1bevRypTqysbKv8q4GCPGxatbJyCCT  
XDwIRbW4xWdfX6qsjSzcxmYZnqM08Gh8dNnmMUFataJLgvKvuXAvAAAAAFQDFrvhthkCKzmGb  
MdV5WTvD9TbvKQAAAIbh/9/qctBjaejzMoAMc7I+NPMEm9wQGylhor5J9MQoxoJvulpPps7hQ7lj  
SLcaQuwx7Z+N9yqljqtg08mzH+tE5BGevCWIRfbfXCacpwZMXtousMzw7KRLZwE9qk5QSVfWM  
aciVnyWb6M54AatVz0vIO9/keJyTWGIwt9ogQ03aQAAAIbDXGjhUh2Ik8a8LEssZrEMH3a7flG58  
QuxP1MJgwpG16ToCuqloRHzt9l0HJqaDwQc0fvmWrRDU9eQfhi1GqjpdQjdmSi/StR2f0vomQ55iqi  
n6Rz+csTaJKGD7XVAXmco38Ku/SA+NeIRMrloWoUMrdinIC2gjoio6fwlZIF54w==  
user_local@local.localdomain.it
```



Autenticazione: 2) Chiave Pubblica/Privata

Configurazione della macchina locale:

```
user_local@local ~ $ cat .ssh/config
```

```
# SSH – configuration file
```

```
Host remote remote_2.remotedomain2.it *.remotedomain3.it
```

```
    User user_remote
```

```
    IdentityFile ~/.ssh/id_dsa_mykey
```

```
Host remote_alias
```

```
    HostName remote_3.remotedomain.it
```

```
    User user_remote
```

```
    IdentityFile ~/.ssh/id_dsa_mykey2
```

```
user_local@local ~ $ ls -l .ssh/config
```

```
-rw----- 1 user_local users 737 Oct 13 15:35 .ssh/config
```

Autenticazione: 2) Chiave Pubblica/Privata

Configurazione della/e macchina/e remota/e:

```
user_local@local ~ $ scp .ssh/id_dsa_mykey.pub user_remote@remote.remotedomain.it:
```

```
user_remote@remote ~ $ cat id_dsa_mykey.pub >> .ssh/authorized_keys
```

```
user_remote@remote ~ $ cat .ssh/authorized_keys
```

```
ssh-dss AAAAB3NzaC1kc3MAAACBAK2TdgO8KBHfN6zul2y5EWY3sXIQgvpSqqdU1Lvhdol++e  
aUmYOYcxP4yxOFYsm6Oo3Zfe/aGMC+Y0hC6quWxphj/I1bevRypTqysbKv8q4GCPGxatbJyCCT  
XDwlRbW4xWdfX6qsjSzcxmYZnqM08Gh8dNnmMUFataJLgvKvuXAvAAAAAFQDFrvhthkCKzmGb  
MdV5WTvD9TbvKQAAAIbh/9/qctBjaejzMoAMc7I+NPME9wQGylhor5J9MQoxoJvulpPps7hQ7lj  
SLcaQuwx7Z+N9yqljqtg08mzH+tE5BGevCWIRfbfXCacpwZMXtousMzw7KRLZwE9qk5QSVfWM  
aciVnyWb6M54AatVz0vIO9/keJyTWGIwt9ogQ03aQAAAIBDXGjhUh2lk8a8LEssZrEMH3a7flG58  
QuxP1MJgwpG16ToCuqloRHzt9l0HJqaDwQc0fvmWrRDu9eQfhi1GqpjdQjdmSi/StR2f0vomQ55iqi  
n6Rz+csTaJKGD7XVAXmco38Ku/SA+NeIRMrloWoUMrdinIC2gjoio6fwlZIF54w==
```

```
user_local@local.localdomain.it
```

```
user_remote@remote ~ $ ls -l .ssh/authorized_keys
```

```
-rw-r--r-- 1 user_remote users 2255 Jan 31 2006 .ssh/authorized_keys
```

Autenticazione: 2) Chiave Pubblica/Privata

- chiave non protetta con passphrase -

```
user_local@local ~ $ ssh remote
```

```
-----  
remote.remotedomain.it
```

```
Unauthorized access is prohibited
```

```
-----  
Last login: Fri Oct 13 11:02:34 2006
```

```
user_remote@remote ~ $
```

- chiave protetta con passphrase -

```
user_local@local ~ $ ssh remote
```

```
-----  
remote.remotedomain.it
```

```
Unauthorized access is prohibited
```

```
-----  
Enter passphrase for key '/home/user_local/.ssh/id_dsa_mykey':
```

```
Last login: Fri Oct 13 11:02:34 2006
```

```
user_remote@remote ~ $
```

Autenticazione: 2) Chiave Pubblica/Privata

Utilizzo di chiavi protette con passphrase (ssh-agent / ssh-add)

```
user_local@local ~ $ ssh-agent
SSH_AUTH_SOCK=/tmp/ssh-XX4LkMJS/agent.26916;
export SSH_AUTH_SOCK;
SSH_AGENT_PID=26917; export SSH_AGENT_PID;
echo Agent pid 26917;
```

```
user_local@local ~ $ eval `ssh-agent`
```

```
user_local@local ~ $ ssh-add ~/.ssh/id_dsa_mykey
Enter passphrase for key '/home/user_local/.ssh/id_dsa_mykey':
```

(reset della sessione di ssh-agent: `eval `ssh-agent -k``)

Non e' molto comodo!



keychain



Autenticazione: 2) Chiave Pubblica/Privata

Utilizzo di chiavi protette con passphrase (keychain)

```
user_local@local ~ $ keychain --nolock -q --timeout 120 ~/.ssh/id_dsa_mykey
```

```
.bash_profile e/o .bashrc (man keychain)
```

```
keychain ~/.ssh/id_dsa_mykey  
[[ -f $HOME/.keychain/$HOSTNAME-sh ]] && \  
source $HOME/.keychain/$HOSTNAME-sh
```

```
(~/.keychain/$HOSTNAME-sh / eval `ssh-agent -k`)
```



Autenticazione: 2) Chiave Pubblica/Privata

Soluzione ad eventuali problemi:

- Controllare che i permessi siano corretti;
- "ssh -vvv" per avere un' output piu' dettagliato del processo di autenticazione;
- Consultare la documentazione ufficiale:
 - man ssh (client ssh);
 - man ssh_config (configurazione client ssh);
 - man ssh-keygen (generazione chiavi);
 - man ssh-agent / man kychain (caching della chiave privata);
 - <http://www.openssh.org/>
 - <http://www.gentoo.org/doc/en/keychain-guide.xml>



Documentazione Interna

Lista del software installato sulle workstations:

- Il pdf contiene:
 - nome del programma;
 - descrizione sintetica;
 - path d'installazione (eseguibili / documentazione);
 - Homepage;
 - eventuali altre informazioni aggiuntive;

Web: http://www.ts.astro.it/services/doc_machine_Gentoo.pdf

Locale: `/usr/local/doc/doc_machine_Gentoo.pdf`

“Backup remainder”

- I dati degli utenti presenti sulle workstation **NON** sono salvati automaticamente in alcun modo;
- **E' RESPONSABILITA' DELL'UTENTE** salvare manualmente i dati che ritiene importanti (copie multiple in altre macchine / dischi-supporti removibili / altro);
- La posta **NON** viene salvata automaticamente;

Sistema di backup centralizzato – non automatico:

strangelove.oat.ts.astro.it

Compilatore fortran g77

- **gfortran** diventa il compilatore FORTRAN (77/90/95) di riferimento per GNU a partire dalla "GCC's official release 4.0.0" (g77 NON e' piu' incluso nelle release ufficiali GNU);
- **gfortran** e' un compilatore NUOVO e NON ha come base di sviluppo **g77**;
- **gfortran** e **g77** NON sono compatibili:
 - In termini di opzioni di compilazione e sintassi d'utilizzo;
 - In termini di binari prodotti (eg. file oggetto);
- **gfortran** NON e' **g95** (sono due compilatori diversi);

Compilatore fortran g77 – PORTABILITA'

Indipendentemente da linguaggio e compilatore scelto:

- rimanere consistenti con standard "forti" (es. **ANSI / POSIX**);
- evitare l'utilizzo di funzioni intrinseche del compilatore;
- evitare di utilizzare / integrare nei propri progetti componenti e/o librerie che non rispettano i primi due punti.

NOTA: queste tre sono regole elementari per svincolarsi da un particolare compilatore ed ottenere un codice che risulti poco sofferenti ai cambi di piattaforma e/o compilatore.