

# sslpaswd e sslpwdd

Una soluzione OpenSSL  
client/server

# sslpwdd/sslpasswd

- Applicazione SSL che viene utilizzata dalla sezione INFN di Firenze per consentire agli utenti di cambiare la propria password IMAP sul server di sezione da un qualsiasi client remoto in ambiente Linux/Windows
- Consiste in 2 programmi, il server sslpwdd ed il client sslpasswd



# sslpwdd

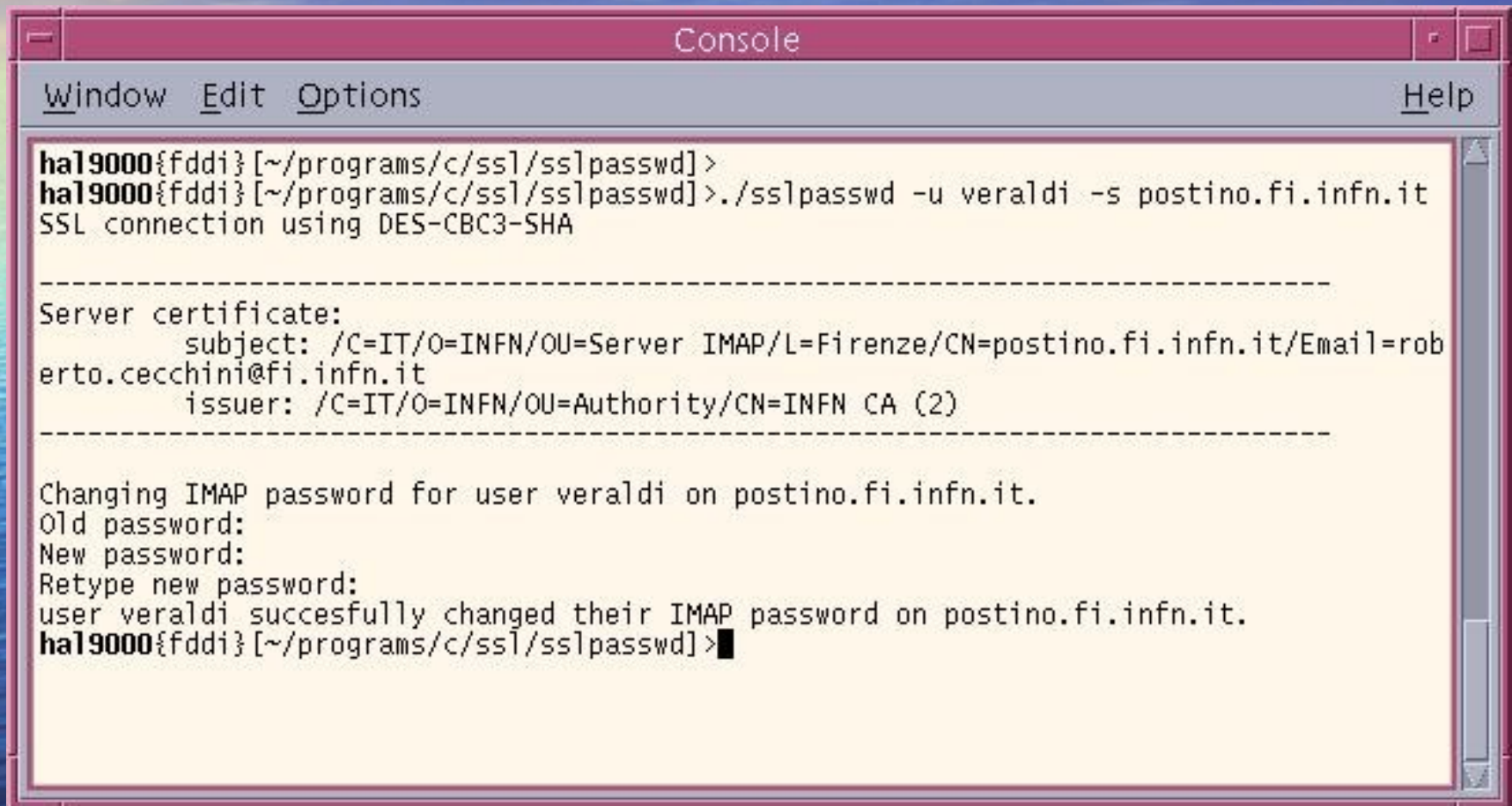
- Applicazione OpenSSL server-side
  - Demone in esecuzione sul server di posta
  - Autentica gli utenti tramite password su connessione sicura (SSL)
  - Modifica la password nel database del sistema operativo (file *passwd*) e/o nel database *sasl*
  - Logging degli accessi da parte dei client tramite **syslogd**
  - Ho scritto per ora soltanto una versione per il sistema operativo FreeBSD (i386 e Alpha).

# sslpaswd

- Applicazione OpenSSL client-side
  - Front-end per gli utenti che desiderano cambiare la propria password sul server di posta in modo sicuro (SSL) eseguendo il client *sslpaswd* dal proprio PC.
  - Si collega al server *sslpwdd* e presenta agli utenti un'interfaccia simile al comando **passwd** di unix.
  - Esiste in 3 versioni:
    - FreeBSD
    - Linux
    - Windows (*cygwin*)



# Esempio di sessione sslpasswd(1)

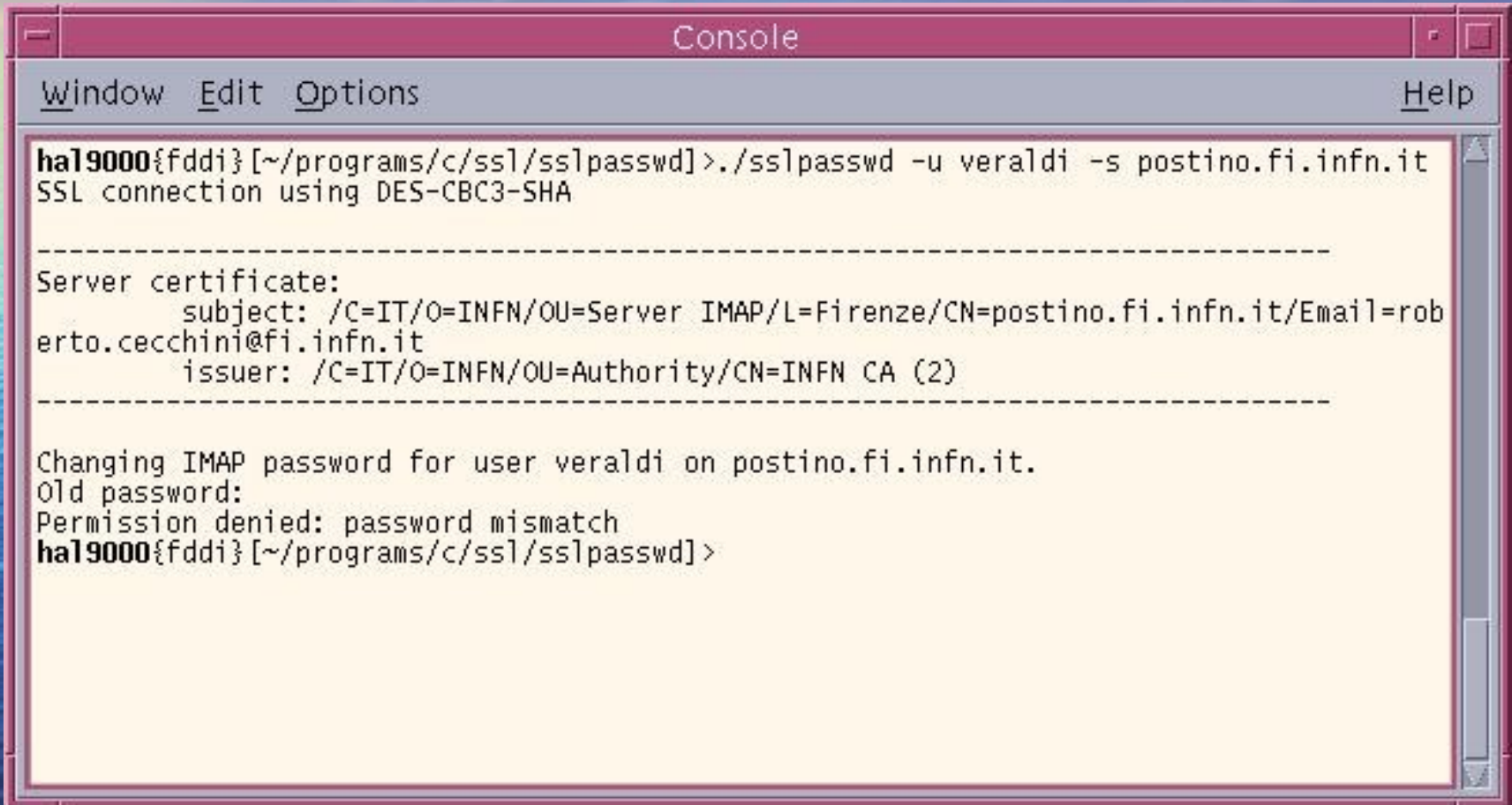


```
ha19000{fddi}[~/programs/c/ssl/sslpasswd]>
ha19000{fddi}[~/programs/c/ssl/sslpasswd]>./sslpasswd -u veraldi -s postino.fi.infn.it
SSL connection using DES-CBC3-SHA

-----
Server certificate:
      subject: /C=IT/O=INFN/OU=Server IMAP/L=Firenze/CN=postino.fi.infn.it/Email=roberto.cecchini@fi.infn.it
      issuer: /C=IT/O=INFN/OU=Authority/CN=INFN CA (2)
-----

Changing IMAP password for user veraldi on postino.fi.infn.it.
Old password:
New password:
Retype new password:
user veraldi succesfully changed their IMAP password on postino.fi.infn.it.
ha19000{fddi}[~/programs/c/ssl/sslpasswd]>■
```

# Esempio di sessione sslpaswd(2)



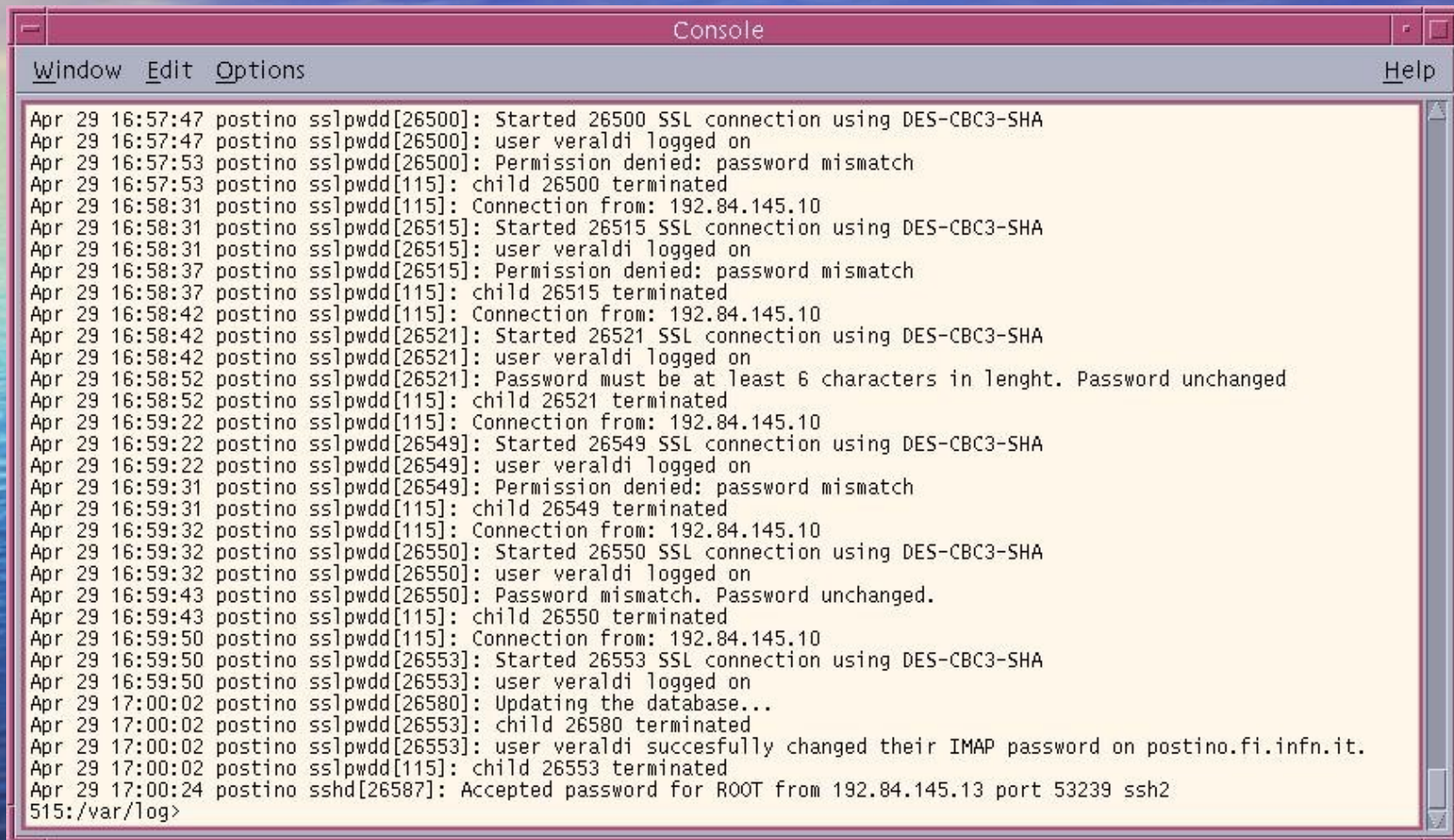
```
ha19000{fddi}[~/programs/c/ssl/sslpaswd]>./sslpaswd -u veraldi -s postino.fi.infn.it
SSL connection using DES-CBC3-SHA

-----
Server certificate:
      subject: /C=IT/O=INFN/OU=Server IMAP/L=Firenze/CN=postino.fi.infn.it/Email=rob
erto.cecchini@fi.infn.it
      issuer: /C=IT/O=INFN/OU=Authority/CN=INFN CA (2)
-----

Changing IMAP password for user veraldi on postino.fi.infn.it.
Old password:
Permission denied: password mismatch
ha19000{fddi}[~/programs/c/ssl/sslpaswd]>
```



# Session sslpasswd vista dal server sslpwdd



```
Window Edit Options Help
Apr 29 16:57:47 postino sslpwdd[26500]: Started 26500 SSL connection using DES-CBC3-SHA
Apr 29 16:57:47 postino sslpwdd[26500]: user veraldi logged on
Apr 29 16:57:53 postino sslpwdd[26500]: Permission denied: password mismatch
Apr 29 16:57:53 postino sslpwdd[115]: child 26500 terminated
Apr 29 16:58:31 postino sslpwdd[115]: Connection from: 192.84.145.10
Apr 29 16:58:31 postino sslpwdd[26515]: Started 26515 SSL connection using DES-CBC3-SHA
Apr 29 16:58:31 postino sslpwdd[26515]: user veraldi logged on
Apr 29 16:58:37 postino sslpwdd[26515]: Permission denied: password mismatch
Apr 29 16:58:37 postino sslpwdd[115]: child 26515 terminated
Apr 29 16:58:42 postino sslpwdd[115]: Connection from: 192.84.145.10
Apr 29 16:58:42 postino sslpwdd[26521]: Started 26521 SSL connection using DES-CBC3-SHA
Apr 29 16:58:42 postino sslpwdd[26521]: user veraldi logged on
Apr 29 16:58:52 postino sslpwdd[26521]: Password must be at least 6 characters in lenght. Password unchanged
Apr 29 16:58:52 postino sslpwdd[115]: child 26521 terminated
Apr 29 16:59:22 postino sslpwdd[115]: Connection from: 192.84.145.10
Apr 29 16:59:22 postino sslpwdd[26549]: Started 26549 SSL connection using DES-CBC3-SHA
Apr 29 16:59:22 postino sslpwdd[26549]: user veraldi logged on
Apr 29 16:59:31 postino sslpwdd[26549]: Permission denied: password mismatch
Apr 29 16:59:31 postino sslpwdd[115]: child 26549 terminated
Apr 29 16:59:32 postino sslpwdd[115]: Connection from: 192.84.145.10
Apr 29 16:59:32 postino sslpwdd[26550]: Started 26550 SSL connection using DES-CBC3-SHA
Apr 29 16:59:32 postino sslpwdd[26550]: user veraldi logged on
Apr 29 16:59:43 postino sslpwdd[26550]: Password mismatch. Password unchanged.
Apr 29 16:59:43 postino sslpwdd[115]: child 26550 terminated
Apr 29 16:59:50 postino sslpwdd[115]: Connection from: 192.84.145.10
Apr 29 16:59:50 postino sslpwdd[26553]: Started 26553 SSL connection using DES-CBC3-SHA
Apr 29 16:59:50 postino sslpwdd[26553]: user veraldi logged on
Apr 29 17:00:02 postino sslpwdd[26580]: Updating the database...
Apr 29 17:00:02 postino sslpwdd[26553]: child 26553 terminated
Apr 29 17:00:02 postino sslpwdd[26553]: user veraldi succesfully changed their IMAP password on postino.fi.infn.it.
Apr 29 17:00:02 postino sslpwdd[115]: child 26553 terminated
Apr 29 17:00:24 postino sshd[26587]: Accepted password for ROOT from 192.84.145.13 port 53239 ssh2
515:/var/log>
```

# Stato del software - TODO

- sslpwdd
  - Svincolare la parte dipendente dal sistema operativo (file delle password) da quella non dipendente (OpenSSL)
  - Porting del programma su altri sistemi operativi:
    - Linux
    - OpenBSD, NetBSD
    - Solaris



# Conclusioni

Può essere una buona soluzione per consentire agli utenti di autenticarsi su un server remoto e modificare la propria password in modo sicuro senza dovere utilizzare un'interfaccia web.