INSTALLAZIONE OPENVPN
DA OGS.TRIESTE.IT A DT.INSU.CNRS.FR
PER BACKUP PC DI COMANDO GLIDER

VERSIONE 1

A. BUSSANI

Approved by: ……

Dr. Paola Del Negro

Abstract

Documentazione relativa all'installazione di un client VPN per piattaforma Windows, GNU/Linux e freebsd.
Per poter permettere l'uso di un pc di backup per il controllo del glider, i colleghi francesi hanno fornito un accesso tramite vpn. Tale abstract include le procedure di installazione sulle piattaforme windows, linux e freebsd, che possono essere usate per la connessione con tale server di backup.

Indice

Pre requisiti

L'archivio cognome.nomeXX.tar.gz
in questo caso l'archivio:
elena.mauri93.tar.gz contenente:

- updown-script.sh
- openvpn.conf
- elena.mauri92.conf
- elena.mauri92.ovpn

e i relativi certificati

- elena.mauri92.crt
- elena.mauri92.key
- terena.pem

La documentazione da rispedire firmata con le risorse utilizzabili e le limitazioni relative ai sistemi remoti francesi.
file: openvpn_client.pdf in allegato

Contatti per spedizione richiesta d'accesso e relativi certificati

karim.bernardet@dt.insu.cnrs.fr>

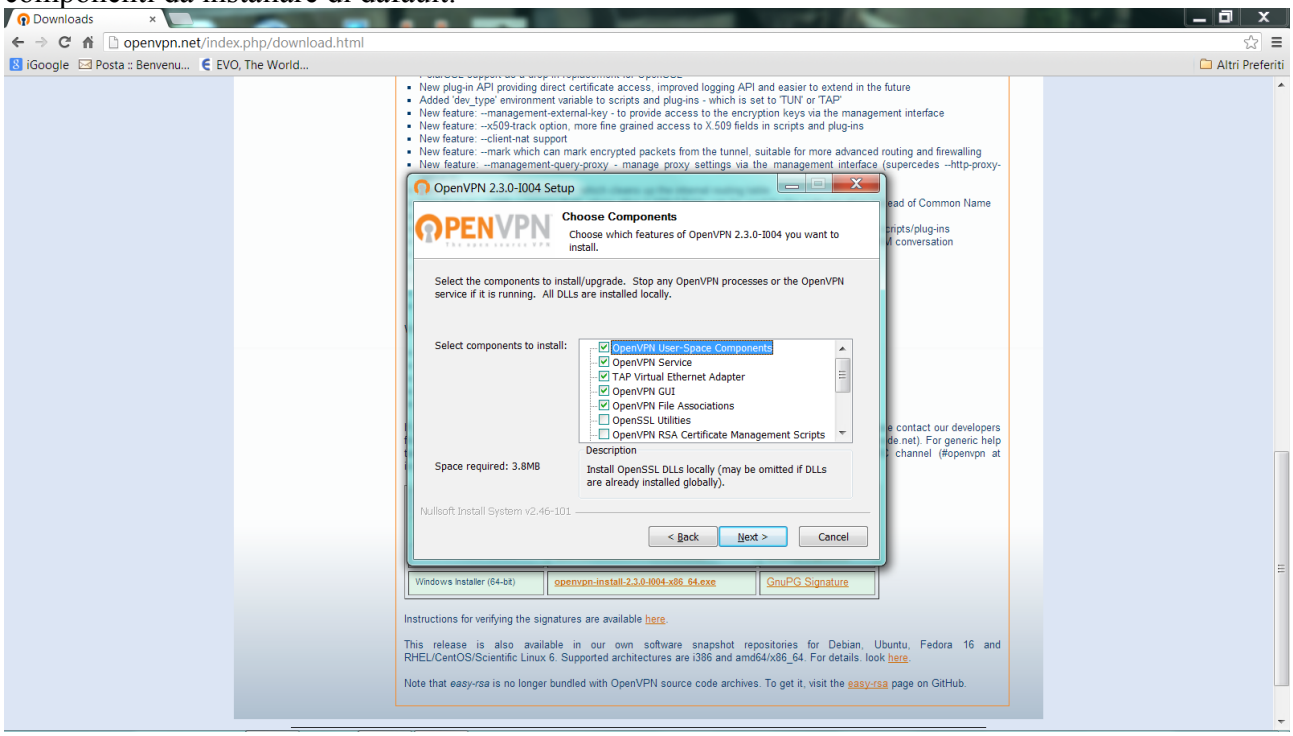
Installazione Windows XP, Vista e Windows 7

Sulla pagina
http://openvpn.net/index.php/download.html
scaricare il file corretto per il computer sul quale si sta installando, facendo attenzione a scaricare la versione a 32/64 bit corrispondente. Il sito dove scaricare è il seguente:

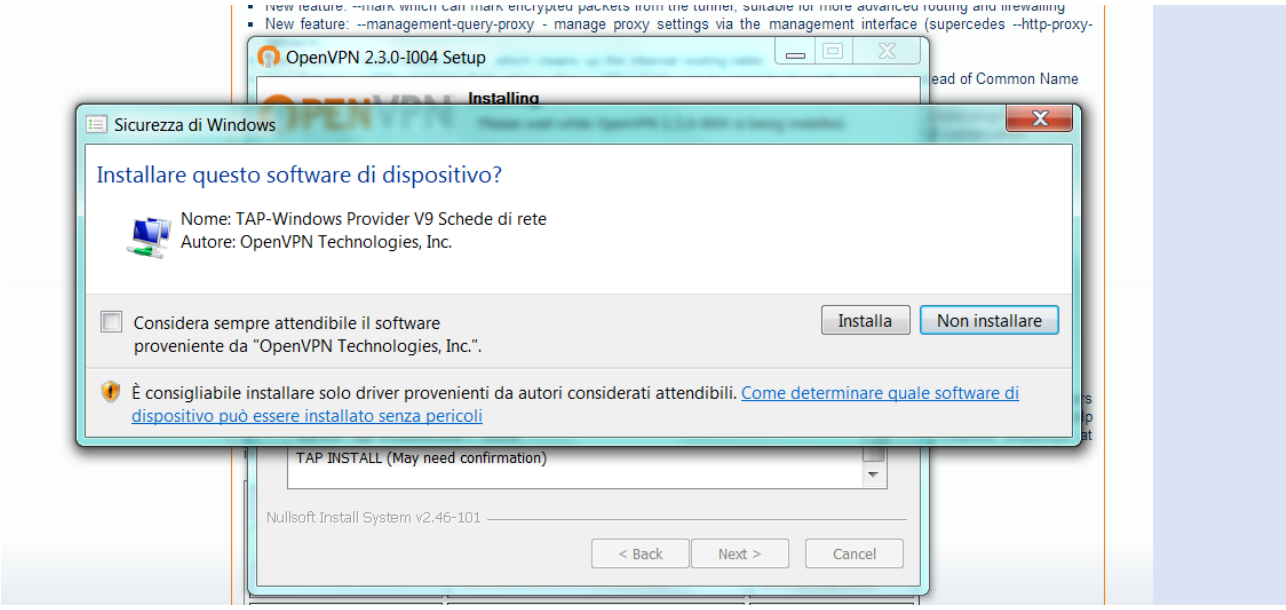
http://openvpn.net/index.php/download.html
http://swupdate.openvpn.org/community/releases/openvpn-install-2.3.0-I004-x86_64.exe

Source Tarball	openvpn-2.3.0.tar.gz	GnuPG Signature
Source Zip	openvpn-2.3.0.zip	GnuPG Signature
Windows Installer (32-bit)	openvpn-install-2.3.0-I004-i686.exe	GnuPG Signature
Windows Installer (64-bit)	openvpn-install-2.3.0-I004-x86_64.exe	GnuPG Signature

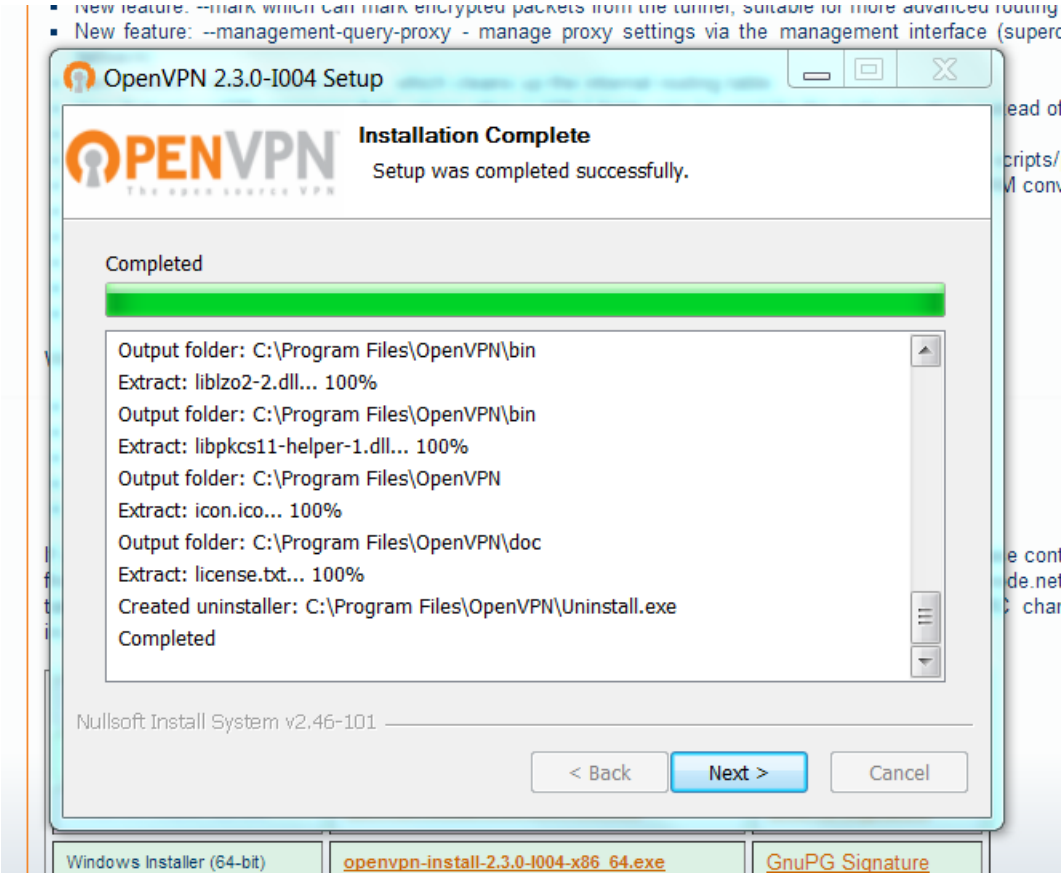
In ambiente Windows 7 è necessario accettare la richiesta di installazione, lasciare inalterati i componenti da installare di dafault.



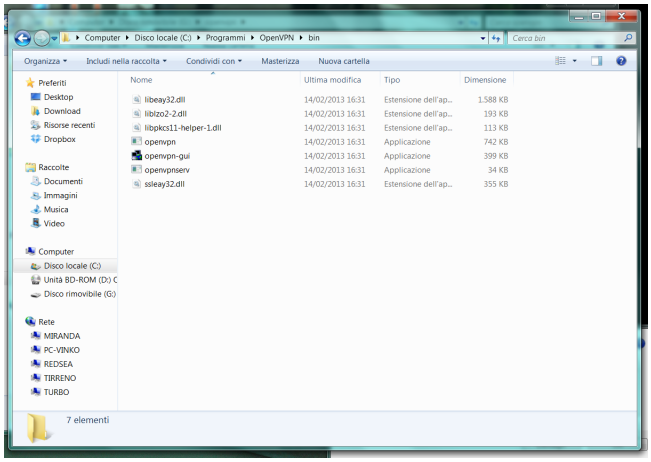
Accettare l'installazione della tap interface

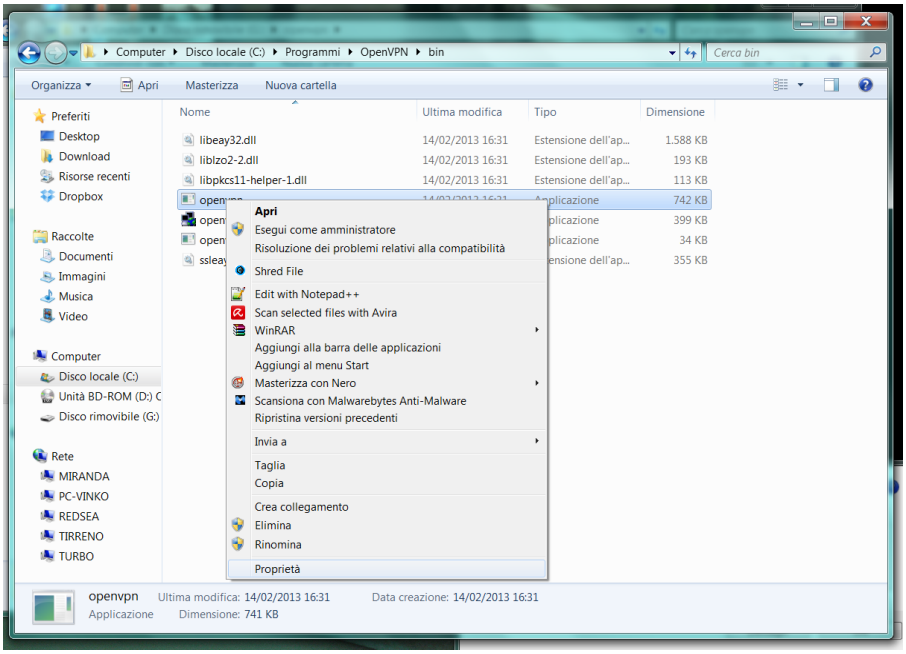


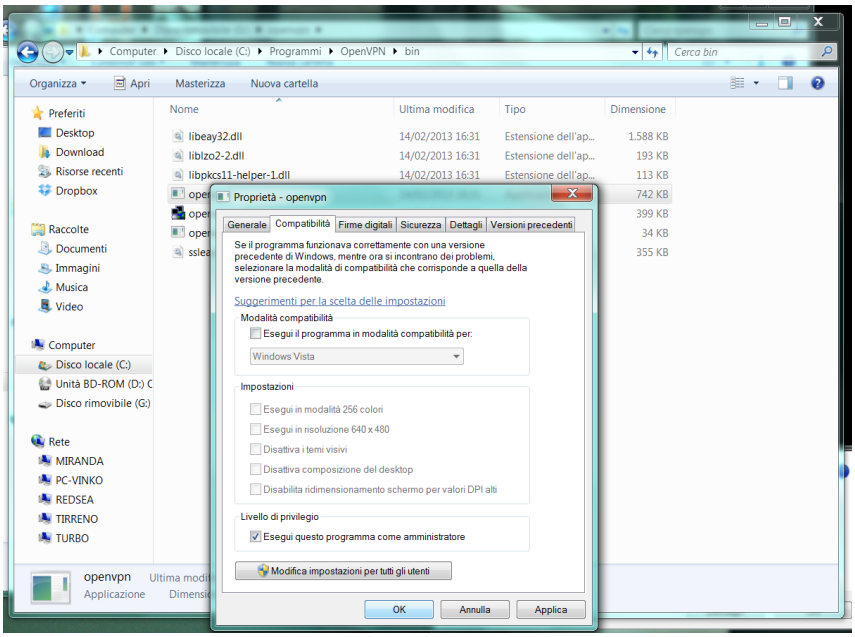
Cliccare il bottone next



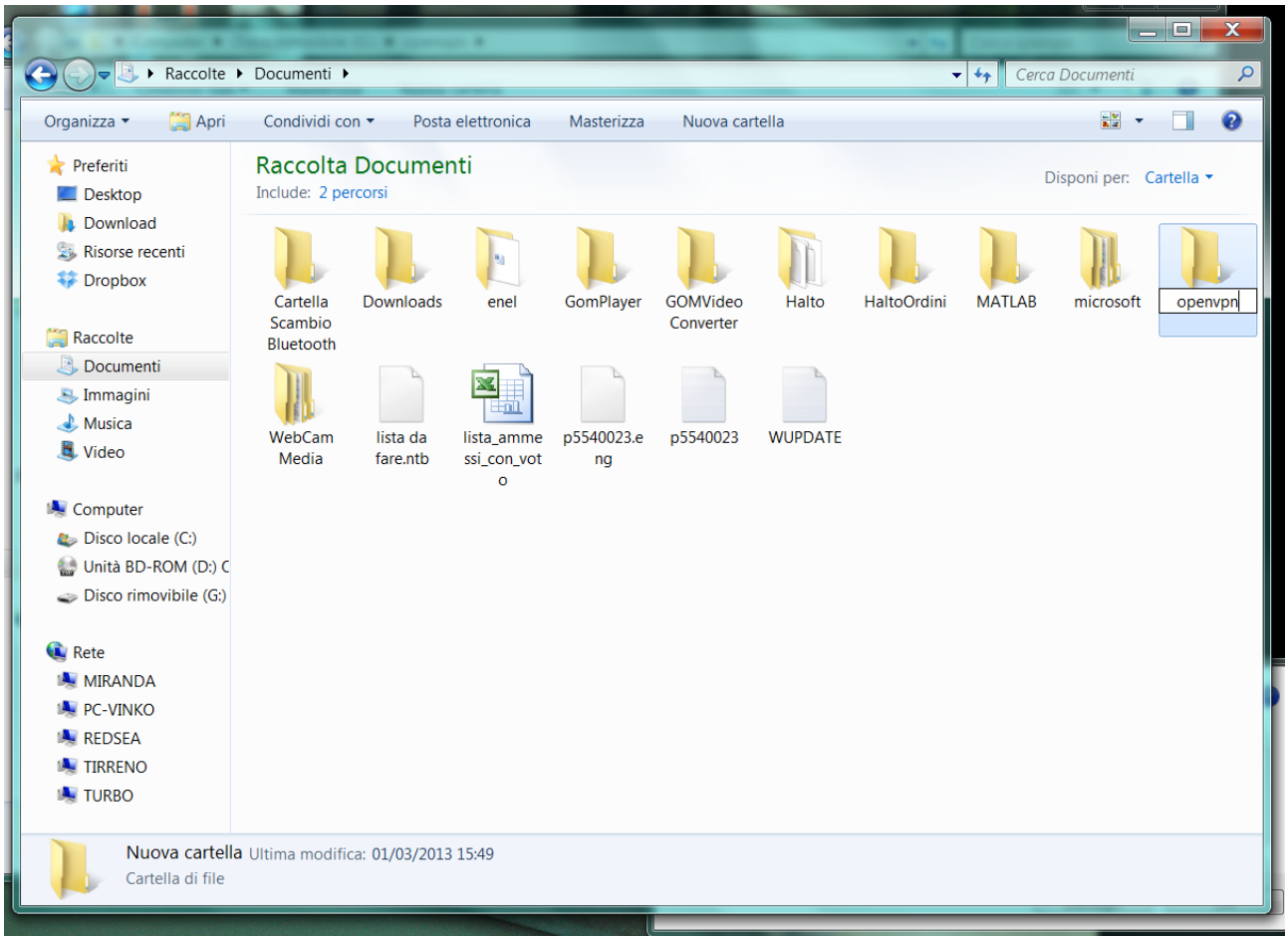
Settare l'esecuzione del programma come utente amministratore (successive 3 figure)


Computer ▸ Disco locale (C:) ▸ Programmi ▸ OpenVPN ▸ bin
Organizza
Includi nella raccolta
Condividi con
Masterizza
Nuova cartella
Preferiti
Desktop
Download
Risorse recenti
Dropbox
Raccolte
Documenti
Immagini
Musica
Video
Computer
Disco locale (C:)
Unità BD-ROM (D:)
Disco rimovibile (G:)
Rete
MIRANDA
PC-VINKO
REDSEA
TIRRENO
TURBO
Nome
Ultima modifica
Tipo
Dimensione
libeay32.dll 14/02/2013 16:31 Estensione dell'ap... 1.588 KB
liblzo2-2.dll 14/02/2013 16:31 Estensione dell'ap... 193 KB
libpkcs11-helper-1.dll 14/02/2013 16:31 Estensione dell'ap... 113 KB
openvpn 14/02/2013 16:31 Applicazione 742 KB
openvpn-gui 14/02/2013 16:31 Applicazione 399 KB
openvpnserv 14/02/2013 16:31 Applicazione 34 KB
ssleay32.dll 14/02/2013 16:31 Estensione dell'ap... 355 KB
7 elementi

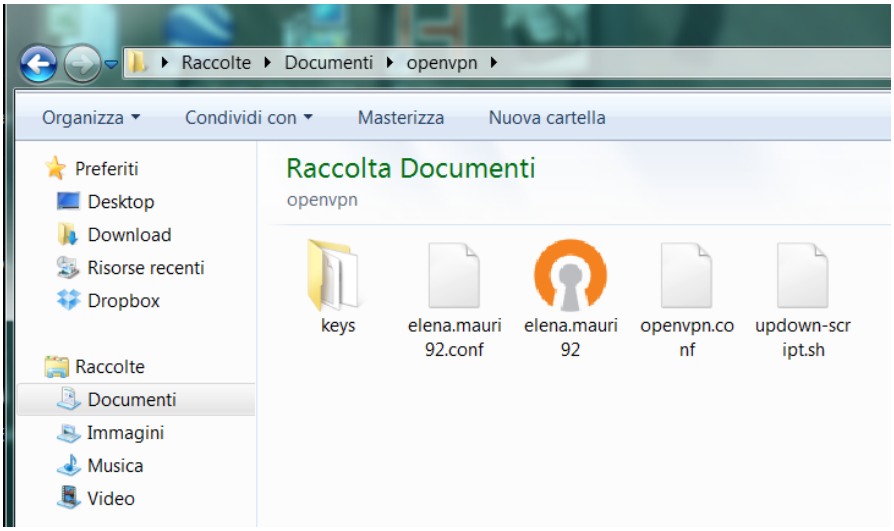

Computer ▸ Disco locale (C:) ▸ Programmi ▸ OpenVPN ▸ bin
Cerca bin
Organizza
Apri
Masterizza
Nuova cartella
Preferiti
Desktop
Download
Risorse recenti
Dropbox
Raccolte
Documenti
Immagini
Musica
Video
Computer
Disco locale (C:)
Unità BD-ROM (D:)
Disco rimovibile (G:)
Rete
MIRANDA
PC-VINKO
REDSEA
TIRRENO
TURBO
Nome
Ultima modifica
Tipo
Dimensione
libeay32.dll 14/02/2013 16:31 Estensione dell'ap... 1.588 KB
liblzo2-2.dll 14/02/2013 16:31 Estensione dell'ap... 193 KB
libpkcs11-helper-1.dll 14/02/2013 16:31 Estensione dell'ap... 113 KB
742 KB
399 KB
34 KB
355 KB
Apri
Esegui come amministratore
Risoluzione dei problemi relativi alla compatibilità
Shred File
Edit with Notepad++
Scan selected files with Avira
WinRAR
Aggiungi alla barra delle applicazioni
Aggiungi al menu Start
Masterizza con Nero
Scansiona con Malwarebytes Anti-Malware
Ripristina versioni precedenti
Invia a
Taglia
Copia
Crea collegamento
Elimina
Rinomina
Proprietà
openvpn Ultima modifica: 14/02/2013 16:31 Data creazione: 14/02/2013 16:31
Applicazione Dimensione: 741 KB


Computer ▸ Disco locale (C:) ▸ Programmi ▸ OpenVPN ▸ bin
Organizza
Apri
Masterizza
Nuova cartella
Proprietà - openvpn
Generale
Compatibilità
Firme digitali
Sicurezza
Dettagli
Versioni precedenti
Se il programma funzionava correttamente con una versione precedente di Windows, mentre ora si incontrano dei problemi, selezionare la modalità di compatibilità che corrisponde a quella della versione precedente.
Suggerimenti per la scelta delle impostazioni
Modalità compatibilità
Esegui il programma in modalità compatibilità per:
Windows Vista
Impostazioni
Esegui in modalità 256 colori
Esegui in risoluzione 640 x 480
Disattiva i temi visivi
Disattiva composizione del desktop
Disabilita ridimensionamento schermo per valori DPI alti
Livello di privilegio
Esegui questo programma come amministratore
Modifica impostazioni per tutti gli utenti
OK
Annulla
Applica

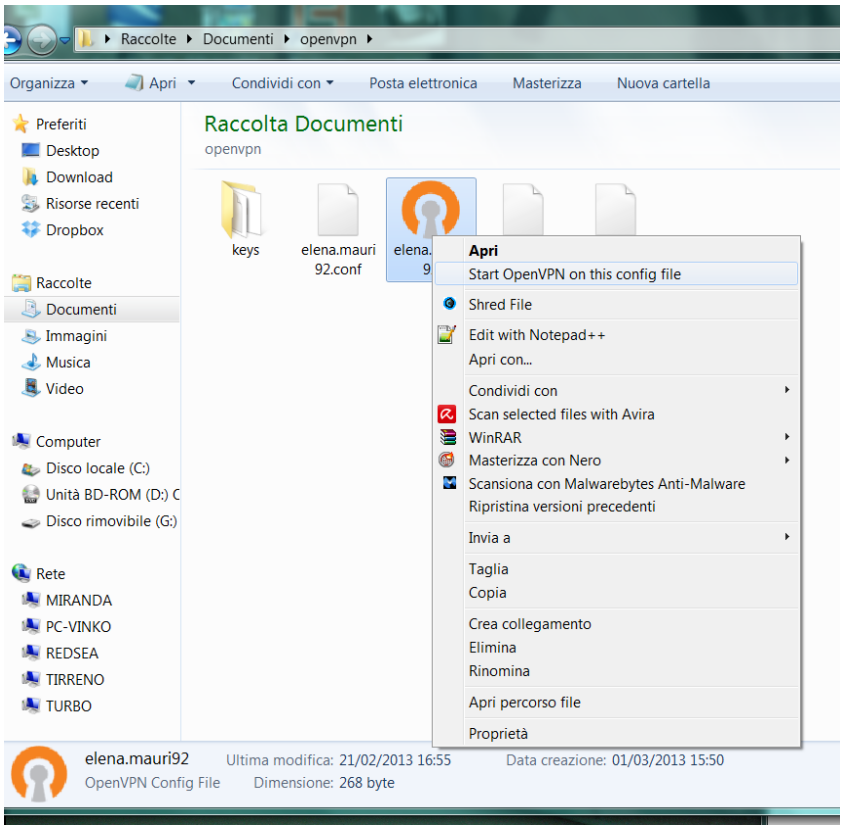
Creare la cartella openvpn in Documenti.



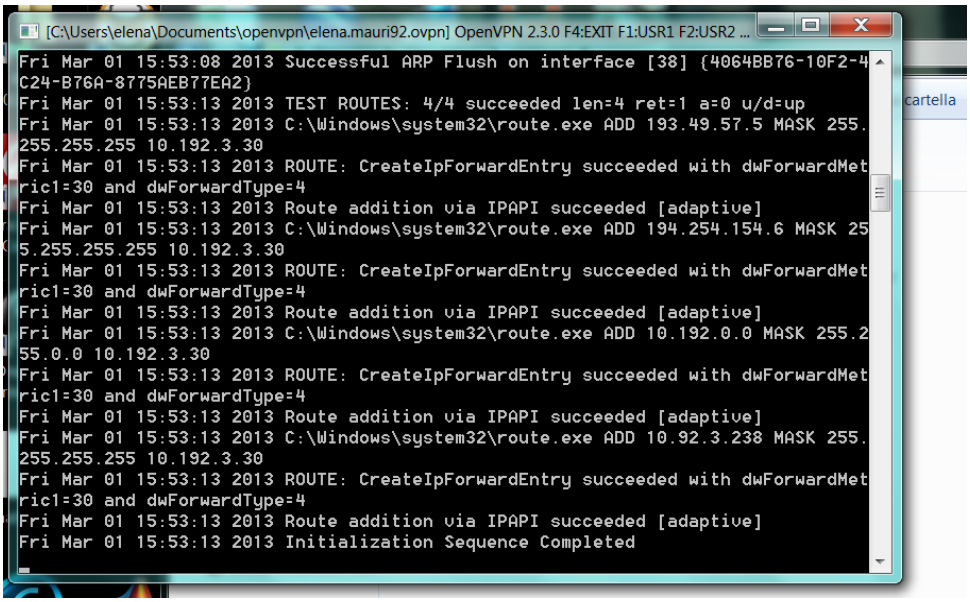
Copiare i file che si trovano all'interno del file di configurazione della vpn (file .tar.gz)



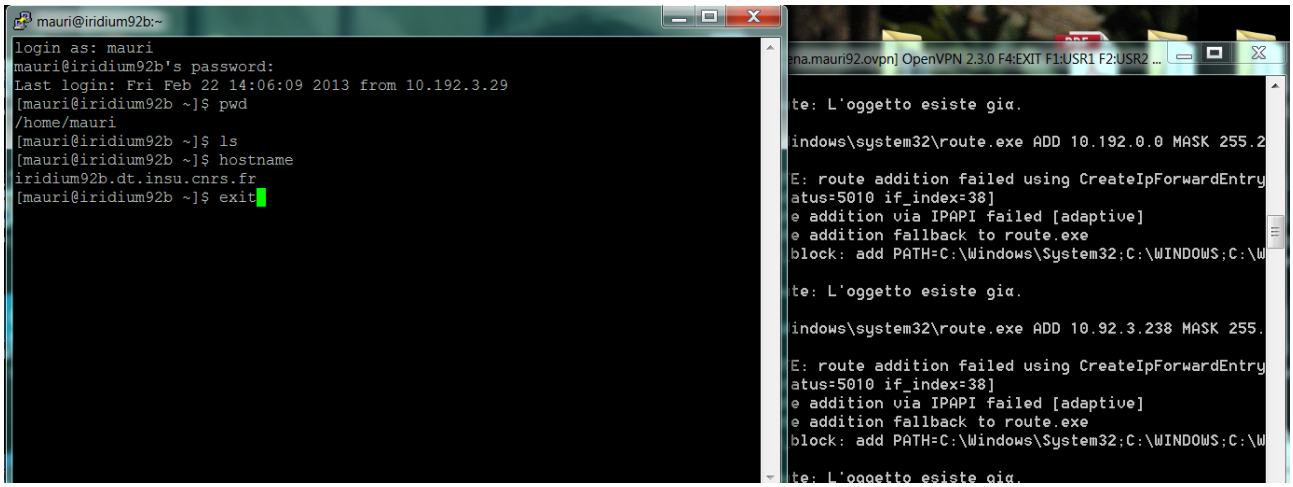
Per iniziare ad usare la vpn, è necessario cliccare con il tasto destro sul file elena.mauri92 e cliccare con il sinistro su “Start OpenVPN on this config file”
Login e password della VPN
login : [redacted]
password : XXXXXXXXXX



Dopo che il sistema si e' connesso



La connessione è avvenuta, per connettersi ora è necessario usare un client SSH, quale putty.
Oppure usare il comando ssh mauri@iridium92b
Login e password quelli della VPN
login : [redacted]
password : XXXXXXXXXX



Installazione per GNU/Linux

1. Installare il pacchetto ufficiale openvpn per la distribuzione Linux utilizzata, o scaricare l'archivio openvpn-2.1.1.tar.gz dal sito ufficicale OpenVPN.

Esempio con un pacchetto ufficiale di CentOS/:

```
$ sudo yum install openvpn
```

2. Decomprimere l'archivio in una cartella prenom.nom92.tar.gz:

```
$ tar zxvf elena.mauri93.tar.gz
```

3. Eseguire il comando di seguito CI in una shell con privilegi di root nella cartella di installazione prenom.nom92 l'archivio:

```
$ sudo openvpn --config elena.mauri93.conf
Wed Mar 24 15:13:24 2010 OpenVPN 2.1_rc19 i486-pc-linux-gnu
[SSL] [LZO2] [EPOLL] [PKCS11] built on Oct 13 2009
Enter Auth Username:
```

4. Inserire il proprio nome utente / password (lo stesso utilizzato per accedere ala VPN)
Login e password quelli della VPN
login : [redacted]
password : XXXXXXXXXX

Pagina di installazione VPN Client Fedora
Link: http://fedoraproject.org/wiki/Openvpn

Installazione per freebsd

Link: http://www.freebsddiary.org/openvpn.php
Link: http://battleship-potemkin.com/2011/03/16/openvpn-on-freebsd-windows-clients/

Aggiornamento ports:
Link http://www.freebsd.org/doc/handbook/updating-upgrading-portsnap.html

Scaricare uno snapshot della collezione dei ports in /var/db/portsnap.

```
    # portsnap fetch
```

Se eseguite il portsnap per la prima volta, estrarre lo snapshot in /usr/ports:

```
    # portsnap extract
```

Dopo il primo uso del portsnap /usr/ports può essere aggiornato con:

```
    # portsnap update
```

Installazione

```
cd /usr/ports/security/openvpn
make install clean/usr/ports/security/openvpn
```

Potete trovare una configurazione di test in /usr/local/share/doc/openvpn/sample-config-files

Usando l'interfaccia TAP
Like: http://openvpn.net/index.php/open-source/documentation/miscellaneous/76-ethernet-bridging.html
E' necessario caricare l'interfaccia virtuale prima di far partire OpenVPN. Tale comando abilita l'interfaccia:

```
kldload if_tap
```

Per assicurarsi che il modulo sia caricato all'avvio del sistema aggiungere la seguente linea al file /boot/loader.conf:

```
if_tap_load="YES"
```

If you see an error like this one, then you have forgotten to load this particular kernel module:

Configurazione client freebsd

Sul client (come sul server) abbiamo in /etc/rc.conf queste righe:

```
openvpn_enable="YES"
openvpn_if="tap"
```

Il file /usr/local/etc/openvpn/openvpn.conf contiene:

```
Sample OpenVPN configuration file for
# home using SSL/TLS mode and RSA certificates/keys.
#
# '#' or ';' may be used to delimit comments.

# Use a dynamic tun device.
# For Linux 2.2 or non-Linux OSes,
# you may want to use an explicit
# unit number such as "tun1".
# OpenVPN also supports virtual
# ethernet "tap" devices.
dev tap

# Our OpenVPN peer is the office gateway.
float
remote myserver.example.com

# 192.168.100.2 is our local VPN endpoint (home).
# 192.168.100.3 is our remote VPN endpoint (office).
ifconfig 192.168.100.2 255.255.255.0
route 10.55.0.0 255.255.255.0 192.168.100.3

# In SSL/TLS key exchange, Office will
# assume server role and Home
# will assume client role.
tls-client

ns-cert-type server

# Certificate Authority file
ca /usr/local/etc/openvpn/keys/ca.crt

# Our certificate/public key
cert /usr/local/etc/openvpn/keys/client.example.com.crt

# Our private key
key /usr/local/etc/openvpn/keys/client.example.com.key

# OpenVPN 2.0 uses UDP port 1194 by default
# (official port assignment by iana.org 11/04).
# OpenVPN 1.x uses UDP port 5000 by default.
# Each OpenVPN tunnel must use
# a different port number.
# lport or rport can be used
# to denote different ports
# for local and remote.
port 1194

# Downgrade UID and GID to
# "nobody" after initialization
# for extra security.
user nobody
group nobody

persist-key
persist-tun
```

```
# Send a UDP ping to remote once
# every 15 seconds to keep
# stateful firewall connection
# alive.  Uncomment this
# out if you are using a stateful
# firewall.
ping 15
#keepalive 10 60

# Verbosity level.
# 0 -- quiet except for fatal errors.
# 1 -- mostly quiet, but display non-fatal network errors.
# 3 -- medium output, good for normal operation.
# 9 -- verbose, good for troubleshooting
verb 3
```

Per far partire il client, eseguire questi comandi (ip di esempio, da cambiare con i corretti)

```
# /usr/local/etc/rc.d/openvpn start
Starting openvpn.
add net 10.55.0.0: gateway 192.168.100.3
```

Di seguito un esempio di quello che dovreste vedere in /var/log/messages

```
openvpn[62722]: OpenVPN 2.0.6 i386-portbld-freebsd6.3 [SSL] [LZO] built on Nov
26 2008
openvpn[62722]: WARNING: --ping should normally be used with --ping-restart or
--ping-exit
openvpn[62722]: Control Channel MTU parms [ L:1573 D:138 EF:38 EB:0 ET:0 EL:0 ]
openvpn[62722]: gw 64.147.113.41
openvpn[62722]: TUN/TAP device /dev/tap0 opened
openvpn[62722]: /sbin/ifconfig tap0 192.168.100.2 netmask 255.255.255.0 mtu 1500
up
openvpn[62722]: /sbin/route add -net 10.55.0.0 192.168.100.3 255.255.255.0
openvpn[62722]: Data Channel MTU parms [ L:1573 D:1450 EF:41 EB:4 ET:32 EL:0 ]
openvpn[62722]: Local Options hash (VER=V4): 'ea8adc0d'
openvpn[62722]: Expected Remote Options hash (VER=V4): '6ab3b73a'
openvpn[62727]: GID set to nobody
openvpn[62727]: UID set to nobody
openvpn[62727]: UDPv4 link local (bound): [undef]:1194
openvpn[62727]: UDPv4 link remote: 172.28.123.191:1194
openvpn[62727]: TLS: Initial packet from 172.28.123.191:1194, sid=9a791e73
6db7b2f9
openvpn[62727]: VERIFY OK: depth=1, /C=US/ST=PA/L=Warrington/O=The_FreeBSD_Diary
                                     /emailAddress=dan@example.com
openvpn[62727]: VERIFY OK: nsCertType=SERVER
openvpn[62727]: VERIFY OK: depth=0,
/C=US/ST=PA/O=The_FreeBSD_Diary/CN=myserver.example.com
                                     /emailAddress=dan@example.com
openvpn[62727]: Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit
key
openvpn[62727]: Data Channel Encrypt: Using 160 bit message hash 'SHA1' for
                                      HMAC authentication
openvpn[62727]: Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit
key
openvpn[62727]: Data Channel Decrypt: Using 160 bit message hash 'SHA1' for
```

```
                                        HMAC authentication
openvpn[62727]: Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA,
1024 bit RSA
openvpn[62727]: [myserver.example.com] Peer Connection Initiated with
172.28.123.191:1194
openvpn[62727]: Initialization Sequence Completed
```

Sul server dovreste vedere una cosa simile a:

```
bast openvpn[52597]: TLS: new session incoming connection from
172.10.10.101:1194
bast openvpn[52597]: VERIFY OK: depth=1,
/C=US/ST=PA/L=Warrington/O=The_FreeBSD_Diary
                                          /emailAddress=dan@example.com
bast openvpn[52597]: VERIFY OK: depth=0, /C=US/ST=PA/O=The_FreeBSD_Diary
                                          /CN=client.example.com
                                          /emailAddress=dan@example.com
bast openvpn[52597]: Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128
bit key
bast openvpn[52597]: Data Channel Encrypt: Using 160 bit message hash 'SHA1' for
                                            HMAC authentication
bast openvpn[52597]: Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128
bit key
bast openvpn[52597]: Data Channel Decrypt: Using 160 bit message hash 'SHA1' for
                                            HMAC authentication
bast openvpn[52597]: TLS: move_session: dest=TM_ACTIVE src=TM_UNTRUSTED
reinit_src=1
bast openvpn[52597]: TLS: tls_multi_process: untrusted session promoted to
trusted
bast openvpn[52597]: Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-
SHA,
                                        1024 bit RSA
```

Sul client dovreste vedere la tap device cosi':

```
# ifconfig tap0
tap0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet 192.168.100.2 netmask 0xffffff00 broadcast 192.168.100.255
        ether 00:bd:10:e7:72:00
        Opened by PID 62722
```

Test delle comunicazioni:
Questi test vengono svolti sul client
Test di connessioni, è possibile pingare la macchina con la VPN installata?

```
# ping -c 5 192.168.100.2
PING 192.168.100.2 (192.168.100.2): 56 data bytes
64 bytes from 192.168.100.2: icmp_seq=0 ttl=64 time=0.043 ms
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=0.035 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=0.028 ms

--- 192.168.100.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.028/0.037/0.043/0.005 ms
```

Test di connessioni, è possibile pingare la macchina remota sulla VPN?

```
# ping -c 5 192.168.100.3
PING 192.168.100.3 (192.168.100.3): 56 data bytes
64 bytes from 192.168.100.3: icmp_seq=0 ttl=64 time=30.379 ms
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=39.191 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=15.725 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=17.148 ms
64 bytes from 192.168.100.3: icmp_seq=4 ttl=64 time=21.225 ms

--- 192.168.100.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 15.725/24.734/39.191/8.853 ms
```

Se non si riesce a pingare la VPN remota, è necessario controllare le tabelle di routing, le regole del firewall.
Se il ping funziona il traffico dal client al server dovrebbe funzionare.
Se si riscontrano errori sul server quali “Unroutable control packet” controllare in /var/log/messages

Allegato 1: Charter for the use of IT resources and internet services

The purpose of this document, in conjunction with the entities' by-laws, is to set forth the responsibility of users in-line with legislation, so as to establish compliant use of the IT resources and Internet services which the CNRS and, where applicable, other establishments, manage. These resources and services represent a major element of the CNRS' scientific and technical asset base.

The due and proper operation of the information system requires compliance with the relevant legislative and regulatory provisions and, in particular, security, processing performance levels and the retention of professional data.

1. Definitions

Generally speaking, the following shall be designated as *"IT resources*": the networks, the IT calculation or local management equipment, and that which is able to be remotely accessed, either directly or in cascade mode from the entity's network, the software, applications, databases...

The following shall be designated as *"Internet services*the provision by local or remote servers of sundry exchange and information resources: web, message application, chat-room, IP (Internet Protocol) telephony, videoconferencing...

"User" shall mean the person having access to, or using, the IT resources and Internet services no matter what his/her status may be.

"Entity" shall mean all the entities created by the CNRS in order to carry out its assignments such as, in particular, its in-house or combined research units and the administrative departments and divisions.

2. Access to IT resources and Internet services

Use of the IT resources and Internet services, and the network to access the former, is destined for the professional activity of users in compliance with effective legalisation. Professional activity shall be understood as having the meaning defined in the documents setting forth the CNRS' assignments.

Use of the entity's shared IT resources and the connection of private, external equipment (such as a computer, switch, modem, wireless access station...) to the network is subject to the authorisation of the entity's manager and to the entity's security rules. Such authorisations shall be strictly personal and may not, under any circumstances, be transferred to a third party, even temporarily. They may be withdrawn at any time. All authorisations shall be cancelled when the professional activity justifying such comes to an end.

In addition, the entity may introduce access restrictions which are specific to its organisation (electronic certificates, access or authentication chip cards, secure access filtering,...).

3. Rules of use and security

All users are responsible for the use made of the IT resources to which they have access.

Use of these resources must be rational and compliant in order to avoid saturation or their misuse for personal purposes.

In particular:

3.1 Security rules

■ they shall apply the security recommendations made by the entity to which they belong and, in particular, comply with the systems implemented by the entity to combat viruses and attacks by IT programs,

■ they are responsible for protecting their data by using various individual back-up methods, or those provided to them,

■ they shall protect their information and, particularly, that which is deemed as being sensitive within the meaning of the information systems' security policy (CNRS' ISSP (PSSI)). Notably, they shall not transport, without relevant protection (such as encryption), sensitive data on mediums which have not been burnt-in, such as laptops, USB keys, external hard drives, etc... These mediums, which are known as "mobile IT equipment", make the IT resources vulnerable and shall therefore be subject to the entity's security rules and shall be used in accordance with the provisions of this charter,

■ they shall guarantee permanent access to their professional data within the context of the data recovery policy[1] implemented within the entity,

■ they shall not leave their work station, or the work stations which are available for use by everyone, without first shutting-down the resources or ensuring that the services are not accessible.

3.2 Rules of use

■ All information is considered as being professional with the exception of data which the user specifically identifies as relating to his/her private life. Consequently, the user is responsible for storing any personal data in directories which are specifically created for this purpose and which are designated as being "private".

The user is responsible for the protection and regular back-up of the data In these files and the entity may not be held liable as regards the retention of this storage space,

■ Users shall comply with the effective rules within the entity as regards installing any and all software and shall not download onto, or use software or software packages on, the entity's equipment without express authorisation.

In particular, they shall not install game-type software, or fail to comply with the restrictions relating to use of a software application. The software shall be used under the conditions of the licences granted,

■ they shall ensure the protection of the various personnel means of authentication. In particular, they shall choose fail-safe passwords, which shall be kept secret, and which they shall under no circumstances pass-on to third parties. If, in exceptional and one-off circumstances, a user were to be obliged to communicate his/her password, he/she shall ensure that the latter is changed as soon as reasonably possible. He/she shall also protect his/her electronic certificate by a fail-safe password which he/she shall keep secret. As with handwritten signatures, the electronic certificate is strictly personal and the user undertakes not to allow anyone to use it in his/her place,

■ they shall report any attempted hacking of their account and, generally, any and all anomaly which they may note,

[1] Recovery is the safety measure allowing an authorised person access to data when the main system is no longer able to be used (loss or destruction of the key, forgotten password,...) or in the event of the unavailability of the key owner (*agent détenteur).*

■ they undertake not to provide (an) unauthorised user(s) with access to the IT resources or to the Internet services, via the equipment which they are entitled to use, ■ they shall not use, or attempt to use, accounts other than their own or conceal their identity,

■ they shall not access information and documents saved in the IT resources other than those belonging to them, and those which are either public or shared. They shall not attempt to read, modify, copy or destroy them, even if access thereto is technically possible.

4. Compliance with the Act on information technology and civil liberties[2]

If, whilst carrying out his/her work, the user is obliged to create files which are subject to the provisions of the Act "*informatique et libertés",* he/she shall carry out the formalities required by the CNIL through the CNRS' information systems' division, together with the manager of his/her entity and shall ensure that the data is processed in accordance with legal provisions. It is hereby stipulated that this procedure is only valid for the processing defined in the request and not for the file itself.

5. Respect for intellectual property

The user shall not reproduce, download, copy, distribute, modify or use software, databases, web pages, photographs or other creations which are protected by copyright or by a proprietary claim, without having obtained the prior authorisation of the holder of such rights.

6. Preservation of the integrity of the IT resources

The user undertakes not to voluntarily cause disruption to the due and proper operation of the IT resources and networks, either by abnormal manipulation of the equipment, or by installing parasite software known under the generic name of viruses, Trojan horses, logic bombs...

All research or other work which may cause a violation of the rule set forth in the previous paragraph may only be carried out with the authorisation of the entity's manager, and in strict compliance with the rules which may be defined in this case.

7. Use of Internet services (web, message application, chat-room, IP telephony...) 7.1 Internet

The Internet is a work tool which is available for professional use and its use shall comply with the general principles and the rules which are specific to the different sites which offer such professional content, and with effective legislation.

In particular, the user:

■ shall not log-on, or attempt to log-on, to a server by means other those complying with the provisions provided for by such server, or without being authorised to do so by the authorised managers,

[2] The CNRS[1] CNIL Guide, which was published in 2006, reiterates the main principles governing the creation or use of personal data processing (the rights and obligations of all parties and the formalities to be carried out).

■ shall not carry out acts which intentionally compromise the security or due and proper operation of the servers to which he/she has access,

■ shall not take the identity of any and all other person and shall not intercept communications between third parties,

■ shall not use these services to offer, or to provide, third parties with data and information which is confidential or which violates effective legislation,

■ shall not leave data on an in-house server or a server which is accessible by the general public (google, tree, orange, ...) or on another user's work station, unless he/she is authorised to do so by the authorised managers,

■ shall ensure the highest standards of politeness vis-a-vis his/her contacts in electronic exchanges either by e-mail or in chat-rooms...,

■ shall not state personal opinions which are unrelated to his/her professional activity and which may be detrimental to the CNRS,

■ shall ensure that he/she complies with legislation and, in particular that relating to offensive, racist, pornographic, defamatory publications.

The entity may not be held liable for the deterioration of information or for violations committed by a user who has failed to comply with these rules.

7.2 Electronic message application

The electronic message application is a work tool which ¡s available for professional use.

■ All messages shall be deemed as being professional unless they specifically and explicitly mention their private nature on the subject line, or unless they are stored in a private data storage space.

■ All users shall organise and implement the means required to save messages which may be essential or simply useful as elements of proof.

■ It is forbidden to send classified data[3] unless specific provisions have been authorised, and so-called sensitive data should either not be sent or sent in encrypted form.

■ The user shall ensure that messages are only sent to the relevant recipients so as to avoid mass-mailing, the unnecessary clogging-up of the message application, and a reduction in service level.

► The permanent progression of IT technologies provides users with new services which may be accessed via their entities' network. Such new technologies, which may create a specific vulnerability risk, may only be used with the prior agreement of the entity's manager and in strict compliance with the information systems' security policy (CNRS' 1SSP).

8. Analysis and verification of use of the resources

For the purposes of technical maintenance and management, verification for statistical purposes, tracking, optimisation, security or the detection of misuse, use of the IT resources and the Internet services, and exchanges via the network, may be analysed and verified in compliance with applicable legislation, in particular, the Act on information technology and civil liberties.

Users whose work stations are subject to remote maintenance shall be informed thereof beforehand.

[3] This means classified defence data which covers "confidential defence", "secret defence" and "top secret defence" data.

Staff responsible for the verification work are subject to a non-disclosure obligation. Consequently, they may not disclose the information of which they become aware whilst carrying out their duties, in particular when such information is covered by secrecy of correspondence or relates to the user's private life, provided such information does not compromise either the due and proper technical operation of the applications, or their security, or the interest of the department.

9. Tracking

The CNRS is legally obliged to introduce a logging system of Internet access, the message application and exchanged data.

Consequently, tracking tools are installed in all the information systems.

The CNRS has submitted a declaration to the CNIL mentioning, in particular, the period during which connection tracking and time records are kept, under the effective legislation.

10. Reminder of the main legal provisions

It is hereby reiterated that all the CNRS' officers, no matter what their status may be, are subject to effective French legislation and, in particular:

► the Act of 29 July 1881, as modified, on the freedom of the press,

► the Act no. 78-17 of 6 January 1978, as modified, on information technology, files and civil liberties,

► legislation relating to the corruption of the automated processing of data (Art. L 323-1 *et seq.* of the French Penal Code),

► the Act no. 94-665 of 4 August 1994, as modified, on the use of the French language,

► the Act no. 2004-575 on 21 June 2004 on confidence in the digital economy,

► the provisions of the French Intellectual Property Code on literary property and copyright.

11. Application

This charter applies to all officers of the CNRS' entities, no matter what their status may be and, more generally, to all persons, whether permanent or temporary [employees], who use, in any capacity whatsoever, the entity's IT resources and Internet services, and those which may be remotely accessed, either directjy or in cascade mode, from the entity's network.

The persons referred to in the previous paragraph shall be informed of the charter by any and all means and, in particular:

> by a message sent on the message application when the user has an account, with the latter being obliged to represent that he/she has familiarised him/herself with this charter, by means of displaying in the entity's premises, by means of an appendix to the entity's by-laws, or by the supplying of a hard copy of the charter.

The charter may be appended to employment contracts and to procurement contract agreements, for which the performance requires access to the CNRS' IT resources and Internet services.

The charter is also available in English. Only the French version shall be deemed authentic.