

Zeroshell: access point

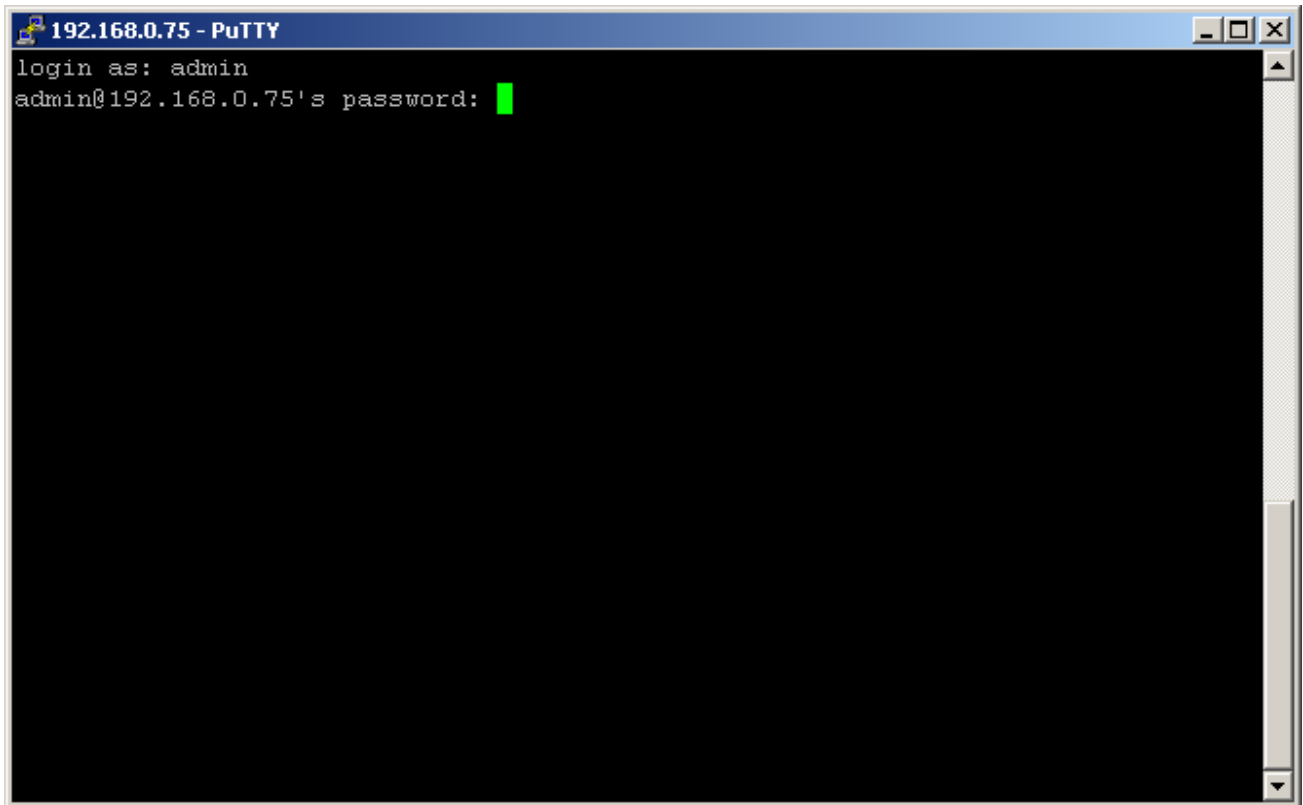


Il sistema operativo multifunzionale
creato da Fulvio.Ricciardi@zeroshell.net
www.zeroshell.net

Situazione in cui Zeroshell lavora come access point
(Autore: cristiancolombini@libero.it)

CONFIGURARE ZEROSHELL COME ACCESS POINT:

Una volta installato Zeroshell ed avviato il sistema, sulla console dello stesso o tramite ssh (usando per esempio Putty) si trovano i comandi per attivare la scheda wireless premendo il tasto W (WiFi Manager):



```
192.168.0.75 - PuTTY
login as: admin
admin@192.168.0.75's password: █
```

```
192.168.0.75 - PuTTY
-----
Z e r o S h e l l - Net Services 1.0.beta8      February 13, 2008 - 20:26
-----
Hostname : fw.lordch.net
CPU (1)  : Pentium III (Coppermine) 731MHz
Kernel   : 2.6.19.7
Memory   : 125196 kB                    https://192.168.0.75
Uptime   : 0 days, 0:18                 User      : admin
Load     : 0.00 0.01 0.00                Password  : zeroshell
Database : 4feb2008
-----
COMMAND MENU
<A> Activate database          <P> Change admin password
<D> Deactivate database       <T> Show Routing Table
<S> Shell Prompt              <F> Show Firewall Rules
<R> Reboot                    <N> Show Network Interface
<H> Shutdown                  <Z> Fail-Safe Mode
<B> Create a Bridge           <I> IP Manager
<W> WiFi Manager

                               Select: █
```

In alto si vede l'hardware rilevato:

```
192.168.0.75 - PuTTY
[wifi0] Chipset AR5212/AR5213 Multiprotocol MAC/baseband processor (rev 01)
-- If -- Mode -- SSID ----- Hide -- Security --

COMMANDS
<N> New SSID                   <M> Modify SSID
<D> Delete SSID                <I> Show Information
<C> Std/Channel/Tx-Power       <S> Channel Scanning
<L> List Stations              <Q> Quit
<R> Restarting Devices

>> █
```

Col tasto **N** settiamo seguiamo la procedura che ci aiuta a configurare il dispositivo “wifi0” (fra parentesi quadra ci viene mostarto il [**valore di default**] che si può confermare semplicemente con invio :

```
[wifi0] Chipset AR5212/AR5213 Multiprotocol MAC/baseband processor (rev 01)
-- If -- Mode -- SSID ----- Hide -- Security --
```

```
COMMANDS
  <N> New SSID           <M> Modify SSID
  <D> Delete SSID       <I> Show Information
  <C> Std/Channel/Tx-Power
  <L> List Stations     <S> Channel Scanning
  <R> Restarting Devices <Q> Quit
```

```
>> n
```

```
wifi0 - Chipset AR5212/AR5213 Multiprotocol MAC/baseband processor (rev 01)
```

```
WiFi device on which you want to add a new SSID [wifi0]:wifi0
```

```
Creating interface for the new SSID ...
```

```
Detecting ethernet interfaces...
```

```
ETH02 (new) : Atheros Communications, Inc. AR5212/AR5213 Multiprotocol
MAC/baseband processor (rev 01)
```

```
<1> Access Point
<2> Client Station
```

```
Mode [1]:1
```

```
SSID [SSID-064096B5AE45]: Colombo
```

```
Hide SSID [no]: no
```

A questo punto ci viene proposto di configurare la sicurezza di accesso alla nostra rete wireless:

```
<1> Plaintext (No encryption)
<2> WPA-EAP/RSN/802.1x+WEP (RADIUS authentication)
<3> WPA-PSK (Pre-Shared Key)
<4> WEP
```

```
Encryption [1]:
```

Finire questa procedura vedendo nei dettagli di seguito i 4 casi.

In ciascuno dei 4 casi, dopo aver terminato la procedura guidata, entriamo in configurazione via web ed assegnamo un indirizzo ip alla scheda di rete ETH02:

<input type="radio"/> ETH02	AP:064096B5AE45	Freq:2.412 GHz (Channel 1)	Tx-Power:20dBm (100mW)	UP
WiFi - [SSID:Colombo] [Mode:ap] [Security:wpa-eap] [Hidden:no]				<input checked="" type="checkbox"/>
<input type="radio"/> 192.168.2.75	255.255.255.0			<input checked="" type="checkbox"/>

Dynamic IP: 0.0.0.0	MAC: 064096B5AE45	Show Info	
Dyn.IP	Add IP	Edit IP	Remove IP

Primo caso: <1> Plaintext (No encryption)

Configuriamo l'accesso alla rete wireless in modo non protetto:

```
Encryption [1]: 1
```

```
WARNING: SSID Colombo is not authenticated and not encrypted.
```

```
Starting WiFi subsystem ...
```

```
Loading Kernel modules (MadWifi) for Atheros Chipsets ...
```

```
Configuring physical WiFi devices ( wifi0 )
```

```
Creating virtual WiFi interfaces:
```

```
ETH02(wifi0) (Mode:ap Sec:plaintext SSID:Colombo)
```

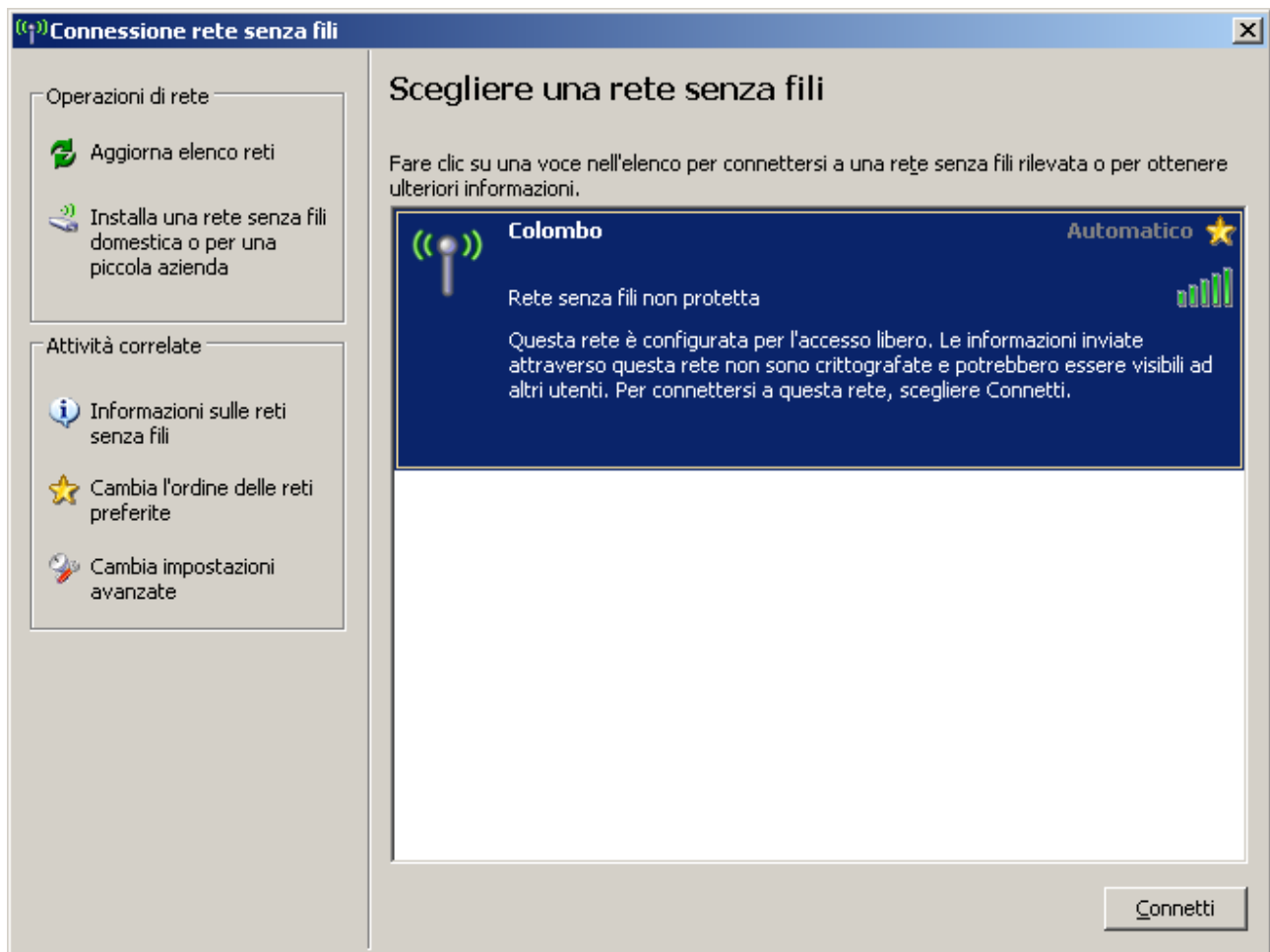
```
Running WiFi /etc/rc.wifi script ...
```

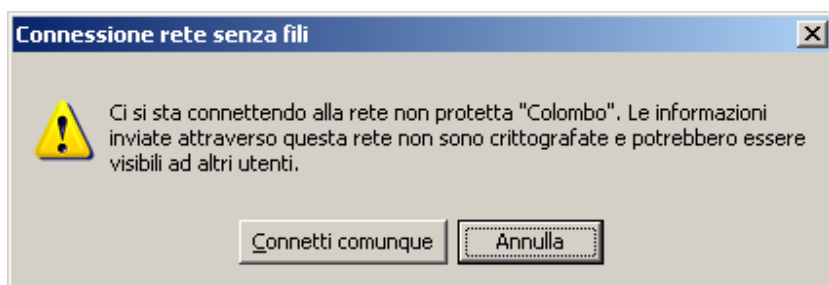
```
[wifi0] Chipset AR5212/AR5213 Multiprotocol MAC/baseband processor (rev 01)
```

```
-- If -- Mode -- SSID ----- Hide -- Security --
```

```
>> ETH02 AP Colombo no Plaintext
```

Ecco che il nostro access point comincia a dare connettività in modo non protetto ed in windows la rete wireless viene connessa senza protezioni:





Connetti comunque:

Connessione rete senza fili (Colombo)
Velocità: 54.0 Mbps
Potenza segnale: Eccellente
Stato: Connesso.

Ricordiamoci in tutti questi casi che ovviamente la scheda di rete wireless del pc deve avere un indirizzo ip della stessa rete della scheda wireless del firewall; come gateway (e se si vuole anche dns server) l'indirizzo ip della scheda wireless del firewall.

Secondo caso: <2> WPA-EAP/RSN/802.1x+WEP (RADIUS authentication)

Scegliamo questa opzione per dare l'accesso alla nostra rete wireless in modo sicuro solo ad alcuni utenti che possiedono determinati requisiti.

Encryption [1]: 2

- <1> Local RADIUS server
- <2> External RADIUS server

RADIUS type [1]: 1

Starting WiFi subsystem ...

```
Loading Kernel modules (MadWifi) for Atheros Chipsets ...
Configuring physical WiFi devices ( wifi0 )
Creating virtual WiFi interfaces:
ETH02(wifi0) (Mode:ap  Sec:wpa-eap  SSID:Colombo)
Running WiFi /etc/rc.wifi script ...
```

```
[wifi0] Chipset  AR5212/AR5213 Multiprotocol MAC/baseband processor (rev 01)
-- If -- Mode -- SSID ----- Hide -- Security -
>> ETH02  AP      Colombo                               no   WPA-EAP
```

Scegliamo di usare il server Radius interno di Zeroshell con la scelta 1.

Ora bisogna fare 3 semplici passi in configurazione del firewall:

1 - Creare un certificato del firewall entrando nella voce "X.509 CA" nel menu a sinistra della pagina di configurazione del firewall:

X.509 CA | List | Manage | CRL | Imported | Trusted CAs | Setup

CA Certificate and Private Key [Generate] [Export] Key [PEM]

Common Name: LordCH

Key Size: 1024 bits

Validity (Days): 3650 Expire: Feb 4 23:02:42 2018 GMT

Country Name: IT Status: OK

State or Province:

Locality:

Organization: lordch.net

Organizational Unit: firewall-ap

E-Mail Address: cristiancolombini@liber

Importing CA from external source [Import]

Private Key: [Sfoglia...]

Certificate: [Sfoglia...]

CA Default Parameters [Apply]

Key Size: 1024 bits

Certificate Validity (days): 365

Personalizzare i campi e poi cliccare su GENERATE.

2 - Attivare poi il server Radius dal menu a sinistra RADIUS:

RADIUS Manage Access Points Proxy

RADIUS Server for Wireless and Identity Based Networking Services

Status: **ACTIVE** Enabled Show Requests 802.1x

802.1x Configuration Save Cancel

X.509 Host Certificate

Local CA OU=Hosts, CN=fw.lordch.net

View Status: **OK** Check CRL Imported Trusted CAs

Flaggare Enable e cliccare il bottone SAVE

3 - Creare l'utente dal menu a sinistra USERS:

USERS List View Add Edit Delete X509 Kerberos 5

cristian colombini - lordch net (cristian) Submit Reset

Account

Username cristian UID 1 Primary Group nobody GID 65534

Home Directory /home/cristian Default Shell bash sh tcsh other /bin/sh

User Information

Firstname cristian Lastname colombini Organization lordch net

Description cristian colombini - lordch net E-Mail cristiancolombini@libero.it Phone ?

User Password

Password

Confirm

Enabled Services

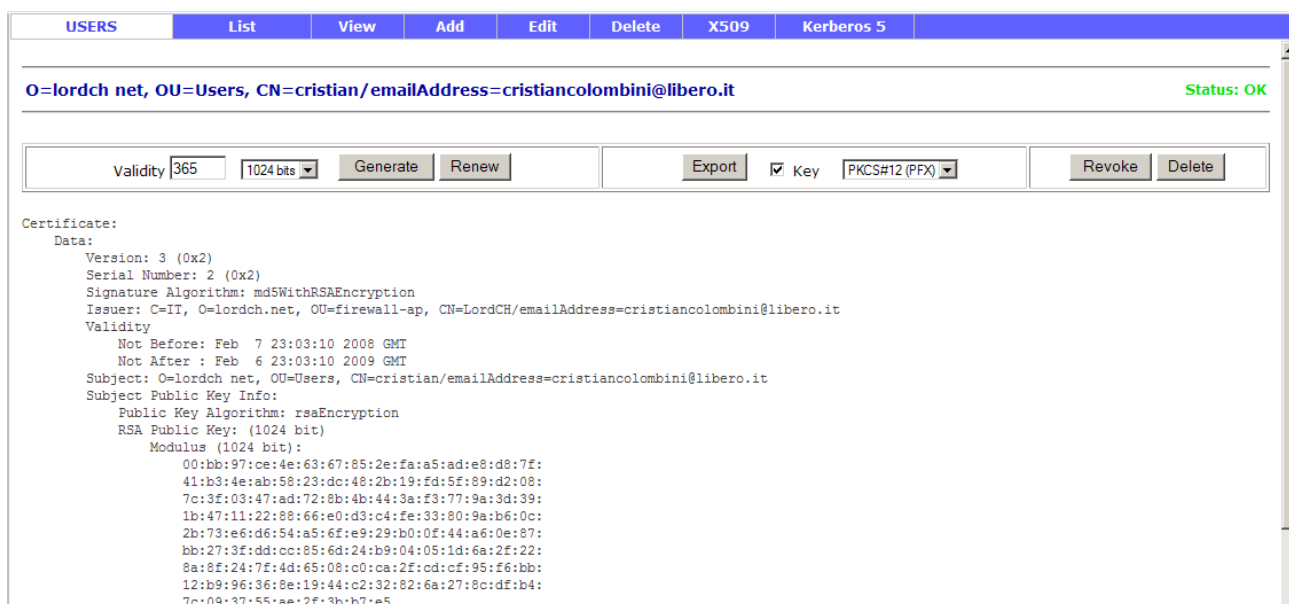
Kerberos 5 Authentication

Host-to-Lan VPN (L2TP/IPsec)

802.1X Access (VLAN)

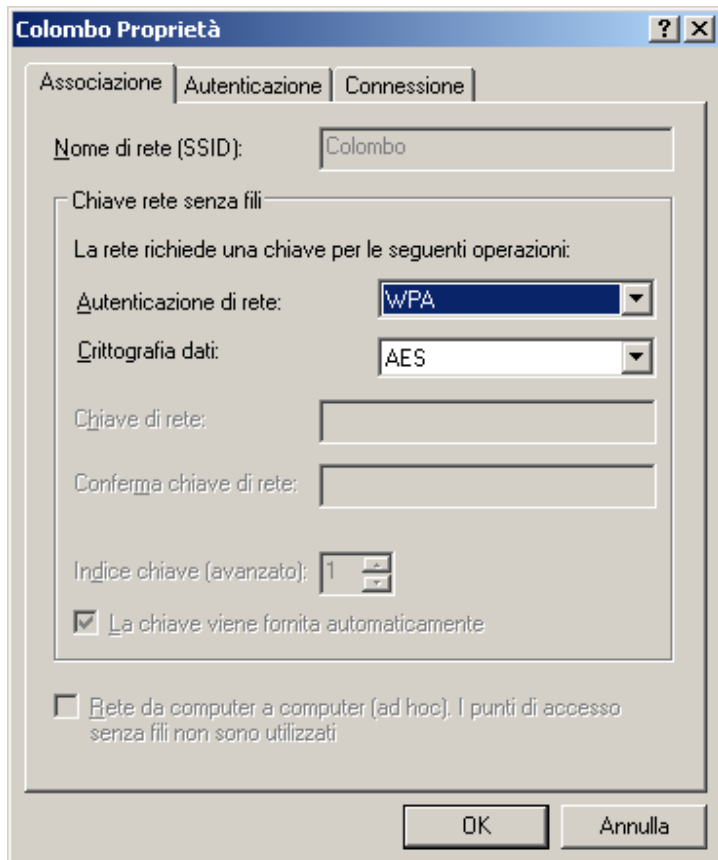
Per configurare il client Ms Windows xp

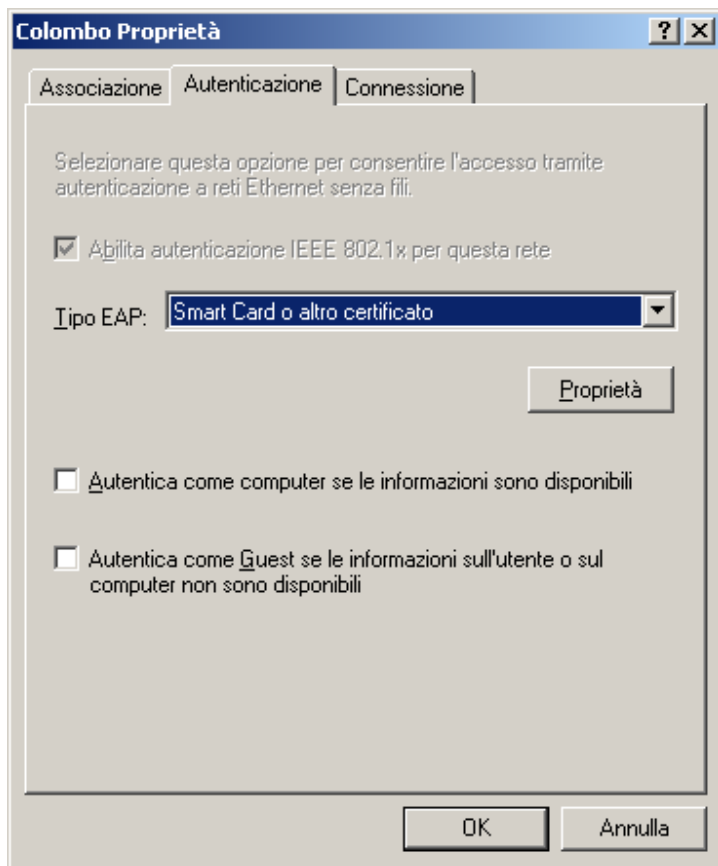
esportare il certificato dell'utente ed installarlo sul pc (scegli l'utente col bottone radio, clicca X509 ed export):



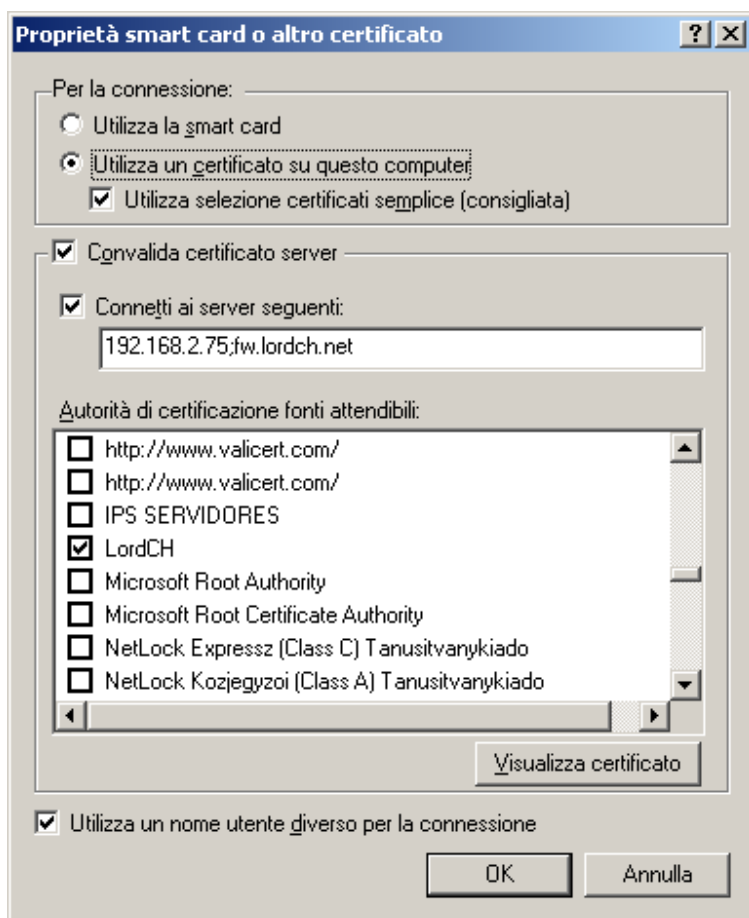
Seguire la procedura guidata di installazione del certificato: dopo averlo salvato sul pc basta fare doppio clic sul certificato stesso.

Entrare nella configurazione della scheda di rete e seguire quanto nelle immagini:

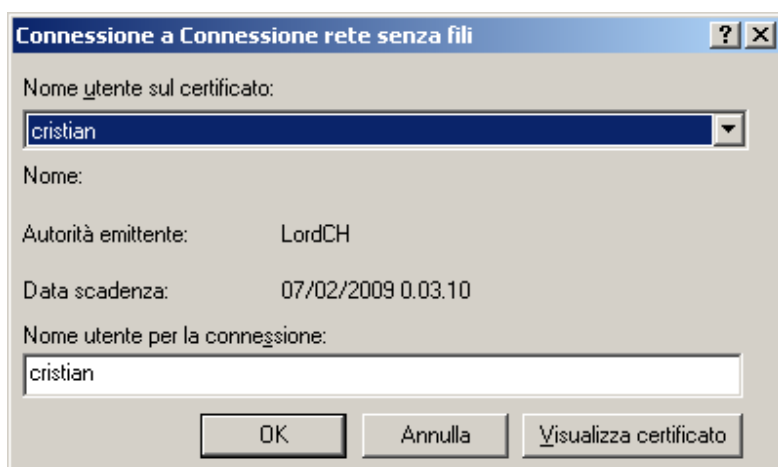




Cliccare sul bottone Proprietà:



Notare che il pc deve trovare il firewall per nome: fw.lordch.net per autenticarsi; quindi il campo “connetti ai server seguenti” va compilato con “indirizzo ip della scheda del firewall” ; “nome host del firewall”. Selezionare poi fra i certificati quello giusto relativo al nostro firewall (LordCH nel mio caso). Se necessario avere conferma visiva dell’utente che viene utilizzato tramite il certificato, flaggare “Utilizza un nome utente diverso per la connessione”. Abilitare la connessione; ci verrà chiesto:





La rete verrà connessa.

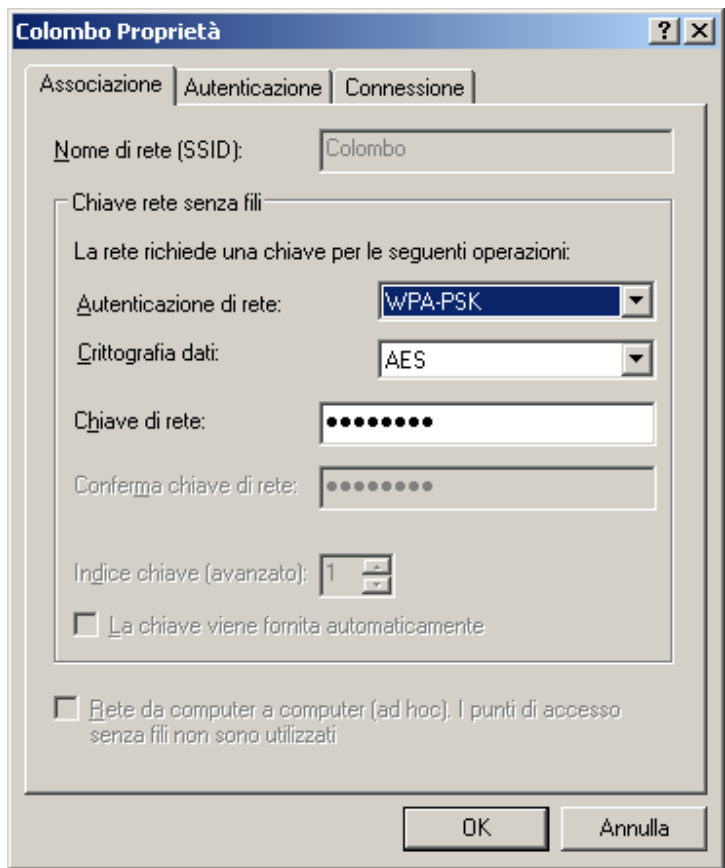
Terzo caso: <3> WPA-PSK (Pre-Shared Key)

```
Encryption [3]: 3
Pre-Shared Key [Zeroshell Net Services]: 12
The size of this value must be between 8 and 64.
Pre-Shared Key [Zeroshell Net Services]: 12345678
Starting WiFi subsystem ...
```

```
Loading Kernel modules (MadWifi) for Atheros Chipsets ...
Configuring physical WiFi devices ( wifi0 )
Creating virtual WiFi interfaces:
ETH02(wifi0) (Mode:ap Sec:wpa-psk SSID:Colombo)
ETH02: 192.168.2.75/255.255.255.0
Running WiFi /etc/rc.wifi script ...
```

```
[wifi0] Chipset AR5212/AR5213 Multiprotocol MAC/baseband processor (rev 01)
-- If -- Mode -- SSID ----- Hide -- Security -
>> ETH02 AP Colombo no WPA-PSK
```

Se sull'access point si sceglie 3) WPA-PSK (pre-shared key), viene chiesto di impostare una password; questa dovrà essere di almeno 8 caratteri. Tale pre-shared-key consentirà ai client che la possiedono nella loro configurazione di accedere alla rete wireless. Nel client windows:



Quarto caso: <4> WEP

```
Encryption [1]: 4  
WEP Key [Zeroshell Net]: 1234567890123  
Key index [1]: 1
```

Starting WiFi subsystem ...

```
Loading Kernel modules (MadWifi) for Atheros Chipsets ...  
Configuring physical WiFi devices ( wifi0 )  
Creating virtual WiFi interfaces:  
ETH02(wifi0) (Mode:ap Sec:wep SSID:Colombo)  
Running WiFi /etc/rc.wifi script ...
```

```
[wifi0] Chipset AR5212/AR5213 Multiprotocol MAC/baseband processor (rev 01)  
-- If -- Mode -- SSID ----- Hide -- Security --  
>> ETH02 AP Colombo no WEP128
```

Se sull'access point si sceglie 4) WEP viene chiesta la WEP Key di 13 caratteri: "1234567890123" e la Key index: 1

Nel client windows:

