

1. La rete wireless per noi.

Stiamo allestendo un servizio di rete wireless esteso per quanto possibile a tutto il Dipartimento. Per cominciare le antenne sono state disposte nei luoghi in cui è più difficile offrire un cavo a ogni computer e cioè le zone di riunione: l'aula Rostagni, l'aula S, l'aula T e l'aula R. Abbiamo proseguito con qualche base ai piani. Chi ha già usato il wireless in Istituto, sa che è necessario registrare il Mac address della propria scheda di rete rivolgendosi al servizio calcolo, questa procedura resta valida anche adesso.

Le reti su cui ci si può collegare si chiamano **pd-wep** e **pd-wpa** e sono reti che usano cifratura e autenticazione.

La differenza tra pd-wep e pd-wpa sta nel tipo di cifratura e nella gestione della sicurezza del collegamento; pd-wep segue uno standard non a prova di bomba, ma molto diffuso, mentre pd-wpa garantisce maggior sicurezza ma non è supportato da tutte le schede, né da tutti i sistemi operativi. L'accesso alle reti richiede la *registrazione del mac address*, come già detto, l'uso del proprio *username*, quello dei mail, e della propria *password di Windows*. Chi non ha mai usato la password di Windows può definirselo autonomamente andando alla pagina <https://webmail.pd.infn.it/cgi-bin/passwd.pl>.

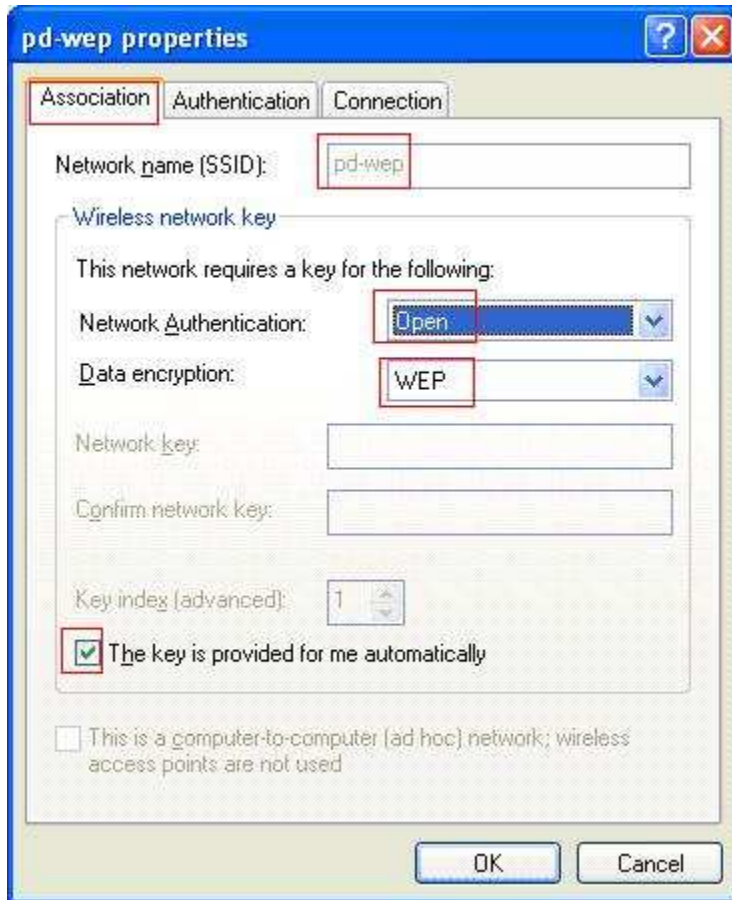
La configurazione della rete wireless sul proprio portatile varia a seconda dei computer e dei sistemi operativi; alcune marche offrono programmi specifici perciò è difficile fornire una ricetta per tutti. Per chi ha familiarità con il wireless le linee guida sono le seguenti:

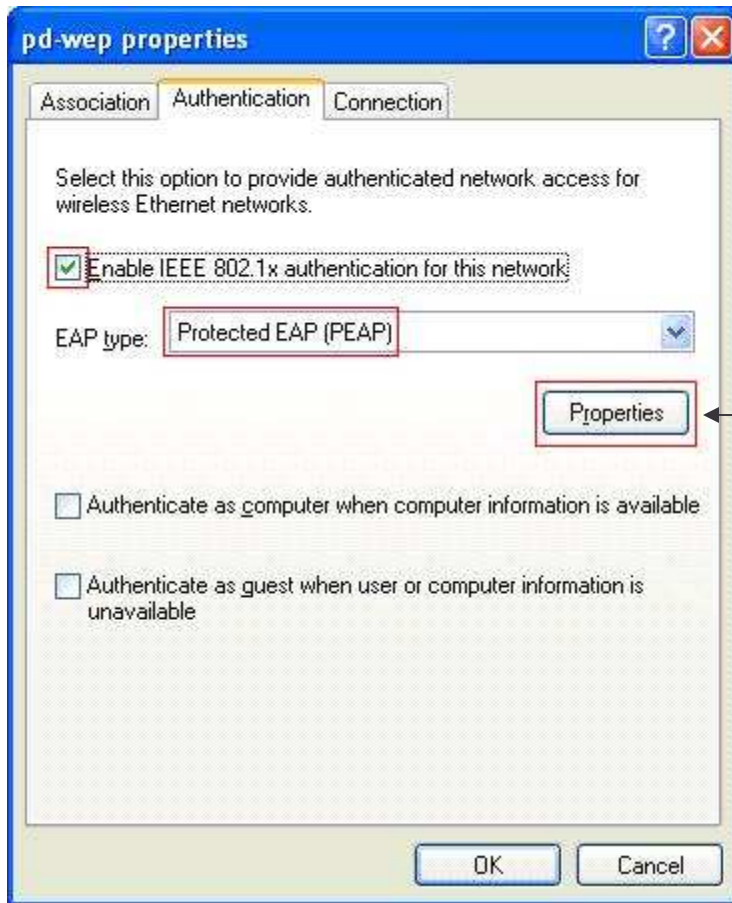
| SSID | pd-wep | pd-wpa |
|------------------------|----------|-----------------------|
| Network authentication | open | wpa2 (wpa enterprise) |
| Encription | wep | aes o ccmp |
| Eap type | peap | peap |
| Authentication method | mschapv2 | mschapv2 |

Qui sotto troverete due esempi di configurazione uno per Windows e uno per Linux.

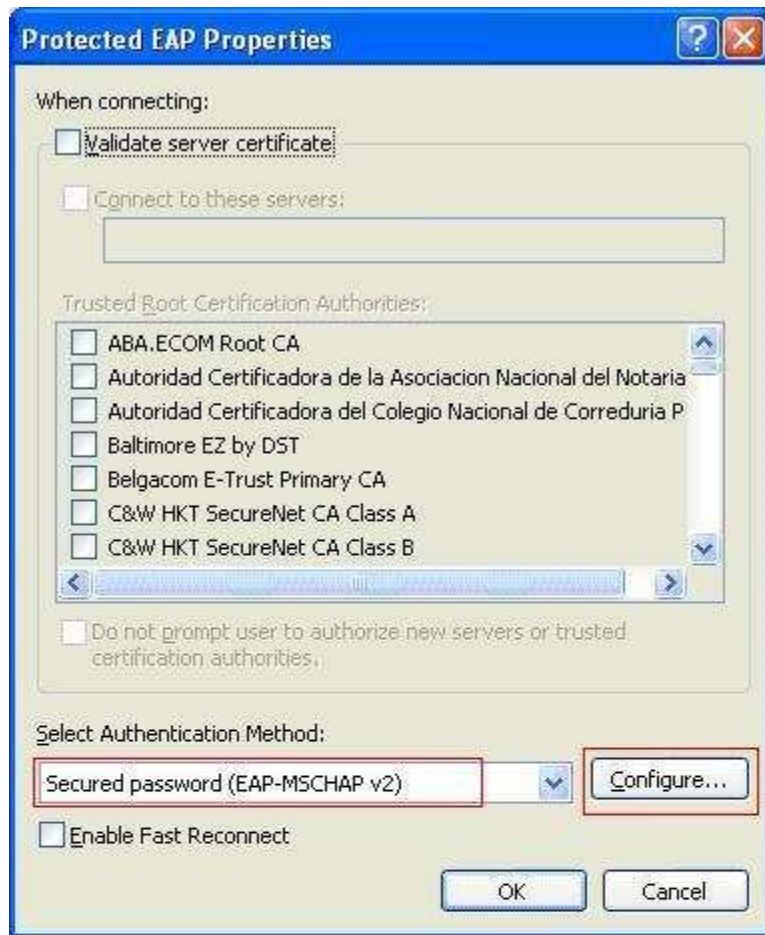
Windows.

Questo è un esempio di configurazione delle proprietà della rete pd-wep per Windows Xp SP2. Ho messo un rettangolo rosso intorno a quello da modificare o da verificare.





Selezionare



ATTENZIONE: quando inserite le credenziali il campo domain va lasciato vuoto.

La configurazione di pd-wpa è analoga, bisogna però che sul computer con Xp sia installata la service pack 2 e la patch KB917021 per poter disporre di WPA2, a meno che non si abbia già un programma proprietario che lo fornisca. È importante avere WPA2 perché è lo standard accettato dal progetto Trip che permette la connessione wireless nelle Sezioni INFN, autenticandosi con lo username e la password della propria Sezione.

Linux.

Devono essere installati i wireless tools (iwconfig, ecc), un driver che supporti 802.1x (madwifi per esempio) e wpa_supplicant.

Se non avete il wpa_supplicant potete trovarlo alla Url
http://atrpms.net/dist/el4/wpa_supplicant/

Nel file di configurazione (che potrebbe essere /etc/wpa_supplicant.conf) bisogna inserire:

```
network={
    ssid="pd-wpa"
    proto=WPA2
    scan_ssid=1
    key_mgmt=WPA-EAP
    pairwise=CCMP
    group=CCMP
    eap=PEAP
    phase2="auth=MSCHAPV2"
    identity="user name"
    password="password"
}
```

Start del daemon:

```
wpa_supplicant -B -w -iath0 -Dmadwifi -c /etc/wpa_supplicant.conf
```

Dove:

-B indica lo start in background

-w mette il processo in attesa dello start della scheda di rete

-i deve essere seguito dal nome dell'interfaccia di rete wireless (ath0 nell'esempio, ma potrebbe avere un nome diverso)

-D deve essere seguito dal nome del driver, se non funziona madwifi può essere utilizzato wext (l'help del comando elenca i driver supportati)

-c seguito dal nome del file di configurazione

Start della rete:

```
/sbin/dhclient ath0
```

come per il comando precedente il nome dell'interfaccia può essere diverso

Si può usare wpa_cli per l'interattivo, invece di mettere la password nel file di configurazione

Se la scheda di rete non supporta wpa bisognerà usare wep; in questo caso il file di configurazione (/etc/wpa_supplicant.conf) sarà:

```
network={
    ssid="pd-wep"
    key_mgmt=IEEE8021X
    eap=PEAP
    phase2="auth=MSCHAPV2"
    identity="user name"
    password="password"
}
```

Autenticazione con certificato

È possibile autenticarsi sulle reti pd-wep, pd-wpa, o INFN-dot1x usando il certificato personale rilasciato dalla Certification Authority (CA) dell'Infn. Le reti pd-* sono riservate a coloro che hanno un portatile registrato nel dhcp di Sezione, mentre la rete INFN-dot1x, che non accede ai servizi della nostra Lan, è riservata a coloro che hanno un account valido in una Sezione Infn diversa da Padova o dispongono di un certificato.

L'autenticazione via certificato richiede che sul proprio computer vengano installati il certificato della CA e il proprio certificato personale.

Windows.

Il certificato della CA è alla URL <https://security.fi.infn.it/CA/mgt/getCA.php> e bisogna scaricarlo in formato pem sul proprio computer. Per inserirlo nel database bisogna seguire il percorso:

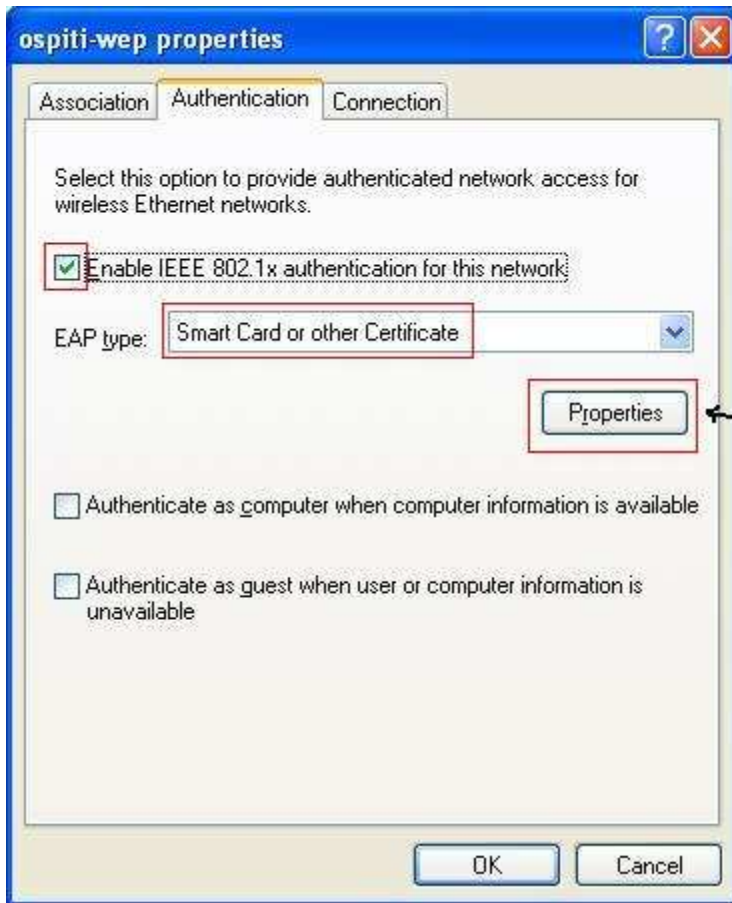
Control Pannel → Internet Options → Content → Certificates → Trusted Root CA

A questo punto si seleziona Import e parte una procedura automatica che chiede il nome del file, poi propone di inserire il certificato tra le Trusted Root Certification Authorities del computer locale.

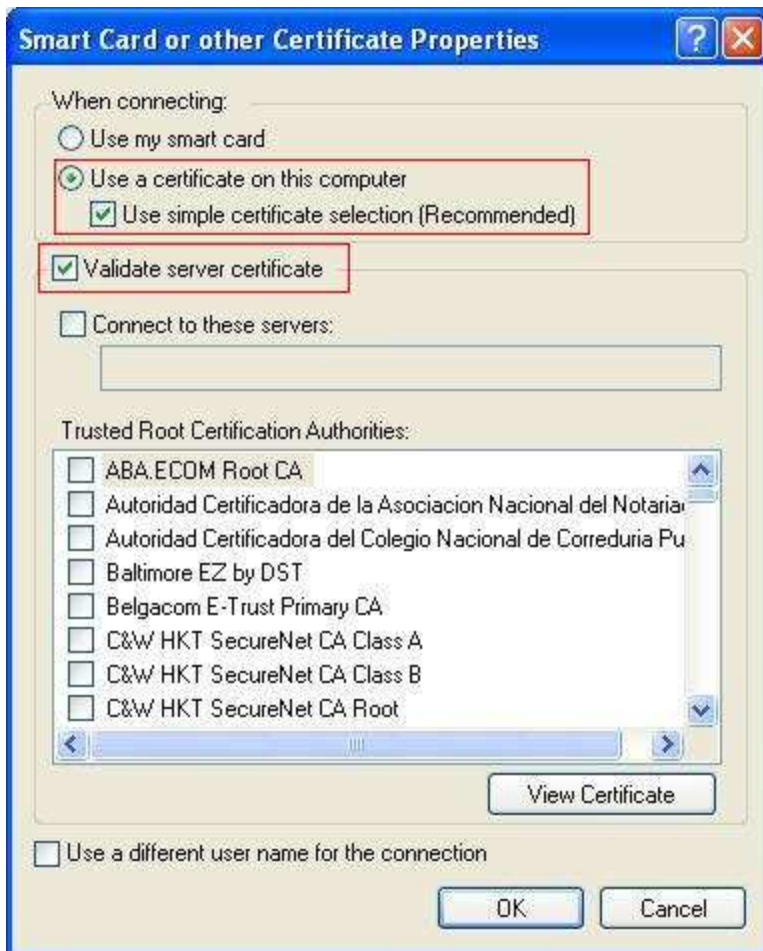
Il proprio certificato personale si inserisce da:

Control Pannel → Internet Options → Content → Certificates → Personal
selezionando il tasto Import.

La configurazione della rete wireless sarà del tipo:



Selezionare



Linux

Il certificato della CA è alla URL <https://security.fi.infn.it/CA/mgt/getCA.php> e bisogna scaricarlo in formato pem sul proprio computer, salvandolo in un file; es. /etc/INFNCA.pem

Il proprio certificato personale è in genere esportato dal browser con il quale è stato scaricato in formato pkcs12. Per metterlo in formato pem bisogna usare il comando:

```
openssl pkcs12 -in <mio-certificato.p12> -out /etc/mio-certificato.pem -clcerts
```

Il file di configurazione wpa_supplicant .conf avrà la struttura seguente:

```
network={
    ssid="pd-wpa"
    proto=WPA2
    scan_ssid=1
    key_mgmt=WPA-EAP
    pairwise=CCMP
    group=CCMP
    eap=TLS
    identity="Nome Cognome"
    ca_cert="/etc/INFNCA.pem"
    client_cert="/etc/mio-certificato.pem"
    private_key="/etc/mio-certificato.pem"
    private_key_passwd="password del certificato"
}
```

```
network={
    ssid="pd-wep"
    key_mgmt=IEEE8021X
    eap=TLS
    identity="Nome Cognome"
    ca_cert="/etc/INFNCA.pem"
    client_cert="/etc/mio-certificato.pem"
    private_key="/etc/mio-certificato.pem"
    private_key_passwd="password del certificato"
}
```

Nota: Nome e Cognome sono quelli che compaiono nel certificato personale.

2. La rete wireless per i nostri ospiti.

Per gli ospiti sono state configurate 2 reti wireless: **INFN-dot1X** e **cap**. La prima è riservata ai dipendenti/associati INFN che possiedono o un certificato rilasciato dalla Certification Authority dell'Infn o un account sul radius server della sezione di appartenenza. La configurazione di queste reti è analoga rispettivamente a pd-wpa; non è più necessaria la registrazione del mac address perché l'utente deve necessariamente autenticarsi. La differenza tra le reti per noi e le reti per gli ospiti consiste nei diversi diritti di accesso ai servizi locali.

La rete cap è per tutti gli altri utenti. Richiede la registrazione del portatile con il modulo <http://www.pd.infn.it/calcolo/modulo-portatile.pdf> dove al posto del mac address si può specificare semplicemente cap. L'utente riceverà dal servizio calcolo uno username e una password, validi strettamente per il periodo di tempo richiesto. La configurazione della rete wireless non necessita né di cifratura né di autenticazione, basta scegliere l'SSID cap. All'apertura di un web browser qualsiasi comparirà una pagina in cui vengono chiesti username e password.

3. La rete wireless per noi in trasferta.

Analogamente a quanto facciamo noi per gli ospiti, altre sedi Infn consentono l'accesso alle loro reti wireless previa autenticazione. A Padova abbiamo un server radius per l'autenticazione in remoto dei nostri utenti, perciò chi è ospite presso sedi che hanno abilitato Trip, può loggarsi alla rete INFN-dot1X usando come account il proprio username seguito da @pd.infn.it e come password la password di Windows (<https://webmail.pd.infn.it/cgi-bin/passwd.pl> per chi vuole cambiarla o non la ricorda). La configurazione della rete è identica a quella di pd-wpa. Ricordo che l'autenticazione va fatta con il proprio username, non con l'e-mail address.