



creato:
doc.:

17.05.2007
imoTD001b
rev. 0.1

Associazione Culturale Imola & Faenza Linux User Group – Via Machiavelli 8 – 40026 – Imola (Bo) - C.F. 90040120371

Manuale Utilizzo Certificati Client del LUG

Indice generale

Navigare in HTTPS.....	2
Navigare in HTTPS utilizzando il Certificato Client.....	3
Utilizzo del Certificato Client nella posta elettronica.....	5
Utilizzo del Certificato Client per documenti OpenOffice.....	6
Utilizzo del Certificato Client per firmare e crittografare File.....	6

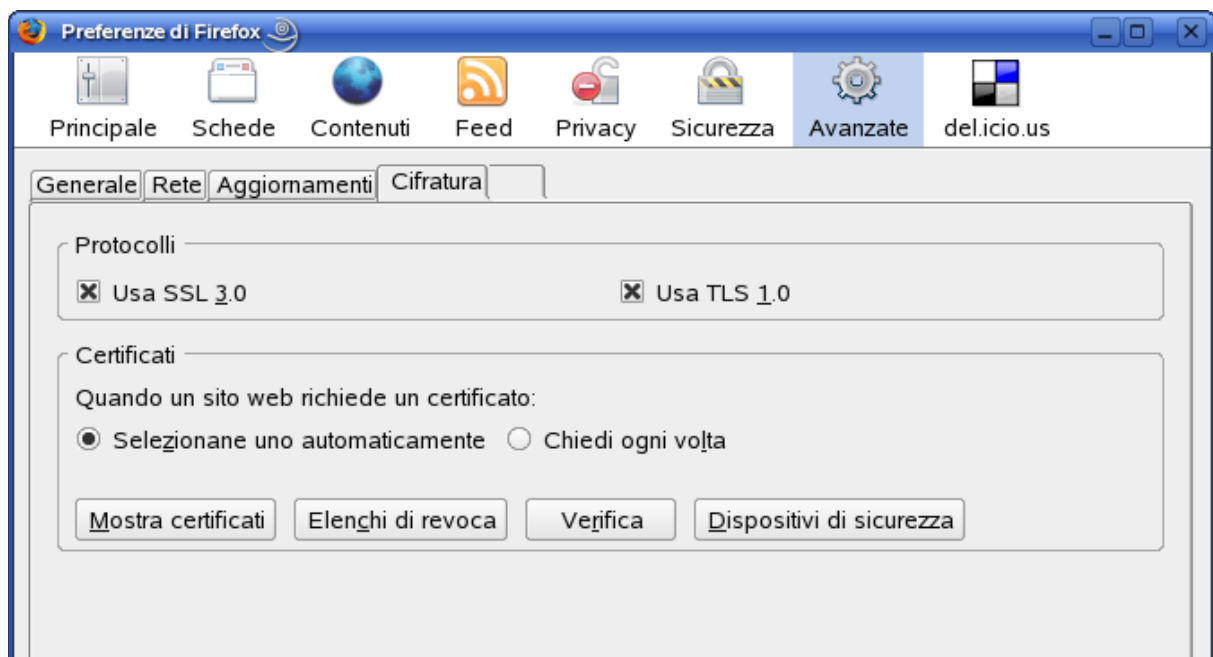
Navigare in HTTPS

Per navigare su un sito protetto da certificato ssl (leggasi accesso al sito in https) non serve altro che il vostro browser preferito. Mi immagino che il sito della vostra banca sia protetto con questi paradigmi e mi immagino che il certificato utilizzato sia stato firmato da una CA ufficialmente riconosciuta.

Se andiamo a scorrere la lista delle CA conosciute dal nostro browser... ovviamente mancherà quella appena generata del LUG. Questa mancanza è la causa della finestra di popup che il browser vi presenterà navigando sul link <https://www.imolug.org>.

Per sanare questa situazione una volta per tutte basta importare il certificato della CA del LUG all'interno del vostro browser.

Ad esempio, in Firefox 2.0.0.1, si va in Modifica->Preferenze



Poi -> Mostra certificati -> Autorità -> Importa
Scegliere cacert.pem e potrete visualizzare questo:

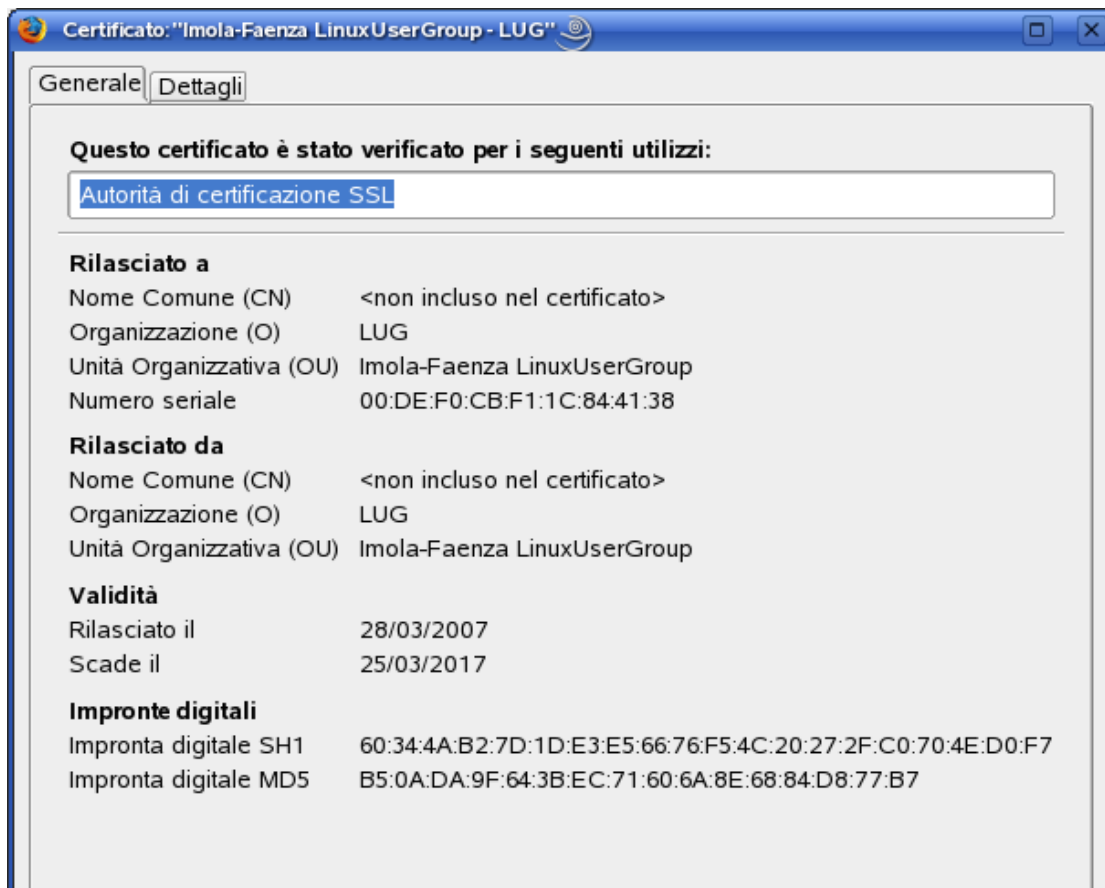


IMO LUG
Imola & Faenza Linux User Group

Associazione Culturale Imola & Faenza Linux User Group - Via Machiavelli 8 - 40026 - Imola (Bo) - C.F. 90040120371

creato:
doc.:

17.05.2007
imoTD001b
rev. 0.1



Navigare in HTTPS utilizzando il Certificato Client

Per quei siti protetti da ssl per i quali sia richiesta il controllo di un certificato client, basterà importare il pacchetto pkcs12 contenenti la chiave privata ed il certificato firmato dalla CA. Alla fine dell'import vi troverete qualcosa di simile a questo panel:

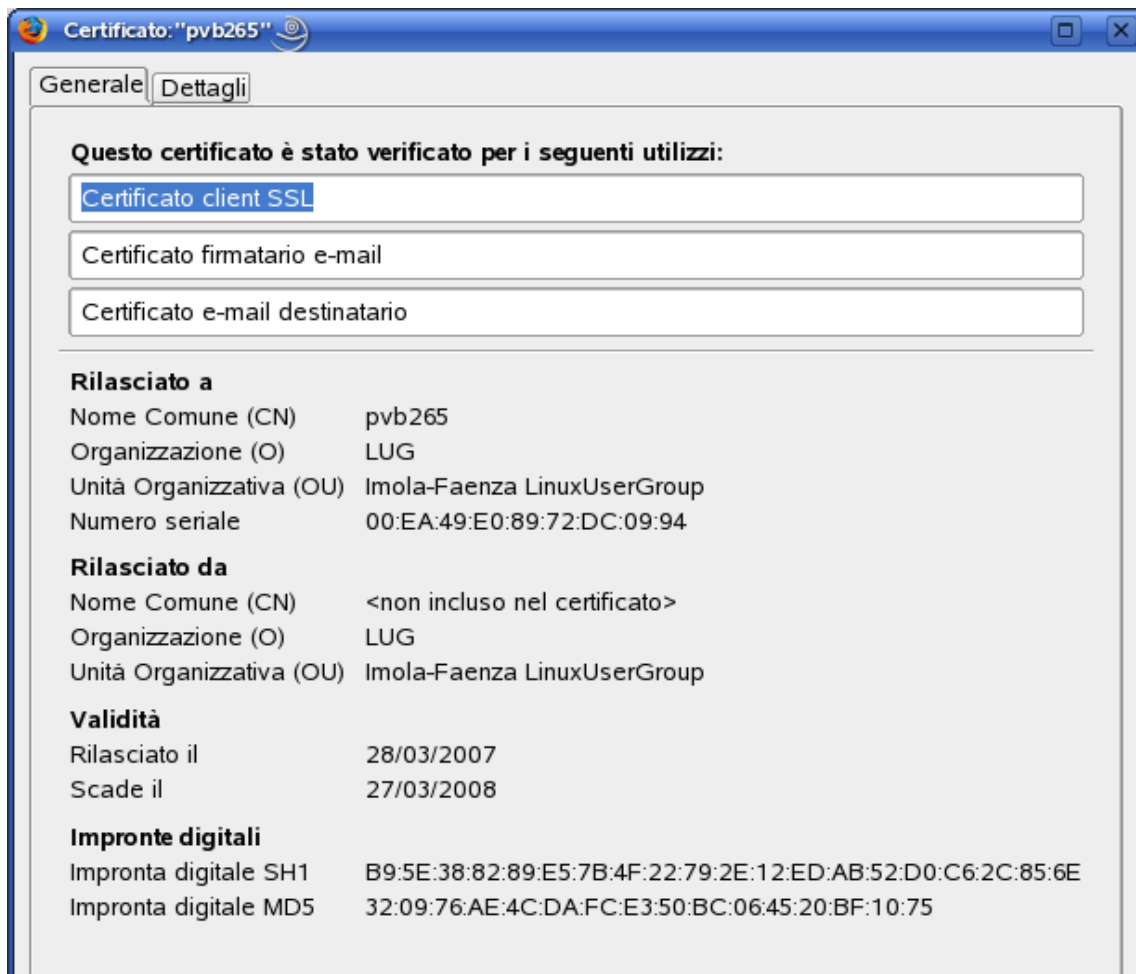
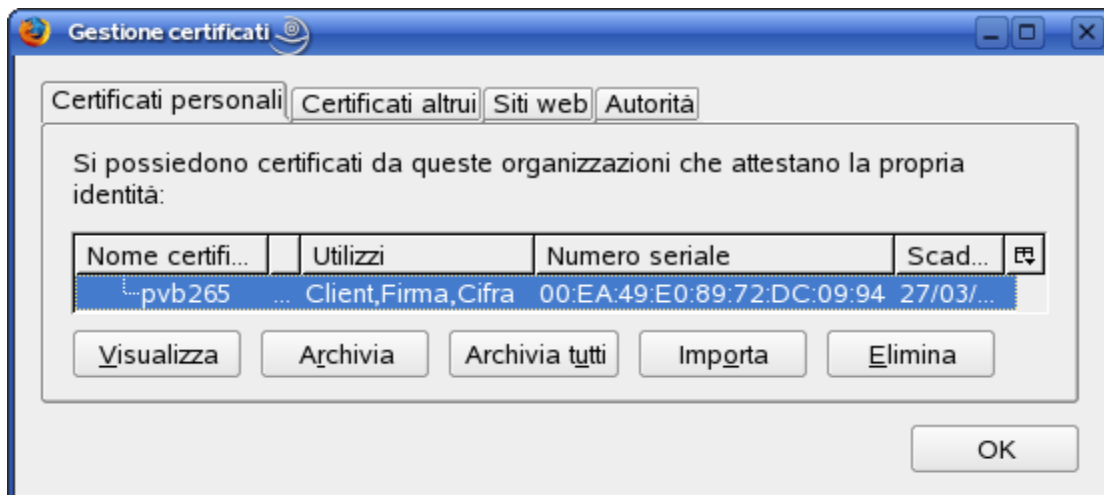


IMOLUG
Imola & Faenza Linux User Group

Associazione Culturale Imola & Faenza Linux User Group - Via Machiavelli 8 - 40026 - Imola (Bo) - C.F. 90040120371

creato:
doc.:

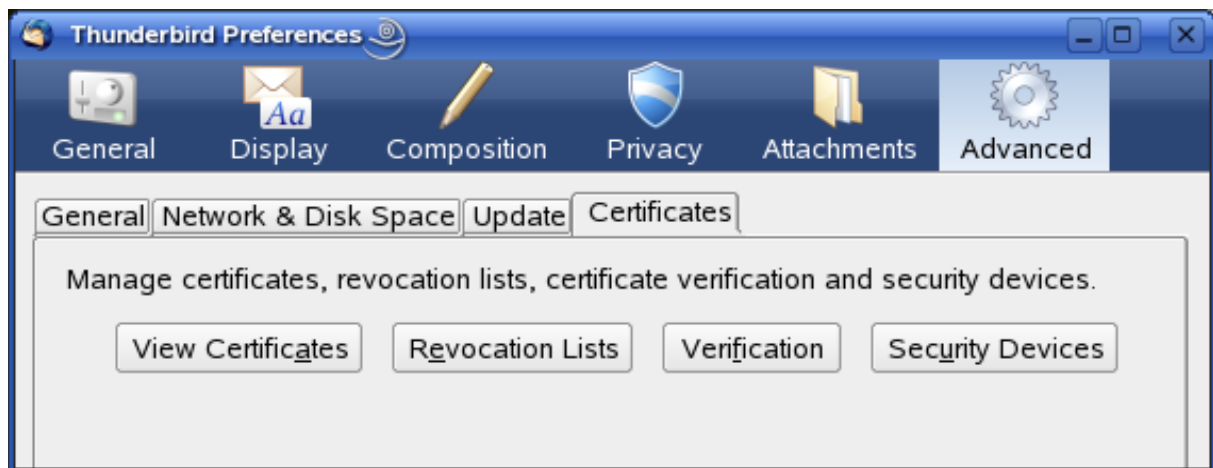
17.05.2007
imoTD001b
rev. 0.1



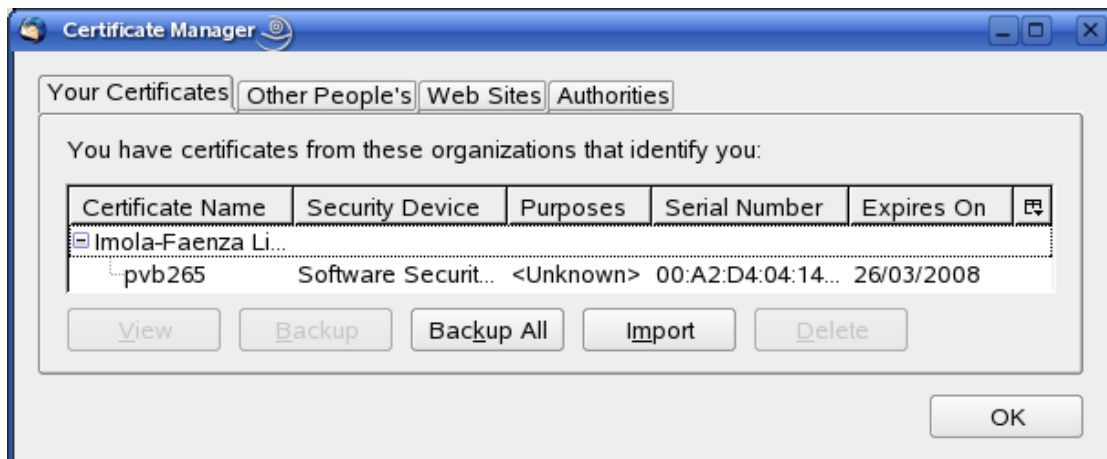
Utilizzo del Certificato Client nella posta elettronica

Alla stessa maniera, è possibile importare il certificato client all'interno del client di posta. Per esempio Thunderbird 2 beta 1.

Edit -> Preferences



View Certificates -> Import





creato:
doc.:

17.05.2007
imoTD001b
rev. 0.1

Associazione Culturale Imola & Faenza Linux User Group – Via Machiavelli 8 – 40026 – Imola (Bo) - C.F. 90040120371

Utilizzo del Certificato Client per documenti OpenOffice

Su un sistema Linux, per dire ad OpenOffice, dove andare a prendere i certificati bisogna esportare la variabile:

```
MOZILLA_CERTIFICATE_FOLDER=~/.mozilla/firefox/xr34w2ib.default
```

cartella contenente i certificati di firefox per esempio...

Fatto questo potrete includere il vostro certificato al documento

Utilizzo del Certificato Client per firmare e crittografare File

Di solito siamo abituati ad usare PGP o GPG per crittografare un file. Queste due modalità sono imperniate sul concetto di anello delle chiavi. Con i certificati x509 la firma e la crittografia vengono veicolate dalla CA.

In questo senso dovrebbe essere possibile utilizzare il pacchetto PKCS12 come sorgente per firmare e criptare i nostri file dati.

A tal proposito ho trovato riferimenti al binomio KGPG e Kleopatra...