Consorzio Sistema Bibliotecario Nord - Ovest
Sede amministrativa: Corso Europa, 291 - Villa Burba 20017 Rho
Tel. 02 9320951 - Fax 02 93209520 - C.F. - P. IVA 11964270158
www.csbno.net - mailto: consorzio@csbno.net
Sede legale: via V. Veneto, 18 – 20026 Novate Milanese

Rho, Luglio 07, 2006

CORSI ON-LINE

La nuova Posta Elettronica IMAP del C.S.B.N.O.

di Restelli Paolo

Appendice 2 : Protocolli sicuri, autenticazione sicura e certificati (P. Restelli)

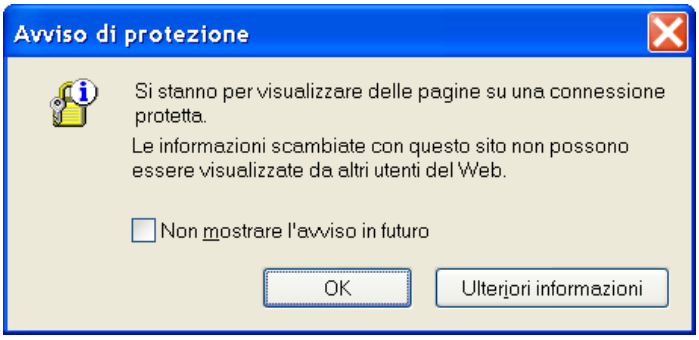
Attualmente la maggior parte dello scambio di informazioni sulla rete avviene senza alcuna forma di protezione sulla confidenzialità dei dati e senza alcun tipo di controllo sulla identità di coloro che partecipano a tale comunicazione. Per di più, l'utilizzo di password, qualora vengano trasmesse in chiaro e quindi siano intercettabili da malintenzionati, spesso genera un falso senso di sicurezza.

L'uso di protocolli sicuri (che, per esempio, consentano di codificare le informazioni rendendole accessibili solo agli interlocutori, o che diano la possibilità di identificare inequivocabilmente mittente e/o destinatario di un messaggio) permette di ovviare a questi problemi ma bisogna comprenderne i principi di funzionamento per non vanificarne i vantaggi.

Supponiamo di connetterci con un browser (Internet Explorer, Netscape, Opera, etc.) alle sezioni "sicure" del nostro sito web (per esempio la webmail, che consente la consultazione della posta via web).

Come sappiamo, le informazioni viaggiano crittografate, quindi non sono utilizzabili da un eventuale ascoltatore indesiderato. Ma se un malintenzionato, invece, decidesse in qualche maniera non di limitarsi ad ascoltare la comunicazione ma di interporsi tra noi ed il server (non è questo il documento in cui discutere delle modalità), non saremmo noi stessi a fornirgli le password per l'accesso ai nostri servizi? Insomma, chi ci garantisce che noi stiamo parlando direttamente col server desiderato?

Appena accediamo ad una sezione sicura, riceviamo un warning di questo genere (tutti gli esempi forniti d'ora in avanti faranno riferimento alla versione 6 –italiana- di Internet Explorer e alla 7 –inglese- di Netscape, le più utilizzate):



(Internet Explorer)

oppure

Con tali avvertimenti ci viene segnalato dal browser che stiamo contattando il server utilizzando una connessione crittografata. È importante NON disabilitare questo warning e prestare attenzione che esso compaia sempre quando tentiamo di accedere a delle pagine che sappiamo essere protette.

Questo è, in condizioni normali, l'unico **warning** che dovremmo ricevere dal browser (oltre a quello che otterremo quando decideremo di ritornare ad una connessione non sicura).

Al di là di questa segnalazione possiamo riceverne altre a cui dobbiamo prestare la massima attenzione.

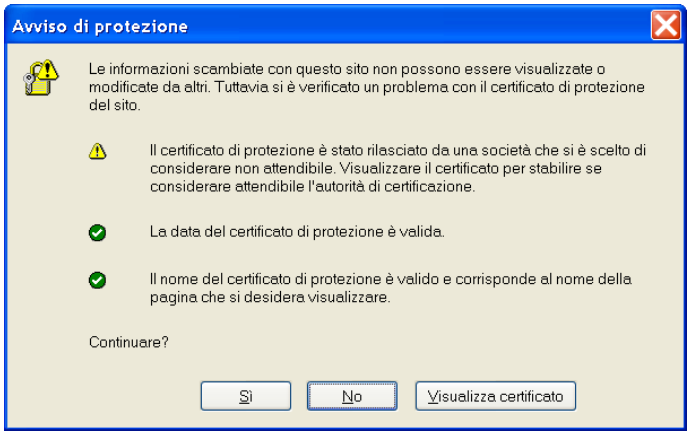
Il server presenta al browser (client) un certificato con cui (tra le altre cose) dichiara la sua identità. Tale certificato deve essere stato firmato da qualcuno; perché ci si possa fidare di questo qualcuno è necessario che il browser lo riconosca come affidabile garante dell'altrui identità.

Questo qualcuno è detto Certification Authority, o CA. Perché possa essere riconosciuto come valido un certificato recante la firma della CA, il certificato di quest'ultima deve essere inserito nel browser.

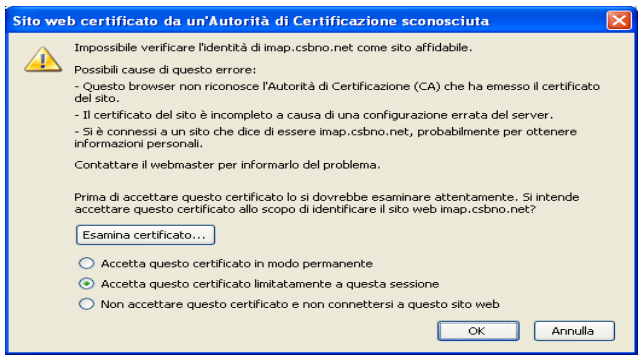
I certificati delle CA riconosciute a livello internazionale come affidabili sono inseriti di default nei browser più famosi.
Il problema è che la Certification Authority dell'INFN (Firenze) non è riconosciuta di default come "CA attendibile" dai browser. Quando uno di questi tenta di verificare l'identità del server (per es. www.csbno.net, laddove si acceda in maniera sicura), non riesce a trovare il certificato della CA che ha garantito per il server stesso, cioè che ha firmato il suo certificato.

S
ottopone, quindi, tale segnalazione all'utente finale, il quale può evitare di andare avanti oppure accettare (temporaneamente o a tempo indefinito) tale certificato (quello presentato dal server e finora non verificato).

Nel caso di IE:



Firefox :



In sostanza viene chiesto all'utente di assumersi tutte le responsabilità derivanti dalla connessione con un server che presenta un attestato la cui firma è stata apposta da qualcuno che non si conosce.

Accettando questo certificato permanentemente NON stiamo installando il certificato della CA ma stiamo solo dicendo che ci fidiamo ciecamente di quello presentato dal server in questione (www.csbno.net) , quindi lo consideriamo accettabile da adesso fino alla data di validità presente nel certificato stesso. Tale azione è sconsigliabile.

- **Installazione del certificato della CA.**

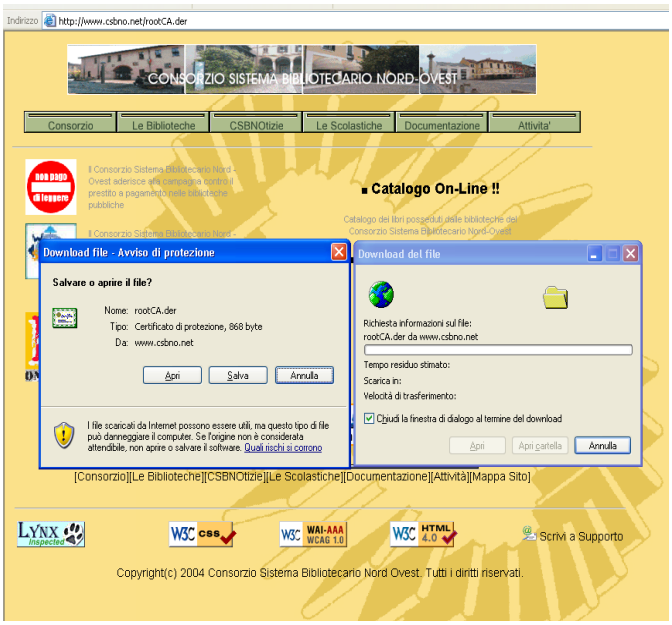
È preferibile invece installare il certificato della CA. Tale procedura va fatta per ogni browser che intendiamo utilizzare (se utilizziamo sia IE che Netscape dovremo applicarla due volte).

Usando il browser in cui vogliamo inserire il certificato digitiamo nella barra degli indirizzi l'URL:

http://www.csbno.net/csbnocert.der

Trattandosi di una connessione sicura, riceveremo sia il warning relativo alla protezione, sia quello relativo all'assenza del certificato della CA. In questo caso (ma solo in questo) procediamo.

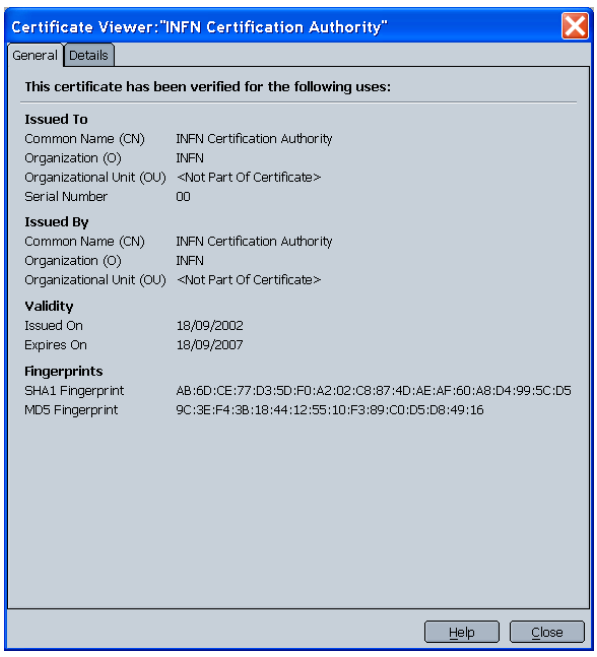
La pagina che ci compare nel caso di IE la pagina è :



Si tratta semplicemente di cliccare su “Scarica Certificato”, lasciando selezionato il formato di default, “DER”. A questo punto, se il browser utilizzato è Firefox, bisogna selezionare tutte e tre le caselle proposte nella finestra di dialogo ma…

…aspettiamo a confermare con “OK”. Abbiamo prestato attenzione alla segnalazione scritta con caratteri blu nella schermata iniziale?

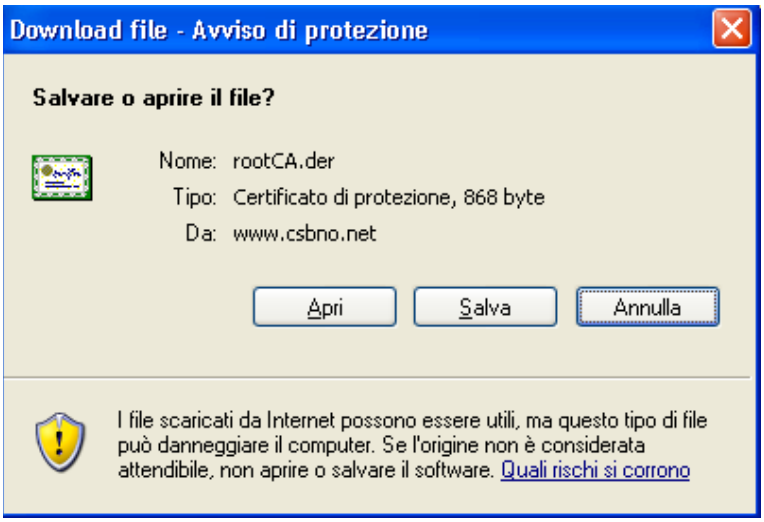
Clicchiamo allora su “View” per esaminare il certificato



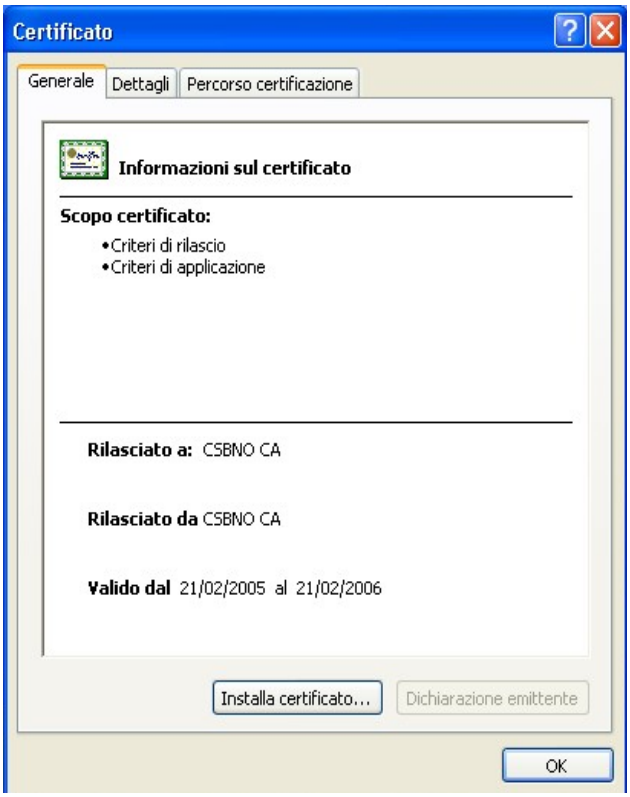
e verifichiamo che i fingerprint (cioè le impronte digitali) siano quelli aspettati.
Clicchiamo quindi su “Close” e, se tutto corrisponde, rispondiamo con “OK” nella finestra precedente con le 3 caselle di spunta.

La procedura per Internet Explorer è apparentemente leggermente diversa, ma i principi di base sono gli stessi.

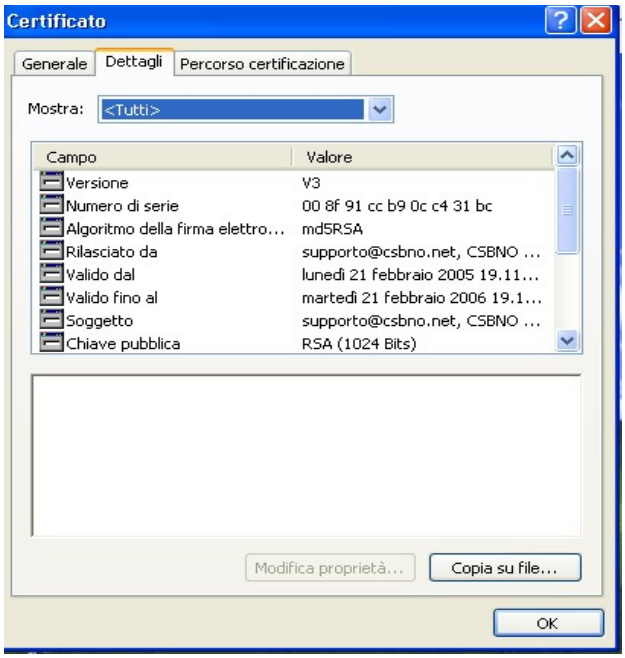
Dopo aver confermato “Scarica certificato” ci appare questa finestra



in cui possiamo rispondere con “Apri”.
Comparirà questa finestra



Stesso discorso di prima: verifichiamo l’impronta digitale del certificato andando nella sezione “Dettagli”. Per maggiore chiarezza facciamo mostrare “Solo proprietà”, quindi selezioniamo “Identificazione personale” e verifichiamo che il tutto corrisponda.



Ritorniamo quindi nella sezione “Generale” e clicchiamo su “Installa certificato”.
Procediamo accettando i valori proposti fino alla fine.

Ad installazione ultimata, comparirà

Si potrà quindi cliccare su “OK” sia qui che nella finestra per l’installazione del certificato.

D'ora in avanti il nostro browser riconoscerà i certificati dei server (e quelli personali) CSBNO.

Altre verifiche fatte dal browser sul certificato riguardano la validità temporale dello stesso e la corrispondenza del nome del server a cui si sta accedendo al nome dichiarato nel certificato.

Sono possibili infatti azioni mediante le quali un malintenzionato, interponendosi nel percorso tra client e server, può riuscire ad ottenere, per esempio, le password di accesso ai servizi utilizzati dagli utenti e fornite inconsapevolmente dagli stessi, che credono di connettersi direttamente col server reale ma comunicano, in realtà, con il server fasullo che a sua volta parla con quello vero.

È possibile evitare tali attacchi interrompendo la connessione qualora il certificato presentato dal server dovesse far scattare qualche allarme da parte del browser.

Ovviamente non è possibile che questo malintenzionato si faccia firmare da una CA affidabile (cioè una riconosciuta dal browser) un certificato attestante l’identità che vuole impersonare (in questo caso www.csbno.net)

Quindi, o il certificato se lo firma da solo o se lo fa rilasciare da una CA non affidabile (in tal caso il browser segnalerà che non è stato possibile verificare l'identità del server).

Una puntualizzazione per fugare qualche possibile dubbio: "rubare" un certificato intercettandolo mentre è in transito sulla rete non serve a niente. Ogni certificato è associato ad una chiave privata che soltanto il possessore del certificato possiede e che non viene mai comunicata in rete. Senza questa chiave non è possibile nessuna forma di comunicazione con chi presenta il certificato stesso.

Ma il malintenzionato potrebbe anche presentare un certificato effettivamente rilasciato da una CA affidabile. In questo caso, essendo la CA attendibile, non è possibile che l'identità dichiarata nel certificato sia quella del server che il malintenzionato vuole impersonare. Quindi il browser segnalerà questa discrepanza.

Va anche verificato che, passando dalle pagine in chiaro a quelle che ci si aspetta siano crittografate, si riceva una segnalazione in merito da parte del programma utilizzato per la navigazione (è quindi consigliabile non disabilitare permanentemente tale segnalazione).

Dunque, ricapitolando: installiamo il certificato della CA una volta per tutte (in realtà fino a quando non scade). Ogni volta che ci connettiamo alle sezioni sicure del web server verifichiamo che ci sia il warning che ci avvisa che la connessione è protetta.
Quando avremo finito la nostra navigazione criptata e passeremo ad una connessione in chiaro avremo la relativa segnalazione.

Nel primo caso siamo noi a dire al browser (tramite la procedura prima descritta) di accettare implicitamente tutti i certificati (compreso quello di www.csbno.net) dalla CA rilasciati (sempre se i successivi controlli, per es. quello sulla validità temporale e quello sulla corrispondenza dei nomi, lo tranquillizzano), nel secondo caso accettiamo solo quello di www.csbno.net presentato all'atto della connessione per il periodo di tempo dichiarato nel certificato.

Per quello che riguarda, comunque, la sicurezza delle mail inviate e ricevute tramite webmail, c'è da dire che l'unico tratto sicuramente criptato è quello che va dal client al server web, cosa che assicura la comunicazione protetta della password al server e la confidenzialità durante la consultazione della posta ricevuta - in realtà è anche garantito l'invio criptato della posta in uscita fino al server web, ma da lì in poi essa viaggia in chiaro, come pure non criptate sono generalmente le mail che riceviamo nel momento in cui viaggiano sulla rete fino a quando raggiungono il server di posta (IMAP/POP).

Per garantire la confidenzialità delle mail si dovrebbe usare qualche forma di codifica/decodifica end-to-end, cioè il mittente codifica e il ricevente decodifica.
Una possibilità è offerta dall'uso dei certificati personali (e qua entra nuovamente in gioco la CA , che rilascia anche questo genere di certificati).

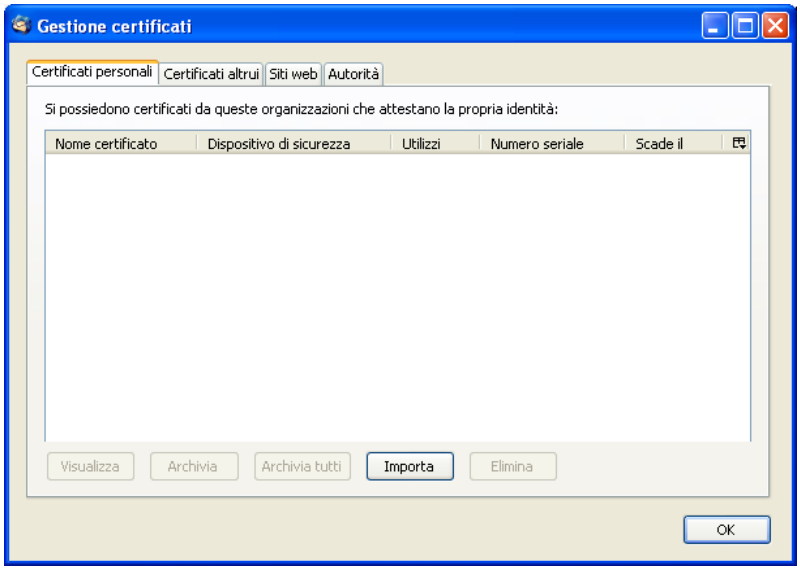
Se vi sono persone interessate, posso scrivere un nuovo documento dedicato esplicitamente a questo argomento.

- **Recupero posta sicuro.**

Se non si utilizza la webmail ma un client per la consultazione della posta come Outlook (Express), Thunderbird, Eudora, etc., è possibile comunque abilitare la ricezione tramite connessione cifrata (SSL).

La prima cosa da fare è installare (secondo la procedura descritta nella sezione precedente) il certificato della CA nel browser come visto sopra o nei client non intimamente legati ad un browser, all'interno del programma.

Ecco in Strumenti-> opzioni-> Privacy-> Sicurezza il menu' di gestione certificati di Thunderbird

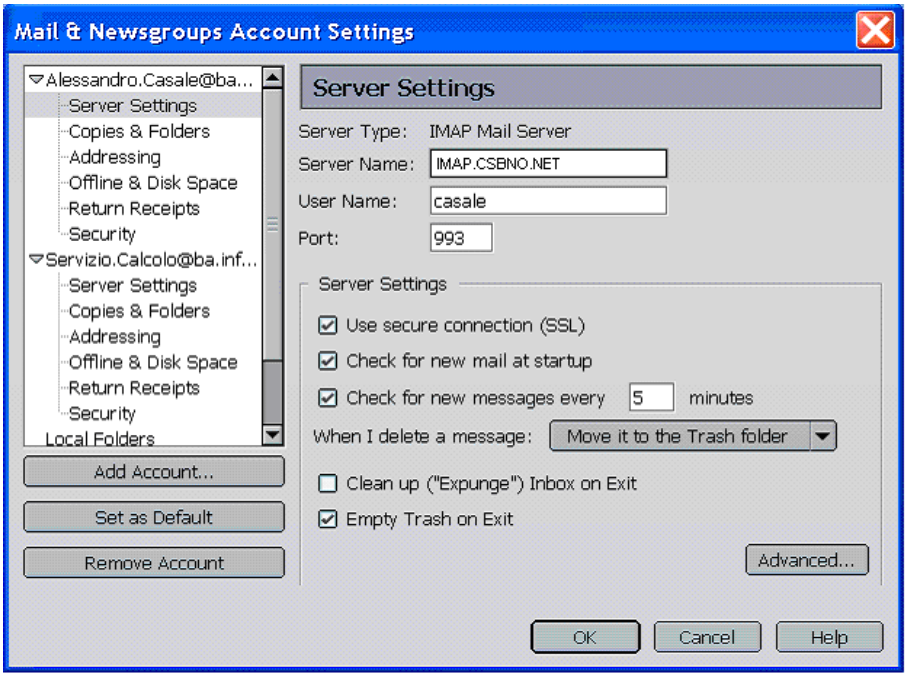


Poi, nella configurazione dell'account di posta bisogna specificare come nome del server per la ricezione (IMAP/POP) imap.csbno.net (è importante utilizzare il nome di dominio completo), che è il nome ufficiale del server IMAP/POP (quello che compare nel certificato), così come www.csbno.net è quello del server web.

Se non si fa ciò il programma, per quanto spiegato nella sezione precedente, segnalerà che il nome presentato nel certificato è diverso da quello del server a cui ci si sta connettendo (e noi non vogliamo avere dei warnings, altrimenti, se ci abituiamo a ignorarli, continueremo a farlo anche quando non saranno inutili).

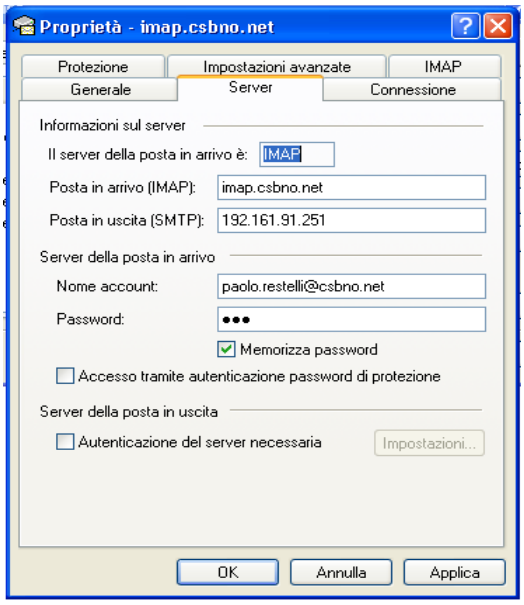
L'ultima cosa da fare è dire al programma di utilizzare SSL per la ricezione della posta.

In Netscape 7 ad esempio, selezionare il menù Edit, quindi la voce "Mail & Newsgroups Account Settings". Andare nella sezione "Server Settings" relativa all'account desiderato,



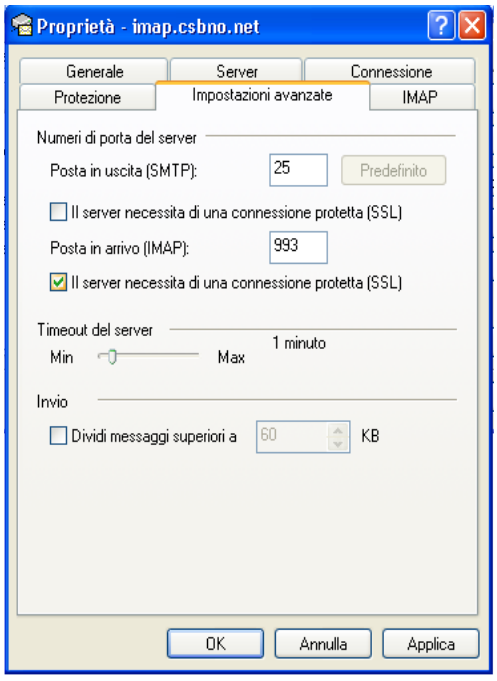
quindi immettere il nome del server e cliccare su “Use secure connection (SSL)”.
Si noterà che il numero di porta cambierà a 993 (IMAP) oppure 995 (POP).

In Outlook Express 6 le impostazioni da modificare si trovano nel menù Strumenti alla voce Account.
Selezionare l’account di posta elettronica da modificare, quindi cliccare su Proprietà.



Nei settaggi relativi al server cambiare “Posta in arrivo” digitando imap.csbno.net

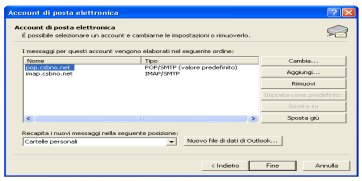
Nelle “Impostazioni Avanzate”



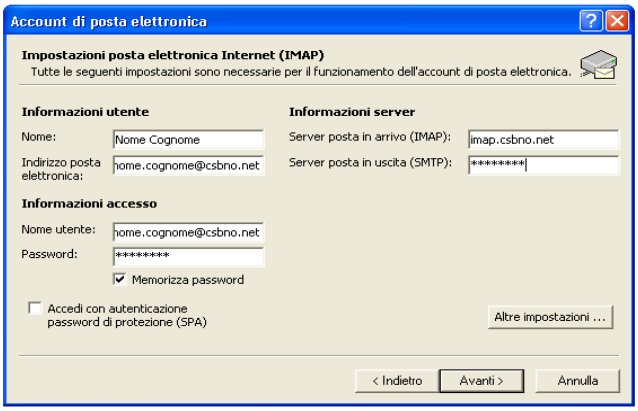
immettere la spunta nella casella “il server necessita di una connessione protetta (SSL)” relativa alla “Posta in arrivo” (notare anche qui la variazione del numero di porta).
Quindi dare “OK” e chiudere.

In Outlook, andare in “Strumenti”, “Account di posta elettronica”, “Visualizza o cambia gli account di posta elettronica esistenti”.

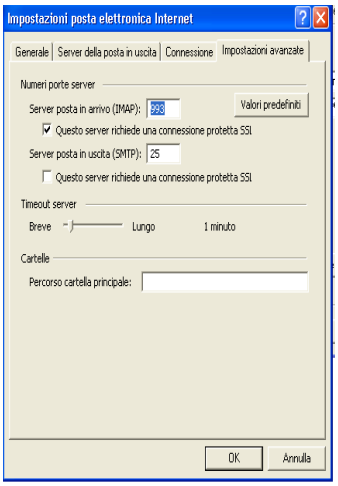
Cliccare su “Avanti”, selezionare l’account desiderato



e cliccare su “Cambia”.



Modificare “Server di posta in arrivo” in “imap.csbno.net”, quindi cliccare su “Altre impostazioni” e, nella sezione “Impostazioni avanzate”,



per quello che riguarda il “Server posta in arrivo” indicare (mettendo la spunta) che “il server richiede un connessione protetta (SSL)”. Anche in questo caso il numero di porta diventerà 993 o 995 (IMAP/POP).
Infine dare “OK”, “Avanti”, “Fine”.