

Manuale servizio SMTP autenticato

Introduzione ai protocolli di invio della posta elettronica	2
SMTP	2
Crittografia	2
Outlook Express	3
Attivazione della crittografia	5
Outlook 2003	6
Attivazione della crittografia	8
Outlook 2007	9
Attivazione della crittografia	12
Eudora 7	13
Attivazione della crittografia	14
Altri client di posta.....	15

Introduzione ai protocolli di invio della posta elettronica

SMTP

Il protocollo SMTP è il più diffuso protocollo utilizzato per l'invio della posta elettronica.

Solitamente per l'invio di posta è consigliabile utilizzare il server SMTP fornito dal provider utilizzato per la connessione a Internet (es: Alice, Libero, Wind, Tiscali, Tele2, NGI, MCLink, ecc...), in questo caso solitamente non è richiesta l'autenticazione.

Questo però pone una limitazione: il server SMTP del proprio provider può essere utilizzato solo se la linea Internet è quella del provider.

Chi utilizza un computer portatile e si trova spesso ad utilizzare provider diversi, se non vuole o non può creare diversi account per l'utilizzo dei diversi server SMTP, oppure chi ha problemi con il server SMTP del proprio provider, può utilizzare un servizio chiamato "SMTP autenticato".

Quest'ultimo permette di utilizzare un server SMTP apposito che accetta messaggi da qualsiasi computer, tramite un semplice meccanismo di autenticazione.

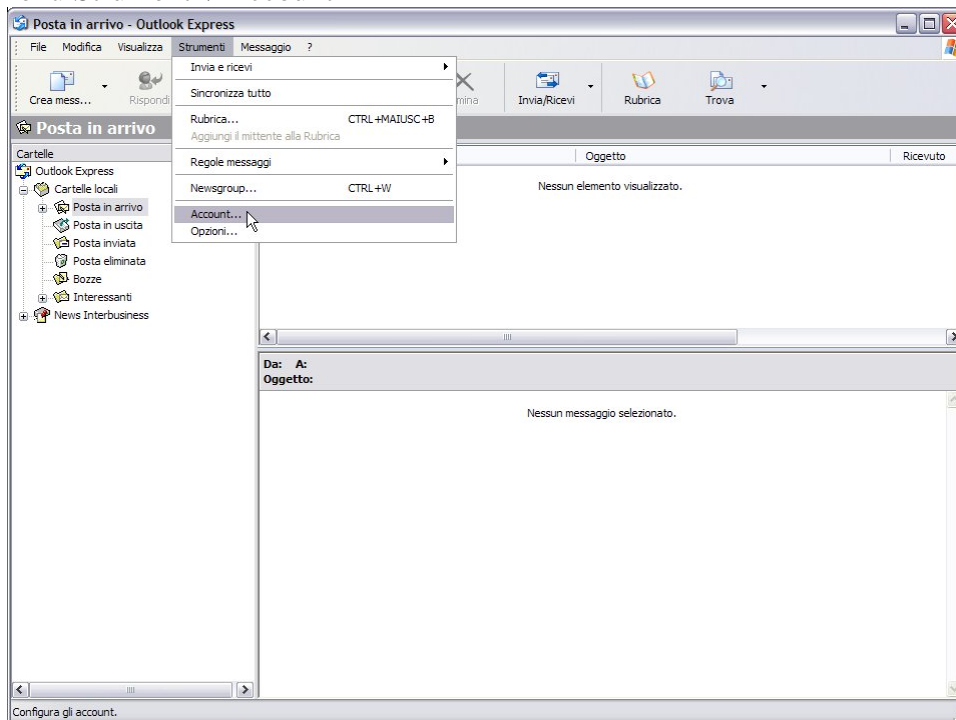
Crittografia

I meccanismi di crittografia permettono di cifrare la comunicazione dal client al server di posta sia per quanto riguarda l'invio (abilitando SSL o TLS nel protocollo SMTP) che per la ricezione dei messaggi (abilitando SSL con POP3 o IMAP).

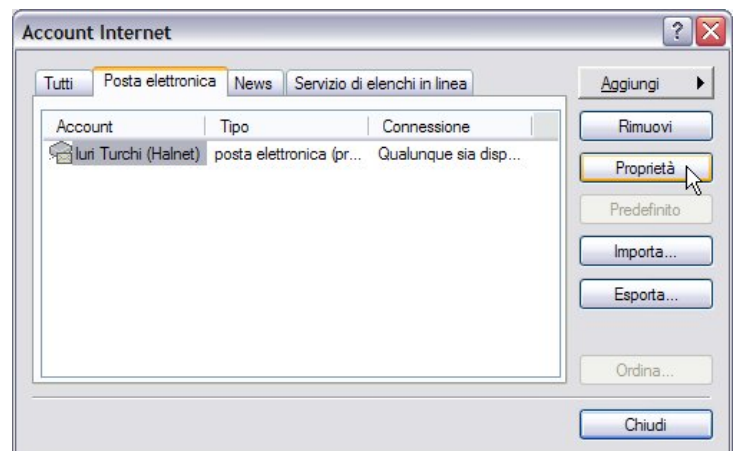
Questo è un meccanismo utile nel caso si desideri aver un maggiore grado di sicurezza. Ovviamente però comporta un maggior scambio di informazioni e quindi una maggior lentezza nelle comunicazioni con il server.

Outlook Express

Andare nel menù Strumenti / Account

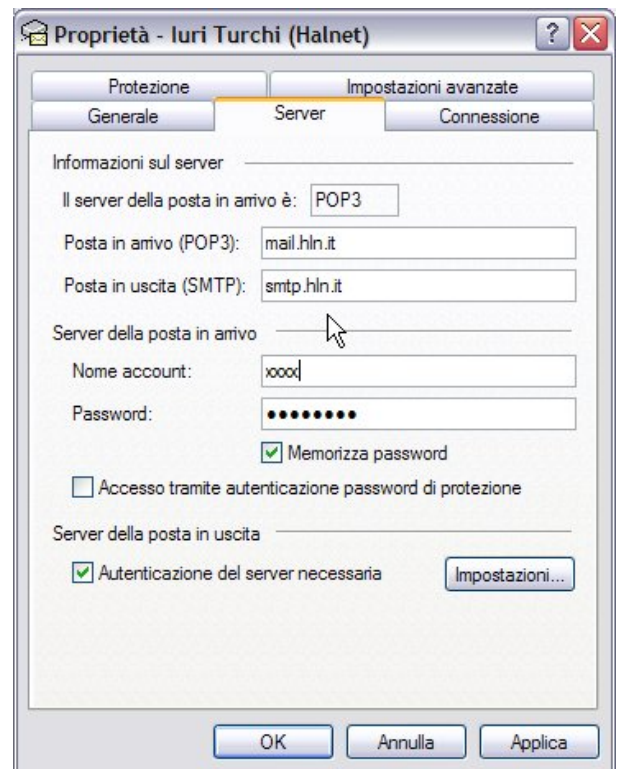


Selezionare con un click singolo l'account di posta per cui si desidera mandare la posta tramite il server SMTP di Halnet e premere sul tasto "Proprietà".



Aprire la scheda “Server” e inserire nella voce “Posta in uscita (SMTP)” la stringa **smtp.hln.it**.

Sempre nella stessa scheda, in basso c’è un riquadro “Server della posta in uscita”, bisogna abilitare la casella “Autenticazione del server necessaria”.



Premere sul pulsante “Impostazioni” attivare l’opzione “Accedi come” e inserire le credenziali username/password fornite per il servizio SMTP.

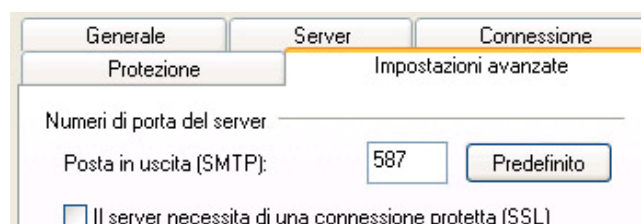
Premere il tasto ok.

Infine, andare nella scheda “Impostazioni avanzate”, e impostare la porta 587 per la posta in uscita.

Questa impostazione serve perché non tutti i provider lasciano aperta la porta 25 in uscita (serve per ostacolare lo spam). A tale scopo gli standard per la posta in uscita indicano di utilizzare la porta 587.

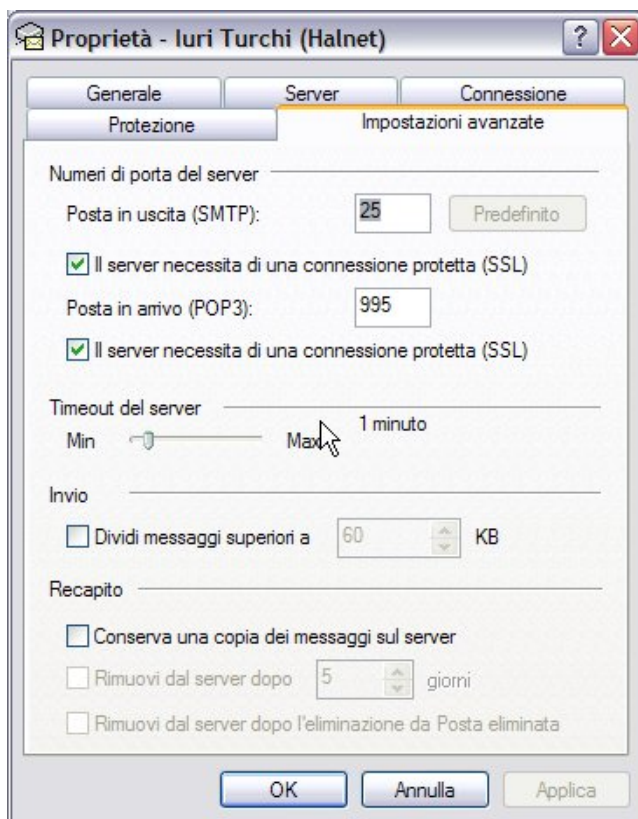
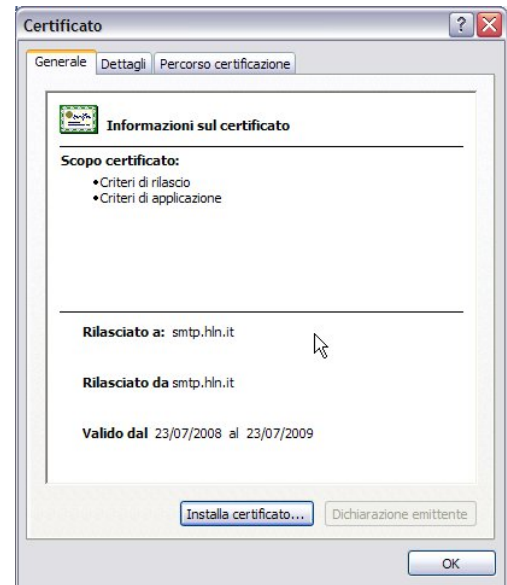
Se si lascia la porta 25 c’è la possibilità che il nostro server di posta segnali come spam la mail inviata in quanto non dovrebbe essere utilizzata dai client.

Premere sul tasto ok e chiudere la finestra degli account.



Attivazione della crittografia

Se si intende abilitare la cifratura delle comunicazioni con il server SMTP, bisogna scaricare innanzitutto il certificato principale della Halnet (<http://www.hln.it/file/cacert.crt>). Dopo aver scaricato il certificato, effettuare un doppio click sul file, premere sul tasto “Installa certificato” e andare avanti con il wizard fino al termine in cui apparirà il messaggio di importazione terminata.



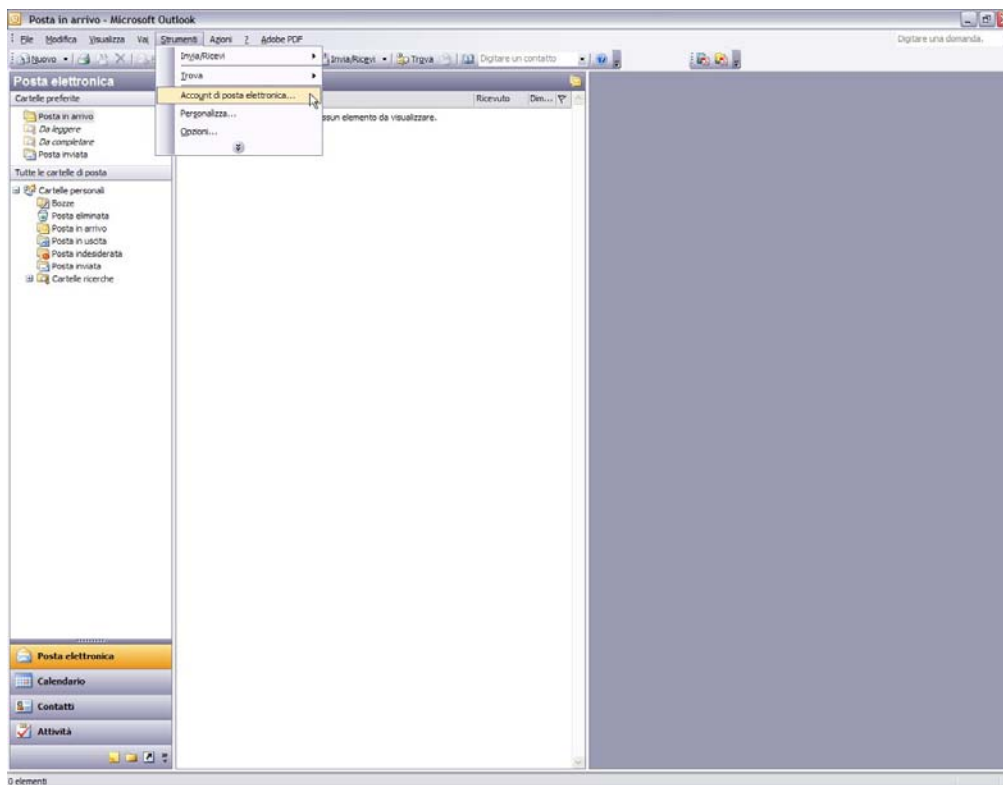
A questo punto, nel programma Outlook Express, aprire il menù Strumenti / Account. Selezionare con un click singolo l'account di posta in cui è stato configurato in precedenza il server SMTP e premere sul tasto “Proprietà”. Aprire la scheda “impostazioni avanzate”. **Sotto alla voce “Posta in uscita (SMTP)” abilitare la casella “il server necessita di una connessione protetta (SSL)”**, premere il tasto ok e chiudere la finestra degli account.

Nota: se lo si desidera, invece della porta **587** (in cui viene usato il protocollo SMTP+TLS) è possibile utilizzare la porta 465 (nella quale verrà usato il protocollo SMTP+SSL).

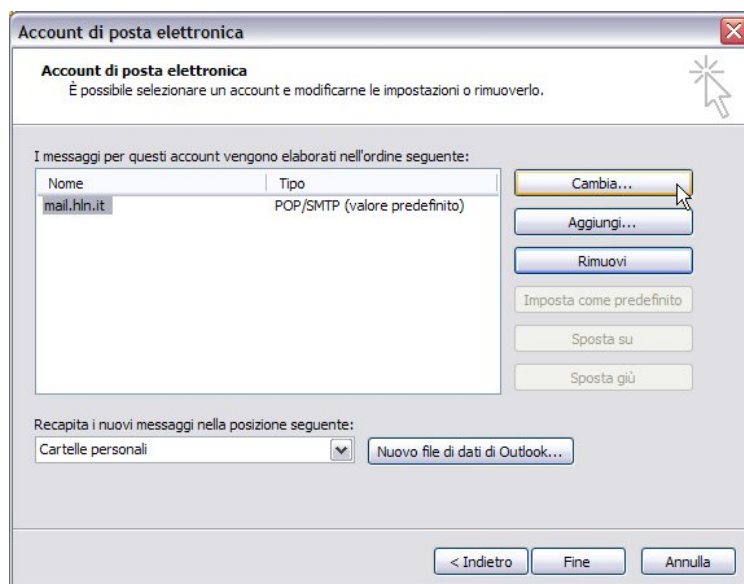
I due protocolli sono equivalenti in termini di sicurezza.

Outlook 2003

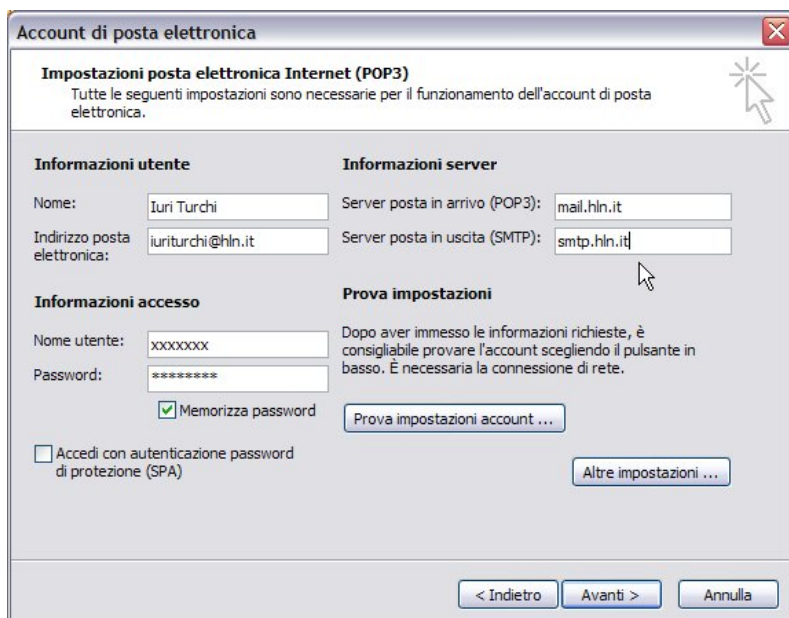
Andare nel menù Strumenti / Account di posta elettronica



Lasciare indicato “Visualizza o cambia gli account di posta elettronica esistenti” e premere su avanti. Selezionare con un click singolo l’account di posta per cui si desidera mandare la posta tramite il server SMTP di Halnet e premere sul tasto “Cambia”.



Inserire nella voce “Server posta in uscita (SMTP)” la stringa **smtp.hln.it**. Premere sul tasto “Altre impostazioni” a aprire la scheda “Server della posta in uscita”. Abilitare la casella “il server della posta in uscita (SMTP) richiede l’autenticazione”.



Account di posta elettronica

Impostazioni posta elettronica Internet (POP3)
Tutte le seguenti impostazioni sono necessarie per il funzionamento dell'account di posta elettronica.

Informazioni utente

Nome: Iuri Turchi
Indirizzo posta elettronica: iuriturchi@hln.it

Informazioni server

Server posta in arrivo (POP3): mail.hln.it
Server posta in uscita (SMTP): smtp.hln.it

Informazioni accesso

Nome utente: xxxxxxx
Password: xxxxxxxx
 Memorizza password

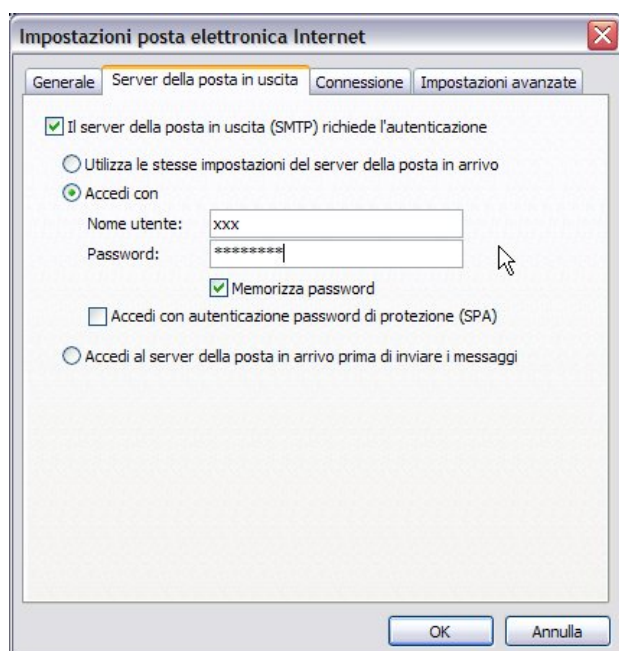
Prova impostazioni

Dopo aver immesso le informazioni richieste, è consigliabile provare l'account scegliendo il pulsante in basso. È necessaria la connessione di rete.

Accedi con autenticazione password di protezione (SPA)

Prova impostazioni account ...
Altre impostazioni ...

< Indietro Avanti > Annulla



Impostazioni posta elettronica Internet

Generale **Server della posta in uscita** Connessione Impostazioni avanzate

Il server della posta in uscita (SMTP) richiede l'autenticazione

Utilizza le stesse impostazioni del server della posta in arrivo

Accedi con

Nome utente: xxx
Password: xxxxxxxx
 Memorizza password

Accedi con autenticazione password di protezione (SPA)

Accedi al server della posta in arrivo prima di inviare i messaggi

OK Annulla

Attivare l’opzione “Accedi con” e inserire le credenziali username/password fornite per il servizio SMTP.

Andare poi nella scheda “Impostazioni avanzate” e impostare la porta **587** nella casella “Server di posta in uscita (SMTP)”.

Questa impostazione serve perché non tutti i provider lasciano aperta la porta 25 in uscita (serve per ostacolare lo spam). A tale scopo gli standard per la posta in uscita indicano di utilizzare la porta 587.

Se si lascia la porta 25 c’è la possibilità che il nostro server di posta segnali come spam la mail inviata in quanto non dovrebbe essere utilizzata dai client.

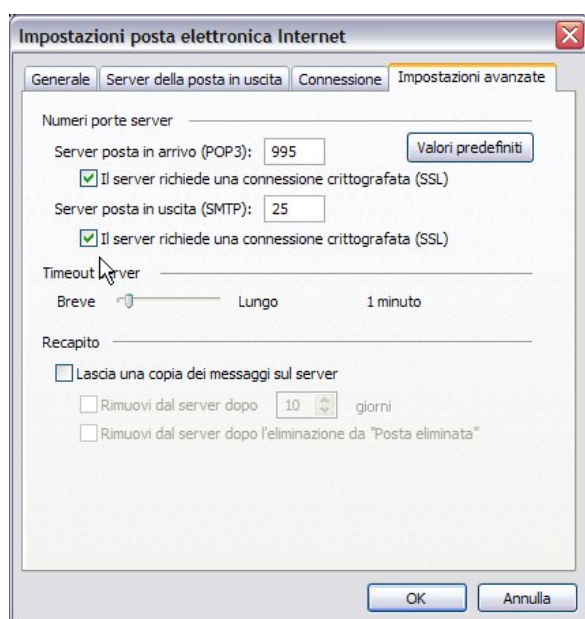
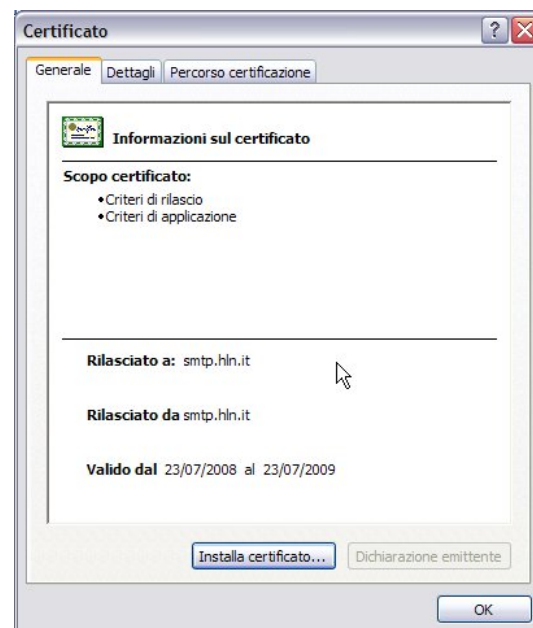
Premere il tasto “ok” per chiudere le altre impostazioni, premere il tasto “avanti” per chiudere le impostazioni dell’account e poi il tasto “fine” per chiudere la finestra degli account.

Attivazione della crittografia

Se si intende abilitare la cifratura delle comunicazioni con il server SMTP, bisogna scaricare innanzitutto il certificato principale della Halnet (<http://www.hln.it/file/cacert.crt>).

Dopo aver scaricato il certificato, effettuare un doppio click sul file, premere sul tasto “Installa certificato” e andare avanti con il wizard fino al temine in cui apparirà il messaggio di importazione terminata.

Andare nel menù Strumenti / Account di posta elettronica
Lasciare indicato “Visualizza o cambia gli account di posta elettronica esistenti” e premere su avanti. Selezionare con un click singolo l’account di posta per cui si desidera attivare la crittografia con il server SMTP di Halnet e premere sul tasto “Cambia”.



Premere il tasto “Altre impostazioni”, e aprire la scheda “Impostazioni avanzate”. **Sotto la dicitura “Server di posta in uscita (SMTP)” attivare la casella “il server richiede una connessione crittografata (SSL)”.**

Nota: se lo si desidera, invece della porta **587** (in cui viene usato il protocollo SMTP+TLS) è possibile utilizzare la porta 465 (nella quale verrà usato il protocollo SMTP+SSL).

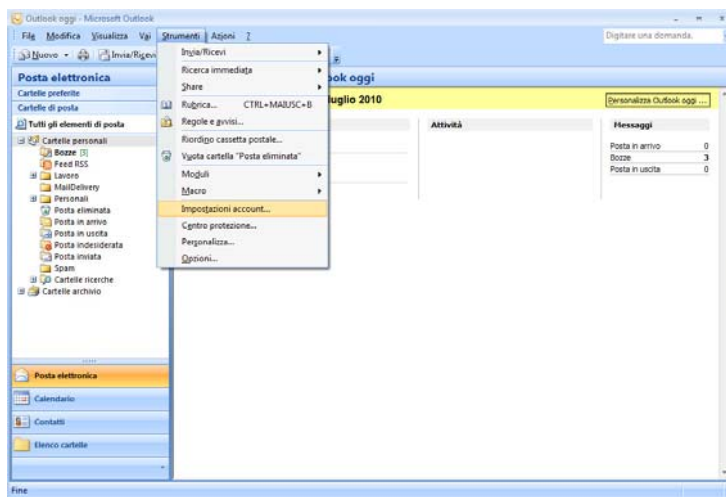
I due protocolli sono equivalenti in termini di sicurezza.

Premere il tasto “ok” per chiudere le altre impostazioni, premere il tasto “avanti” per chiudere le impostazioni dell’account e poi il tasto “fine” per chiudere la finestra degli account.

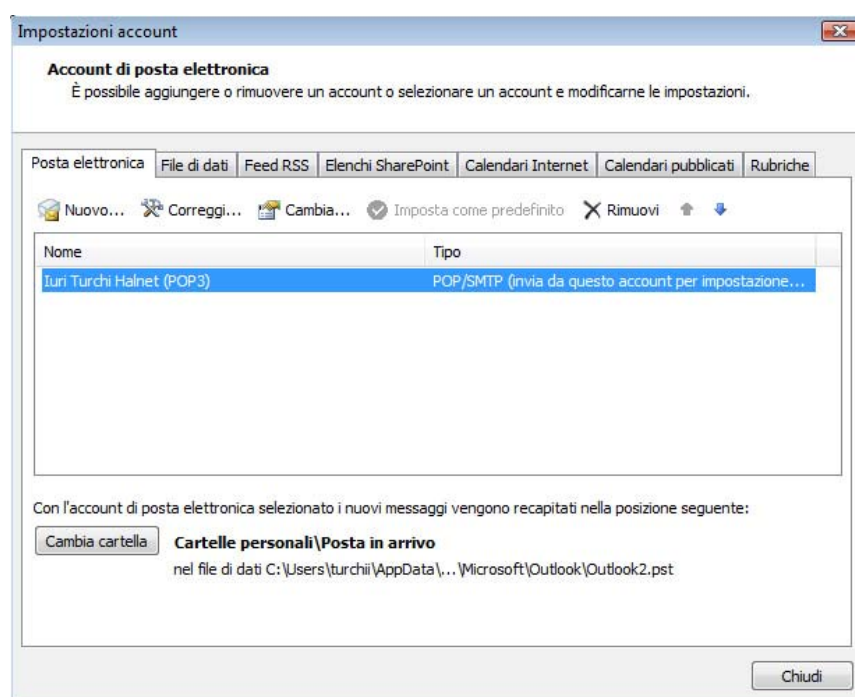
Nota: se lo si desidera, invece della comune porta 25 (in cui viene usato il protocollo SMTP+TLS) è possibile utilizzare la porta 465 (nella quale verrà usato il protocollo SMTP+SSL).

Outlook 2007

Andare nel menù Strumenti / Impostazioni Account



Selezionare con un click singolo l'account di posta per cui si desidera mandare la posta tramite il server SMTP di Halnet e premere sul tasto "Cambia".



Inserire nella voce “Server posta in uscita (SMTP)” la stringa **smtp.hln.it**. Premere sul tasto “Altre impostazioni” a aprire la scheda “Server della posta in uscita”. Abilitare la casella “il server della posta in uscita (SMTP) richiede l’autenticazione”.

Attivare l’opzione “Accedi con” e inserire le credenziali username/password fornite per il servizio SMTP.

Andare poi nella scheda “Impostazioni avanzate” e impostare la porta **587** nella casella “Server di posta in uscita (SMTP)”. Lasciare “nessuna” nel tipo di connessione crittografata (vedi sotto per attivare la crittografia).

Questa impostazione serve perché non tutti i provider lasciano aperta la porta 25 in uscita (serve per ostacolare lo spam). A tale scopo gli standard per la posta in uscita indicano di utilizzare la porta 587.

Se si lascia la porta 25 c'è la possibilità che il nostro server di posta segnali come spam la mail inviata in quanto non dovrebbe essere utilizzata dai client.

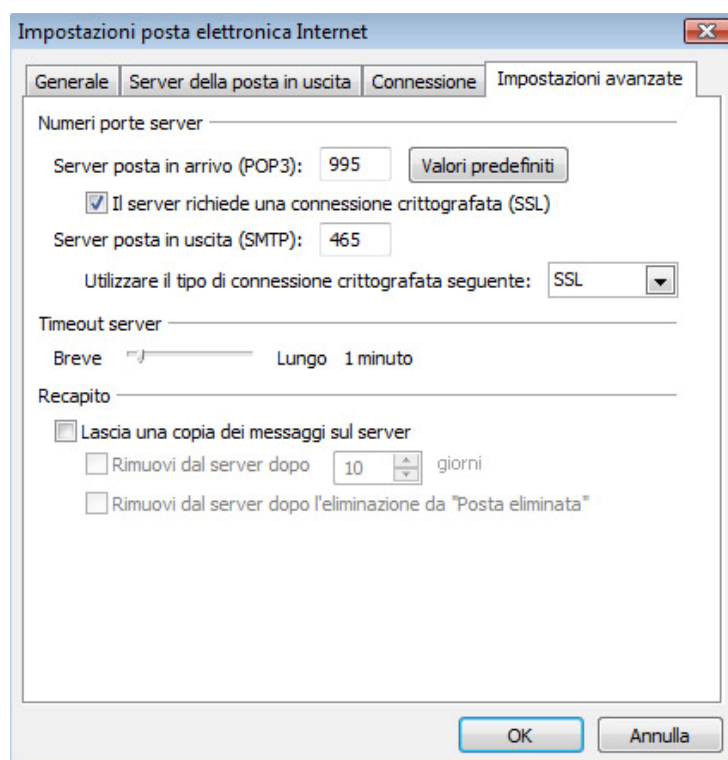
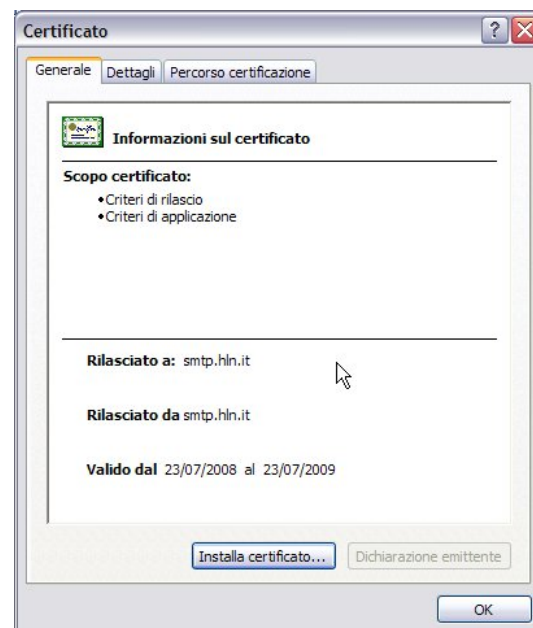
Premere il tasto “ok” per chiudere le altre impostazioni, premere il tasto “avanti” per chiudere le impostazioni dell'account e poi il tasto “fine” per chiudere la finestra degli account.

Attivazione della crittografia

Se si intende abilitare la cifratura delle comunicazioni con il server SMTP, bisogna scaricare innanzitutto il certificato principale della Halnet (<http://www.hln.it/file/cacert.crt>).

Dopo aver scaricato il certificato, effettuare un doppio click sul file, premere sul tasto “Installa certificato” e andare avanti con il wizard fino al termine in cui apparirà il messaggio di importazione terminata.

Andare nel menù Strumenti / Account di posta elettronica. Lasciare indicato “Visualizza o cambia gli account di posta elettronica esistenti” e premere su avanti. Selezionare con un click singolo l’account di posta per cui si desidera attivare la crittografia con il server SMTP di Halnet e premere sul tasto “Cambia”.



finestra degli account.

Premere il tasto “Altre impostazioni”, e aprire la scheda “Impostazioni avanzate”. Sotto la dicitura “Server di posta in uscita (SMTP)” indicare il tipo di crittografia voluta nel menù “Utilizzare il tipo di connessione crittografata seguente:”.

Se viene scelto il protocollo TLS lasciare la porta 587 (impostazione consigliata). Se invece viene scelta la crittografia SSL, è necessario importare la porta 465.

I due protocolli sono equivalenti in termini di sicurezza.

Premere il tasto “ok” per chiudere le altre impostazioni, premere il tasto “avanti” per chiudere le impostazioni dell’account e poi il tasto “fine” per chiudere la

Eudora 7

Purtroppo Eudora non permette, nella configurazione del server SMTP una coppia username/password diversa per l'invio.

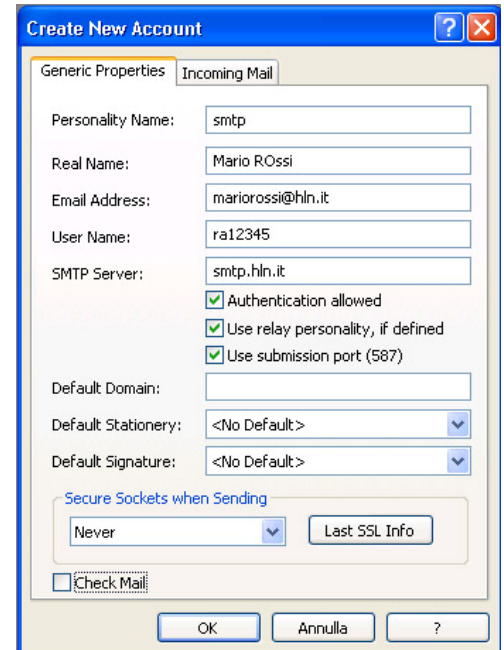
Quindi siamo costretti a creare una nuova identità con il menù Tool / Personalities.

Nella colonna di sinistra, utilizzare il tasto destro e indicare "New...", poi selezionare la voce "Skip directly to advanced account setup" e cliccare su Avanti.

Chiamiamo l'account "smtp", poi inseriamo nome, indirizzo email, e username (quello per l'invio tramite smtp).

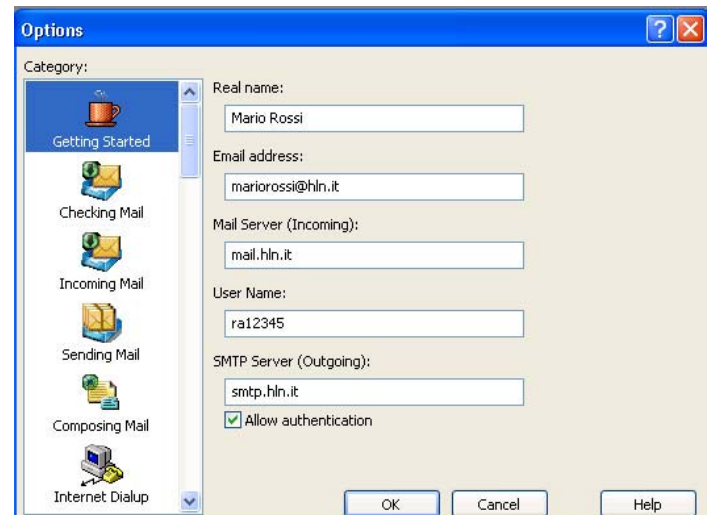
Come server SMTP indichiamo "smtp.hln.it" e ci assicuriamo che siano abilitate le voci "Authentication allowed", "Use relay personality, if defined" e "Use submission port (587)".

Nella voce "Secure Sockets" mettiamo "Never" per disabilitare la crittografia (vedi sotto nel caso si voglia abilitarla).



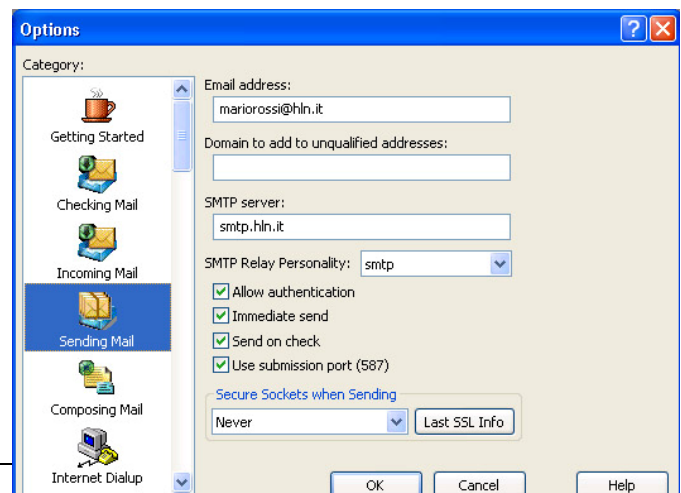
Inoltre disabilitiamo "Check Mail" in quanto questo account viene utilizzato solo per l'invio.

Poi con il menù Tools / Options torniamo nella scheda "Getting Started" e mettiamo "smtp.hln.it" nella voce "SMTP Server" e attiviamo "Allow authentication" se non è già attiva.



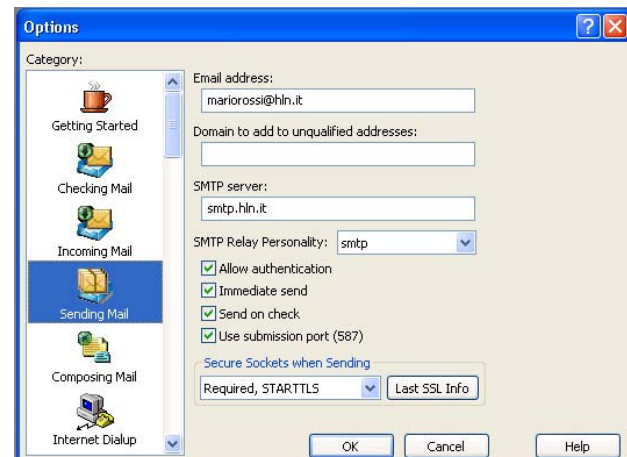
Infine, nella scheda "Sending mail" mettiamo "smtp.hln.it" nella voce "SMTP server", poi indichiamo "smtp" nella voce "SMTP Relay Personality" e mettiamo "Never" nella voce "Secure Sockets".

Abilitiamo inoltre anche la voce "Use submission port (587)".

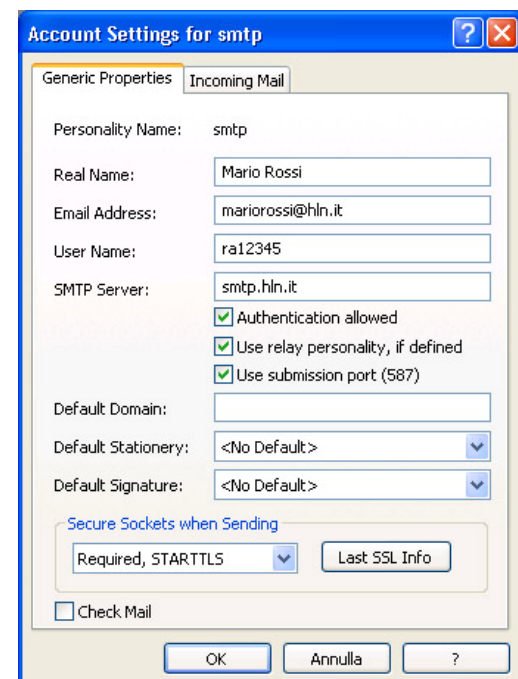


Attivazione della crittografia

Nel menù Tools / Options, andiamo nella scheda “Sending Mail” e mettiamo “Required, STARTTLS”.

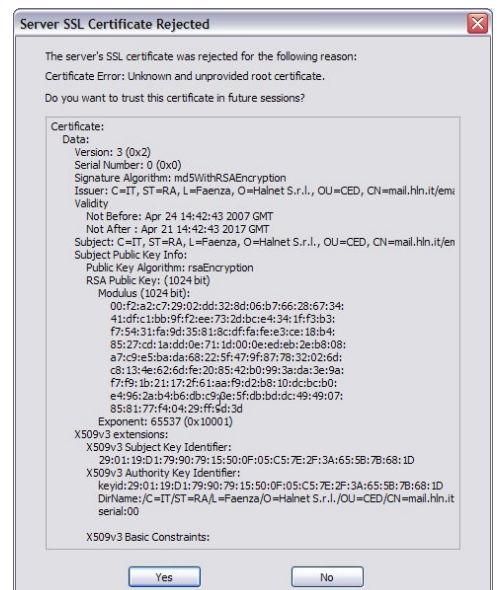


Poi richiamiamo il menù Tools / Personalities, clicchiamo con il tasto destro sull'identità “smtp” creata in precedenza e richiamiamo le proprietà. Nella voce “Secure Sockets” mettiamo “Required, STARTTLS”.



A questo punto al primo tentativo di inviare i messaggi apparirà la seguente schermata che mostra il certificato del server di posta.

Premere su “Yes” per accettare il certificato. A questo punto basta rieseguire il download dei messaggi e questi verranno scaricati.



Altri client di posta

Allo stesso modo, il servizio è compatibile con tutti i più comuni client di posta (ad esempio Mozilla Thunderbird).

La configurazione con gli altri client è molto simile (solitamente cambiano solo le diciture e il metodo di importazione dei certificati).

Per problemi di configurazione con altri client di posta contattateci.