RuparPiemonte

Manuale di installazione certificato digitale per la sicurezza

Certification Authority di SistemaPiemonte

SOMMARIO

1. PREMESSE

Questo documento fornisce le istruzioni necessarie all'installazione e all'utilizzo dei certificati per autenticazione rilasciati dalla Certification Authority di SistemaPiemonte all'interno dei browser più comunemente usati, Netscape Communicator e Microsoft Internet Explorer.
Per poter installare il certificato digitale è necessario avere a disposizione il CIP e la password, oltre al dischetto che contiene il file con il certificato digitale in formato PKCS12.

2. IL CERTIFICATO DIGITALE

Il **certificato digitale** è una sorta di carta di identità digitale che permette ad un soggetto di fornire le proprie credenziali durante le transazioni in rete. Consideriamo ad esempio una Carta d'Identità emessa dal Comune di Torino per la persona Bianchi Andrea. La Carta di Identità attesta che la fotografia apposta rappresenta proprio Bianchi Andrea e nessun altro. Chiunque riconosca l'autorità del Comune di Torino, e più in generale dell'Italia, può fidarsi che colui che espone tale carta di identità è proprio Bianchi Andrea. Su Internet l'autorità riconosciuta si chiama **Certification Authority (CA)**, la carta di identità viene sostituita dal certificato digitale, la fotografia viene sostituita dalla chiave pubblica generata e di proprietà dell'utente.
La CA è un'entità pubblica o privata la cui principale funzione è di "certificare" il legame tra un utente e la propria chiave pubblica. In base a questo certificato si possono determinare le generalità dell'utente.
La Certification Authority deve essere depositaria di fiducia in quanto si fa garante del fatto che ogni chiave pubblica sia legata al proprietario attraverso un certificato.
Secondo lo standard definito a livello internazionale (**X 509)**, un certificato è un insieme di informazioni binarie suddivise in campi e contiene sostanzialmente i seguenti dati:

- la CA che lo ha emesso;
- il nome del soggetto cui il certificato si riferisce;
- la chiave pubblica del soggetto;
- il periodo di tempo in cui il certificato deve essere utilizzato (periodo di validità o "certificate validity");
- le estensioni standard e/o private (questi campi determinano caratteristiche aggiuntive al certificato).

Lo scopo dell'utilizzo di certificati digitali nella comunicazione su Web è duplice:

- è l'equivalente elettronico di un documento di identità, quindi attesta l'identità di una parte che sta scambiando informazioni (sia esso una persona o un server);
- permette di scambiare dati in maniera sicura senza che altri soggetti possano leggerli o modificarli.

Una volta che le due parti coinvolte nella comunicazione accettano l'una il certificato dell'altra, attraverso la tecnologia Secure Socket Layer (SSL) viene stabilito un canale sicuro (criptato) su cui scambiare le informazioni.

3. VERIFICA DELLA VERSIONE CORRETTA DEL BROWSER

Per garantire un livello di sicurezza, autenticazione e riservatezza adeguato alla tipologia di informazioni trasmesse nel contesto di questo servizio, i certificati digitali emessi dalla CA di SistemaPiemonte sono basati su chiavi asimmetriche di lunghezza minima di 1024 bit e richiedono l'utilizzo di browser in grado di supportare crittografia simmetrica con chiavi a 128 bit.[1]

[1] È noto che messaggi cifrati con chiavi DES a 56 bit sono stati decifrati in tempi molto brevi

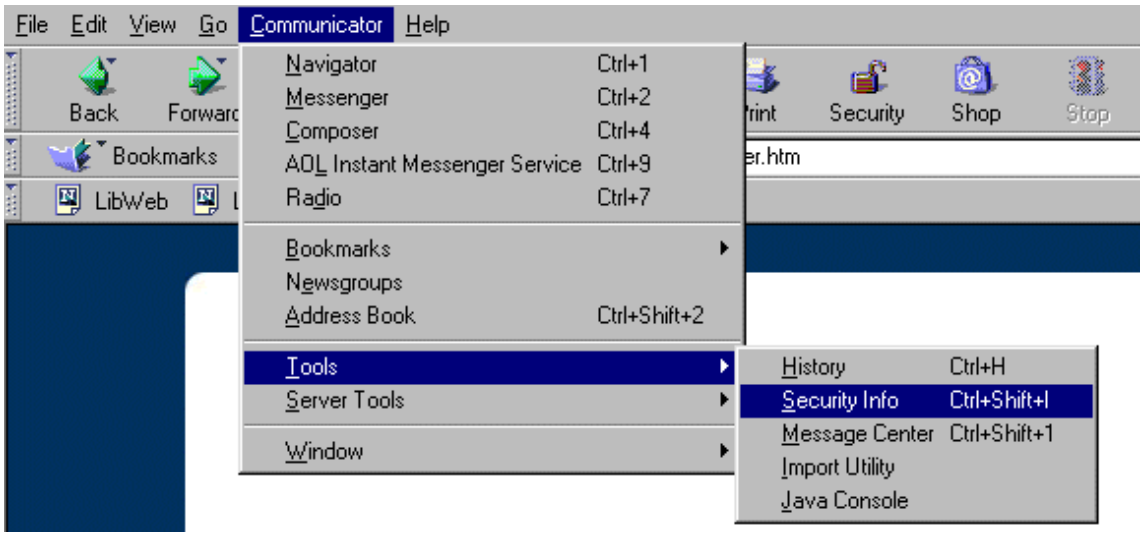
La prima operazione da effettuare è la verifica del tipo di cifratura a cui è abilitato il proprio browser. Per questo tipo di operazione si può fare riferimento al paragrafo **Individuazione del browser e del modulo di cifratura**.
Il browser deve poter consentire l'utilizzo di chiavi DES a 128 bit ("strong encryption") per la cifratura dei dati.

4. INSTALLAZIONE DI CERTIFICATI CON NETSCAPE NAVIGATOR 4.5 E 4.7

I passi successivi descrivono la procedura di installazione di certificati mediante Netscape Navigator nella versione in italiano e in inglese.

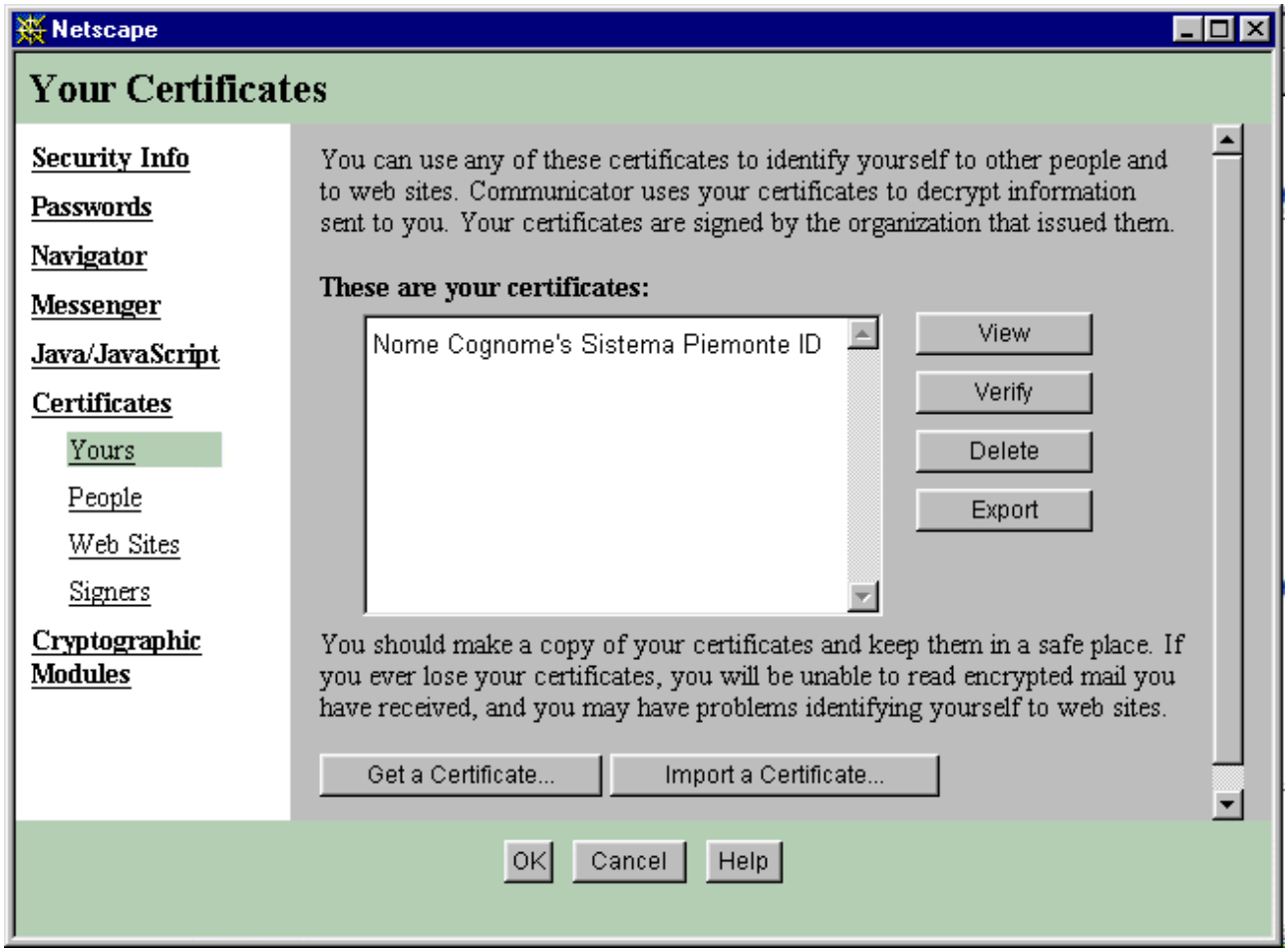
4.1 IMPORT DEL CERTIFICATO

- Lanciare Netscape Navigator.
- Selezionare dalla barra degli strumenti il menu "**Communicator**" e scegliere "**Strumenti**" ("**Tools**").
- Selezionare "**Info sicurezza**" ("**Security Info**").

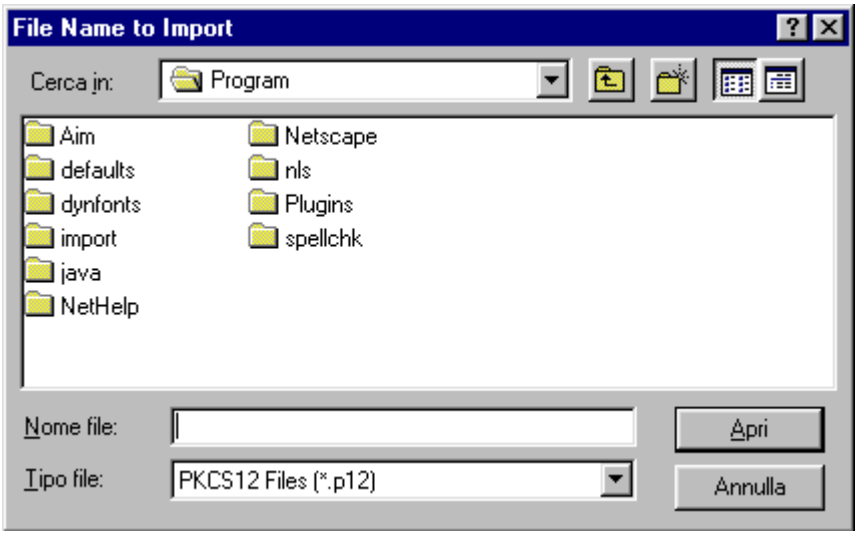


- Cliccare su "**Personale**" ("**Yours**"), apparirà una finestra con una casella elenco per la visualizzazione dei certificati in vostro possesso.

- Cliccare sul pulsante "**Importa un certificato**" ("**Import a certificate**").



- Selezionare il certificato, costituito da un file con estensione p12 e cliccare sul pulsante "**Apri**". Se il file si trova su dischetto è necessario spostarsi dal disco rigido al disco A.



- Successivamente viene richiesta la password con cui avete protetto il database dei certificati nel vostro browser. Se non avete indicato nessuna password potete inserirne una o cliccare direttamente su invio (nessuna password).

- Inizia a questo punto la procedura di installazione del certificato. Comparirà una finestra dove viene richiesto di inserire la password con cui è stato protetto il vostro certificato e che vi è stata fornita insieme al dischetto contenente il certificato.

  *Esempio: se la password riportata sulla seconda lettera è **abcdefgh** e il Codice di Identificazione Personale stampato sulla prima lettera è **5678X234,** la password che protegge il certificato sarà **abcdefgh5678X234**.*

- Al termine dell'operazione vi verrà detto se l'importazione del certificato ha avuto successo.

4.2 VERIFICA DEL CERTIFICATO

Dopo aver concluso la fase di importazione del certificato è opportuno fare una verifica dello stesso. La prima operazione da effettuare riguarda l'organismo di certificazione (CA o Certification Authority) che ha emesso il certificato:

- occorre posizionarsi, nella finestra "**Info sicurezza**" ("**Security info**"), sulla voce "**Certificati**" ("**Certificates**") e scegliere la sotto-voce "**Firmatari**" ("**Signers**");
- selezionare "CA di sicurezza di SistemaPiemonte" e quindi cliccare sul bottone "**Modifica**" ("**Edit**");
- appare una finestra dove compaiono le informazioni sul certificato e le checkbox per riconoscere fiducia all'organismo di certificazione;
- abilitare tutte le voci di accettazione per il riconoscimento dell'organismo di certificazione.

La seconda operazione consiste nel verificare il proprio certificato:

- posizionarsi, nella finestra "**Info sicurezza**" ("**Security info**"), in "**Certificati**" ("**Certificates**") e scegliere la voce "**Personale**" ("**Yours**");
- selezionare il proprio certificato;
- cliccare sul tasto "**Verifica**" ("**Verify**");
- dovrà apparire un messaggio che conferma la verifica del certificato in oggetto. Infatti oltre alla verifica dell'integrità del certificato viene riconosciuta fiducia all'entità che lo ha emesso;
- dare "**OK**" per chiudere l'operazione.

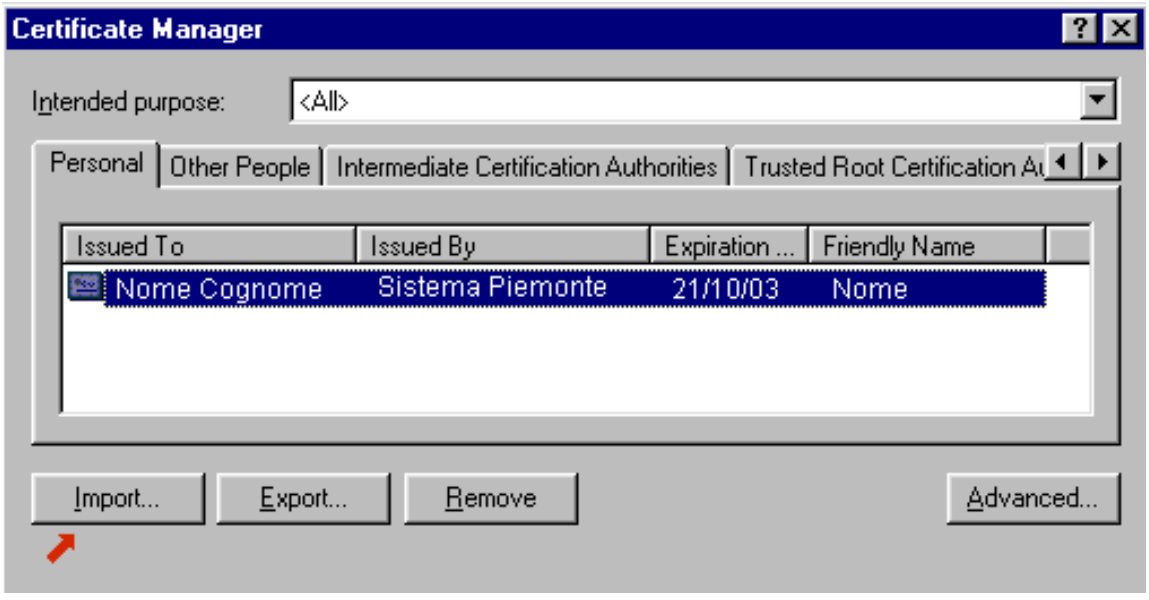
5. INSTALLAZIONE DI CERTIFICATI CON MICROSOFT INTERNET EXPLORER 5, 5.5 E 6.0

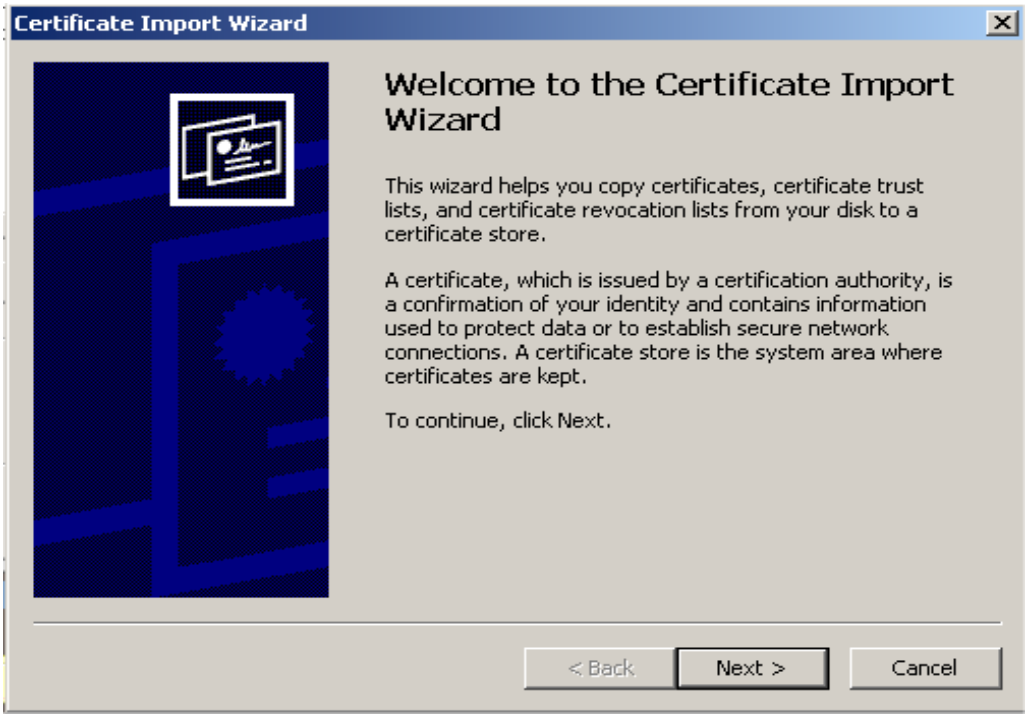
5.1 IMPORT DEL CERTIFICATO

- Lanciare Internet Explorer.
- Selezionare dalla barra degli strumenti il menu "**Strumenti**" ("**Tools**") e cliccare su "**Opzioni Internet**" ("**Internet Options**").
- Nella finestra apparsa cliccare sulla voce:

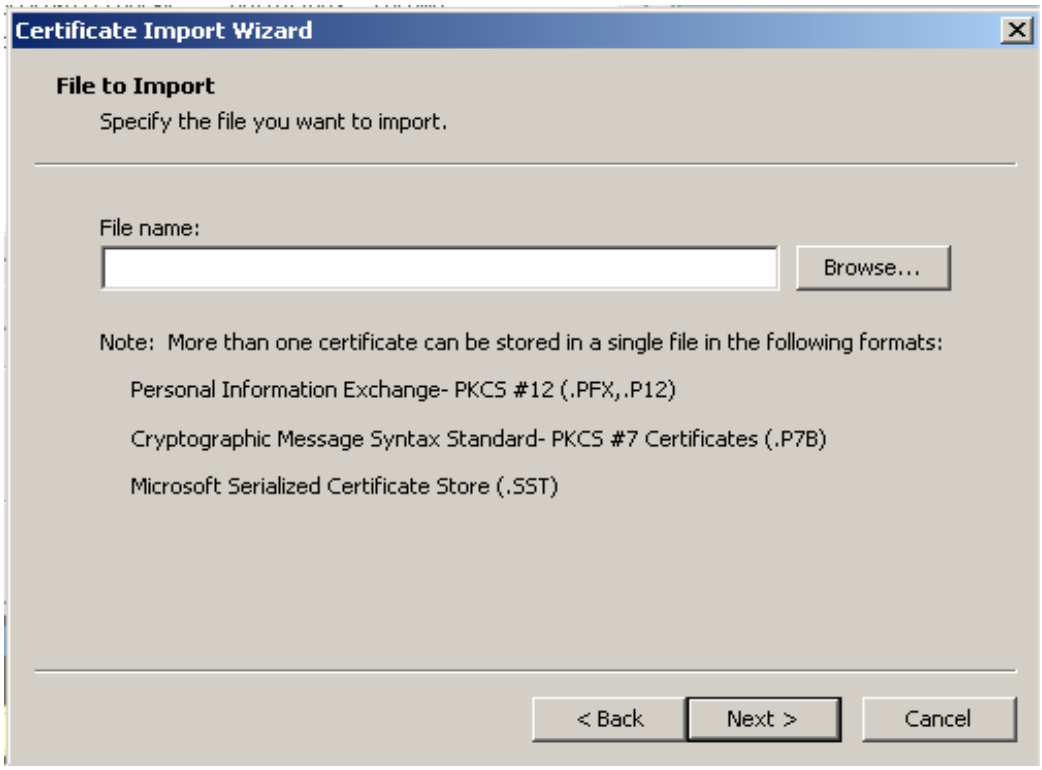
  Explorer 5.0 e 5.5: "**Contenuto**" ("**Content**") e quindi sul pulsante "**Certificati**" ("**Certificates**");
  Explorer 6.0: sulla voce "**Protezione**" ("**Security**") e quindi su "**ID digitali**" ("**Digital ID's**").

- Appare la finestra dei certificati. Premere il pulsante "**Importa**" ("**Import**") e seguire i seguenti passi.





- Cliccare su "**Avanti**" ("**Next**").
- Premere il tasto "**Sfoglia**" ("**Browse**").



- Selezionare come Tipo File:

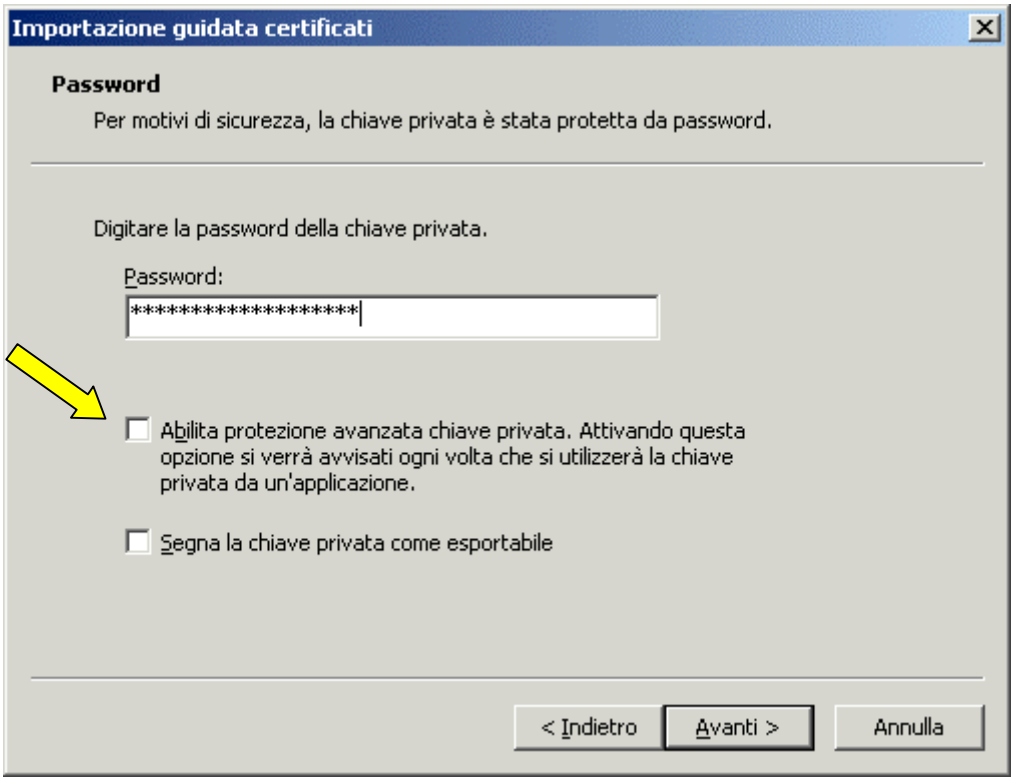
  *Sotto Windows NT – "**Tutti i file (*.*)" ("All Files (*.*)");*

Sotto Windows 2000 – "**File di scambio informazioni personali (*.pfx, *.p12)**" (" **.... (*.pfx, *.p12)**").

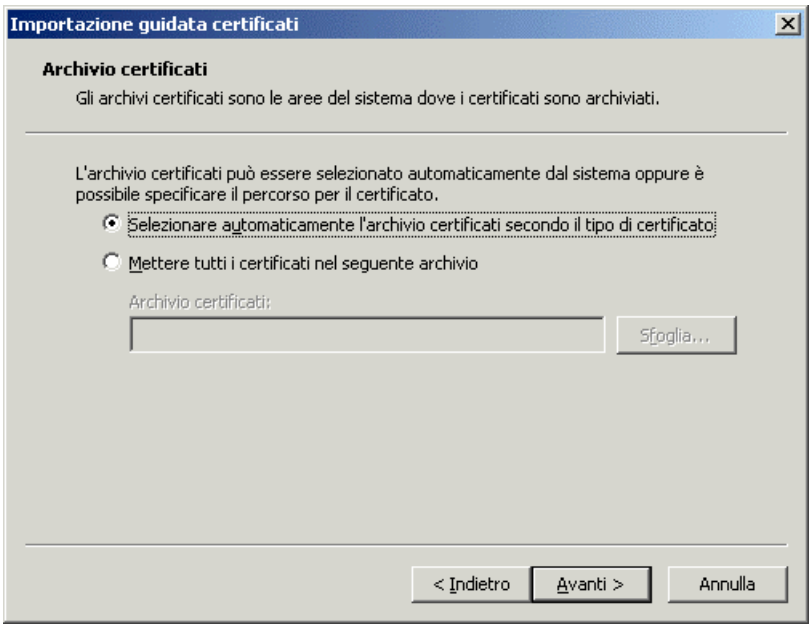
- Selezionare la cartella contenente il file.
- Selezionare il file contenente il certificato.
- Cliccare su "**Apri**" ("**Next**").
- Cliccare su "**Avanti**" ("**Next**").
- Compare una finestra dove viene richiesto di inserire la password con cui è stato protetto il vostro certificato e che vi è stata fornita insieme al dischetto contenente il certificato.

  *Esempio: se la password riportata sulla seconda lettera è **abcdefgh** e il Codice di Identificazione Personale stampato sulla prima lettera è **5678X234,** la password che protegge il certificato sarà **abcdefgh5678X234**.*

In questa finestra selezionare anche la checkbox per abilitare la protezione avanzata della chiave privata, indicata in figura.

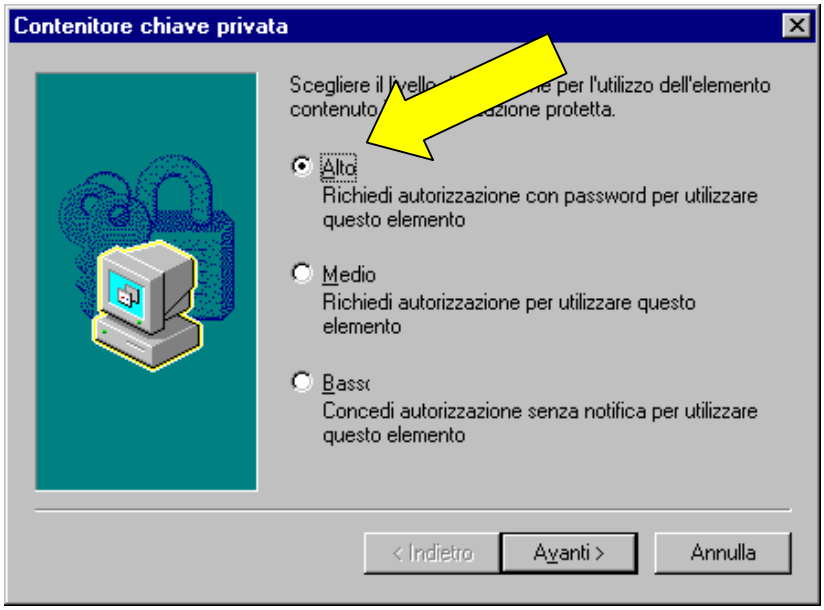


- Cliccare su "**Avanti**" ("**Next**").
- Compare una nuova finestra. Lasciare "**Selezionare automaticamente l'archivio certificati secondo il tipo di certificato**" ("**Automatically select the certificate store**").

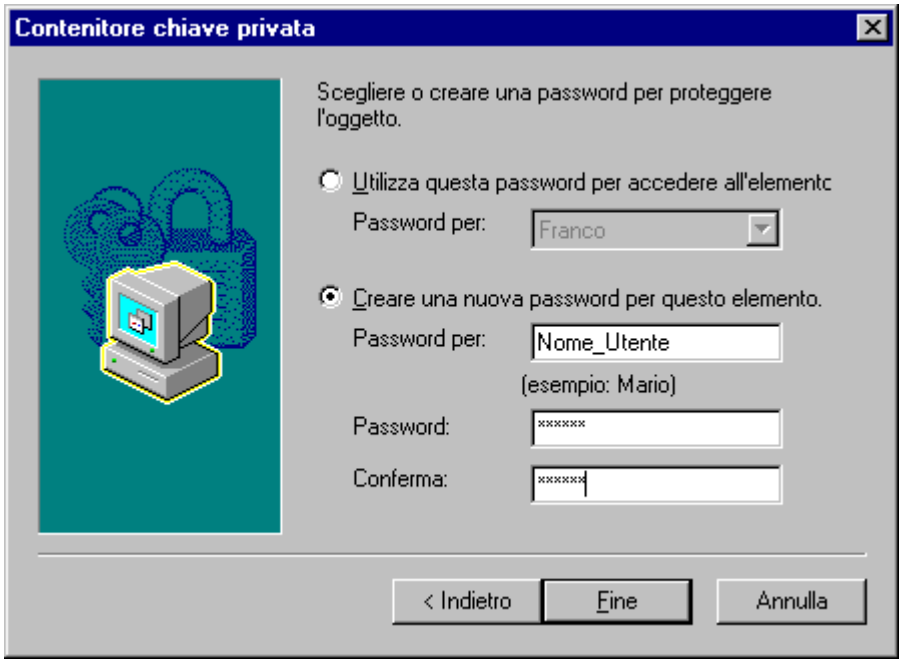


- Cliccare su “**Avanti**” (“**Nex**t”).
- Nella finestra successiva cliccare su “**Fine**” (“**Finish**”).
- Apparirà una finestra come la seguente, sulla quale dovete impostare il livello di protezione del certificato cliccando su “Imposta livello di protezione”.

- L’utente può impostare il livello di protezione: qualora il livello sia alto verrà richiesta la password ad ogni cambio pagina.

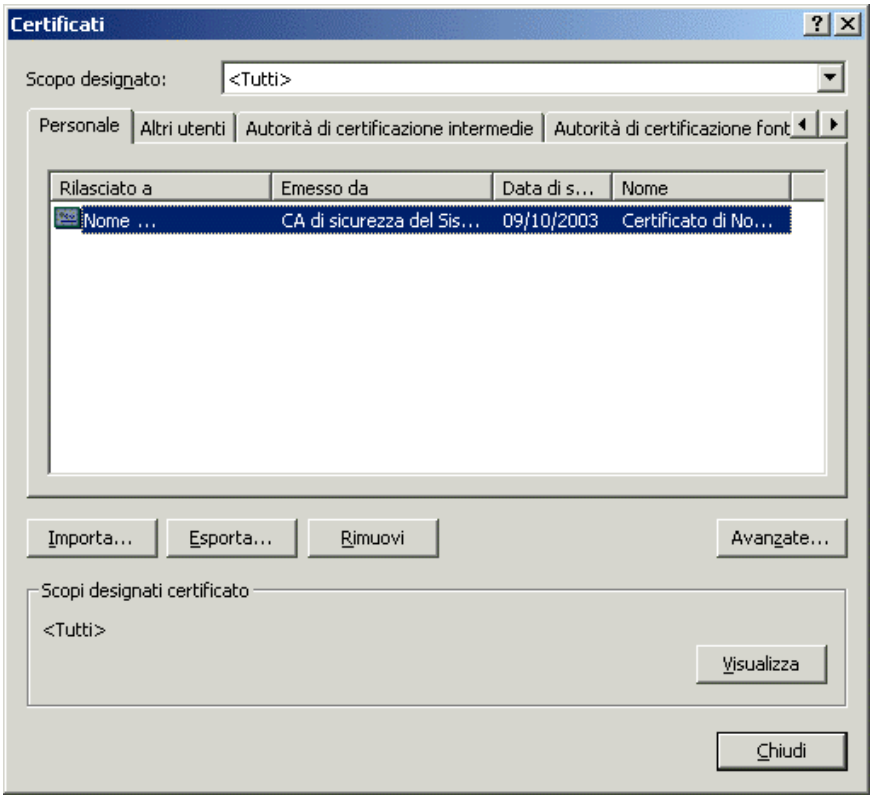


- La finestra successiva richiede la creazione di un profilo utente per la gestione personale del certificato (nel caso in cui la postazione venisse utilizzata da più utenti contemporaneamente tale configurazione permette di mantenere protetta da una password personale il proprio certificato) o l'associazione del certificato appena installato ad un profilo già presente.



- Nell'ultima finestra viene richiesto di digitare nuovamente la password prescelta per la memorizzazione sul disco fisso del PC. Nel caso in cui la postazione venisse utilizzata da più utenti contemporaneamente, è opportuno verificare che l'opzione "**Registra password**" (o "**Remember password**") non sia selezionata.

- Cliccare su "**OK**".
- A conclusione delle operazioni descritte nella finestra dei certificati deve comparire il nuovo certificato appena inserito.

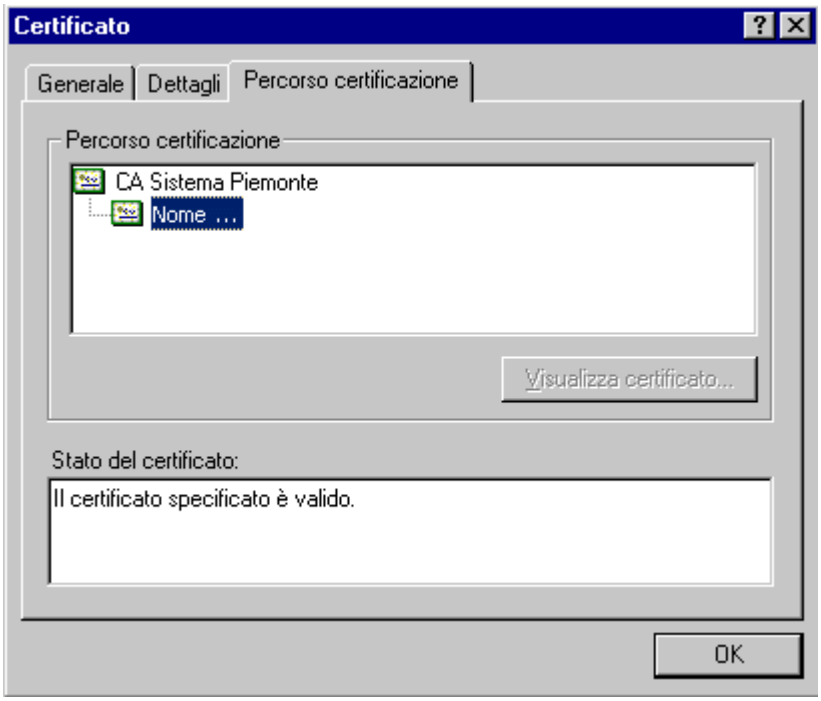


- Chiudere la finestra dei certificati con il tasto "**Chiudi**" ("**Close**").

5.2 VERIFICA DEL CERTIFICATO

Al termine delle seguenti operazioni, prima di accedere al servizio applicativo al quale siete stati abilitati attraverso la consegna del certificato, può essere opportuno verificare il corretto funzionamento del sistema.

- Nella finestra "**Gestione Certificati**" dovrebbe apparire il vostro certificato, selezionarlo cliccandoci sopra.
- Cliccare sul pulsante "**Visualizza**" ("**View**").
- Nella nuova finestra cliccare su "**Percorso di certificazione**" ("**Certification Path**"). All'interno dell'area denominata "**Stato del Certificato**" ("**Certificate status**") dovrebbe essere riportata l'indicazione "**Il certificato specificato è valido**" ("**This certificate is ok**"). Nel caso in cui l'indicazione non fosse tale, il certificato potrebbe non essere valido o potrebbe non essere stato installato quello della CA SistemaPiemonte.

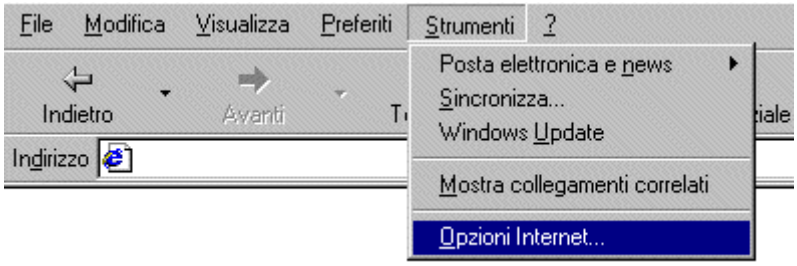


Nel caso non siano stati verificati i certificati si faccia riferimento al paragrafo seguente.

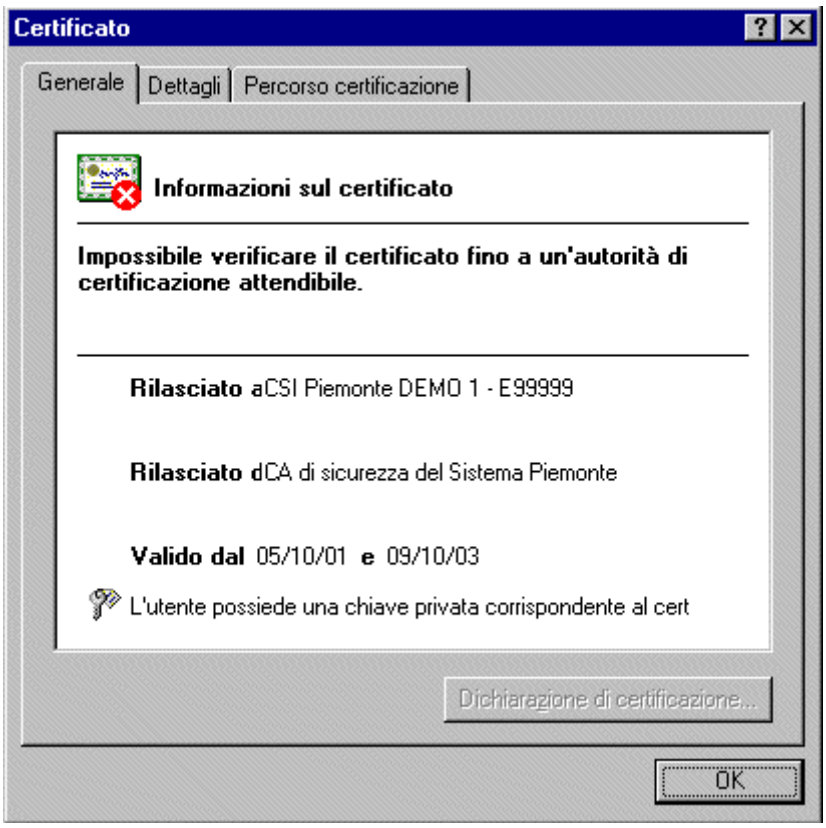
5.3 RISOLUZIONE PROBLEMI DI RICONOSCIMENTO DELLA CA

Quando viene installato il certificato digitale il browser automaticamente dovrebbe acquisire il certificato digitale della CA che l'ha emesso. In alcune versioni di Microsoft Internet Explorer 6.0 (e Outlook Express 6.0) questo non accade e quindi, mancando il certificato digitale della CA, il certificato installato non viene riconosciuto come attendibile. Lo stato del proprio certificato digitale può essere visualizzato nel seguente modo:

1.1 Lanciare Internet Explorer.
1.2 Selezionare dalla barra degli strumenti la voce "**Strumenti**" e cliccare su "**Opzioni Internet**".



1.3 Appare una nuova finestra. Cliccare sulla voce "**Contenuto**" e quindi sul pulsante "**Certificati**".
1.4 Nella nuova finestra cliccare sulla voce "**Personale**" e selezionare il proprio certificato.
1.5 Cliccando sul pulsante "**Visualizza**" verranno visualizzate le informazioni relative al certificato digitale.



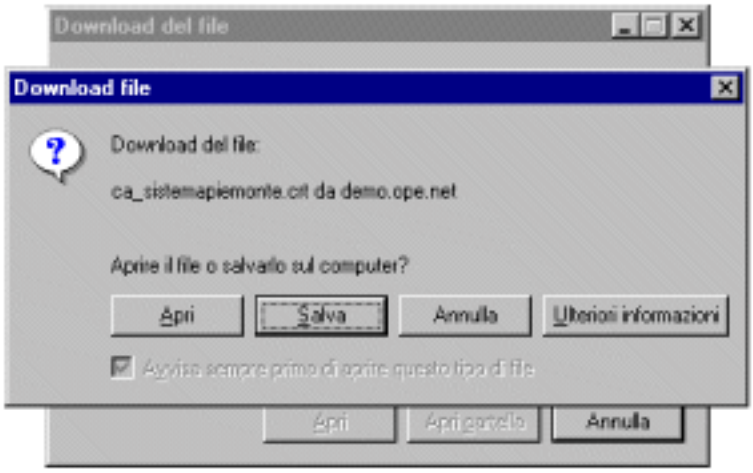
La figura mostra il certificato con un asterisco rosso e l'indicazione che il certificato non può essere verificato. Questo significa che manca il certificato digitale della CA. Per correggere questo problema è possibile utilizzare due modalità alternative:

1. installare il certificato della CA;
2. disinstallare il proprio certificato, installare un aggiornamento software dei browser fornito da Microsoft e quindi reinstallare il proprio certificato.

Modalità 1

Per installare il certificato della CA occorre procedere come segue:

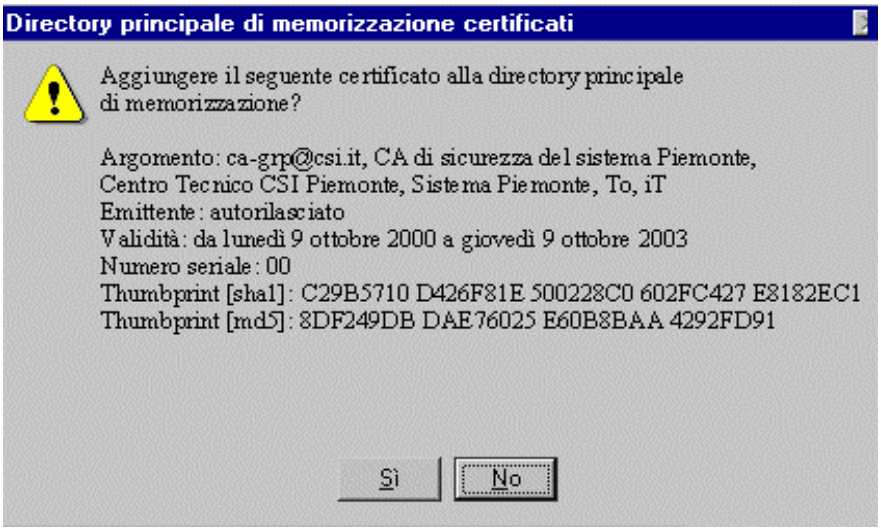
1.1 Scaricare dalla pagina di accesso al servizio il **certificato della CA** e aprirlo cliccando sul pulsante "**Apri**".



1.2 Cliccare sul pulsante "**Installa certificato**"

1.3 Cliccare sui pulsanti "**Avanti**" e "**Fine**" senza cambiare le impostazioni di default date.

1.4 Sulla finestra di conferma cliccare su "**SI**" e quindi su "**OK**" fino a chiudere tutte le finestre.



A questo punto il certificato digitale è stato correttamente installato.
Per verificare se il proprio certificato viene riconosciuto rieseguire la procedura indicata ad inizio pagina.

Modalità 2
Per disinstallare il certificato della CA procedere come segue:
- rieseguire i passi da 1.1 a 1.4;
- cliccare sul pulsante "**Rimuovi**" e confermare.

A questo punto il certificato digitale è stato disinstallato e si può procedere con lo scarico del **software di aggiornamento**. Una volta scaricato, eseguire il file che attiverà la procedura di aggiornamento. Al termine della procedura riavviare il PC. Dopo aver effettuato questa operazione è sufficiente reinstallare il proprio certificato digitale.

6. NOTE SULLA GESTIONE DEI CERTIFICATI

Nel caso in cui il certificato digitale venga installato su postazioni di lavoro utilizzate da più utenti (ad esempio nel laboratorio di una scuola) è consigliabile procedere alla disinstallazione dello stesso dopo l'utilizzo per evitare rischi di sicurezza. Ad esempio alcuni browser come Netscape 4.7 non permettono di associare una password ad un singolo certificato, ma solo all'archivio che contiene tutti i certificati installati sul browser. Ciò comporta che un utente che conosce la password dell'archivio dei certificati possa di fatto utilizzare uno qualunque dei certificati dell'archivio nelle comunicazioni via Web.

7. REQUISITI SOFTWARE PER L'INSTALLAZIONE DEI CERTIFICATI DIGITALI

Le versioni di browser che supportano il protocollo di sicurezza SSL con cifratura DES a 128 bit sono: Microsoft Internet Explorer ver. 5.5 o successive e Netscape Communicator 4.7 - italiano.
Se si dispone di versioni precedenti è possibile scaricare gli aggiornamenti dai siti:
http://www.microsoft.com/windows/ie_intl/it/download/
http://wp.netscape.com/download/

7.1 MICROSOFT INTERNET EXPLORER

- Aprire il browser.
- Selezionare la voce "**About Internet Explorer**" ("**Informazioni su Internet Explorer**" per la versione italiana) dal menu a tendina "**Help**" ("**?**" per la versione italiana).

- Appaiono la versione del browser e il tipo di cifratura supportata.
- Sotto l'indicazione del browser viene riportato il modulo di cifratura usata.
  Se il modulo di cifratura è quello corretto appare la dicitura:
  "**Cipher strength 128-bit**" ("**Livello di codifica 128 – bit**")

- Se manca il modulo di cifratura a 128 bit è possibile scaricarlo dal sito:
  http://www.microsoft.com/windows/ie_intl/it/download/128bit/intro.htm

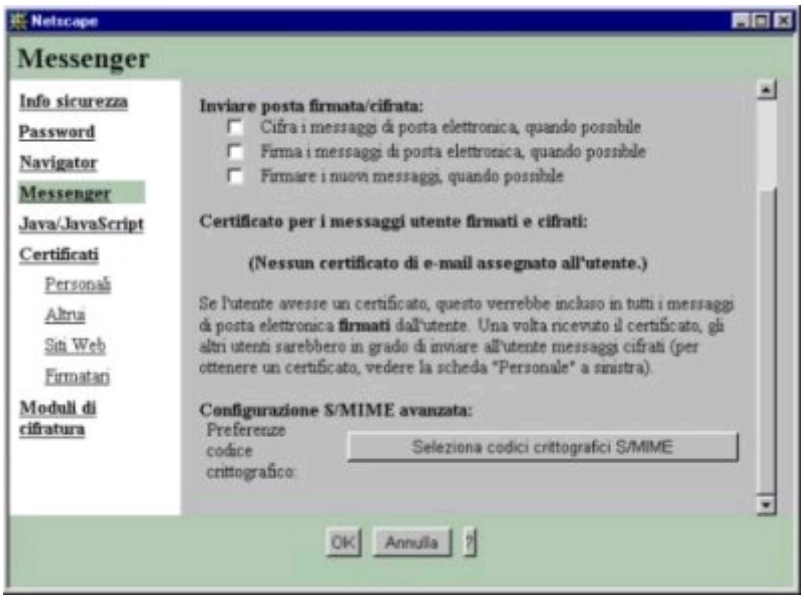
7.2 NETSCAPE COMMUNICATOR

- Aprire il browser.
- Selezionare la voce "**Informazioni su Communicator**" dal menu a tendina contrassegnato col simbolo "**?**"

- Appare la versione del browser: se la versione è antecedente alla 4.04 è necessario installare una versione aggiornata (con cifratura a 128 bit).

Il modulo di cifratura per Netscape Communicator va verificato attraverso le seguenti operazioni:

- Aprire il menu "**Communicator**"
- Posizionarsi su "**Strumenti**" e selezionare "**Info sicurezza**"
- Scegliere la voce "**Messenger**" e cliccare sul bottone "**Seleziona codici crittografici S/MIME**"



- Viene visualizzato l'elenco dei codici e delle lunghezze delle chiavi di cifratura.
  Se sono presenti chiavi a 128 bit controllare che siano abilitate o abilitarle in caso contrario.
  Se tali chiavi non sono presenti occorre scaricare un aggiornamento del browser, con cifratura a 128 bit, dal sito **http://www.fortify.net/intro.html**.

Settembre 2002

Assistenza tecnica

Help Desk CSI-Piemonte - Numero Verde 800.250.505 - E-mail hd_rupar@csi.it

REGIONE PIEMONTE

csipiemonte

www.ruparpiemonte.it