

**MANUALE DI INSTALLAZIONE DEL
CERTIFICATO DIGITALE RILASCIATO DALLA
CERTIFICATION AUTHORITY DEL SISTEMA PIEMONTE**



www.sistemapiemonte.it

INDICE

1. PREMESSE	3
2. VERIFICA DELLA VERSIONE CORRETTA DEL BROWSER	3
3. INSTALLAZIONE DI CERTIFICATI CON NETSCAPE NAVIGATOR	3
3.1 IMPORT DEL CERTIFICATO.....	3
3.2 VERIFICA DEL CERTIFICATO	5
4. INSTALLAZIONE DI CERTIFICATI CON MICROSOFT INTERNET EXPLORER 5 , 5.5 E 6.0	7
4.1 IMPORT DEL CERTIFICATO.....	7
4.2 VERIFICA DEL CERTIFICATO	12
4.3 RISOLUZIONE PROBLEMI DI RICONOSCIMENTO DELLA CA.....	13
5. NOTE SULLA GESTIONE DEI CERTIFICATI	17
6. INFORMAZIONI GENERALI SUL CERTIFICATO DIGITALE	17

1. PREMESSE

In questo manuale sono contenute le istruzioni per poter installare ed utilizzare i certificati digitali per autenticazione, rilasciati dalla Certification Authority del Sistema Piemonte, nei browser più comunemente usati, Netscape Communicator e Microsoft Internet Explorer. Prima di poter installare il certificato digitale è necessario controllare:

- che il proprio browser sia adeguato (seguendo le istruzioni riportate al par.2);
- di avere a disposizione il CIP, la password e il file con il certificato digitale in formato PKCS12.

2. VERIFICA DELLA VERSIONE CORRETTA DEL BROWSER

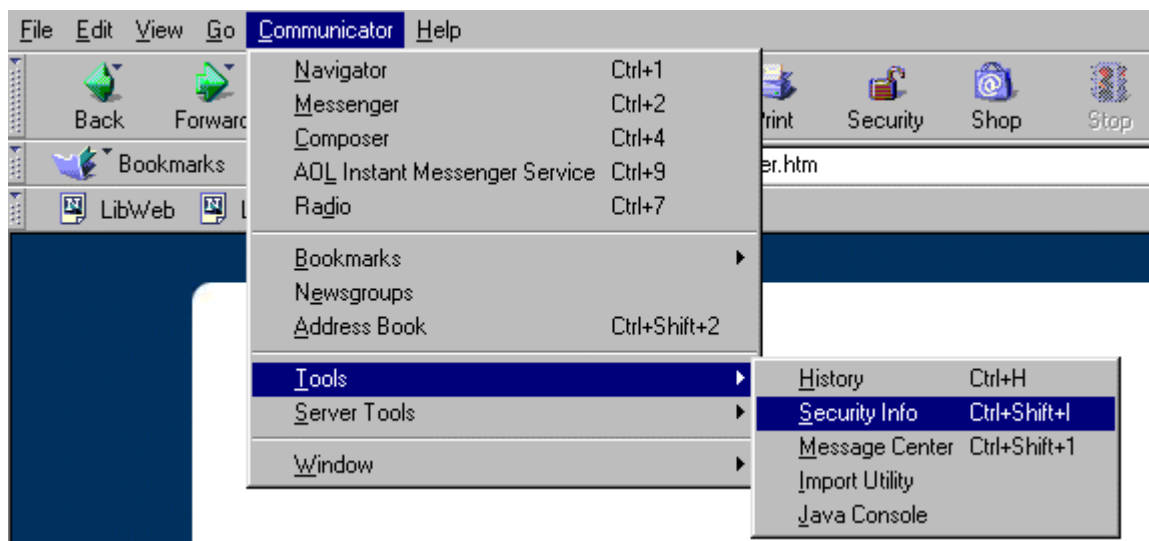
Per garantire un livello di sicurezza adeguato i certificati SistemaPiemonte richiedono il supporto da parte del browser utilizzato di un determinato tipo di cifratura dei dati trasmessi. Per verificare il livello di cifratura a cui è abilitato il browser, si faccia riferimento al **documento**. Il browser deve poter consentire l'utilizzo di chiavi DES a 128 bit ("strong encryption") per la cifratura dei dati.

3. INSTALLAZIONE DI CERTIFICATI CON NETSCAPE NAVIGATOR

In questo paragrafo, vengono riportati i passi da seguire per installare il proprio certificato nel browser Netscape Navigator. Vengono riportate le diverse finestre che vanno aperte e le opzioni da configurare, sia per la versione italiana che inglese.

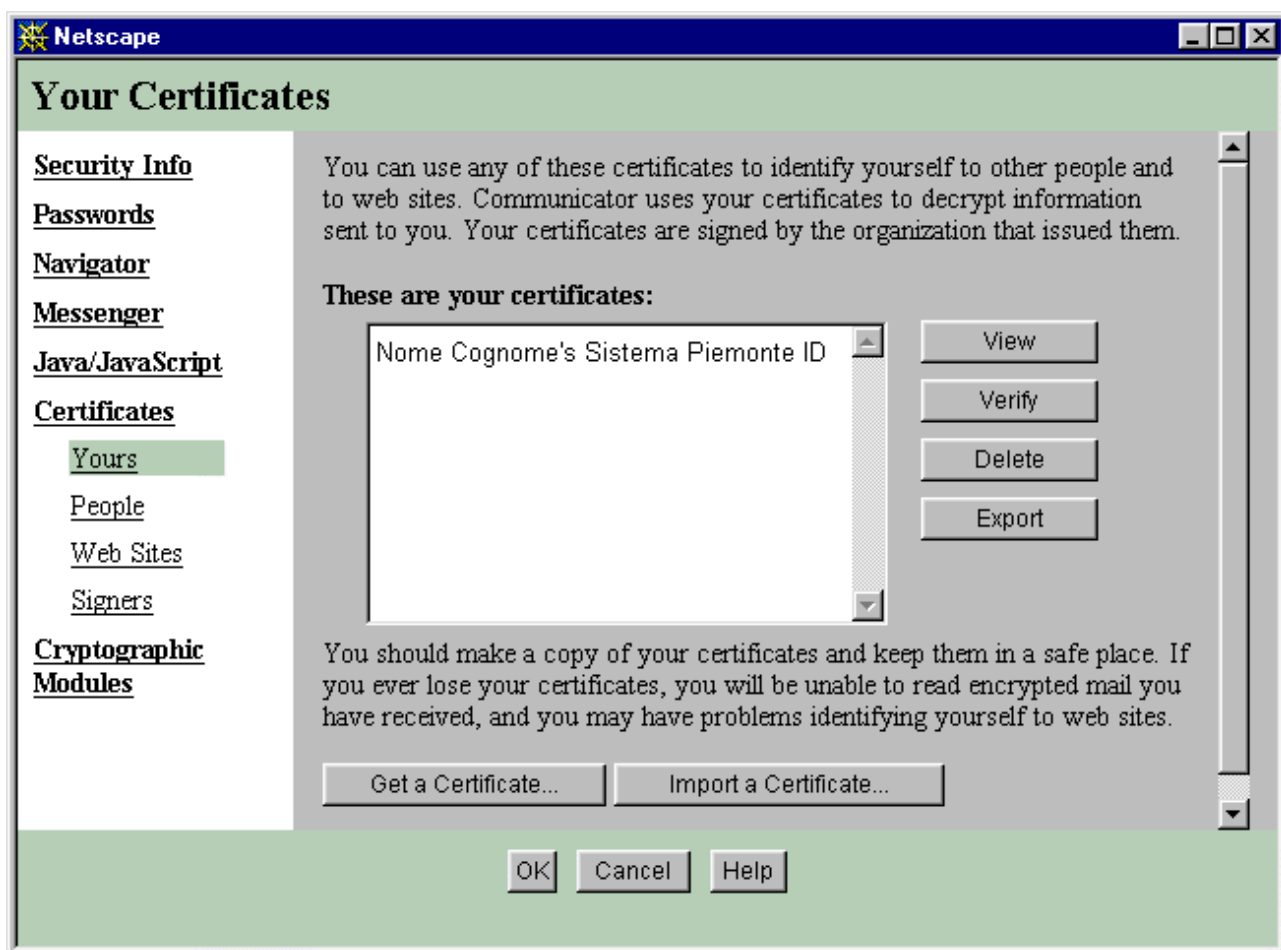
3.1 IMPORT DEL CERTIFICATO

- 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 l'archivio dei certificati nel vostro browser. Se non avete mai 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 certificato stesso.

*Esempio: se la password che vi è stata comunicata è **abcdefgh** e il Codice di Identificazione Personale (CIP) è **5678X234**, la password che protegge il certificato sarà **abcdefgh5678X234**.*

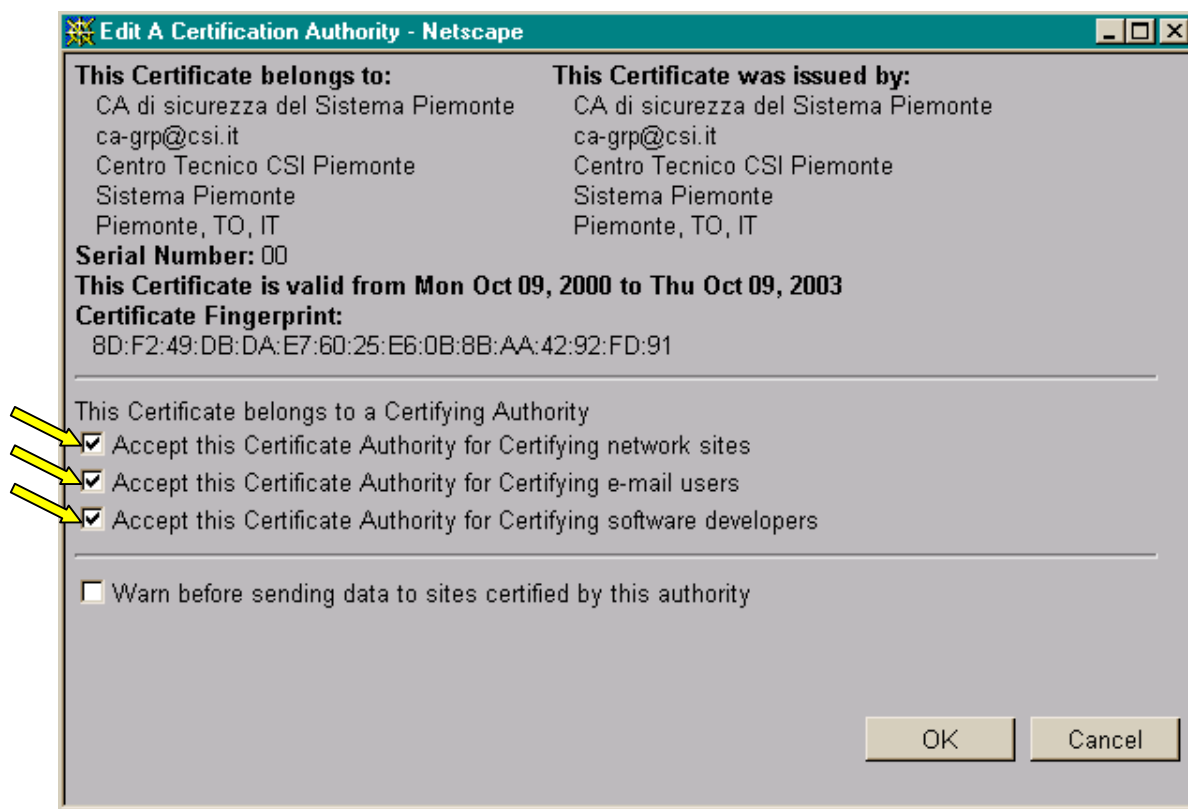
- Al termine della procedura vi verrà detto se l'importazione del certificato ha avuto successo.

3.2 VERIFICA DEL CERTIFICATO

Dopo aver concluso la fase di importazione del certificato è opportuno fare una verifica dello stesso, per controllare che sia riconosciuto correttamente dal proprio browser.

La prima operazione da effettuare riguarda l'organismo di certificazione (CA o Certification Authority) che ha emesso il certificato:

- occorre posizionarsi, sempre nella finestra "**Info sicurezza**" ("Security info), sulla voce "**Certificati**" ("Certificates") e scegliere la sotto-voce "**Firmatari**" ("Signers").
- selezionare "CA di sicurezza del Sistema Piemonte" 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, sempre 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.
- Dare **"OK"** per chiudere l'operazione.

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

4.1 IMPORT DEL CERTIFICATO

- Lanciare Internet Explorer

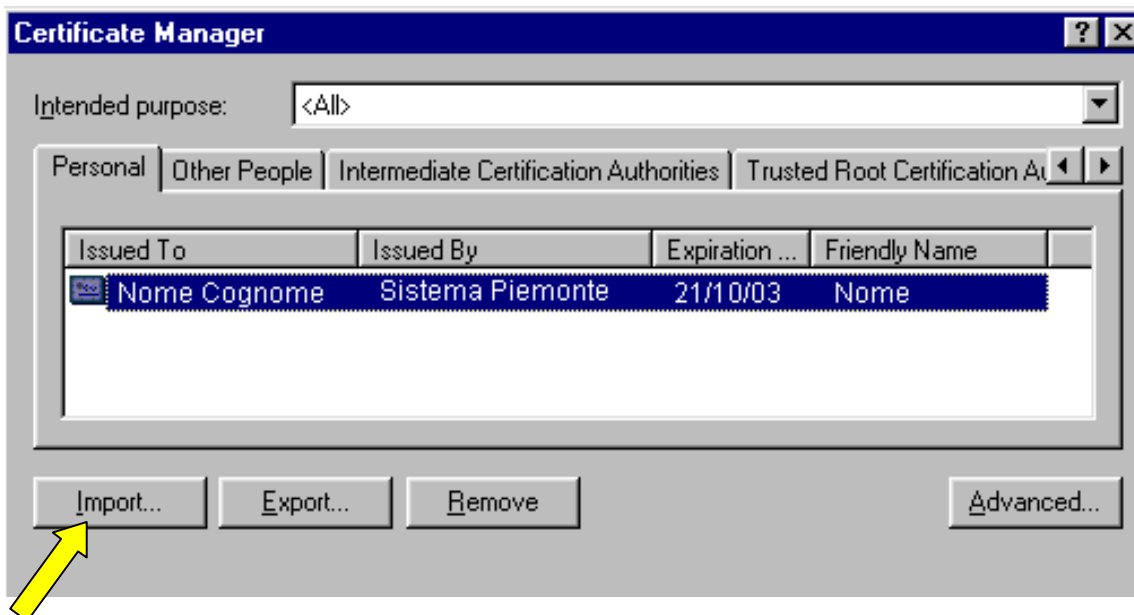
Selezionare dalla barra degli strumenti il menu “**Strumenti**” (“Tools”) e cliccare su “**Opzioni Internet**” (“Internet Options”).

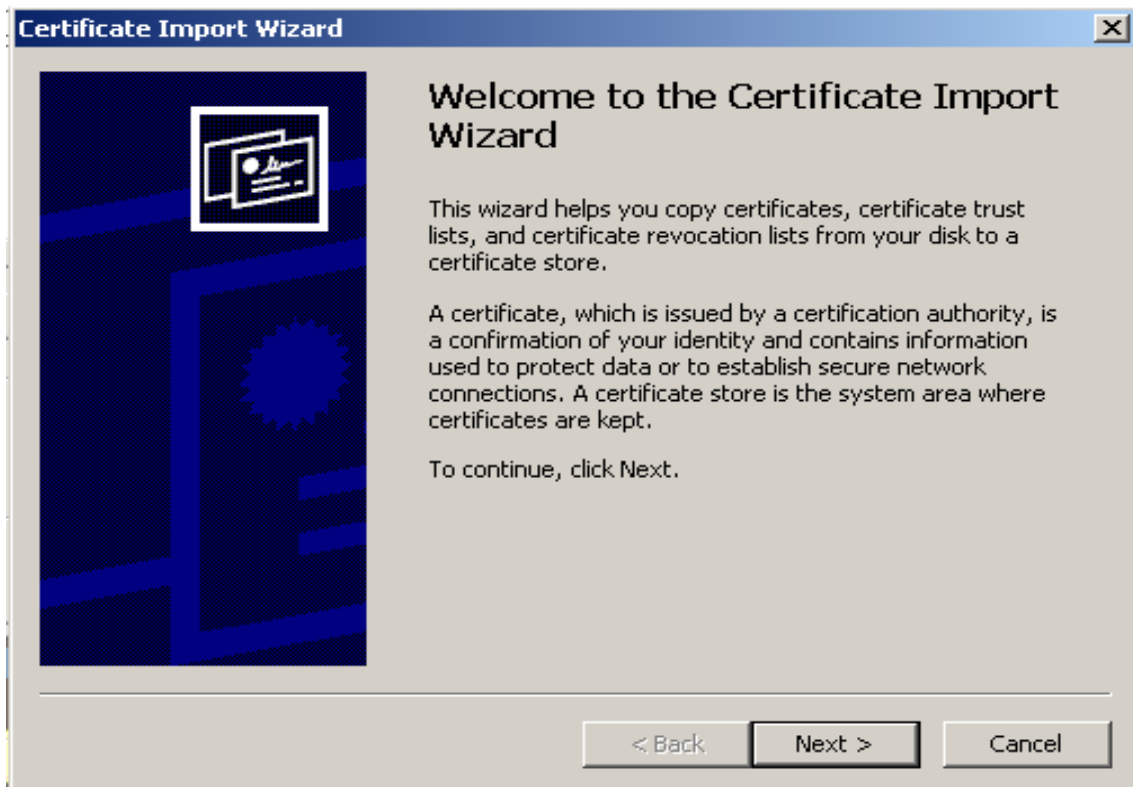
- Nella finestra apparsa cliccare sulla voce

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”).

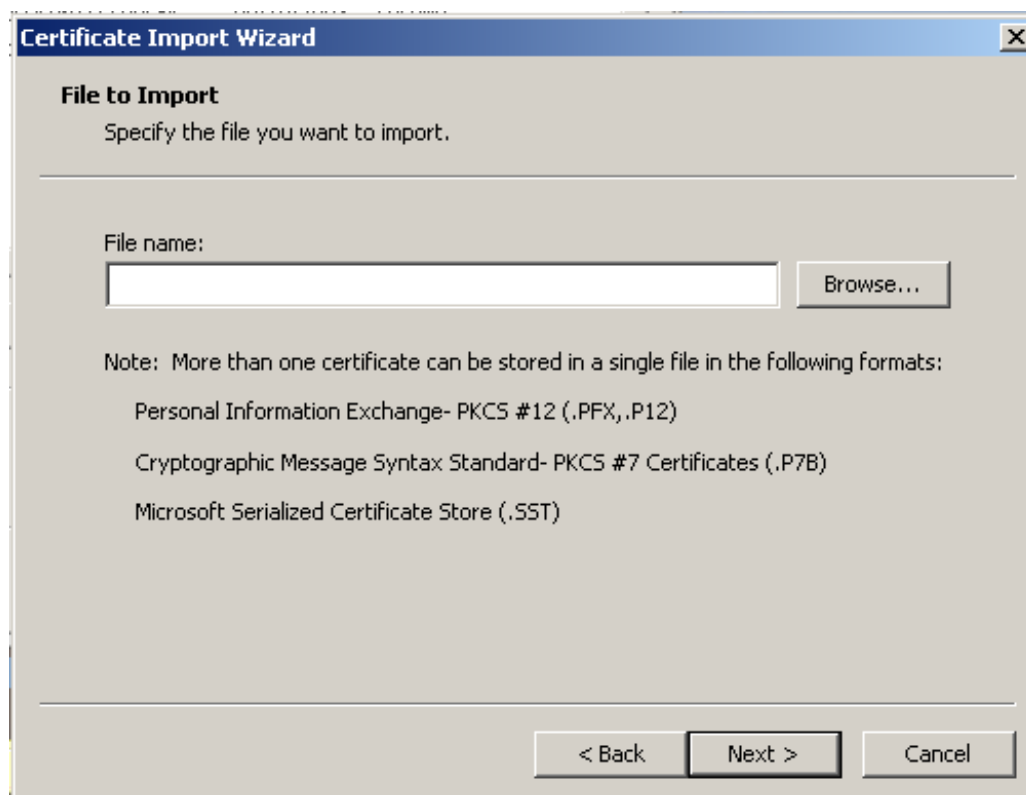


- Appare la finestra dei certificati. Premere il pulsante “**Importa**” (“Import”) e seguire i seguenti passi.





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



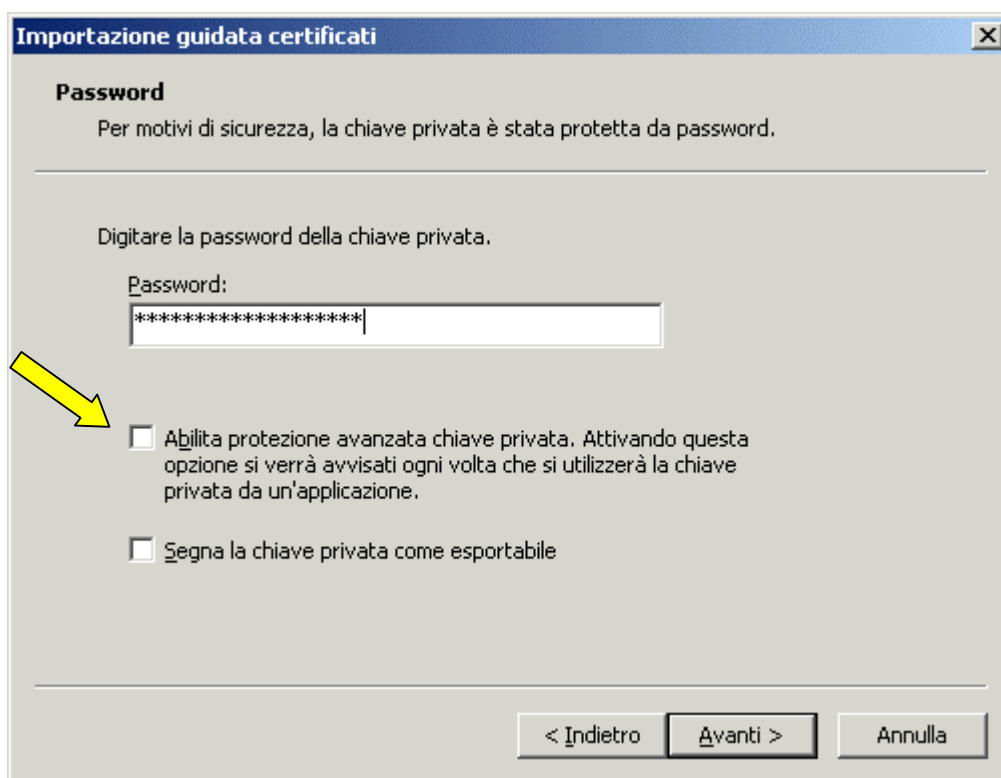
- Selezionare come Tipo File:
Sotto Windows NT - "Tutti i file (*.*)" ("All Files (*.*)").

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

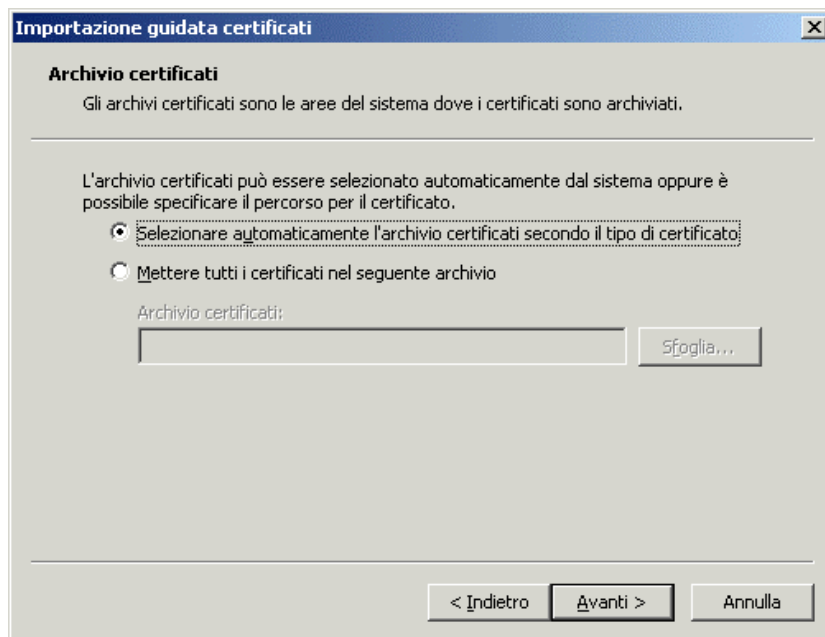
- Selezionare la cartella contenente il file.
- Selezionare il file contenente il certificato.
- Cliccare su "Apri" ("Next")
- Cliccare su "Avanti" ("Next")
- Compare una finestra dove viene richiesto di inserire la password con cui è stato protetto il vostro certificato e che vi è stata fornita insieme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

*Esempio: se la password che vi è stata assegnata è **abcdefgh** e il Codice di Identificazione Personale (CIP) 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



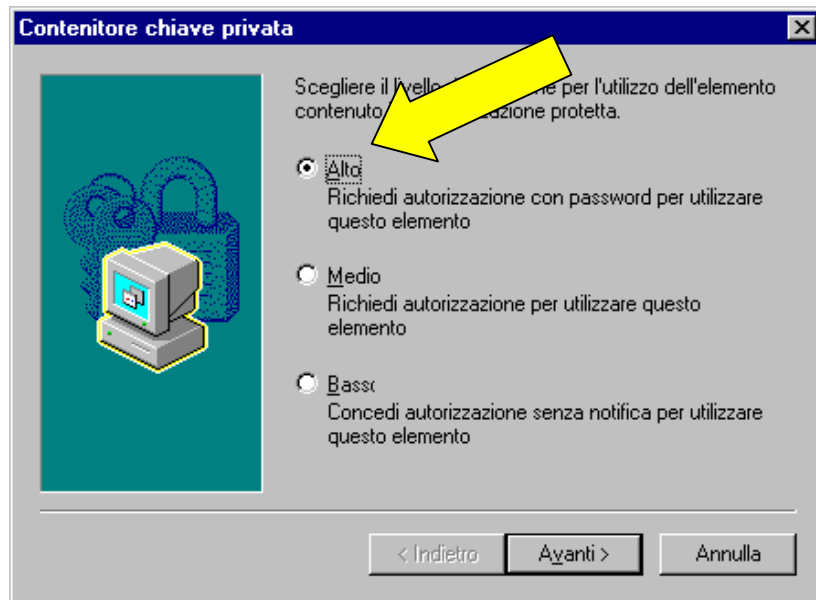
- Cliccare su "Avanti" ("Next")
- Compare una nuova finestra. Lasciare selezionato "**Selezionare automaticamente l'archivio certificati secondo il tipo di certificato**" ("Automatically select the certificate store").



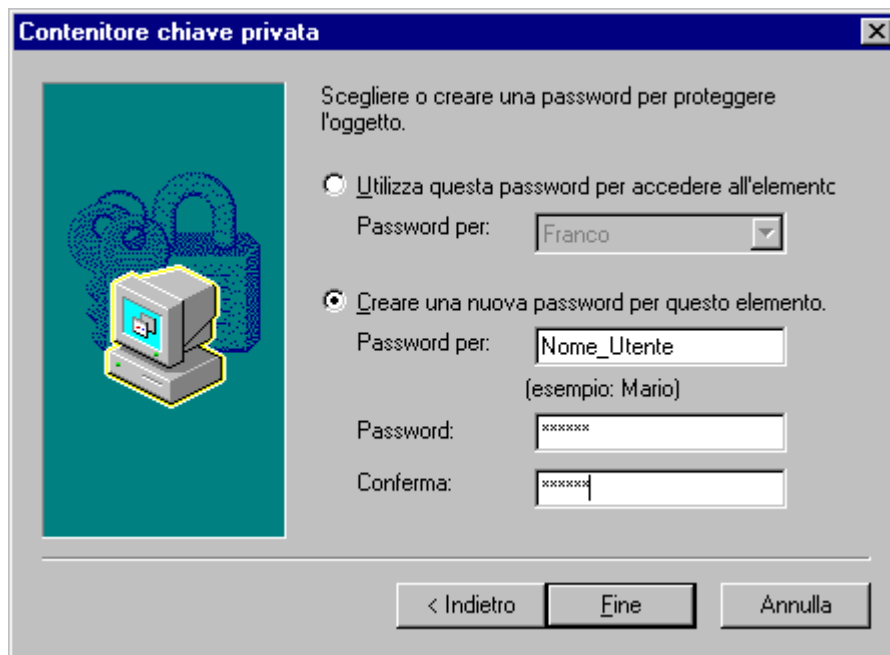
- Cliccare su **"Avanti"** ("Next")
 - Nella finestra successiva cliccare su **"Fine"** ("Finish")
- Apparirà una finestra come la seguente, sulla quale dovete impostare il livello di protezione del certificato, cliccando su "Imposta livello di protezione" :



- Selezionare il livello di protezione ad ALTO



- 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 :

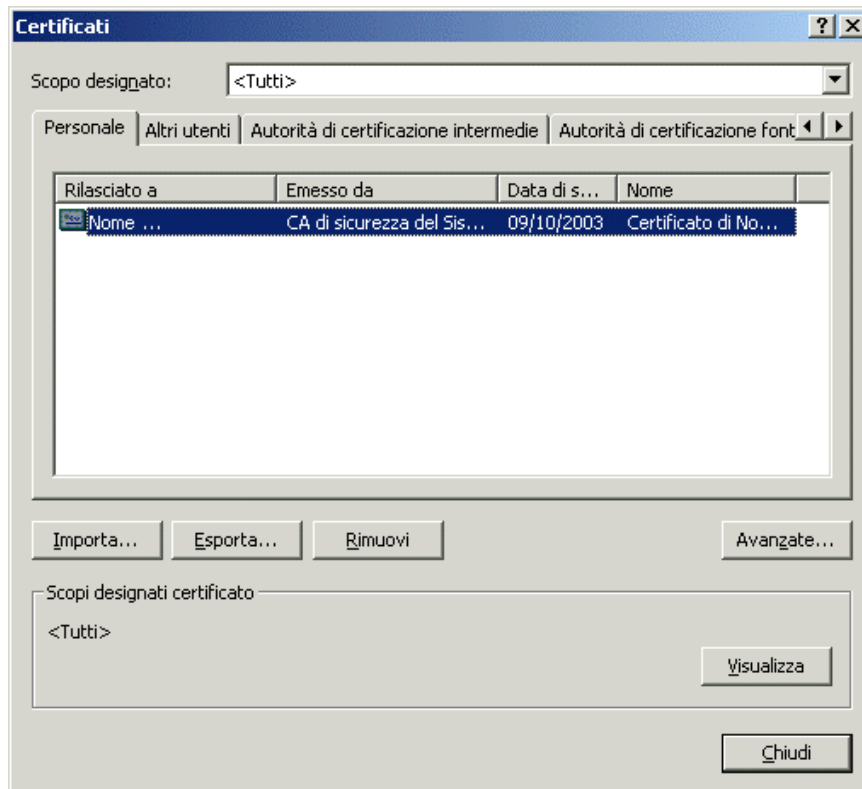


- Come ultima finestra, viene richiesto di ridigitare la password prescelta per la sua memorizzazione sul disco fisso del PC. Anche qui, per maggior sicurezza nel caso in cui la postazione sia utilizzata da più utenti contemporaneamente, è opportuno verificare che sia DESELEZIONATA l'opzione "registra password" (o "remember password") :



- Cliccare su OK

Dopo queste operazioni nella finestra dei certificati deve comparire il nuovo certificato appena inserito



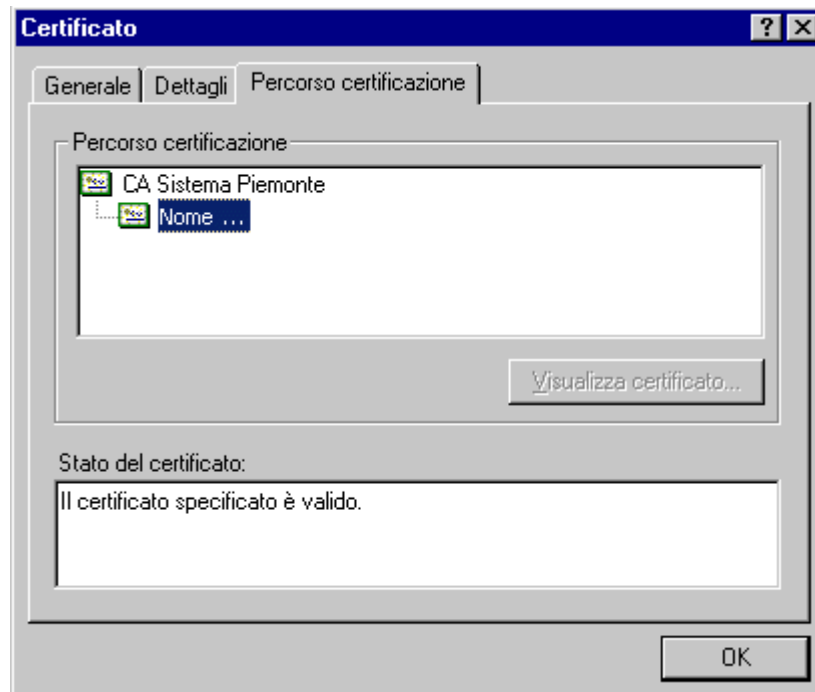
- Chiudere la finestra dei certificati con il tasto "**Chiudi**" ("Close").

4.2 VERIFICA DEL CERTIFICATO

Dopo aver concluso la fase di importazione del certificato è opportuno fare una verifica dello stesso.

- Nella finestra "**Gestione Certificati**" ora 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 il certificato dell'Autorità di Certificazione di Sistema Piemonte.



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

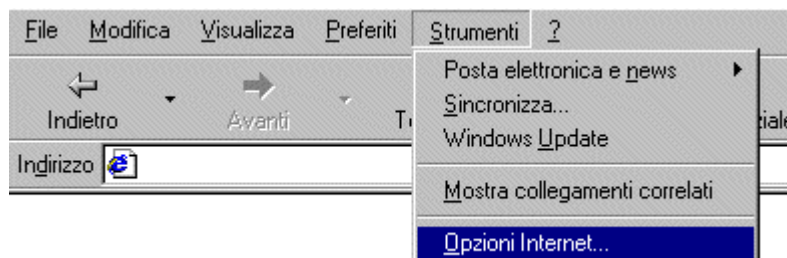
4.3 RISOLUZIONE PROBLEMI DI RICONOSCIMENTO DELLA CA

Quando viene installato il certificato digitale, automaticamente il browser dovrebbe contemporaneamente acquisire il certificato digitale della CA (Autorità di certificazione) che l'ha emesso.

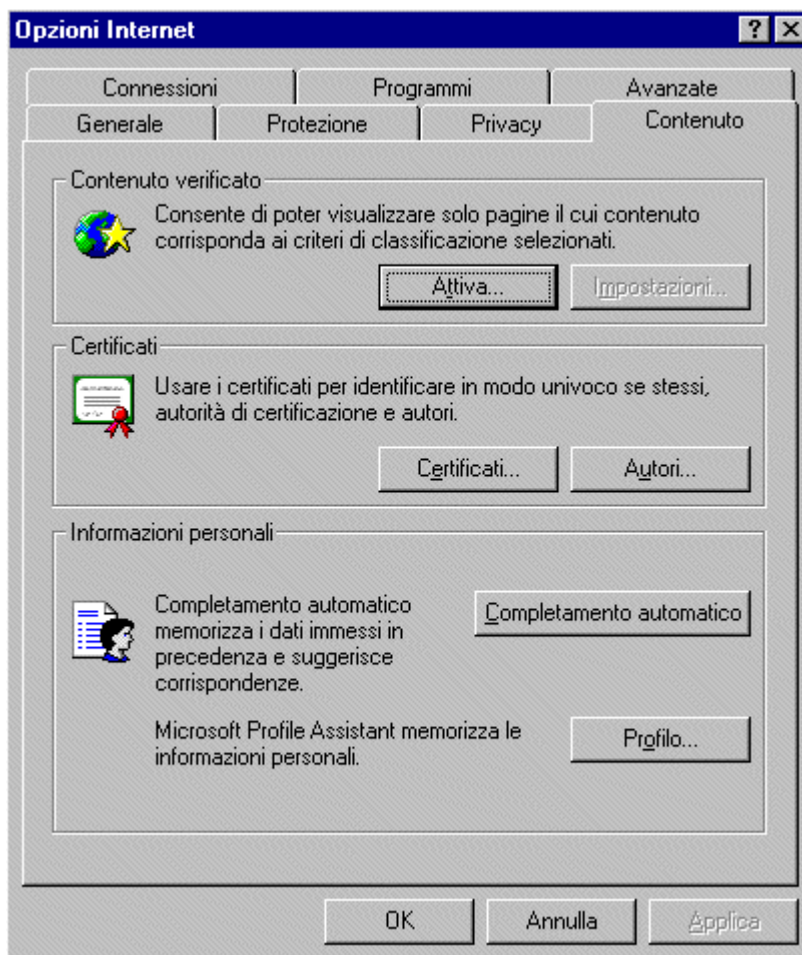
In alcune versioni di Microsoft Internet Explorer 6.0 (e Outlook Express 6.0), questo non accade e quindi, mancando il certificato digitale della CA, il certificato installato non viene riconosciuto come attendibile. Lo stato del proprio certificato digitale può essere visualizzato seguendo i passi descritti:

1.1 Lanciare Internet Explorer

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

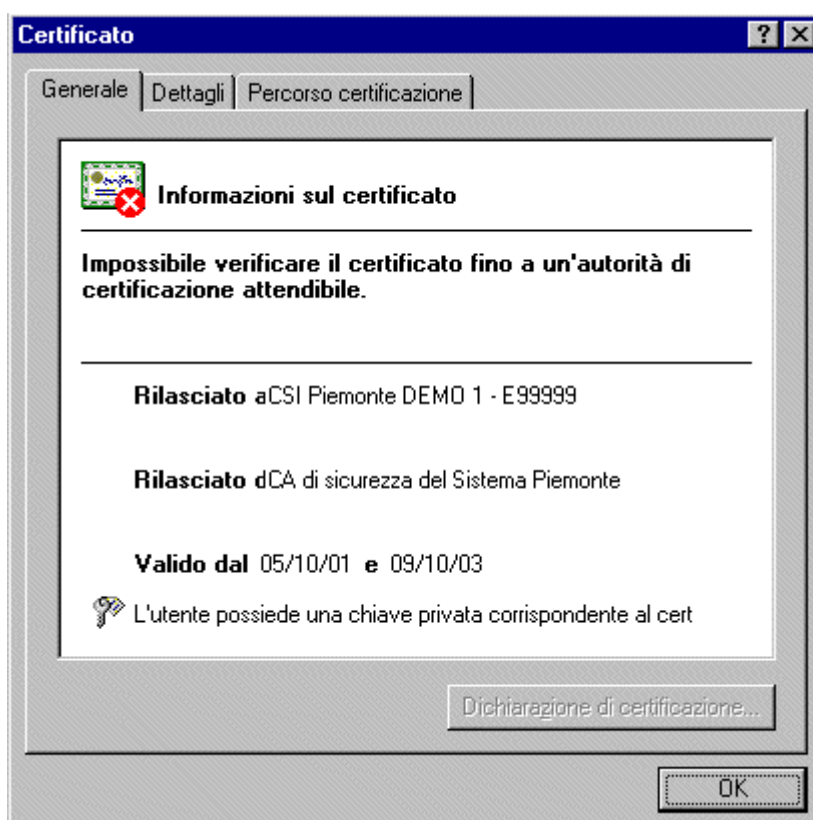


1.3 Appare una nuova finestra. Cliccare sulla voce "**Contenuto**" e quindi sul pulsante "**Certificati**".



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.



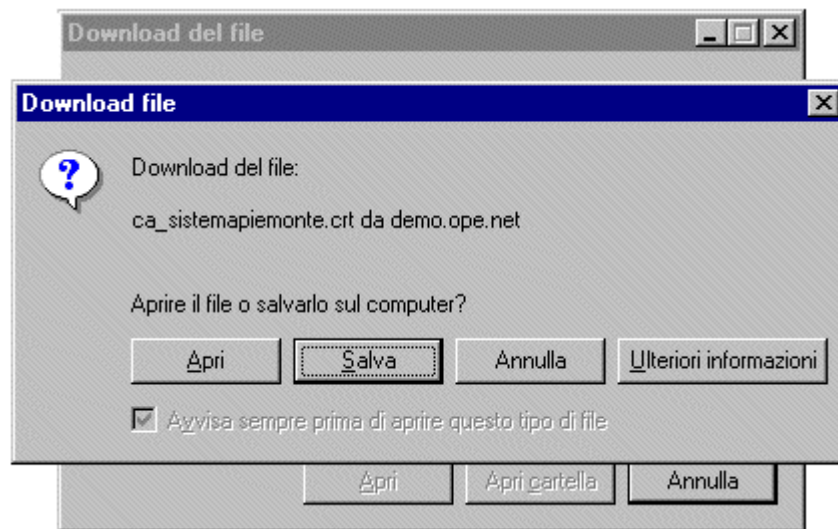
La figura mostra il certificato con un asterisco rosso e l'indicazione che il certificato non può essere verificato. Questo significa che manca il certificato digitale della CA. Per risolvere questo problema è possibile seguire due strade alternative.

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.

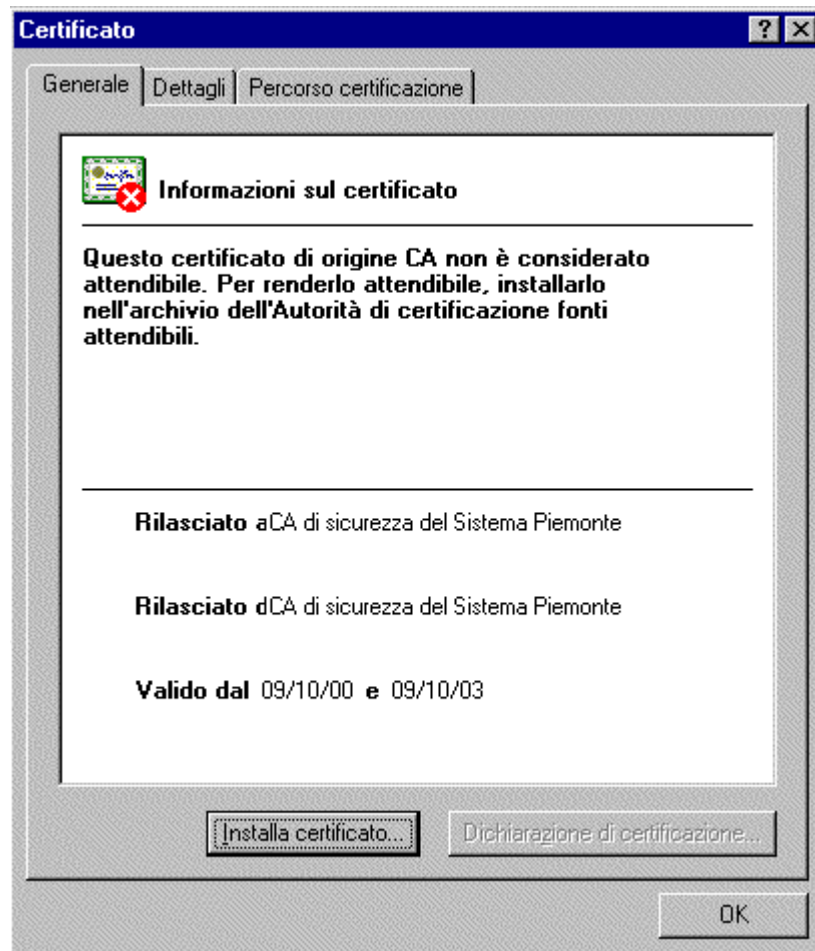
Modalità 1

Per installare il certificato della CA procedere come segue:

- 1.1 Scaricare il [certificato della CA](#) e aprirlo cliccando sul pulsante "apri".

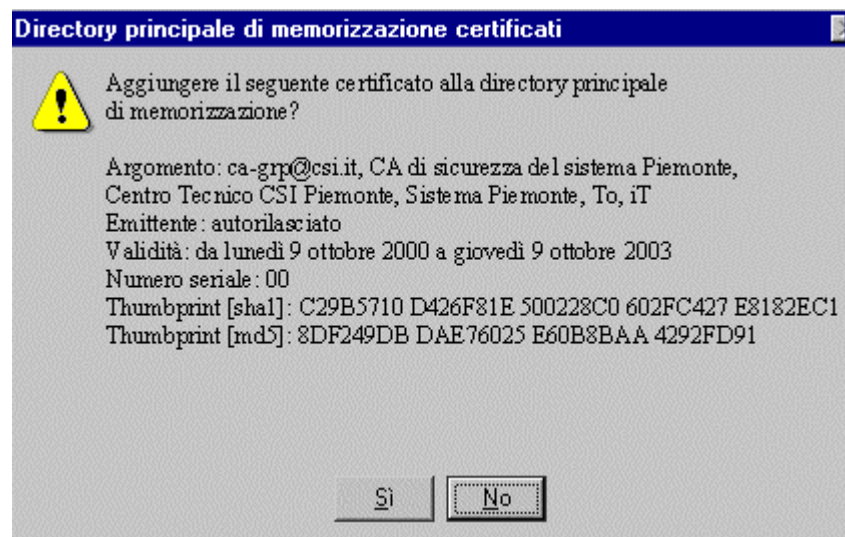


- 1.2 Cliccare sul pulsante "**Installa certificato**"



1.3 Quindi cliccare in successione 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.



Ora il certificato è stato installato.

Per vedere se ora il proprio certificato digitale viene riconosciuto correttamente rieseguire la procedura indicata al par. 4.2.

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

Ora il certificato è stato disinstallato.

A questo punto si procede 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.

5. NOTE SULLA GESTIONE DEI CERTIFICATI

Nel caso 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.

6. INFORMAZIONI GENERALI SUL CERTIFICATO DIGITALE

Un **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 fiducia che si può attribuire a tale determinazione dipende dalla fiducia che si ha della CA. 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.

E' stato definito uno standard a livello internazionale, chiamato X.509, per il formato di un certificato. Un certificato (secondo tale standard) è un insieme di informazioni binarie suddivise in campi.

Un certificato contiene sostanzialmente i seguenti dati:

- la Certification Authority che lo ha emesso
- il nome del soggetto a cui il certificato si riferisce
- la chiave pubblica del soggetto
- il periodo di tempo in cui il certificato può 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), possono utilizzare un canale sicuro (criptato) su cui scambiare le informazioni.