

**MANUALE DI INSTALLAZIONE
CERTIFICATO DIGITALE PER LA SICUREZZA
CERTIFICATION AUTHORITY DEL SISTEMA PIEMONTE**



INDICE

1. PREMESSE	3
2. VERIFICA DELLA VERSIONE CORRETTA DEL BROWER	3
3. INSTALLAZIONE DI CERTIFICATI CON NETSCAPE NAVIGATOR	3
3.1 IMPORT DEL CERTIFICATO	3
3.2 VERIFICA DEL CERTIFICATO.....	5
4. MICROSOFT INTERNET EXPLORER 7	6
4.1 IMPORT DEL CERTIFICATO	6
4.2 VERIFICA DEL CERTIFICATO.....	11
5. MOZILLA FIREFOX	12
5.1 IMPORT DEL CERTIFICATO	12
5.2 VERIFICA DEL CERTIFICATO.....	16
6. MICROSOFT INTERNET EXPLORER 5 , 5.5 E 6.0.....	16
6.1 IMPORT DEL CERTIFICATO	16
6.2 VERIFICA DEL CERTIFICATO.....	21
7. TEST DI FUNZIONAMENTO.....	22

1. PREMESSE

Questo documento fornisce le istruzioni necessarie all'installazione ed utilizzo dei certificati per autenticazione, rilasciati dalla Certification Authority del Sistema Piemonte, all'interno dei browser più comunemente usati, Netscape Communicator e Microsoft Internet Explorer.

2. VERIFICA DELLA VERSIONE CORRETTA DEL BROWSER

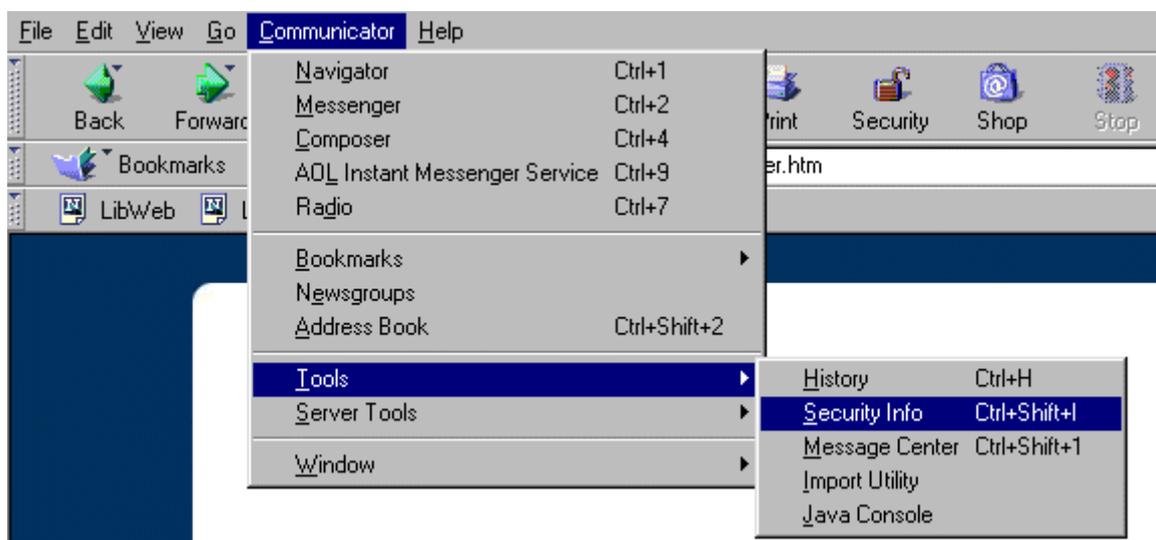
Per garantire un livello di sicurezza, autenticazione e riservatezza, adeguato alla tipologia di informazioni trasmesse nel contesto di questo servizio, i certificati digitali emessi dalla Certification Authority del Sistema Piemonte sono basati su chiavi asimmetriche di lunghezza minima di 1024 bit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

Grazie alla nuova normativa statunitense, in vigore da Gennaio 2000, relativa all'esportazione di tecnologia basata su cifratura forte è possibile oggi scaricare via rete browser con capacità di cifratura a 128 bit e l'utilizzo di certificati con chiavi a 1024 bit.

3. INSTALLAZIONE DI CERTIFICATI CON NETSCAPE NAVIGATOR

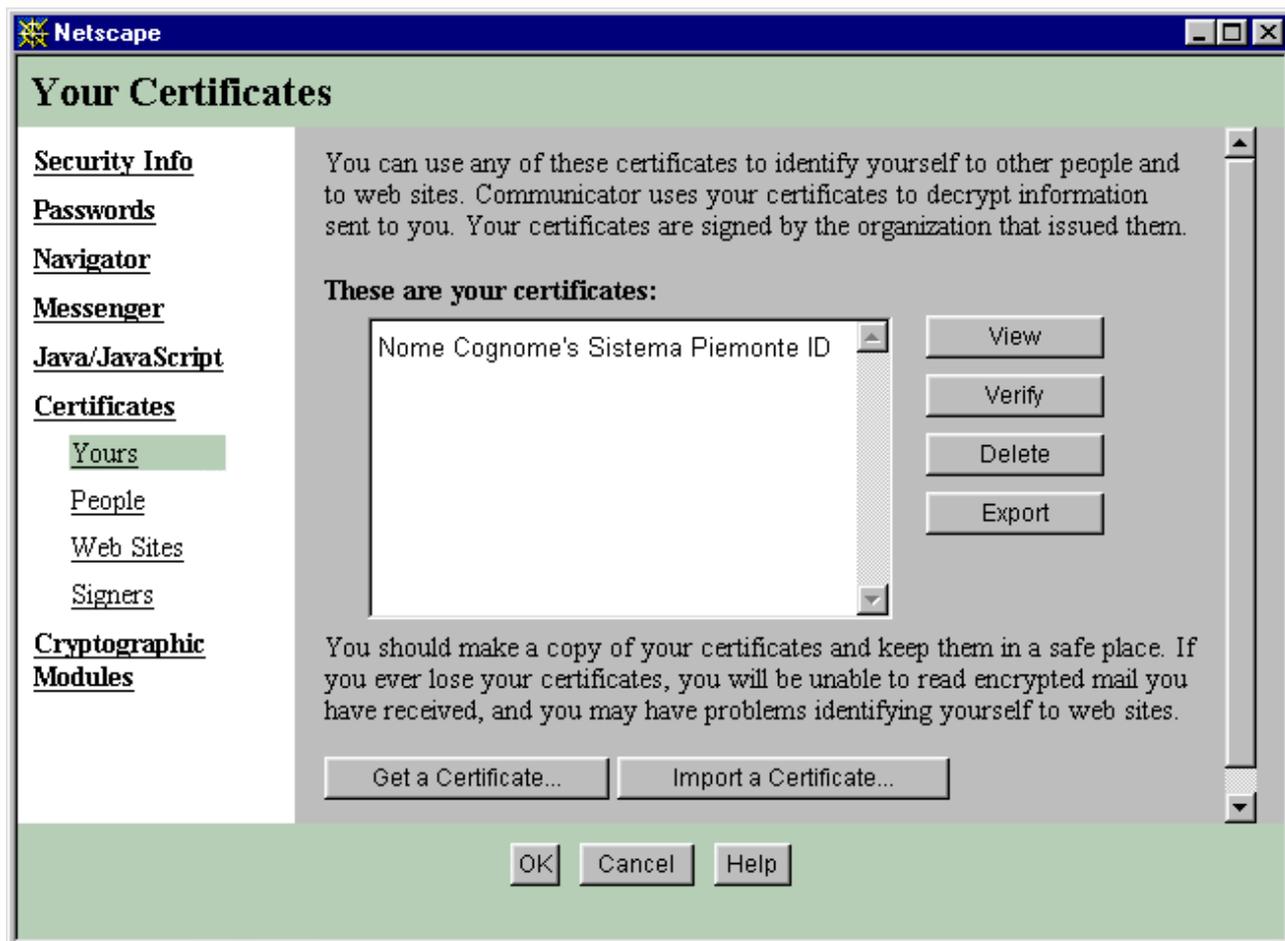
3.1 IMPORT DEL CERTIFICATO

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

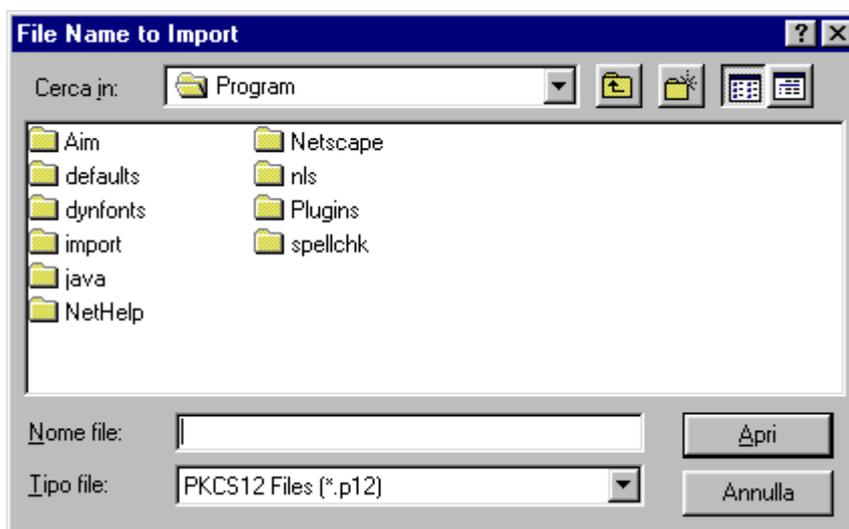


- Selezionare "**Personale**" ("**Yours**"), apparirà una finestra con una casella elenco per la visualizzazione dei certificati già presenti.
- Premere il pulsante "**Importa un certificato**" ("**Import a certificate**").

¹ E' noto che messaggi cifrati con chiavi DES a 56 bit sono stati decifrati in tempi molto brevi



- Se non avete mai indicato la password del repository dei certificati del vostro browser, vi viene richiesto di inserirne una.
- Inserire la password due volte, come richiesto dal programma, e confermare l'operazione.
- A questo punto compare la finestra di accesso ai file disponibili. Selezionare il certificato costituito dal file personale con estensione **.p12** precedentemente scaricato.
- Premere il pulsante "**Apri**" ("**Open**").



- 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.
- Successivamente viene richiesta la password con cui avete protetto il database dei certificati nel vostro browser. Se non avete mai indicato nessuna password potete inserirne una o cliccare direttamente su invio (nessuna password).
- Al termine 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. 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 premere il tasto "**Modifica**" ("Modify").
- Appare una finestra contenente le informazioni sul certificato e le checkbox per riconoscere la fiducia all'organismo di certificazione.
- Abilitare tutte le **voci di accettazione dell'organismo di certificazione** e confermare.

La seconda operazione consiste nel verificare il proprio certificato

- Posizionarsi sempre nella finestra "**Info sicurezza**" ("Security info"), sulla voce "**Certificati**" "Certificates" e scegliere la voce "Personali" ("Yours").
- Selezionare il proprio certificato.
- Premere il 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.
- Chiudere la finestra di "**Info sicurezza**" ("Security info).

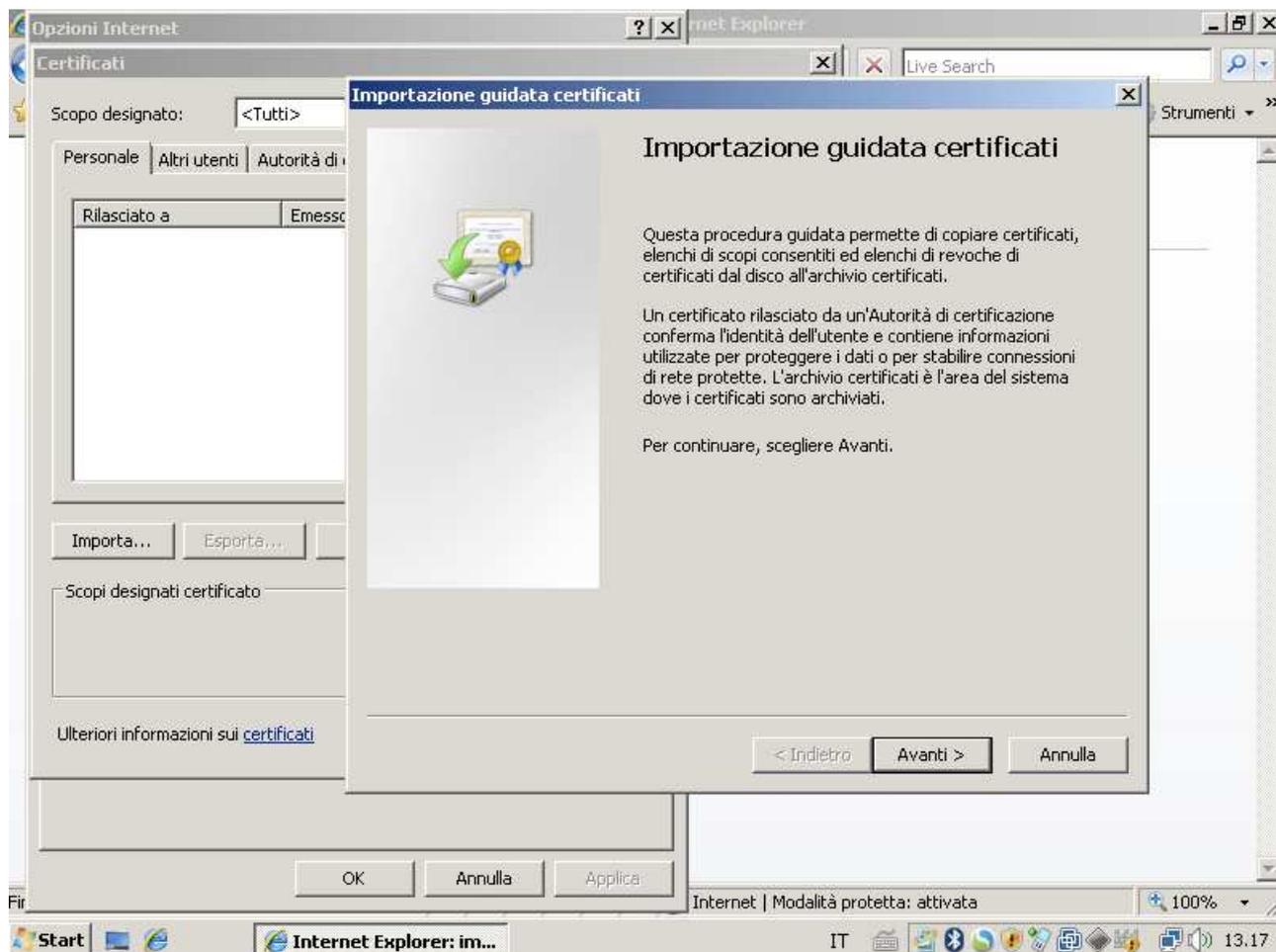
4. MICROSOFT INTERNET EXPLORER 7

In questo paragrafo si riportano i passi operativi per le versioni 7 in italiano e in inglese di Microsoft Internet Explorer installati sotto i Sistemi Operativi Windows 2000 e Windows XP/Vista mostrando le differenze caso per caso.

4.1 IMPORT DEL CERTIFICATO

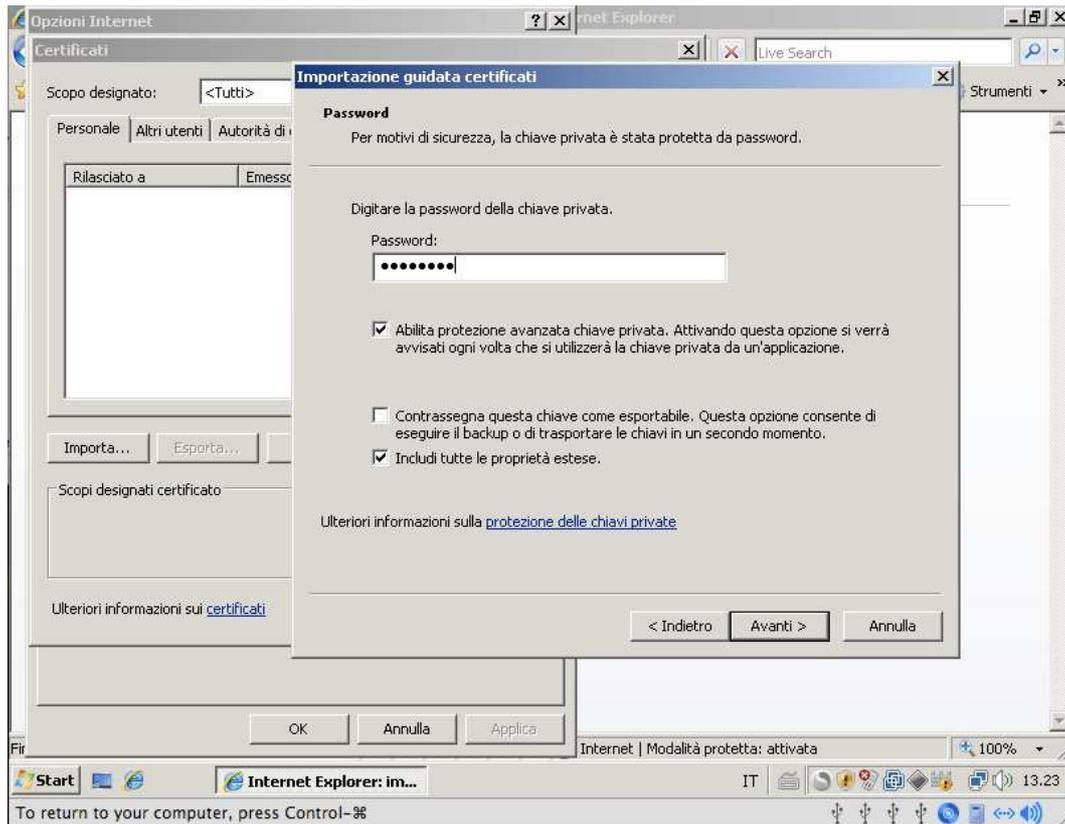
- Lanciare Internet Explorer
- Selezionare dalla barra degli strumenti il menu "**Strumenti**" ("**Tools**") e scegliere la voce "**Opzioni**" ("**Options**").
- Nella finestra apparsa cliccare sulla voce
- "**Contenuto**" ("**Content**") e quindi sul pulsante **Certificati** ("**Certificates**")



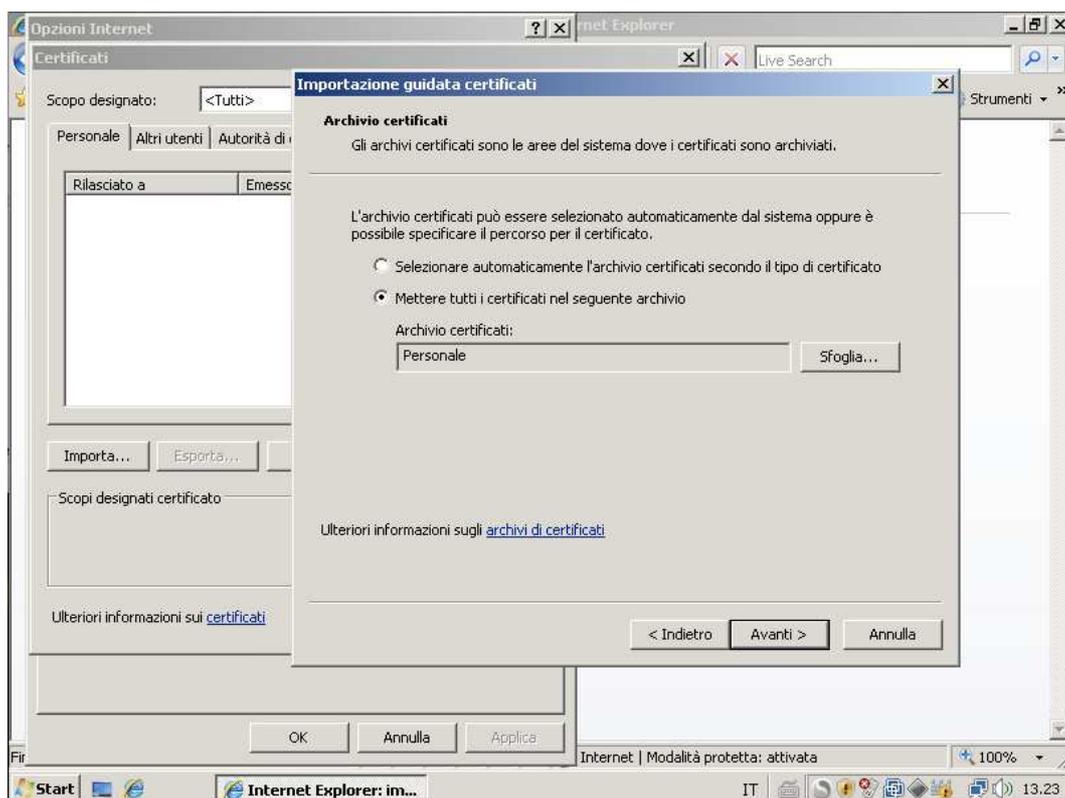


- Appare la finestra dei certificati. Premere il pulsante "**Importa**" ("**Import**") e seguire i seguenti passi.

- Nella nuova finestra apparsa cliccare su "**Avanti**" ("**Next**")
- Premere il tasto "**Sfoggia**" ("**Browse**").
- Selezionare come Tipo File:
*Sotto Windows XP/Vista - "**Tutti i file (*.*)**" ("**All Files (*.*)**").*
*Sotto Windows 2000 - "**File di scambio informazioni personali (*.pfx, *.p12)**" .*
- Ricercare e selezionare il file scaricato contenente il certificato. Deve avere estensione **.p12**.
- Cliccare su "**Apri**" ("**Next**")
- Cliccare su "**Avanti**" ("**Next**")
- Comparirà una finestra dove viene richiesto di inserire la password (che chiameremo PIN) con cui è stato protetto il vostro certificato. Il PIN è costituito dall'unione della password scelta durante la fase di richiesta della carta e del CIP (Codice di Identificazione Personale).
*Esempio: l'utente al momento della richiesta ha scelto la password **abcdefgh** e il CIP stampato sulla carta è **5678X234**. Il PIN che protegge il file sarà **abcdefgh5678X234**.*



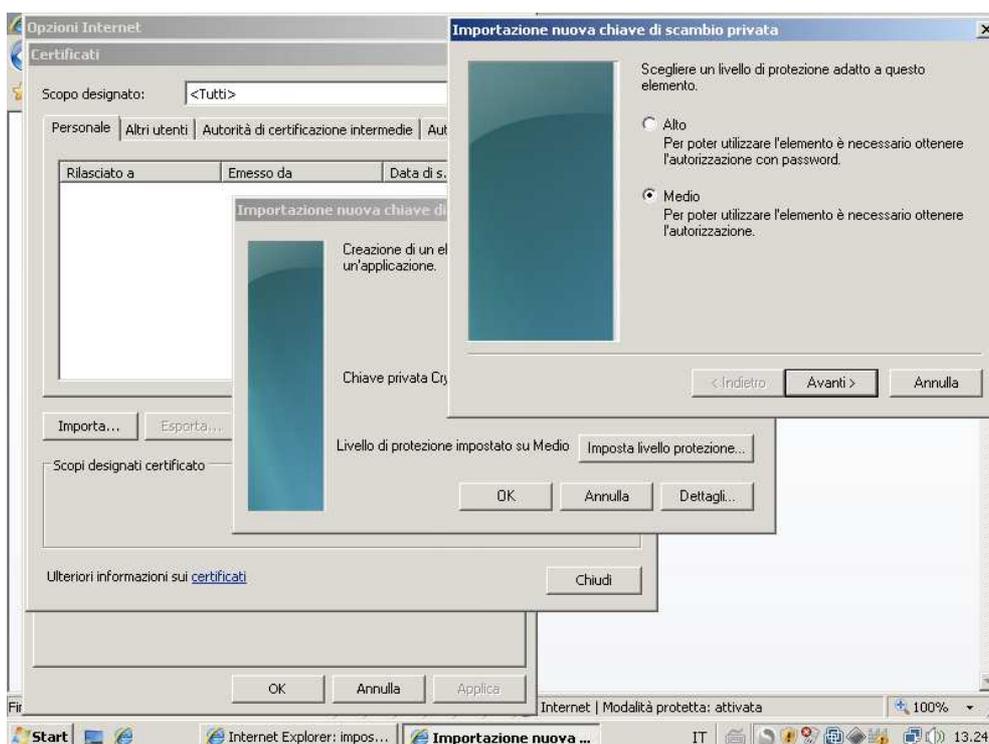
- Se si vuole proteggere l'uso del certificato all'interno del proprio browser con una password, occorre cliccare sulla checkbox "Abilita protezione avanzata chiave privata...."
- Cliccare su "Avanti"
- Compare una nuova finestra. Lasciare selezionato "Selezionare automaticamente l'archivio certificati secondo il tipo di certificato" ("Automatically select the certificate store").



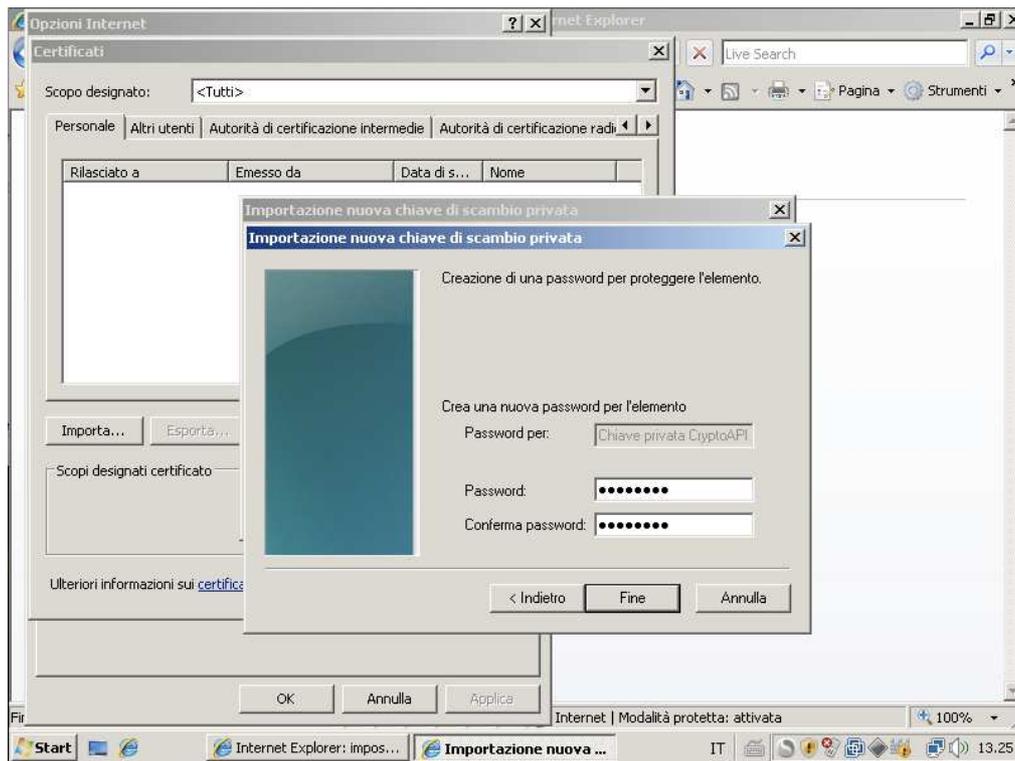
- Cliccare su "**Avanti**".
- Cliccare su "**Fine**".

Se si è selezionata l'opzione "Abilita protezione avanzata chiave privata..." allora la procedura di importazione richiede di indicare la password di protezione con questi passi:

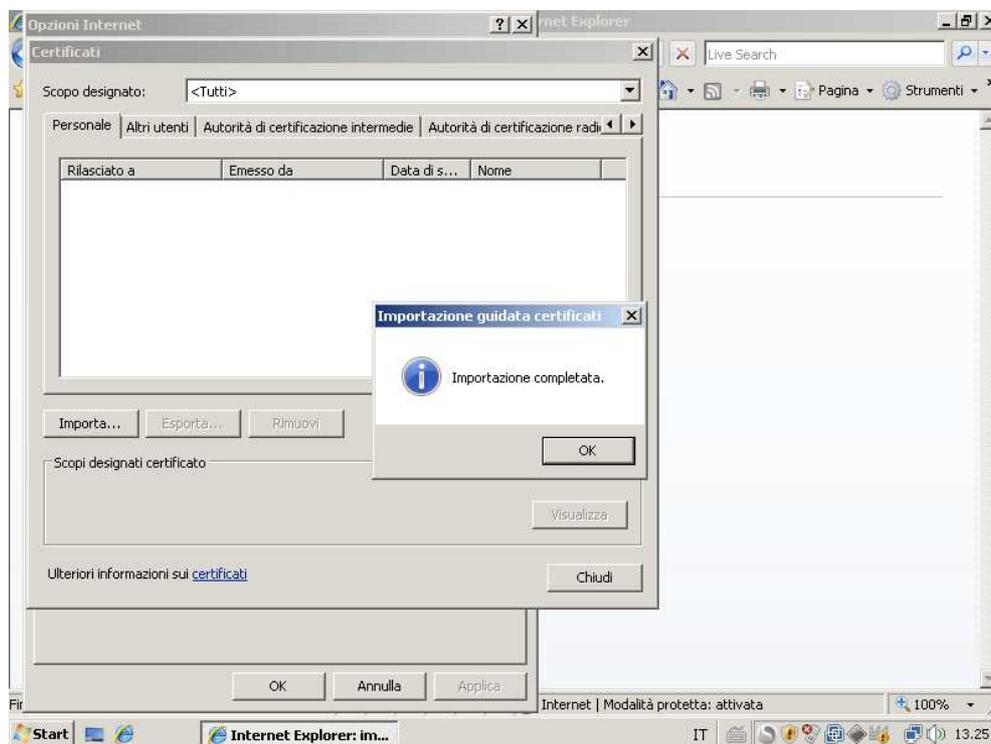
- Compare una nuova finestra nella quale occorre cliccare su "**Imposta livello protezione**" (se si clicca su ok la procedura termina ed installa il certificato senza password di protezione).

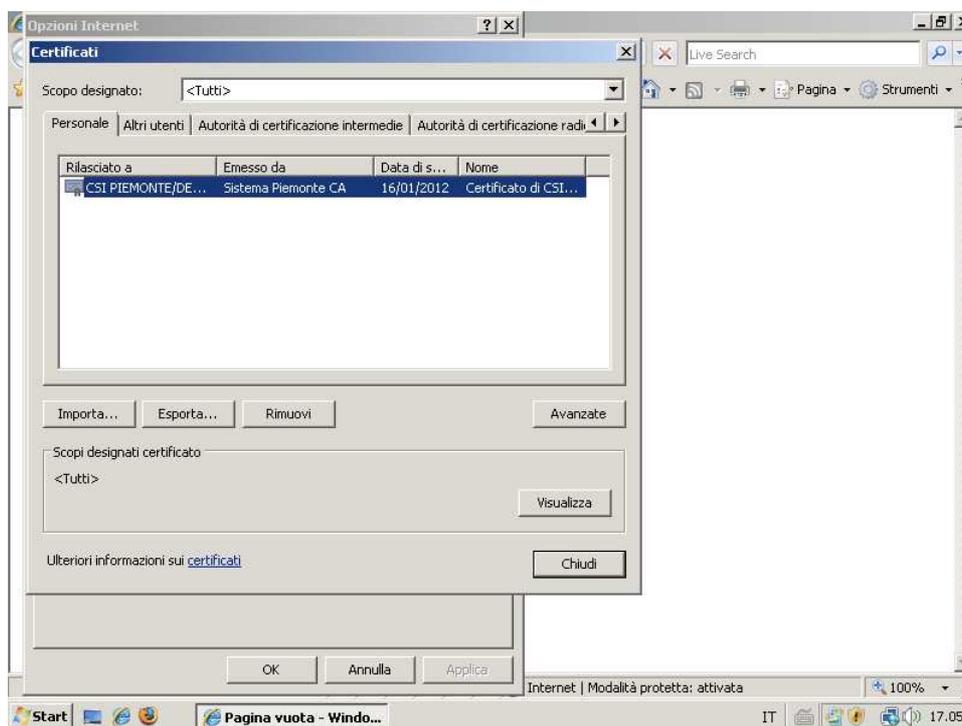


- Quindi selezionare il livello di protezione **Alto**
- Nella finestra successiva viene richiesto di indicare il nome dell'utente, la password e la conferma della password. Quindi cliccare su "**fine**".
Il nome dell'utente serve solo per la creazione di un profilo riconoscibile dall'utente stesso nel caso in cui il pc ed il browser siano utilizzati da utenti diversi (può essere un nome qualunque).



Nella finestra dei certificati deve comparire il nuovo certificato appena inserito.



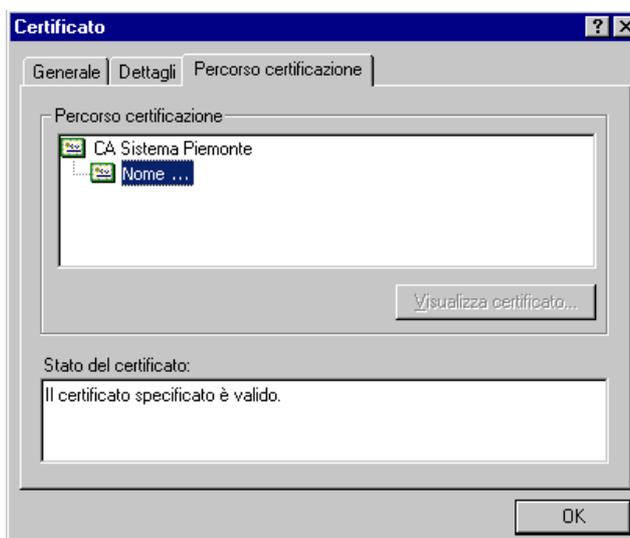


- Chiudere la finestra dei certificati con il tasto "**Chiudi**" ("**Close**").

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.

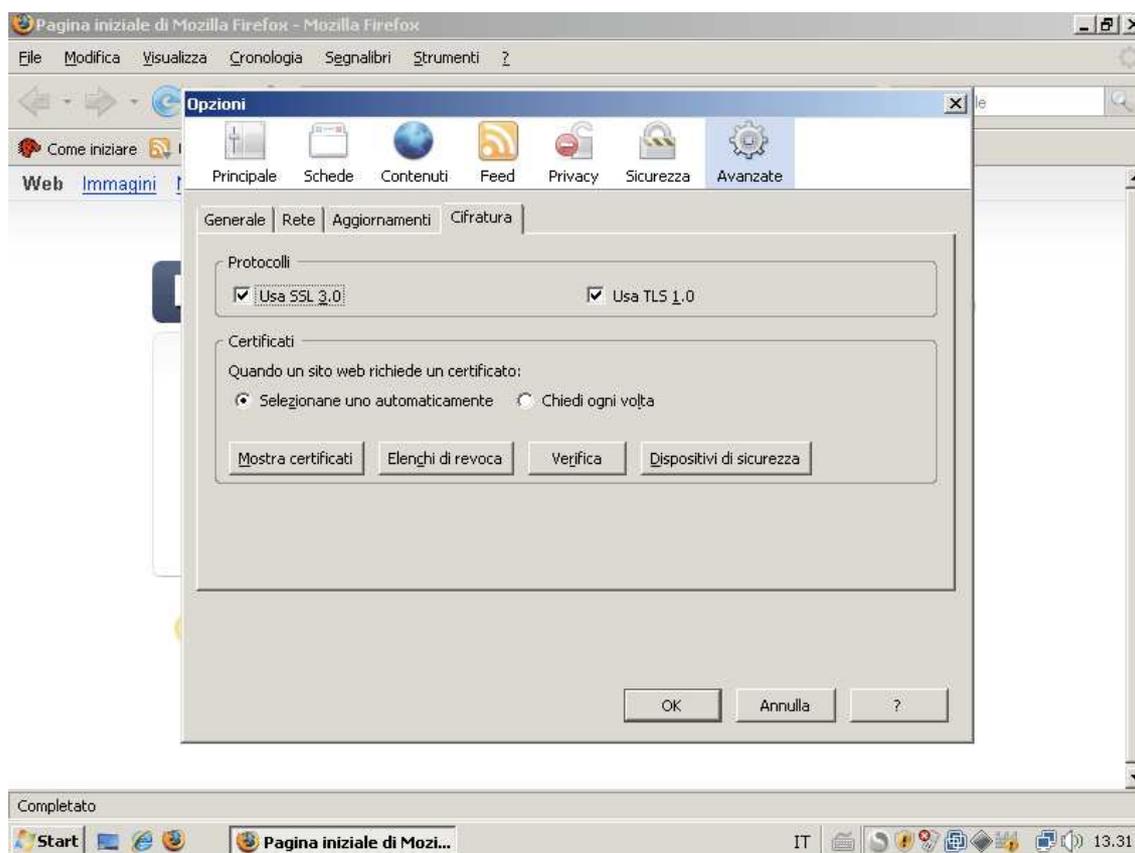


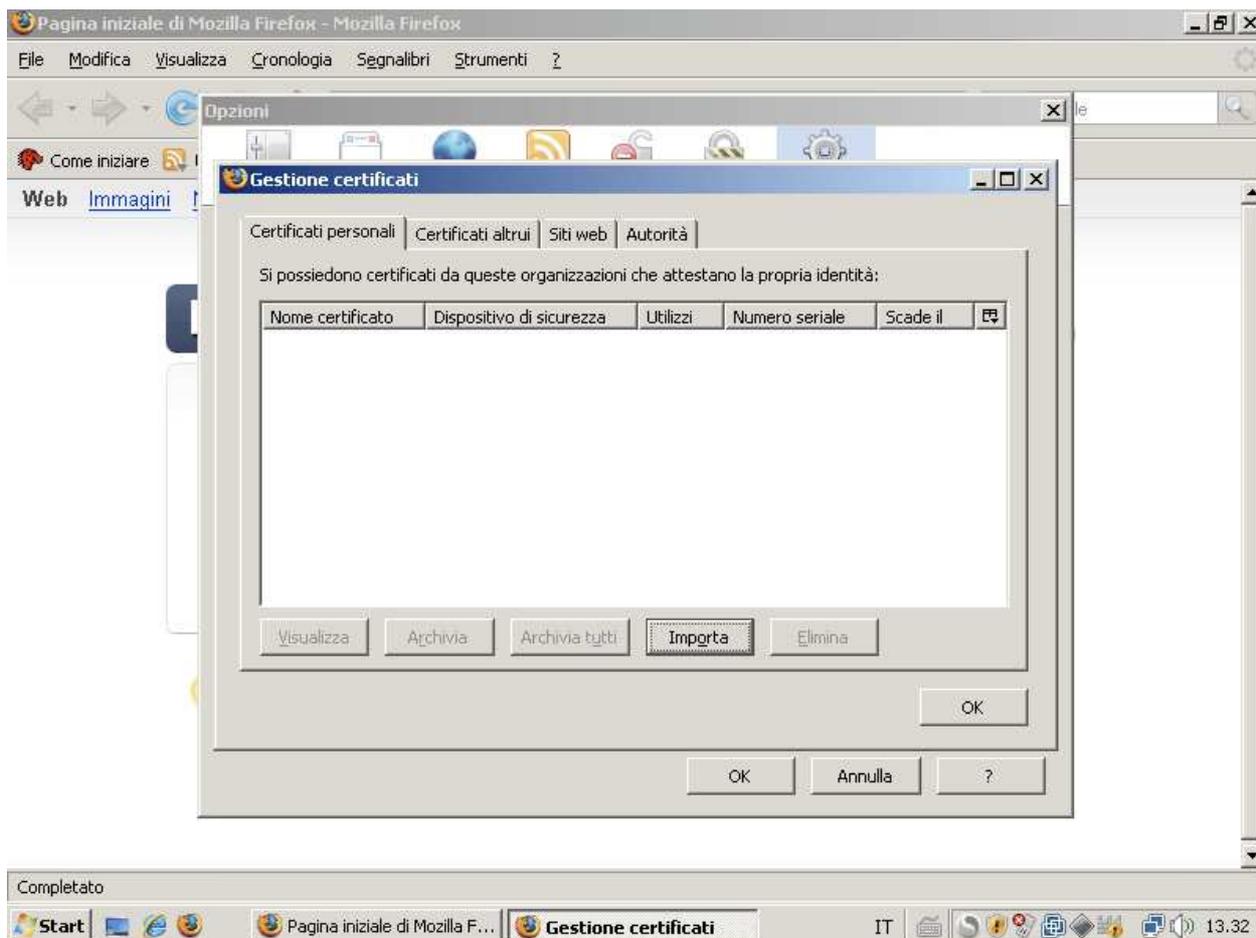
5. MOZILLA FIREFOX

In questo paragrafo si riportano i passi operativi per le versioni in italiano e in inglese di Mozilla Firefox installati sotto i Sistemi Operativi Windows 2000 e Windows XP/Vista mostrando le differenze caso per caso.

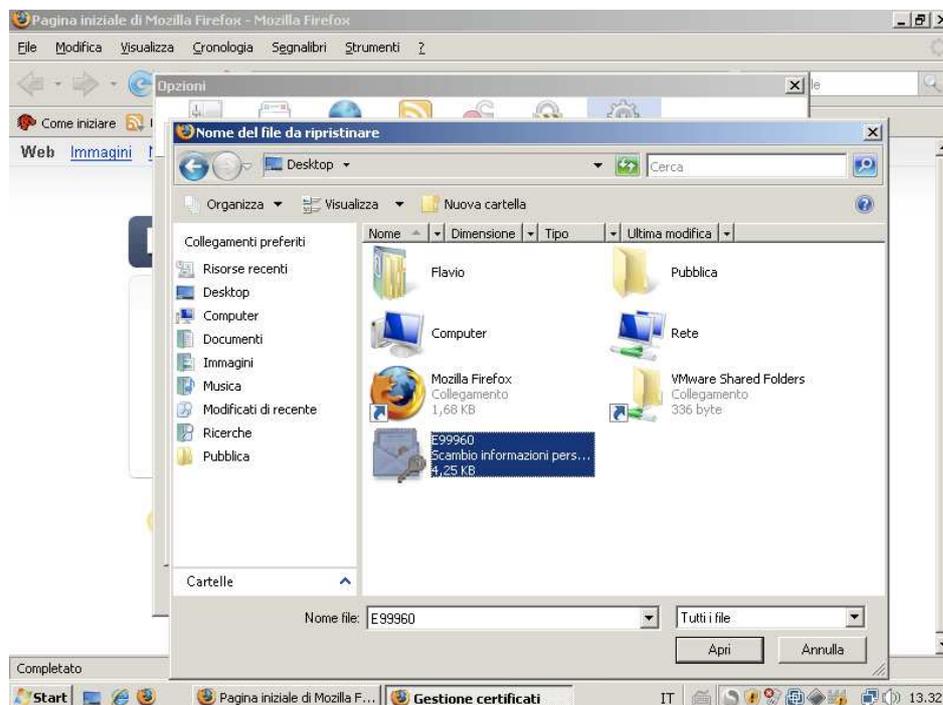
5.1 IMPORT DEL CERTIFICATO

- Lanciare Mozilla Firefox
- Selezionare dalla barra degli strumenti il menu "**Strumenti**" ("**Tools**") e scegliere la voce "**Opzioni**" ("**Options**").
- Nella finestra apparsa cliccare sulla voce "Avanzate"
- "**Mostra certificati**"



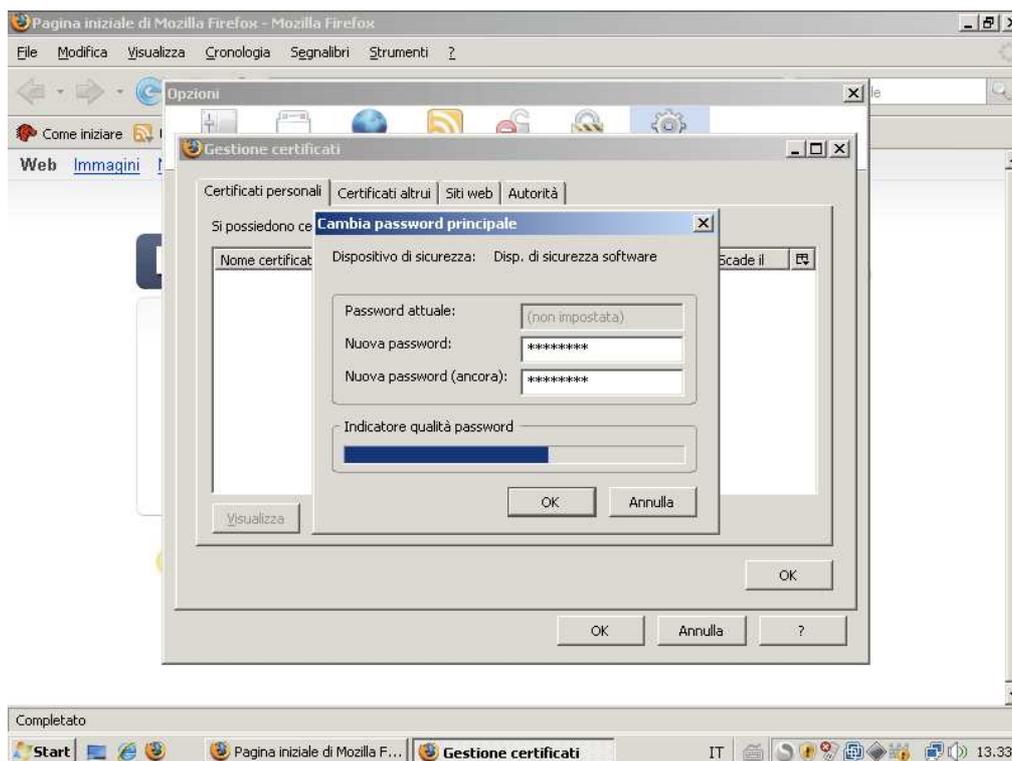


- Appare la finestra dei certificati. Premere il pulsante **"Importa"** ("**Import**") e seguire i seguenti passi.



- Premere il tasto **"Sfoggia"** ("**Browse**").

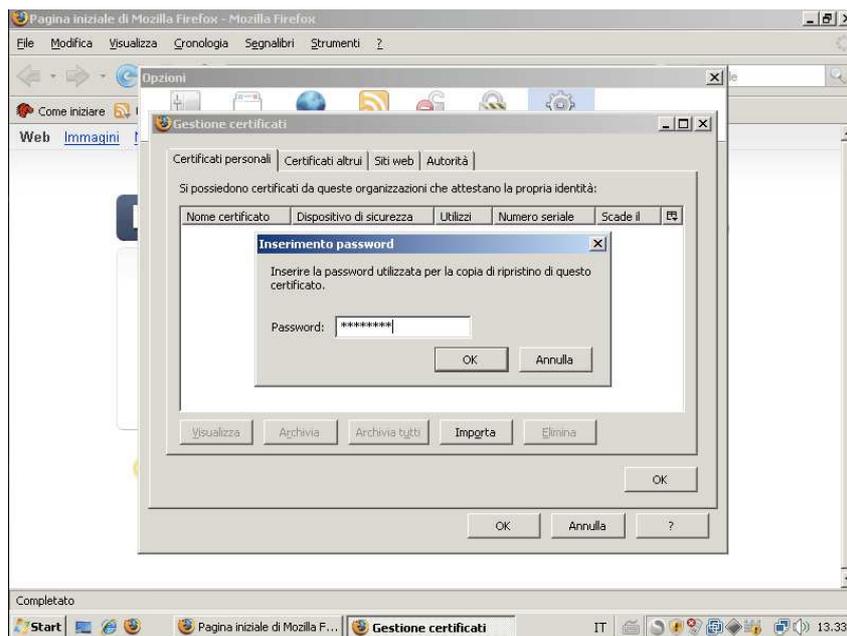
- Selezionare come Tipo File:
Sotto Windows 2000/XP/Vista - "Tutti i file (.*)" ("All Files (*.*)").*
- Ricercare e selezionare il file scaricato contenente il certificato. Deve avere estensione **.p12**.
- Cliccare su "Apri" ("Next")
- Comparirà una finestra dove viene richiesto di inserire la password (che chiameremo PIN) con cui è stato protetto il vostro certificato. Il PIN è costituito dall'unione della password scelta durante la fase di richiesta della carta e del CIP (Codice di Identificazione Personale).
*Esempio: l'utente al momento della richiesta ha scelto la password **abcdefgh** e il CIP stampato sulla carta è **5678X234**. Il PIN che protegge il file sarà **abcdefgh5678X234**.*



- Cliccare su "OK".

Verrà richiesto di inserire la password di ripristino per il certificato importato.

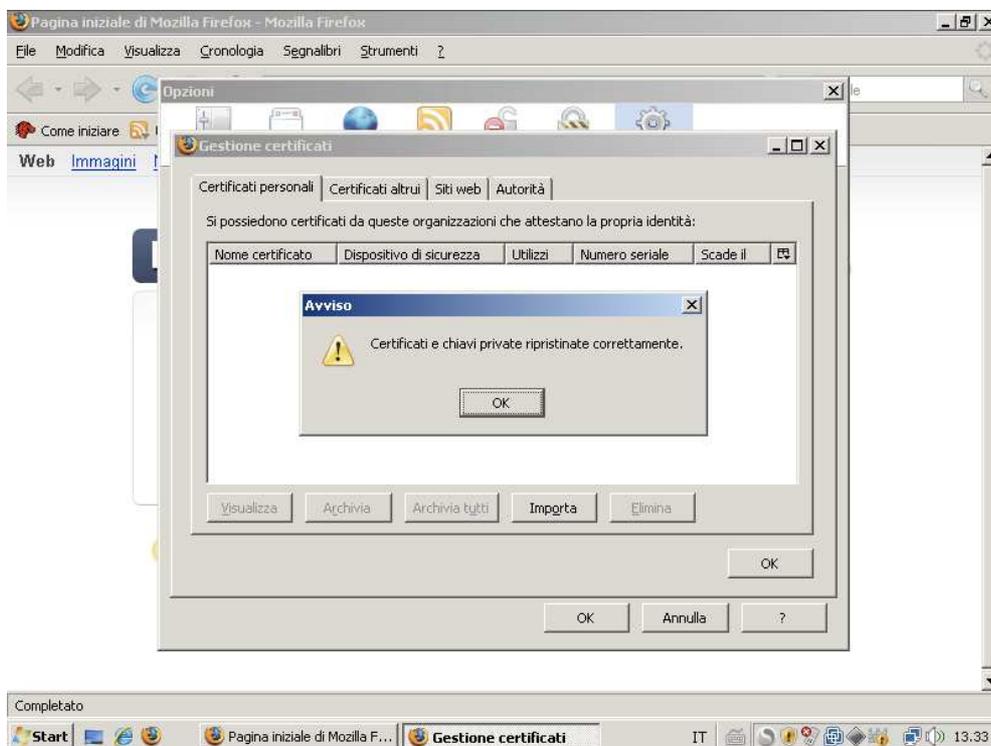
La password è a scelta dell'utente e può coincidere con quella del certificato indicate precedentemente.



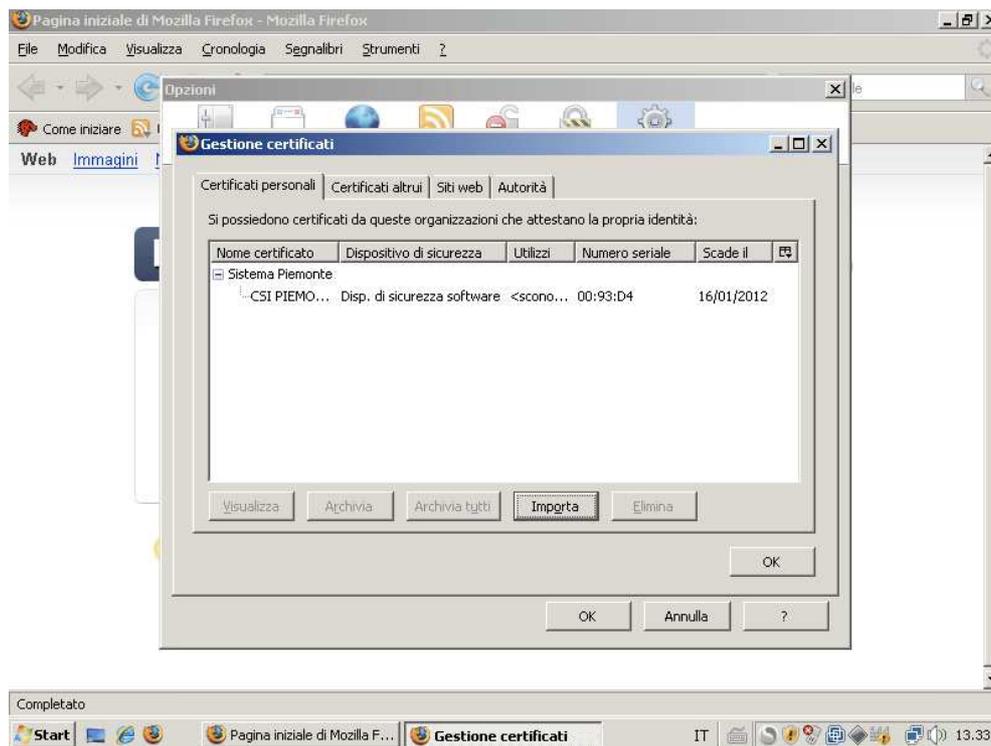
- Cliccare su "OK".

Il passo successivo verrà segnalata la corretta importazione del certificato.

- Cliccare su "OK".



Nella finestra dei certificati deve comparire il nuovo certificato appena inserito.



- Cliccare su "OK".

5.2 VERIFICA DEL CERTIFICATO

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

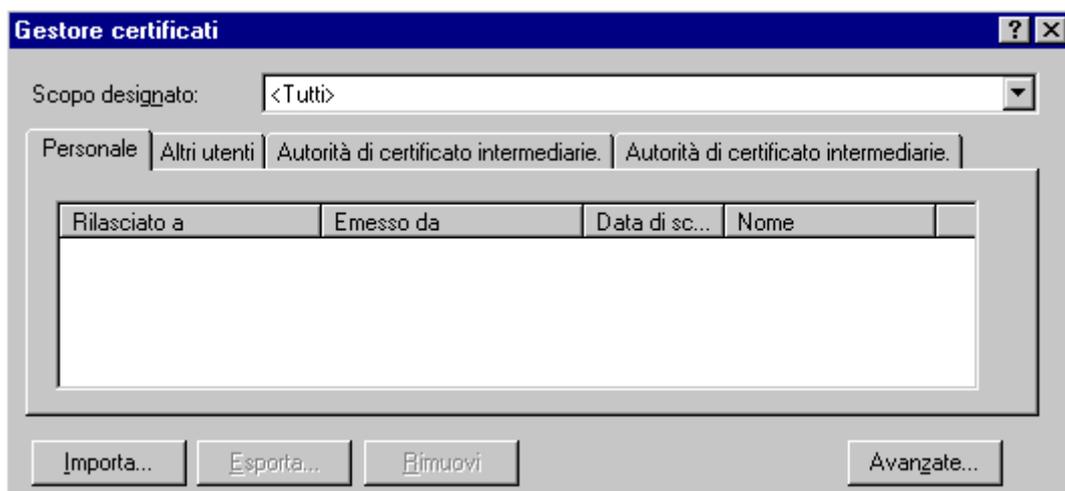
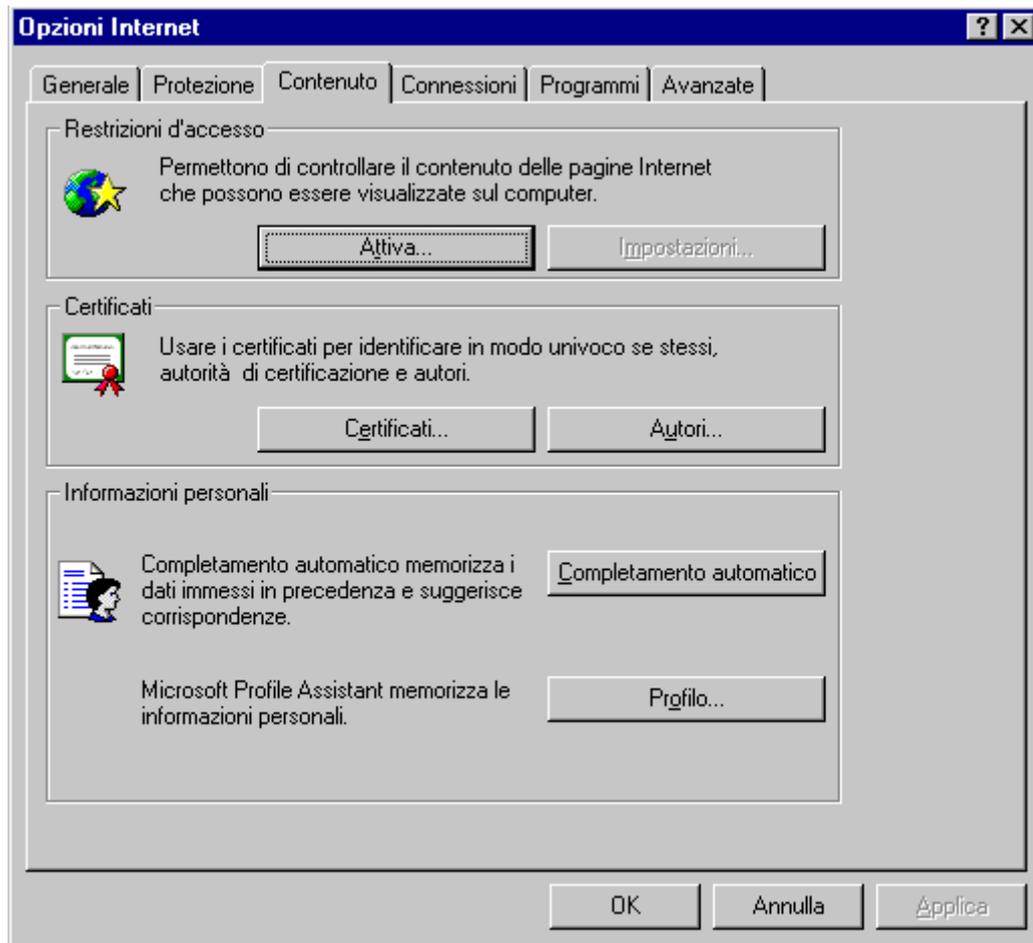
- Nella finestra "**Mostra Certificati**" ora dovrebbe apparire il vostro certificato; nella stessa potrete verificare il percorso di certificazione.
- Nel caso in cui l'indicazione non fosse tale, il certificato potrebbe non essere valido o potrebbe non essere stato installato il certificato dell' Autorità di Certificazione di Sistema Piemonte.

6. MICROSOFT INTERNET EXPLORER 5 , 5.5 E 6.0

In questo paragrafo si riportano i passi operativi per le versioni 5, 5.5 e 6.0 in italiano e in inglese di Microsoft Internet Explorer installati sotto i Sistemi Operativi Windows NT e Windows 2000 mostrando le differenze caso per caso.

6.1 IMPORT DEL CERTIFICATO

- Lanciare Internet Explorer
- Selezionare dalla barra degli strumenti il menu "**Strumenti**" ("**Tools**") e scegliere la voce "**Opzioni**" ("**Options**").
- Nella finestra apparsa cliccare sulla voce
- "**Contenuto**" ("**Content**") e quindi sul pulsante **Certificati** ("**Certificates**")

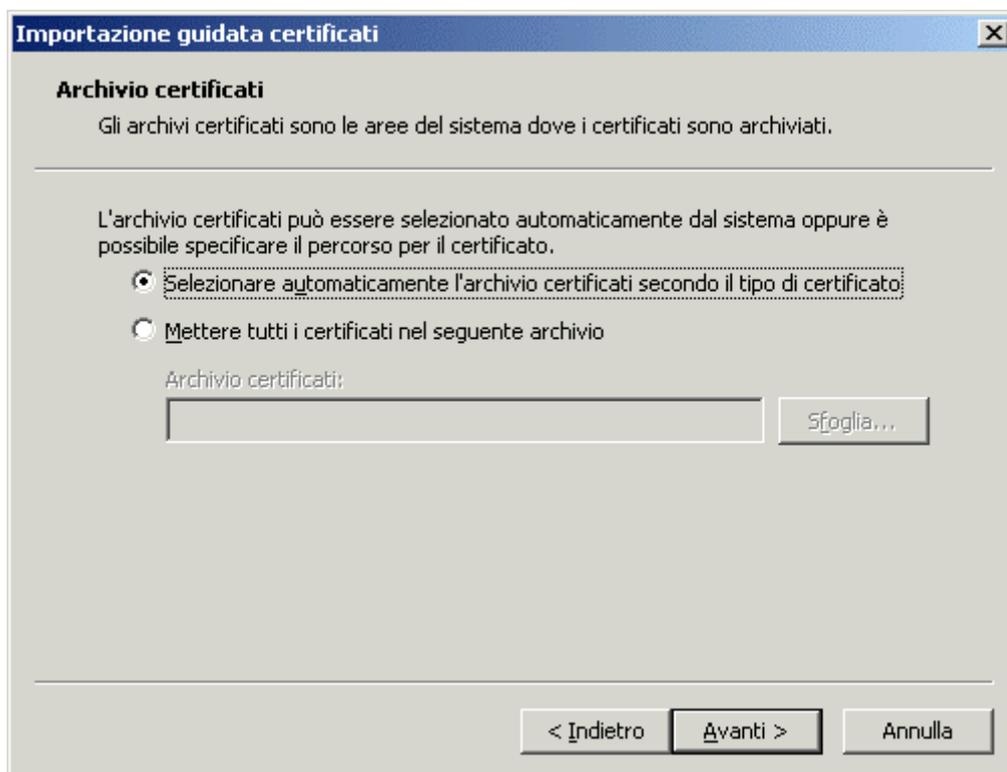


- Appare la finestra dei certificati. Premere il pulsante "**Importa**" ("**Import**") e seguire i seguenti passi.



- Nella nuova finestra apparsa 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)".*
- Ricercare e selezionare il file scaricato contenente il certificato. Deve avere estensione **.p12**.
- Cliccare su "Apri" ("Next")
- Cliccare su "Avanti" ("Next")
- Comparirà una finestra dove viene richiesto di inserire la password (che chiameremo PIN) con cui è stato protetto il vostro certificato. Il PIN è costituito dall'unione della password scelta durante la fase di richiesta della carta e del CIP (Codice di Identificazione Personale).
*Esempio: l'utente al momento della richiesta ha scelto la password **abcdefgh** e il CIP stampato sulla carta è **5678X234**. Il PIN che protegge il file sarà **abcdefgh5678X234**.*

- Se si vuole proteggere l'uso del certificato all'interno del proprio browser con una password, occorre cliccare sulla checkbox "Abilita protezione avanzata chiave privata..."
- Cliccare su "**Avanti**"
- Compare una nuova finestra. Lasciare selezionato "**Selezionare automaticamente l'archivio certificati secondo il tipo di certificato**" ("**Automatically select the certificate store**").



- Cliccare su "**Avanti**".

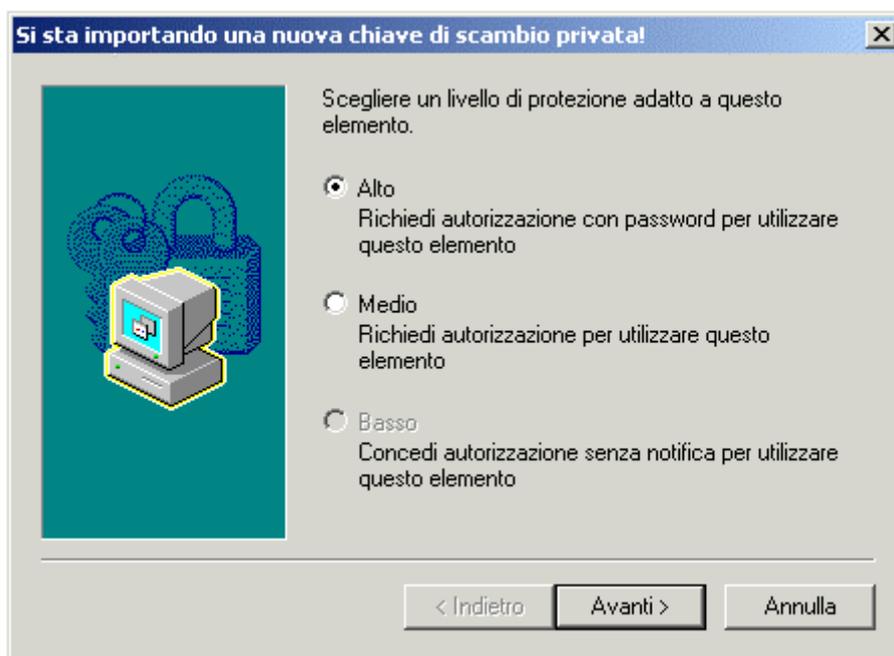
- Cliccare su "**Fine**".

Se si è selezionata l'opzione "Abilita protezione avanzata chiave privata..." allora la procedura di importazione richiede di indicare la password di protezione con questi passi:

- Compare una nuova finestra nella quale occorre cliccare su "**Imposta livello protezione**" (se si clicca su ok la procedura termina ed installa il certificato senza password di protezione).



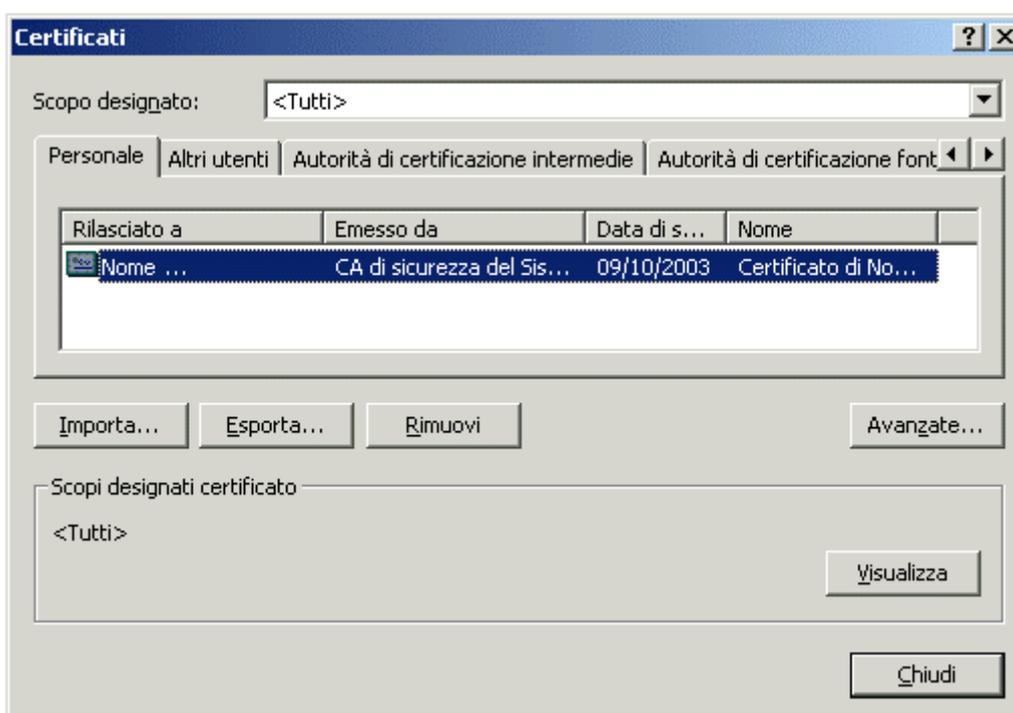
- Quindi selezionare il livello di protezione **Alto**



- Nella finestra successiva viene richiesto di indicare il nome dell'utente, la password e la conferma della password. Quindi cliccare su "**fine**".
Il nome dell'utente serve solo per la creazione di un profilo riconoscibile dall'utente stesso nel caso in cui il pc ed il browser siano utilizzati da utenti diversi (può essere un nome qualunque).



Nella finestra dei certificati deve comparire il nuovo certificato appena inserito.



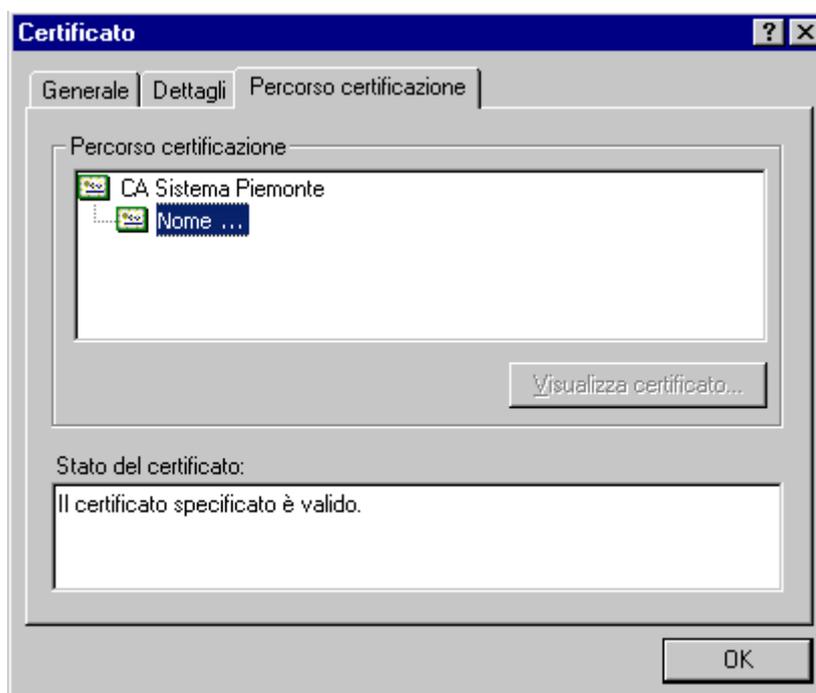
- Chiudere la finestra dei certificati con il tasto "**Chiudi**" ("Close").

6.2 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.



7. TEST DI FUNZIONAMENTO

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.

Collegandosi all'indirizzo <https://webgate.sistemapiemonte.it> e cliccando su **“visualizza il certificato di autenticazione digitale”** vengono visualizzati i dati contenuti nel certificato che avrete selezionato nella finestra di richiesta di autenticazione.

Se la procedura web visualizza i vostri dati, il vostro posto di lavoro è ora pronto per accedere al servizio applicativo al quale siete stati abilitati.