APPLICAZIONE FIRMA E VERIFICA

MANUALE UTENTE
AMBIENTE WIN

INDICE

1 Scopo del documento

Il presente documento è una guida per l'installazione e l'utilizzo dell'applicazione prodotto **Firma e Verifica**, da utilizzare per predisporre il file da trasmettere, costituito dai dati utente e dal codice di autenticazione e per verificare le risposte restituite dall'Amministrazione finanziaria.

1.1 Definizioni

CA	Sigla utilizzata per identificare la Certification Authority
Certification Authority	Server dell'Amministrazione che genera e custodisce i certificati utilizzati per il calcolo dei codici di autenticazione
Certificato	File che contiene la chiave pubblica del titolare
Codice di autenticazione	Sequenza di caratteri, estratta dal file cui si riferisce, crittografata con la chiave privata di colui che richiede l'operazione di firma
Common Name	Sezione del certificato che contiene i dati identificativi del titolare (codice fiscale, pogressivo sede, cognome e nome, ecc.)
Dispositivo di firma	Floppy che contiene la chiave pubblica e la chiave privata dell'utente.
Firma	Tecnicamente, coincide con il codice di autenticazione
Key store	File che contiene la chiave pubblica e la chiave privata dell'utente
Root CA	Certificato principale della CA

2 Introduzione

L'applicazione permette di:

- Firmare un file generico.
- Verificare la correttezza della firma; tale verifica consiste in:
  - Controllo di validità della firma (il codice di autenticazione è stato calcolato correttamente e il documento non è stato modificato successivamente);
  - Validità del certificato del firmatario;

In questa versione l'applicazione consente anche di firmare un file con il certificato rilasciato dall'Agenzia delle Entrate.

Al termine dell'operazione di verifica, il documento viene salvato nel formato originario, a disposizione delle successive elaborazioni da parte dell'utente.

Per le operazioni di firma e di verifica vengono utilizzati due "repository" che contengono:

- il key store dell'utente (file creato al termine dell'operazione di Genera Ambiente, con la chiave pubblica e la chiave privata dell'utente);
- il Gestore delle Autorità di Certificazione, dove viene conservata la chiave pubblica dell'Amministrazione finanziaria.

Entrambi i repository sono protetti da password:

- la prima viene prescelta dall'utente durante la fase di generazione;
- la seconda al momento dell'installazione dell'applicazione assume il valore di default "**123456**".

3 Installazione

Per installare l'applicazione occorre eseguire due programmi di Setup :

- **Setup JRE** per installare la Java Virtual Machine;
- **Setup base** per installare **Firma e Verifica**

Non è necessario ripetere l'installazione se il componente JRE è già presente sul vostro PC; provate ad eseguire le istruzioni partendo dal punto 2; se ricevete il messaggio di errore analogo a quello mostrato nella figura che segue:

riprendete dal punto 1; altrimenti proseguite, in quanto è stata rilevata automaticamente la presenza della Java Virtual Machine nella versione richiesta.

Per eseguire l'installazione occorre eseguire i seguenti passi:

1. Aprire **Risorse del computer** , selezionare l'unità CD ROM ed eseguire un doppio click con il tasto sinistro del mouse sul file **j2re1_3_0-win.exe** . Partirà l'installazione guidata del prodotto; confermare l'installazione sulle finestre successive, e al termine cliccare con il tasto sinistro del mouse sul bottone **Fine.**

2. Selezionare la voce **FirmaVerifica.exe** e cliccare due volte con il tasto sinistro del mouse.

3. Si apre una finestra di dialogo visibile in Figura –1; cliccare con il tasto sinistro del mouse sul bottone **Avanti.**

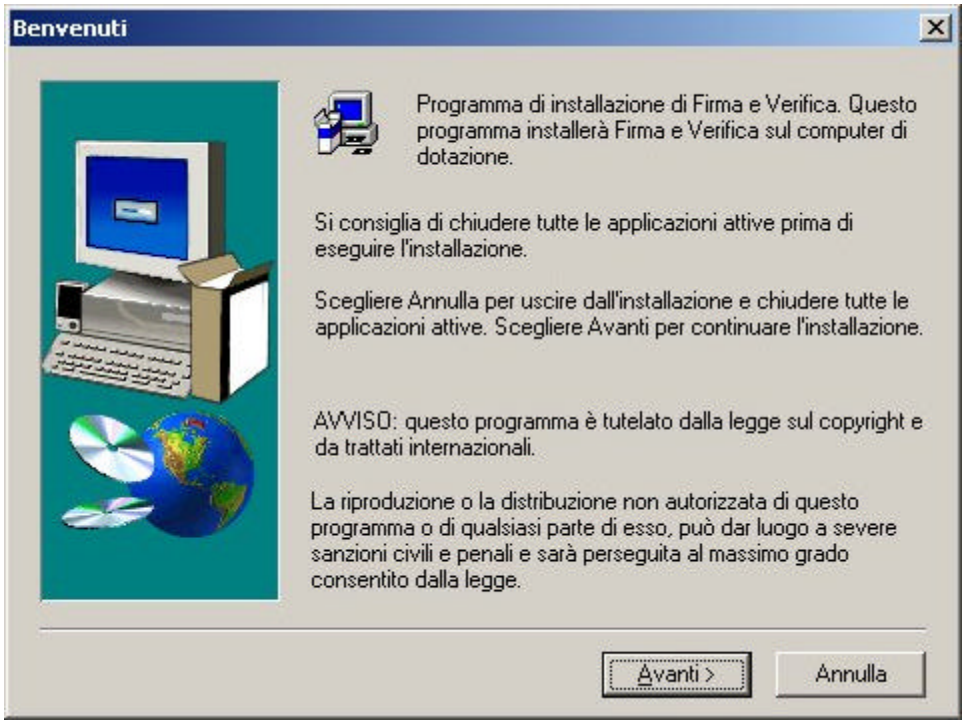


Figura – 1

3. Verrà visualizzata la finestra riportata in Figura-2, la quale propone come percorso di installazione la directory **C:\FirmaVerifica** che potrà comunque essere cambiata cliccando sul bottone **Sfoglia;** per continuare l'installazione premere il bottone **Avanti**.

Figura – 2

4. Inizierà la copia dei file ed al termine verrà visualizzata l'ultima finestra di dialogo (Figura –3). Per terminare l'installazione occorrerà cliccare con il tasto sinistro del mouse sul bottone **Fine**.

Figura – 3

Completata l'installazione verrà creata l'icona Firma e Verifica sul Desktop :

Figura – 4

e verrà aggiunta la voce **Firma e Verifica** nel menù Programmi.

4 Avvio dell'applicazione

Per avviare l'applicazione occorre eseguire un doppio click sull'icona predisposta sul Desktop **Firma e Verifica** (Figura-4) oppure cliccare con il tasto sinistro del mouse sul bottone **Start** o **Avvio** di Windows , selezionare la voce **Programmi** e cliccare con il tasto sinistro sulla voce **Firma e Verifica**.

Figura - 5

All'avvio dell'applicazione, sono disponibili tre finestre mostrate nella figura che segue:

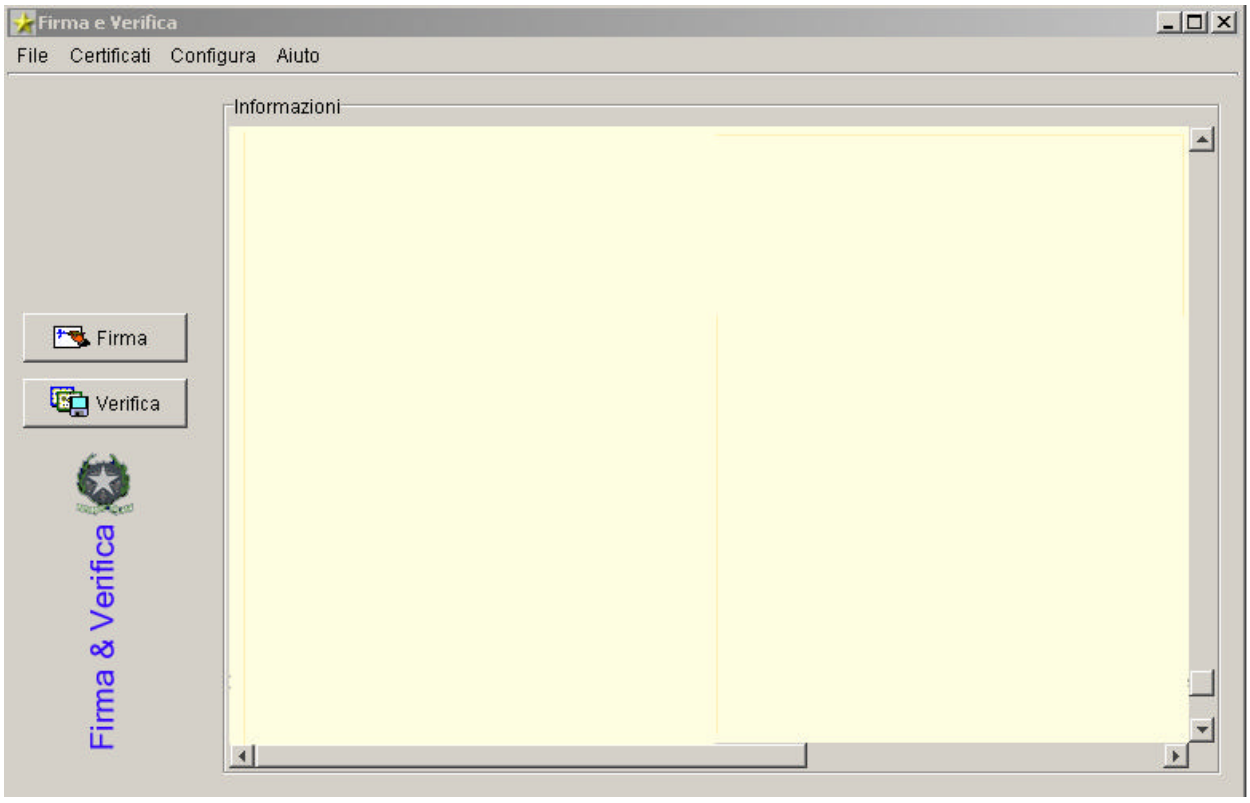


Figura – 6

L'area di testo "**Informazioni"**, non editabile, contiene tutti i messaggi relativi allo svolgimento delle varie operazioni effettuate e gli eventuali messaggi di errore. Le operazioni sono infatti storicizzate in un file che viene visualizzato all'avvio dell'applicazione; alla prima esecuzione, oppure quando il contenuto dell'area viene salvato in un file prescelto dall'utente (menu Aiuto-Archivia log), questa sezione "Informazioni" risulta vuota.

Dalla stessa finestra è possibile selezionare le principali funzioni:

- **Firma**: per calcolare il codice di autenticazione di un file;

- **Verifica**: per verificare la validità del codice di autenticazione.

Per eseguire le funzioni, occorre cliccare con il tasto sinistro del mouse sul bottone corrispondente.

Il menù (in alto sulla finestra) consente di accedere ad altre funzionalità.

Menu file :

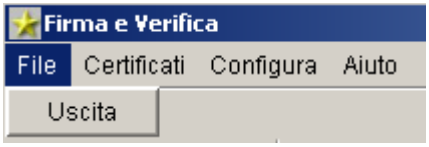


Figura – 7

Uscita permettere di chiudere l'applicazione.

Menu Certificati

Figura – 8

Gestore certificati utente permette di accedere alle funzionalità del Gestore dei certificati utente.

Gestore autorità di certificazione permette di accedere alle funzionalità del Gestore dei certificati relativi alla CA (Certification Autority).

Menu Configura

Configura permette di salvare il Repository di firma dell'utente (file keystore.ks creato al termine dell'operazione di Genera Ambiente) in una posizione del disco fisso a scelta dell' utente oppure lasciarlo sul floppy disk.

Figura – 8a

Menu Aiuto

Figura – 9

Aiuto in linea permette di visualizzare il contenuto del presente manuale utente in formato html.

Versione permette di visualizzare la versione dell'applicazione **Firma e Verifica** installata sul PC.

Archivia Log permette di archiviare il contenuto del log in un file prescelto dall'utente.

5 Firma

La funzione consente il calcolo del codice di autenticazione di un file e la predisposizione del file da trasmettere.

I passi che l'utente deve eseguire sono i seguenti:

1. Cliccare con il tasto sinistro del mouse sul bottone **Firma**. Viene visualizzato nella finestra principale il pannello mostrato nella figura che segue :

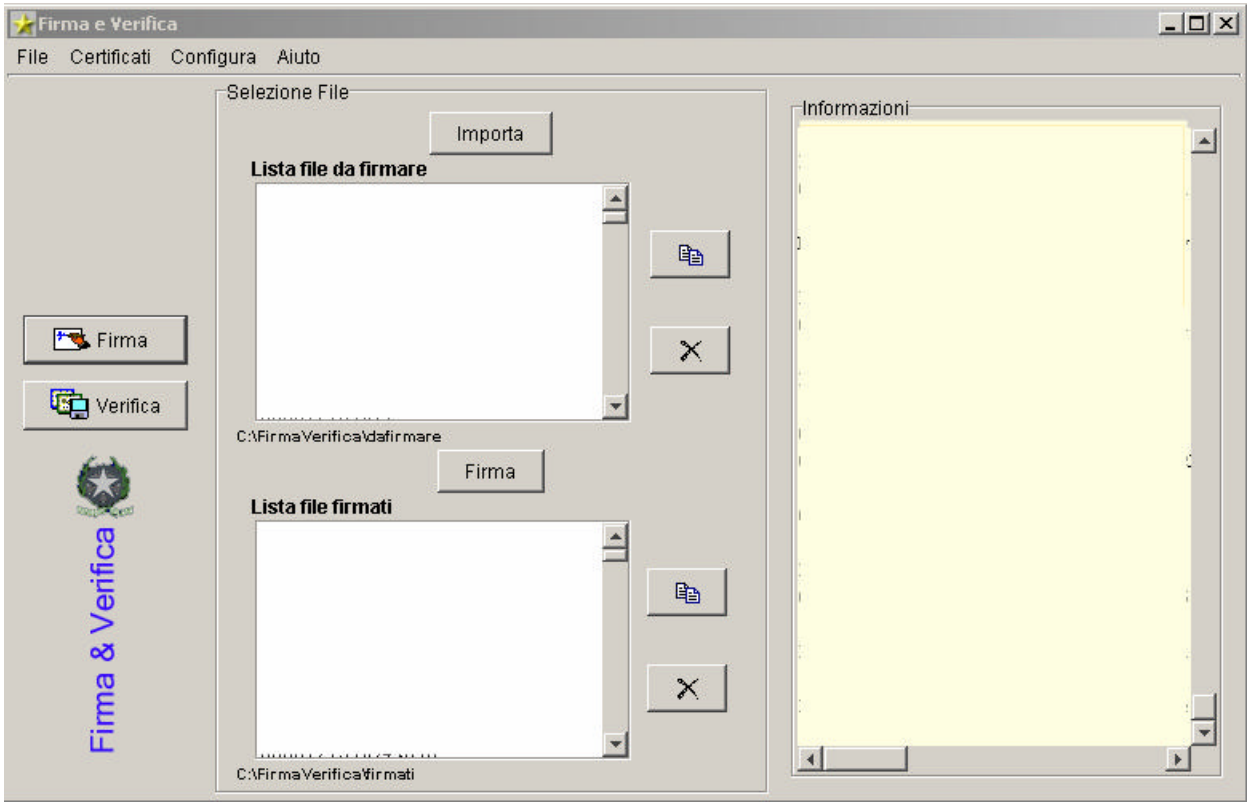
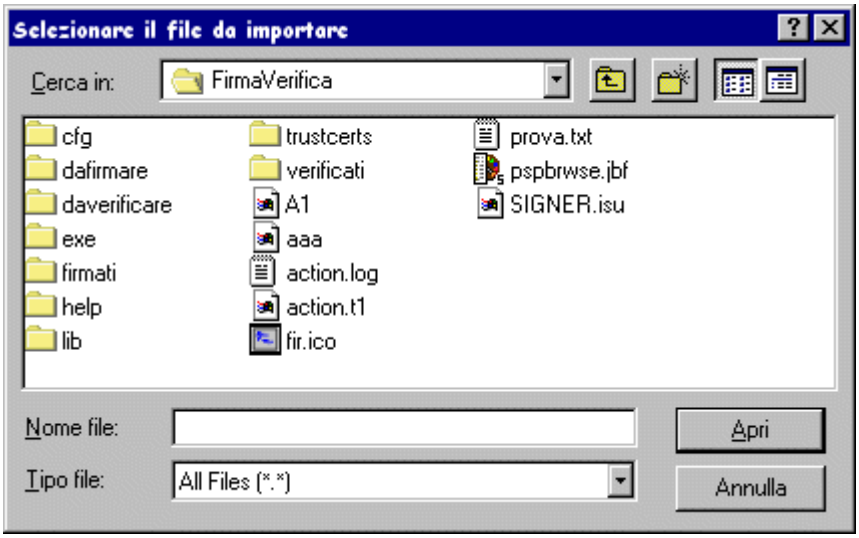


Figura – 10

2. Prima di eseguire l'operazione di firma è necessario importare il file nella directory di lavoro **dafirmare**, cliccando con il tasto sinistro del mouse sul bottone **Importa.** Verrà visualizzata una finestra di dialogo con la quale è possibile selezionare il file da importare:



3. Scegliere il file e premere il bottone **Apri**; al termine il nome del file importato (Figura – 11) compare nella **Lista File da firmare**.

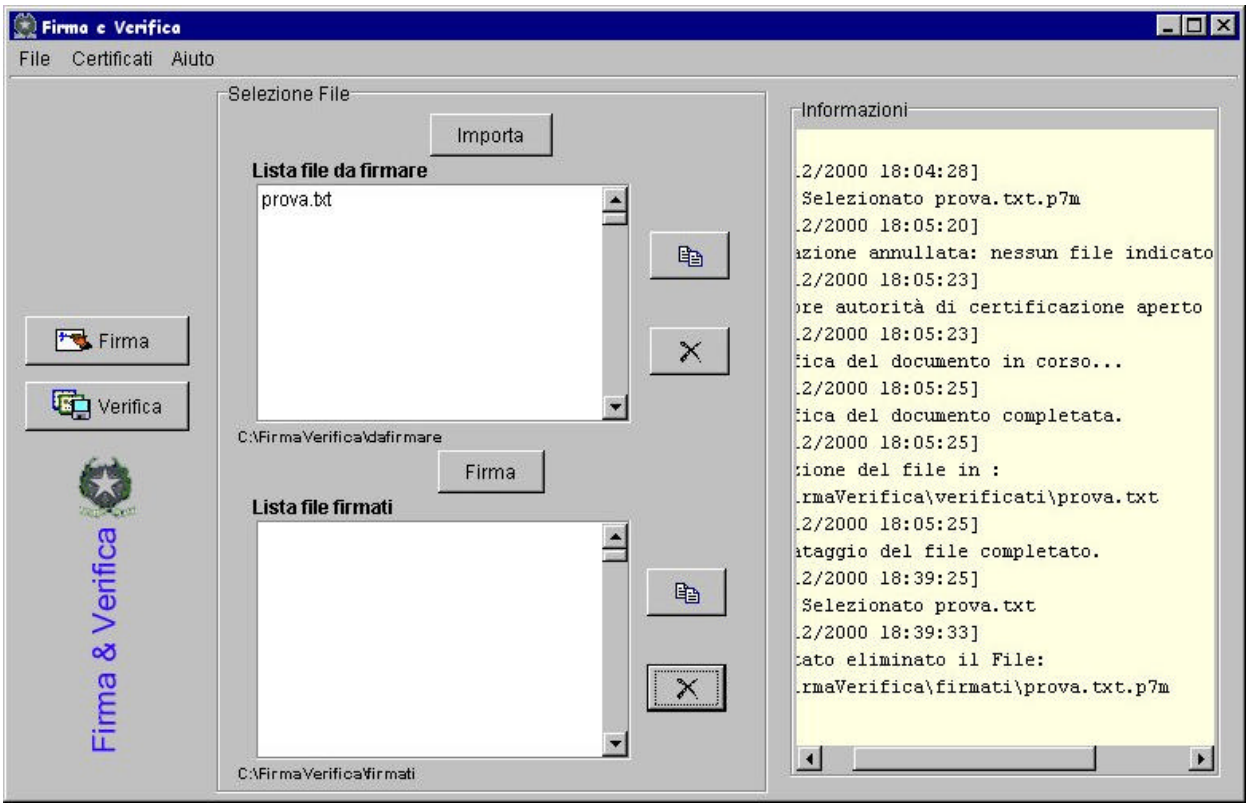


Figura – 11

4. Per firmare il file importato, occorre selezionare il file dalla "**Lista file da firmare**"; tale operazione abilita il bottone **Firma** posizionato sotto la lista.

L'applicazione chiederà di inserire la password che protegge il Keystore.ks, ovvero il file che contiene la chiave pubblica e la chiave privata dell'utente. Tale operazione consente di evitare un accesso improprio dall'operazione di firma da parte di soggetti non autorizzati

Nel caso il Keystore.ks sia su floppy-disk è necessario assicurarsi che esso sia inserito; in caso contrario, l'applicazione segnalerà un messaggio di errore.

5. Dopo aver digitato la password, premere il pulsante **OK** (Figura – 12).

Figura – 12

Per annullare l'operazione cliccare con il tasto sinistro del mouse sul bottone **Annulla**.

6. Viene visualizzata una finestra di dialogo (Figura – 13) mediante la quale è possibile scegliere se visualizzare o meno il contenuto del file che si sta firmando. Selezionando il bottone **Visualizza** l'applicazione aprirà il file utilizzando l'applicazione ad esso associata (in base alla estensione). Per continuare senza la visualizzazione, premere il bottone **Non Visualizzare**.

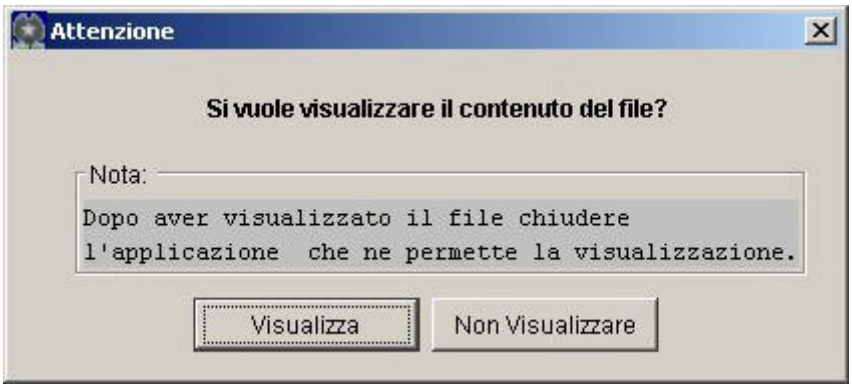


Figura – 13

7. Viene visualizzata una finestra di dialogo (Figura – 14) che richiede all'utente di confermare l'operazione di firma del documento; la finestra riporta il nome completo del file che si intende firmare.
Per confermare l'operazione cliccare con il tasto sinistro del mouse sul bottone **Conferma firma**.
Per annullare l'operazione cliccare con il tasto sinistro del mouse sul bottone **Annulla**.

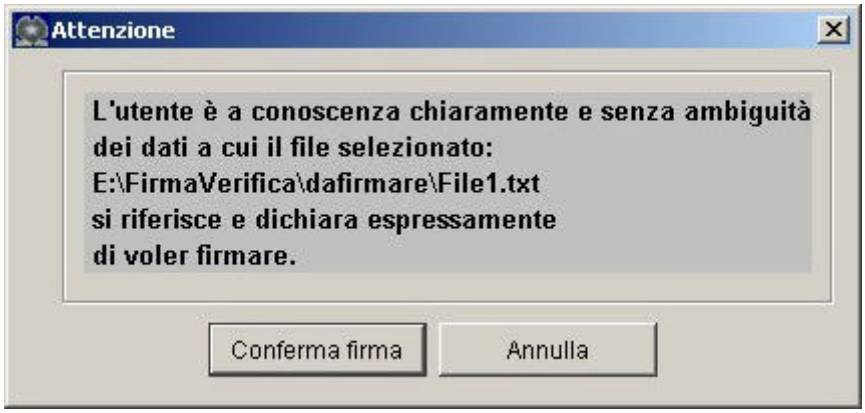


Figura – 14

8. Dopo aver confermato l'operazione, l'applicazione calcola il codice di autenticazione e crea un nuovo file (nel formato **PKCS7**) che contiene il file originario e il codice di autenticazione. Durante questa fase, viene visualizzato il messaggio **"Firma del file in corso..**" nell'area **Informazioni** della finestra principale.
Il file creato avrà il nome del file originale con l'aggiunta dell'estensione **p7m**. Verrà creato nella directory di lavoro **firmati** e comparirà nella **Lista File firmati** come mostrato in Figura – 15.

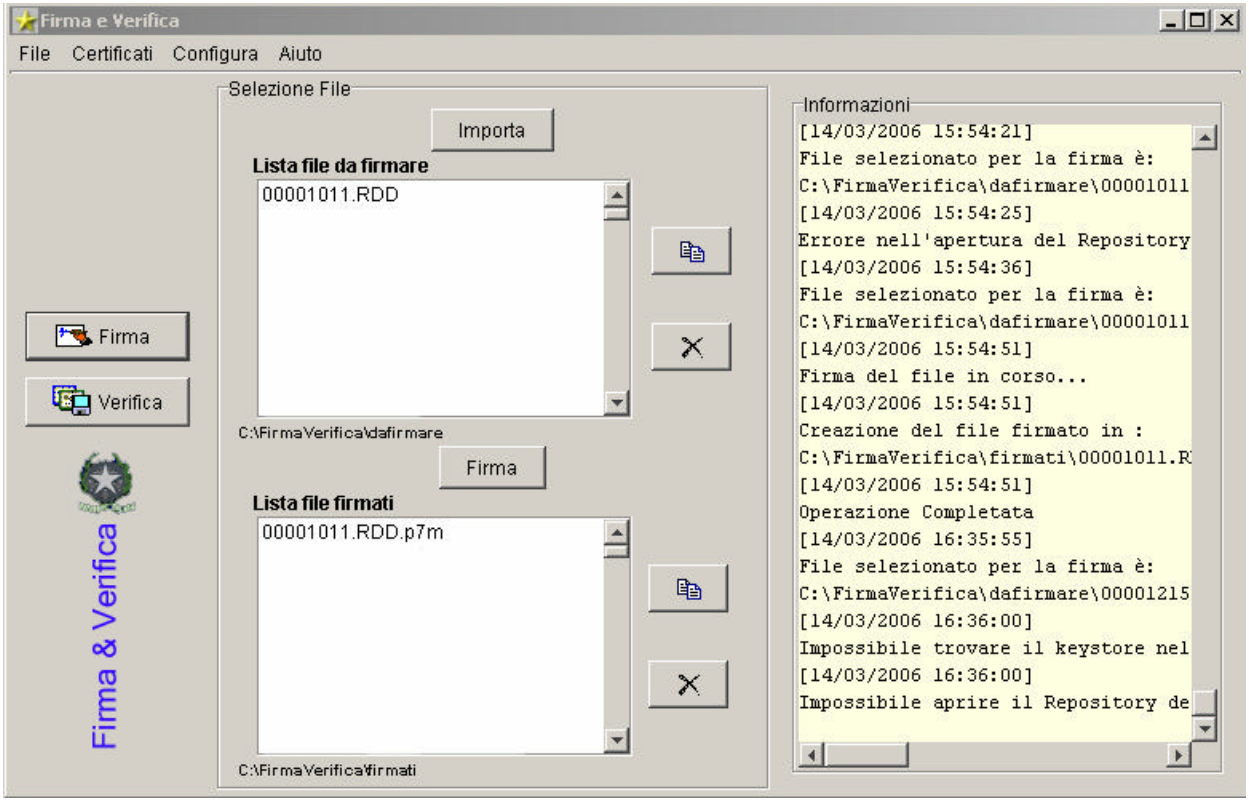
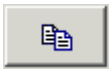


Figura – 15

9. Selezionando un file dalla **Lista file da firmare** (oppure dalla **Lista file firmati**) e cliccando con il tasto sinistro del mouse sul bottone  **Copia,** è possibile effettuare una copia del file selezionato in una directory e con un nome a scelta dell'utente, da indicare nella finestra di dialogo che viene utilizzata dal sistema operativo per il salvataggio dei file.

10. Selezionando un file dalla **Lista file da firmare** (oppure dalla **Lista file firmati**) e cliccando con il tasto sinistro del mouse sul bottone  **Elimina,** è possibile eliminare il file selezionato dalla corrispondente lista, dopo una richiesta di conferma.

6 Verifica

La funzione consente di verificare il codice di autenticazione di un file, salvandone il contenuto nel formato originario. La verifica controlla che il codice di autenticazione sia stato calcolato correttamente, che il file cui si riferisce non sia stato modificato successivamente e che il certificato del firmatario sia attendibile. Per eseguire quest'ultima operazione, viene utilizzato il **Gestore delle autorità di certificazione**, descritto in seguito, che contiene la chiave pubblica dell'Amministrazione finanziaria.

I passi che occorre eseguire per verificare il codice di autenticazione sono i seguenti:

1. Cliccare con il tasto sinistro del mouse sul bottone **Verifica**. Viene visualizzato nella finestra principale il pannello mostrato nella figura che segue:

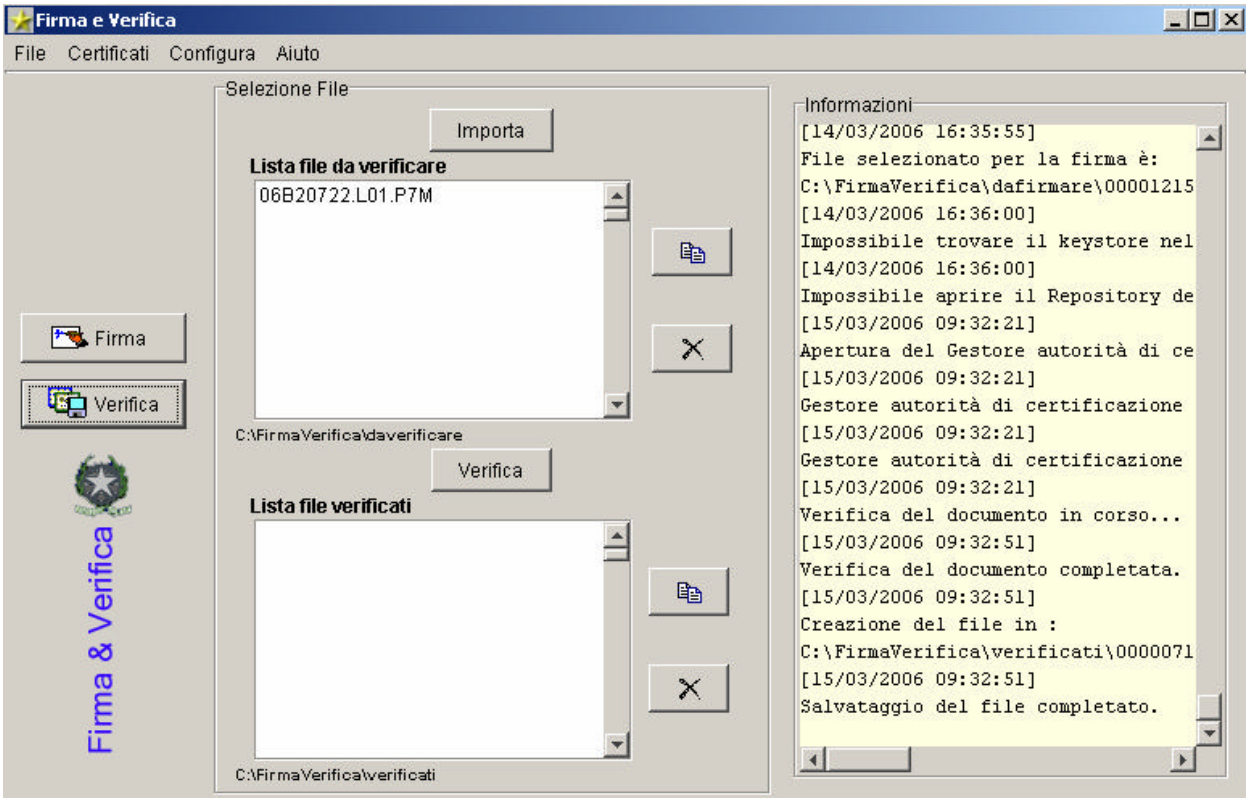


Figura – 16

2. Per verificare un file occorre importare il file nella directory di lavoro **daverificare**, cliccando con il tasto sinistro del mouse sul bottone **Importa.** Viene visualizzata una finestra di dialogo con la quale è possibile selezionare il file da importare. Al termine il nome del file importato compare nella **Lista file da verificare** (Figura – 17).

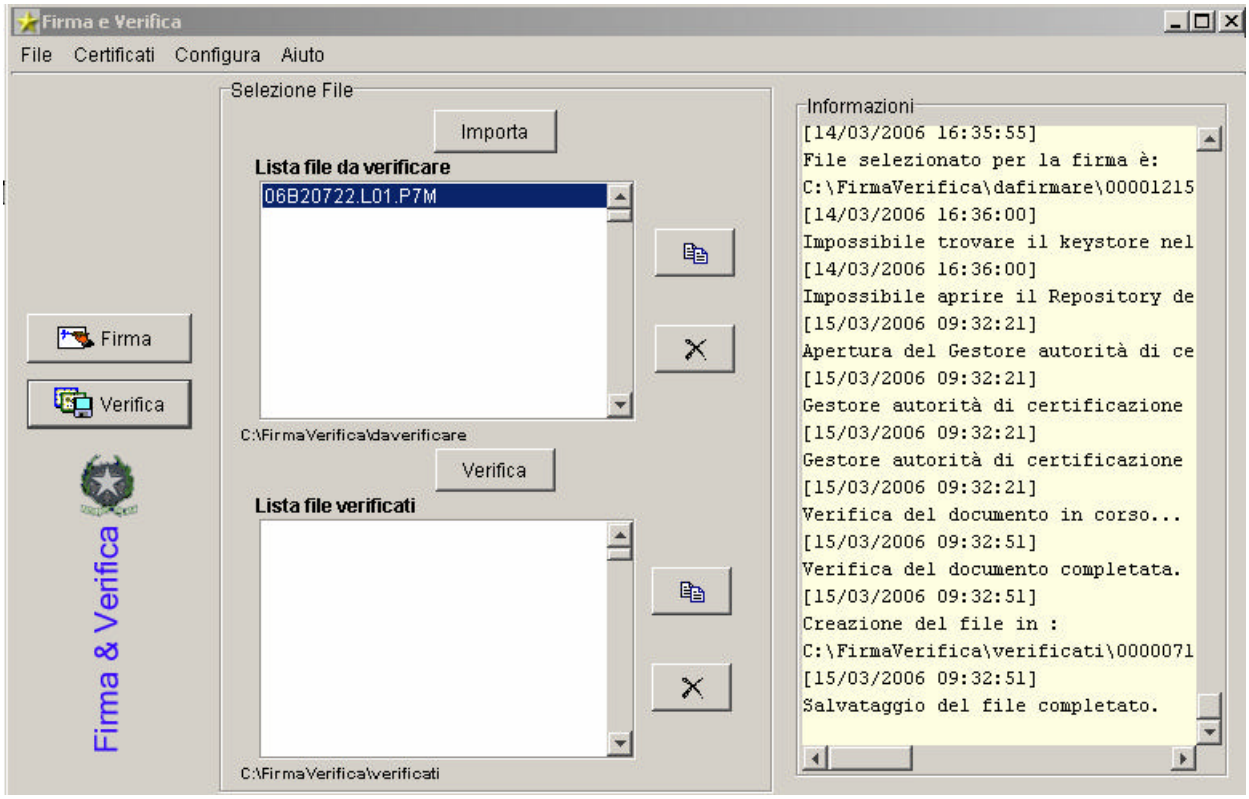


Figura – 17

3. Occorre quindi selezionare il file dalla **Lista file da verificare**, cliccando sul nome con il tasto sinistro del mouse. Tale operazione rende selezionabile il bottone **Verifica** posizionato sotto la lista. L'applicazione chiederà di inserire la password che protegge il Gestore delle autorità di certificazione (Figura – 18).

Figura – 18

Digitare la password e premere il bottone **OK**. Se non è stata modificata, la password assume il valore di default "**123456**".
Per annullare l'operazione premere il bottone **Annulla**.
La richiesta di password viene presentata solo al primo utilizzo dopo l'apertura dell'applicazione.

4. Se la password inserita è corretta e non si verificano errori nell'apertura del **Gestore**, l'applicazione legge il file, verificandone il formato e il codice di autenticazione. Ad operazione terminata viene visualizzata una finestra di dialogo che indica il risultato dell'operazione di verifica:

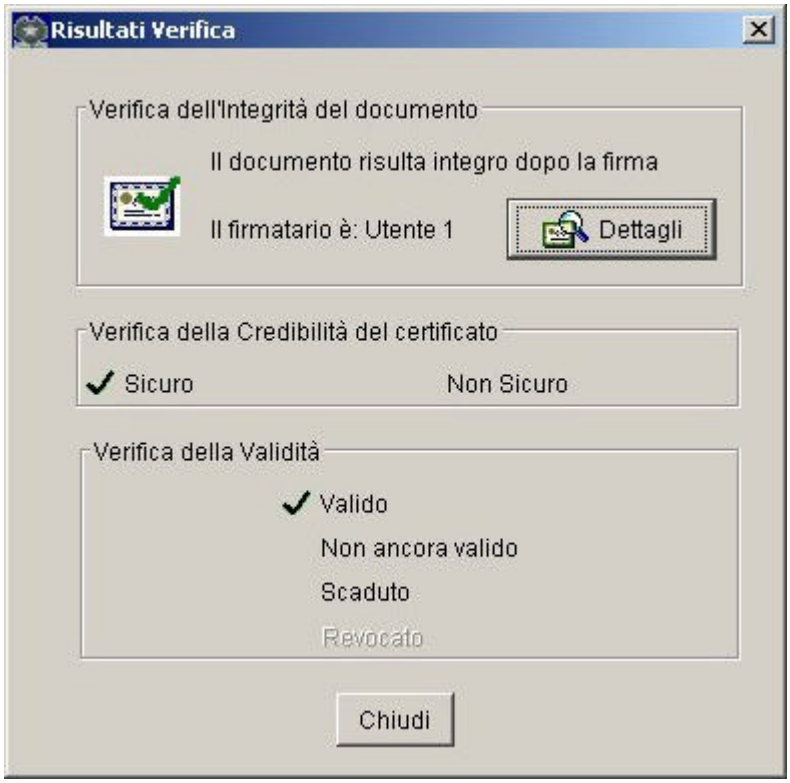


Figura – 19

Nella finestra sono visibili tre aree:

Verifica dell'integrità del documento:

- *"Il documento risulta integro dopo la firma"* in caso di esito positivo della verifica;
- *"Il documento NON risulta integro dopo la firma"* in caso di esito negativo, come mostrato nella figura che segue

Figura – 20

Verifica della credibilità del certificato: Visualizza se il certificato del firmatario è **Sicuro** o **Non Sicuro** tramite l'apposito simbolo grafico (✓).

Verifica della Validità: visualizza lo stato di validità del certificato indicando con un simbolo grafico (✓) la voce corrispondente:

Valido	Se la data corrente è antecedente alla data di scadenza e posteriore alla data di inizio validità
Non ancora valido	Se la data corrente è antecedente alla data di inizio validità
Scaduto	Se la data corrente è posteriore alla data di scadenza

Premendo il bottone **Dettagli** è possibile consultare le informazioni relative al certificato del firmatario, così come illustrato al successivo paragrafo 9.1.

5. Premendo il bottone **Chiudi** la finestra di dialogo viene chiusa e viene creato il file nel formato originario senza l'estensione **p7m**. Il file si trova nella directory di lavoro **verificati** e compare nella **Lista file verificati** come mostrato in Figura – 21.

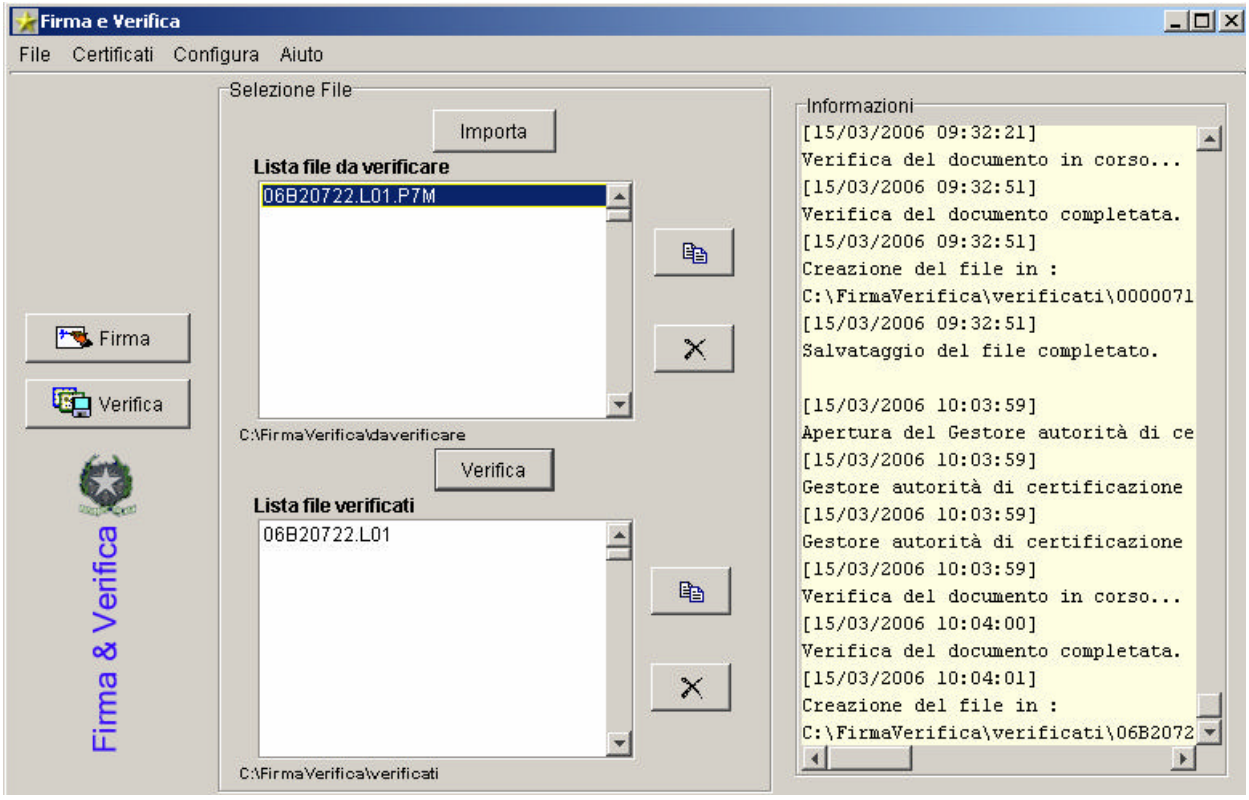
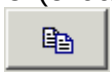


Figura – 21

6. Selezionando un file dalla **Lista file da verificare** (o dalla **Lista file verificati**) e cliccando con il tasto sinistro del mouse sul bottone  **Copia,** è possibile creare una copia del file selezionato in una directory e con un nome a scelta dell'utente, da indicare nella finestra di dialogo che il sistema operativo utilizza per il salvataggio dei file.

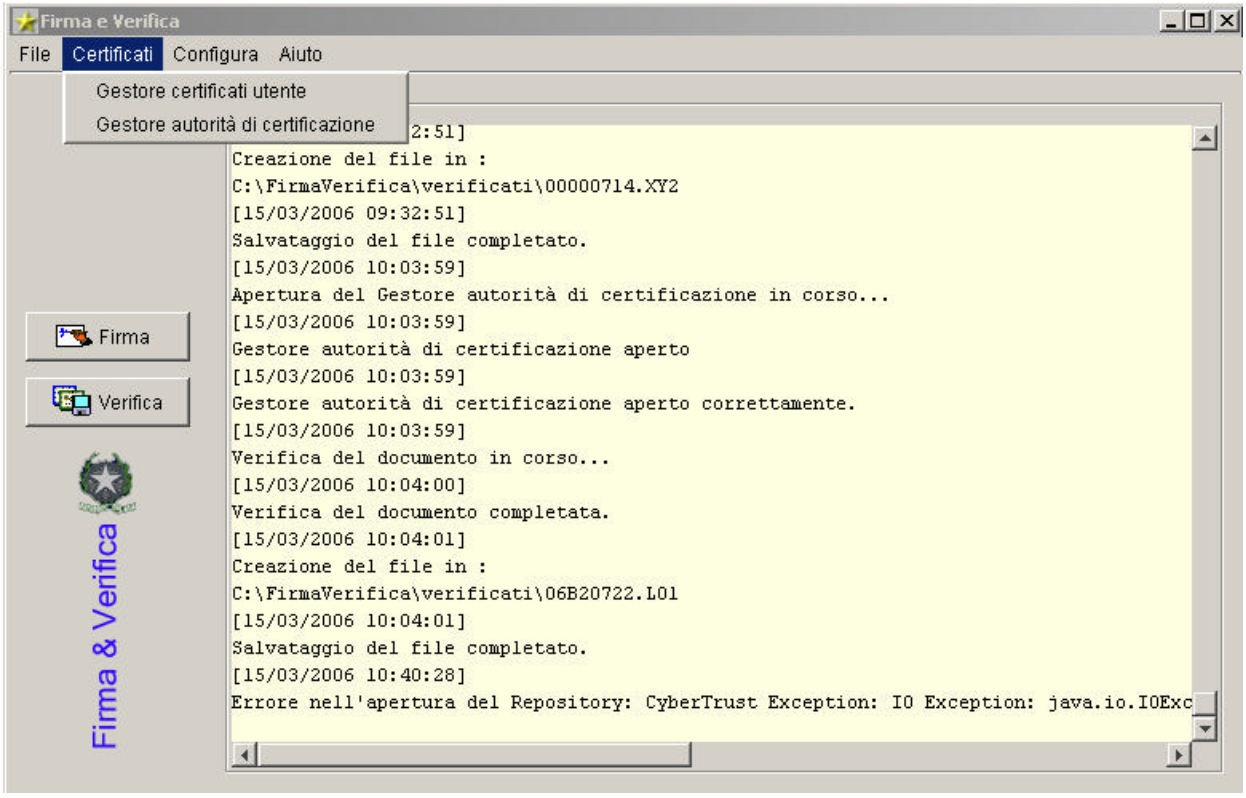
7. Selezionando un file dalla **Lista file da verificare** (o dalla **Lista file verificati**) e cliccando con il tasto sinistro del mouse sul bottone  **Elimina,** è possibile eliminare il file selezionato dalla corrispondente lista, dopo una richiesta di conferma.

7 Gestore certificati utente

La funzione consente di visualizzare i dettagli del certificato intestato all'utente.

7.1 Gestore certificati utente

1. Cliccare con il tasto sinistro del mouse sulla voce **Gestore certificati utente** nel menù **Certificati**.



2. Viene visualizzata una finestra (Figura - 22) in cui sono visibili alcune informazioni del certificato di firma:

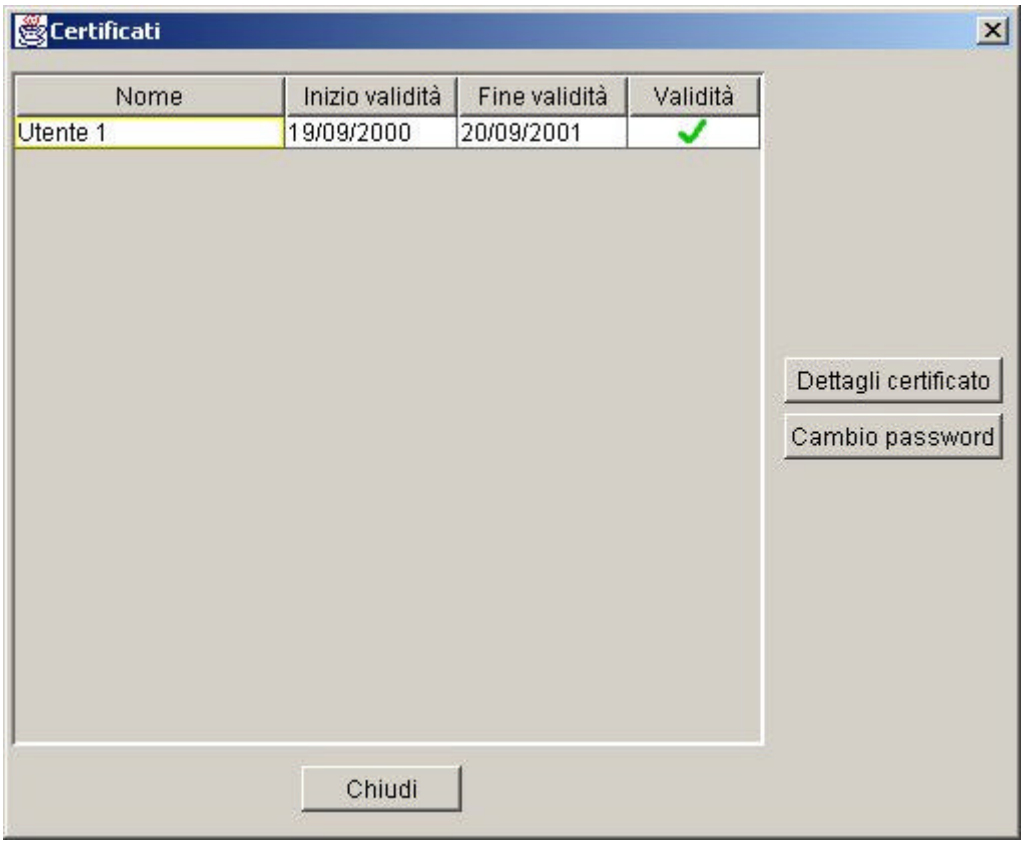


Figura – 22b

Le informazioni sono in particolare:

Nome: il *Common Name* presente nel certificato.
Inizio validità: La data di inizio validità indicata nel formato GG/MM/AAAA.
Fine validità: La data di fine validità del certificato indicata nel formato GG/MM/AAAA.

Validità: un'immagine che indica se il certificato è ancora valido o meno:

✔	Il certificato è valido
⛔	Il certificato è scaduto

3. Per chiudere la finestra cliccare sul bottone **Chiudi**.

7.1.1 Visualizzare i dettagli di un certificato

Per ***visualizzare il certificato,*** occorre cliccare con il tasto sinistro del mouse sulla riga corrispondente e premere il bottone **Dettagli certificato**.

Viene visualizzata una finestra (Figura - 23) contenente tre cartelle: **Generale**, **Validità**, **Estensioni.**

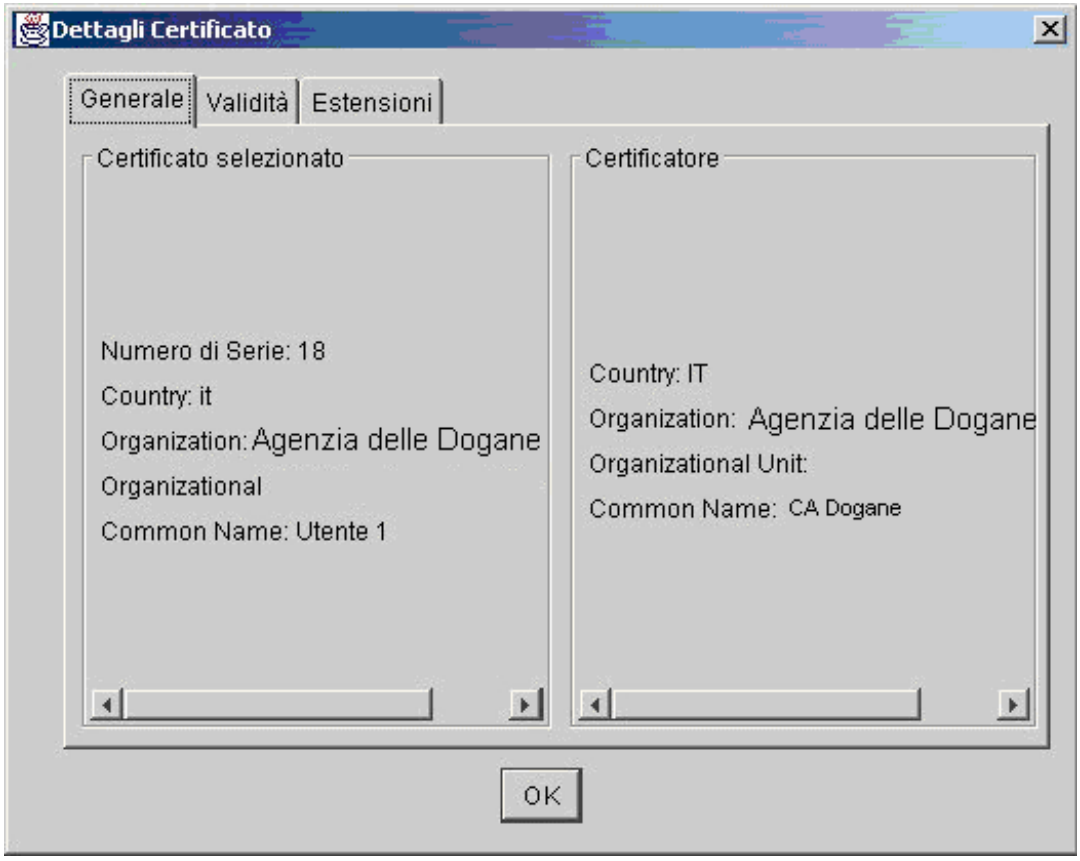


Figura – 23

Il contenuto delle cartelle è il seguente:

- **Generale** (Figura – 23) : contiene due aree: ***Contenuto certificato*** e ***Certificatore ,*** con le informazioni, rispettivamente, relative al titolare del certificato e al firmatario del certificato.
- **Validità** (Figura - 24):

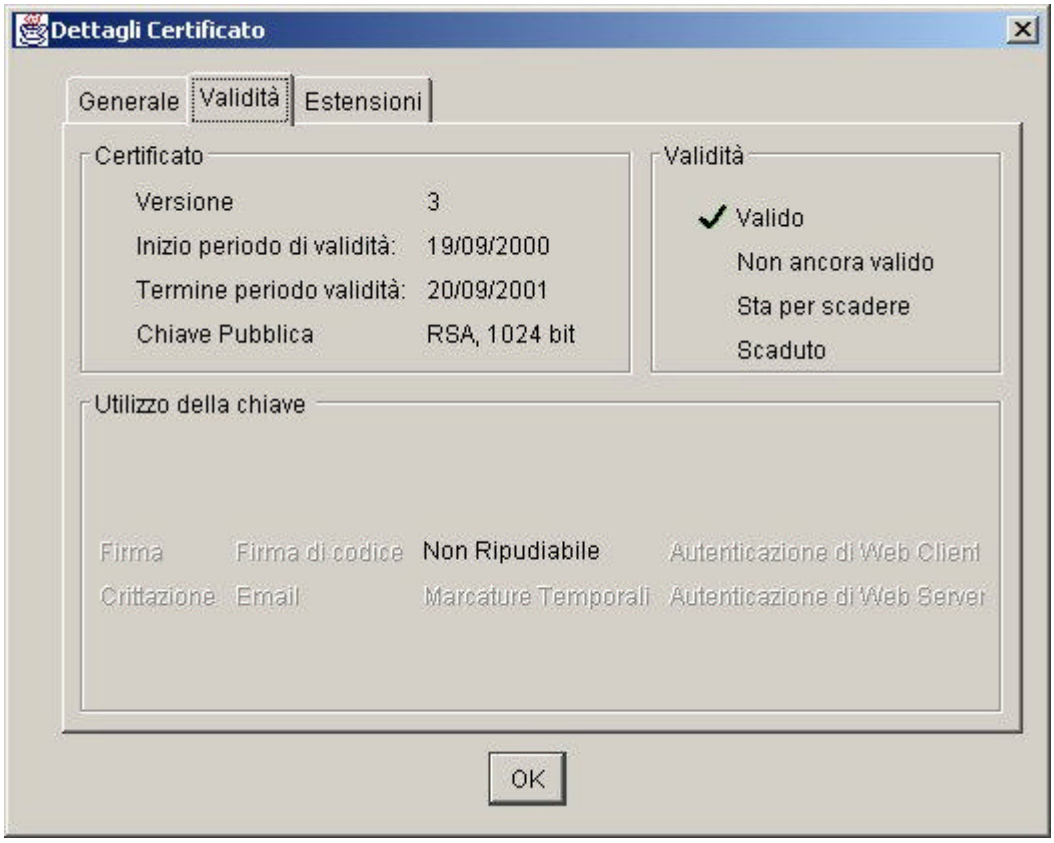


Figura – 24

che contiene sono visualizzate tre aree:

- ***Certificato***:

Nome	**Descrizione**
Versione	La versione del certificato
Inizio Periodo di validità	La data di inizio della validità (GG/MM/AAAA)
Termine Periodo di validità	La data di scadenza (GG/MM/AAAA)
Chiave Pubblica	Algoritmo utilizzato (RSA, DSA , Diffie-Hellman) e la Lunghezza della chiave

- ***Validità***:

Valido	Se la data corrente è antecedente alla data di scadenza e posteriore alla data di inizio validità
Non ancora Valido	Se la data corrente è antecedente alla data di

	inizio validità
Sta per scadere	Se manca un giorno alla scadenza
Scaduto	Se la data corrente è posteriore alla data di scadenza

Lo "stato" del certificato è evidenziato con un simbolo grafico.

- ***Utilizzo della chiave***:

Possibili significati	**Valore presente nel certificato**
Firma	digital segnature
Crittazione	**RS**A: key encipherment, dat encipherment **Diffie-Hellma**n: key agreement, enciphe only, decipher only
Non Ripudiabile	non repudiation
Informazioni di Revoca	Crl sign
CA	Key cert sign (se il certificato è di CA)
Email	Email protection
Firma di codice	Code signing
Autenticazione di Web Server	Tls web server authentication
Autenticazione di Web Client	Tls web client authentication
Marcature Temporali	Time stamping

L'utilizzo relativo al certificato dell'utente è evidenziato in grassetto.

? **Estensioni** (Figura - 25): contiene tre aree: ***Estensioni Critiche***, ***Estensioni Non Critiche, Estensioni Private***. E' prevista attualmente l'utilizzo della sezione "Estensioni non critiche".

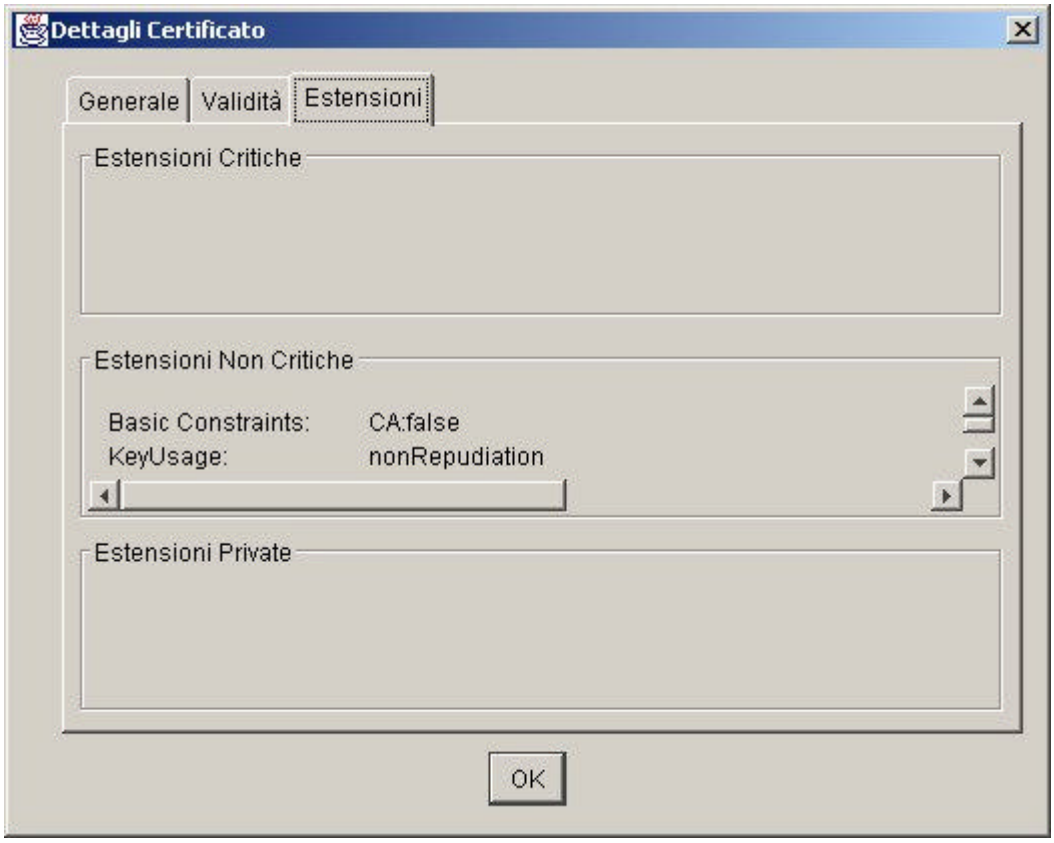


Figura – 25

Per chiudere la finestra premere il bottone **OK.**

7.1.2 Modifica password Utente

Per modificare la password di protezione del Keystore.ks che contiene la chiave privata dell'utente (dispositivo di firma) , occorre cliccare con il tasto sinistro del mouse sul bottone **Cambio password**.
Viene aperta la finestra di dialogo (Figura - 26)

Figura - 26

per indicare :

- la password che protegge il Keystore.ks; se non corretta, viene visualizzato un messaggio d'errore)
- la nuova password
- la nuova password per conferma; se diversa dal valore indicato nel campo "nuova password", viene visualizzato un messaggio d'errore.

Premere il bottone **Conferma** per salvare la nuova password, oppure il bottone **Annulla** per annullare l'operazione.

La password deve essere composta almeno di 4 caratteri, non deve contenere spazi e caratteri speciali, non deve essere composta esclusivamente da lettere minuscole. Se questi requisiti non sono rispettati, viene, visualizzato un messaggio di errore.

Nel caso in cui siano state eseguite più copie del dispositivo di firma, è opportuno ripetere le copie oppure inserire la nuova password su tutte le copie disponibili.

7.2 Gestore autorità di certificazione

E' possibile visualizzare i dettagli dei certificati relativi alla CA (autorità di certificazione).

Per accedere al Gestore autorità di certificazione occorre eseguire i seguenti passi:

1. Cliccare con il tasto sinistro del mouse sulla voce **Gestore autorità di certificazione** nel menù **Certificati**.
2. Digitare la password del Gestore: se non è stata modificata, la password assume il valore presente al momento dell'installazione (123456). Viene visualizzata una finestra di dialogo per l'inserimento della password del Gestore, digitare la password e cliccare con il tasto sinistro del mouse sul bottone **OK** (Figura - 27).

Figura – 27

La richiesta di password viene presentata solo al primo utilizzo del Gestore dopo l'apertura dell'applicazione.

Per annullare l'operazione premere il bottone **Annulla**.

Se la password è corretta viene aperta la finestra del Gestore che visualizza l'elenco dei certificati in esso contenuti:

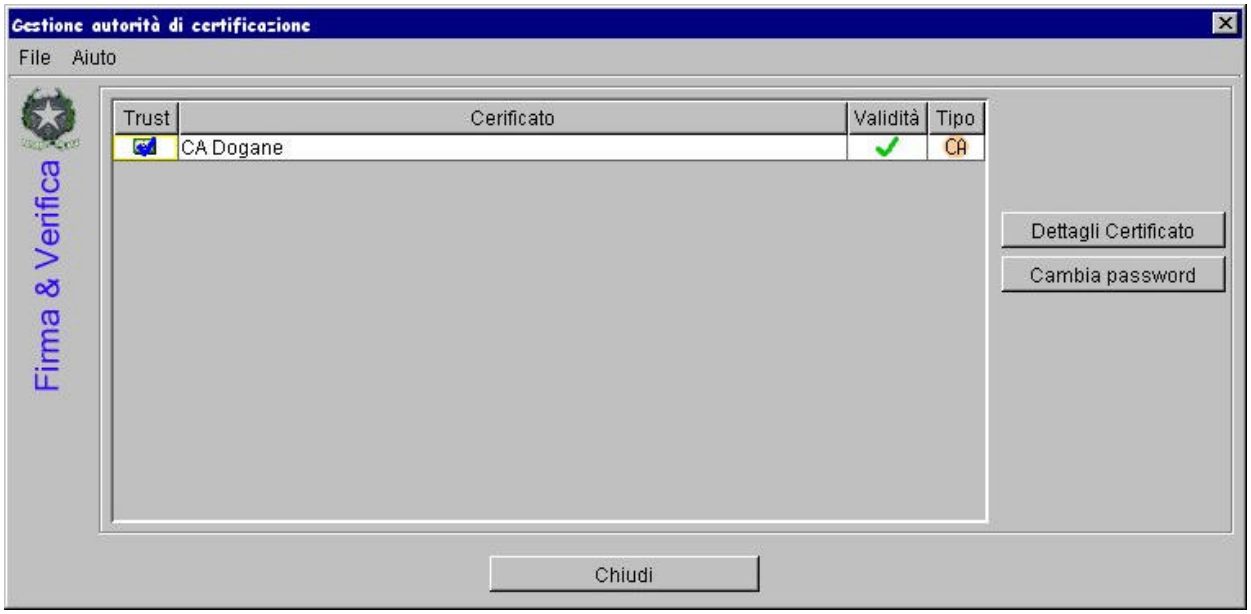


Figura – 28

Nella colonna "**trust**" è presente un immagine che assume il seguente significato:

	È fidato
	E' fidato in quanto "eredita" tale caratteristica dal certificato firmatario e/o dalla RootCA
	Non è fidato

Certificato: la colonna riporta i dati identificativi del titolare del certificato.

Validità: contiene un'immagine che indica se lo "stato" del certificato:

	Valido
	Sta per scadere
	Non valido

Tipo: contiene un'immagine che indica se il tipo di certificato :

CA	Certificato di CA
EE	Certificato utente
CA	Certificato di Root CA

7.2.1 Visualizzare i dettagli di un certificato

Per visualizzare i dettagli di un certificato occorre eseguire i seguenti passi:
1. Selezionare il certificato cliccando con il tasto sinistro del mouse sulla riga della tabella corrispondente al certificato che si vuole visualizzare.
2. Cliccare col tasto sinistro del mouse sul bottone **Dettagli Certificato.**
In alternativa, cliccare con il tasto destro del mouse sulla riga della tabella corrispondente al certificato che si vuole visualizzare:

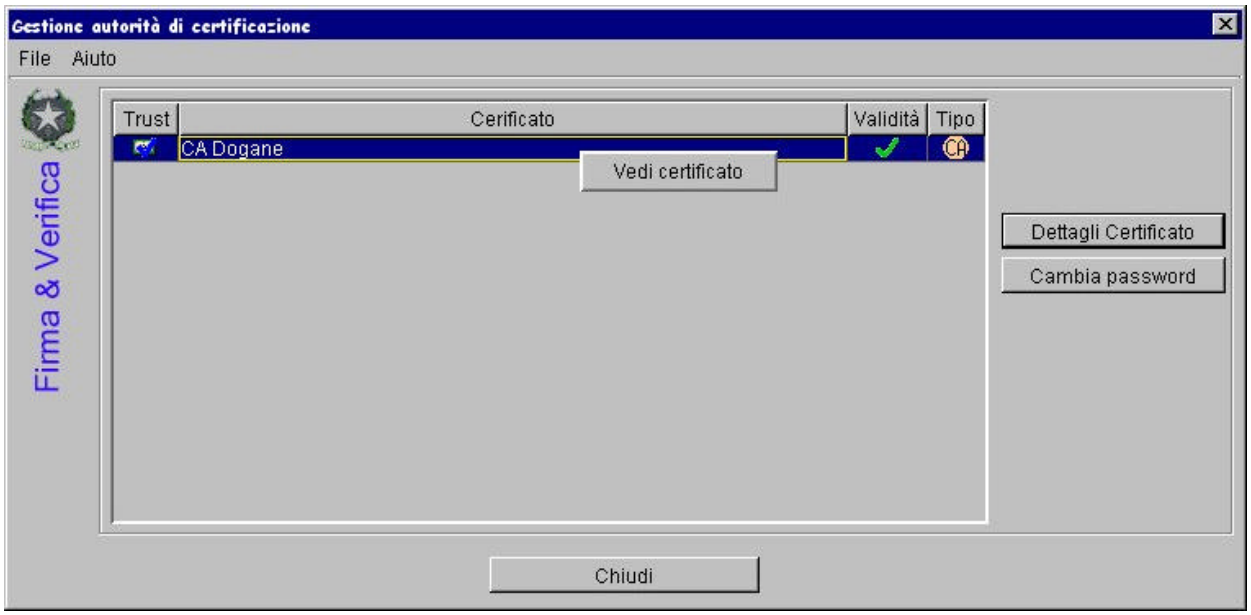


Figura – 29

3. Le informazioni disponibili sono descritte al precedente paragrafo 8, passo 4.

7.2.2 Modifica password del Gestore

1. Cliccare sul bottone **Cambia Password** o cliccare sul menù **File** e sulla voce **Cambia password** :

Figura - 30

2. Viene aperta la finestra di dialogo che segue:

Figura - 31

dove occorre indicare :

- la password del Gestore; se non corretta, viene visualizzato un messaggio d'errore)
- la nuova password;
- la nuova password per conferma; se viene indicato una valore diverso da quello del campo "Nuova Password", viene visualizzato un messaggio d'errore.

Premere il bottone **Conferma** per salvare la nuova password, oppure il bottone **Annulla** per annullare l'operazione.

8 Uscita dall'applicazione

Per chiudere l'applicazione, cliccare sul menù **File** e sulla voce **Uscita**,
In alternativa, è possibile cliccare con il tasto sinistro del mouse sul bottone **"X**" posto sulla finestra in alto a destra.

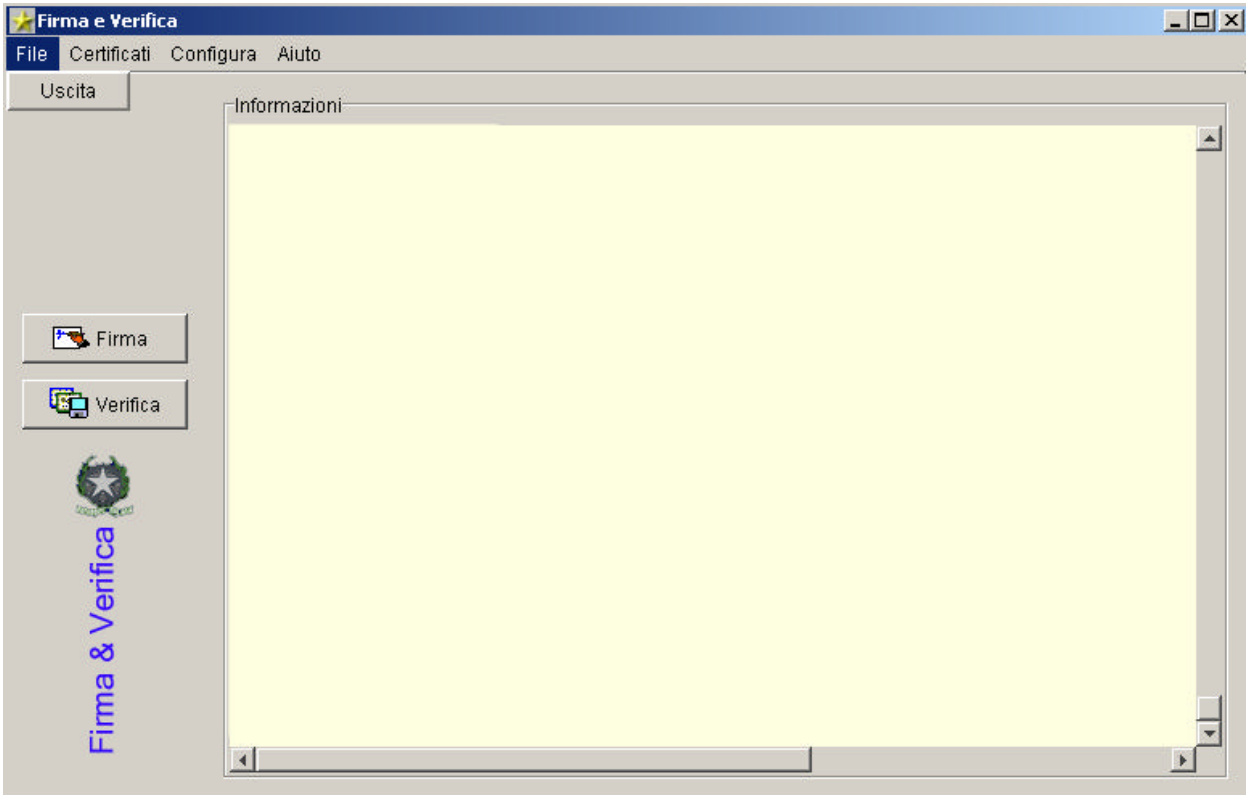


Figura – 33

9 Disinstallazione applicazione

L'applicazione può essere disinstallata utilizzando le funzioni previste dal sistema operativo installato sul vostro computer. Ad esempio, se utilizzate Windows NT, per eseguire la disinstallazione occorre:

- selezionare sul desktop l'icona "**Risorse del Computer**";
- sul menu che vi viene proposto, selezionate la voce "**Pannello di controllo**" e di seguito "**Installazione/disinstallazione applicazioni**";
- compare la lista delle applicazioni installate sul vostro PC, tra le quali occorre selezionare "**Firma e Verifica**".

L'operazione descritta rimuove i file dell'applicazione, lasciando inalterati eventuali file utente, a condizione che non sia stata alterata la struttura originaria delle cartelle e dei vari componenti, così come risulta dopo l'installazione iniziale.