

# INVIO TELEMATICO

## Leggere i file firmati










AMMIRATI Geom. Alberto  
[amalgeo@gmail.com](mailto:amalgeo@gmail.com)

I files Docfa e Pregeo da trasmettere per via telematica all'Agenzia del Territorio, come sappiamo, devono essere preventivamente firmati con il software FirmaVerifica mediante il quale si avrà la generazione di un nuovo file con estensione \*.p7m inserito nella directory C:\FirmaVerifica\firmati.

Il file p7m non è altro che il nostro documento al quale viene aggiunta una firma digitale che permette all'A.d.T. di eseguire alcuni controlli sull'autenticità, e integrità del documento inviato.

Le caratteristiche salienti di un documento informatico firmato digitalmente sono:

- Autenticità: certezza dell'identità del sottoscrittore.
- Integrità: garanzia che il documento informatico non è stato manomesso dopo la sua sottoscrizione.
- Non ripudio: la firma digitale si presume riconducibile al titolare del dispositivo di firma, salvo che sia data prova contraria.
- Valore legale: il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 (del D.Lgs 7 marzo 2005, n. 82-CAD ) che garantiscano l'identificabilità dell'autore e l'integrità del documento.

Elenco dei documenti che compongono la pratica			
	Descrizione	Data	Dimensioni
	Documento trasmesso	21/09/2007	96.6KB (98,922 bytes)
	Ricevuta di Trasmissione	21/09/2007	6.5KB (6,658 bytes)
	Ricevuta di Trasmissione	21/09/2007	7.96KB (8,152 bytes)
	Ricevuta di ricezione	21/09/2007	6.1KB (6,249 bytes)
	Ricevuta di ricezione	21/09/2007	7.56KB (7,741 bytes)
	Ricevuta di Approvazione	24/09/2007	36.25KB (37,123 bytes)
	Ricevuta di Approvazione	24/09/2007	37.77KB (38,677 bytes)
	Ricevuta di cassa	24/09/2007	4.93KB (5,048 bytes)
	Ricevuta di cassa	24/09/2007	6.38KB (6,538 bytes)

**File "firmati" elettronicamente**

Anche l'A.d.T. ci invia dei documenti firmati digitalmente, sempre in formato p7m. Se da Sister andiamo in “presentazione documenti” è possibile selezionare l’elenco delle pratiche presentate, e per ognuna vedere il relativo stato (scartato dal sistema, elaborato dall’ufficio – respinto, elaborato dall’ufficio – registrato, ecc.)

Nell’elenco delle pratiche presentate è possibile salvare e/o stampare la ricevuta anche in formato pdf. Le varie icone permettono di visualizzare le informazioni relative ad una pratica o di scaricare su di un disco locale i file di ricevuta relativi alla pratica, anche quando siano state riscontrate delle anomalie.

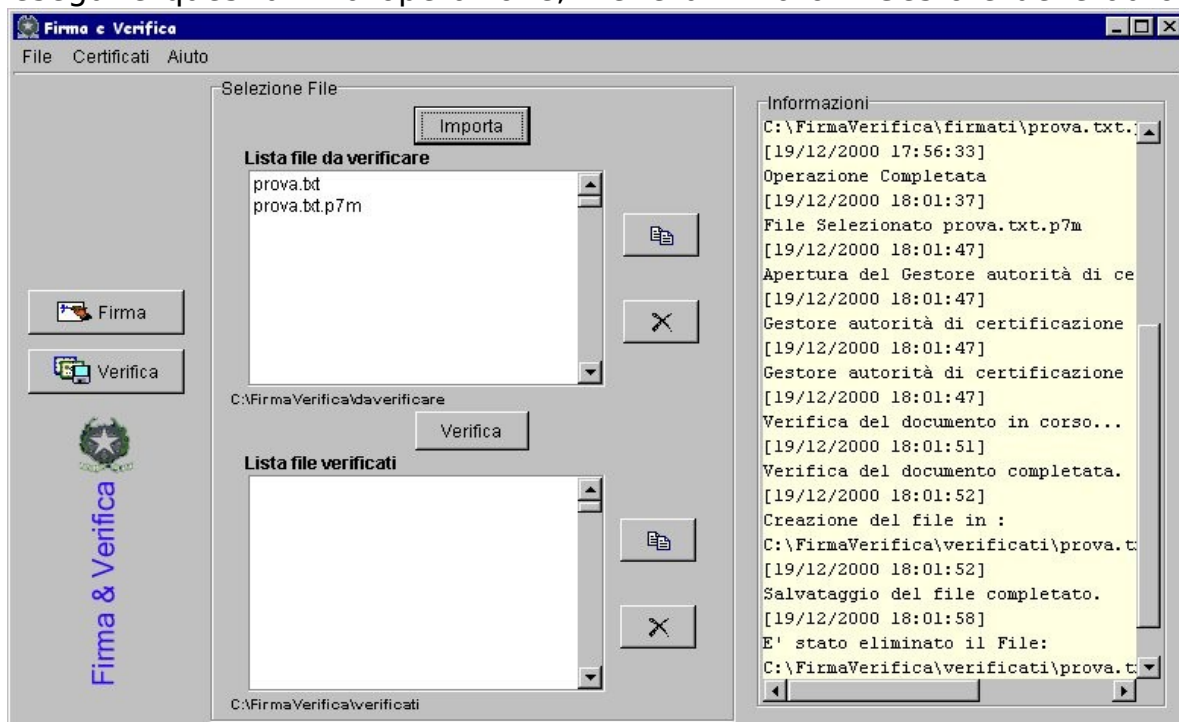
	<b>Ricevuta di Trasmissione</b>	21/09/2007	6.5KB (6,658 bytes)
	<b>Ricevuta di Trasmissione</b>	21/09/2007	7.96KB (8,152 bytes)

Come è possibile vedere dall'immagine, ci vengono inviati due serie di documenti che potremo rispettivamente definire “*in chiaro*” quelli con il simbolo della manina che tiene un foglio e quelli “*firmati*” con la manina che tiene il foglio più il simbolo di un certificato. Questi ultimi (che sono in formato p7m) sono identici a quelli in chiaro, solo che sono “firmati” dall'A.d.T. che ne certifica l'autenticità ed integrità. Solo questi avranno valore legale in un eventuale disputa.

Mentre quelli “*in chiaro*” è possibile scaricarli e leggerli (sono tutti in formato pdf) come fare per leggere quelli “*firmati*”?

Il software FirmaVerifica (con la funzione “verifica”) ci permette 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 che contiene la chiave pubblica dell'Amministrazione finanziaria.

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

Cliccare con il tasto sinistro del mouse sul bottone Verifica.

- 1) Per verificare un file occorre importare il file nella directory di lavoro da verificare, 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
- 2) 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.
- 3) 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.

Il programma verifica l'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
- 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

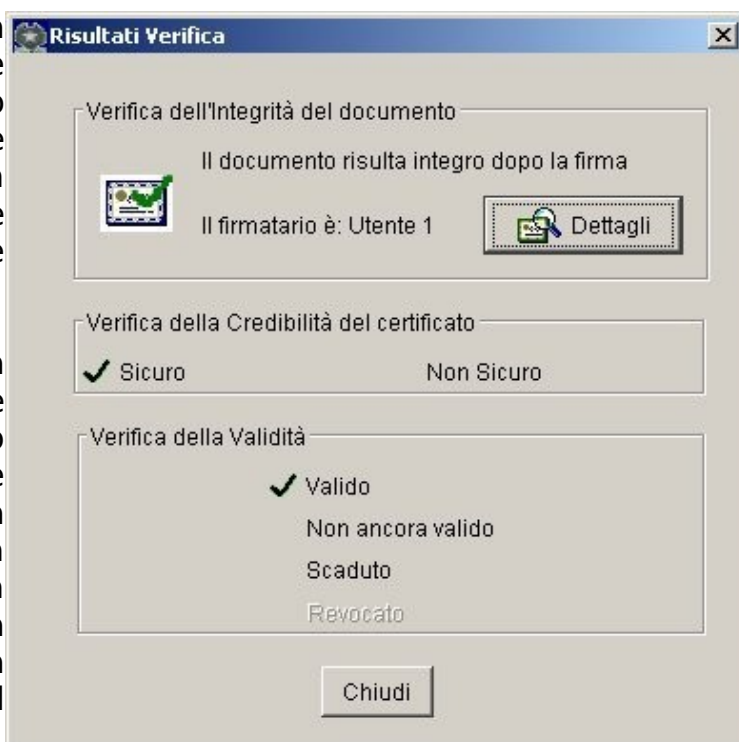
Inoltre viene verificato se il certificato risulta:

- 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

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 troverà nella directory di lavoro verificati e comparirà nella Lista file verificati.

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.



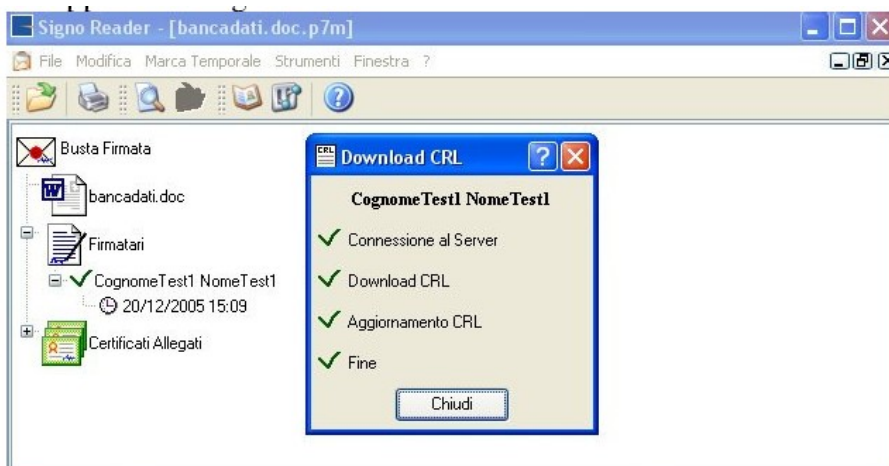
Selezionando un file dalla Lista file da verificare (o dalla Lista file verificati) e cliccando con il tasto sinistro del mouse sul bottone Elimina, è possibile eliminare il file selezionato dalla corrispondente lista, dopo una richiesta di conferma.

Il sistema è sicuramente valido, però risulta alquanto macchinoso e ostico. Per ovviare a ciò, possiamo utilizzare un altro software (free) che risulta essere molto più "user friendly" e di immediata comprensione.

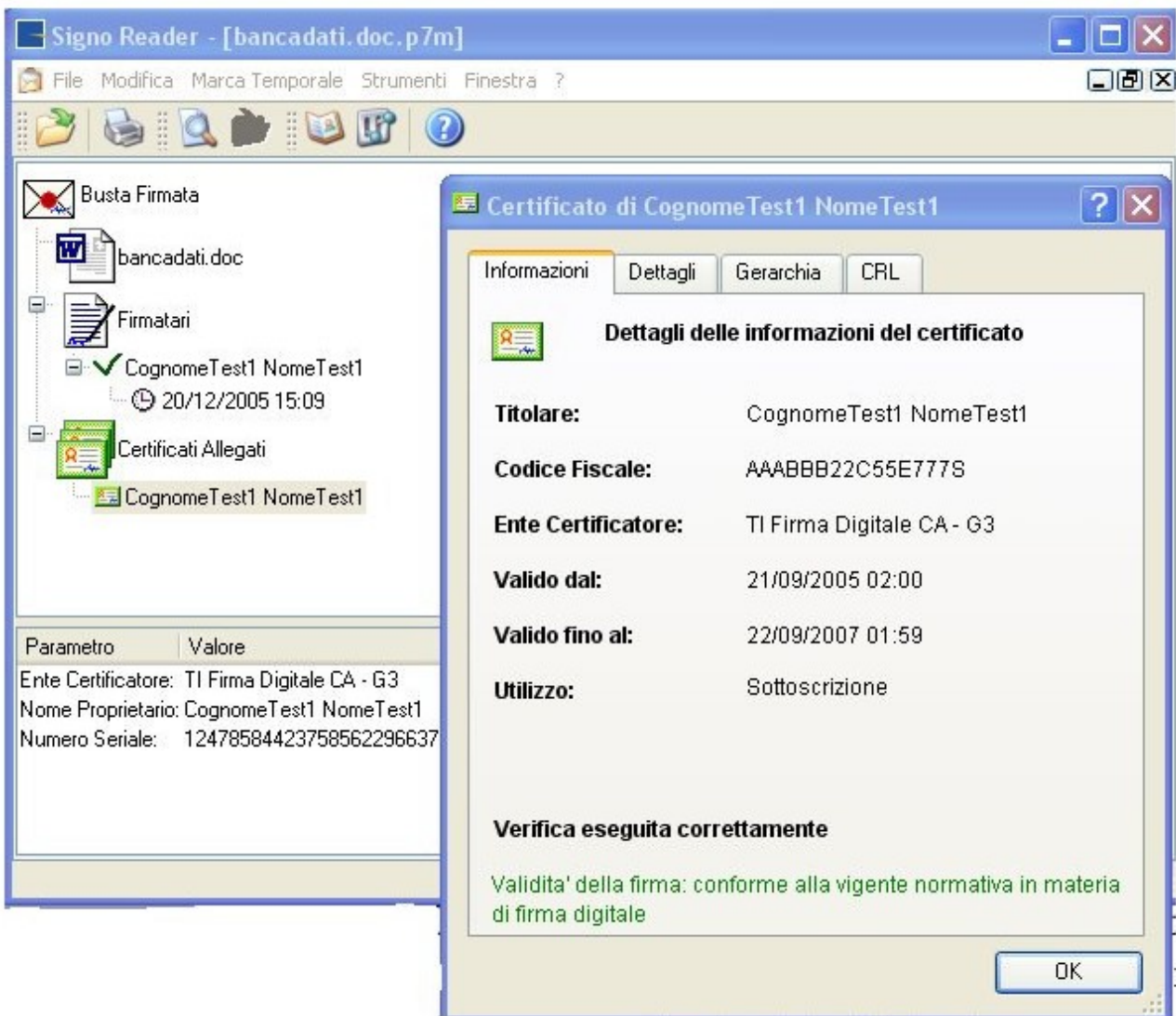
Il programma in questione è "Signo Reader" che si può scaricare cliccando al seguente indirizzo: <https://www.trustitalia.it>.

Come utilizzare Signo Reader :

- 1) Aprire il programma Signo Reader
- 2) Cliccare sulla prima cartella nella barre delle icone
- 3) Scegliere il file firmato (.p7m) di cui devi verificare l'integrità, provenienza ed identità del sottoscrittore
- 4) Apparirà la seguente schermata:



- 5) Il Download CRL (finestra popup) aggiornerà (e possibile) il registro dei certificati e ti consentirà di verificare che il certificato del sottoscrittore sia valido, non revocato o scaduto o sospeso. Occorre essere connessi ad Internet altrimenti la verifica non può essere effettuata (apparirà una croce rossa a fianco all'operazione fallita);
- 6) Per effettuare questa operazione di verifica esegui i seguenti controlli:
  - a) Chiudere la finestra popup del download CRL
  - b) Fare doppio clic sulla icona "Certificati Allegati"
  - c) Fare doppio clic sul "Cognome Nome" che apparirà subito sotto.



Ora impariamo a leggere un certificato:

Nel primo riquadro (Informazioni) troviamo le informazioni (cognome, codice fiscale, ..) attinenti al Titolare della Firma Digitale e dell'Ente che ha rilasciato il certificato;

In basso troviamo le dizioni che indicano che si tratta di una Firma forte (a valore legale)

- Utilizzo: Sottoscrizione
- Verifica eseguita correttamente
- Validità della firma: conforme alla vigente normativa...

Nel secondo riquadro (Dettagli) trovi altre informazioni importanti:

- Ruolo: è la professione auto certificata dal titolare
- Validità: periodo temporale di validità legale del certificato

I documenti firmati digitalmente riportano la data e l'ora dell'apposizione della Firma Digitale. I documenti firmati digitalmente entro il periodo di validità del certificato continuano a mantenere validità legale anche dopo la scadenza del certificato.

Nel terzo riquadro (Gerarchia) appare il certificatore che ha rilasciato il certificato

Nel quarto riquadro (CRL – Lista dei certificati revocati) vi è la possibilità di accedere ad Internet per andare a verificare la validità del certificato in tempo reale (cliccare su “Aggiorna CRL”) nella Lista dei certificati tenuti in costante aggiornamento dai certificatori accreditati CNIPA; quest'ultima operazione dovrebbe essere stata già effettuata (download CRL) se connessi correttamente ad Internet.

E finalmente....

Si può ora aprire il file con un doppio clic.

Verrà richiamata l'applicazione che lo ha generato (word processor, database, foglio elettronico, gestore immagini, file pdf....) e che è presente nel PC.

*(nдр: teniamo presente che tutti i file che ci vengono inviati dall'A.d.T. sono in formato pdf – quindi facilmente visionabili con Acrobat Reader – con l'unica eccezione del file originario del Docfa che essendo in formato compresso dc3 dovrà essere scaricato sul computer e aperto con il Docfa stesso)*

Studiando l'argomento per la redazione di queste note ho capito che:

I file che noi inviamo all'A.d.T. e che questa a sua volta ci invia non sono “crittografati” ma semplicemente “firmati”.

Pertanto, la firma digitale:

- Garantisce l'autenticità del mittente
- Garantisce l'integrità dei dati trasmessi
- Garantisce la non ripudiabilità di un documento (anche la data di apposizione della firma)
- Se il certificato digitale è rilasciato da una CA riconosciuta dal CNIPA, la firma ha valore legale ed è equipollente alla firma autografa.
- Non garantisce la riservatezza dei dati