firma4ng

Manuale d'uso

www.bit4id.com

Sommario

1. Introduzione

Il presente manuale d'uso descrive le principali funzionalità dell'applicazione di firma digitale ***firma4ng***. In particolare, il documento si propone di supportare l'utente nello svolgimento delle seguenti operazioni:

- Apposizione di firme digitali in formato .P7M
- Apposizione di firme digitali in formato .PDF
- Apposizione di firme digitali in formato .XML
- Apposizione di marche temporali
- Verifica di firme digitali in formato .P7M
- Verifica di firme digitali in formato .PDF
- Verifica di firme digitali in formato .XML
- Verifica di marche temporali
- Cifratura e decifratura di file
- Creazione di cartelle cifrate
- Gestione PIN e PUK del dispositivo crittografico (smart card o token USB)

2. Caratteristiche del software

2.1 Distribuzioni disponibili e requisiti

L'applicazione *firma4ng* viene distribuita nelle seguenti versioni:

- *firma4ng* per Windows, installazione disponibile per ambienti desktop Windows 7, Windows 8.1, Windows 10 (32 che 64 bit);
- *firma4ng* per Mac OS X, installazione disponibile per ambienti desktop Mac OS X (10.12.X, 10.13.X, 10.14.X e superiori);
- *firma4ng* per Linux 32, distribuito come archivio tar.gz per ambienti desktop Linux (Ubuntu 18.04 LTS);
- *firma4ng* per Linux 64, distribuito come archivio tar.gz per ambienti desktop (Ubuntu 18.04 LTS).

Uso via USB (PC)

Requisiti HW

- Porta USB disponibile
- Connettività Internet

Requisiti SW

- MS Windows 7 | 8 | 8.1 | 10
- Mac OSx 10.12.X (Sierra)
- Mac OSx 10.13.X (High Sierra)
- Mac OSx 10.14.X (Mojave)
- Linux 18.04 LTS

Uso via Bluetooth (PC)

Requisiti HW

- Bluetooth 4.1 o superiore

Requisiti SW

- MS Windows 10 (versione 17.03)
- Mac OSx 10.14.X (Mojave)

2.2 Requisiti di sistema

Prima di utilizzare *firma4ng*, a garanzia del corretto funzionamento dell'applicazione, è bene verificare:

- La disponibilità di connessione Internet;
- La possibilità di instaurare connessioni HTTP, HTTPS e LDAP.

Inoltre, per una corretta visualizzazione, si suggerisce di impostare una risoluzione dello schermo pari almeno a 1024x768.

2.3. Installazione Windows

Per installare l'applicazione su sistemi operativi Windows (a 32 e 64 bit), avviare il programma di installazione (con estensione "**.exe**") con doppio click e seguirne tutti i passi.

Occorre accettare, per presa visione, le condizioni ed i termini di utilizzo per poter procedere con l'installazione di firma4ng.

2.4. Installazione Mac OS X

Per installare l'applicazione su sistemi operativi Mac OS X avviare il programma di installazione individuato dall'estensione "**.pkg**" e seguirne tutti i passi.

Occorre accettare, per presa visione, le condizioni ed i termini di utilizzo per poter procedere con l'installazione di firma4ng.

2.5. Installazione Linux

Per installare l'applicazione su sistemi operativi Linux (32 e 64 bit) occorre estrarre il contenuto dell'archivio individuato dal file con estensione "**.tar.gz**" nella home dell'utente ed eseguire lo script setup.run con opzione i ("*setup.run –i*") e seguire le opzioni a video.

2.6 Aggiornamento automatico

Il software *firma4ng* è dotato della funzionalità di aggiornamento automatico: ad ogni avvio dell'applicativo viene effettuato un controllo sulla disponibilità di nuove versioni e, a seguito dell'autorizzazione da parte dell'utente, viene effettuato l'aggiornamento.

Tale funzionalità è attiva se il PC è collegato ad Internet.

3. Menu

Una volta completata l'installazione, è sufficiente fare doppio click sull'icona di avvio per aprire il programma di firma digitale. Apparirà sullo schermo il menu principale di *firma4ng* (Figura 1), da cui accedere alle diverse funzioni dell'applicazione.

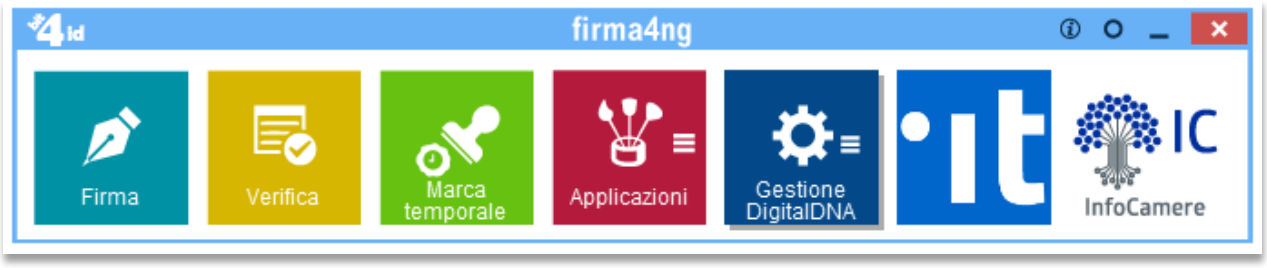


Figura 1

Il menu contiene le seguenti voci:

- Firma
- Verifica
- Marca Temporale
- Applicazioni
- Gestione DigitalDNA
- Cassetto digitale dell'imprenditore

Nota: prima di avviare una delle operazioni, controllare di aver inserito correttamente la DigitalDNA Key.

4. Firma digitale

La funzione **"Firma digitale"** permette di firmare digitalmente uno o più documenti con certificati digitali.

Fase 1

A partire dal menu principale (Figura 1), è possibile avviare l'operazione di Firma attraverso una delle seguenti modalità:

- Selezionando e trascinando uno o più documenti sul pulsante "Firma" presente nel menu principale (drag&drop);

- Cliccando sul pulsante "Firma" presente nel menu principale e selezionando uno o più documenti da firmare dalla finestra di navigazione del PC (Figura 2).

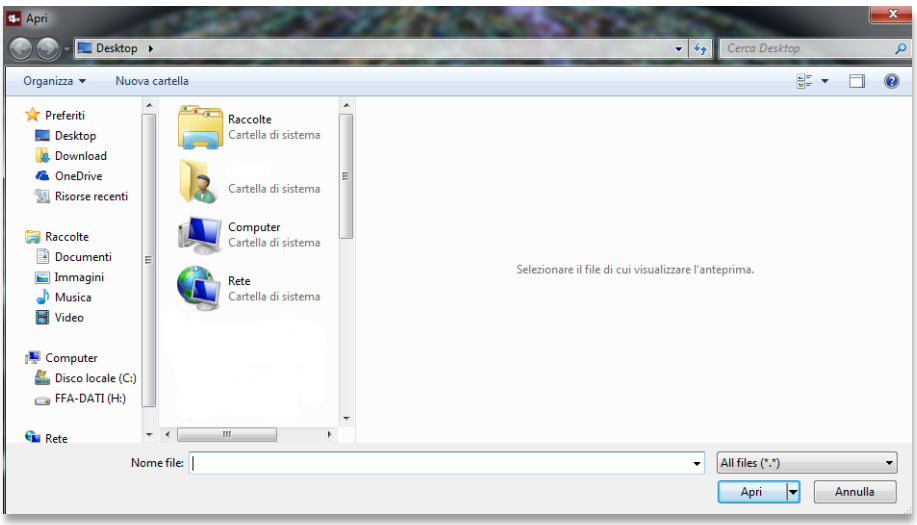


Figura 2

Fase 2

Attendere il caricamento dei certificati (Figura 3).

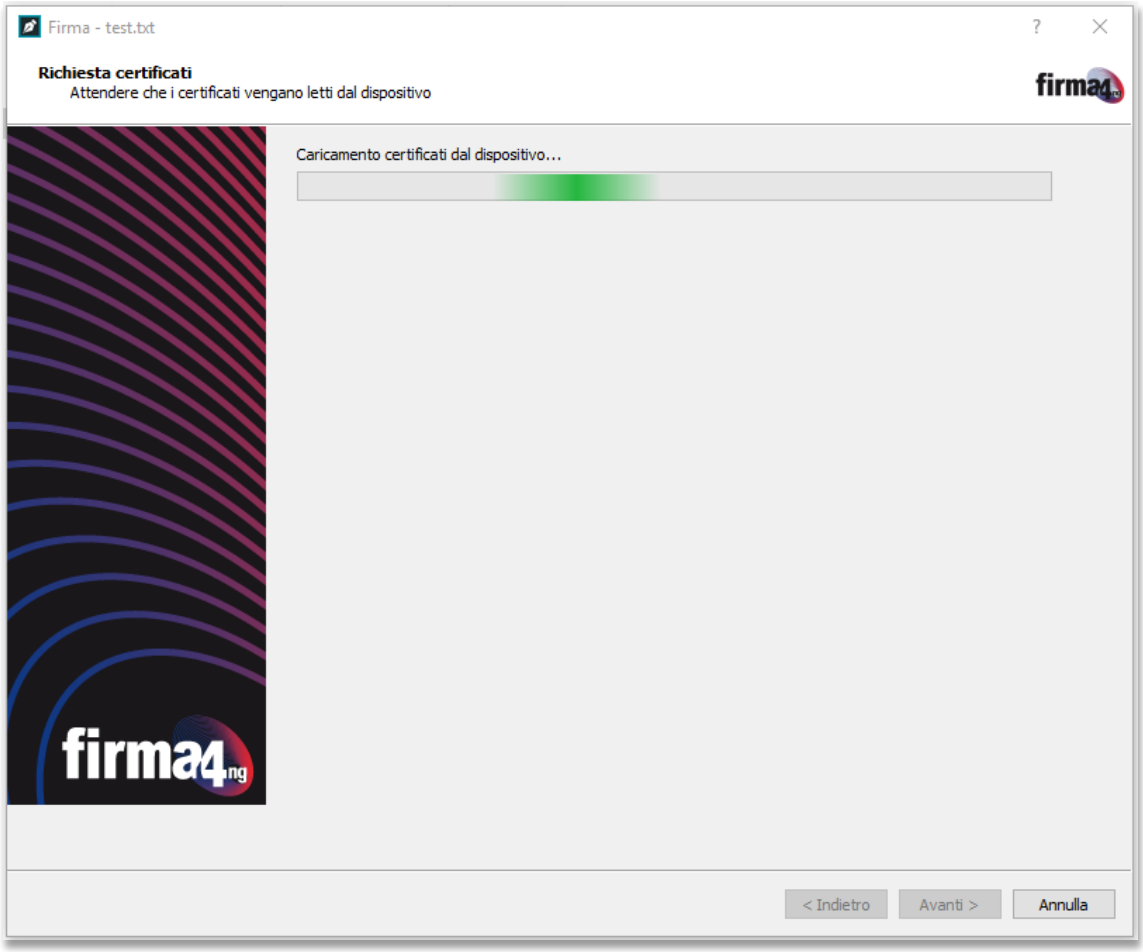


Figura 3

Fase 3 (FIRMA P7M o XML)

Al termine del caricamento dei certificati, si apre la finestra di configurazione in cui inserire i parametri e le preferenze da applicare alla firma che si sta effettuando (Figura 4):

Seleziona il certificato: risulterà automaticamente selezionato il certificato di firma digitale a validità legale (o di "non ripudio") identificato da Nome e Cognome dell'intestatario. Per utilizzare un certificato diverso da quello preimpostato, selezionare una voce dal menu a tendina.

Inserisci il PIN: inserire il PIN riportato sul retro della Secret Card.

Salva come: selezionare la cartella in cui salvare il documento firmato cliccando sul pulsante "...". Lasciando invariato questo campo, il file firmato verrà salvato automaticamente nella stessa cartella in cui si trova il file originale non firmato.

Questa sezione riporta due opzioni facoltative da attivare/disattivare:
Cifra il documento al termine della firma
Distruggi il documento al termine della firma

Tipologia di firma: selezionare dal menu a tendina la tipologia di firma che si vuole apporre al documento. I formati di firma disponibili sono:

- *Busta crittografica P7M (CAdES)* - formato valido per qualunque tipo di documento;
- *Documento XML* – formato valido per qualunque tipo di documento (eccetto quando l'operazione di firma viene lanciata dai pulsanti "Aggiungi firma" o "Aggiungi controfirma" presenti nella schermata di "Verifica");

Richiedi Timestamp: attivare l'opzione per aggiungere una marca temporale alla firma che si sta effettuando. Selezionare dal menu a tendina il formato con cui si vuole apporre la marca digitale al documento (formato .M7M, .TSD o .P7M).

Questa sezione riporta due opzioni facoltative da attivare/disattivare:
Codifica in Base64
Separa la firma dal documento (firma "detached")

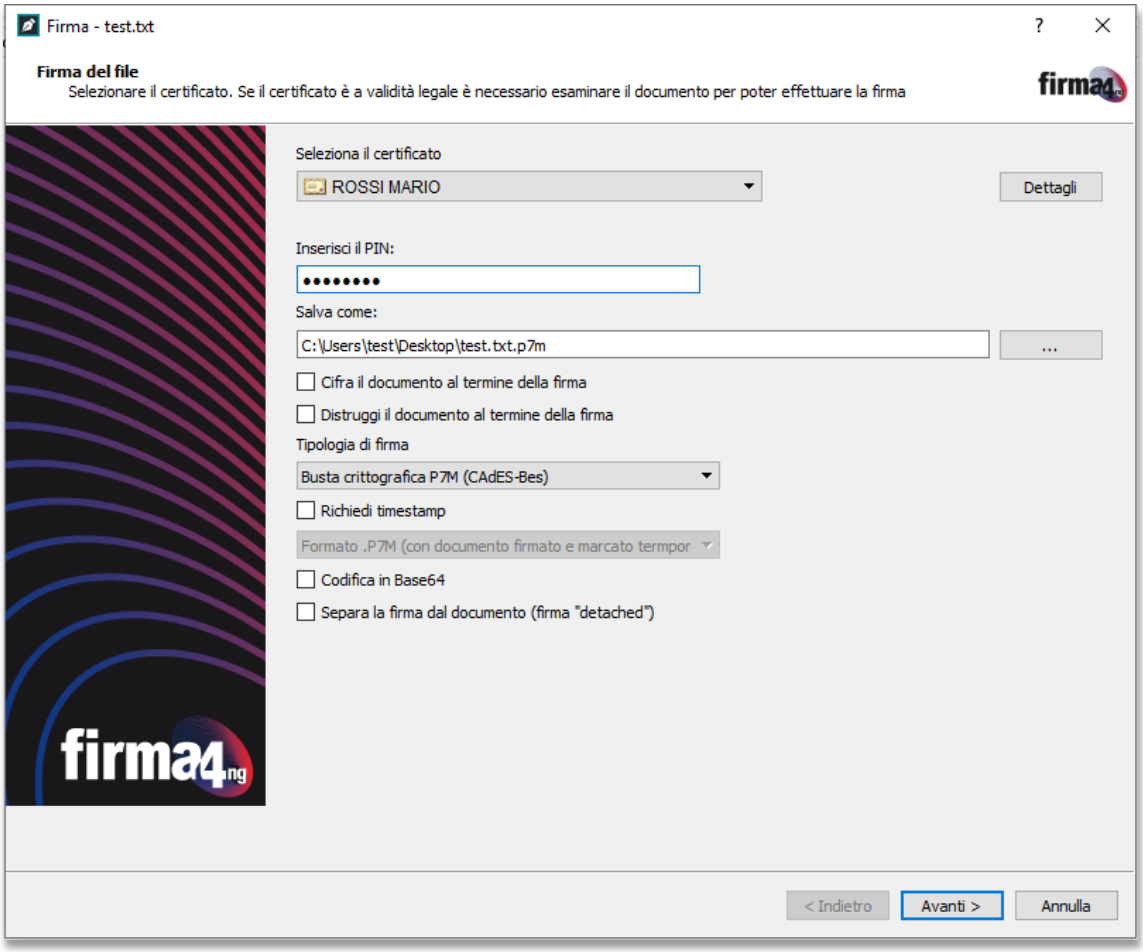


Figura 4

Al termine delle modifiche, cliccare su "Avanti" per proseguire.

Fase 3 (FIRMA PDF)

Questa configurazione riguarda solo la firma PDF. Si tratta infatti di un formato valido solo nel caso in cui il documento da firmare sia un file PDF.
Al termine del caricamento dei certificati (Figura 3), appare la finestra di configurazione in cui inserire parametri e preferenze da applicare alla firma che si sta effettuando (Figura 5):

Seleziona il certificato: risulterà automaticamente selezionato il certificato di firma digitale a validità legale (o di "non ripudio") identificato da Nome e Cognome dell'intestatario. Per utilizzare un certificato diverso da quello preimpostato, selezionare una voce dal menu a tendina.

Inserisci il PIN: inserire il PIN riportato sul retro della Secret Card.

Salva come: selezionare la cartella in cui salvare il documento firmato cliccando sul pulsante "...". Lasciando invariato questo campo, il file firmato verrà salvato automaticamente nella stessa cartella in cui si trova il file originale non firmato.

Questa sezione riporta due opzioni facoltative da attivare/disattivare:
Cifra il documento al termine della firma
Distruggi il documento al termine della firma

Tipologia di firma: selezionare dal menu a tendina la tipologia di firma che si vuole apporre al documento. I formati di firma disponibili sono:

- *Busta crittografica P7M (CAdES)* - formato valido per qualunque tipo di documento;
- *Aggiungi la firma al PDF* - formato selezionabile solo nel caso in cui il documento da firmare sia un file PDF (anche nella modalità di firma di più documenti, questo formato sarà presente solo se tutti i documenti selezionati sono esclusivamente documenti PDF);
- *Documento XML* – formato valido per qualunque tipo di documento (eccetto quando l'operazione di firma viene lanciata dai bottoni "Aggiungi firma" o "Aggiungi controfirma" presenti nella schermata di "Verifica");

Richiedi Timestamp: attivare l'opzione per aggiungere una marca temporale alla firma che si sta effettuando.

Scegliere come rappresentare la firma nel documento PDF selezionando una delle opzioni:
Firma invisibile: il PDF verrà firmato senza aggiungere alcun dettaglio di tipo "grafico" al documento;
Firma grafica (modalità avanzata): è possibile selezionare la posizione della firma ed eventualmente aggiungere un'immagine (opzione non disponibile per firma multipla di più documenti PDF);
Firma grafica (con opzioni di default): il PDF verrà firmato aggiungendo i dettagli e la grafica definiti nella sezione "Firma PDF" del menu "Opzioni" (par. 6.1.4); sarà comunque possibile modificare le impostazioni spuntando la casella "Modifica opzioni" e personalizzando al momento le opzioni di firma PDF.

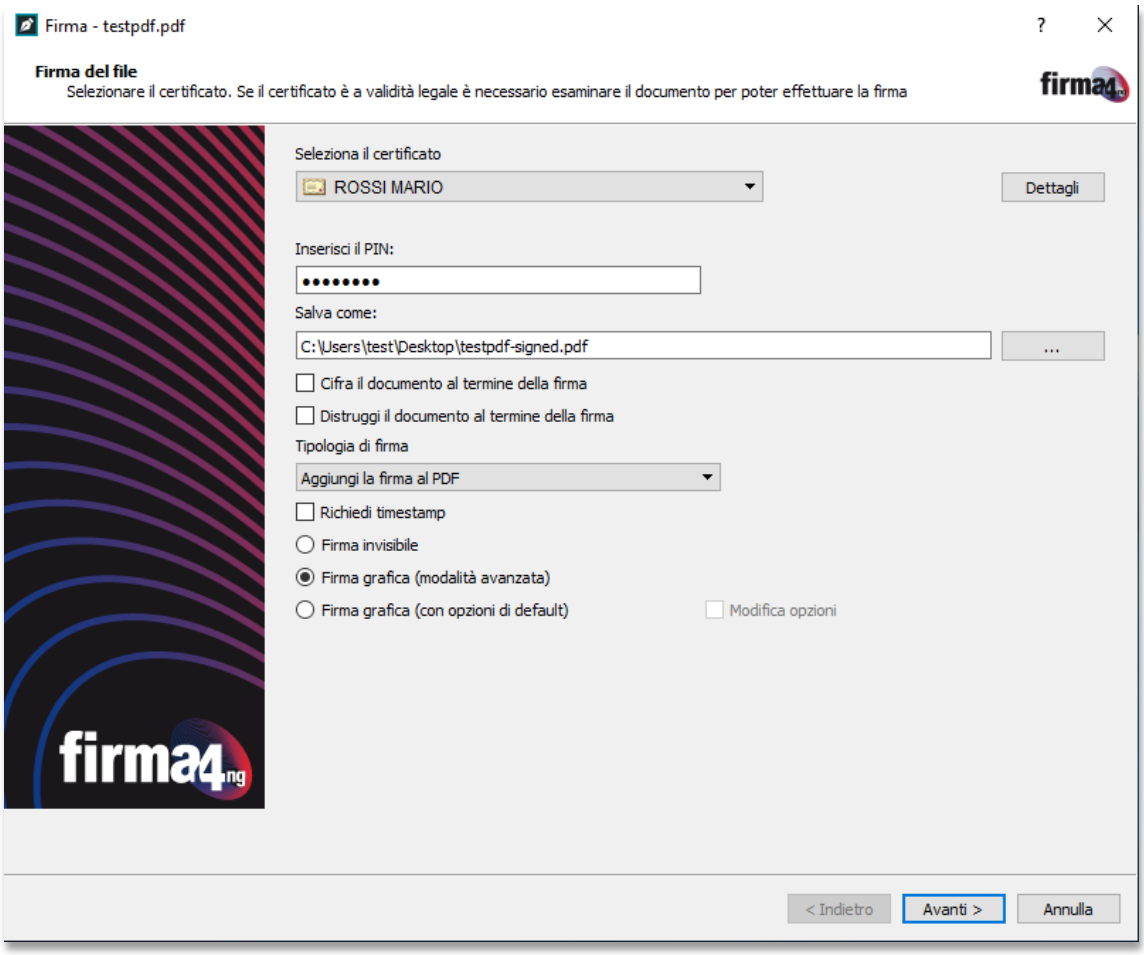


Figura 5

Al termine delle modifiche, cliccare su "Avanti" per proseguire.

Fase 4 (FIRMA P7M o XML)

Nel caso in cui si stia firmando un singolo documento, occorre prendere visione del contenuto del documento che si sta per firmare cliccando sul pulsante "*Apri documento*". Quindi selezionare la checkbox "Dichiaro di aver preso visione del documento, di sottoscriverne il contenuto e di essere consapevole della validità ai sensi della legge della firma apposta." e cliccare su "Avanti" (Figura 6).

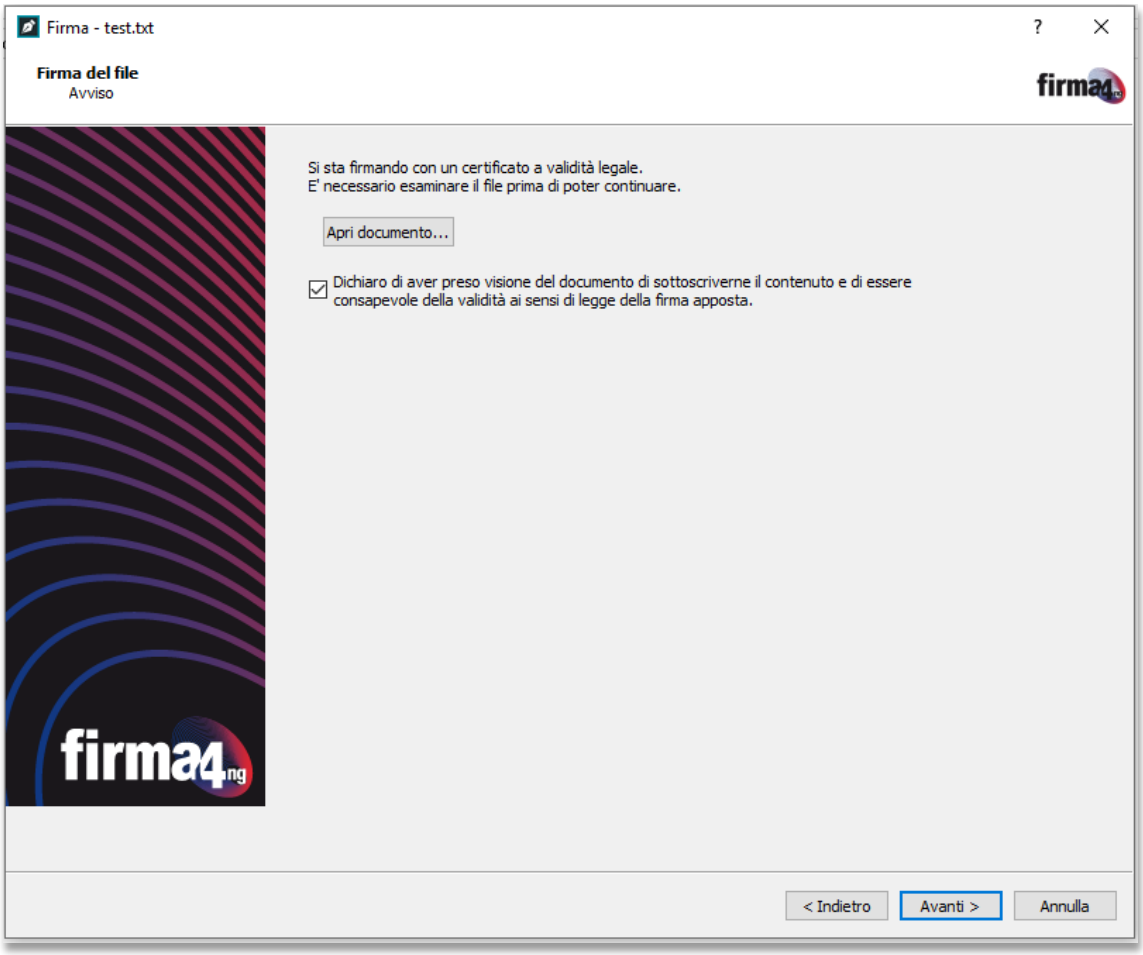


Figura 6

Fase 4 (FIRMA PDF)

Nel caso in cui si stia firmando un singolo documento, occorre prendere visione del contenuto del documento che si sta per firmare cliccando sul pulsante "*Apri documento*". Quindi selezionare la checkbox "Dichiaro di aver preso visione del documento, di sottoscriverne il contenuto e di essere consapevole della validità ai sensi della legge della firma apposta." e cliccare su "Avanti" (Figura 6).

- Se nella Fase 3 è stata selezionata l'opzione **"Firma grafica (modalità avanzata)"** verrà mostrata la schermata per la selezione e il posizionamento della grafica (Figura 7):

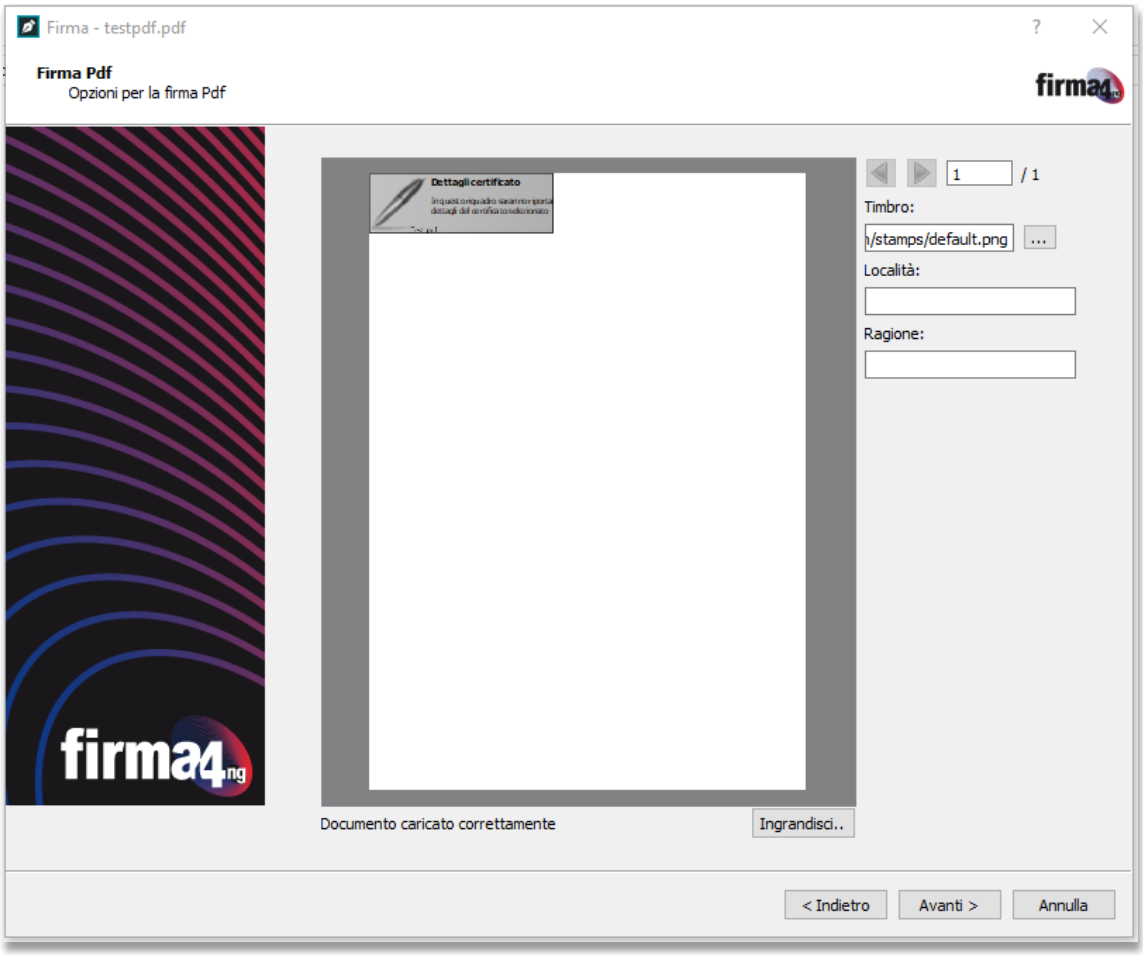


Figura 7

In questa schermata è possibile:

a. Sfogliare le pagine del documento per scegliere dove apporre la firma;
b. Selezionare un'immagine da associare alla firma (facoltativo);
c. Inserire i campi "Località" e "Ragione" da aggiungere alla firma (facoltativo).

- Se nella Fase 3 è stata selezionata l'opzione **"Firma grafica (con opzioni di default)"** con la spunta sulla voce "Modifica opzioni" verrà mostrata la schermata in cui modificare gli standard della firma grafica (Figura 8).

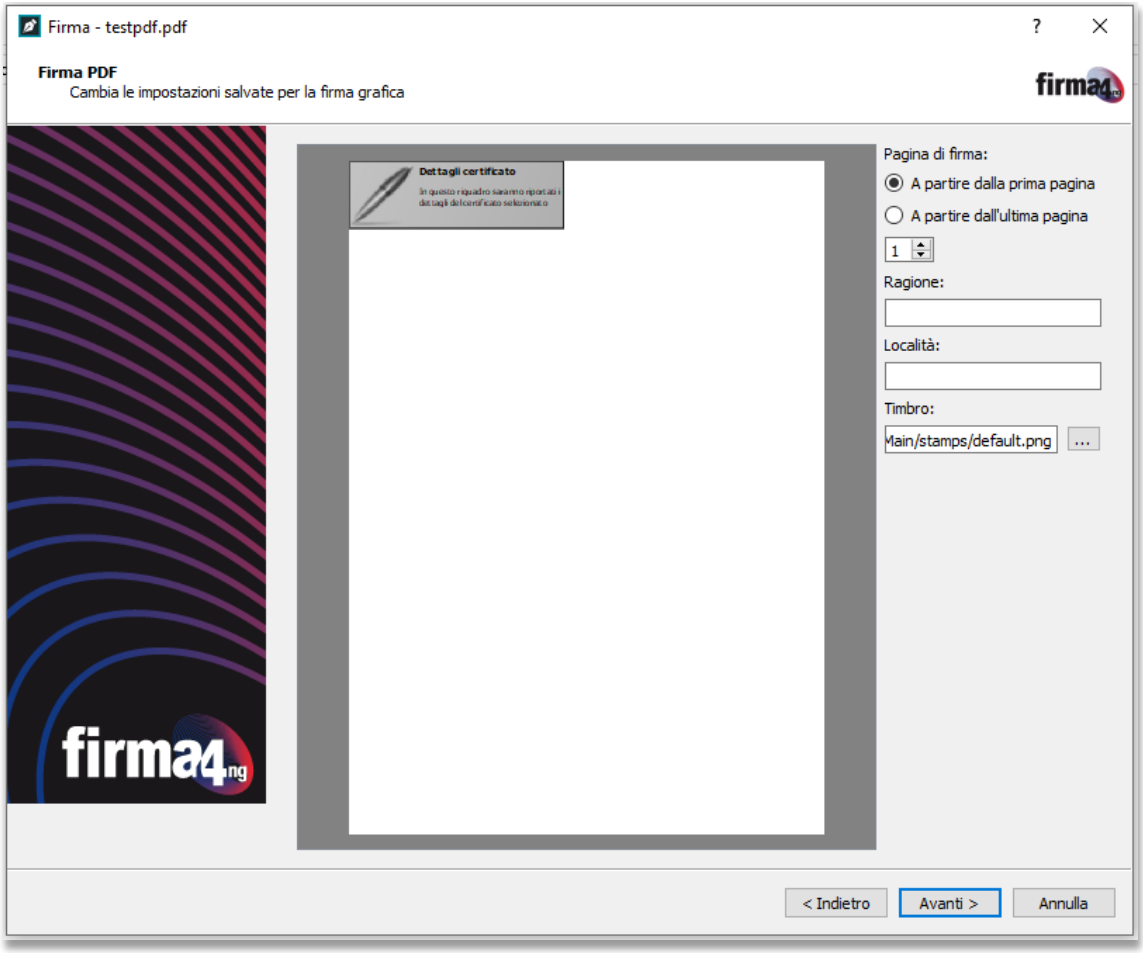


Figura 8

In questa schermata è possibile modificare/inserire:

a) la posizione della firma
b) le dimensioni della firma grafica da apporre
c) la pagina del documento su cui apporre la firma
d) la Ragione e Località
e) l'immagine da includere nella firma.

Al termine delle modifiche, cliccare su "Avanti" per proseguire.

Fase 5

Al termine dell'operazione di firma, il documento firmato viene salvato sul PC, al percorso indicato nella schermata "Operazione conclusa" (Figura 9). Cliccando sul percorso del documento firmato si avvia automaticamente l'operazione di "Verifica" della firma digitale.

Per chiudere la schermata, cliccare su "Termina".

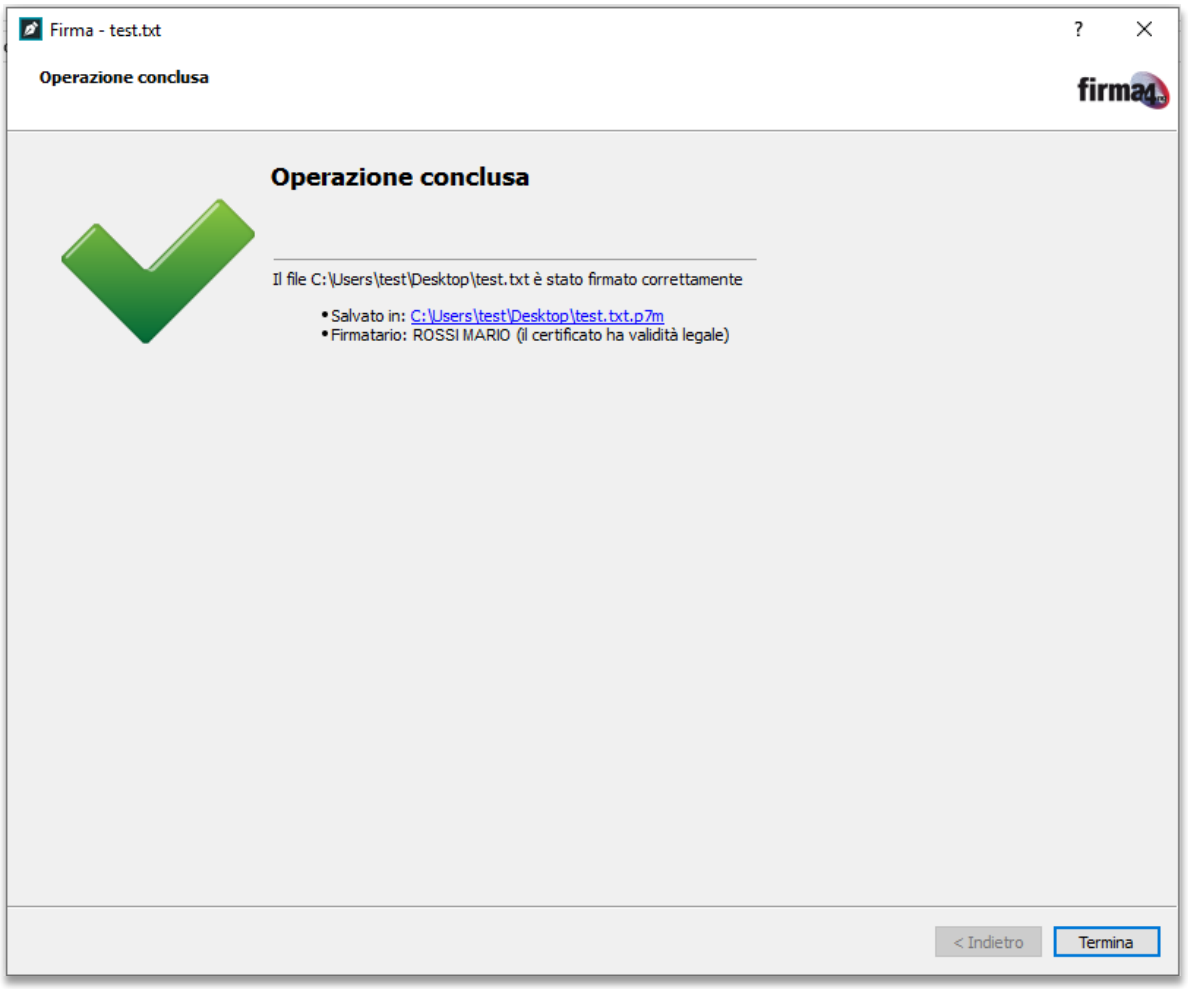


Figura 9

Verifica

La funzione **"Verifica"** permette di verificare la validità di un file firmato e/o marcato temporalmente.

Fase 1

A partire dal menu principale (Figura 1), è possibile avviare l'operazione di Verifica attraverso una delle seguenti modalità:

- Selezionando e trascinando il documento sul pulsante "Verifica" presente nel menu principale (drag&drop);
- Cliccando sul pulsante "Verifica" presente nel menu principale e selezionando il documento da verificare dalla finestra di navigazione del PC (Figura 10).

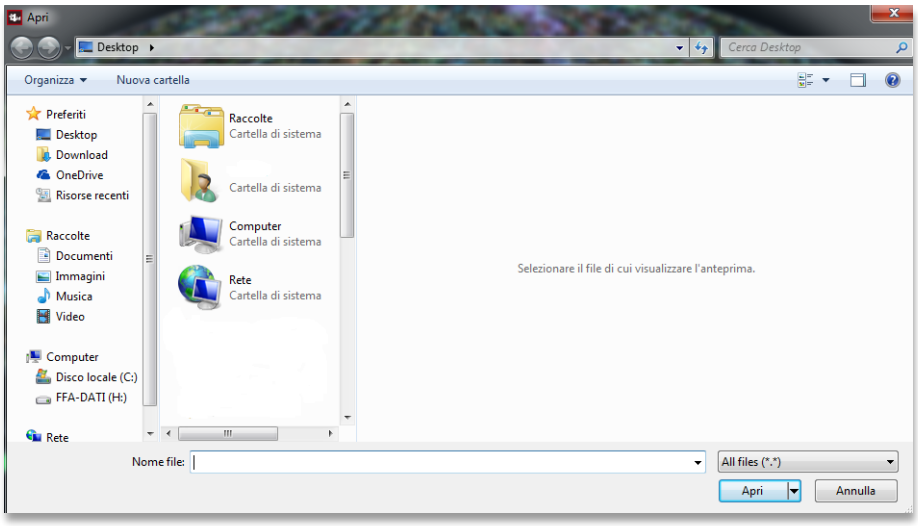


Figura 10

Fase 2

Attendere il completamento dell'operazione. Al termine dell'analisi, la schermata riporta l'esito della verifica (Figura 11).

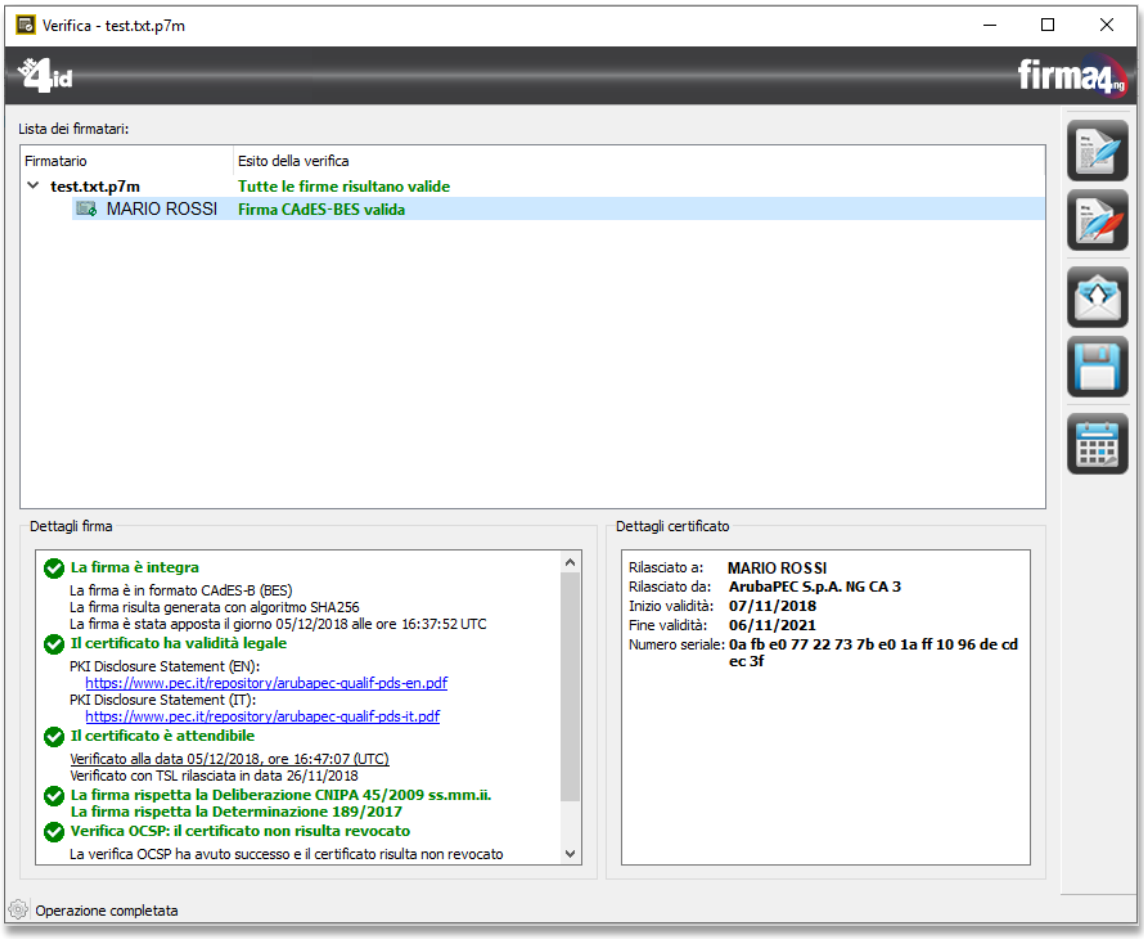


Figura 11

- Nella sezione in alto viene mostrato l'elenco delle firme (ed eventuali marche temporali) apposte sul documento. Sono riportati anche i certificati dei firmatari del documento (Figura 12). E' possibile visualizzare i dettagli di un certificato con un doppio click su ognuno di essi.

Figura 12

- Nella sezione in basso a sinistra della schermata sono mostrati i dettagli delle verifiche effettuate su una specifica firma/marca temporale (Figura 13):

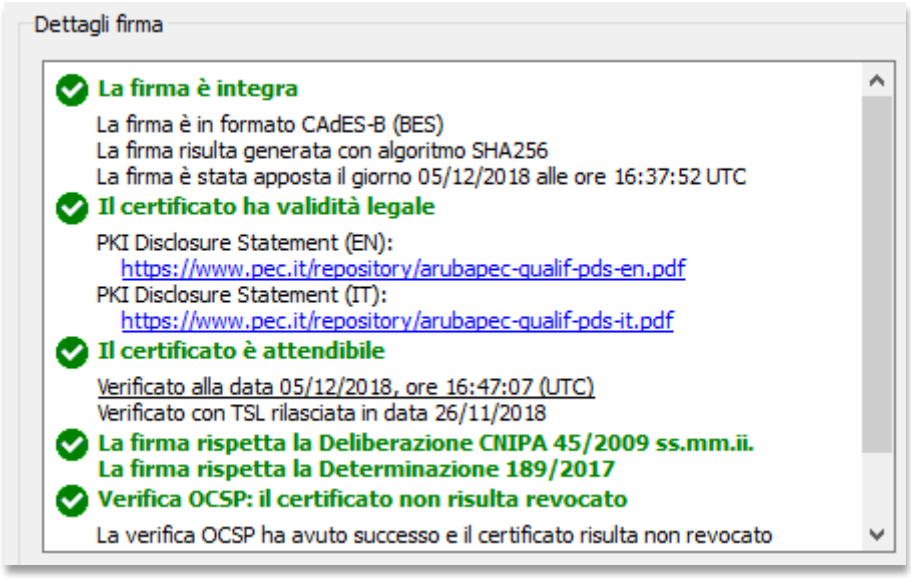


Figura 13

Integrità: viene mostrato l'esito della verifica di integrità del documento firmato, per controllare che non sia stato alterato dopo la firma. Vengono inoltre visualizzati i dettagli relativi al formato di firma, l'algoritmo utilizzato e la data in cui è stata realizzata la firma. In caso di esito positivo viene mostrato il messaggio: "La firma è integra".

Validità legale: viene mostrato l'esito del controllo effettuato sull'attributo del certificato (Key Usage) che ne definisce l'utilizzo. Per la normativa italiana, il certificato di firma digitale deve avere il Key Usage valorizzato con il solo valore "Non Repudiation". In caso di esito positivo viene mostrato il messaggio: "Il certificato ha validità legale".

Attendibilità: viene mostrato l'esito del controllo effettuato sul Certificatore che ha emesso il certificato del firmatario. In caso di esito positivo, ossia nel caso in cui il Certificatore emittente sia presente nella lista dei Certificatori Accreditati presso l'AgID (Agenzia per l'Italia Digitale), viene mostrato il messaggio: "Il certificato è attendibile".

Aderenza alle Regole Tecniche previste dalla Normativa vigente: viene mostrato l'esito del controllo relativo all'aderenza e al rispetto della Normativa Vigente. In caso di esito positivo viene mostrato il messaggio: "La firma rispetta la Deliberazione CNIPA 45/2009 ss.mm.ii". La firma rispetta la Determinazione 189/2017".

Stato di revoca/sospensione del certificato: viene mostrato l'esito del controllo sullo stato di validità del certificato, per verificare che non sia scaduto temporalmente e, attraverso le CRL (Certificate Revocation Lists), che non sia stato sospeso o revocato. Se lo stato del certificato è valido viene mostrato il messaggio: "Il certificato non risulta revocato".

- Nella sezione in basso a destra vengono mostrati i dettagli del certificato con cui è stato firmato il documento selezionato (Figura 14).

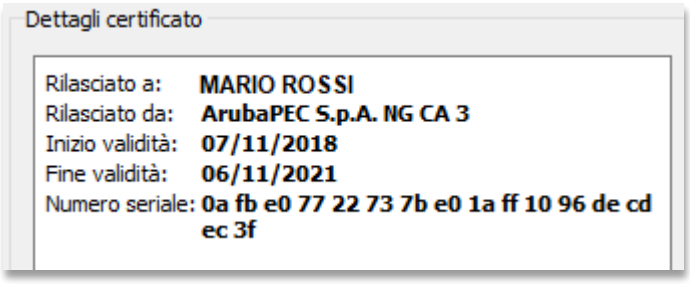


Figura 14

Fase 3

Dal menu verticale presente sul bordo destro della schermata di Verifica (Figura 11), è possibile effettuare le seguenti operazioni:

Aggiungi firma:

Per aggiungere un'ulteriore firma al documento.

Aggiungi controfirma:

Per aggiungere una controfirma alla firma selezionata.

Apri contenuto:

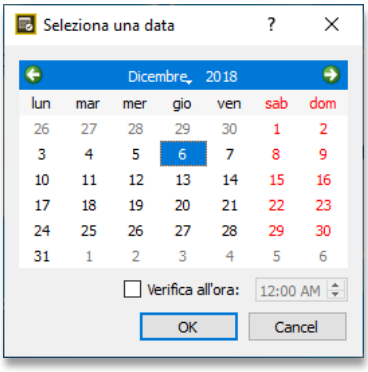
Per visualizzare il contenuto del documento firmato o marcato temporalmente.

Salva contenuto:

Per salvare il documento originale oggetto della verifica. Nel caso in cui si stia verificando una marca temporale apposta al documento, questa funzione è disponibile solo se il formato della marca temporale è ".tsd".

Verifica alla data:

Per effettuare la verifica a una specifica data selezionata. Cliccando sul pulsante si apre un calendario da cui selezionare una data (se il documento firmato contiene delle firme marcate temporalmente, la verifica di tali firme viene sempre effettuata alla data indicata nella marca temporale).



5. Marca temporale

La funzione **"Marca temporale"** permette di apporre una marca temporale su un documento. Il software *firma4ng* supporta tutti formati di marche temporali previsti dagli standard e dalla normativa Nazionale attualmente in vigore.

Fase 1

A partire dal menu principale (Figura 1), è possibile avviare l'operazione di Marca temporale attraverso una delle seguenti modalità:

- Selezionando e trascinando il documento sul pulsante "Marca temporale" presente nel menu principale (drag&drop);

• Cliccando sul pulsante "Marca temporale" presente nel menu principale e selezionando il documento da verificare dalla finestra di navigazione del PC (Figura 15).

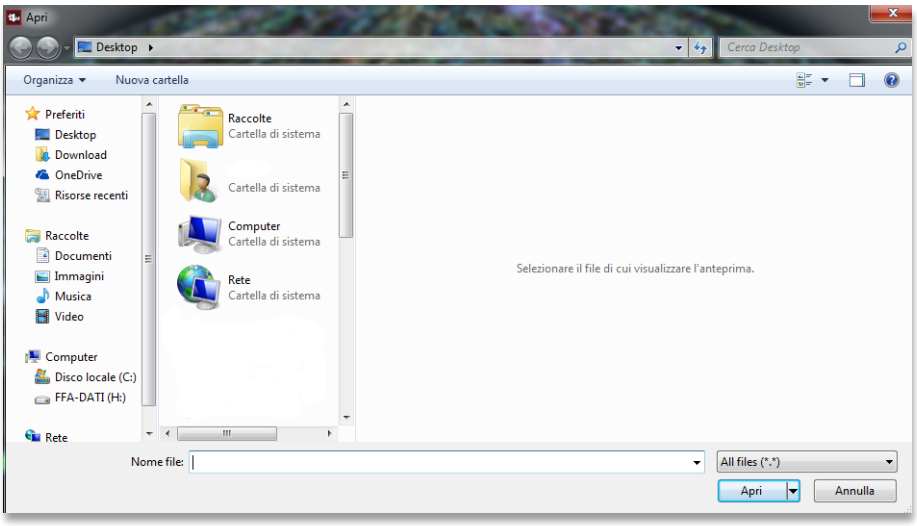


Figura 15

Nota: è possibile appore una marca temporale anche contestualmente all'operazione di firma (paragrafo 4 fase 3).

Fase 2

Dopo aver selezionato il documento, appare una finestra (Figura 16) nella quale indicare:

Servizio di marcatura temporale da utilizzare;

Username;

Password;

Cartella di destinazione;

Formato della marca temporale tra quelli presenti nel menu a tendina:

- .M7M: unisce al suo interno sia il documento elettronico firmato (di tipo .p7m), che la relativa Marca Temporale (in formato .tsr);
- .TSD: formato che racchiude il documento originale e la marca temporale;
- .TSR: formato che racchiude la sola marca temporale;
- .TST: formato che racchiude la sola marca temporale;
- .PDF: inglobando la marca temporale nel file pdf in cui è apposta la firma.

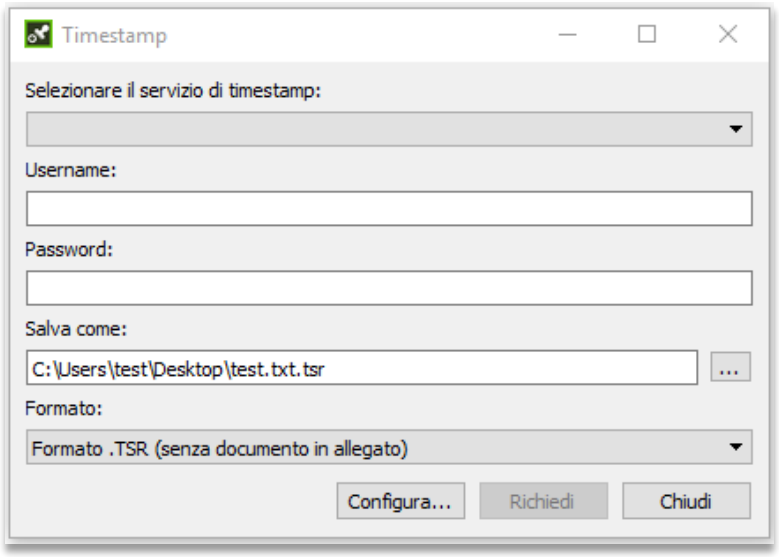


Figura 16

L'operazione di marcatura temporale necessita della connessione a Internet in quanto per completare tale operazione *firma4ng* comunica con il servizio di Timestamp selezionato. È possibile modificare la configurazione cliccando sul pulsante "Configura".

Al termine delle modifiche, cliccare sul pulsante **"Richiedi"** per inviare la richiesta di marcatura temporale.

Fase 3

Al termine dell'operazione di marcatura temporale, appare un messaggio con l'esito dell'operazione. Cliccare su "OK" per chiudere il messaggio; per chiudere la finestra "Timestamp" cliccare su "Chiudi".

6. Applicazioni

Cliccando sul pulsante **"Applicazioni"** presente nel menu principale (Figura 1) si apre un menu secondario che contiene le seguenti voci (Figura 17):

- Cifra
- Decifra
- Cartella cifrata
- Impostazioni

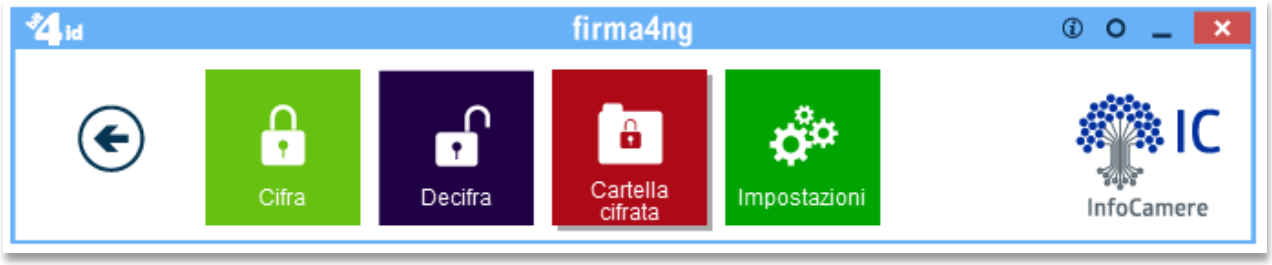


Figura 17

6.1 Cifratura

Al pulsante **"Cifra"** corrisponde la funzione di cifratura di uno o più documenti.

Fase 1

A partire dal menu secondario "Applicazioni" (Figura 17), è possibile avviare l'operazione di cifratura attraverso una delle seguenti modalità:

- Selezionando e trascinando il documento sul pulsante "Cifra" presente nel menu secondario (drag&drop);
- Cliccando sul pulsante "Cifra" presente nel menu secondario e selezionando il documento da verificare dalla finestra di navigazione del PC (Figura 18).

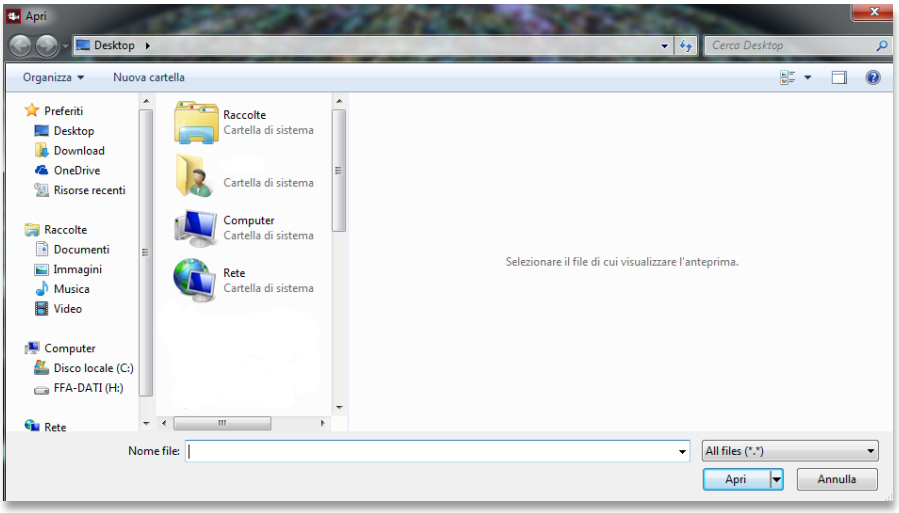


Figura 18

Fase 2

Attendere il caricamento dei certificati. Terminato il caricamento, i certificati vengono visualizzati nella schermata all'interno della sezione **"Contatti"** (Figura 19).

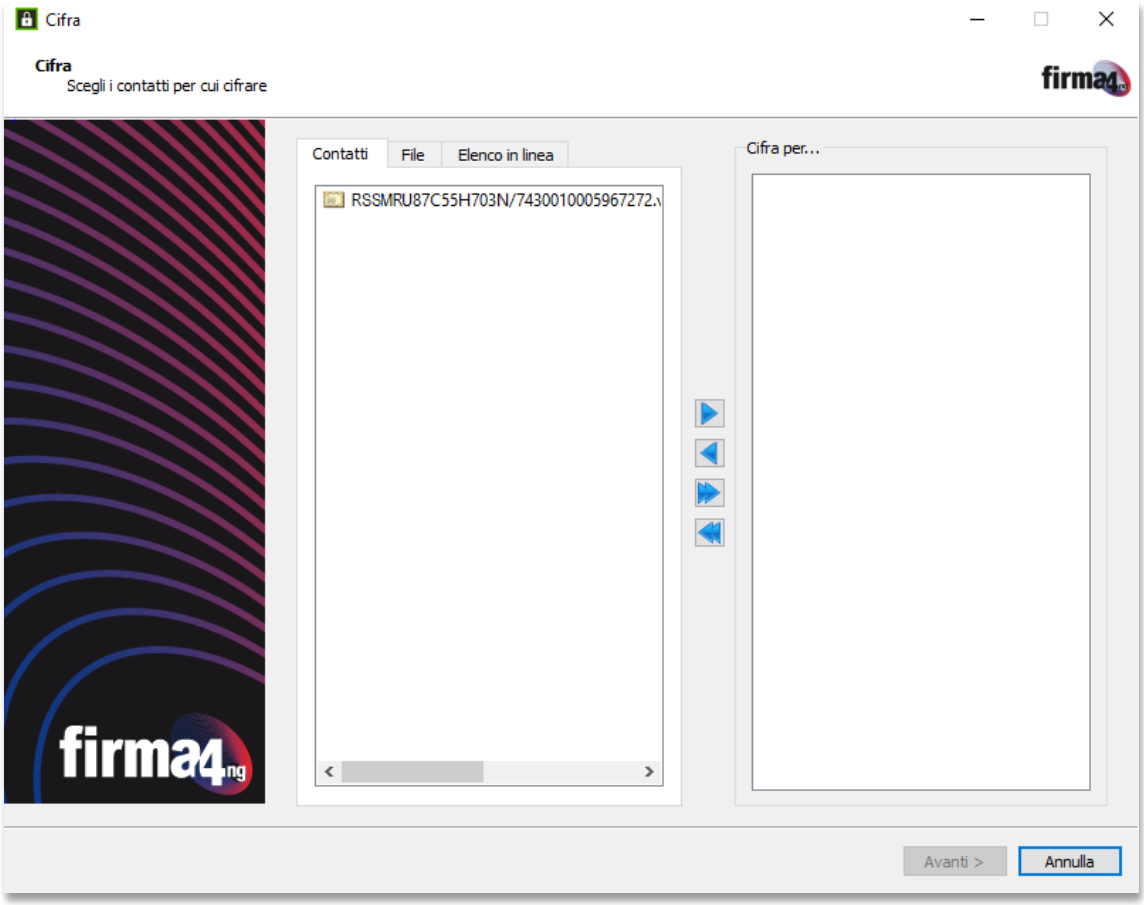


Figura 19

La rubrica di contatti permette di memorizzare i certificati dei contatti per i quali cifrare un documento.
Se si desidera cifrare un documento per un destinatario specifico, è possibile importare contatti all'interno della rubrica sia caricandoli dal PC, sia ricercandoli sul Registro pubblico dei certificati gestito dal Certificatore, tramite le seguenti modalità:

File

Per inserire nella rubrica dei Contatti un destinatario il cui certificato è disponibile su file, dalla sezione "File" cliccare su "Importa da file" e scegliere il certificato (.cer) da importare (Figura 20).
Una volta che il file del certificato è stato correttamente 'caricato', cliccando con il tasto destro del mouse su di esso e scegliendo "Aggiungi ai contatti...", il contatto verrà inserito nei "Contatti personali" (Figura 22).

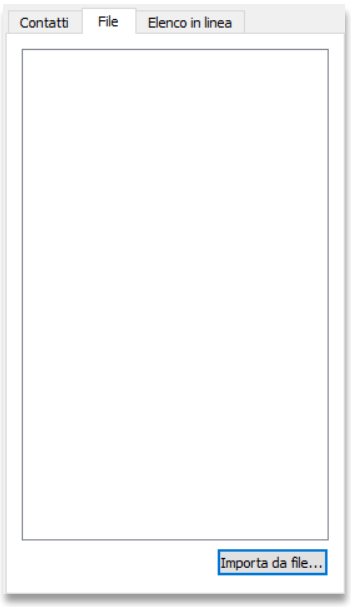


Figura 20

Elenco in linea

È possibile importare il certificato di un contatto cercandolo sul Registro pubblico dei certificati gestito dal Certificatore, impostando i parametri di ricerca presenti nella sezione e cliccando su "Cerca" (Figura 21).
Al termine della ricerca, nel riquadro in basso verrà mostrata la lista dei certificati ottenuti come risultato. Dopo aver selezionato il certificato di interesse, cliccando con il tasto destro del mouse su di esso e scegliendo "Aggiungi ai contatti...", questo verrà inserito nei "Contatti personali" (Figura 22).

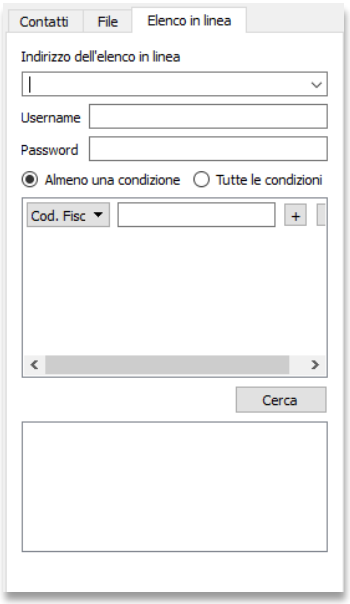


Figura 21

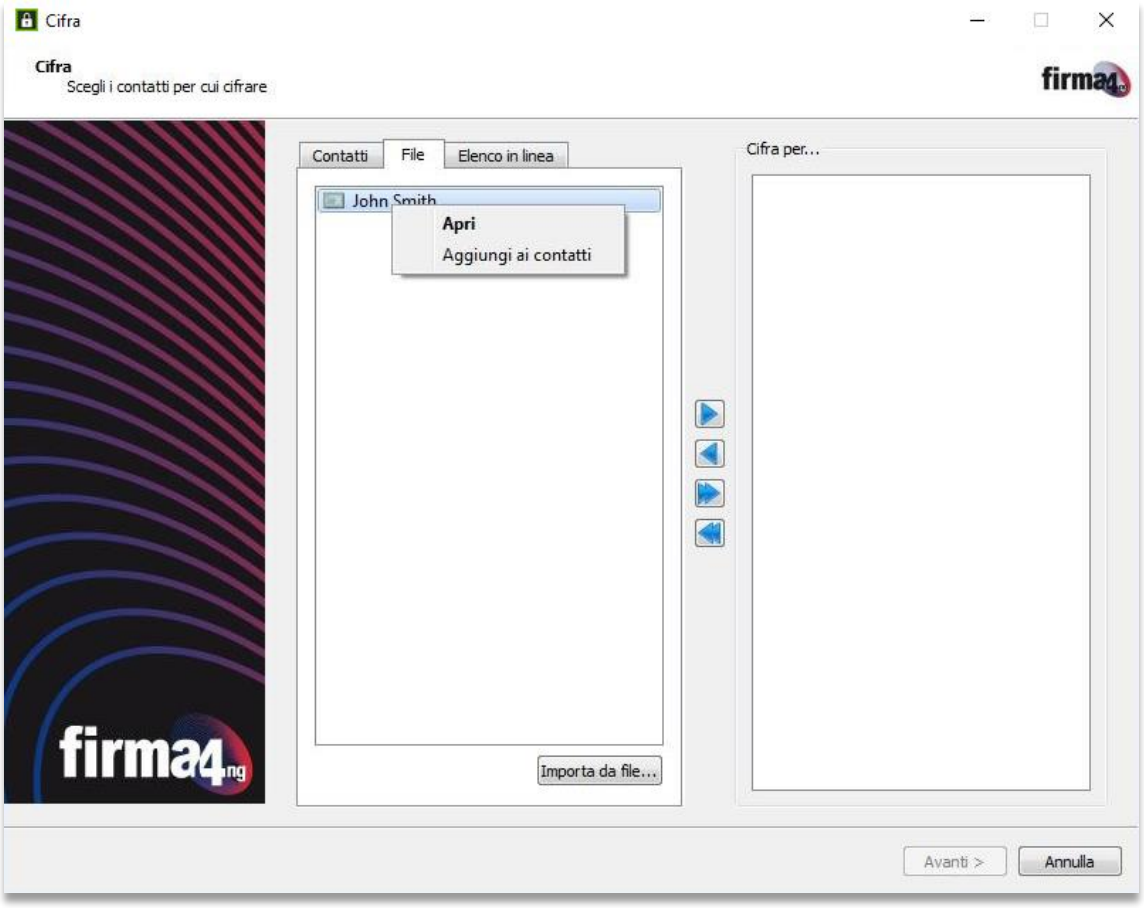


Figura 22

Al temine delle operazioni di caricamento dei certificati, per cifrare un documento selezionare della sezione "Contatti" il certificato da utilizzare presente e cliccare il pulsante con la freccetta rivolta a destra ( ) per spostarlo nella sezione **"Cifra per…"** (Figura 23).

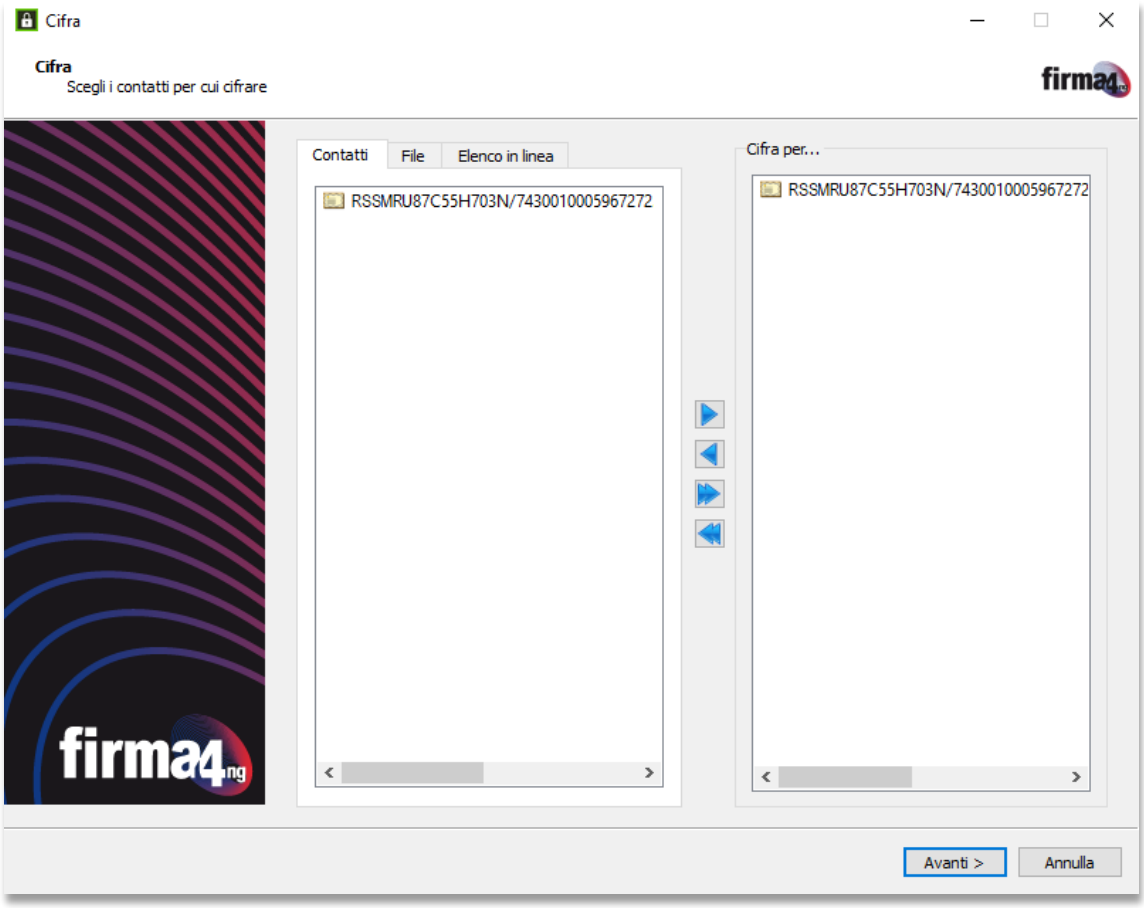


Figura 23

E' possibile aggiungere o rimuovere i contatti per cui si intende cifrare il documento utilizzando i pulsanti posti al centro delle due sezioni:

 Per aggiungere il contatto selezionato alla lista dei certificati con cui cifrare il documento;

 Per rimuovere il contatto selezionato dalla lista dei certificati con cui cifrare il documento;

 Per aggiungere tutti i contatti della lista alla lista dei certificati con cui cifrare il documento; il documento verrà cifrato per tutti i destinatari indicati;

 Per rimuovere tutti i contatti dalla lista dei certificati con cui cifrare il documento.

Al termine delle modifiche, cliccare su "Avanti" per continuare.

Fase 3

Dopo aver selezionato un contatto, appare la schermata in cui selezionare le opzioni da utilizzare per la cifratura del documento (Figura 24).

Figura 24

Nella schermata è possibile:

- Scegliere la cartella di destinazione e il nome con cui verrà salvato il documento cifrato, cliccando sul pulsante **"..."**;

- Selezionare l'algoritmo da utilizzare per cifrare fra quelli elencati nel menu a tendina (DES-EDE3-CBC oppure AES-256-CBC);
  Nota: per maggiore sicurezza si consiglia di utilizzare l'algoritmo AES-256-CBC;

- Spuntare la casella **"Salva in formato PEM"** per salvare il documento cifrato in formato PEM;

- Spuntare la casella **"Distruggi il documento originale"** per cancellare definitivamente dal PC il documento originale al termine dell'operazione di cifratura.
  Nota: attivando questa funzione il file originale non potrà più essere recuperato.

Cliccare "Avanti" per procedere con la cifratura del documento; al termine dell'operazione appare una schermata con l'esito e la cartella di destinazione in cui è stato salvato il documento cifrato (Figura 25).

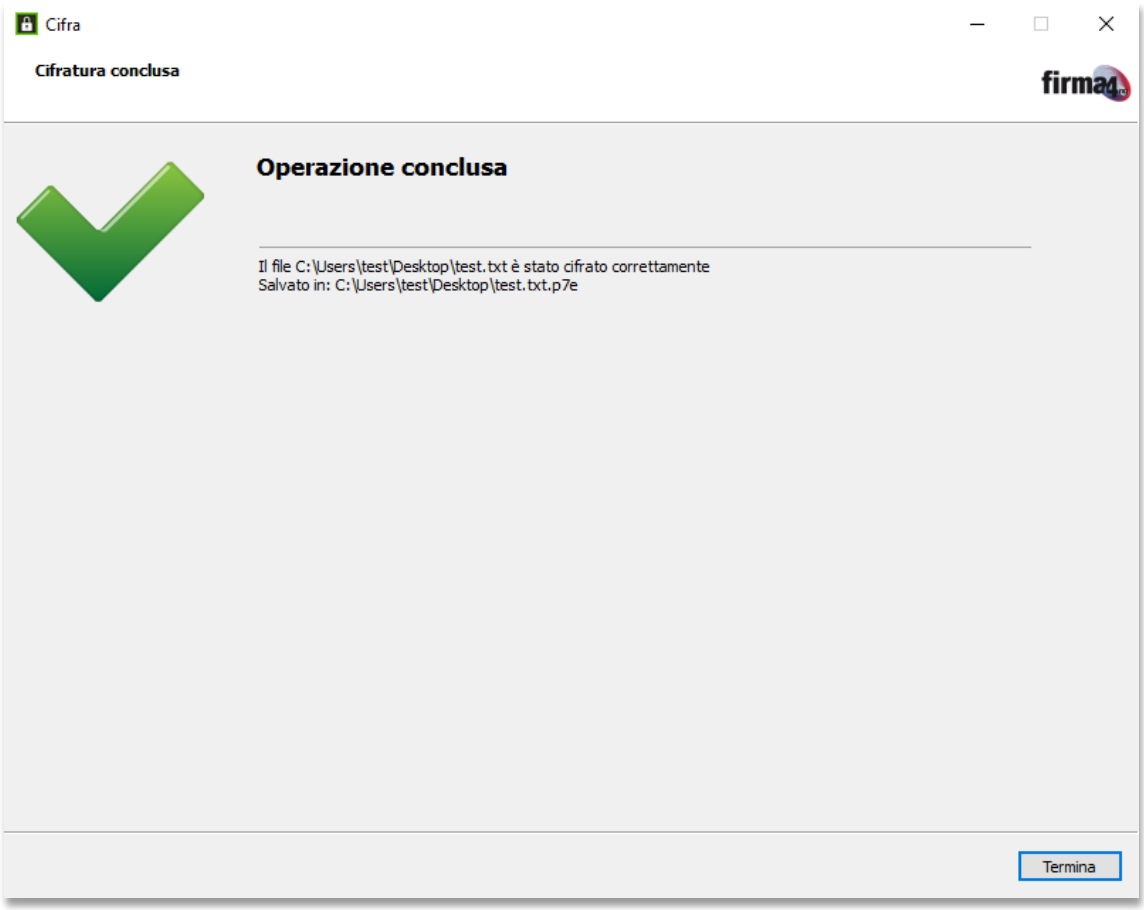


Figura 25

Cliccare su "Termina" per chiudere la schermata.

6.2 Decifratura

Al pulsante **"Decifra"** corrisponde la funzione di cifratura di uno o più documenti.

Fase 1

A partire dal menu secondario "Applicazioni" (Figura 17), è possibile avviare l'operazione di decifratura attraverso una delle seguenti modalità:

• Selezionando e trascinando il documento sul pulsante "Decifra" presente nel menu secondario (drag&drop);

• Cliccando sul pulsante "Decifra" presente nel menu secondario e selezionando il documento da verificare dalla finestra di navigazione del PC (Figura 26).

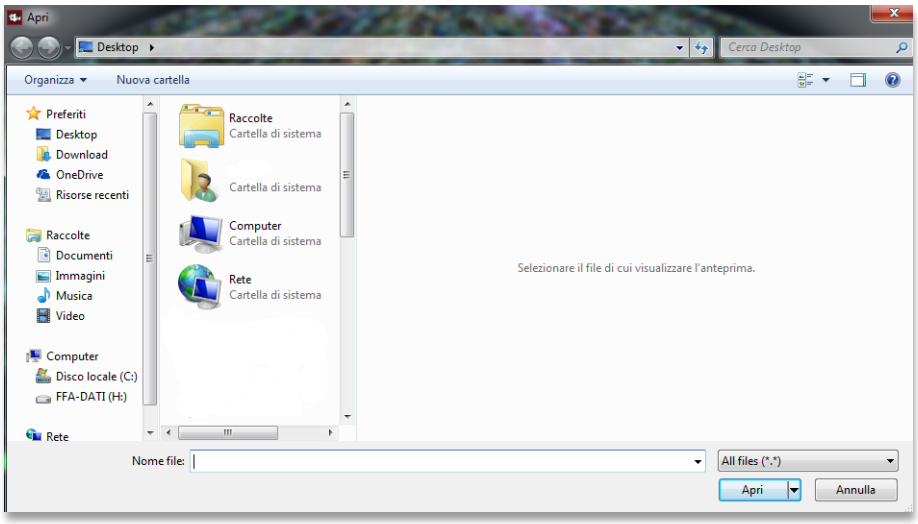


Figura 26

Attendere il caricamento dell'operazione.

Fase 2

Se è presente il certificato con cui è possibile decifrare il documento, si apre la schermata nella quale inserire il PIN del dispositivo (Figura 27). Inserire il PIN, poi cliccare su "Avanti" per procedere alla decifratura del documento.

Figura 27

Fase 3

Attendere l'analisi del file.

Al termine dell'analisi viene riportato l'esito dell'operazione. In caso di esito positivo, è possibile aprire il documento appena decifrato cliccando su "Apri contenuto" oppure salvarlo sul proprio PC cliccando su "Salva contenuto…".

Per chiudere la finestra "Decifra" cliccare su "Termina".

6.3 Cartella cifrata

Al pulsante **"Cartella cifrata"** corrisponde la funzione che permette di creare una cartella cifrata sul file system del PC accessibile solo attraverso il software *firma4ng*.

Cliccando sul pulsante "Cartella cifrata" presente nel menu secondario "Applicazioni" (Figura 17) appare la finestra in cui inserire il PIN per decifrare il contenuto della cartella (Figura 28).

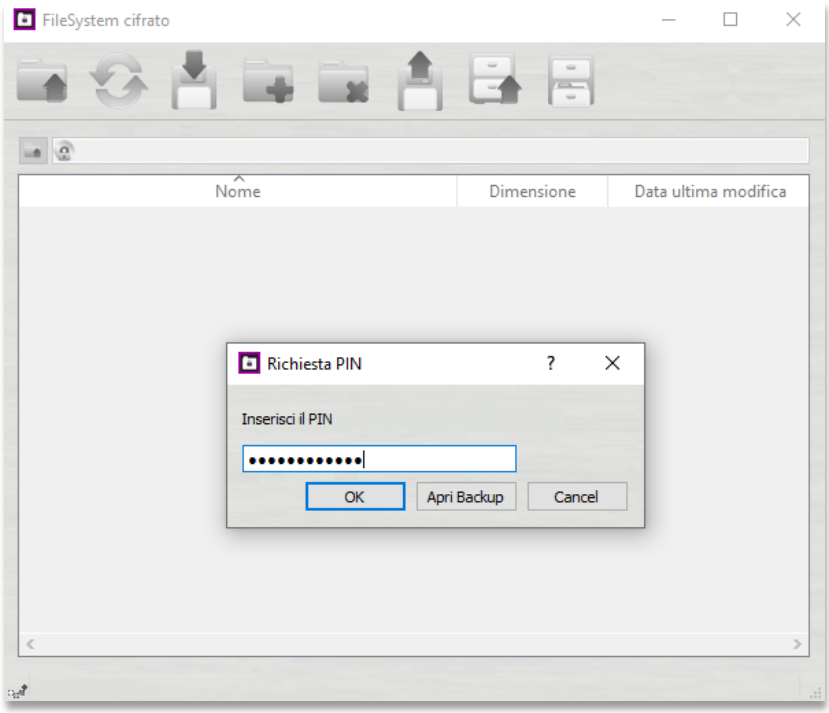


Figura 28

Una volta inserito il PIN è possibile navigare all'interno della cartella cifrata, creare e rimuovere cartelle e sottocartelle, importare ed esportare file e creare eventuali copie di backup attraverso i seguenti pulsanti:

Sali di livello: quando si è all'interno di una cartella, questo pulsante consente all'utente di salire di un livello fino a tornare nella cartella principale;

Aggiorna: permette di aggiornare la visualizzazione delle cartelle;

Aggiungi File: trascinando un file su questa icona o cliccandoci sopra, il file verrà automaticamente salvato nella cartella cifrata;

Crea Nuova Cartella: permette di creare una nuova cartella

 **Rimuovi Selezionati**: permette di eliminare file e/o cartelle precedentemente selezionate.

 **Esporta Selezionati:** per esportare file presenti all'interno di una cartella ad esempio sul desktop del Pc. Quando un file viene esportato, esso potrà essere aperto utilizzando il programma corrispondente alla sua estensione (es. un file .doc verrà aperto con Word).

 **Crea Backup del disco cifrato:** per creare una cartella di backup dell'intero File System cifrato. Per crearne una è necessario specificare il percorso su cui salvarla ed inserire una password.

 **Apri Backup**: per aprire una cartella di cui era stata fatta una copia di backup. Per aprire la cartella è necessario richiamare il percorso su cui era stata memorizzata ed inserire la password scelta in fase di backup.

6.4 Impostazioni

Cliccando sul pulsante **"Impostazioni"** si apre la finestra per la configurazione di *firma4ng*.

6.4.1 Generale

Nella sezione "Generale" (Figura 29) è possibile effettuare le seguenti operazioni:

- Cancella cache CRL: permette di cancellare le CRL (Certificate Revocation Lists, contenenti la lista dei certificati revocati e/o sospesi) salvate localmente sul PC. Per le operazioni di verifica successive a tale cancellazione sarà necessario scaricare e salvare in locale le CRL;
- Configurazione di default: ripristina la configurazione iniziale dell'applicazione;
- Avvia aggiornamento del software: avviare manualmente l'aggiornamento del software;
- Avvia aggiornamento TSL: avviare manualmente l'aggiornamento della TSL.

Al termine delle modifiche, cliccare su "Salva".

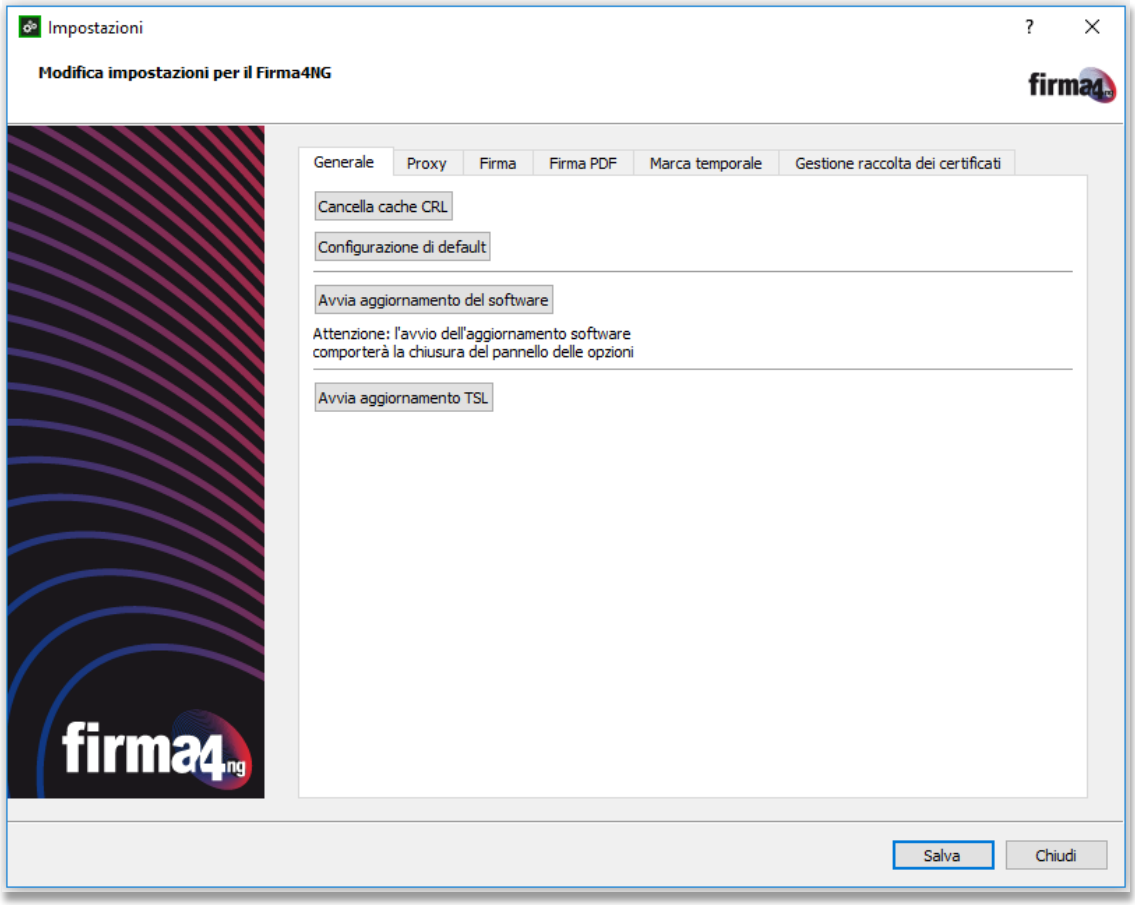


Figura 29

6.4.2 Proxy

Nella sezione "Proxy" (Figura 30) è possibile configurare un Proxy HTTP o LDAP. Per ciascuna delle due configurazioni (Proxy generico e Proxy LDAP) è possibile selezionare le seguenti opzioni:

- Nessun proxy: se selezionato non viene utilizzato nessun proxy;
- Configurazione manuale: se si desidera configurare manualmente i parametri per l'utilizzo del proxy specificando 'Tipo', 'Host' e 'Porta';

Le credenziali di accesso presenti nella sezione si riferiscono ai valori nome utente e password per l'autenticazione al proxy. Se non specificate in fase di configurazione, le credenziali verranno richieste solo se è necessaria l'autenticazione al proxy.

Nella sezione di configurazione 'Proxy LDAP' è possibile inoltre selezionare l'opzione "Usa la configurazione generica" per utilizzare la stessa configurazione specificata nella sezione 'Proxy generico'.

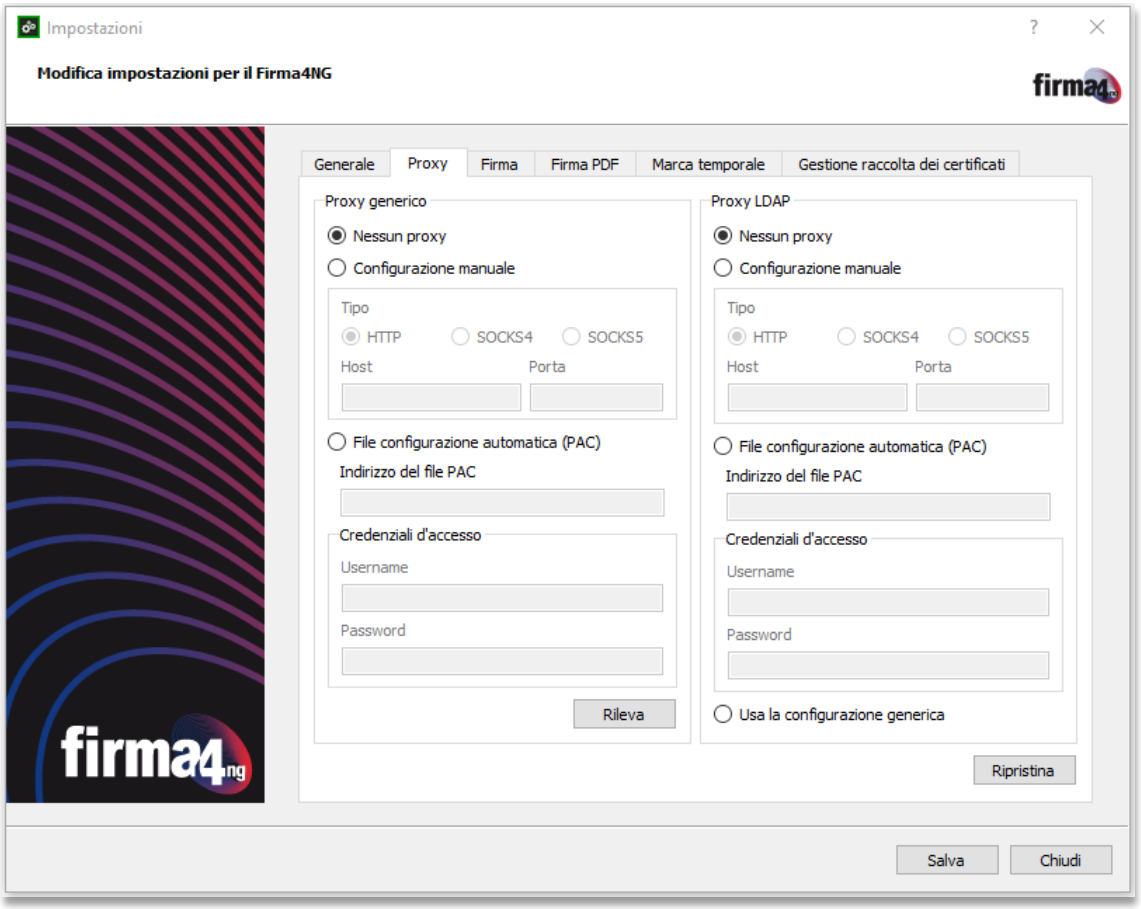


Figura 30

Per ripristinare la configurazione iniziale, cliccare su "Ripristina".

Al termine delle modifiche, cliccare su "Salva".

6.4.3 Firma

Nella sezione "Firma" (Figura 31) è possibile configurare il formato in cui verranno salvati i documenti firmati, scegliendo tra:

- In funzione dell'input: formato stabilito in base alla tipologia di documento da firmare;
- Firma P7M/Cades;
- Firma PDF;
- Firma XML.

È anche possibile scegliere la cartella di destinazione in cui salvare i documenti firmati con la procedura di firma multipla, cliccando su "Cerca…"

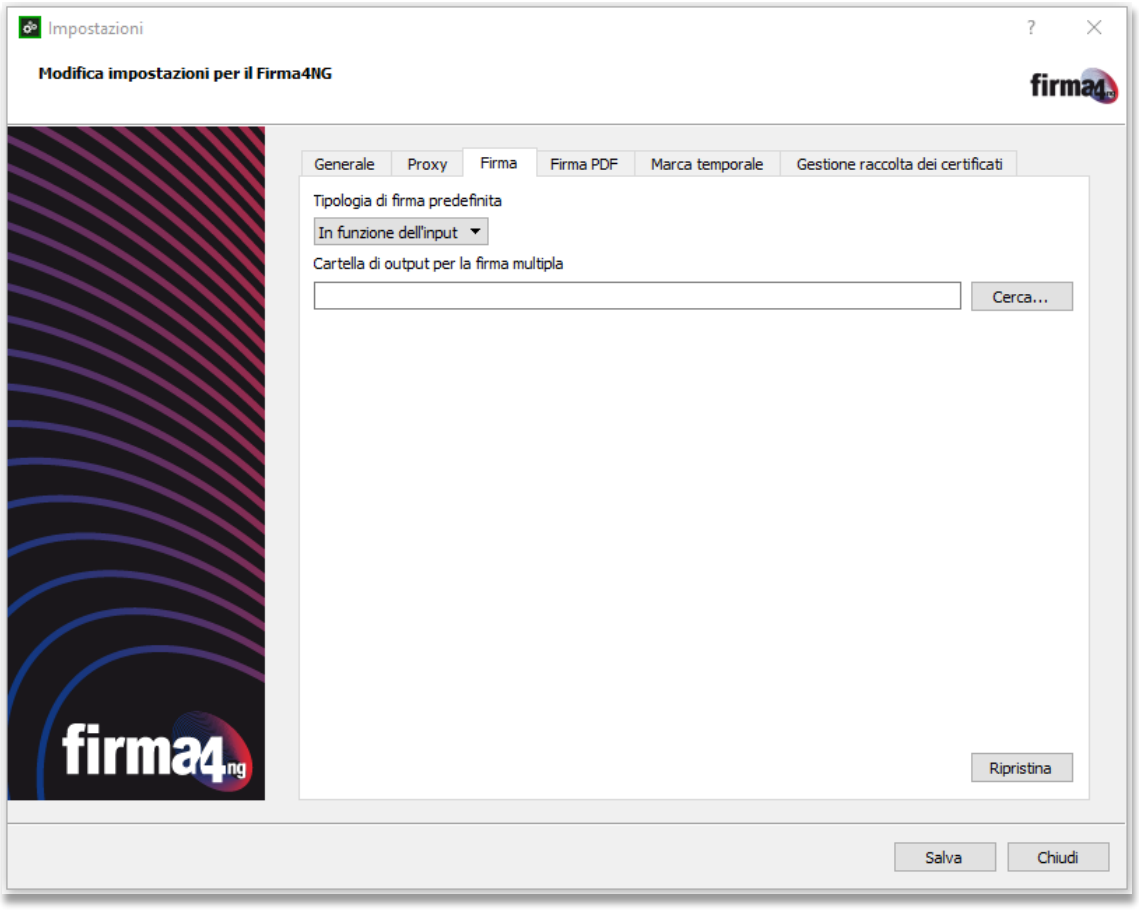


Figura 31

Per ripristinare la configurazione iniziale di *firma4ng*, cliccare su "Ripristina".

Al termine delle modifiche, cliccare su "Salva".

6.4.4 Firma PDF

Nella sezione "Firma PDF" (Figura 32) è possibile definire la configurazione standard da utilizzare per apporre la firma grafica in formato PDF, personalizzando i valori dei seguenti campi:

- Posizione
- Altezza
- Larghezza
- Pagina
- Località
- Ragione
- Timbro

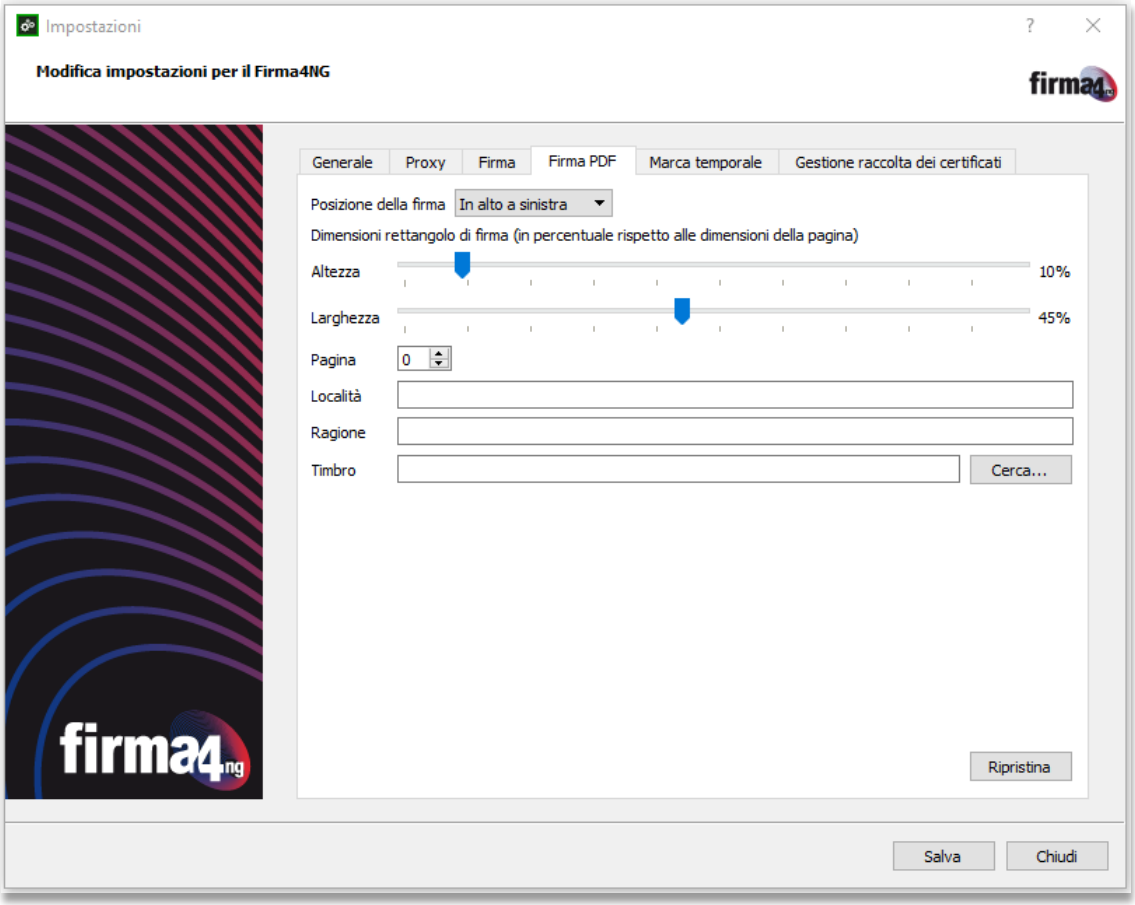


Figura 32

Per ripristinare la configurazione iniziale di *firma4ng*, cliccare su "Ripristina".

Al termine delle modifiche, cliccare su "Salva".

6.4.5 Marca temporale

Nella sezione "Marca temporale" (Figura 33) è possibile configurare il servizio di marcatura temporale da contattare per le richieste di marche temporali.

È possibile configurare nuovi servizi di marcatura temporale cliccando su "Nuovo" e valorizzando i parametri richiesti:

- Nome del servizio;
- Indirizzo della Time stamping authority;
- Username (opzionale);
- Password (opzionale);
- Policy OID (opzionale).

È anche possibile eliminare un servizio di marcatura temporale selezionandone il nome dall'elenco e cliccando su "Elimina".

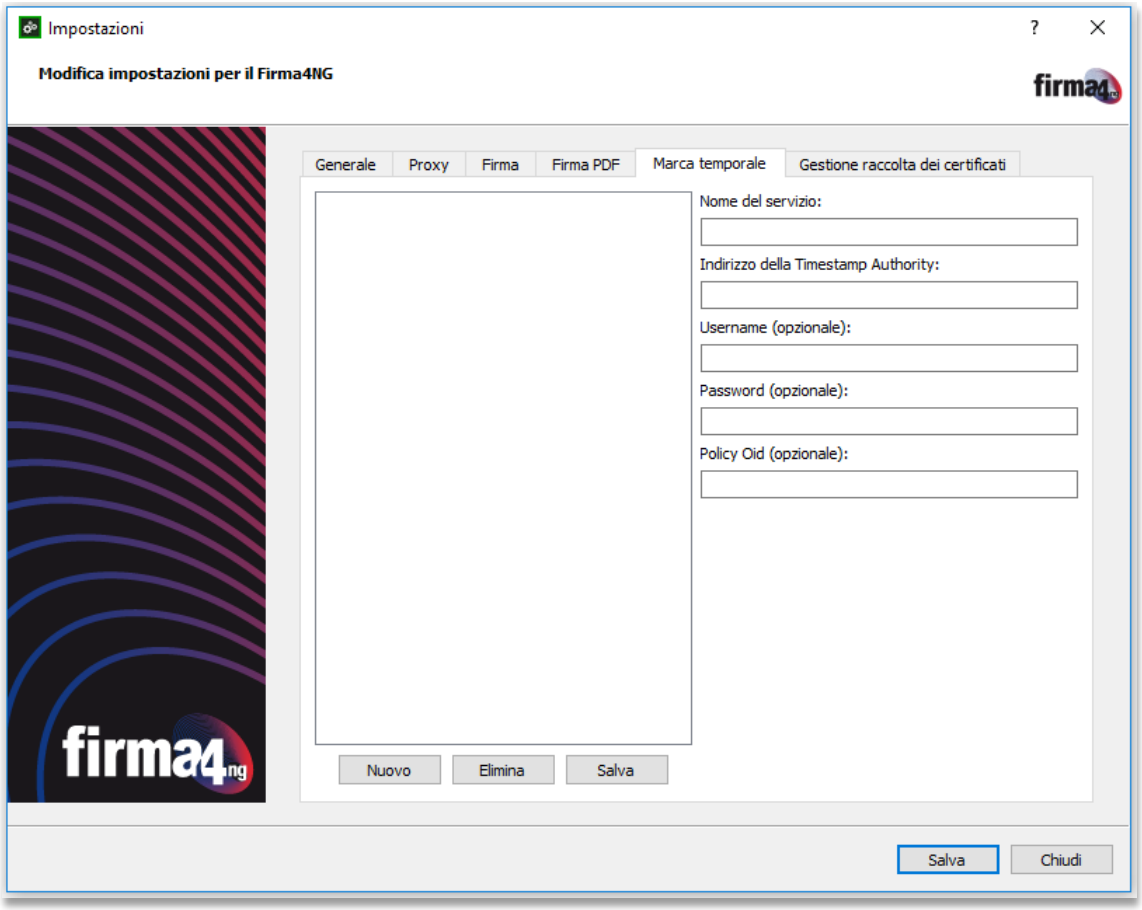


Figura 33

Al termine delle modifiche, cliccare su "Salva".

6.4.6 Gestione raccolta dei certificati

Nella sezione "Gestione raccolta dei certificati" (Figura 34) è possibile gestire l'archivio dei certificati utilizzato da *firma4ng*. In particolare, nell'area "*Raccolta certificati*" questi sono raggruppati nelle seguenti cartelle:

Affidabili: contiene certificati delle Autorità di Certificazione (CA) presenti nell'elenco pubblico tenuto da AgID;

TSA: contiene certificati delle Autorità di Certificazione del servizio di Marcatura temporale erogato dai vari Certificatori Accreditati;

Altre CA: contiene certificati di Autorità di Certificazione che seppure non presenti nell'elenco pubblico delle CA accreditate, sono reputati attendibili;

Contatti personali: contiene la lista dei certificati dei contatti per i quali cifrare i documenti.

Nell'area "*Importa da…*" è invece possibile caricare i certificati da "*File*" cliccando su "*Importa*", oppure ricercarli sul Registro pubblico dei certificati tenuto dal Certificatore tramite il tab "*Servizio in linea*", selezionando l'indirizzo LDAP e la base di ricerca. Una volta effettuata la ricerca, è possibile inserire i certificati trovati nella cartella "Contatti personali" utilizzando gli appositi pulsanti nella parte centrale della schermata.

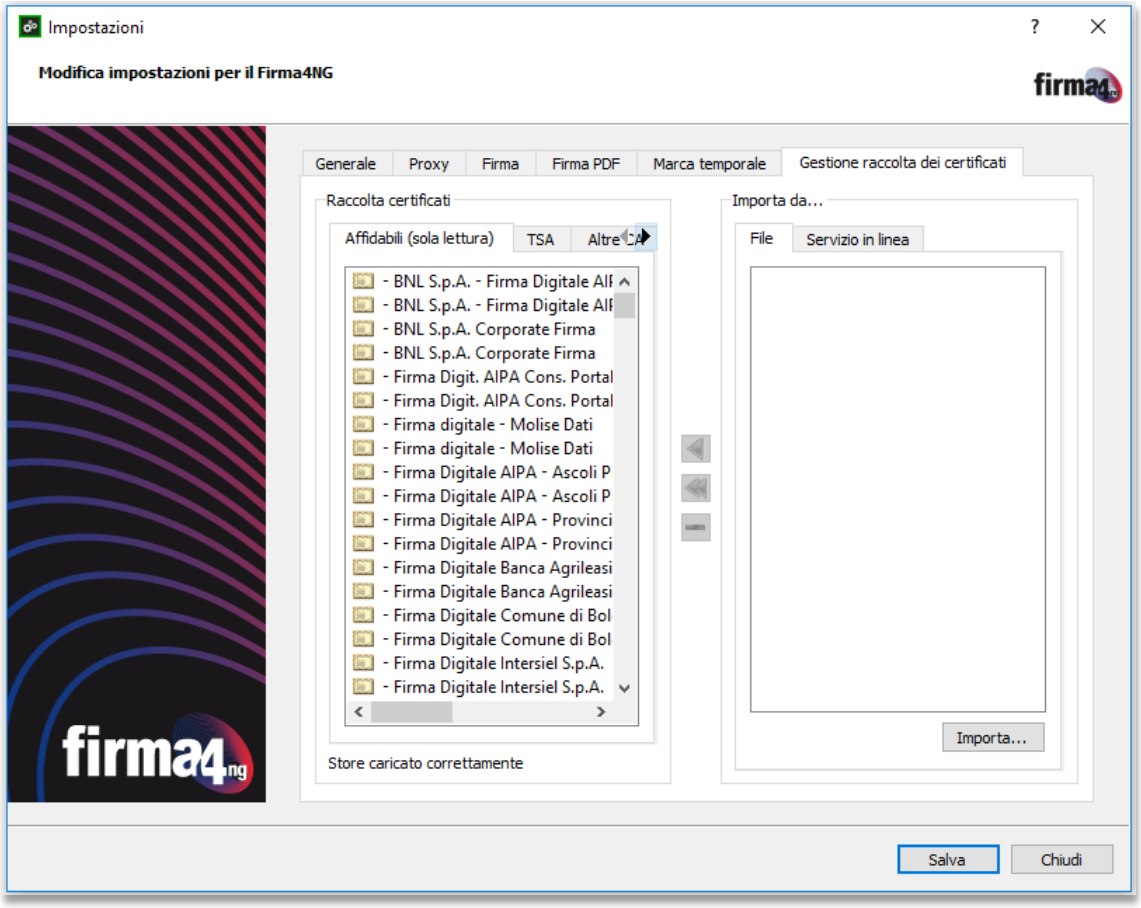


Figura 34

Al termine delle modifiche, cliccare su "Salva".

7. Gestione DigitalDNA

Cliccando sul pulsante **"Gestione DigitalDNA"** presente nel menu principale (Figura 1), si apre un menu secondario (figura 35) che contiene le seguenti voci:

- Cambio PIN
- Sblocco PIN
- Associazione
- Diagnostica

Figura 35

7.1 Cambio PIN

Cliccando sul pulsante **"Cambio PIN"** è possibile cambiare il codice PIN del dispositivo, inserendo negli appositi campi il PIN attuale e il nuovo PIN scelto, confermando nuovamente quest'ultimo (Figura 36).

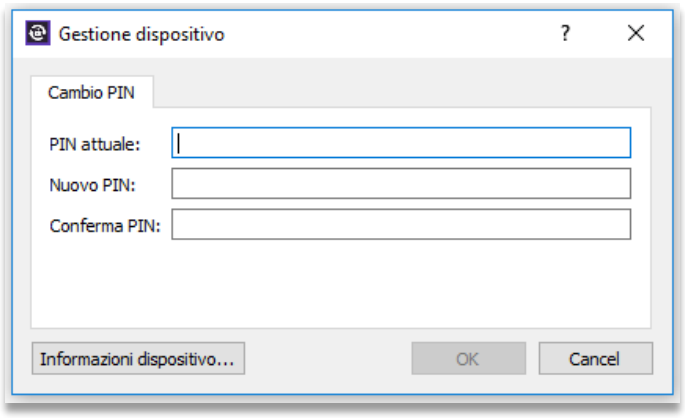


Figura 36

Cliccando su "Informazioni dispositivo" vengono visualizzate alcune informazioni relative al dispositivo di firma collegato (numero seriale, certificati, ecc.) (Figura 37).

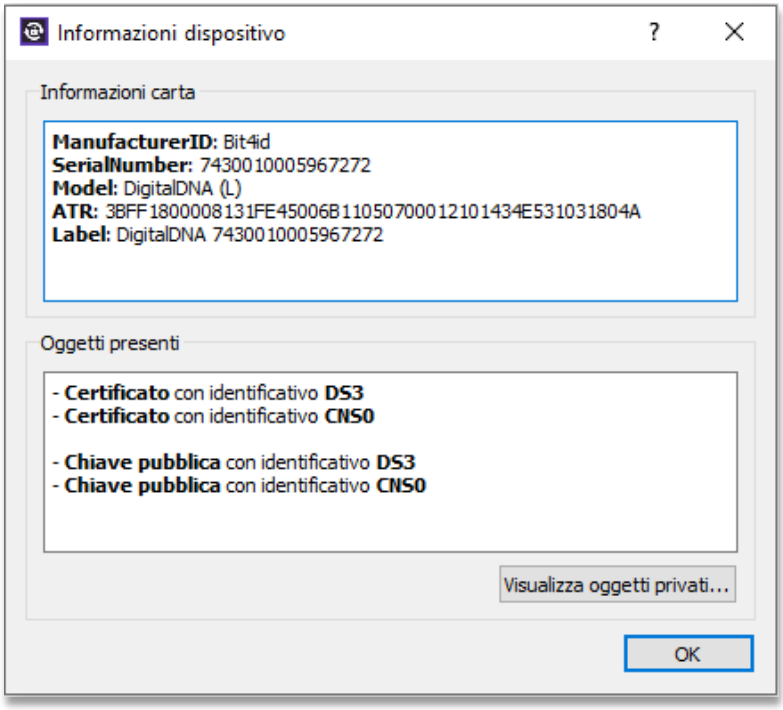


Figura 37

Al termine delle modifiche, cliccare su "OK" per cambiare il PIN.

7.2 Sblocco PIN

Cliccando sul pulsante **"Sblocco PIN"** è possibile sbloccare il codice PIN del dispositivo (a seguito di tre tentativi errati di inserimento PIN) inserendo negli appositi campi il codice PUK del dispositivo, un nuovo PIN di otto cifre numeriche e confermando nuovamente quest'ultimo (Figura 38).

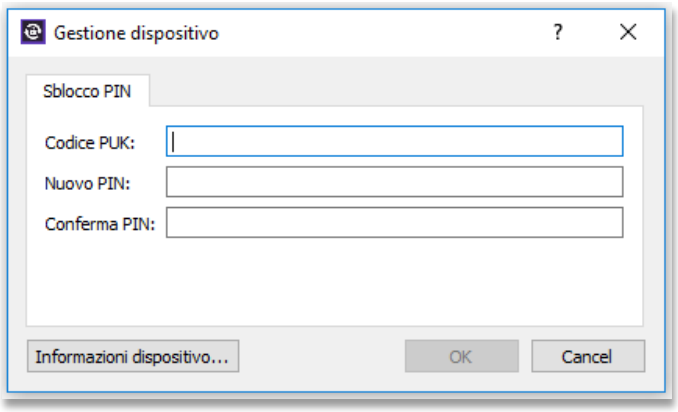


Figura 38

Cliccando su "Informazioni dispositivo" vengono visualizzate alcune informazioni relative al dispositivo di firma collegato (numero seriale, certificati, ecc.) (Figura 37).

Al termine delle modifiche, cliccare su "OK" per sbloccare il PIN.

7.3 Associazione

Cliccando sul pulsante **"Associazione"** si avvia automaticamente la configurazione del dispositivo DigitalDNA Key collegato al PC. La procedura guidata illustra in poche schermate i passaggi da seguire per abbinare correttamente il dispositivo al software *firma4ng* (Figura 39).

1. Accendere il dispositivo
2. Selezionare dall'elenco dei dispositivi rilevati la DigitalDNA Key da configurare
3. Tenere premuto il pulsante fino a quando il LED inizia a lampeggiare
4. Fatto!

Figura 39

Per associare un nuovo dispositivo cliccare su "Ripeti abbinamento".

Una volta conclusa l'associazione, cliccare sulla "X" in alto a destra per chiudere la schermata.

7.4 Diagnostica

Cliccando sul pulsante **"Diagnostica"** si avvia automaticamente il tool di diagnostica, ovvero lo strumento che consente di analizzare lo stato dei dispositivi DigitalDNA Key.

Prima di iniziare la scansione, verificare che il tasto della batteria sul dispositivo sia impostato su ON. Quindi cliccare su *"Avvia il tool di diagnostica del dispositivo"* (Figura 40).

Figura 40

Il tool di diagnostica esegue una scansione per verificare il corretto funzionamento del dispositivo e per identificare potenziali problemi.

Attendere il completamento della scansione (Figura 41).

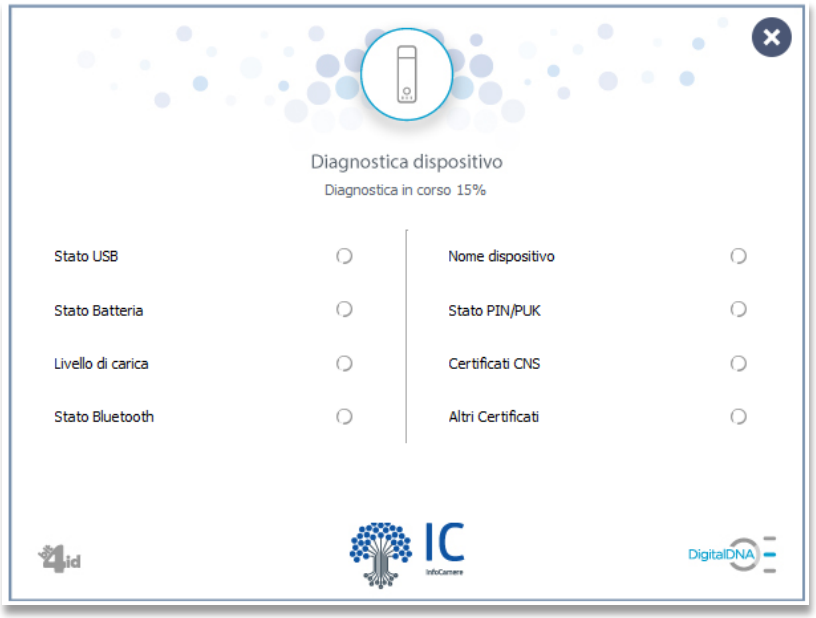


Figura 41

Una volta completata la scansione, la schermata riporta un'analisi delle prestazioni e informazioni sullo stato del dispositivo collegato (Figura 42). Eventuali anomalie o errori di funzionamento vengono segnalati con la scritta in rosso *"Errore"* e vengono esplicitati nella sezione in basso.

Cliccare su "Test del buzzer" per verificare il corretto funzionamento del segnalatore acustico.

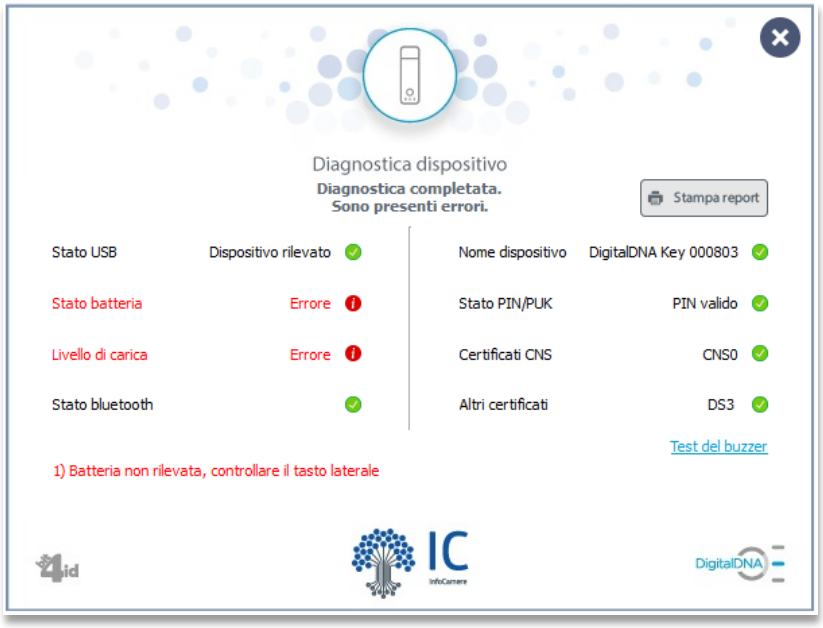
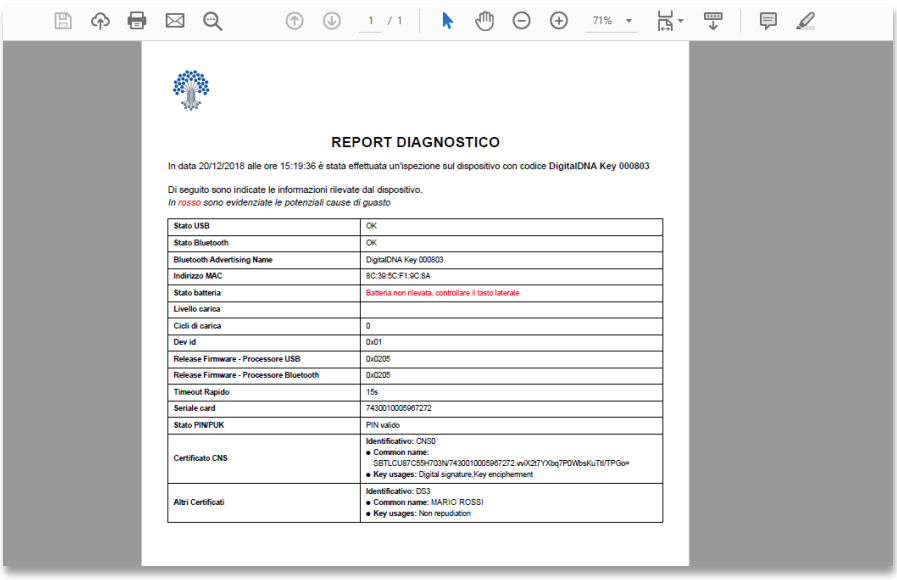


Figura 42

Al termine della scansione, il tool di diagnostica genera automaticamente un report con il riepilogo dei risultati. Cliccando sul pulsante "Stampa report" (Figura 42) è possibile salvare e stampare il report della diagnostica effettuata sul dispositivo. Dopo aver cliccato sul pulsante, selezionare la cartella di destinazione sul proprio PC per salvare il file, quindi aprire il PDF e avviare la stampa (Figura 43).



REPORT DIAGNOSTICO

In data 20/12/2018 alle ore 15:19:36 è stata effettuata un'ispezione sul dispositivo con codice **DigitalDNA Key 000803**

Di seguito sono indicate le informazioni rilevate dal dispositivo.
In rosso sono evidenziate le potenziali cause di guasto

Stato USB	OK
Stato Bluetooth	OK
Bluetooth Advertising Name	DigitalDNA Key 000803
Indirizzo MAC	8C:39:5C:F1:9C:8A
Stato batteria	Batteria non rilevata, controllare il tasto laterale
Livello carica	
Cicli di carica	0
Dev id	0x01
Release Firmware - Processore USB	0x0205
Release Firmware - Processore Bluetooth	0x0205
Timeout Rapido	15s
Seriale card	7430010005967272
Stato PIN/PUK	PIN valido
Certificato CNS	**Identificativo:** CNS0 • **Common name:** SBTLCU87C55H703N/7430010005967272.vvIX2t7YXbq7P0WbsKuTti/TPGo= • **Key usages:** Digital signature,Key encipherment
Altri Certificati	**Identificativo:** DS3 • **Common name:** MARIO ROSSI • **Key usages:** Non repudiation

Figura 43

8. Cassetto digitale dell'imprenditore

Cliccando sul pulsante **"Cassetto digitale dell'imprenditore"** presente nel menu principale (Figura 1) si apre automaticamente il browser Internet sulla pagina web *impresa.italia.it* dedicata al Cassetto digitale, il servizio per il cittadino imprenditore (Figura 41).

Figura 44

bit4id in the world

Bit4id Italia
Via Diocleziano, 107
80125 – Napoli
Tel. +39 081 7625600
Fax. +39 081 19731930
info@bit4id.com

Milano
Tel. +39 02 40042990
Fax. +39 02 45500675
www.bit4id.com

Bit4id Iberica s.l.
Barcellona
Barcelona Advanced Industry Park
C/ Marie Curie, 8-14
08042 – Barcelona
Tel: +34 902 60 20 30
Info.es@bit4id.com

Lisbona
Rua A Gazeta de Oeiras, N° 2, 2° B
2780-171 Oeiras (Lisboa)
Tel: +351 214 694 060
info.pt@bit4id.com

Lima
Mártir Olaya, n° 129
Oficina 1204 – Miraflores
Lima
Tel: +(51) 1 242 9994
Info.pe@bit4id.com

Guatemala
5ª Avenida, 42-56 zona 8,
01008 – Guatemala
Tel: +502 44888144
aor@bit4id.com
cma@bit4id.com

Ecuador
Pasaje S9 y Garcia Moreno
OE1 482 – Quito
Ecuador
Tel: +593 99 282 5835
info.ec@bit4id.com

Bit4id Ltd
Londra
2 London Wall Buildings
London EC2M 5UU – UK
Tel. +44 1422 570673
Fax +44 20 78553780
info@bit4id.com