DigitalSign 5.0

Guida Utente

Sommario

1 Generalità e Concetti

1.1 Principi e riferimenti normativi sulle firme elettroniche

1.1.1 Concetti di "firma elettronica", "firma elettronica avanzata", "firma digitale", "firma elettronica qualificata"

Una **firma elettronica** può essere definita come:

"un insieme di dati in forma elettronica, allegati o logicamente associati con altri dati elettronici e che servono come metodo di autenticazione".

Si tratta evidentemente di una definizione assai generale, in cui ricade un vasto spettro di strumenti. Anche scrivere il proprio nome in calce ad un messaggio e-mail può essere considerato una forma di firma elettronica.

La normativa distingue poi diverse fattispecie di firma elettronica:

- **Firma Elettronica** (talvolta menzionata con l'aggettivo **"semplice"**)
- **Firma Elettronica Avanzata**
- **Firma Digitale**
- **Firma Elettronica Qualificata**

Mentre nell'attuale formulazione delle norme la **firma digitale** e la **firma qualificata** sono pressoché coincidenti, la Firma Elettronica Avanzata (di cui – ricordiamo – la firma qualificata è un caso particolare) è una fattispecie più ampia, che si apre a diverse interpretazioni.

Per quanto riguarda ***DigitalSign***, una firma elettronica basata su una coppia di chiavi crittografiche e su un certificato di chiave pubblica, può avere il rango di Firma Elettronica Avanzata se è basata su una infrastruttura che rispetta i vincoli imposti dalle Regole Tecniche in vigore (che sono vincoli procedurali, più che tecnologici).

In particolare, gli utenti di ***DigitalSign***:

- possono produrre **Firme Digitali** usando dispositivi di firma di tipo smartcard (eventualmente integrate in chiavette USB rilasciate o gestiti da un Certificatore Accreditato, oppure servizi di Firma Remota compatibili, gestiti da Certificatori Accreditati
- possono generare **Firme Elettroniche Avanzate** usando smartcard di tipo CNS o CIE
- possono generare Firme Elettroniche (semplici o avanzate) usando smartcard con a bordo certificati rilasciati da Certification Authority tecniche o servizi di firma remota gestiti da provider tecnici con le proprie infrastrutture.

NOTA: ***DigitalSign*** non consente l'uso diretto di chiavi di firma software (contenute in container PKCS#12) per generare firme. Tuttavia, è sempre possibile realizzare moduli di interfaccia PKCS#11 in grado di emulare il comportamento di una smartcard e utilizzarli con ***DigitalSign***.

Questa tecnica è usata, per esempio, per interfacciare alcuni servizi di Firma Digitale Remota, ma potrebbe essere usata anche per interfacciare chiavi software per la firma elettronica semplice o avanzata.

1.1.2 La "meccanica" delle firme elettroniche

Le firme elettroniche generate e/o verificate da ***DigitalSign*** sono sempre del tipo basato su una coppia di chiavi crittografiche: *"un particolare tipo di firma elettronica basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare provenienza e integrità di un documento informatico".*

In altre parole, una firma di questo tipo è realizzata mediante l'uso di algoritmi di *hashing* per derivare un'impronta dai dati oggetto della firma, e da algoritmi di crittografia asimmetrica per derivare la firma dall'impronta.

Le due chiavi di una coppia vengono gestite in modo che la chiave privata resti in totale ed esclusiva disponibilità del sottoscrittore, e che la chiave pubblica sia effettivamente accessibile a chiunque si trovi nella necessità di verificare la firma.
Per rendere la chiave pubblica effettivamente fruibile e per associare la coppia di chiavi ad una identità, si adotta lo strumento del Certificato di Chiave Pubblica (si veda la prossima sezione).

Questa tecnica soddisfa i requisiti delle firme elettroniche perché:

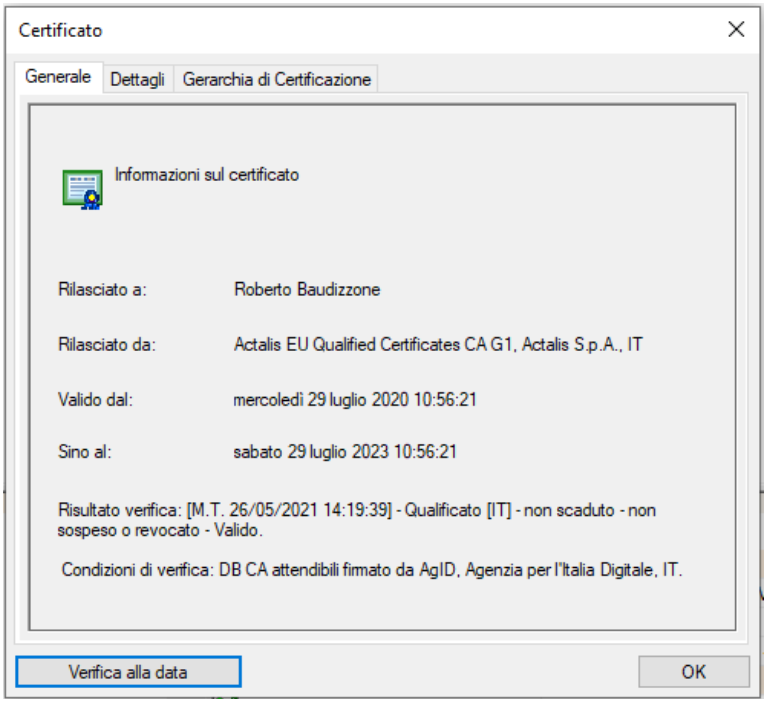
1. la firma è generata con la chiave privata in possesso esclusivo del sottoscrittore; quindi, è univocamente collegata a tale soggetto;
2. permette di identificare il sottoscrittore, perché un ente attendibile (certificatore) emette un certificato che associa la chiave pubblica ad una identità;
3. rivela ogni modifica successiva apportata ai dati, perché in fase di verifica non si avrebbe corrispondenza tra l'impronta calcolata sui dati e quella decifrata dalla firma.

1.1.3 Il certificato di chiave pubblica

Elemento fondamentale di una cosiddetta "infrastruttura di chiave pubblica" è il **certificato**, che corrisponde direttamente ad una coppia di chiavi (parte privata e parte pubblica) associate ad un titolare.

Si tratta di un file contenente alcune informazioni fondamentali:

- numero di serie
- dati anagrafici o identificativi del titolare del certificato stesso
- copia della parte pubblica della coppia di chiavi associata al titolare
- data di emissione e data di scadenza del certificato
- indicazione del soggetto che ha emesso il certificato (Certificatore)
- informazioni ausiliarie per definire formato e caratteristiche di utilizzabilità del certificato
- indicazioni che consentono di verificare, tramite un accesso automatico al sistema del certificatore, l'eventuale stato di revoca anticipata della validità del certificato
- firma digitale, calcolata sul contenuto del certificato stesso, generata dal "Certificatore"



Il motivo per cui un certificato è sempre generato con una vita a termine, cioè con una data di scadenza predefinita, è collegato alla necessità di non mantenere indefinitamente in uso una coppia di chiavi.

La parte privata e la parte pubblica di una coppia di chiavi sono legate da una relazione matematica; quantunque non sia possibile calcolare direttamente la chiave privata essendo nota la pubblica, è possibile usare la cosiddetta "forza bruta" e provare tutte le combinazioni sino a trovare la chiave giusta.

La contromisura è usare chiavi di tale lunghezza che un procedimento di "forza bruta" costi un tempo di elaborazione molto lungo, misurabile in anni, anche usando i più veloci supercomputer che la tecnologia attuale mette a disposizione. E quindi postulare una durata massima di una coppia di chiavi – registrata nel certificato – molto minore di questo tempo minimo necessario per trovare una chiave privata.

Da notare che la firma digitale apposta dal Certificatore, coprendo tutti gli altri dati contenuti nel certificato stesso, ne protegge *l'integrità* – per il fatto che eventuali alterazioni verrebbero rivelate, per definizione, in fase di verifica di questa firma – e *l'autenticità* – perché la firma del certificatore garantisce, sotto la responsabilità di quest'ultimo e nei limiti preventivamente concordati, la veridicità dei dati contenuti (e i dati più importanti contenuti in un certificato sono quelli che attestano l'identità del suo titolare).

1.1.4 Il Certificatore

Sul piano tecnico il soggetto che emette certificati di chiave pubblica si definisce "Autorità di Certificazione" o "*Certification Authority*" o **CA**.

Una CA è un organo che genera i certificati con il contenuto predefinito e li firma digitalmente con una propria chiave privata (detta "chiave privata di certificazione").
Naturalmente, come qualunque altro soggetto che emette firme ed è quindi dotato di una chiave privata, la CA deve anche essere dotata di un certificato associato alla relativa coppia di chiavi. Tale certificato si chiama "Certificato di CA".

La domanda scontata è: *"Ma chi emette allora il certificato della CA? Chi lo firma?"*
La risposta è, in generale: *"Una CA di livello superiore"*

Evidentemente questa iterazione di livelli non può ripetersi all'infinito e, prima o poi, la "catena di certificazione" deve arrivare ad una fine (più esattamente, in cima alla catena gerarchica).

Il certificato della CA di livello più alto non viene dunque emesso da alcun organo superiore, ma è emesso dalla stessa CA: si tratta di un certificato *"self-signed"* o "di tipo *root*".
La particolarità è che questi certificati sono firmati con la chiave privata appartenente alla stessa coppia la cui chiave pubblica è contenuta nel certificato.

È il caso, per esempio, dei Certificatori Accreditati in Italia per emettere Certificati Qualificati: la verifica dell'autenticità di un certificato, dunque, richiede che il sistema di verifica "conosca" preventivamente i certificati delle CA di cui si può fidare.

Tornando a livello di definizioni, la **CA** è normalmente intesa come l'organo tecnico, corrispondente ad una chiave privata ed un **certificato di CA**.
Il soggetto o ente che effettivamente svolge le attività correlate, viene definito "Certification Service Provider" o "Fornitore di Servizi di Certificatore", in breve "**Certificatore**".
Un Certificatore può, in generale, gestire più CA. Di solito questo avviene per emettere certificati di diversa tipologia (Firma Digitale, Autenticazione, Marcatura Temporale, ecc.).

1.1.5 Le liste di Sospensione e Revoca (e il protocollo OCSP)

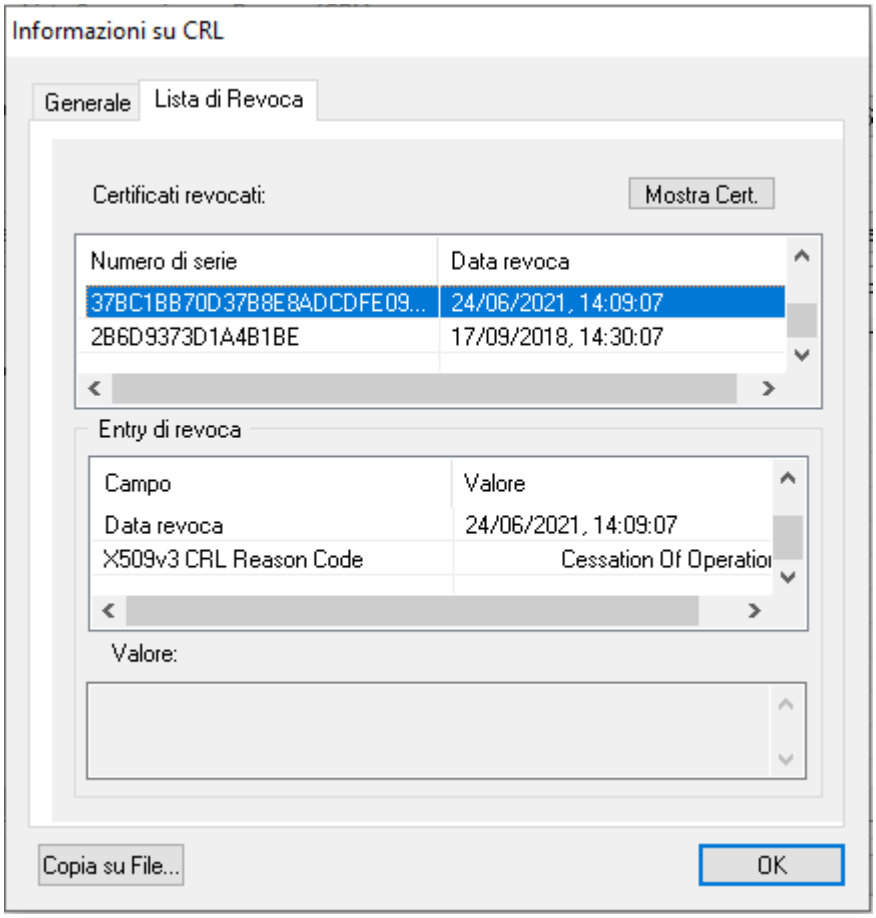
Come spiegato nella sezione Il certificato di chiave pubblica un certificato nasce con una durata massima prefissata, dipendente dalla scelta commerciale del Certificatore che lo emette, ma comunque determinata dalla lunghezza delle chiavi oggetto di certificazione.

Tuttavia, possono verificarsi diverse ragioni per terminare anzitempo la durata di un certificato. Il caso più tipico è quello in cui il legittimo titolare ha perduto – o teme di aver perduto – il possesso esclusivo della chiave privata e vuole evitare che un malintenzionato emetta firme digitali a suo nome: un'esigenza molto simile al "blocco" di una carta di credito smarrita o rubata.

Ma la revoca di un certificato ha senso soltanto se chi verifica un documento firmato può determinare se il certificato associato alla firma è stato effettivamente revocato.

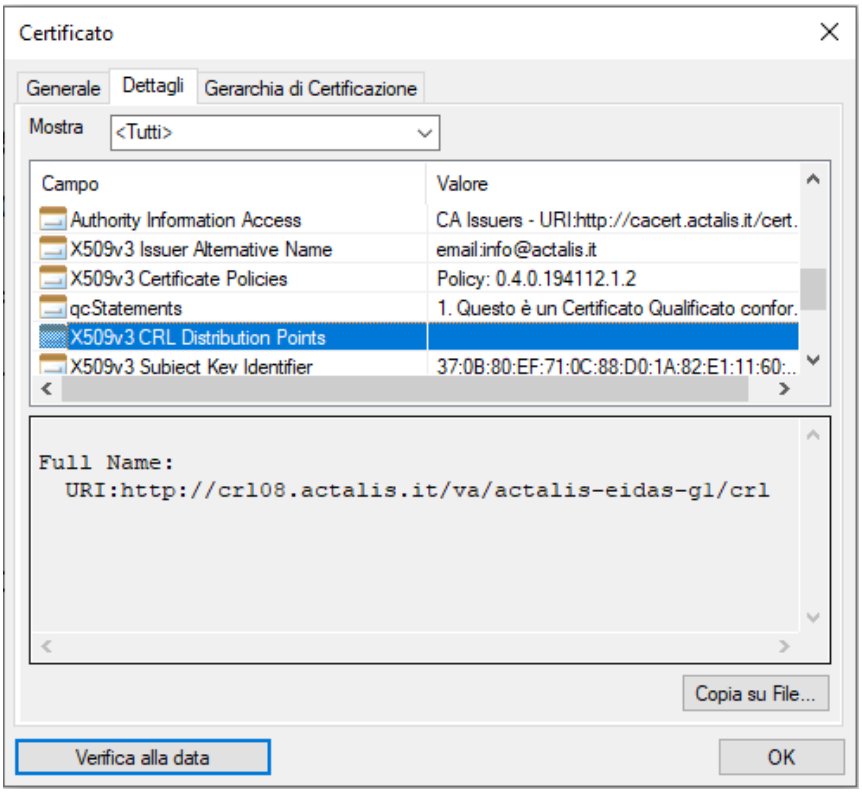
Lo strumento più comune per soddisfa questa esigenza è la Lista di Sospensione e Revoca, o *Certificate Revocation List* (CRL).

Una CRL, banalmente, è una lista di numeri di serie di certificati emessi da una data CA, associati a data, ora e motivo della revoca.



La lista stessa è corredata da un'indicazione di data ed ora di emissione, nonché data ed ora della prossima emissione programmata. La lista è ovviamente firmata digitalmente dalla stessa CA e resa accessibile su un server, ad un indirizzo ben determinato.

Ogni certificato contiene l'indicazione dell'indirizzo Internet a cui è reperibile una copia della CRL (e il sistema di verifica deve scaricare la lista proprio da tale indirizzo, non altrove):

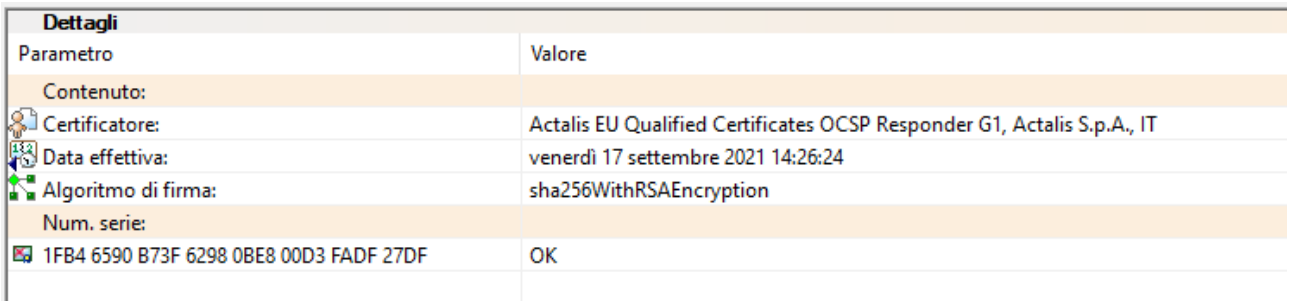


Poiché sia il certificato che la CRL sono firmati digitalmente dalla CA, l'integrità del meccanismo è assicurata.
Naturalmente l'uso di queste liste dovrebbe essere automatico in fase di verifica di qualunque firma o certificato, rivelando se il certificato compare nella lista di revoca.

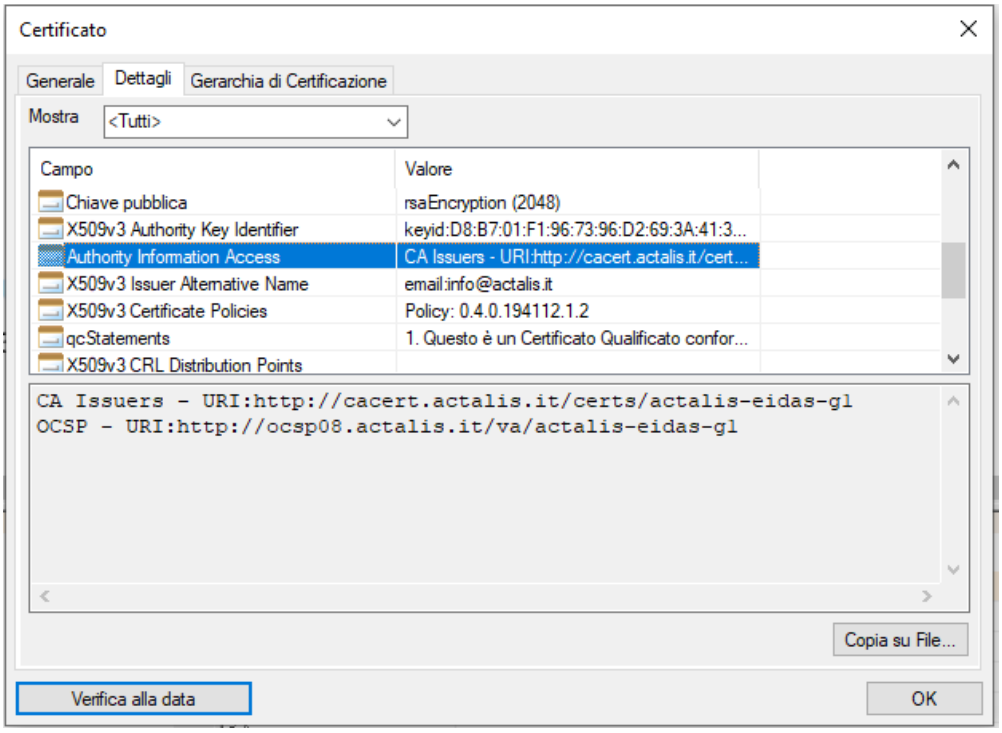
Il Certificatore dovrebbe aggiornare molto frequentemente le proprie CRL, in modo da rendere subito disponibili le revoche che possono avvenire in qualsiasi momento.

NOTA: le CRL si definiscono "Liste di Sospensione e Revoca" perché riportano sia lo stato di revoca che quello di sospensione. Senza entrare troppo nei dettagli possiamo dire che un certificato, di solito, viene posto in uno stato di sospensione (per esempio quando il titolare dichiara telefonicamente di aver perduto il possesso della chiave privata). In seguito, dopo una procedura amministrativa di controllo, la sospensione diventa una revoca a tutti gli effetti, oppure il certificato può sparire dalla lista (per esempio se il titolare dichiara poi di aver ritrovato una smartcard o se la segnalazione telefonica risulta poi non vera).

In generale è disponibile anche un servizio di verifica dello stato di revoca basato sul protocollo OCSP *(Online Certificate Status Protocol)*: in questo caso il software di verifica non è costretto a scaricare una intera lista di certificati revocati, ma trasmette una richiesta di stato specifica per il particolare certificato da verificare; il server del Certificatore risponderà riguardo allo stato del certificato.



Se il certificatore prevede un tale servizio, il certificato riporta anche l'indicazione dell'indirizzo a cui inviare le richieste:



1.1.6 Le Marche Temporali (*Timestamp*)

Una marca temporale è un documento informatico molto particolare.
È firmato digitalmente da un soggetto definito "Fornitore di Servizi di Marcatura Temporale" (*Timestamp Provider*, TSP) e tale firma copre il contenuto: una precisa data e ora, nonché il valore di un'impronta (hash) fornita dal richiedente.

Un utente utilizza questo servizio quando desidera associare una data certa all'esistenza di un documento oppure di una specifica firma apposta al documento:

1. si calcola il valore dell'impronta (*hash*) del documento (o della firma) oggetto della marcatura temporale;
2. si trasmette, via Internet, al server del TSP una richiesta contenente l'impronta calcolata;
3. si riceve la marca temporale (*timestamp*) dal server del TSP;
4. si associa la marca temporale al documento (o alla firma);

Poiché la firma digitale contenuta nel *timestamp* è considerata "opponibile ai terzi" (se ci si rivolge a TSP qualificati) sarà possibile dimostrare l'esistenza di un documento (o di una specifica firma), per esempio, in un istante di tempo in cui il certificato del firmatario era sicuramente valido (non scaduto, non revocato).

In generale una Marca Temporale può essere associata:

i. ad una firma: in questo caso è calcolata sull'impronta della firma stessa, la quale è calcolata sull'impronta del documento; lo scopo principale è dimostrare l'esistenza delle firma (e quindi anche del contenuto) in un certo istante; inoltre, in questo caso, la M.T. è integrata nella struttura del documento;
ii. ad un documento, di qualunque formato, che può essere firmato o non firmato; la M.T. è calcolata sull'impronta dell'intero file ed è detta "*detached*", ossia separata dal documento a cui si riferisce. Peraltro, esistono formati, più o meno standard, per riunire i due file (il documento e la M.T. *detached*) in un unico file, una sorta di archivio, ma le strutture restano separate

1.1.7 I formati di rappresentazione dei documenti firmati

Sin dal 1999, anno di entrata in vigore delle prime regole tecniche in materia di documenti informatici, il formato standard per la rappresentazione dei documenti è stato il PKCS#7: per anni questo è stato l'unico formato ritenuto valido.

Un documento PKCS#7 consiste di una "busta crittografica", ossia una struttura di dati che contiene al proprio interno sia il documento oggetto della firma, sia la firma o le firme digitali, certificati, ecc.

Negli anni più recenti si sono affacciati alla ribalta due altri formati, che nelle ultime evoluzioni della normativa hanno trovato piena dignità:

- il formato **PAdES**, ossia il PDF corredato di firme digitali e marche temporali al proprio interno
- il formato **XAdES**, ossia un formato XML che contiene – direttamente nella struttura XML stessa – anche firme e marche temporali

Lo stesso formato PKCS#7 si è arricchito di alcuni attributi e viene ora denominato **CAdES**.

DigitalSign, supporta i tre formati – CAdES, PAdES, XAdES – in conformità al regolamento eIDAS.

2 Installazione e registrazione

2.1 La procedura di installazione

L'installazione di ***DigitalSign*** è di per sé un processo piuttosto semplice.
Tuttavia, va tenuto presente che il prodotto ***DigitalSign*** esiste in diverse edizioni, dai contenuti anche molto differenti tra un'edizione e l'altra.
Inoltre, spesso ***DigitalSign*** viene distribuito da distributori, rivenditori, organizzazioni che lo integrano nei propri sistemi e provvedono a fornire un ambiente di installazione integrato, spesso congiuntamente a software specifico per particolari smartcard, lettori, ecc.; in tal caso occorre seguire le istruzioni pratiche del fornitore.

In generale l'installazione di ***DigitalSign*** consiste in un solo file eseguibile da lanciare per avviare il processo di installazione vero e proprio.

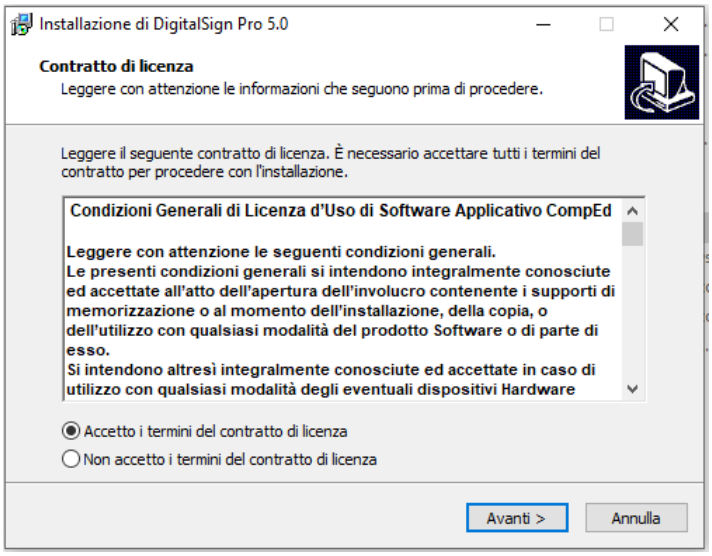
Ad esempio, scaricando DigitalSign Professional da un sito Internet si può ottenere il file

`DS50_PRO_RC596.EXE`

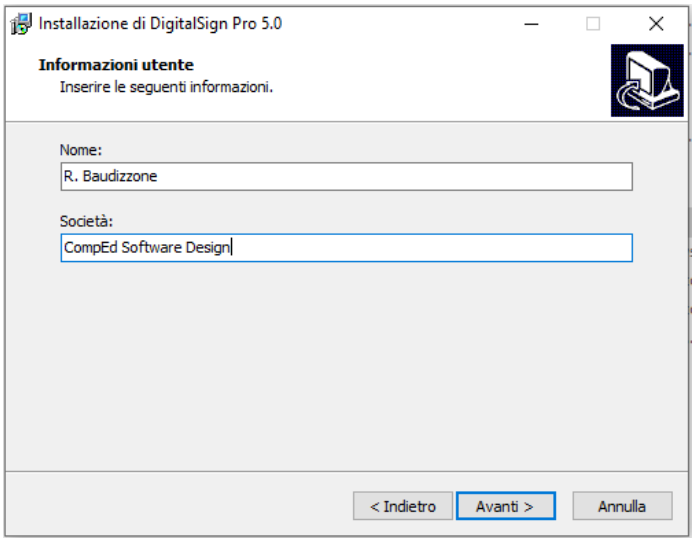
Questo sarebbe il file di installazione per ***DigitalSign Professional*** 5.0.3.596, in edizione standard.

Normalmente l'utente che vede questo file attraverso gli strumenti del proprio sistema farà doppio click su questo programma per avviare il processo di installazione.

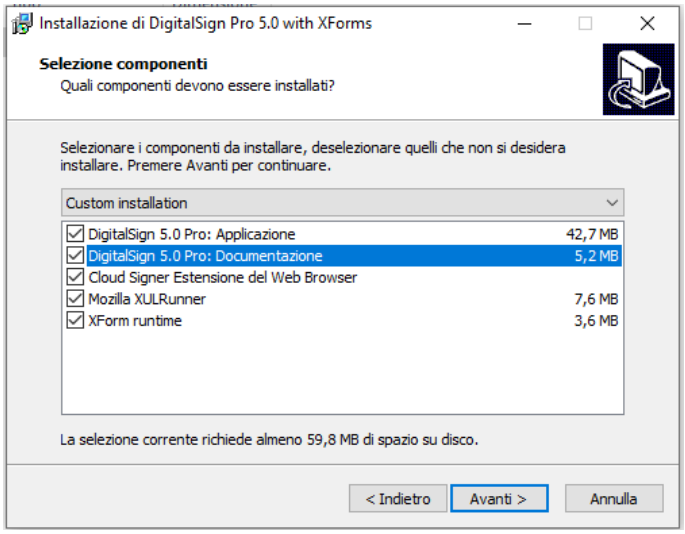
Dopo aver confermato la lingua preferita, tra quelle disponibili, di dovranno accettare le condizioni di licenza d'uso:



Quindi introdurre il proprio nominativo e quello dell'organizzazione di appartenenza, notando che questi dati non vengono trasmessi da ***DigitalSign***, ma vengono solo registrati nel sistema.
È appena il caso di notare che prima di installare e utilizzare una copia di ***DigitalSign*** occorre averne ottenuto regolare licenza.



Seguirà una pagina in cui sono elencati i moduli che possono essere installati:



(questa immagine mostra, in fondo, anche due moduli non presenti in tutte le edizioni: un componente di Mozilla e il runtime XForm, inclusi solo nelle edizioni abilitate all'esecuzione degli XForms, non trattati in questo manuale).

Degno di nota è il ***Cloud Signer - Estensione del Web Browser***: selezionando questa opzione verrà installato anche uno speciale plug-in necessario per far funzionare le estensioni dei browser denominate ***CompEd Cloud Signer***: se l'utente intende usare il sistema ***DigitalSign Cloud*** nella modalità "smartcard" dovrà usare una copia locale di ***DigitalSign Pro*** per interfacciare la smartcard e in tal caso servirà questo plug-in.
Diversamente se ne può fare a meno.

Una vola selezionate le opzioni desiderate si premerà il bottone **Avanti** per avviare l'installazione effettiva (talvolta, se non avevamo chiuso tutte le applicazioni prima di iniziare l'installazione, può essere richiesto il riavvio del sistema).

Si rammenta che l'installazione di ***DigitalSign*** NON COMPRENDE l'installazione di software specifico per lettori e/o smartcard e che tale software deve essere installato separatamente.

2.1.1 Opzioni di linea comando per l'installer

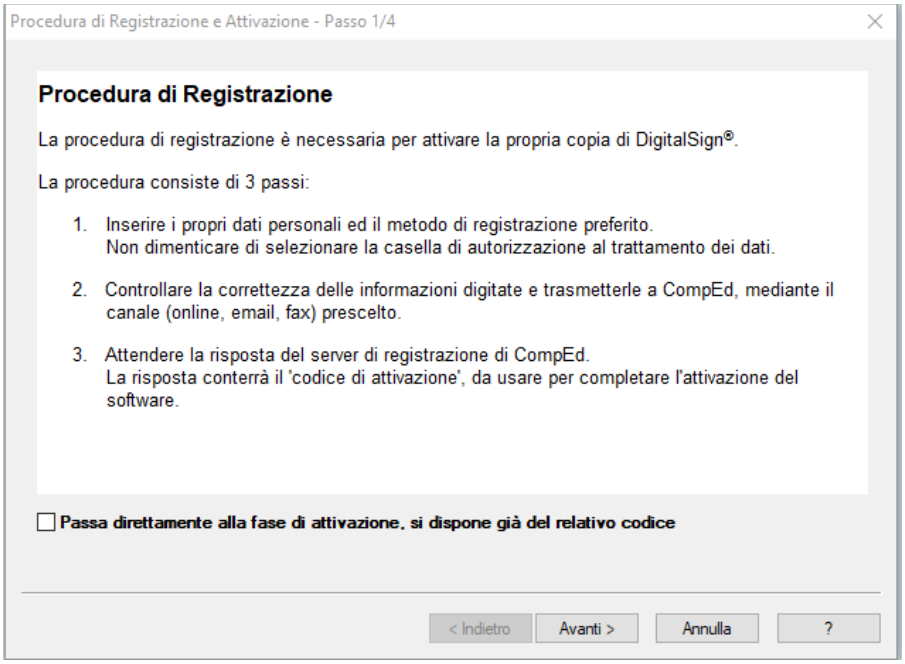
L'eseguibile di installazione (`DS50_PRO_RC596.EXE` nell'esempio della sezione precedente) può essere lanciato dalla linea comandi con alcune opzioni. Di seguito le più significative, gran parte delle quali sono utili quando l'installazione venga lanciata da uno script predisposto dall'utente per automatizzare pe operazioni.

- `/HELP` – visualizza l'intera lista di opzioni disponibili
- `/LANG=it` oppure `/LANG=en` – forza la lingua della localizzazione sull'Italiano o l'Inglese (per default il sistema chiede all'utente, proponendo per default la lingua su cui è impostato il sistema operativo)
- `/SILENT` – il processo di installazione mostra soltanto la schermata con il progresso dell'installazione e null'altro, senza fermarsi a chiedere conferme o scelte dell'operatore
- `/VERYSILENT` – il processo di installazione non mostra nulla e l'installazione avviene in modo invisibile per l'utente
- `/NORESTART` – evita il riavvio del sistema anche nel caso il processo lo raccomandi
- `/RESTARTEXITCODE=<exit code>` – il processo di installazione ritornerà uno specifico codice di uscita nel caso sia raccomandato un riavvio del sistema
- `/SUPPRESSMSGBOXES` – impedisce all'installer di visualizzare qualsiasi MessageBox(). L'effetto finale dipende dalla particolare MessageBox() soppressa: scelta di default, abort dell'installazione, nessun effetto
- `/DIR="x:\dirname"` – consente *l'overriding* del percorso di default visualizzato nella schermata di selezione della cartella di installazione. Occorre fornire un *"fully qualified pathname"*
- `/COMPONENTS="DigitalSign,Help,WebExtension,XULRunner,xform2_rte"` – una stringa che elenchi la lista effettiva di componenti da installare

2.2 Registrazione ed Attivazione

NOTA IMPORTANTE: quasi tutte le edizioni di ***DigitalSign*** richiedono che l'utente esegua una procedura di registrazione preliminare al fine di abilitare il funzionamento.
Tuttavia, anche una copia non registrata può operare con un set minimo di funzionalità: ad esempio interfacciare una smartcard per conto dell'estensione di un browser che esegue una procedura di firma di ***DigitalSign Cloud***. In questo caso l'utente può semplicemente chiudere la procedura di registrazione.

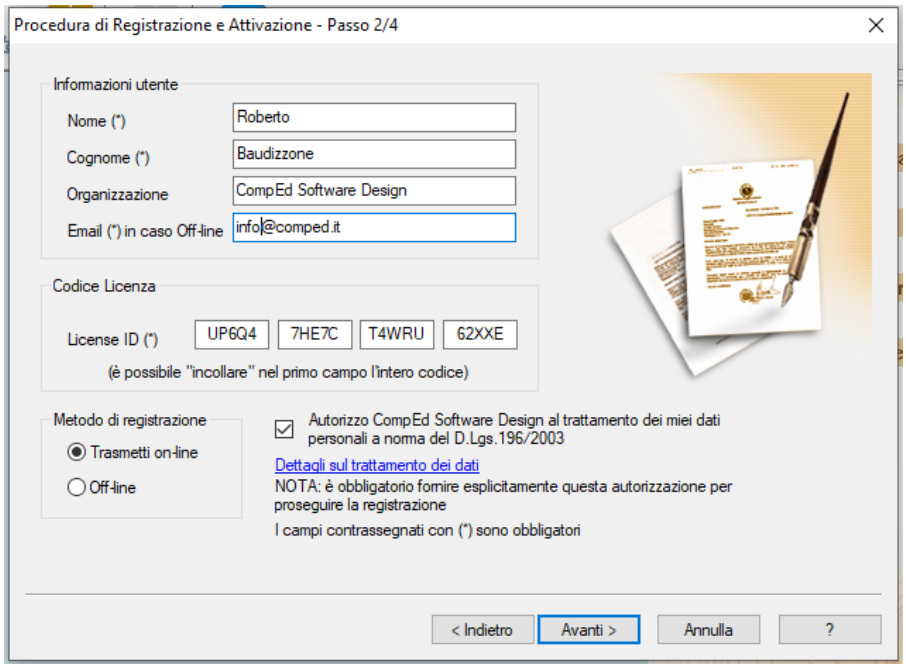
DigitalSign prevede l'esecuzione di una procedura di registrazione, che per alcune edizioni richiede l'introduzione di un **codice licenza**. Al primo avvio la procedura parte automaticamente:



La prima schermata si limita ad informare l'utente sui contenuti della procedura.

NOTA IMPORTANTE: sul fondo di questa pagina si nota una casella, normalmente non selezionata, con l'indicazione **Passa direttamente alla fase di attivazione, si dispone già del relativo codice**.
Come vedremo, questa procedura consente di inserire alcuni dati in modo da ottenere un Codice di Attivazione (da inserire manualmente o automaticamente).
Può capitare che la procedura non si completi fino in fondo e che – dopo aver ricevuto tale codice – sia necessario riavviare la procedura in un secondo tempo: in questo caso, selezionando questa casella l'utente può saltare la prima fase e andare direttamente all'inserimento del Codice di Attivazione.

Con il bottone **Avanti** si procede:

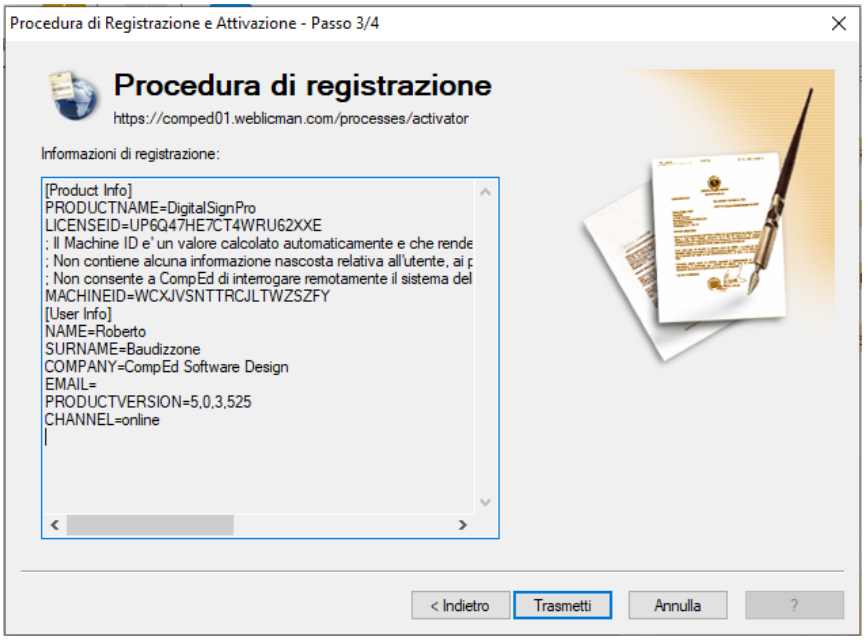


I campi del primo riquadro riguardano i dati personali di registrazione. Tutti i campi contrassegnati con il simbolo '**(*)**' sono obbligatori.

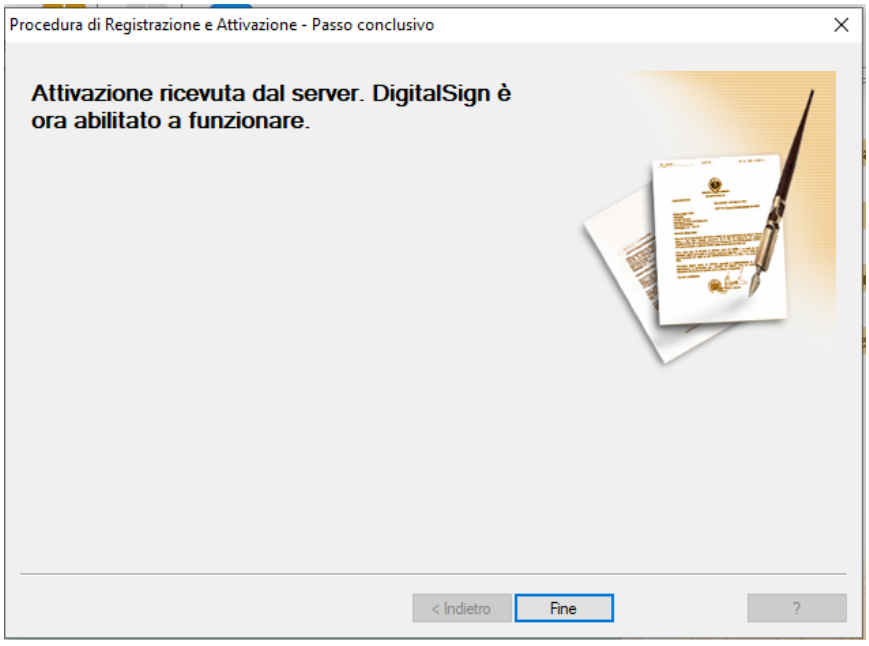
Nel secondo riquadro occorre inserire il Codice Licenza ricevuto dal fornitore, necessario per attivare la propria copia di ***DigitalSign***. Si noti che non tutte le edizioni di prodotto richiedono un Codice Licenza, nel qual caso non è mostrato il simbolo di obbligatorietà **(*)**.

Il terzo riquadro, **Metodo di registrazione**, permette di scegliere la modalità per operare la registrazione/attivazione i dati a CompEd:

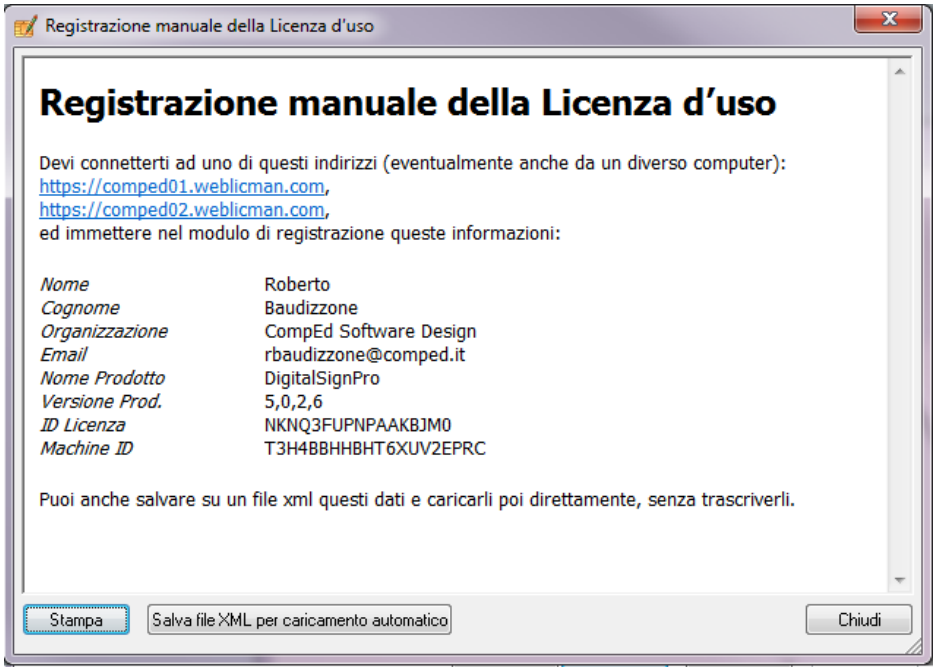
- **Trasmetti on-line** – è il metodo preferito: ***DigitalSign*** si connette direttamente al server di CompEd e trasmette via web i dati di registrazione, così che il server possa immediatamente generare e ritrasmettere il codice di attivazione completando l'attivazione in un attimo.
  Naturalmente questo metodo può essere usato solo se il computer ha un collegamento ad Internet privo di restrizioni per l'accesso alla rete.



Come si vede la finestra visualizza il contenuto dei dati trasmessi e l'indirizzo di spedizione (quest'ultimo può essere utile per la diagnostica di eventuali problemi di rete; si noti che diverse versioni del software possono trasmettere a diversi indirizzi, quello riportato in figura ha solo valore indicativo).
Con il bottone **Trasmetti** avviene il collegamento effettivo e l'attivazione si completa istantaneamente.



- **Off-Line** – questa modalità dovrebbe essere utilizzata quando il computer su cui si effettua l'installazione non ha modo d connettersi direttamente con il server di registrazione via Internet.
  Al passo successivo il sistema si limita a presentare i dati di registrazione ed attendere il bottone Avanti, dopo di che presenterà questa finestra di dialogo:

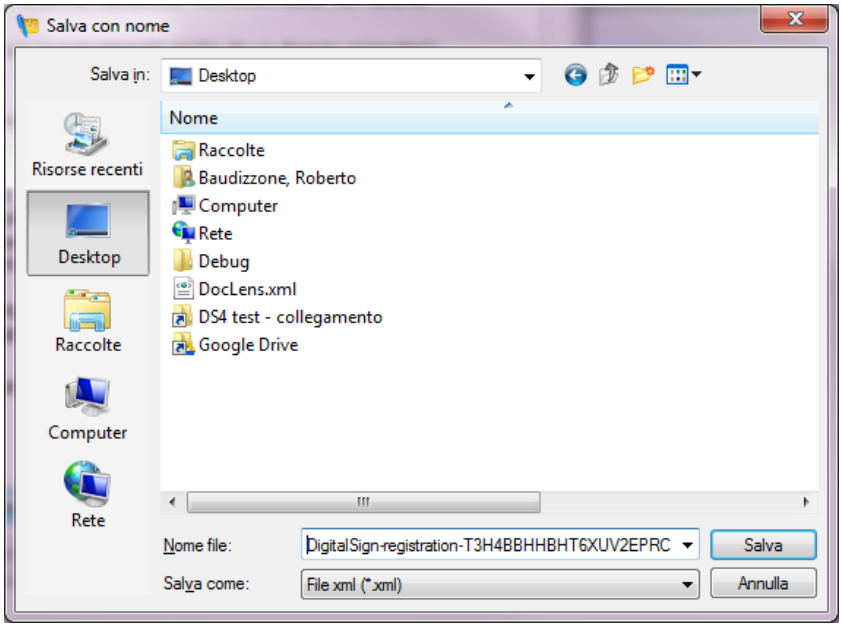


Nelle prossime sezioni illustriamo le diverse modalità per completare questa procedura off-line

2.2.1 Registrazione off-line: modalità XML

Questa modalità è la più comoda, perché non richiede di digitare nulla, ma si basa sul passaggio di un file di parametri.

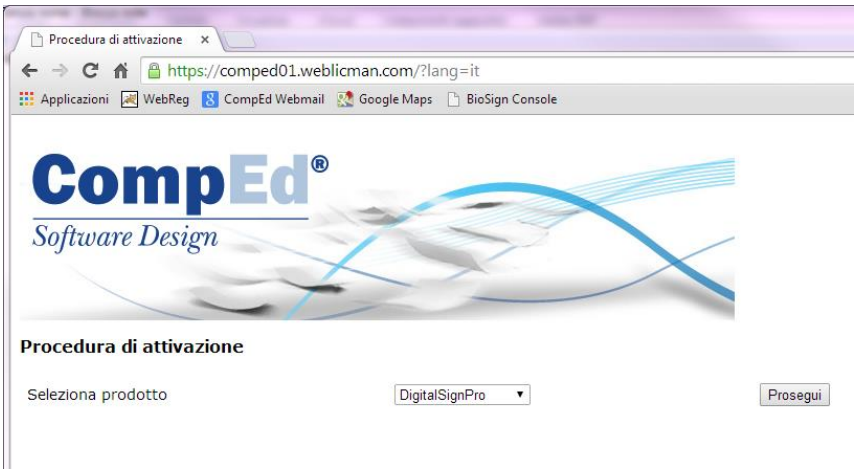
Dalla schermata mostrata in fondo alla sezione precedente si usi il bottone **Salva file XML per caricamento automatico**. Il sistema chiede di indicare una posizione per salvare il file, per esempio sceglieremo il Desktop:



Il file ha un nome piuttosto lungo, composto dal prefisso **DigitalSign-registration-** seguito dal valore del Machine ID e dall'estensione **.xml** (può essere utile ai rivenditori che possono così classificare diversi file relativi a diverse installazioni). Premiamo il bottone **Salva**.

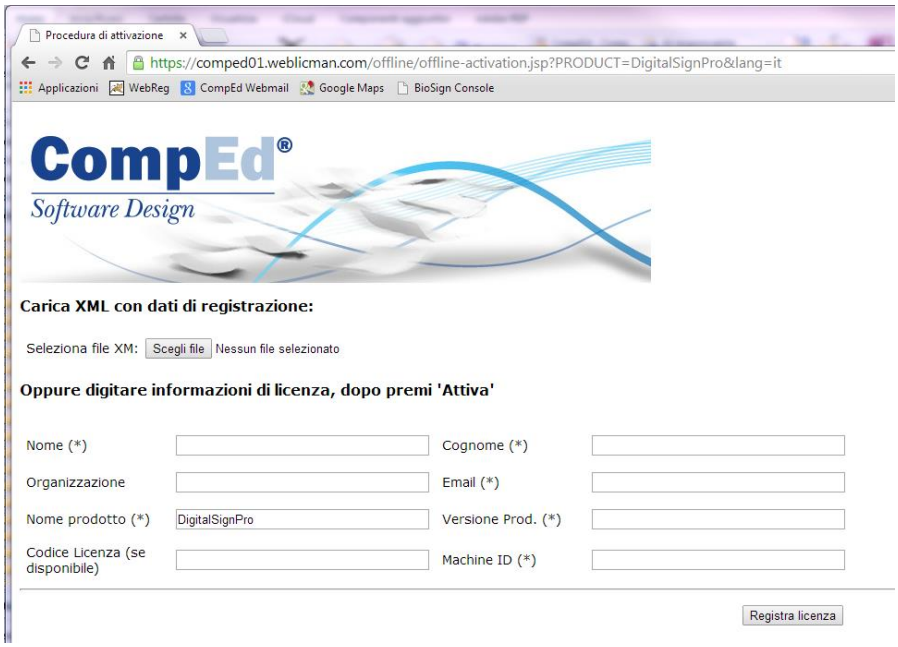
Come indicato dalla schermata della pagina precedente dobbiamo ora aprire un browser Internet (verosimilmente da un diverso computer con accesso a Internet, altrimenti avremmo potuto usare la registrazione Online) e accedere all'indirizzo https://comped01.weblicman.com/?lang=it

Vedremo una pagina di questo tipo:



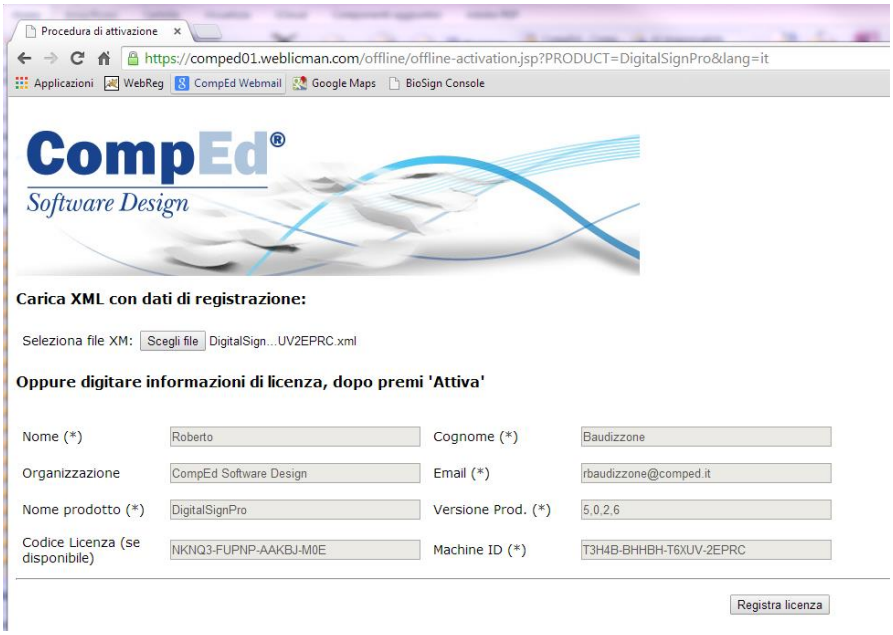
Dopo aver selezionato il prodotto corrispondente alla propria esigenza si agisce su **Prosegui**.

La prossima schermata (ancora in comune con il caso di registrazione manuale) si presenta così:

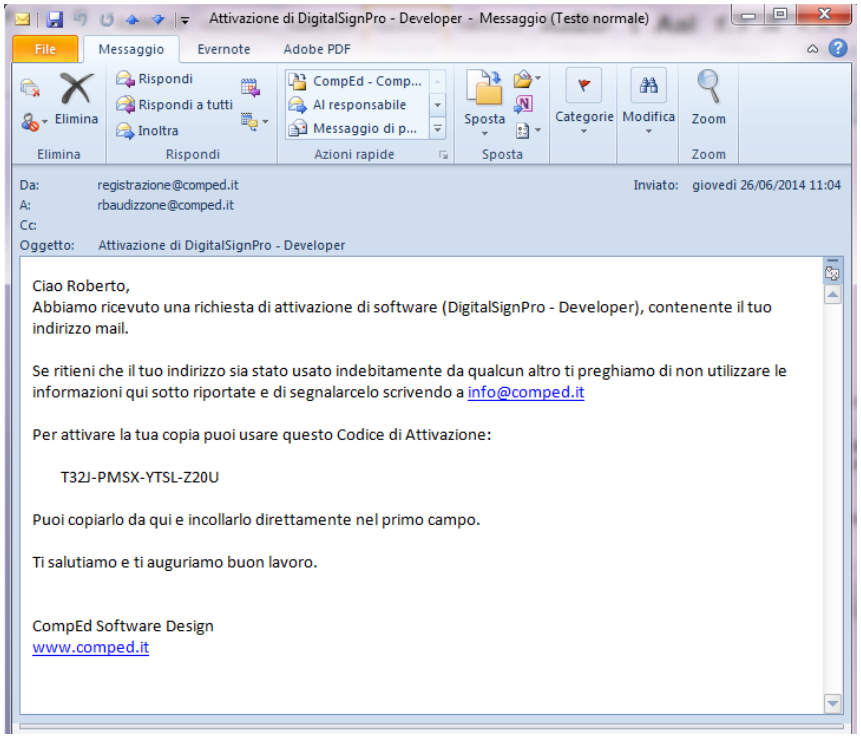


Qui useremo il bottone **Scegli File**, puntando al file XML salvato nel passo precedente. Evidentemente, se ci troviamo su un diverso computer, dovremo aver messo a disposizione il file mediante una chiavetta USB, una email, una cartella condivisa.

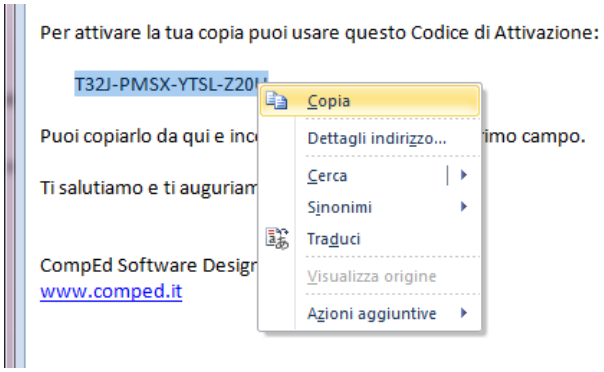
Appena selezionato il file vedremo i campi della registrazione riempirsi automaticamente con il contenuto del file XML:



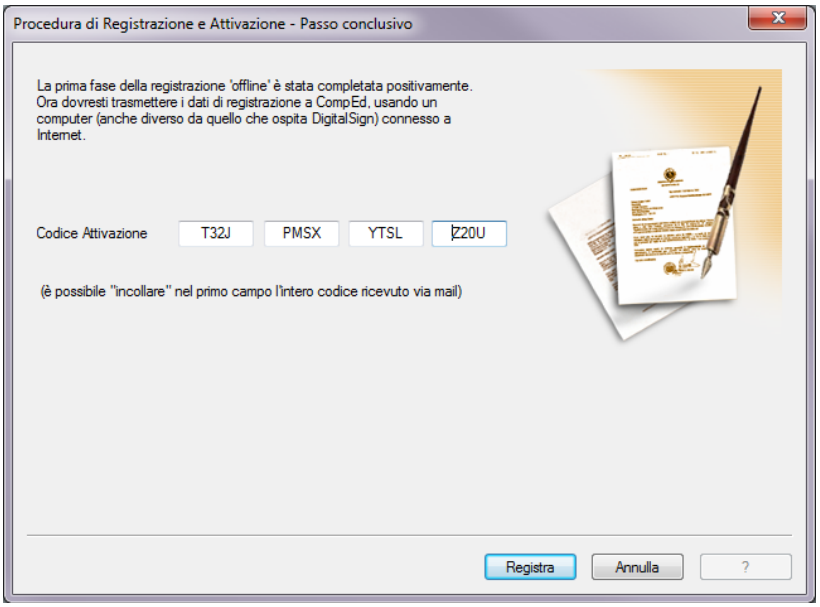
Agendo sul bottone Registra Licenza il sistema genera il Codice di Attivazione e lo trasmette via mail all'indirizzo specificato.



A questo punto selezioneremo e copieremo il Codice di Attivazione dal testo della mail:

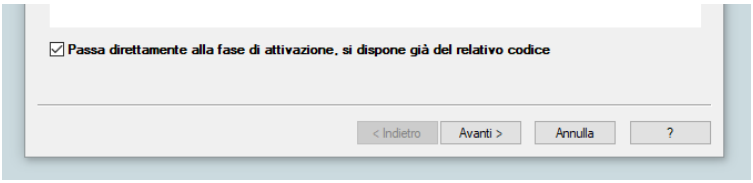


E lo incolleremo direttamente nella finestra di dialogo di ***DigitalSign*** che appare dopo aver premuto **Chiudi** in quella di Registrazione Manuale:

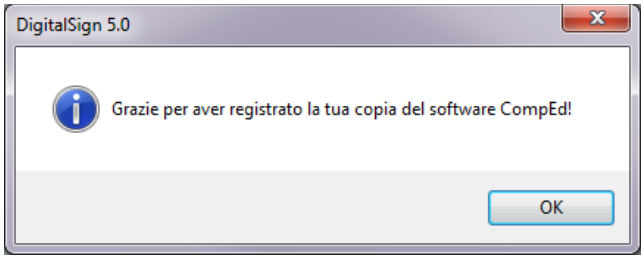


NOTA IMPORTANTE: se avevamo iniziato la procedura di registrazione e avevamo lasciato l'applicazione aperta mentre eseguivamo i passi necessari alla registrazione off-line, avremo ancora questa finestra aperta in attesa sullo schermo.

Ma se questo ci ha richiesto più tempo e nel frattempo avevamo chiuso l'applicazione, potremo tranquillamente riaprirla, quindi selezionare la casella qui indicata per andare direttamente alla pagina di inserimento del Codice di Attivazione:



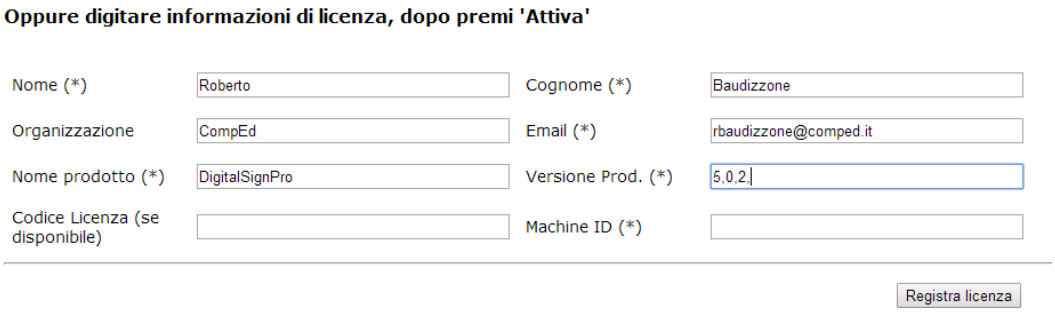
Con **Registra** il processo si conclude:



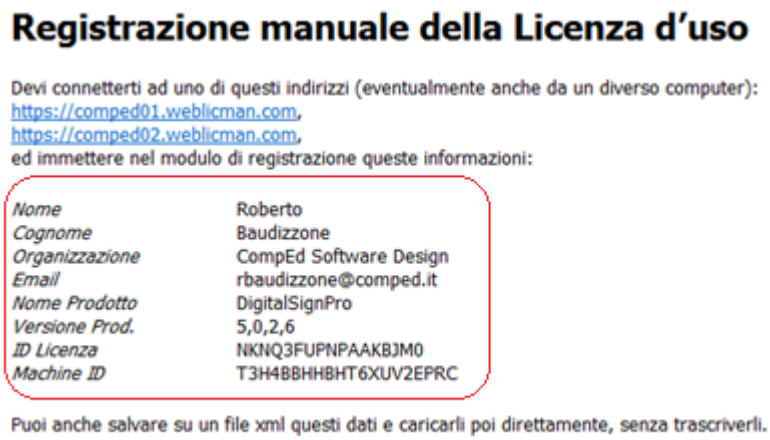
2.2.2 Registrazione off-line: modalità manuale

Questa procedura è quasi identica a quella illustrata al passo precedente.

La differenza consiste nel fatto che non si utilizza il file XML di passaggio dei dati, ma occorre digitare manualmente i dati nella form…



… leggendoli dalla schermata di registrazione manuale:

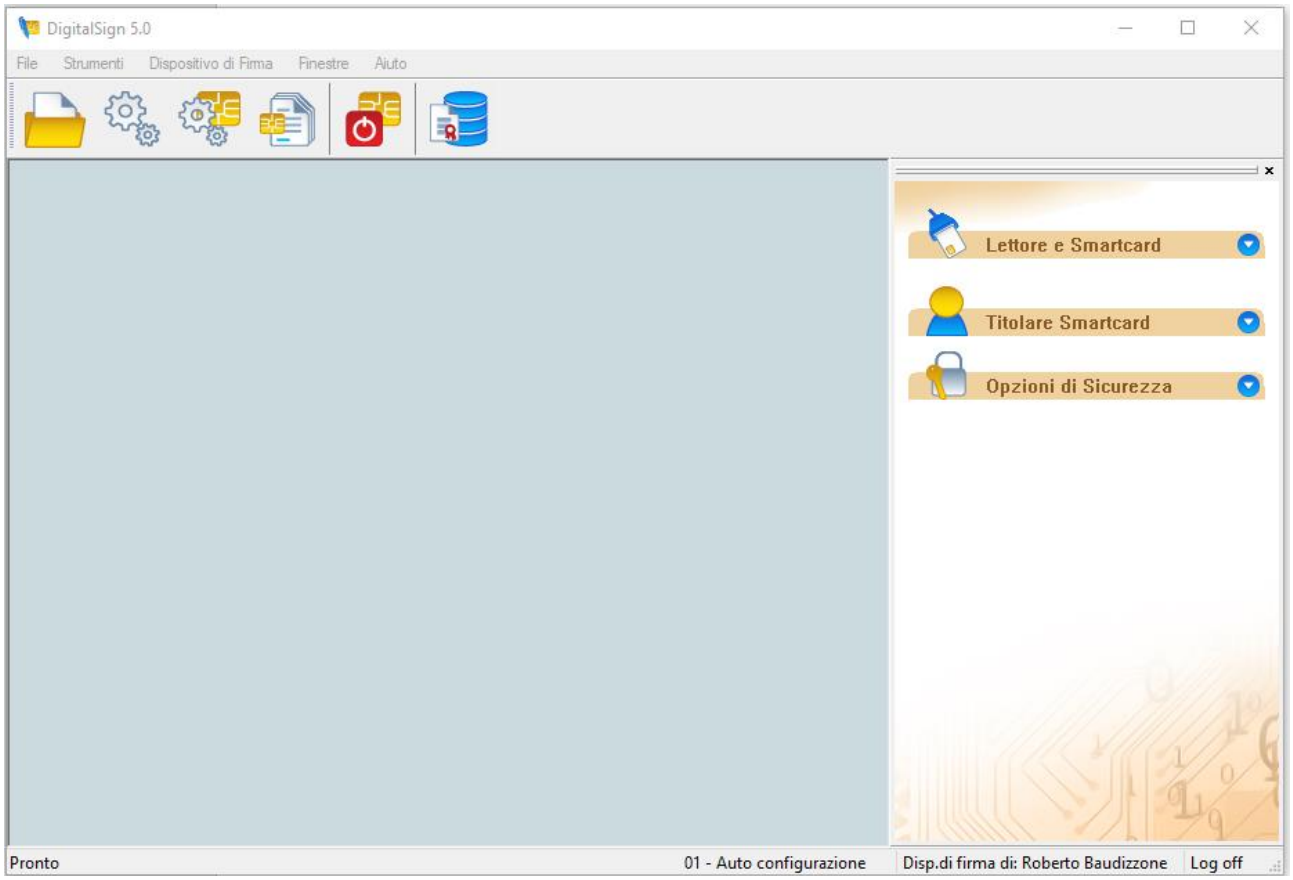


Per il resto la procedura è identica a quella precedente.

3 Riferimento

3.1 DigitalSign sullo schermo

3.1.1 La finestra principale



La finestra principale di ***DigitalSign*** presenta un menu di opzioni di base ed una vista sui pannelli informativi.

In realtà capita di rado di vedere la finestra principale priva di altre finestre, perché normalmente l'applicazione si apre direttamente mostrando una finestra documento.

Da notare che la zona grigia della finestra principale è un'area *drag & drop*, ossia supporta il trascinamento degli oggetti. Questo significa che se da un'altra applicazione (tipicamente **Esplora file** di Windows) si trascina un documento in quest'area, il documento viene immediatamente aperto da ***DigitalSign***.

In ogni caso la finestra principale di ***DigitalSign*** presenta alcuni elementi fondamentali:

- Una barra menu

- Una barra strumenti

- Un'area di pannelli informativi

- Una barra di stato

3.1.2 La finestra documento

DigitalSign gestisce il documento all'interno di una di queste finestre, realizzando una vera e propria modalità **WYSIWYS** *(What You See Is What You Sign)*.

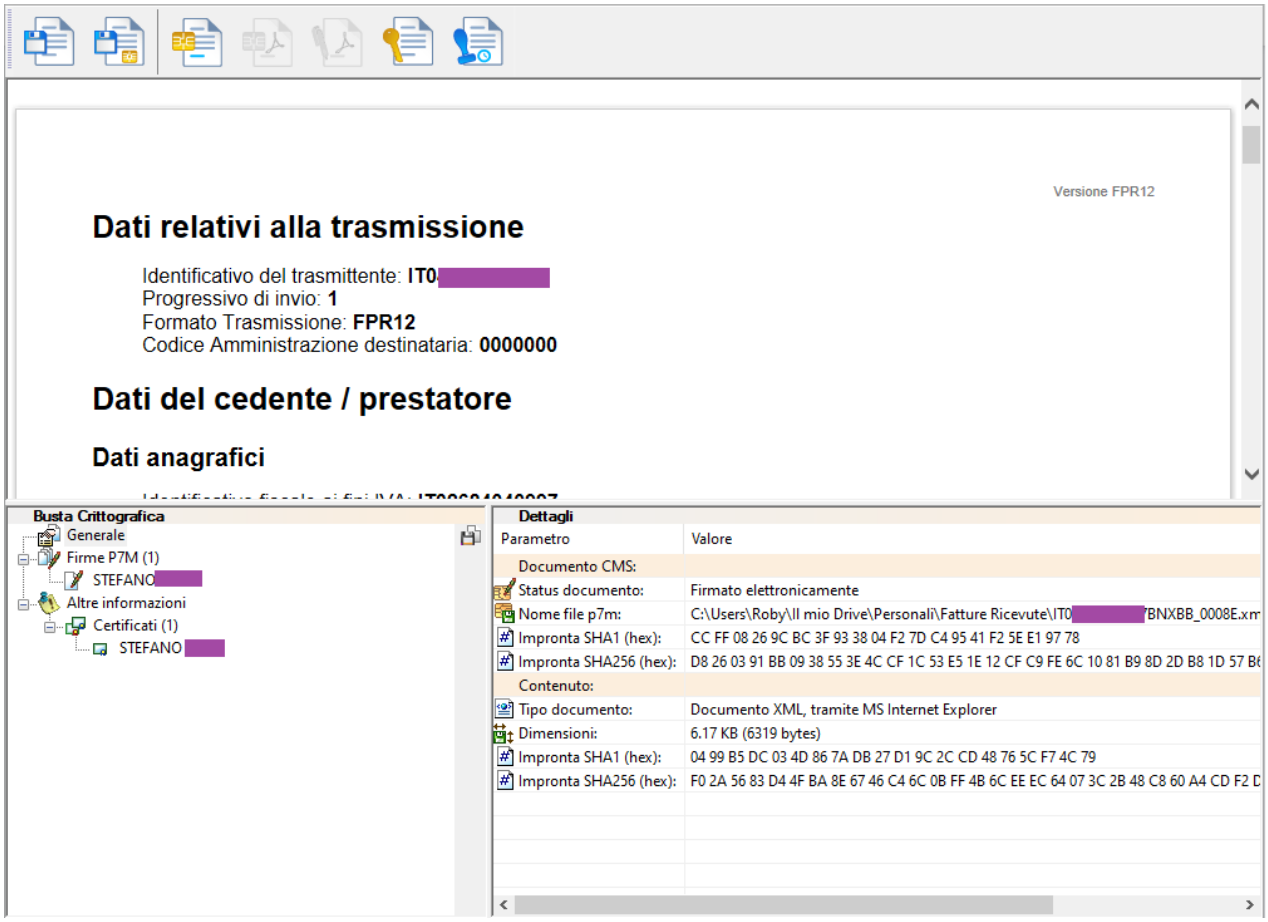
Nelle prossime sezioni illustriamo diversi tipi di documento (CAdES, PAdES, XAdES), ma in ogni caso la finestra documento è composta da diverse aree:

- una **toolbar documento**, diversa da quella della finestra principale, ma che opera con lo stesso principio (ogni icona è associata ad una diversa funzione di menu);
- un'area **viewer**, nella quale viene presentato all'utente il contenuto del documento su cui si sta operando;
- un'area Busta Crittografica, nella quale sono presentati gli oggetti contenuti nella struttura del documento (firme, certificati, ecc.);
- un'area Dettagli, in cui sono visualizzate le informazioni di dettaglio riguardanti l'oggetto correntemente selezionato nell'area **Busta Crittografica**.

3.1.2.1 Documenti di tipo CAdES

I file in formato '**.p7m**' appartengono a questa categoria.
Consistono di una vera e propria "busta crittografica" che contiene sia una copia integrale del documento originari, che la/e firma/e, certificato/i ed opzionalmente marche temporali o altri oggetti.

DigitalSign presenta un documento CAdES in questo modo:



La parte del **viewer** rappresenta il documento originale (una fattura elettronica in formato XML, in questo caso), mentre il pannello in basso a sinistra [**Busta Crittografica**] consente di esaminare tutti gli elementi del documento e quello in basso a destra espande i dettagli dell'elemento correntemente selezionato nel pannello della Busta Crittografica.

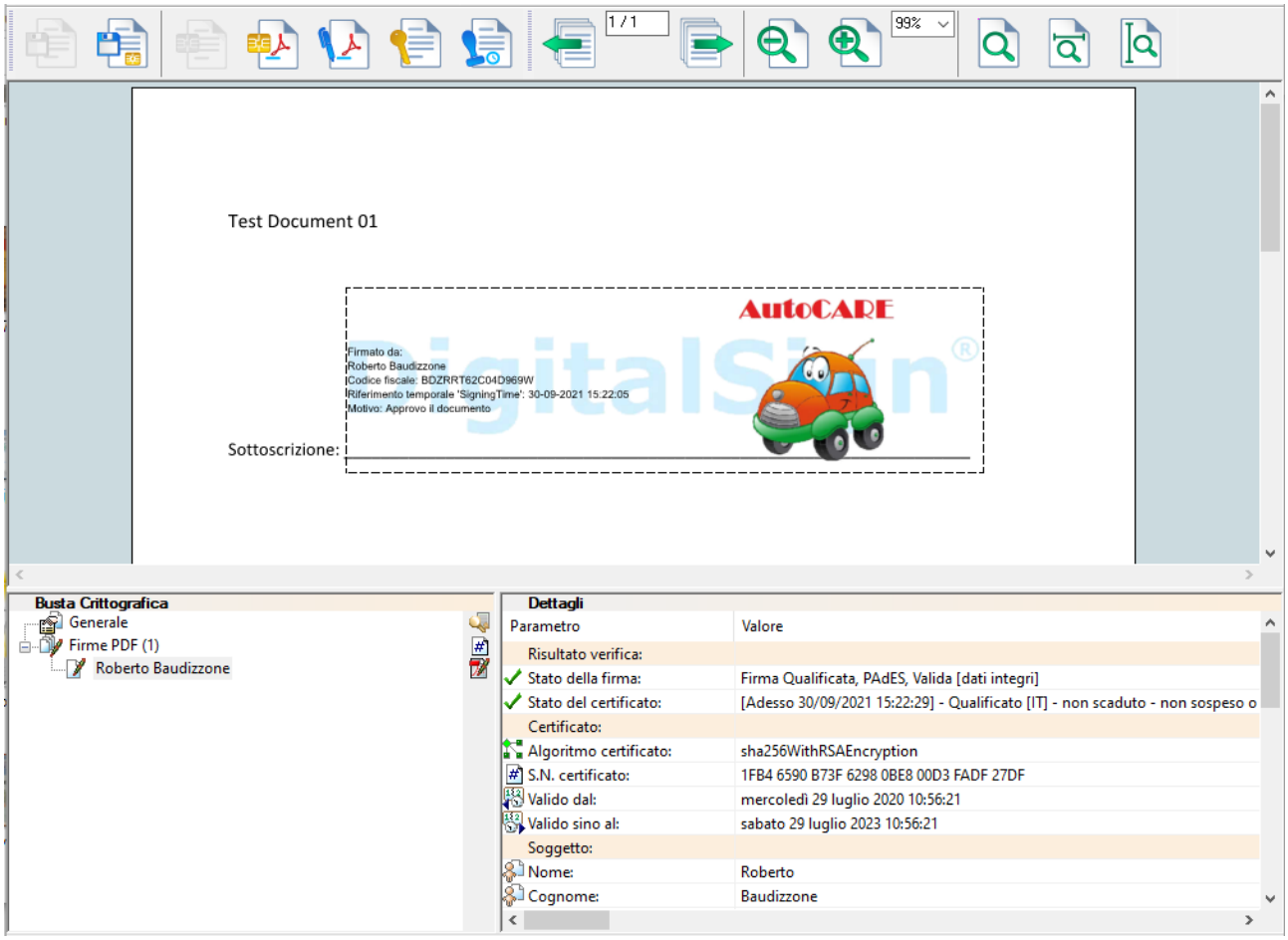
3.1.2.2 Documenti di tipo PAdES

I documenti PDF possono essere corredati di firme digitali e marche temporali direttamente al proprio interno, senza ricorrere ad una sovrastruttura esterna come nel caso CAdES.

Tecnicamente, per ogni firma apposta al documento:

- si aggiunge in coda al file uno spazio vuoto destinato ad accogliere i dati effettivi della firma digitale;
- si aggiunge, in coda allo spazio della firma, una appendice che conterrà le direttive di presentazione grafica della firma (un eventuale oggetto grafico, elementi testuali, posizione, dimensioni, …);
- si calcola la firma digitale sul complesso del documento originario concatenato con l'appendice di presentazione della firma
- si inserisce la firma così calcolata nello spazio vuoto riservato allo scopo

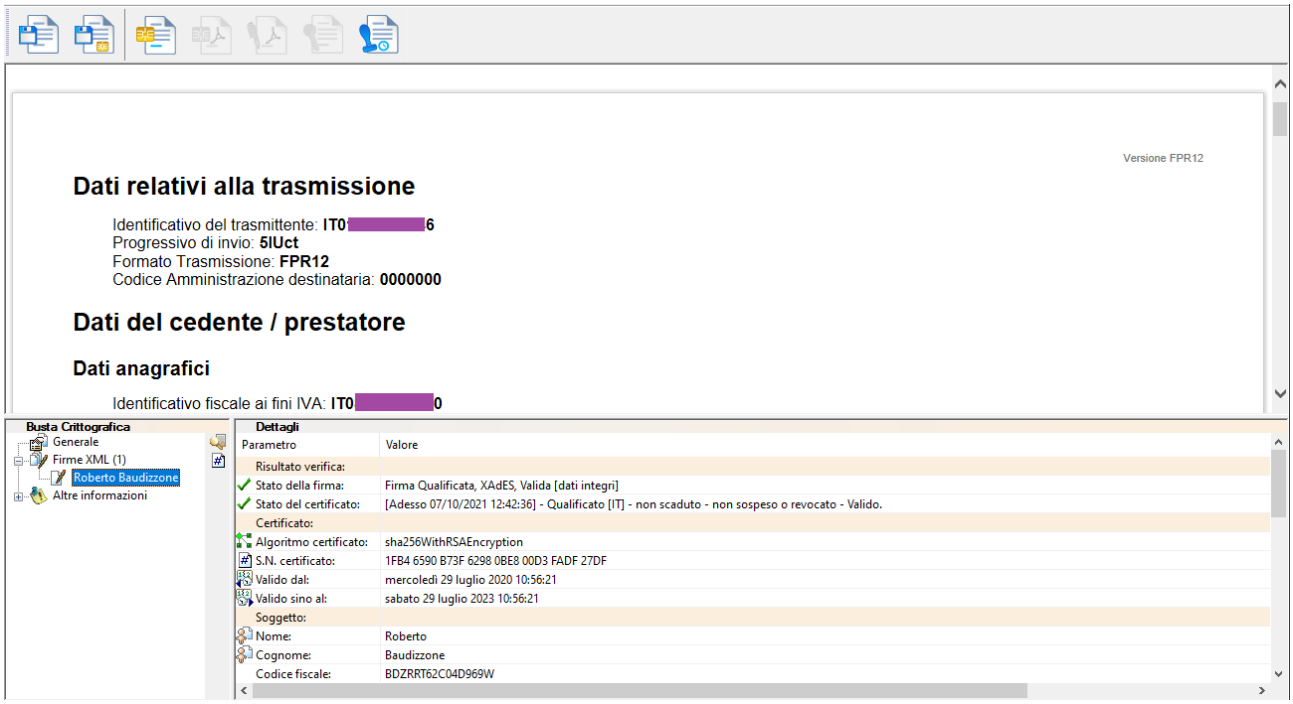
DigitalSign usa per presentare questi documenti lo stesso stile visto prima:



Il vantaggio "ergonomico" del formato PAdES consiste proprio nella possibilità di includere nella presentazione del documento anche una o due immagini (in questo caso un logo sottostante e uno principale), nonché alcune indicazioni estratte dalla firma stessa.

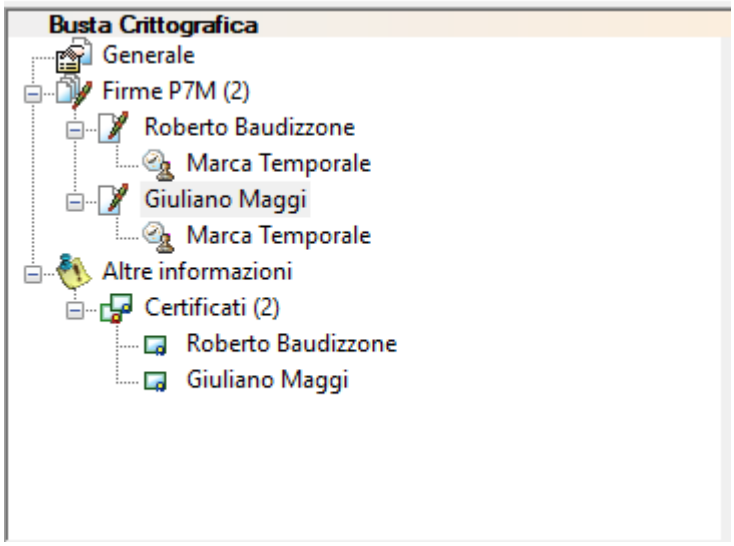
3.1.2.3 Documenti di tipo XAdES

I documenti in formato XML possono essere corredati di firme digitali e marche temporali direttamente al proprio interno, senza ricorrere ad una sovrastruttura esterna come nel caso CAdES.
Tutti gli attributi della firma sono contenuti all'interno dello stesso file XML



3.1.2.4 Finestra documento: area "Busta crittografica"

Questo riquadro, visualizzato in basso a sinistra nella finestra documento, rappresenta l'insieme degli elementi di informazione che, oltre al contenuto vero e proprio del documento, sono contenuti nel file.



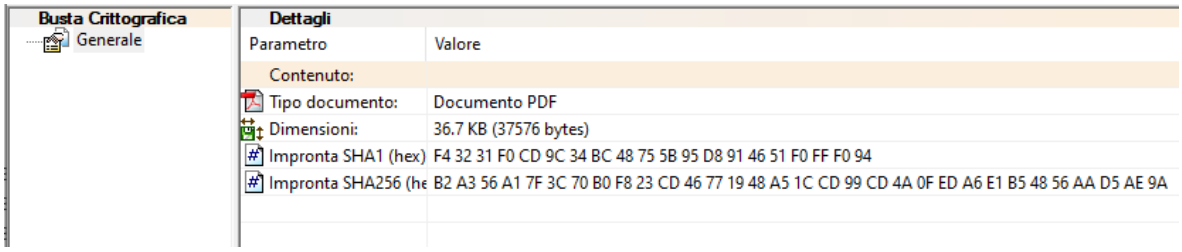
La visualizzazione è presentata come un albero il cui elemento principale è un riepilogo generale. Per gli elementi in cui è riportato il simbolo '+' è possibile agire con il mouse sul simbolo al fine di aprire la visualizzazione del sottoalbero. Analogamente, se è mostrato un simbolo '-', si può richiudere il sottoalbero agendo sul simbolo.

I rami principali dell'albero possono essere:

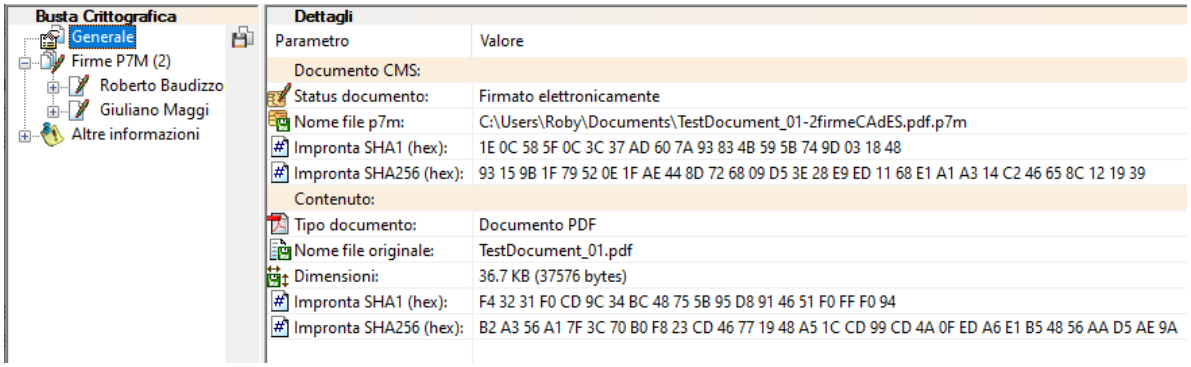
- **Generale**

  Questo elemento presenta un set di informazioni diverse, nell'area Dettagli, secondo il formato del documento aperto.

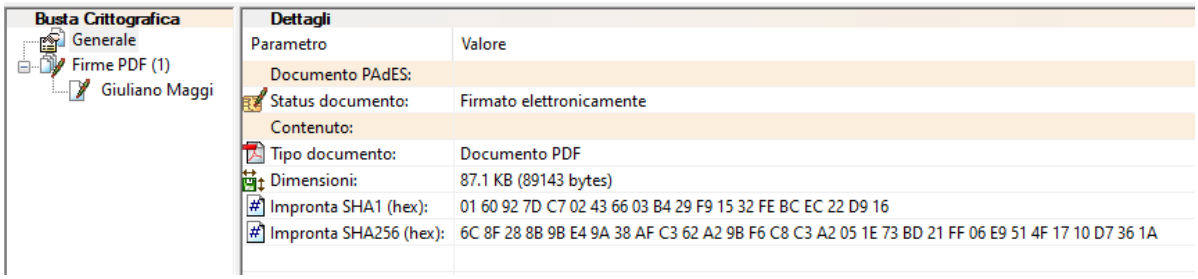
Ad esempio, se il documento non contiene alcuna firma qui si vedono visualizzati il tipo di documento, la dimensione e il valore dell'impronta calcolato con due diverse funzioni hash standard:



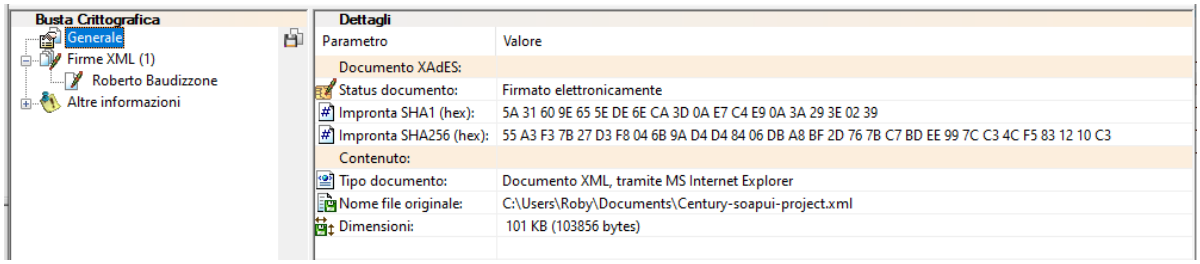
Se il documento è firmato CAdES sono riportate due diverse sezioni: una relativa al file completo (documento + parte crittografica) ed una relativa al contenuto (documento):



Se il documento è firmato PAdES abbiamo una sola sezione, ma si specifica che il documento è firmato:



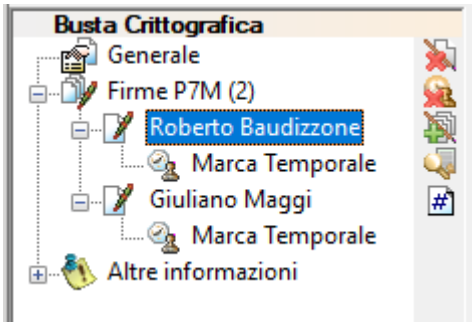
Se il documento è firmato XAdES vedremo:



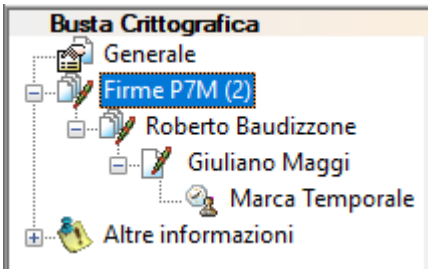
- **Firme**
  Questo sottoalbero, se esistente, contiene una o più *foglie*, ciascuna delle quali corrisponde a una firma elettronica o digitale apposta al documento.
  DigitalSign supporta firme multiple apposte ad un documento, secondo due diverse modalità:

  - ***Firme parallele, o congiunte*** (firme apposte allo stesso livello, riferite al documento, senza reciproci riferimenti tra una firma e l'altra)

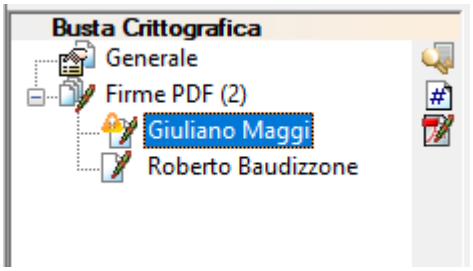
Segue un esempio nel formato CAdES, con due firme parallele (ciascuna corredata anche di una Marca Temporale):



- ***Firme gerarchiche, o controfirme*** (apposte a livelli diversi, una controfirma è riferita alla firma di livello superiore e - solo indirettamente – al documento). In questo esempio la sola controfirma è corredata di una Marca Temporale:
-



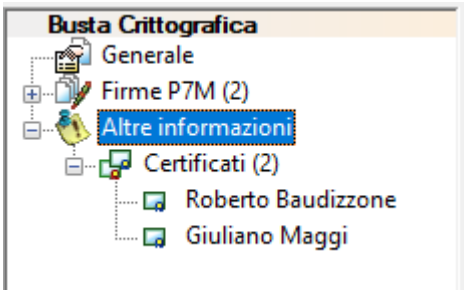
- **Firme Multiple PAdES** (in questo caso la visualizzazione convenzionale è quella di firme parallele, ma di fatto ogni firma è apposta al complesso del documento con tutte le firme già esistenti:



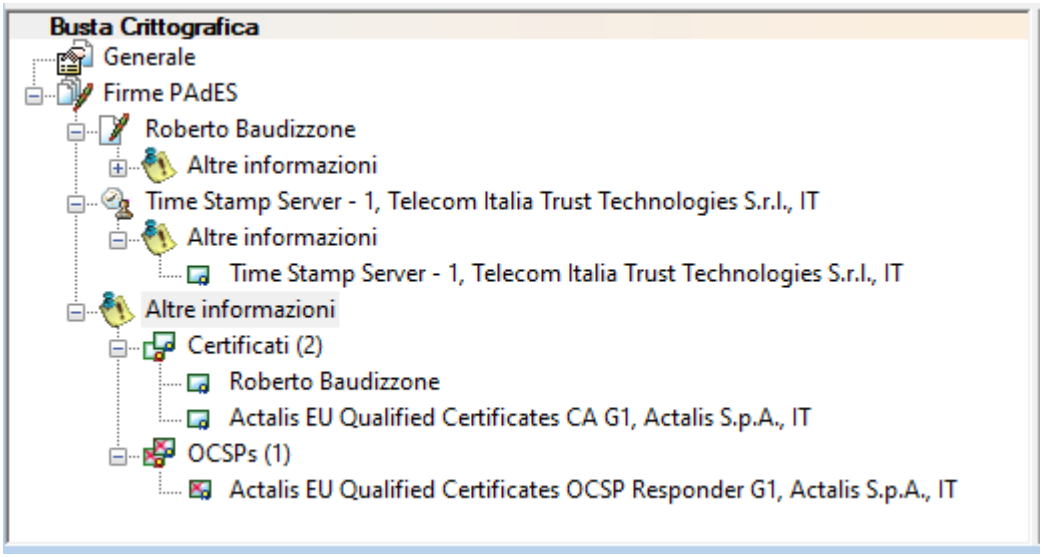
Per questo la prima firma presenta un simbolo di "warning": l'aggiunta della seconda firma non è coperta dalla prima firma.

- **Marche temporali**
  Questo sottoalbero, se esistente, contiene una o più *foglie*, ciascuna delle quali corrisponde a una marca temporale *"detached"*, ossia associata al documento tramite un file distinto (eventualmente riunito con uno formato standard come il '**.tsd'**).
  Si noti che in questo albero non troveremo le M.T. associate alle firme (che sono – appunto – visualizzate con le firme a cui si riferiscono). si veda la sezione dedicata alle marche temporali.

- **Altre informazioni**
  Questo albero può trovarsi al primo livello, nel caso di documenti CAdES, oppure sotto l'albero delle firme o un altro sottoalbero.
  Il suo scopo è contenere (visualizzare) altri oggetti significativi contenuti nella busta crittografica.
  Di regola contiene i certificati usati per generare ogni firma:

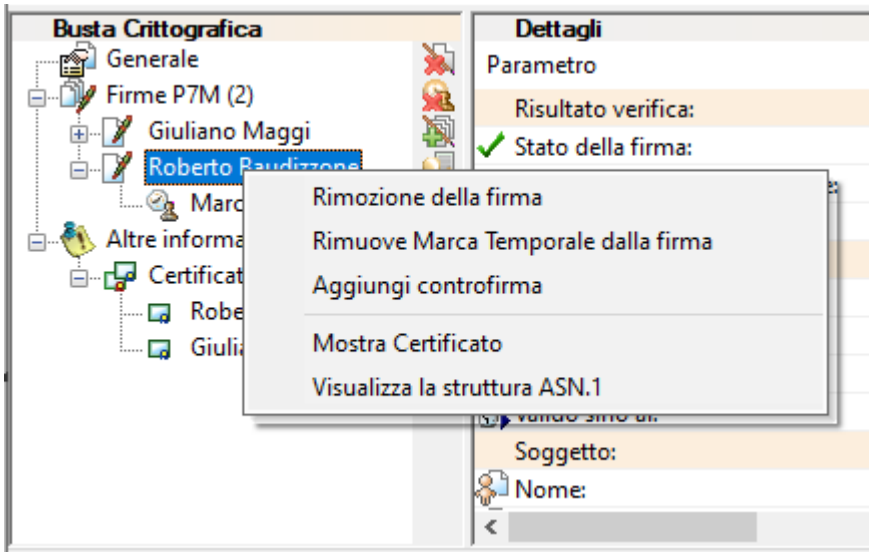


  In altri casi (ad esempio i documenti PDF firmati in modalità LTV) contiene anche le informazioni utili a dimostrare che i certificati non erano sospesi o revocati al momento della firma:



Il lato destro di questo pannello ospita una *toolbar* verticale attraverso la quale l'utente può accedere rapidamente alle operazioni possibile, senza dover utilizzare il menu o le *toolbar* della finestra principale.
Naturalmente le operazioni possibili variano secondo il tipo di elemento correntemente selezionato.
Passando con il cursore sulle relative icone si ottiene una spiegazione di ogni funzione.

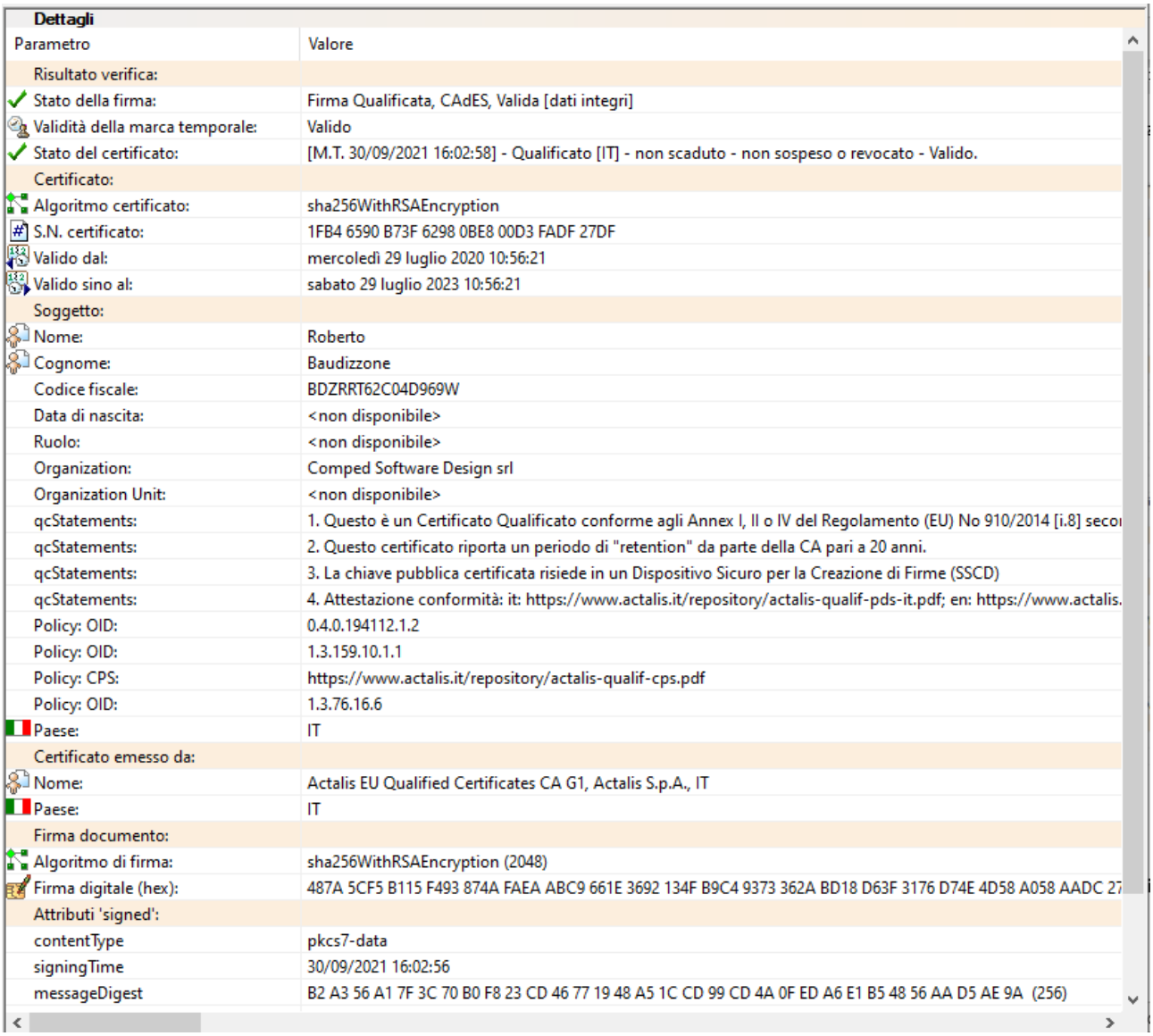
Le stesse funzioni sono anche disponibili tramite un "pop-up" menu che appare agendo con il tasto destro su un elemento della finestra:



3.1.2.5 Finestra documento: area "Dettagli"

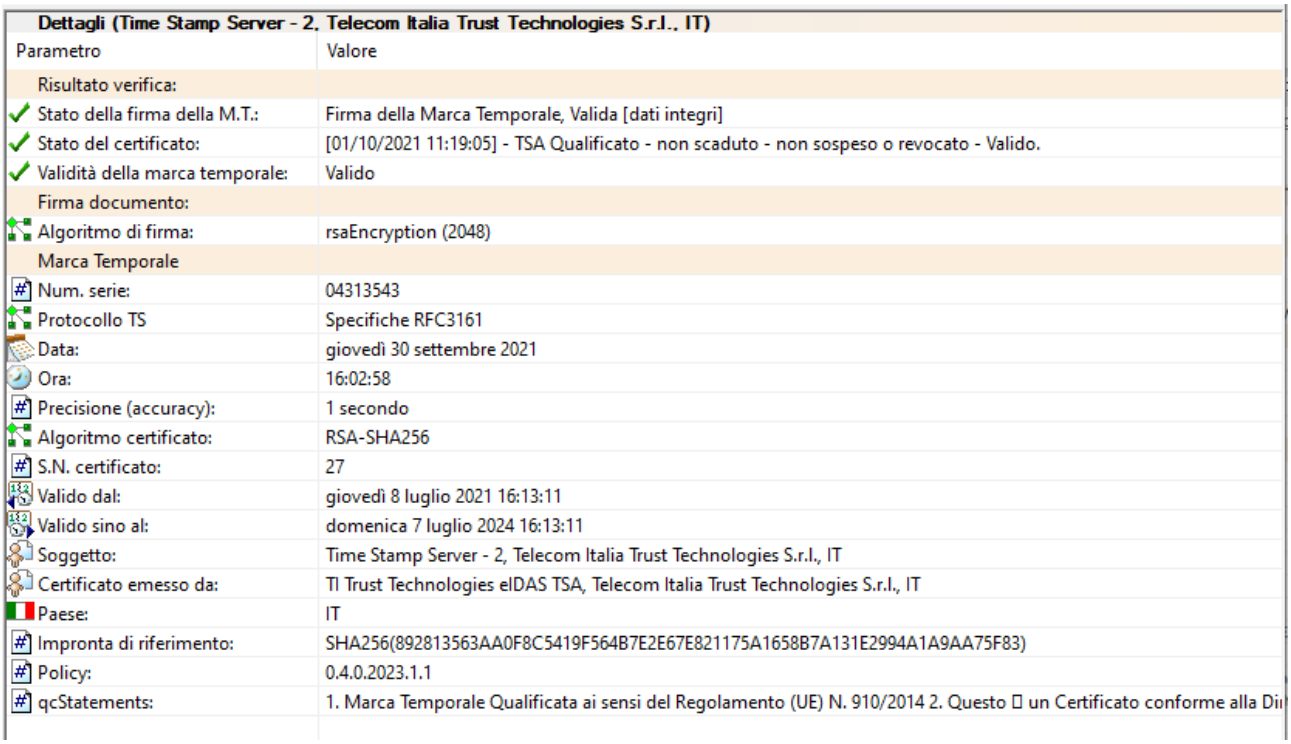
Questo riquadro della finestra documento mostra in generale una tabella in due colonne nella quale sono rappresentate le informazioni di dettaglio disponibili per l'oggetto correntemente selezionato nell'area della Busta Crittografica. Si noti che la rappresentazione è molto completa, consente di ispezionare ogni elemento in profondità

L'esempio che segue mostra il contenuto (parziale) di questo riquadro quando visualizza i dettagli di una **firma digitale**:



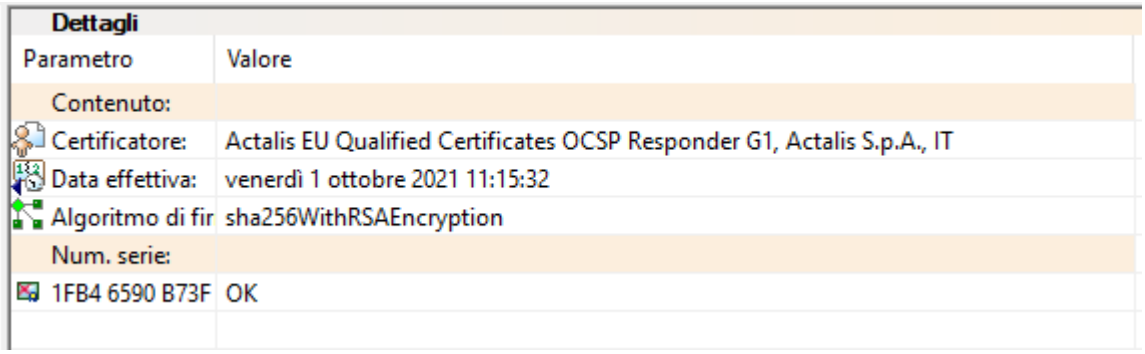
Dettagli	
Parametro	Valore
Risultato verifica:	
Stato della firma:	Firma Qualificata, CAdES, Valida [dati integri]
Validità della marca temporale:	Valido
Stato del certificato:	[M.T. 30/09/2021 16:02:58] - Qualificato [IT] - non scaduto - non sospeso o revocato - Valido.
Certificato:	
Algoritmo certificato:	sha256WithRSAEncryption
S.N. certificato:	1FB4 6590 B73F 6298 0BE8 00D3 FADF 27DF
Valido dal:	mercoledì 29 luglio 2020 10:56:21
Valido sino al:	sabato 29 luglio 2023 10:56:21
Soggetto:	
Nome:	Roberto
Cognome:	Baudizzone
Codice fiscale:	BDZRRT62C04D969W
Data di nascita:	<non disponibile>
Ruolo:	<non disponibile>
Organization:	Comped Software Design srl
Organization Unit:	<non disponibile>
qcStatements:	1. Questo è un Certificato Qualificato conforme agli Annex I, II o IV del Regolamento (EU) No 910/2014 [i.8] seco
qcStatements:	2. Questo certificato riporta un periodo di "retention" da parte della CA pari a 20 anni.
qcStatements:	3. La chiave pubblica certificata risiede in un Dispositivo Sicuro per la Creazione di Firme (SSCD)
qcStatements:	4. Attestazione conformità: it: https://www.actalis.it/repository/actalis-qualif-pds-it.pdf; en: https://www.actalis.
Policy: OID:	0.4.0.194112.1.2
Policy: OID:	1.3.159.10.1.1
Policy: CPS:	https://www.actalis.it/repository/actalis-qualif-cps.pdf
Policy: OID:	1.3.76.16.6
Paese:	IT
Certificato emesso da:	
Nome:	Actalis EU Qualified Certificates CA G1, Actalis S.p.A., IT
Paese:	IT
Firma documento:	
Algoritmo di firma:	sha256WithRSAEncryption (2048)
Firma digitale (hex):	487A 5CF5 B115 F493 874A FAEA ABC9 661E 3692 134F B9C4 9373 362A BD18 D63F 3176 D74E 4D58 A058 AADC 27
Attributi 'signed':	
contentType	pkcs7-data
signingTime	30/09/2021 16:02:56
messageDigest	B2 A3 56 A1 7F 3C 70 B0 F8 23 CD 46 77 19 48 A5 1C CD 99 CD 4A 0F ED A6 E1 B5 48 56 AA D5 AE 9A (256)

Questi i dettagli di una Marca Temporale:



Dettagli (Time Stamp Server - 2, Telecom Italia Trust Technologies S.r.l., IT)	
Parametro	Valore
Risultato verifica:	
Stato della firma della M.T.:	Firma della Marca Temporale, Valida [dati integri]
Stato del certificato:	[01/10/2021 11:19:05] - TSA Qualificato - non scaduto - non sospeso o revocato - Valido.
Validità della marca temporale:	Valido
Firma documento:	
Algoritmo di firma:	rsaEncryption (2048)
Marca Temporale	
Num. serie:	04313543
Protocollo TS	Specifiche RFC3161
Data:	giovedì 30 settembre 2021
Ora:	16:02:58
Precisione (accuracy):	1 secondo
Algoritmo certificato:	RSA-SHA256
S.N. certificato:	27
Valido dal:	giovedì 8 luglio 2021 16:13:11
Valido sino al:	domenica 7 luglio 2024 16:13:11
Soggetto:	Time Stamp Server - 2, Telecom Italia Trust Technologies S.r.l., IT
Certificato emesso da:	TI Trust Technologies elDAS TSA, Telecom Italia Trust Technologies S.r.l., IT
Paese:	IT
Impronta di riferimento:	SHA256(892813563AA0F8C5419F564B7E2E67E821175A1658B7A131E2994A1A9AA75F83)
Policy:	0.4.0.2023.1.1
qcStatements:	1. Marca Temporale Qualificata ai sensi del Regolamento (UE) N. 910/2014 2. Questo □ un Certificato conforme alla Di

Questo è un esempio di *"response OCSP"*, ossia l'informazione fornita dal server della CA quando interrogato sullo stato di sospensione e revoca di un certificato:



Dettagli	
Parametro	Valore
Contenuto:	
Certificatore:	Actalis EU Qualified Certificates OCSP Responder G1, Actalis S.p.A., IT
Data effettiva:	venerdì 1 ottobre 2021 11:15:32
Algoritmo di fir	sha256WithRSAEncryption
Num. serie:	
1FB4 6590 B73F	OK

3.1.3 La barra menu di DigitalSign

La barra menu principale di ***DigitalSign*** raggruppa i menu di comandi e funzioni accessibili all'utente.

La barra menu contiene i seguenti menu:

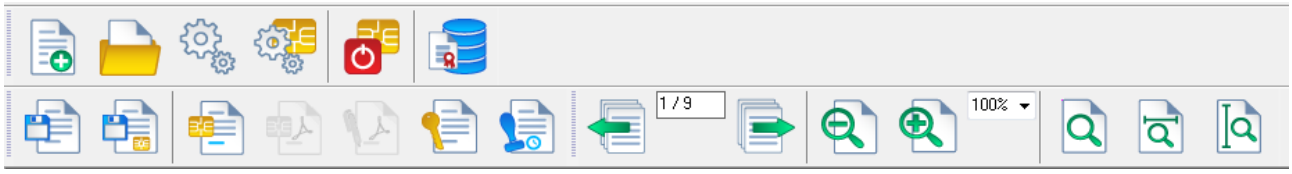
File
Strumenti
Dispositivo di Firma
Finestre
Aiuto

Quando è aperta una finestra documento può essere disponibile anche un altro menu:

Documento

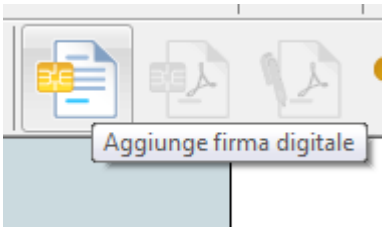
3.1.4 Le barre strumenti *(toolbar)*

Le toolbar di ***DigitalSign*** sono configurabili da parte dell'utente e contengono alcuni bottoni con icone grafiche corrispondenti alle funzioni di uso più comune, normalmente accessibili attraverso il menu.



L'aspetto effettivo delle toolbar dipende dall'edizione di ***DigitalSign*** a disposizione, dalle funzioni abilitate al momento, dal tipo di documento eventualmente aperto e selezionato, dalla disponibilità o meno di un dispositivo di firma inserito, dalle caratteristiche dello stesso dispositivo.

Passando con il puntatore del mouse sopra una icona di una toolbar si visualizza un *tooltip* che richiama l'associata voce del menu:



Le toolbar sono configurabili attraverso il menu Strumenti -> Opzioni, scegliendo poi il tab **Toolbar** che conduce ad una apposita finestra di configurazione.

3.1.5 I Pannelli Informativi

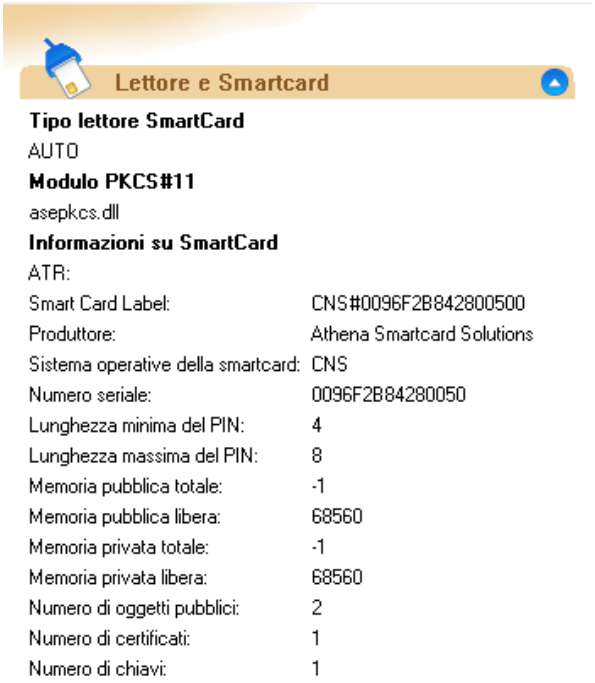
Nella finestra principale di ***DigitalSign*** possono essere visualizzati (per tramite del menu Finestre) alcuni pannelli di informazione, che a loro volta possono essere chiusi o aperti agendo sul simbolo a forma di freccia.

Questi pannelli consentono soltanto di visualizzare rapidamente alcune informazioni relative alla configurazione corrente del dispositivo di firma e delle opzioni di security impostate, ma non permettono di modificare direttamente tali informazioni.

L'illustrazione sopra riportata mostra i pannelli tutti in posizione chiusa. Operando sul simbolo a destra è possibile aprire (o richiudere) tutti i pannelli.

I pannelli disponibili sono:

- **Lettore e smartcard**

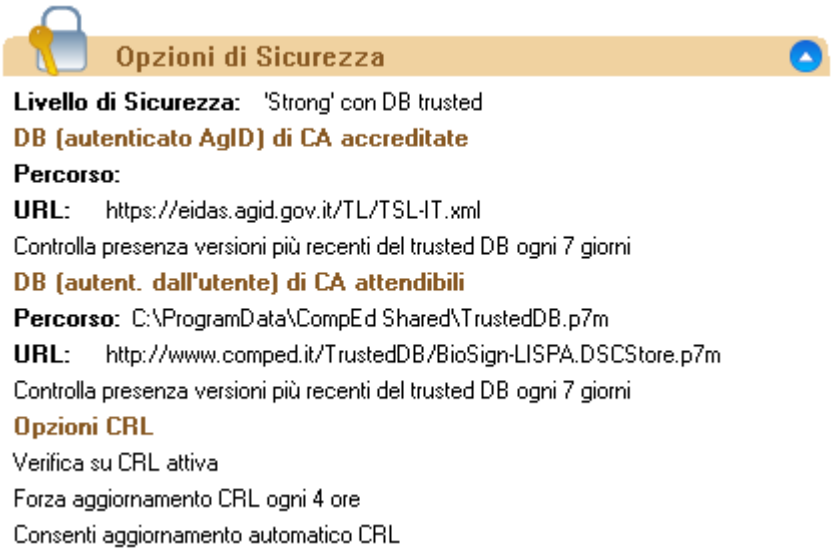


Questo pannello mostra alcuni dettagli relativi al lettore di smartcard correntemente attivo, all'eventuale modulo PKCS#11 tramite cui avviene il collegamento al dispositivo, alla particolare smartcard inserita nel lettore

- **Titolare Smartcard**

Questo pannello mostra alcuni dettagli sull'identità del titolare del dispositivo di firma correntemente inserito nel lettore. I dati visualizzati sono estratti dal certificato letto dal dispositivo stesso.

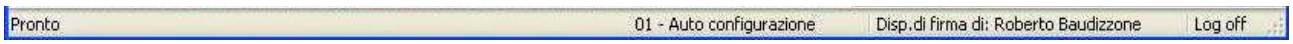
- **Opzioni di Sicurezza**



Questo pannello mostra le informazioni principali relativamente alle opzioni di *security* correntemente attive.
Per modificare la configurazione di tali opzioni si utilizza il menu Strumenti -> Opzioni di Security

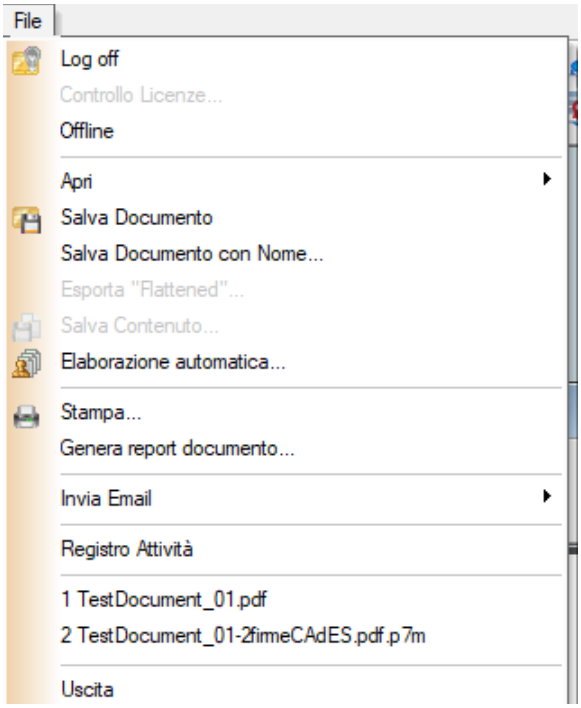
3.1.6 La barra di stato

La barra di stato principale di ***DigitalSign*** viene mostrata alla base della finestra principale dell'applicazione



Come si può notare la status bar principale mostra informazioni relative allo stato di funzionamento di ***DigitalSign***, alla modalità di gestione dell'interfaccia al dispositivo di firma, al titolare del dispositivo di firma correntemente inserito, allo stato di *Logon* o di *Logoff* del dispositivo stesso.

3.2 Il menu "File"



Questo menu contiene diverse funzioni, alcune delle quali possono non essere disponibili, per esempio se nessun documento è aperto.
Oltre alle funzioni descritte nelle sezioni seguenti, è di norma presente – come illustrato in figura – anche una lista di elementi corrispondenti agli ultimi documenti elaborati (max. 5), utili per aprire in modo immediato un documento utilizzato di recente.

Gli elementi di menu sono visualizzati accanto al simbolo dell'eventuale icona della barra strumenti che esegue la stessa funzione.

3.2.1 Log On / Log Off

Funzione non disponibile con DigitalSign Reader

Questa funzione di menu consente di porre il dispositivo di firma (la smartcard o il servizio di firma remota) in uno stato di **Log On**: tale stato consente di accedere a tutte le funzioni riservate al legittimo titolare del dispositivo, in particolare la generazione di una firma.
Per passare allo stato di Log On è necessario immettere il PIN del dispositivo tramite una apposita finestra di dialogo.

La funzione non è utilizzabile se nessun dispositivo di firma è inserito.

Se il dispositivo è già in tale stato di Logon questa funzione lo pone in stato di Logoff, disattivandone le funzioni.

La voce di menu mostra la dicitura **Log On** se il dispositivo è disattivo, oppure **Log Off** se il dispositivo già è attivo.

3.2.2 Controllo licenze

Questa funzione è abilitata soltanto nelle edizioni di DigitalSign fornite in package con altri prodotti CompEd, come Legal Document System ®, o più in generale nei contesti in cui esiste un sistema centralizzato di controllo della licenza d'uso (CompEd License Manager).

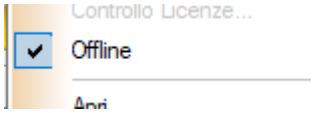
Scopo di questa funzione è visualizzare lo stato della licenza d'uso.

3.2.3 Offline

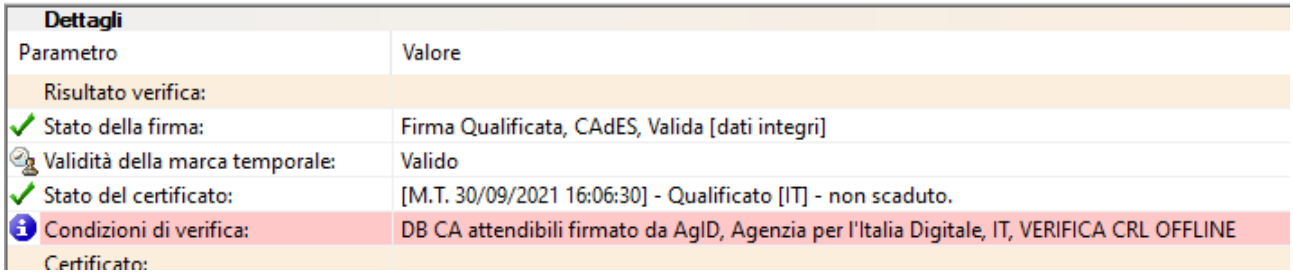
Questa funzione consente di sospendere centralmente tutte le operazioni di ***DigitalSign*** con servizi remoti. Passando a **Offline** non sarà più verificato lo stato di revoca dei certificati, non sarà possibile richiedere Marche Temporali, aggiornare le liste di certificati attendibili, …

Lo stesso risultato, naturalmente, si può ottenere disabilitando singolarmente tutti questi servizi, ma può essere utile usare questa funzione se – temporaneamente – il computer è privo di accesso ad Internet: sarà quindi più rapido tornare allo stato di **Online** disattivando questa impostazione.

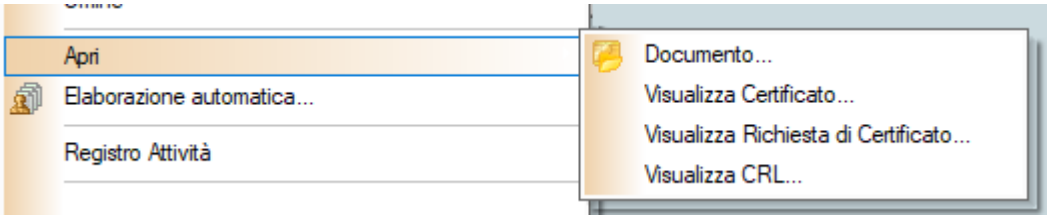
L'elemento di menu mostra il segno di spunta quando lo stato è **Offline**:



La verifica di un documento o di un certificato evidenzia il fatto che non è possibile determinare lo stato di sospensione o revoca del certificato per via dello stato **Offline**:



3.2.4 Il sottomenu "Apri"



Questo sottomenu conduce ad alcune funzioni specifiche per aprire/visualizzare documenti di diverso tipo

3.2.4.1 Documento

Presenta una finestra di dialogo standard per la selezione di un file da aprire.
La posizione di partenza per la selezione del file dipende dalle impostazioni dei percorsi di lavoro, configurabili tramite il menu Strumenti -> Opzioni ed agendo sul tab **Percorsi**.

Se si apre un documento già in formato di busta crittografica allora il documento viene aperto così come si trova; se invece si apre un documento "normale" (es. PDF, DOC, TXT, JPG, ecc.) si creerà una nuova busta crittografica contenente tale documento, pronto per le successive operazioni di firma, cifratura, marcatura temporale, ecc.

Si noti che questa funzione ha un comportamento flessibile: applicandola a documenti di tipologia particolare per ***DigitalSign*** (es. Certificati, Liste di Sospensione e revoca, ecc.) essi verranno aperti con gli appropriati moduli di presentazione, non nella finestra documento, esattamente come se venissero usate le funzioni descritte nelle prossime sezioni.

3.2.4.2 Visualizza certificato

Permette di visualizzare il contenuto di un certificato, previa selezione del file, attraverso il modulo standard di visualizzazione.

3.2.4.3 Visualizza Richiesta di Certificato

Permette di visualizzare il contenuto di una Richiesta di Certificato PKCS#10, previa selezione del file, attraverso lo stesso modulo standard di visualizzazione che normalmente si usa per visualizzare il contenuto di un certificato.

3.2.4.4 Visualizza CRL

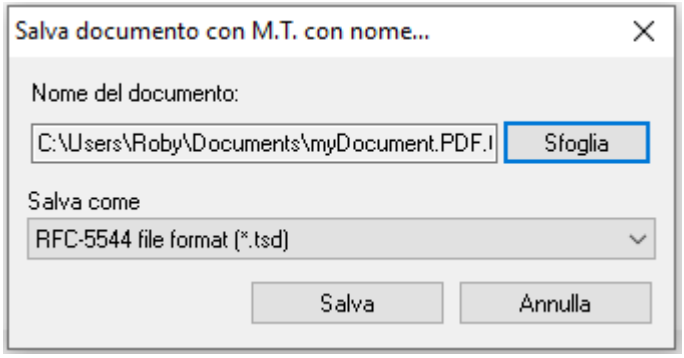
Permette di visualizzare il contenuto di una Lista di Sospensione e Revoca disponibile su un file, attraverso uno specifico modulo di visualizzazione.

3.2.5 Salva Documento

Permette di salvare il documento su cui si sta lavorando.
Poiché ***DigitalSign*** consente una gestione differenziata dei documenti in formato CAdES, PAdES, XAdES il comportamento può essere diverso secondo il tipo di file su cui si sta lavorando:

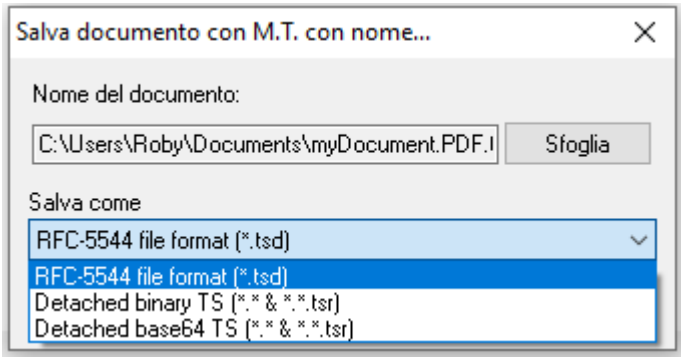
- Se si tratta di un documento DIVERSO dal formato PDF o XML allora si salverà un file in formato **.p7m** (CAdES), anche se non è stata apposta alcuna firma
- Se si tratta di un documento PDF su cui non è stata apposta alcuna firma si salverà ancora in formato **.pdf**
- Se si tratta di un documento PDF su cui è stata apposta una firma PAdES allora si salverà ancora in formato **.pdf**
- Se si si tratta di un documento PDF su cui è stata apposta una firma CAdES allora si salverà un file in formato **.p7m**
- Se si tratta di un documento XML non firmato o corredato di firma XAdES si salverà ancora in formato **.xml**

Se si tratta di un documento corredato di una marca temporale esterna, oppure integrata in formato RFC-5544 allora l'utente ha la possibilità di scegliere il formato di uscita e dunque anche il nome del file.
L'utente vedrà una finestra di dialogo di questo genere:



L'utente può usare il bottone Sfoglia per scegliere la posizione ed il nome del file da creare, quindi completare o annullare l'operazione.

La lista permette di scegliere tra le diverse modalità disponibili:



Per una descrizione delle diverse modalità si veda la sezione relativa.

Se il documento non era ancora stato salvato in precedenza il sistema presenta una finestra di dialogo standard per l'impostazione del nome del file su cui scrivere. La posizione di partenza per la selezione del file dipende dalle impostazioni dei percorsi di lavoro, configurabili tramite il menu Strumenti -> Opzioni ed agendo sul tab **Percorsi.**

Se il file destinazione è già esistente ***DigitalSign*** lo salva direttamente (cioè non chiede il nome), ma nel caso – probabile – che il file sia già esistente chiede conferma della volontà di sovrascriverlo.

3.2.6 Salva Documento con Nome

Funzione assolutamente analoga alla precedente, ma permette di salvare un file di nome differente rispetto all'originale.

3.2.7 Esporta "flattened"

Questa funzione è utilizzabile solo con i documenti firmati in modalità PAdES.
Come noto tali documenti – in genere – presentano una o più firme digitali che hanno anche una parte grafica, visibile sul documento stesso.
Una versione "flattened" di un documento di questo tipo è un altro PDF che conserva la parte grafica, ma è privato della firma, del certificato e di tutti gli attributi che ne costituiscono la "busta crittografica".

Lo scopo, solitamente, è quello di stampare il documento o visualizzarlo mediante applicazioni capaci di gestire un PDF semplice ma non le firme digitali.

3.2.8 Salva Contenuto

Questa funzione consente di salvare una copia del documento contenuto nella busta crittografica su cui si sta operando (non applicabile ai casi di documenti PAdES o XAdES, in cui non esiste una vera e propria busta crittografica da cui estrarre un contenuto).

Se, per esempio, l'utente apre il documento **`proposta_di_contratto.pdf.p7m`**, ossia un documento in formato **pdf** firmato digitalmente e quindi racchiuso in una busta crittografica CAdES, questa funzione permette di salvare una copia del documento **`proposta_di_contratto.pdf`**.

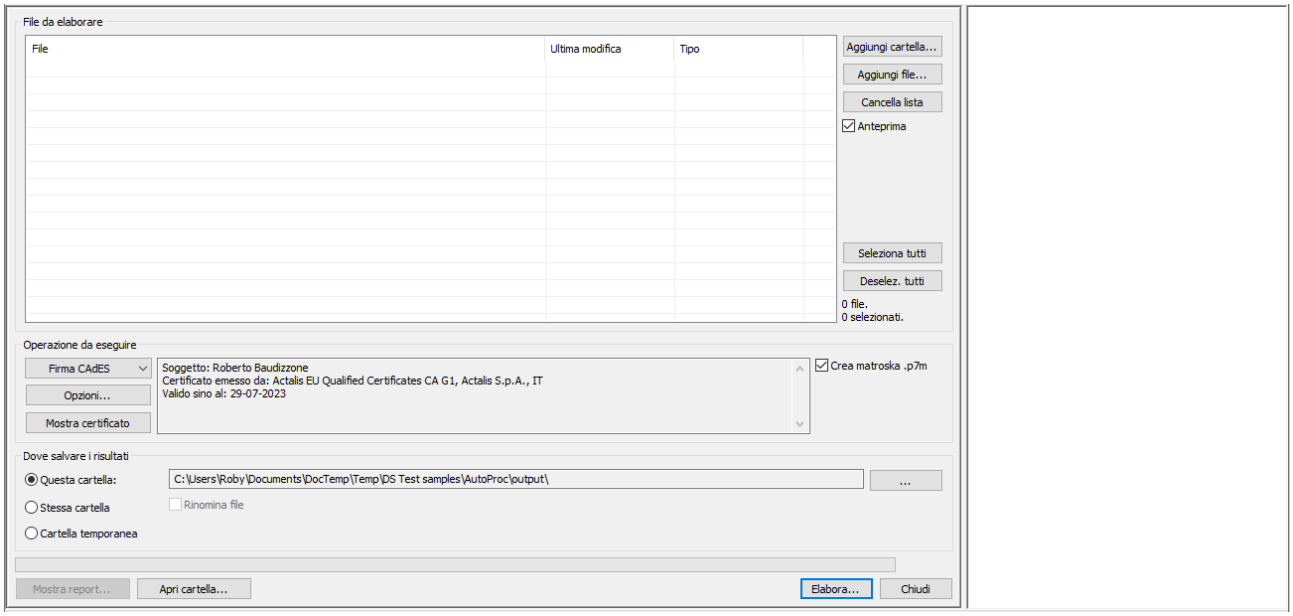
Il sistema presenta una finestra di dialogo standard per l'impostazione del nome del file su cui scrivere. La posizione di partenza per la selezione del file dipende dalle impostazioni dei percorsi di lavoro, configurabili tramite il menu Strumenti -> Opzioni ed agendo sul tab **Percorsi.**

3.2.9 Elaborazione Automatica

Funzione non disponibile con DigitalSign Reader
Questa funzione consente di applicare operazioni di firma, verifica, marcatura temporale, cifratura, decifratura su un intero lotto di documenti.

NOTA: questa funzione può anche essere avviata dalla shell di Windows, si veda l'appendice dedicata.

Inizialmente l'applicazione presenta una schermata di questo tipo:



Il riquadro, inizialmente vuoto, dovrà contenere la lista dei documenti a cui applicare l'operazione automatica prescelta.

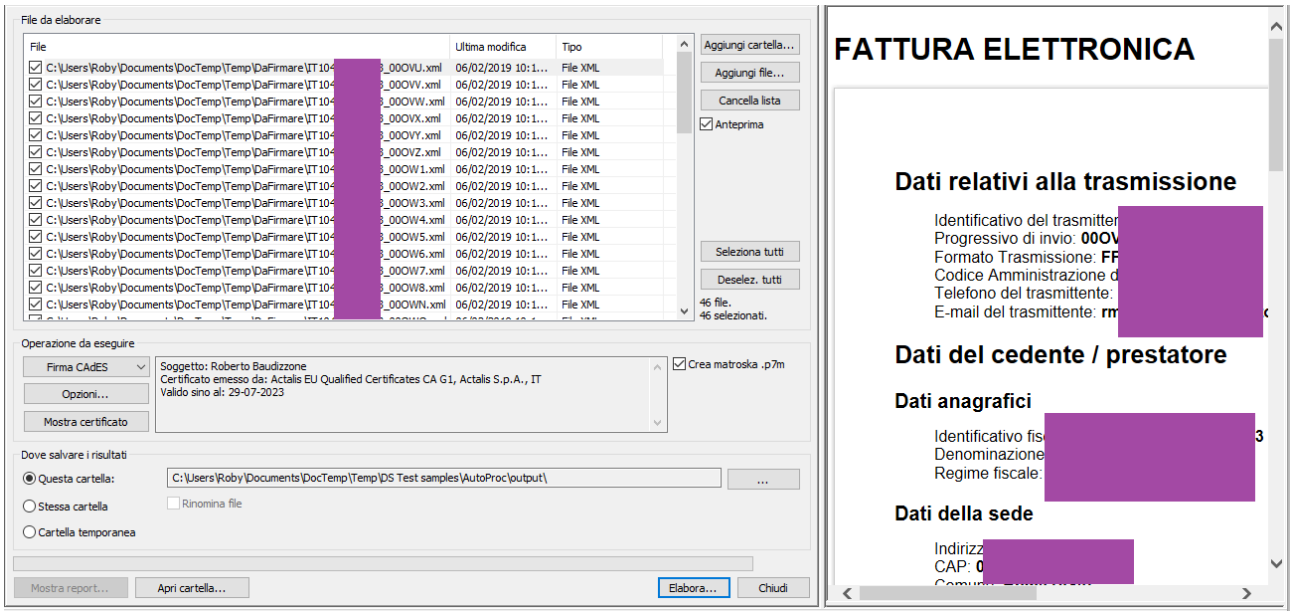
La prima cosa da fare è popolare la lista. Per questo si usano i seguenti comandi:

- **Aggiungi Cartella** – con questo comando possiamo aggiungere alla lista l'intero contenuto di una cartella specificata
- **Aggiungi File** – con questo comando l'utente può selezionare uno o più file da includere nella lista

Si noti che la funzione *drag&drop* di Windows consente di trascinare documenti da una finestra di Windows Explorer e rilasciarli nella lista, ottenendo lo stesso risultato di **Aggiungi File**.

Questi comandi possono essere usati più volte, aggiungendo diversi documenti ad ogni passo.
Il comando **Cancella Lista** permette di svuotare l'intera lista in un click.

Dopo aver popolato la lista vedremo:



Si noti che il riquadro anteprima presenta il contenuto del singolo file su cui eventualmente posizioniamo il cursore, così da permettere l'effettiva visualizzazione di qualunque documento prima di firmarlo.

Si noti anche che tutti i file caricati hanno, a sinistra, una casella di spunta.
Inizialmente sono TUTTI selezionati, ma l'utente può fare click su ciascuna casella per invertire lo stato selezionato/non selezionato: il ciclo di elaborazione automatica agirà SOLTANTO sui documenti SELEZIONATI.

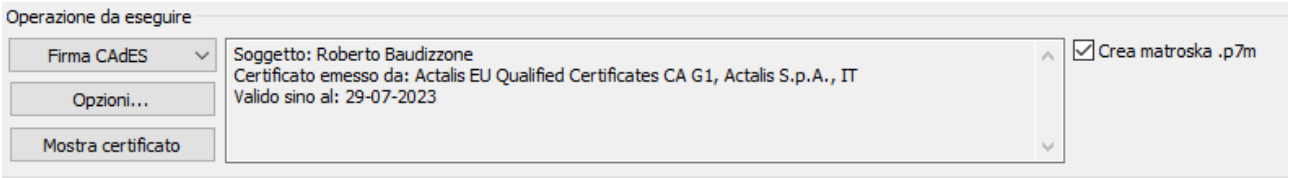
I bottoni comando **Seleziona tutti** e **Deseleziona tutti** permettono di agire in un solo click sullo stato di selezione dell'intera lista.

Dopo aver determinato la lista di documenti su cui vogliamo agire occorre decidere quale operazione eseguire.

In funzione dell'operazione scelta dovremo impostare alcuni parametri specifici:

3.2.9.1 Firma CAdES

Appena scelta questa opzione il sistema chiede il logon al dispositivo di firma e visualizza nel riquadro accanto al bottone comando i dati del certificato che verrà usato per la firma:

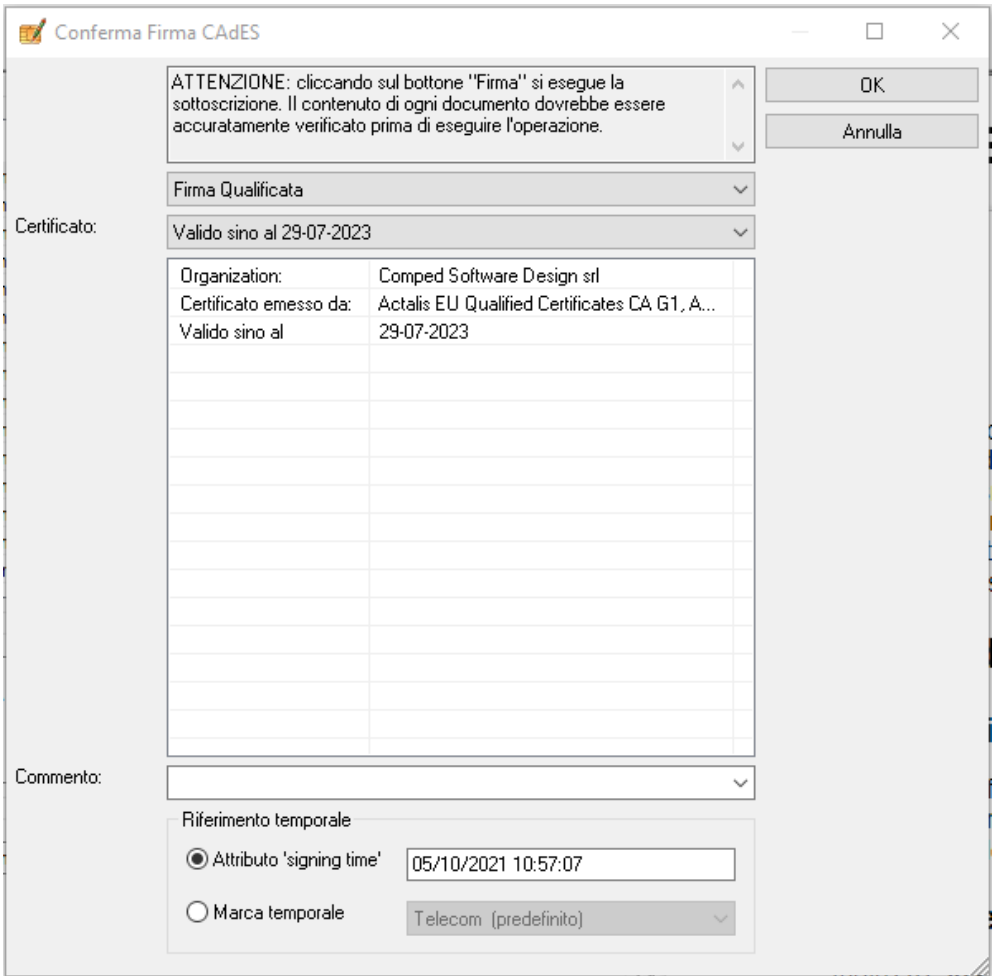


Il bottone Mostra Certificato permette di visualizzare i dettagli del certificato stesso, con la consueta finestra di dialogo.

Si noti che la firma CAdES può applicarsi a qualunque tipo di file; se un file da firmare è già in formato CAdES il sistema appone una ulteriore firma in modo parallelo a quella/quelle eventualmente già presenti, nella stessa busta crittografica.

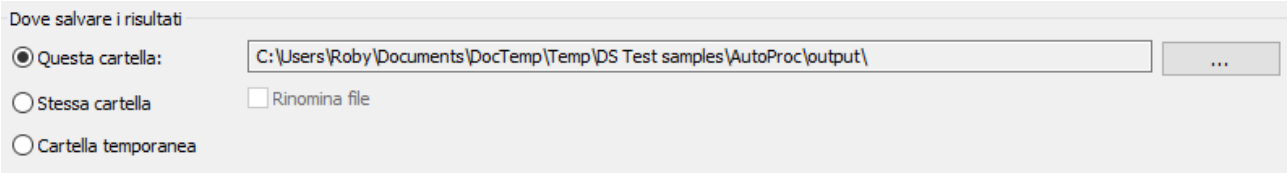
Ma è possibile spuntare il checkbox **Crea matrioska .p7m**: in questo caso se il documento è già un .p7m si creerà comunque una ulteriore busta crittografica esterna con la nuova firma.

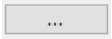
Facendo click su **Opzioni** si aprirà la stessa finestra di dialogo di conferma di una firma CAdES, utilizzata anche nel caso di firma CAdES di un singolo documento:



Qui possiamo scegliere tra le diverse opzioni di firma, se ne esistono più di una, oltre che tra l'uso di un riferimento temporale *"signing time"* (ora proveniente dal computer) o una vera e propria marca temporale.

Quindi dovremo scegliere dove salvare i risultati:

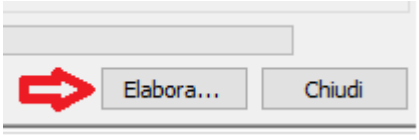


Per default si utilizza una cartella specificamente destinata a contenere il risultato, da impostare mediante il bottone 

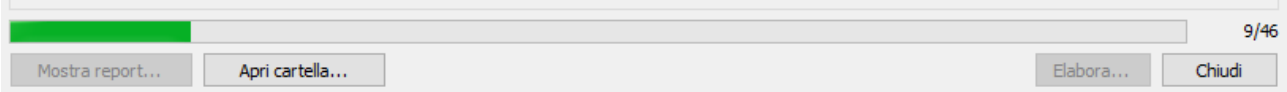
In alternativa si può usare la **stessa cartella** in cui si trova il file origine (eventualmente rinominando il file di destinazione, aggiungendo al nome il suffisso "`-firmato`", oppure usare la **Cartella Temporanea** standard di Windows.

Si noti che, se nella cartella di destinazione esiste già un file con il nome che assumerà il risultato, automaticamente il nuovo file sarà rinominato con il suffisso "-1", "-2", ecc.

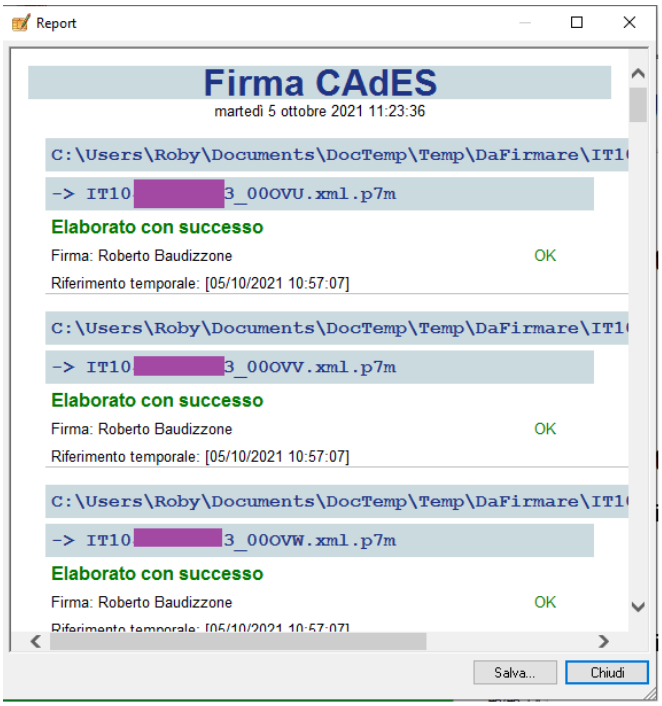
Dopo che tutto è definito si agisce sul bottone **Elabora** per avviare effettivamente il processo:



Durante l'elaborazione l'utente vede una *progress bar* e l'indicazione del numero di documenti via via elaborati:



Al termine dell'elaborazione si apre automaticamente il report dell'esecuzione:



Una volta chiusa questa finestra contenente il report possiamo riaprirla con il bottone **Mostra report**; con **Apri cartella** possiamo invece aprire direttamente la cartella contenente i file prodotti.

NOTA IMPORTANTE: quando si aggiunge una firma (parallela) a un documento singolo ***DigitalSign*** impedisce di farlo se il documento già contiene una firma apposta con il certificato in uso.
Questo controllo non è invece presente nel contesto dell'Elaborazione Automatica.

3.2.9.2 Firma PAdES

L'operazione di Firma PAdES è del tutto simile alla Firma CAdES illustrata nella sezione precedente.
Naturalmente può essere applicata soltanto a documenti PDF, quindi il tentativo di applicarla a documenti d'altro tipo produrrà un errore visibile nel report.

Per il resto cambia l'aspetto della schermata di conferma (**Opzioni**), per i cui dettagli si rimanda alla funzione di Firma PAdES su un singolo documento.

3.2.9.3 Firma XAdES

L'operazione di Firma XAdES è del tutto simile alla Firma CAdES illustrata nella sezione precedente.
Naturalmente può essere applicata soltanto a documenti XML, quindi il tentativo di applicarla a documenti d'altro tipo produrrà un errore visibile nel report.

Per il resto cambia l'aspetto della schermata di conferma (**Opzioni**), per i cui dettagli si rimanda alla funzione di Firma XAdES di un singolo documento.

3.2.9.4 Elevare PAdES-LTV

Questa funzione, applicabile a liste di documenti già firmati PAdES, consente di elevare il loro status a quello di LTV (*Long Term Validation*), mediante l'inclusione nel file delle informazioni necessarie a verificare lo stato di "non revocato" dei certificati e mediante l'aggiunta di una marca temporale.

Il bottone **Opzioni** consente solo di scegliere il servizio di Marcatura Temporale da impiegare per questa operazione.

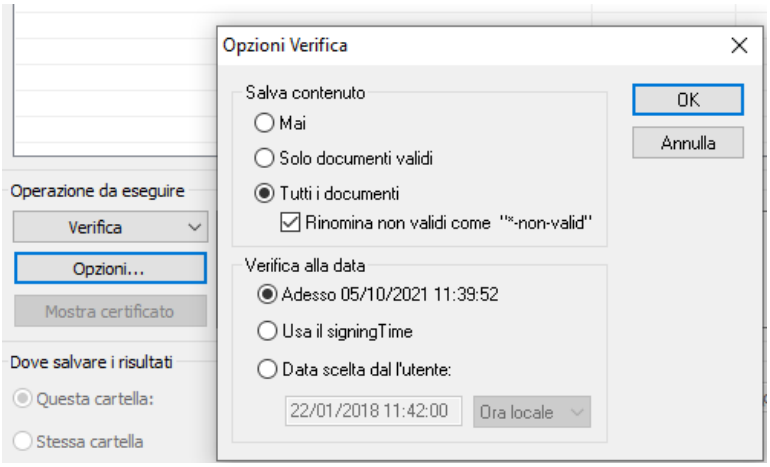
Si veda la sezione dedicata all'elevazione PAdES-LTV di un singolo documento.

3.2.9.5 Verifica

Questa funzione permette di verificare automaticamente le firme di una serie di documenti, ottenendo un report con i risultati della verifica di ciascuno (positiva o negativa):

Si noti che i dettagli ottenuti con questa elaborazione automatica non sono fini come quelli ottenuti aprendo e verificando visivamente un singolo documento, ma certamente con questa tecnica è possibile verificare in un attimo grandi quantità di documenti presenti in una cartella.

Una funzione molto interessante, per il caso di documenti CAdES, è quella del "disimbustamento automatico":



Utilizzando il bottone **Opzioni** si accede alla finestra di dialogo qui visualizzata. I *radio-button* **Salva contenuto** permettono di decidere se operare in effetti il salvataggio del contenuto di un documento CAdES o meno, inoltre se farlo per tutti i documenti o solo per quelli che superano la verifica (eventualmente assegnando un suffisso evocativo a quelli risultati non validi).

Il riquadro sottostante permette di impostare la "verifica alla data", in modo analogo a quanto avviene nel caso di verifica alla data di un singolo documento.

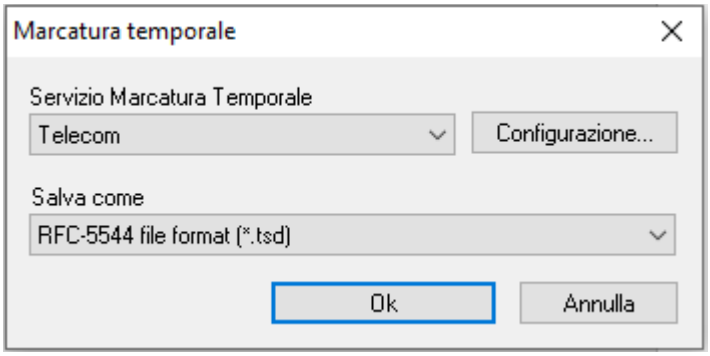
Per il resto anche nella Verifica – proprio per il caso in cui si richieda il salvataggio dei contenuti – è possibile indicare una cartella di destinazione, come nelle operazioni di firma descritte nelle sezioni precedenti.

3.2.9.6 Marcatura Temporale

Questa funziona permette di applicare una marca temporale all'insieme di file selezionato nella lista.

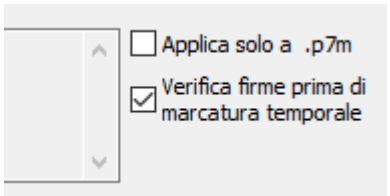
NOTA IMPORTANTE: poiché il servizio di marcatura temporale è una risorsa soggetta a costi, è bene utilizzare usare questa funzione con attenzione. ***DigitalSign*** presenta una schermata di conferma prima di lanciare l'operazione, ricordando il numero totale di documenti selezionati per la marcatura temporale.
L'utente può disabilitare questo ulteriore avvertimento.

Le opzioni prevedono:



- Scelta del **servizio di Marcatura Temporale**, tra quelli correntemente configurati
- Scelta del **formato di output** (per una descrizione delle opzioni disponibili si veda la sezione dedicata alla marcatura temporale di un singolo file.

Si noti la presenza di 2 checkbox per altrettante opzioni:



- **Applica solo a .p7m** – limita l'azione ai soli documenti di tipo .p7m
- **Verifica firme prima di marcatura temporale** – se selezionato evita che una marca temporale sia apposta ad un documento firmato che contenga almeno una firma non valida

3.2.9.7 Controfirma

Questa funzione permette di applicare una Controfirma ad una firma già presente in un documento CAdES.
Si noti che il concetto di controfirma è applicabile solo a documenti CAdES, che contengano già almeno una firma.

L'operatività è analoga a quella della Firma CAdES.

Normalmente, nella modalità interattiva, l'utente naviga nel pannello delle proprietà ed individua la firma già esistente a cui intende apporre una controfirma, ma in questo contesto di elaborazione automatica non è possibile agire così selettivamente.

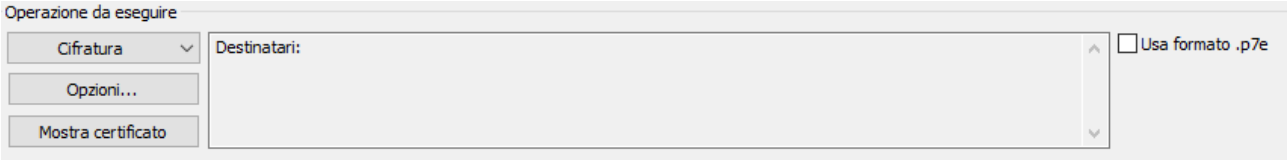
Quindi il sistema applica una regola generale: la controfirma è apposta all'ultima firma (o controfirma) trovata nel documento.
Quindi:

- se il documento contiene una sola firma, la controfirma è apposta a tale firma
- se il documento contiene due o più firme parallele, la controfirma è apposta all'ultima della lista
- se l'ultima (o unica) firma parallela già apposta al documento presenta già uno o più livelli di controfirme, la nuova controfirma è apposta all'ultima controfirma.

NOTA IMPORTANTE: quando si aggiunge una controfirma ad una firma esistente, operando su un documento singolo, ***DigitalSign*** impedisce di farlo se tale firma era stata apposta con lo stesso certificato in uso.
Questo controllo non è invece presente nel contesto dell'Elaborazione Automatica.

3.2.9.8 Cifratura

Questa funzione permette di cifrare il lotto di documenti a beneficio di una lista di "destinatari" abilitati, individuati attraverso i rispettivi certificati di cifratura che devono essere già presenti nel DB dei certificati.



Il bottone Opzioni apre la finestra di dialogo per la selezione dei destinatari della cifratura, del tutto analogo a quello descritto a proposito della cifratura di un singolo documento.

L'opzione **Usa formato .p7e** influisce sul formato di uscita del documento, nel caso i documenti di partenza fossero già firmati in formato CAdES:

- se l'opzione NON è selezionata allora un singolo livello di busta crittografica conterrà sia la firma o le firme e gli elementi di cifratura (certificati dei destinatari, chiavi di sessione cifrate, ecc.); il documento manterrà la sola estensione **.p7m** che aveva in partenza;
- se l'opzione è selezionata allora si genera un'ulteriore busta crittografica più esterna, dedicata ai soli elementi della cifratura; il risultato sarà un documento "a matrioska", con estensione **.p7m.p7e**

3.2.9.9 Decifratura

Funzione "duale" rispetto alla precedente, consente di decifrare i documenti inclusi nella lista, a condizione che siano cifrati con un certificato corrispondente ad una chiave privata disponibile (cioè nella smartcard correntemente inserita o in un file PKCS#12 aggiunto).

Si noti che l'output di questa funzione corrisponde alla funzione **Salva contenuto**: quindi nel caso – ad esempio – di un documento PDF firmato e cifrato nella stessa busta si troverà nella cartella di output il solo PDF.

3.2.10 Stampa

Manda in stampa il documento su cui si sta operando.

Viene presentata una finestra di dialogo standard per il controllo del processo di stampa (scelta del dispositivo, scelta dell'intervallo di pagine, ecc.)

Si noti che la stampa ha per oggetto il documento contenuto: nel caso di busta crittografica CAdES, quindi, non conterrà informazioni sulle firme e sugli altri elementi inclusi nella busta.

Inoltre, si rammenti che la stampa è in generale affidata al sistema operativo, il quale attiva l'applicazione associata al formato del particolare documento.

Si dovrebbe considerare la funzione di stampa di ***DigitalSign*** come una mera funzione ausiliaria, senza aspettarsi particolare qualità o raffinati automatismi.
Per ottenere stampe di qualità è sempre raccomandato:

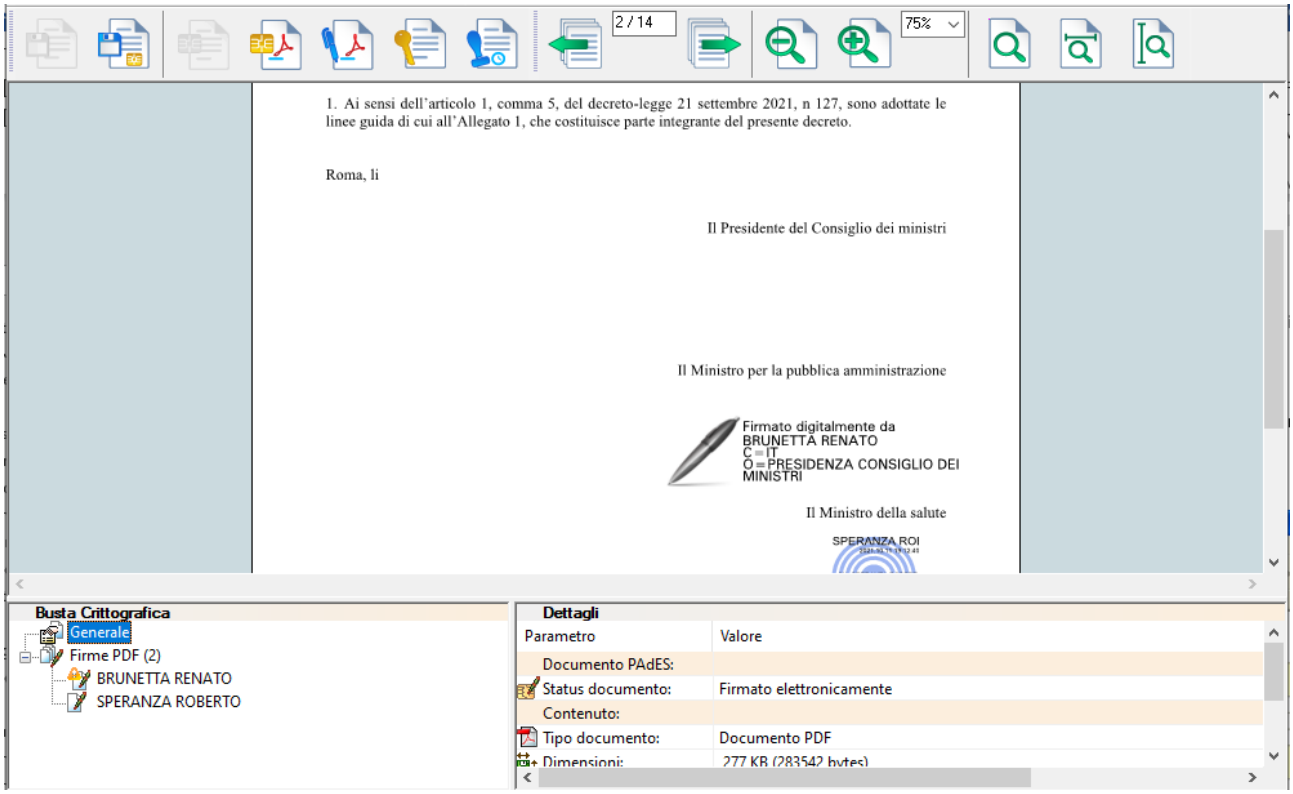
1. Esportare il contenuto del documento (nel caso CAdES) con Salva contenuto
2. Aprire il documento così ottenuto con l'applicazione associata e da lì azionare la stampa

Nel caso di documenti PAdES è sufficiente aprirli dal sistema operativo (che verosimilmente lo affiderà ad Adobe Reader) e da qui lanciare la stampa.

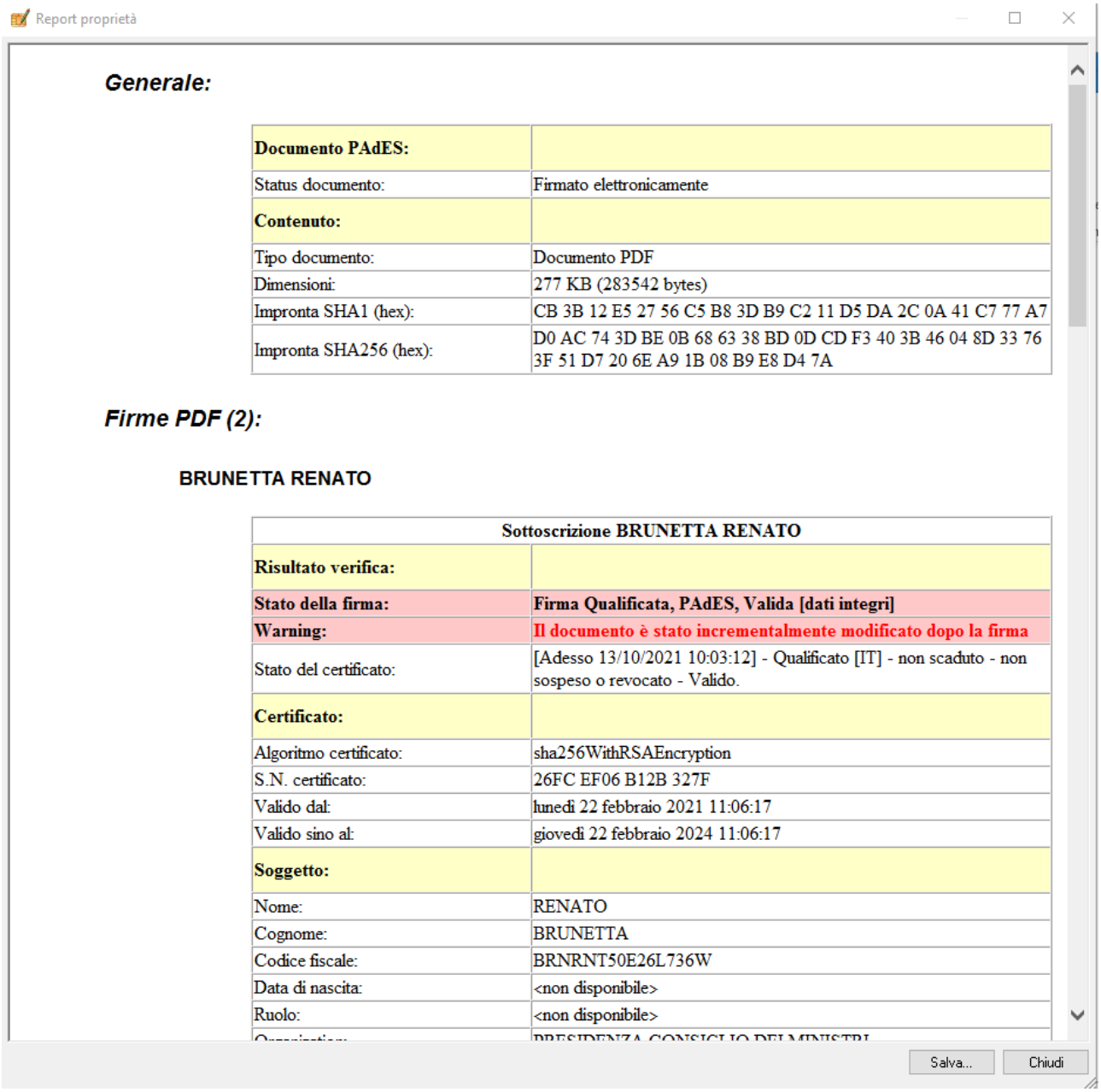
3.2.11 Genera report Documento

Questa funzione consente di generare un rapporto contenente tutti i dettagli tecnici relativi alla busta crittografica del documento correntemente selezionato e al suo contenuto (firme, marche temporali, ecc.).

Supponiamo di avere in corso di esame questo documento:



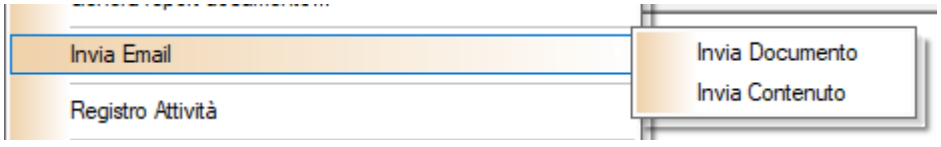
Attivando la funzione **Genera report Documento** vedremo aprire una finestra con i dettagli:



Questo report è costruito in formato HTML e viene successivamente aperto tramite un browser, da cui è possibile salvarlo e poi manipolarlo con un browser o con altre applicazioni.

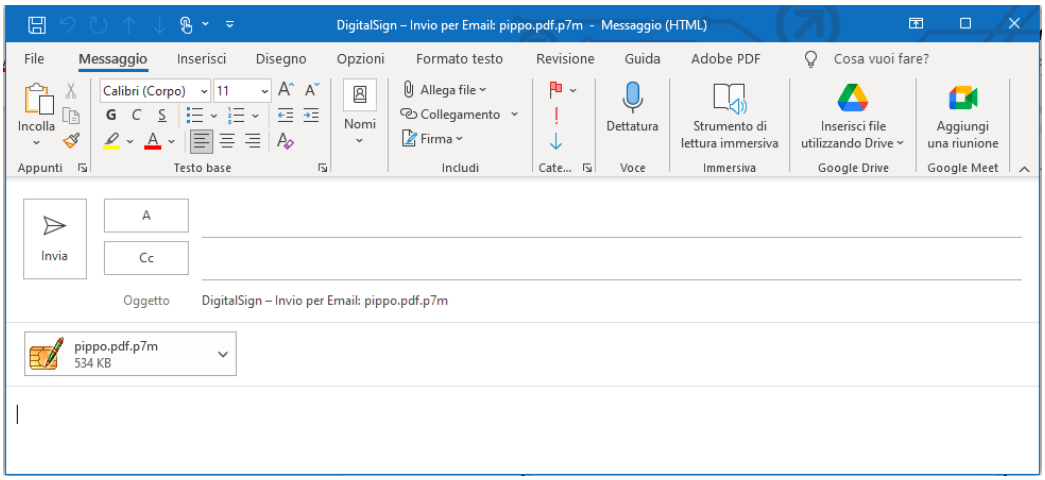
3.2.12 Il sottomenu “Invia Email”

Presenta un sottomenu con due opzioni successive:



L’opzione **Invia Contenuto** è presente solo nel caso il documento correntemente selezionato sia di tipo CAdES: sarà dunque possibile inviare il solo documento contenuto nella busta crittografica, anziché l’intero documento.

È necessario che sul sistema sia impostato un client predefinito di posta elettronica; tramite tale client (es. **MS Outlook ®**) viene creato un nuovo messaggio di posta elettronica contenente l'oggetto selezionato come allegato.



3.2.13 Registro Attività

Funzione non disponibile con DigitalSign Reader

Consente di ispezionare il contenuto del registro delle attività, tramite un componente software separato da ***DigitalSign***.

Per l'abilitazione/disabilitazione della funzione di registrazione degli eventi e per la configurazione sulle categorie di eventi da includere nella registrazione si usa relativa configurazione si usa il menu Strumenti -> Opzioni agendo quindi sul tab **Registro Attività**

Per i dettagli di questa funzione si veda la sezione dedicata.

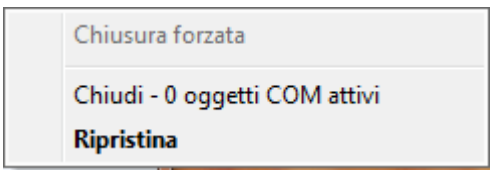
3.2.14 Uscita

Questa funzione provoca la chiusura dell'applicazione.

Si noti che la normale azione su questo comando (o sul simbolo ✕ di chiusura della finestra principale dell'applicazione) ***DigitalSign*** non viene del tutto scaricato dalla memoria e resta quindi pronto per una rapida riattivazione. Questo stato è testimoniato dalla presenza dell'icona di DigitalSign nella *system tray*:

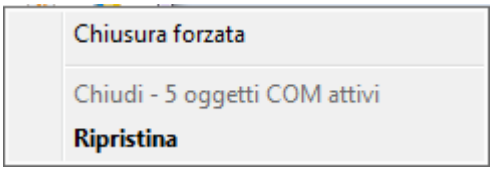
Lo scaricamento dalla memoria avviene spontaneamente dopo qualche minuto di completa inattività di ***DigitalSign*** (considerando anche il fatto che altre applicazioni potrebbero utilizzarne i servizi), oppure:

- tenendo premuto il tasto SHIFT quando si attiva questo comando di uscita (o si clicca sul bottone ✕ di chiusura della finestra);
- facendo click con il tasto destro sull'icona di ***DigitalSign*** presente nella *system tray* dopo la chiusura normale dell'applicazione ed operando sul pop-up menu che appare:



Come si può notare, l'opzione **Chiusura forzata** è disabilitata, perché non necessaria. Da qui si può usare l'opzione **Chiudi – 0 oggetti COM attivi**, perché non esistono altri processi che necessitano di ***DigitalSign*** in funzione.

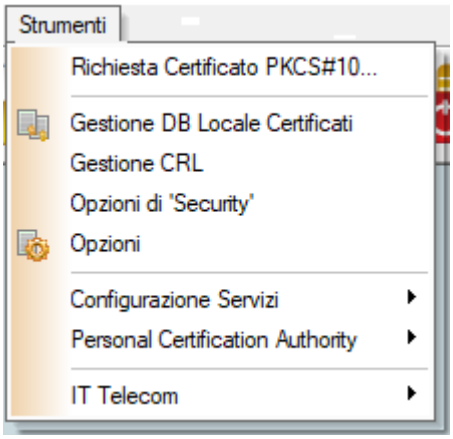
Se invece qualche applicazione stesse usando ***DigitalSign*** lo stesso menu si presenterebbe in questa forma:



Stavolta è l'opzione **Chiudi** ad essere disabilitata (pur mostrando il numero di oggetti COM aperti da altre applicazioni).
La chiusura sarebbe dunque possibile solo con la **Chiusura forzata**, tenendo presente che questo potrebbe avere effetti negativi sulle altre applicazioni aperte.

In entrambi i casi, **Ripristina** riattiva la finestra principale di ***DigitalSign***.

3.3 Il menu "Strumenti"



Questo menu raccoglie diverse funzioni di servizio ed utili alla configurazione del sistema.

Alcune voci conducono ad ulteriori sottomenu.

3.3.1 Richiesta di certificato PKCS#10

Questa funzione non è disponibile in DigitalSign Reader
Inoltre, può essere disabilitata in alcune edizioni Professional OEM distribuite da alcune importanti organizzazioni.

Questa funzione viene di regola utilizzata nei contesti di utilizzo sperimentale o comunque in un gruppo chiuso di utenti, quando non si intendono utilizzare certificati forniti da un Certificatore Accreditato.
In tali casi si istituisce una funzione di *Certification Authority* che emette certificati per gli altri utenti; questi ultimi devono dal canto loro provvedere alla generazione delle coppie di chiavi sui propri dispositivi e quindi produrre, appunto, le relative "Richieste di Certificato" attraverso questa funzione.

Per le modalità d'uso della ***Personal Certification Authority*** e di questa specifica funzione si faccia riferimento alla Guida specifica, da richiedere a CompEd.

3.3.2 Gestione DB Locale dei Certificati

Questa voce di menu consente di accedere al modulo di gestione del DB dei Certificati. A tale modulo è dedicata una specifica sezione di questo manuale, cui si rimanda: si veda la sezione dedicata.

3.3.3 Gestione CRL

Questa voce di menu consente di accedere al modulo di gestione delle Liste di Sospensione e Revoca (CRL). A tale modulo è dedicata una specifica sezione di questo manuale, cui si rimanda: si veda la sezione dedicata.

3.3.4 Opzioni di Security

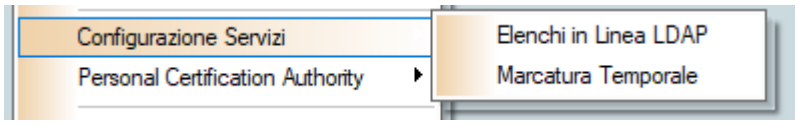
Questa voce di menu consente di accedere al modulo di gestione delle Opzioni di Sicurezza, prevalentemente dedicato alle impostazioni per la verifica di firme e certificati. A tale modulo è dedicata una specifica sezione di questo manuale, cui si rimanda: si veda la sezione dedicata.

3.3.5 Opzioni

Questa voce di menu consente di accedere al modulo di gestione delle Opzioni, attraverso il quale si impostano gran parte dei parametri di configurazione di ***DigitalSign***. A tale modulo è dedicata una specifica sezione di questo manuale, cui si rimanda: si veda la sezione dedicata.

3.3.6 Il sottomenu "Configurazione Servizi"

Questa voce conduce ad ulteriore sottomenu:



- Il primo elemento di questo sottomenu apre il modulo di configurazione degli elenchi di certificati in linea LDAP, si veda la sezione dedicata.

- Il secondo elemento conduce alla configurazione dei servizi di marcatura temporale, si veda la sezione dedicata.
  Funzione non disponibile in DigitalSign Reader

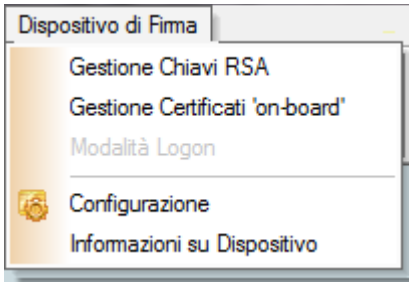
3.3.7 Personal Certification Authority

Questa funzione – insieme a tutte le funzioni del relativo sottomenu - non è disponibile in DigitalSign Reader. Inoltre può essere disabilitata in alcune edizioni Professional OEM distribuite da alcune importanti organizzazioni.

NOTA: CompEd ha realizzato una specifica guida, separata da questo manuale utente, per assistere l'utente nell'utilizzo della ***Personal Certification Authority***. È possibile richiederle tale guida direttamente a CompEd.

3.4 Il menu "Dispositivo di Firma"

Questo menu non è disponibile con DigitalSign Reader.
Ogni specifica funzione è in ogni caso abilitata solo se è inserito un dispositivo di firma compatibile con la funzione stessa.



Questo menu raccoglie alcune funzioni di gestione dell'interfacciamento con i dispositivi di firma (smartcard, token USB, ecc.) e dei relativi contenuti.

3.4.1 Gestione Chiavi RSA

Un dispositivo di firma contiene, tra gli altri oggetti, coppie di chiavi RSA.
Questa funzione permette di esaminare le chiavi attualmente contenute nel dispositivo, ed eventualmente di intervenire con operazioni di creazione, eliminazione, importazione, esportazione.

I dettagli operativi sono descritti in una sezione dedicata.

3.4.2 Gestione Certificati 'on-board'

Un dispositivo di firma contiene, tra gli altri oggetti, uno o più certificati.
Questa funzione permette di accedere al Modulo di Gestione di questi certificati, offrendo in generale opzioni per la visualizzazione e l'esportazione di questi certificati.
Se il particolare dispositivo lo permette è anche possibile caricare certificati nella memoria del dispositivo.

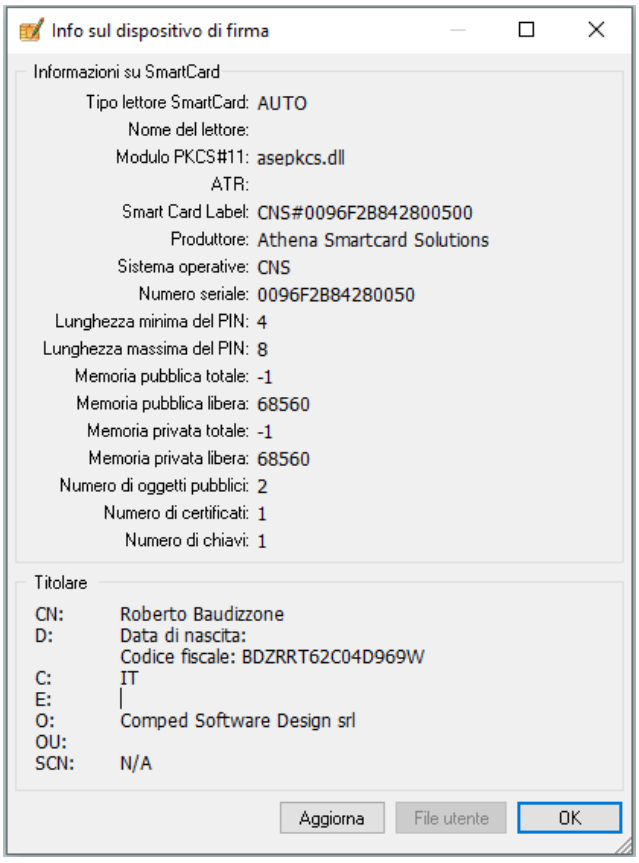
I certificati *on-board* sono particolarmente importanti perché possono essere considerati intrinsecamente attendibili in fase di verifica di firme e certificati (si veda la sezione dedicata alla configurazione delle CA accreditate e attendibili).

3.4.3 Configurazione

Questa importante funzione serve a controllare la modalità di interfacciamento tra ***DigitalSign*** ed il dispositivo di firma.
Per i dettagli si veda la sezione dedicata.

3.4.4 Informazioni sul Dispositivo

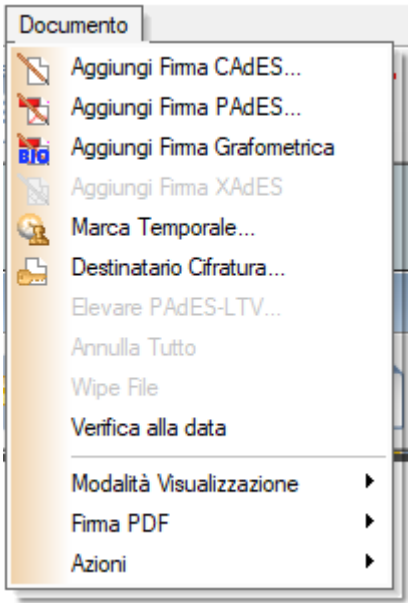
Presenta una schermata di informazioni sul dispositivo di firma correntemente inserito.



- il bottone **Aggiorna** permette di rileggere i dati dal dispositivo ed aggiornare la visualizzazione
- il bottone **OK** chiude la finestra

3.5 Il menu "Documento"

Questo menu può avere elementi diversi secondo il tipo di documento su cui si sta operando; la figura che segue mostra il caso più completo:



Questo menu è visibile solo quando almeno è presente almeno una finestra documento e di norma contiene uno o più sottomenu.

3.5.1 Aggiungi Firma CAdES

Funzione non disponibile con DigitalSign Reader

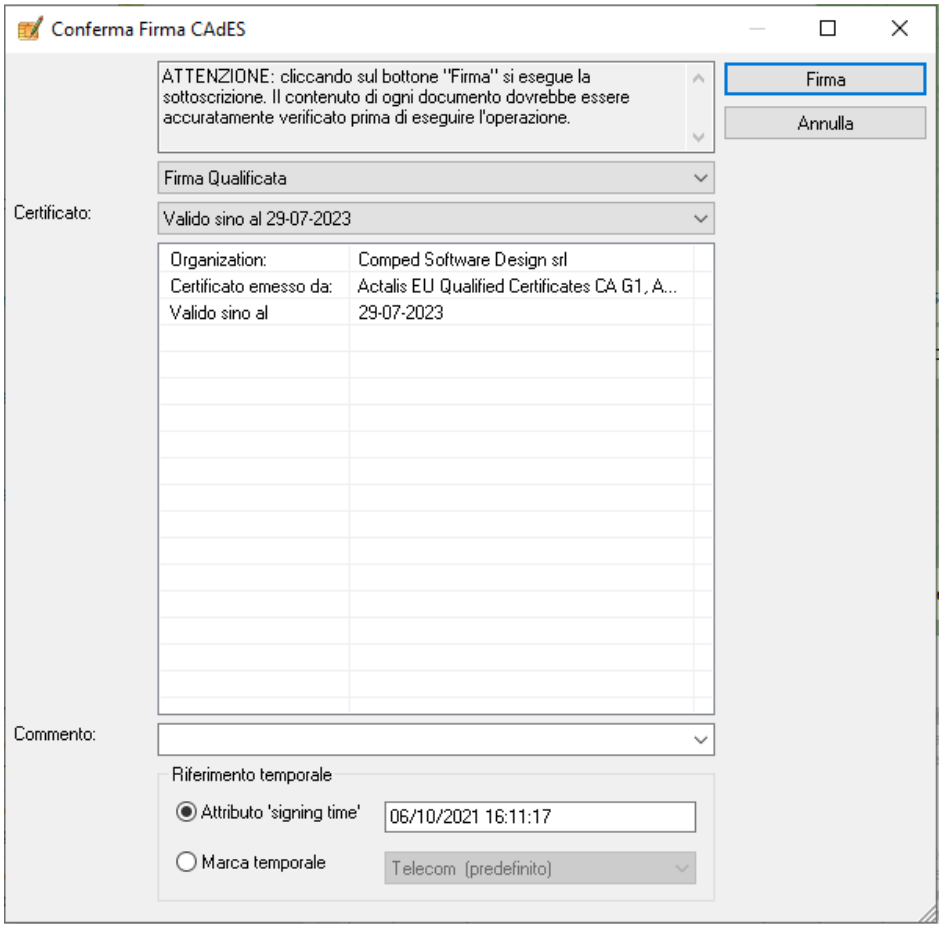
Consente di firmare digitalmente il documento aperto correntemente selezionato, se è disponibile un dispositivo di firma idoneo e se il documento non contiene ancora una firma CAdES generata con lo certificato che si sta usando correntemente.

ATTENZIONE: se il documento aperto è di tipo PDF "semplice", ancora non firmato (prima di scegliere un tipo di firma), usando questa funzione si produce un file in formato CAdES. Se l'intenzione è invece di produrre un PDF firmato (PAdES), senza imbustarlo in una busta crittografica CAdES, allora occorre usare la funzione Aggiungi firma PDF.
Stessa cosa se il documento è in formato XML e si desidera firmarlo in modalità XAdES: si userà Aggiungi Firma XAdES.

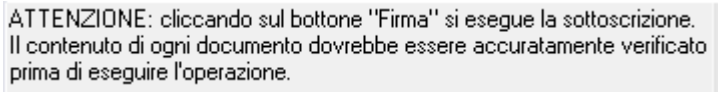
Questa funzione non è disponibile se il documento aperto è di tipo PDF e già contiene una o più firma in formato PAdES, oppure se il documento è di tipo XML e già contiene una firma XAdES

Se il documento già contiene una firma CAdES di un diverso soggetto, con questa funzione si aggiunge una ulteriore firma di tipo "parallelo".

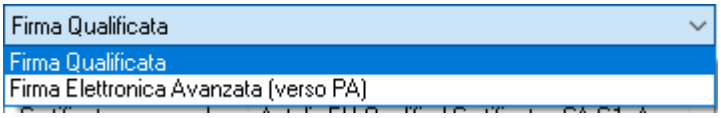
Se il dispositivo non è ancora in stato di *Logon* il sistema presenta innanzitutto la finestra di dialogo relativa, quindi quella specifica per la conferma della firma:



- In alto è riportato un testo informativo che invita l'utente a verificare accuratamente il contenuto del documento:



- Subito sotto compare un selettore per la fattispecie di firma da apporre:



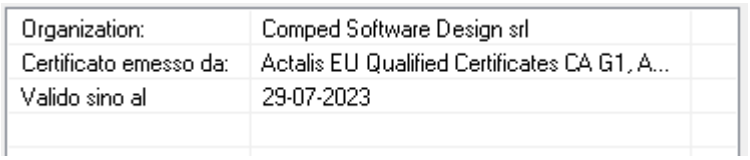
La lista può contenere una o più opzioni secondo quali certificati sono disponibili per il dispositivo di firma correntemente inserito/montato.

Di solito si userà il certificato qualificato e si produrrà una Firma Qualificata, la fattispecie a massimo valore probatorio.
Tuttavia, la normativa più recente chiarisce che utilizzando il certificato di autenticazione contenuto nelle CNS (talvolta non ci sono altri certificati, come nelle "carte cittadino" rilasciate da alcune regioni) la firma prodotta ha valore di Firma Elettronica Avanzata se usata nei confronti della Pubblica Amministrazioni.

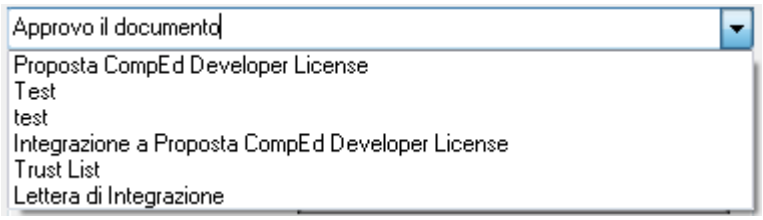
- In base alla fattispecie di firma selezionata al punto precedente appare l'indicazione del certificato correntemente selezionato:

Se la carta contenesse più di un certificato atto allo scopo la lista sarebbe selezionabile per individuare il certificato prescelto. Altrimenti (come nel caso in figura) la lista è bloccata sull'unico certificato.

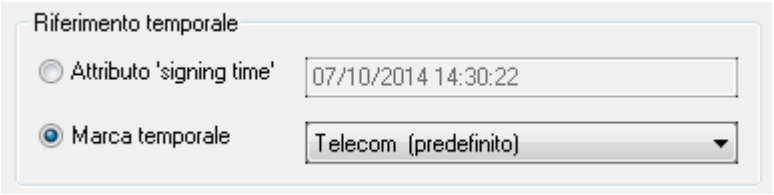
- Segue un riquadro che riassume i dati del certificato correntemente selezionato:



- Il campo Commento: qui l'utente può scrivere un commento alla firma, con la possibilità – grazie alla lista – di richiamare i commenti inseriti in precedenza



- Infine, si sceglie il tipo di riferimento temporale.



Le opzioni sono:

- **Attributo Signing Time –** scegliendo questa opzione si associa alla firma un attributo (*signed*, ossia coperto a sua volta dalla firma) che rappresenta la dichiarazione della data ed ora a cui viene apposta la firma. ***DigitalSign*** compila questo campo con l'ora di sistema, ma l'utente è tecnicamente libero di modificarlo (si tratta di una diretta responsabilità del sottoscrittore).
- **Marca Temporale –** scegliendo questa opzione ***DigitalSign*** genera la firma, dopo di che richiede – al servizio prescelto – una marca temporale calcolata sulla firma stessa.

Con il bottone 

si conferma l'operazione

Con il bottone 

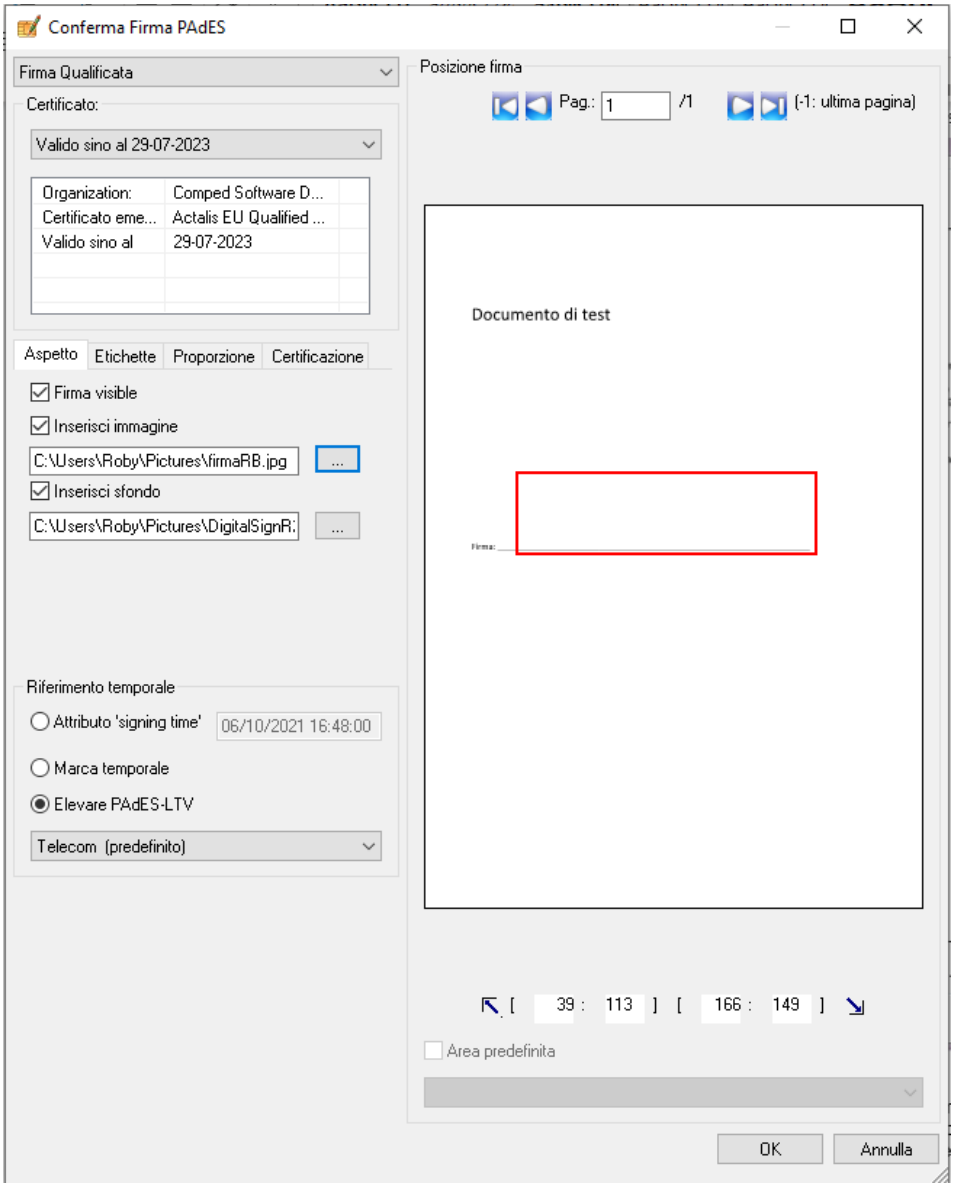
si chiude senza generare la firma

3.5.2 Aggiungi Firma PAdES

Funzione non disponibile con DigitalSign Reader

Se il documento aperto è di tipo PDF e non è già firmato in modalità CAdES, questa funzione consente di apporre una firma digitale all'interno dello stesso file PDF.

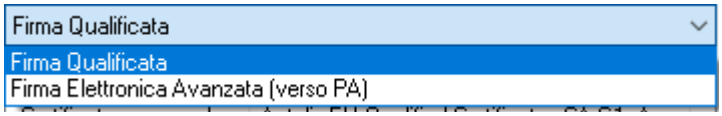
Se il dispositivo non è ancora in stato di *Logon* il sistema presenta innanzitutto la finestra di dialogo relativa, quindi quella specifica per la conferma della firma:



Il processo di apposizione di una firma PAdES è un po' più laboriosa rispetto a quella CAdES, perché una peculiarità di questo formato è proprio quella di consentire l'inserimento di un elemento grafico e di una lista di elementi testuali (ricavati dal certificato) all'interno del documento stesso.
Peraltro molti controlli agiscono come nel caso precedente, quindi rimanderemo direttamente alla sezione firma CAdES per una spiegazione dettagliata.

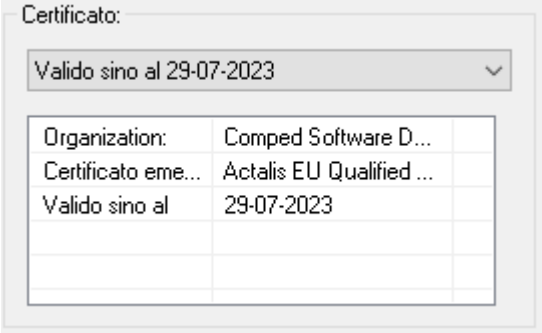
Vediamo gli elementi di questa finestra di dialogo:

- **Selettore della fattispecie di firma**



  Si veda il caso CAdES

- **Riquadro selezione e visualizzazione certificato**

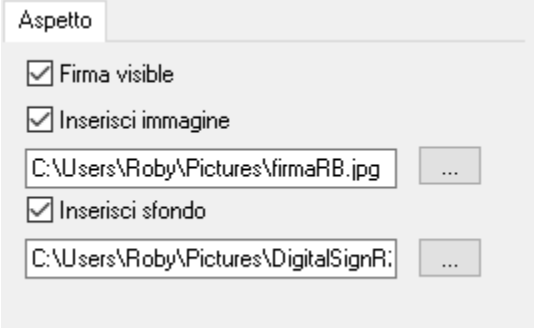


Si veda il caso CAdES

- **Riquadro 'Aspetto e caratteristiche della firma'**

  Questo riquadro presenta 4 diversi "tab" per agire su altrettante sezioni:

  i. Aspetto



  Questo riquadro controlla alcuni aspetti visuali della firma, propri della modalità PAdES:

  - Firma visibile – deselezionando questa casella la firma non avrà una parte visibile nel documento, sarà ispezionabile solo a livello di attributi del documento
  - Inserisci immagine – l'utente può indicare un file di tipo immagine da impiegare per il rettangolo della firma; di solito si usa una scansione della propria firma autografa.
    Per esempio, la firma potrebbe apparire così:

  - Inserisci sfondo – selezionando questa casella ed indicando un ulteriore file immagine si può aggiungere ad esempio un rettangolo colorato oppure una sorta di timbro.
    Ad esempio:


Gentile utente,

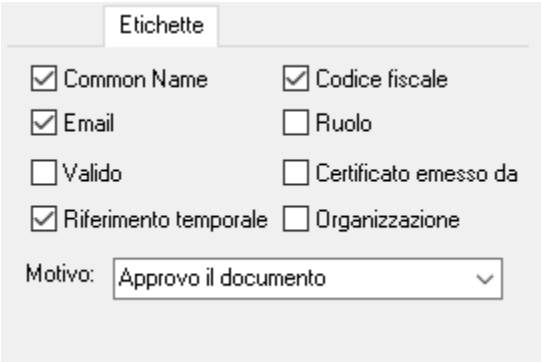
questo file è stato firmato digitalmente con DigitalSign, il software più completo e sicuro per la firma digitale a norma di legge.

Grazie per aver scelto CompEd e DigitalSign.

Cordiali saluti,

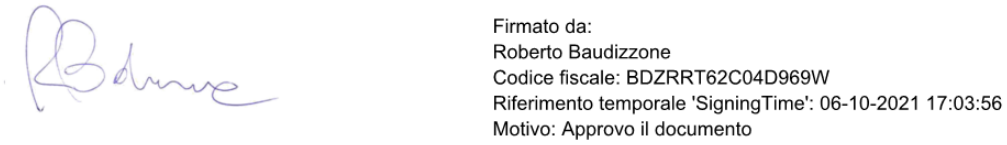
CompEd PROGETTI

ii. Etichette

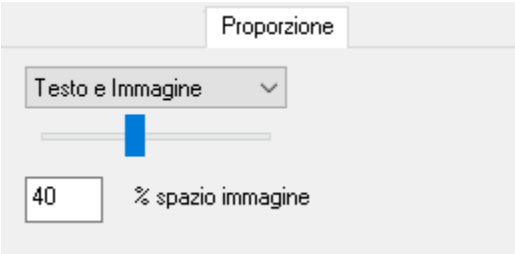


Oltre al campo "Motivo", in cui l'utente può scrivere una motivazione della firma, eventualmente selezionando tra le ultime motivazioni inserite in passato, compaiono alcune caselle selezionabili.
Ogni casella, se selezionata, provoca l'inserimento – accanto alla parte grafica della firma – di una corrispondente etichetta automaticamente impostata con i dati ricavati dal certificato.

Ad esempio, con l'impostazione esemplificata qui sopra si ottiene un risultato di questo tipo:

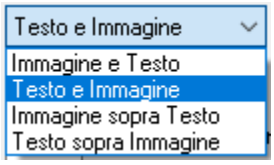

Firmato da:
Roberto Baudizzone
Codice fiscale: BDZRRT62C04D969W
Riferimento temporale 'SigningTime': 06-10-2021 17:03:56
Motivo: Approvo il documento

iii. Proporzione



Questo pannello consente di definire le posizioni dei due rettangoli dedicati alla parte immagine e alla parte etichette del rettangolo contenente la firma.

Il selettore consente di scegliere tra 4 opzioni:



- **Immagine e Testo** divide il rettangolo in due aree verticali, l'immagine a sinistra e le etichette a destra
- **Testo e Immagine** divide il rettangolo in due aree verticali, le etichette a sinistra e l'immagine a destra
- **Immagine sopra Testo** divide il rettangolo in due aree orizzontali, l'immagine in alto e le etichette in basso
- **Testo sopra Immagine** divide il rettangolo in due aree orizzontali, le etichette in alto e l'immagine in basso

Il cursore consente di definire la percentuale di spazio (orizzontale o verticale, secondo il layout impostato con il selettore) da assegnare alla parte immagine.

Sia l'immagine che il font delle etichette saranno automaticamente dimensionate in modo da poter essere sistemate nell'area definita.

iv. Certificazione

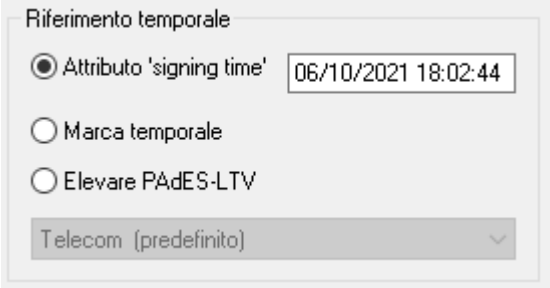
Lo standard PAdES consente di impostare una firma con un attributo che la caratterizza come una sottoscrizione vera e propria, oppure come una forma di CERTIFICAZIONE che, nell'ambito delle applicazioni Adobe, consente di effettuare al documento certe ulteriori operazioni e non altre.

Per default una firma sarà appunto una **Firma**, una sottoscrizione vera e propria.

Tramite questo pannello è possibile impostare la firma come una **Certificazione**, secondo le opzioni visibili in figura.

- **Scelta del Riferimento Temporale**

Questo riquadro presenta tre opzioni:

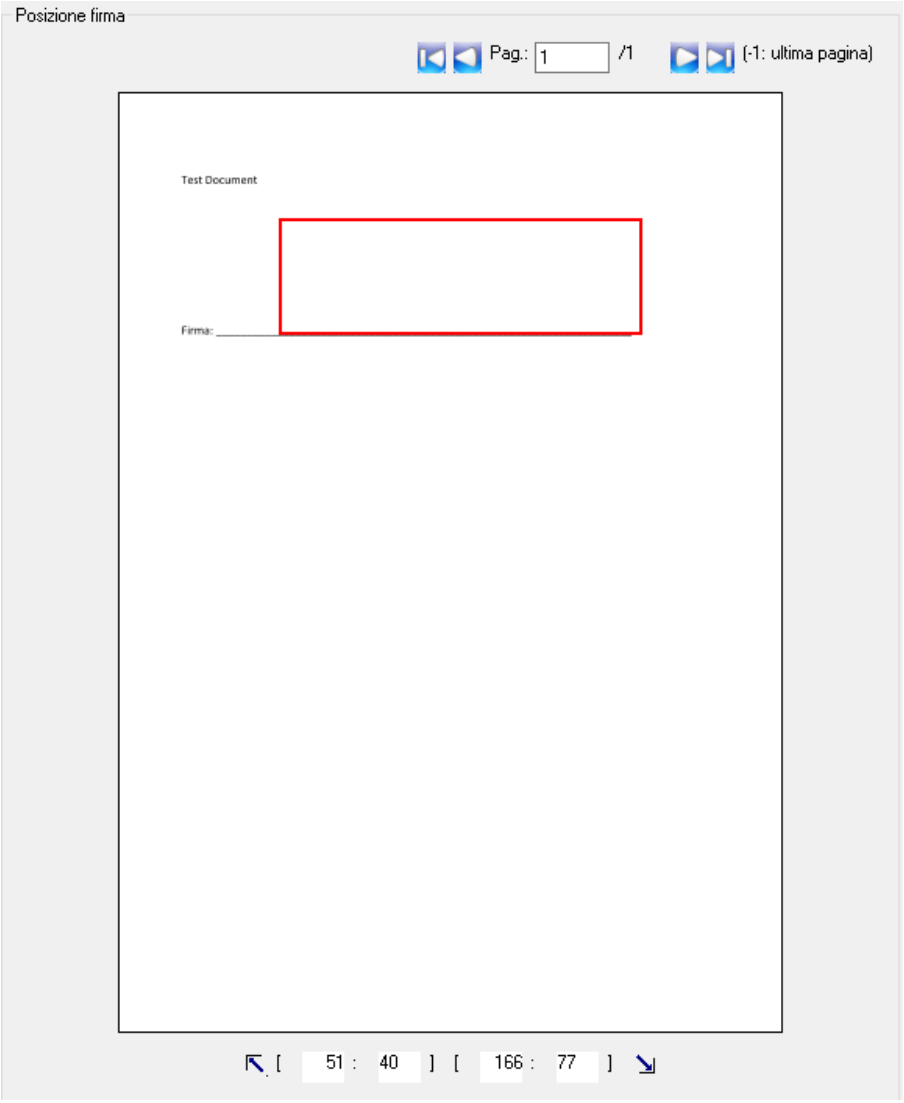


Le prime due operano esattamente come nel caso CAdES, cui si rimanda.

Per il formato PAdES esiste l'opzione **Elevare PAdES-LTV**, che consente di applicare direttamente una firma digitale e inserire nel documento tutti gli elementi che lo rendono idoneo alla *Long Term Validation*: l'intera catena di certificazione del certificato dell'utente (di norma il certificato della CA), le informazioni dello stato di non sospeso e revocato (copia della CRL attuale o della *response* OCSP) e una marca temporale a sigillare il tutto.

Questa operazione equivale ad apporre una semplice firma digitale e successivamente applicare la funzione Elevare PAdES-LTV, si veda la sezione relativa.

- **Posizionamento della firma**

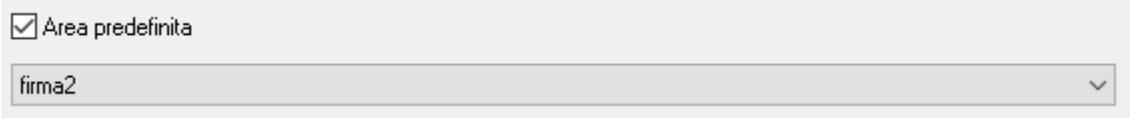


In questo riquadro l'utente definisce la posizione della firma nella pagina.
Puntando il mouse e poi spostandolo mantenendo premuto il tasto sinistro si disegna un rettangolo dal contorno rosso: tale rettangolo è l'area coperta dalla firma, intendendo sia la parte grafica che la parte etichette, secondo le proporzioni impostate.
I controlli in alto permettono di scegliere la pagina su cui posizionare la firma. Opzionalmente è possibile digitare direttamente il numero di pagina, mentre digitando il valore **-1** si indica al sistema che la firma sarà posizionata nell'ultima pagina.
I 4 campi editabili alla base del riquadro rappresentano le coordinate dell'angolo superiore sinistro e di quello inferiore destro, rispettivamente: questi valori sono automaticamente aggiornati mentre si manovra il rettangolo con il mouse, ma è possibile editare direttamente i valori e vedere il rettangolo regolarsi di conseguenza.

- **Campi firma predefiniti**

Alcuni strumenti, come Adobe Acrobat, consentono di predisporre documenti PDF con dei campi "firma" già completamente definiti, lasciando all'utente di applicazioni come Adobe Reader solo la possibilità di apporre la firma in tali posizioni.

Anche DigitalSign, quantunque non obblighi l'utente a restare in tali limiti, può essere istruito a firmare in tal modo:



Se il documento aperto contiene uno o più campi firma si abilitano i controlli mostrati in figura.
Spuntando la casella **Area predefinita** la firma verrà posizionata nel rettangolo predefinito.

Qualora il documento contenga più di un campo firma sarà possibile scegliere, con il selettore sottostante, in quale campo inserire la firma.

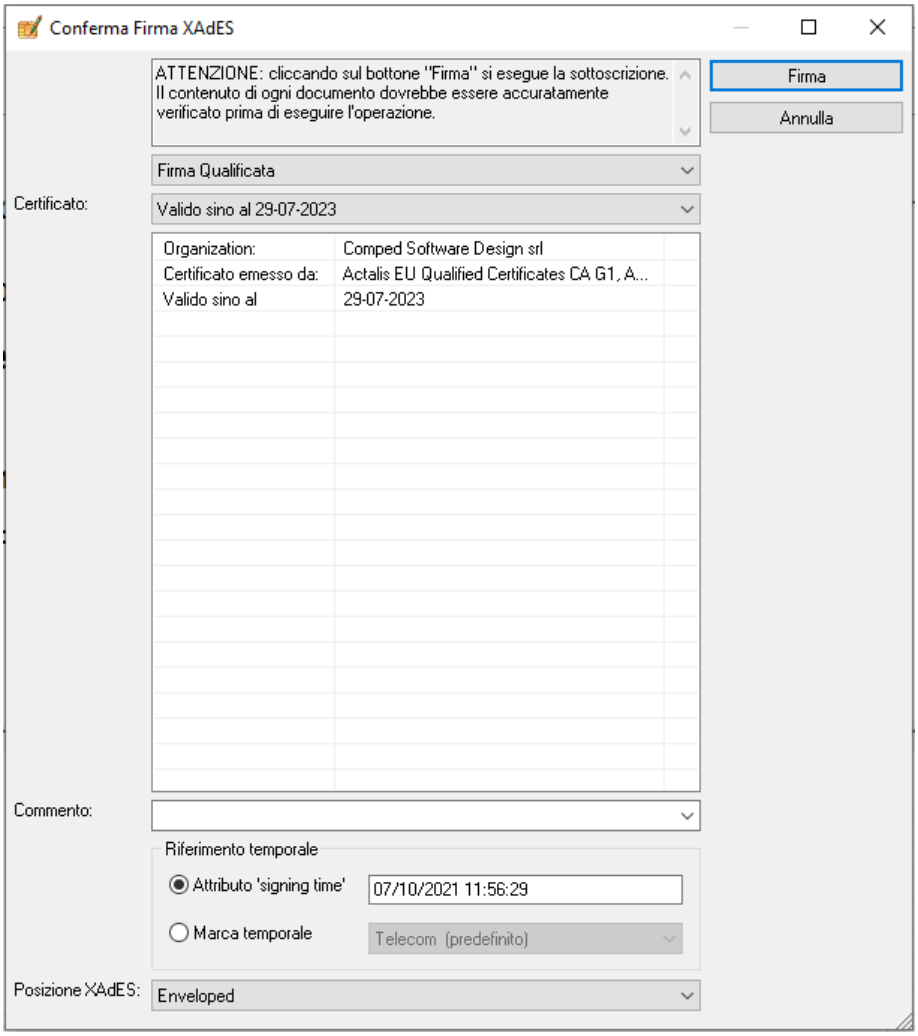
Con il bottone 

si conferma l'operazione
Con il bottone 

si chiude senza generare la firma

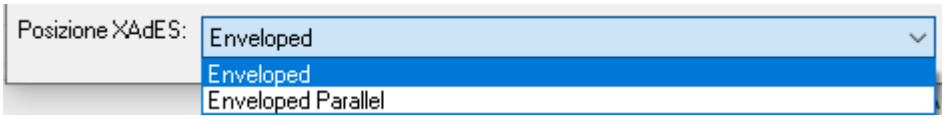
3.5.3 Aggiungi firma XAdES

Consente di apporre una firma XAdES a un documento XML.



La finestra di dialogo di conferma della firma è quasi identica a quella presentata per la firma CAdES, a cui si rimanda.

Si noti, in fondo al pannello, un selettore della posizione XAdES:



Premesso che ***DigitalSign*** può generare solo firme XAdES in modalità *"Enveloped"* (e non in modalità *"Enveloping"*), è possibile scegliere la modalità *"Enveloped Parallel"* se espressamente richiesto dal destinatario del documento. Normalmente si sceglierà il default *"Enveloped"*.

3.5.4 Aggiungi Firma Grafometrica

Funzione non disponibile con DigitalSign Reader

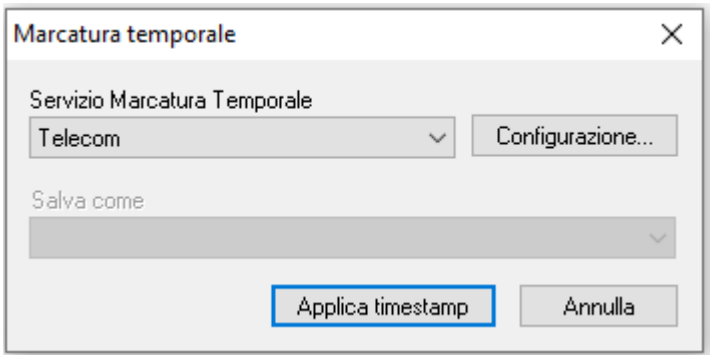
NOTA: questa funzione è abilitata solo se è installato il modulo opzionale ***BioSign Windows Client***.

3.5.5 Marca Temporale

Funzione non disponibile con DigitalSign Reader

Permette di associare una marca temporale ad un documento.

Si noti che la marca temporale è associata all'intero documento, che può essere firmato o meno. É una procedura simile, ma non del tutto identica all'apposizione di una marca temporale ad una singola firma, a titolo di "riferimento temporale".



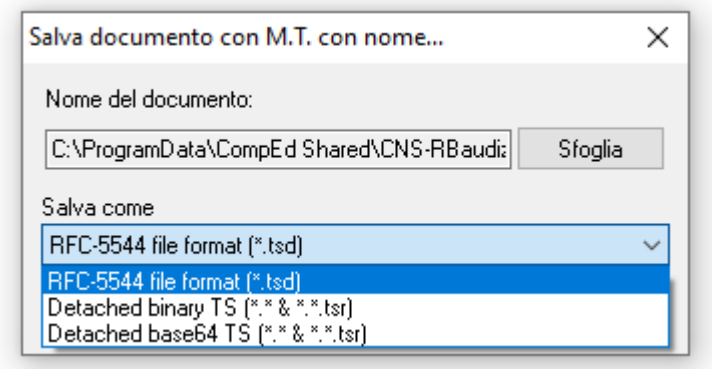
Il sistema presenta questa finestra di dialogo, per chiedere conferma all'utente.
DigitalSign può operare con diversi account di marcatura temporale, da configurare preventivamente (dal menu Strumenti -> Configurazione Servizi).

Il selettore *Servizio Marcatura Temporale* mostra l'account indicato come predefinito, ma consente, nel caso vi siano più account configurati, di scegliere quale impiegare.

L'altro selettore *Salva come* non è utilizzabile in questo contesto.

- Il bottone **Applica timestamp** esegue l'operazione, collegandosi al server della TSA ed ottenendo la marca temporale associata al documento su cui si sta operando
- Il bottone **Annulla** chiude l'operazione senza richiedere la marca temporale alla TSA.

Si noti che subito dopo aver eseguito l'operazione di applicazione del timestamp la marca temporale viene mantenuta solo in memoria.
Soltanto al momento in cui l'utente disporrà il salvataggio su disco (con **File -> Salva Documento** o **Salva Documento con nome...**) verrà richiesto all'utente di scegliere una modalità di rappresentazione tra quelle supportate da DigitalSign.



3.5.6 Destinatario Cifratura

Funzione non disponibile con DigitalSign Reader

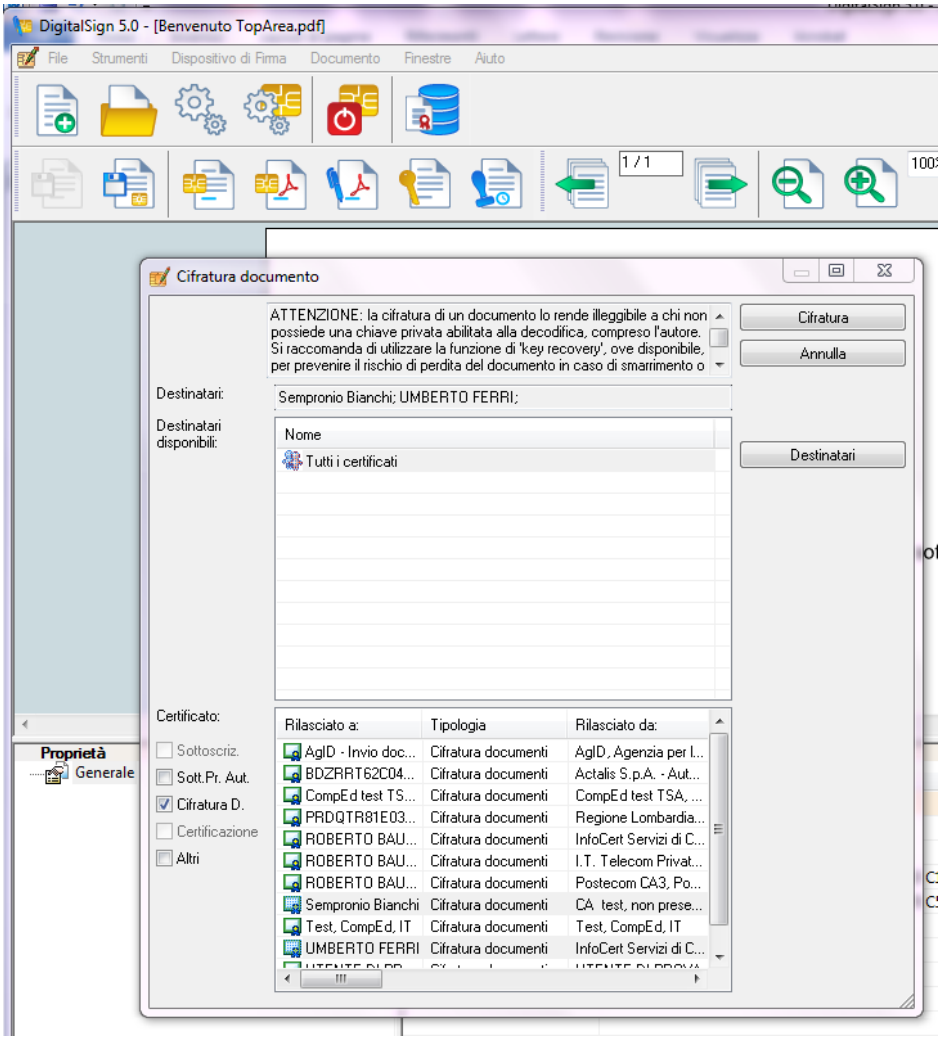
Permette di cifrare il contenuto del documento correntemente aperto a beneficio di uno o più destinatari.
Per i dettagli sulle modalità attuate da ***DigitalSign*** per cifrare i dati si veda la sezione relativa.

Si tenga comunque presente che la cifratura attuata da ***DigitalSign*** è in prima approssimazione di tipo "asimmetrico": si cifra utilizzando la chiave pubblica del soggetto abilitato a leggere i dati, in modo che quest'ultimo possa leggerli usando la corrispondente chiave privata a sua esclusiva disposizione.

In effetti è possibile cifrare a beneficio di molteplici soggetti, che vengono definiti "destinatari".
DigitalSign include sempre nella lista di questi destinatari lo stesso autore del messaggio, in modo che esso possa sempre leggere il contenuto del documento. A tale scopo ***DigitalSign*** richiede che, al momento in cui si richiede la cifratura di un documento aperto, sia inserita una smartcard, così da leggere il certificato da impiegare e da disporre della chiave privata necessaria alla rivisualizzazione una volta eseguita la codifica.

Non tutte le smartcard contengono effettivamente un certificato utilizzabile per questo scopo: se il dispositivo di firma a disposizione contiene soltanto un certificato qualificato per la Firma Digitale non sarà possibile cifrare (è vietato usare una chiave privata di firma per scopi diversi dalla firma).

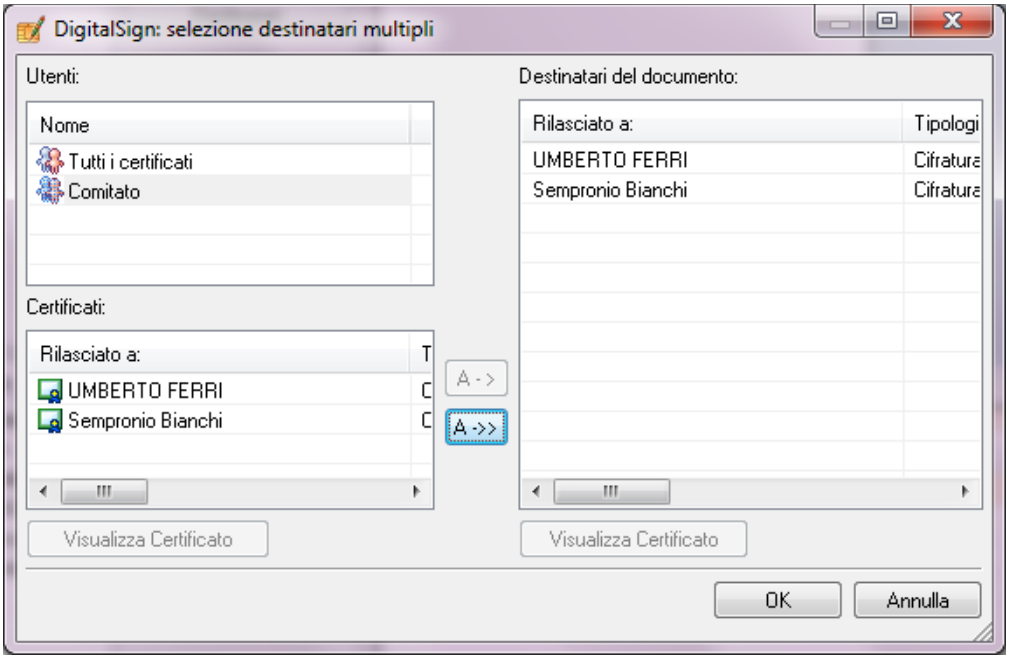
Supponendo di avere un certificato idoneo, ecco cosa appare sullo schermo appena si attiva il comando:



La schermata presenta una lista suddivisa in due riquadri, il primo dei quali mostra tutti i Gruppi di destinatari definiti (incluso il gruppo speciale **Tutti gli utenti**). Il secondo riquadro mostra tutti i certificati appartenente al Gruppo selezionato.
La definizione dei Gruppi si effettua dal modulo di gestione del DB locale dei certificati.

L'utente può posizionarsi sul riquadro inferiore e scegliere uno specifico singolo destinatario, oppure posizionarsi sul riquadro superiore e scegliere un intero Gruppo (escluso Tutti gli utenti): agendo sul bottone **Cifratura** per chiudere la finestra con la selezione effettuata.

Oppure l'utente può desiderare una selezione più articolata di destinatari, magari includendo più gruppi ed alcuni soggetti singoli, agendo sul bottone **Destinatari**, che conduce a questa schermata:



Il riquadro in alto a sinistra elenca i Gruppi disponibili; il riquadro sottostante mostra i certificati contenuti nel Gruppo selezionato.
Si opera selezionando un Gruppo nel primo riquadro oppure un destinatario singolo nel secondo riquadro, quindi premendo il bottone **[A ->]** oppure **[A ->>]** per includere il singolo destinatario o l'intero gruppo, rispettivamente, nella lista finale.
Nel riquadro di destra è sempre possibile selezionare un destinatario ed eliminarlo dalla lista con il tasto **[Canc]**.

i. Con il bottone **Annulla**, naturalmente, si esce senza aggiornare la lista.
ii. Con i bottoni **Visualizza Certificato** è possibile ispezionare i certificati dei riquadri corrispondenti.

Dopo aver cifrato un documento l'utente può desiderare di cancellare dal proprio sistema la versione originale (non cifrata) del documento. Questo è possibile con la funzione Wipe File.

NOTA IMPORTANTE: per facilitare l'utilizzo della cifratura anche con certificati autoprodotti ***DigitalSign*** non richiede che i relativi certificati siano verificati in termini di attendibilità del Certificatore che li ha emessi.
Tuttavia, l'utente dovrebbe assicurarsi dell'autenticità del certificato di un destinatario, specie se tale certificato corrisponde ad un soggetto non conosciuto personalmente o se è stato ricevuto via email.
Le funzioni di visualizzazione del certificato, in ogni contesto, consentono di effettuare la verifica.

NOTA IMPORTANTE: qualora si utilizzino le funzionalità di cifratura per rendere riservati i propri documenti si tenga sempre presente che l'apertura dei documenti cifrati richiede la disponibilità della chiave privata.
Se si utilizzano dunque chiavi contenute nelle smartcard o chiavette ottenute dai Certificatori per la firma digitale si consideri la difficoltà (o la impossibilità) di ottenere un duplicato di tali chiavi in caso di smarrimento o danneggiamento della smartcard.
Una buona strategia è munirsi di almeno due smartcard e includere sempre entrambi i propri certificati nella lista di destinatari.

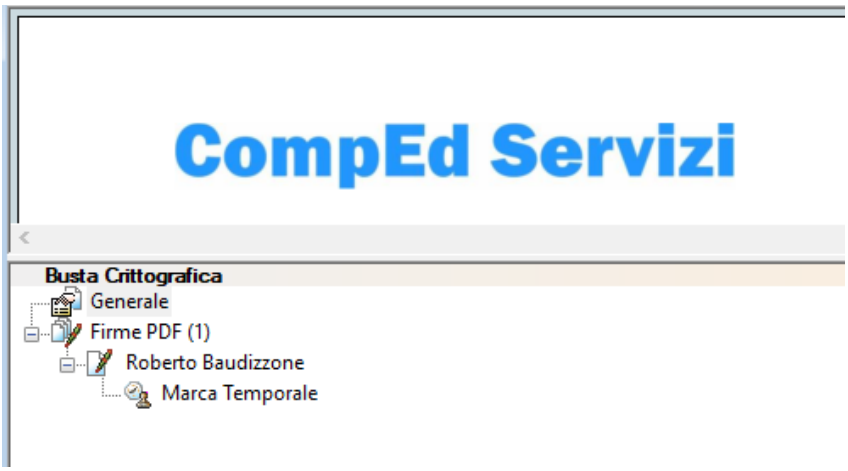
3.5.7 Elevare PAdES-LTV

Questa funzione può essere usata su un documento già firmato PAdES (sulla firma o le firme già presenti può esserci o meno una marca temporale già associata) al fine di elevarne lo status a PAdES-LTV (*Long Term Validation*).

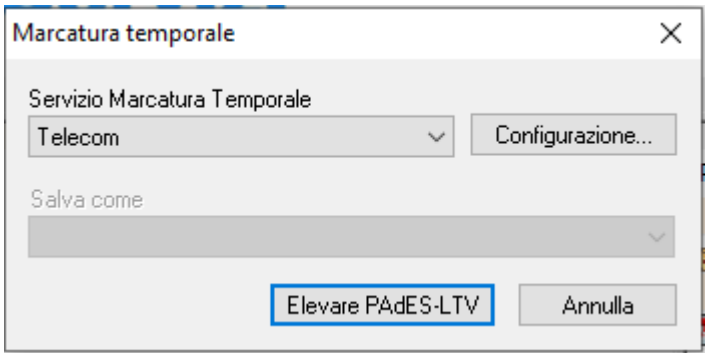
Al fine di preservare la validità di un documento firmato anche oltre la scadenza o la revoca dei certificati usati per firmarlo, si procede in questo modo:

i. si inseriscono all'interno del documento le copie di tutti i certificati dei firmatari e quelli delle CA che tali certificati hanno generato
ii. si inseriscono all'interno del documento le informazioni che permettono di accertare che all'istante presente i certificati non erano sospesi e/o revocati: se disponibili si inseriscono le *response* del server OCSP firmate dalla CA, altrimenti si inseriscono copie delle CRL valide al momento attuale.
iii. Si correda il tutto di una Marca Temporale che dimostra l'esistenza al momento attuale

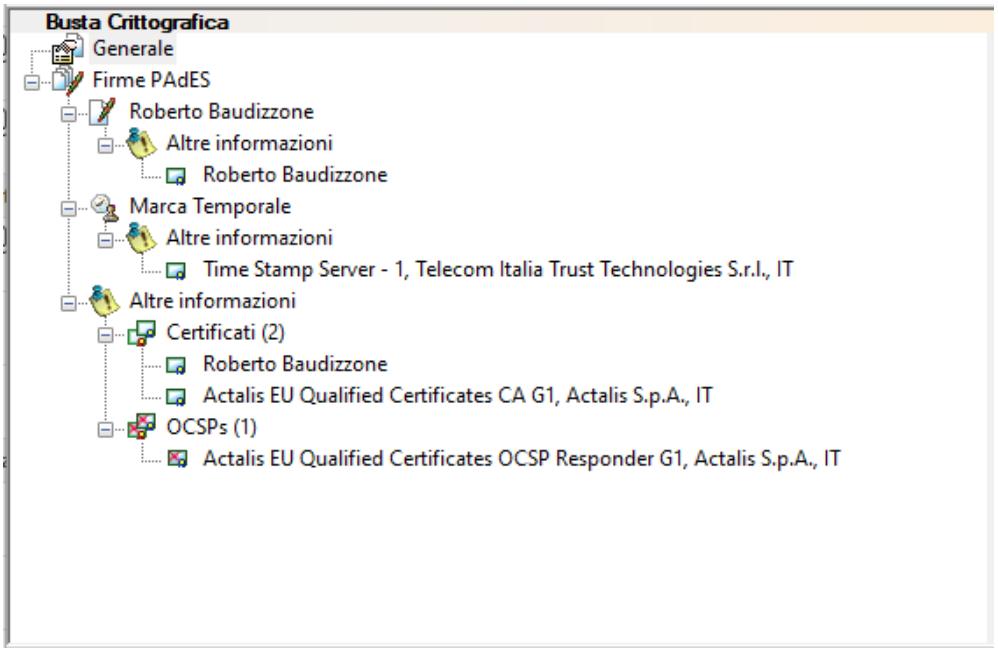
L'operazione è del tutto automatica: supponiamo di voler elevare allo status LTV un documento già firmato e alla cui firma si sia già apposta una marca temporale:



Azionando questa funzione DigitalSign si limita a chiedere conferma selezionando anche l'account di marcatura temporale da impiegare (potrebbero esserne disponibili più d'uno):



Una volta confermata l'operazione ***DigitalSign*** procede autonomamente per qualche secondo (deve consultare i server delle CA coinvolte e quindi richiedere la Marca Temporale).
Al termine la busta crittografica apparirà molto più ricca:



Sarà sufficiente salvare il file con un nome diverso e conservarlo senza preoccuparsi della scadenza dei certificati.

3.5.8 Annulla Tutto

Questo comando, ove applicabile, consente di annullare le modifiche fin qui apportate al documento aperto, ripristinandone lo stato preesistente.

3.5.9 Wipe File

Funzione non disponibile con DigitalSign Reader

Questo comando viene abilitato solo dopo che si realizza la cifratura di un documento e dopo il salvataggio del documento cifrato risultante.
La funzione *"wipe"* consiste nella cancellazione del file originale (in chiaro) ed avviene solo dietro esplicita conferma dell'utente.
DigitalSign, con questa funzione, non si limita a cancellare il file, ma mette in atto alcune misure volte ad aumentare la sicurezza dell'operazione, nel senso di eliminare ogni traccia del documento non cifrato dal file system dell'utente:

1. il file viene sovrascritto per tre volte con dati casuali (per eliminare tracce dei dati originali);
2. il file viene rinominato per tre volte (per eliminare tracce del nome originale);
3. il file viene impostato a lunghezza pari a zero (per rimuovere il collegamento con i settori del dico che ospitavano i dati);
4. il file viene effettivamente cancellato a livello del sistema operativo.

NOTA IMPORTANTE: quantunque le misure descritte rappresentino quanto di meglio ***DigitalSign*** possa fare per evitare che i dati in chiaro siano recuperabili dal sistema, esistono dei limiti oggettivi sull'efficacia di tali misure:

a) se il documento originale era stato predisposto con una applicazione di tipo "office", come per esempio MS Word oppure Excel, tale applicazione probabilmente manterrà – almeno durante la redazione del documento – uno o più file temporanei che potrebbero contenere tracce dei dati. Al termine dell'esecuzione, in generale, queste applicazioni cancellano i propri file temporanei con semplici comandi di cancellazione a livello del sistema operativo. DigitalSign, evidentemente, non può nulla per evitare il recupero dei dati da questi file;
b) quando il sistema operativo adotta un file system come NTFS esso ha la possibilità di spostare autonomamente i dati di un file da una parte all'altra del disco, di fatto eseguendo delle copie dei dati. In questi casi la cancellazione accurata dei dati dall'ultima copia del file nulla può contro la ricuperabilità dei dati dalle copie preesistenti

Per quanto sopra l'utente particolarmente sensibile al problema dell'eliminazione dei propri dati sensibili dopo la cifratura di un documento dovrebbe ricorrere ad altri strumenti specializzati, che provvedano alla sovrascrittura sistematica di tutti i settori del disco dichiarati "spazio libero" dal sistema operativo.

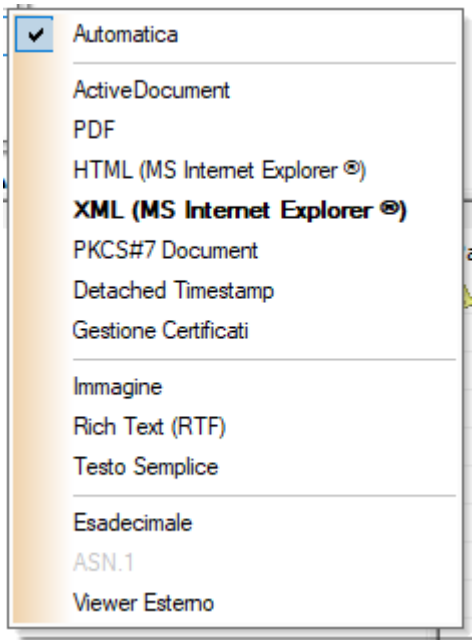
Da ultimo è appena il caso di notare che la cancellazione della copia originale di un documento cifrato va effettuata con cautela: nel caso venisse perduta la chiave privata abilitata a decifrare il documento non esisterà più alcun modo per recuperarne il contenuto.

3.5.10 Verifica alla data

Questo comando consente di impostare una data ed ora di riferimento, diversa dall'istante presente, per la verifica delle firme digitali del documento corrente.
Si rimanda per i dettagli all'apposita sezione

3.5.11 Sottomenu Modalità Visualizzazione

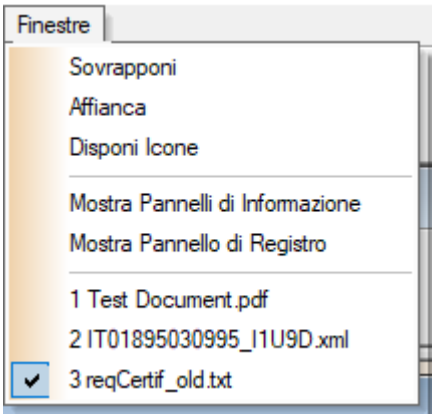
Questo comando conduce ad un sottomenu contenente le varie modalità di visualizzazione supportate.



Di regola la modalità selezionata è quella Automatica, che permette a DigitalSign di utilizzare automaticamente la modalità idonea a presentare il documento.
Nel menu è anche riportata in grassetto la modalità effettiva attualmente utilizzata.

Nel caso l'utente ritenesse di utilizzare una modalità diversa (per esempio quella esadecimale) può operare la propria scelta in questo menu.

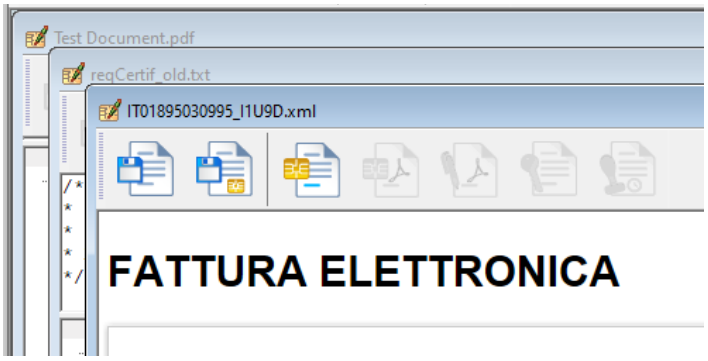
3.6 Il menu "Finestre"



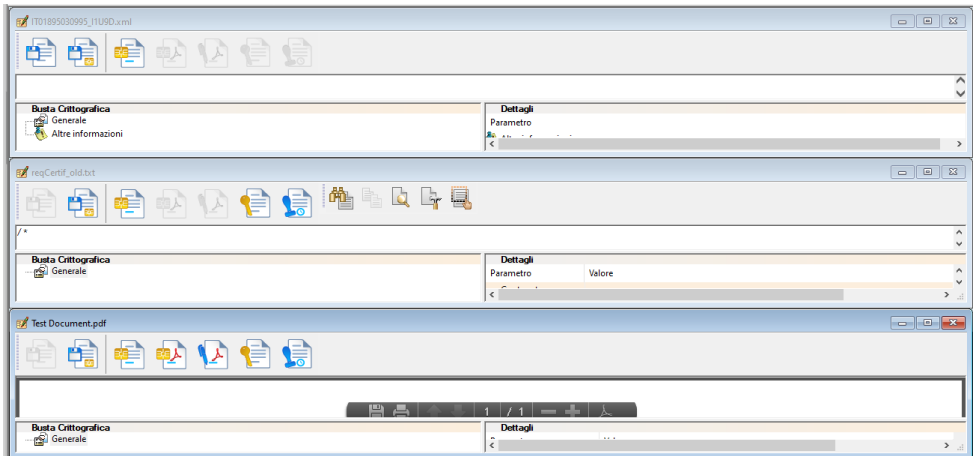
Questo menu fornisce alcuni comandi standard per riorganizzare la visualizzazione delle diverse finestre controllate da ***DigitalSign***.

Se sono aperte una o più finestre documento le ultime voci del menu corrispondono a tali finestre, consentendo di riportarle in primo piano.

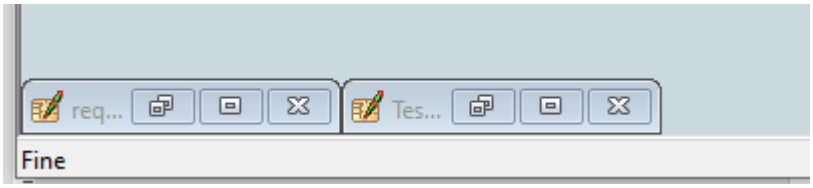
- **Sovrapponi** – presenta le finestre documento una sopra all'altra:



- **Affianca** – cerca di disporre tutte le finestre aperte:



- **Disponi icone**: ordina le finestre già *iconizzate* in fondo all'area dell'applicazione:



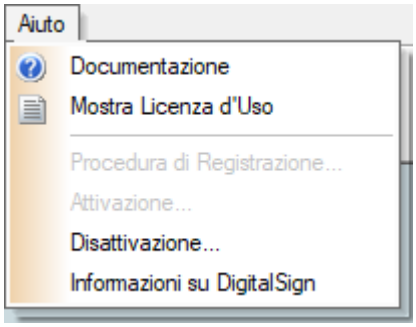
3.6.1 Mostra pannelli di informazione

Attiva o disattiva la visualizzazione dei pannelli informativi decritti nella sezione dedicata

3.6.2 Mostra pannello Registro

Consente di aprire, nella parte bassa della finestra principale dell'applicazione, una vista sul Registro Attività

3.7 Il menu "Aiuto"



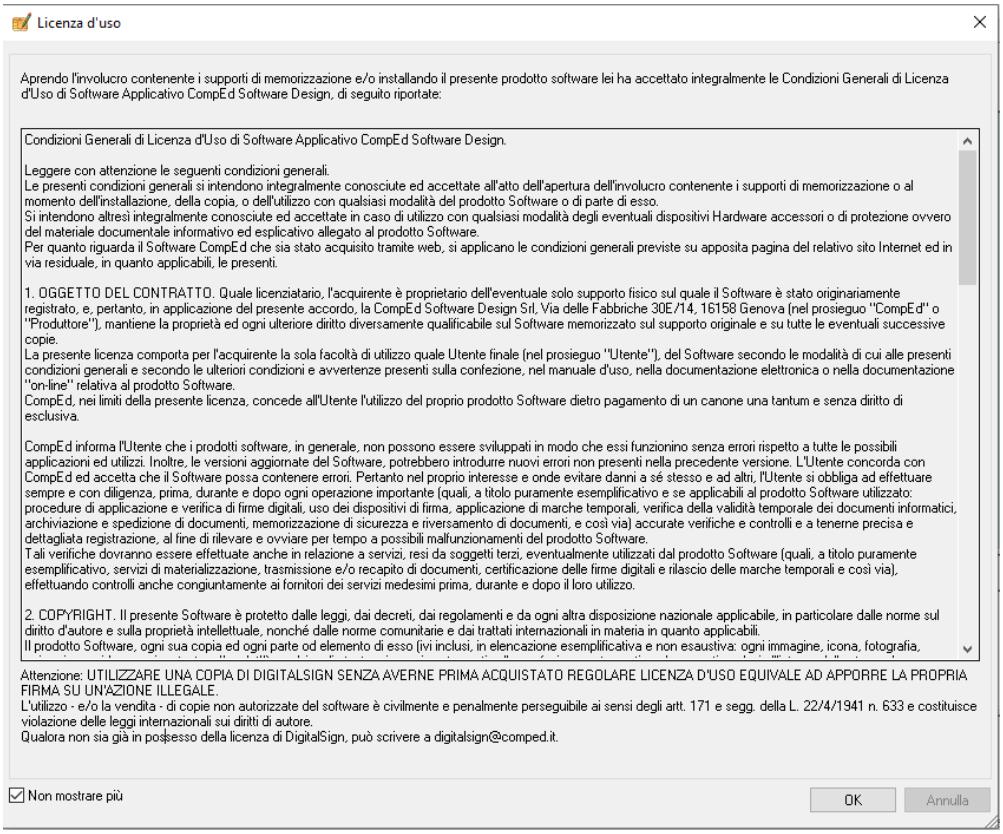
Questo menu offre alcune funzioni per visualizzare informazioni generali sulla versione del software in proprio possesso, sulla licenza d'uso, per registrare o attivare la propria copia del software.

3.7.1 Documentazione

Questa funzione provoca la visualizzazione della presente documentazione, se questa è disponibile e se sul computer è disponibile il software necessario alla visualizzazione (un *viewer* per il formato PDF).

3.7.2 Mostra Licenza d'uso

Visualizza la stessa schermata con le condizioni di licenza d'uso che viene normalmente visualizzata al primo avvio dell'applicazione.



La schermata viene mostrata ad ogni avvio, a meno che l'utente non selezioni il checkbox **Non mostrare più**.
Questo comando nel menu **Aiuto** serve proprio a rivisualizzare il testo in questo caso ed eventualmente modificare l'istruzione di evitare le prossime visualizzazioni.

3.7.3 Procedura di Registrazione

La procedura di Registrazione è obbligatoria su alcune edizioni di DigitalSign mentre può essere opzionale in altre (Professional) o addirittura non prevista (edizioni Professional OEM).

Questo comando, se applicabile, provoca l'esecuzione della procedura di Registrazione del prodotto.
Tale procedura, per le edizioni ed i casi previsti, viene di norma eseguita automaticamente al primo avvio dell'applicazione.

3.7.4 Attivazione

La procedura di attivazione segue quella di Registrazione e consiste nell'inserimento di un Codice di Attivazione fornito dal sistema di registrazione di CompEd.
Di norma questa funzione viene eseguita automaticamente di seguito a quella di Registrazione, ma esistono alcuni casi in cui l'utente può avere la necessità di avviare la procedura autonomamente, tramite questa funzione del menu.

3.7.5 Disattivazione

Se il prodotto è stato attivato mediante un Codice di Attivazione è di norma possibile disattivarlo, recuperando il relativo Codice Licenza per una nuova installazione, su un diverso computer.

3.7.6 Informazioni su DigitalSign

Presenta una schermata di questo tipo:

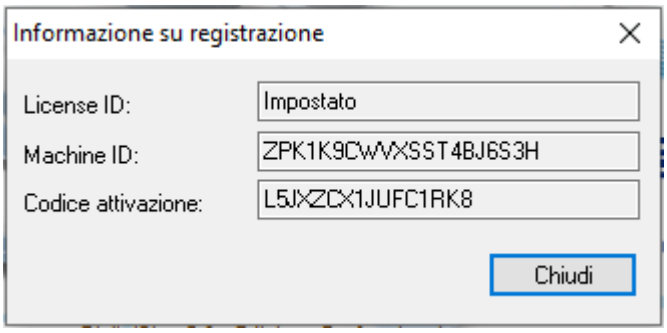
NOTA: In alcune edizioni OEM (personalizzate per grandi clienti) la visualizzazione può essere diversa e contenere il logo dell'organizzazione.

Da questa immagine l'utente può ricavare le indicazioni esatte sull'edizione e sul numero di versione della propria copia di ***DigitalSign***, nonché sull'identità dell'utente registrato.

È anche presente un link per accedere ad una pagina di *"credits"* per **OpenSSL**: si tratta di una libreria crittografica *Open Source* il cui utilizzo (da parte di CompEd, come da parte di migliaia di operatori nel mondo) è condizionato al fatto che siano visibili da parte dell'utente le informazioni riportate a seguito dell'azionamento di tale link.

È presente anche un link alla pagina principale del sito di CompEd.

Il bottone **Info Registrazione**, se presente, apre una piccola finestra di dialogo contenente, a scopo di riferimento, le principali informazioni relative alla registrazione/attivazione del prodotto:

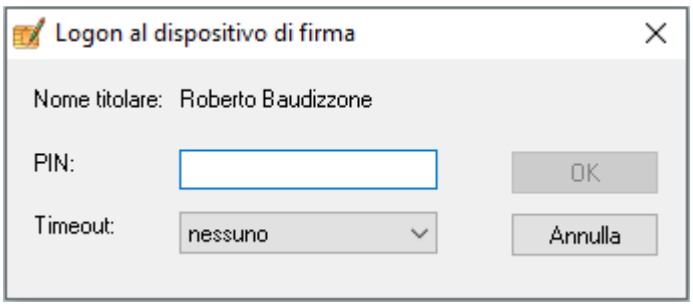


3.8 Moduli di gestione e finestre di dialogo

In questa sezione sono raccolte le descrizioni di alcuni moduli funzionali di ***DigitalSign*** utilizzati in diversi contesti.

3.8.1 Logon al dispositivo di firma

Questa finestra di dialogo viene presentata all'utente al momento in cui è richiesto che esso si identifichi – introducendo il PIN che solo il titolare deve conoscere – come legittimo titolare del dispositivo di firma correntemente in uso.



La finestra viene presentata quando l'utente richiede esplicitamente di effettuare il logon (dal menu **File**) oppure quando viene avviata un'operazione che coinvolge oggetti contenuti nell'area privata del dispositivo stesso, il quale si trova in stato di Logoff.

Nel campo **PIN** si digita appunto il codice di identificazione, che viene visualizzato in modo mascherato per impedire che venga carpito da chi osserva da dietro le spalle dell'utente.

Il selettore **Timeout** permette di scegliere un periodo di tempo, da 1 minuto sino a 10 minuti, oppure 'nessuno': Si tratta del tempo massimo per cui il dispositivo permane in stato di Logon senza che si verifichi alcuna attività con il dispositivo stesso.

Se si seleziona 'nessuno' il dispositivo non andrà in Logoff sino all'esplicito comando, oppure sino a che l'utente non rimuove il dispositivo o chiude l'applicazione.

- Con il bottone **OK** si conferma il dato digitato.
- Con il bottone **Annulla** si esce senza inviare il codice al dispositivo di firma.

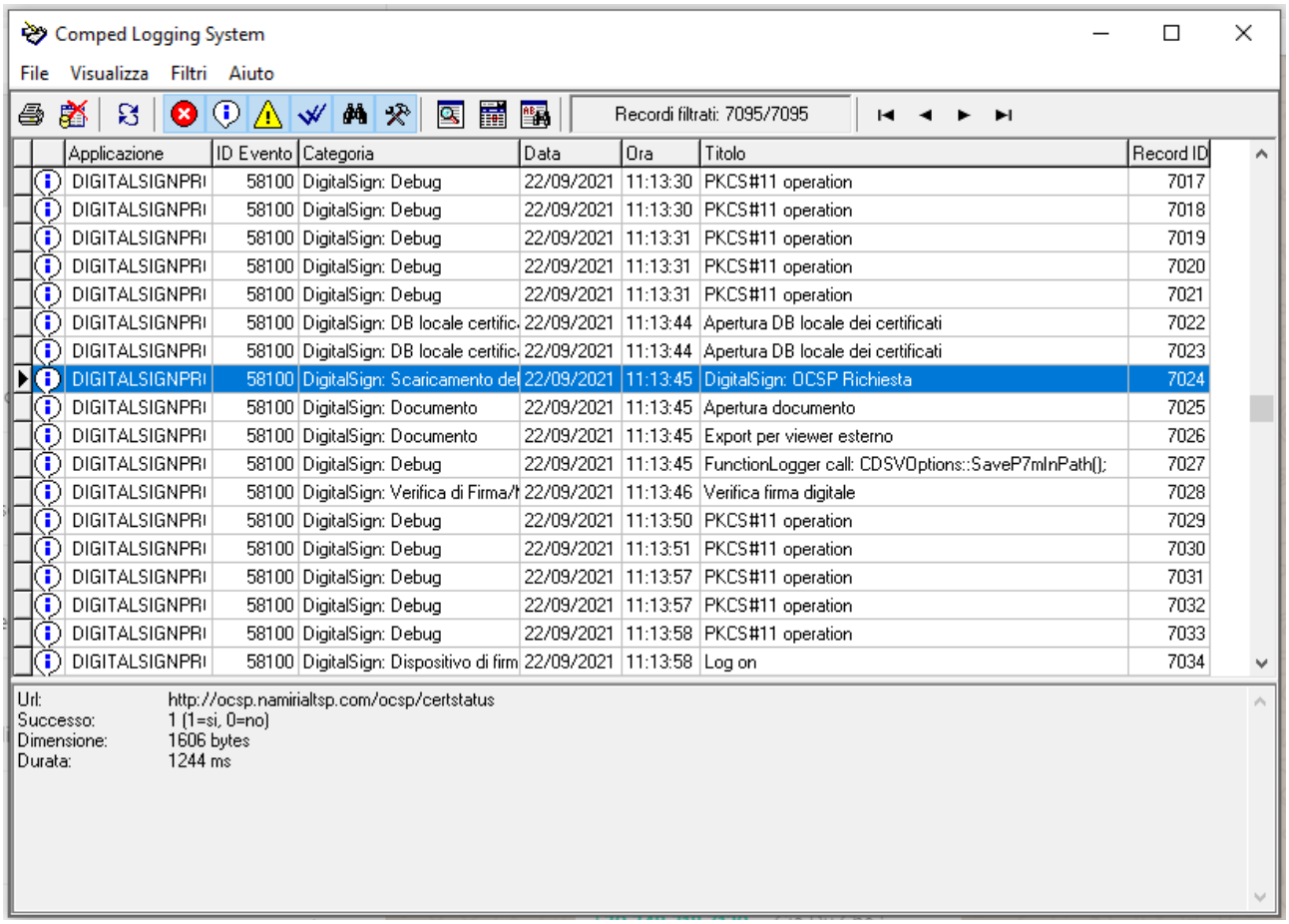
3.8.2 Il Registro Attività

DigitalSign mantiene un registro di attività molto ricco di informazioni.

Scopo principale del registro è fornire a ***CompEd*** informazioni di dettaglio per investigare anomalie.

L'abilitazione/disabilitazione del registro, come pure la preselezione delle categorie di eventi da includere/escludere nella registrazione, si controlla attraverso il menu Strumenti -> Opzioni e selezionando poi il tab **Registrazione Eventi**.

Il registro può essere visualizzato sia dal menu File -> Registro Attività che attivando il pannello registro dal menu Finestre -> Mostra pannello Registro.



La visualizzazione è organizzata con due pannelli:

- **eventi** – una lista organizzata in colonne: qui troviamo il nome dell'applicazione che genera ogni evento, la categoria, data ed ora di ogni evento, il titolo dell'evento
- **dettagli** – il pannello inferiore che contiene i dettagli dell'evento correntemente selezionato

La tool bar consente, intuitivamente, di selezionare le categorie da includere nella visualizzazione, aggiornare la vista, introdurre criteri di filtraggio particolari.
Se il Registro è visualizzato dal menu File -> Registro Attività è disponibile anche un menu che ripete le funzioni accessibili tramite la toolbar.

Importante la funzione **Manutenzione**, che consente di impostare una posizione per i file del registro: da qui è possibile soprattutto ricavare la posizione attuale del DB e – all''occorrenza – copiare i file in un archivio per la trasmissione a CompEd.

3.8.3 Il processo di verifica di una firma digitale

La *meccanica* della verifica di una firma consiste nella decifratura della firma stessa mediante la chiave pubblica dell'asserito sottoscrittore – ottenendo una copia dell'impronta – e nel confronto di tale valore con l'impronta calcolata direttamente sui dati, mediante l'appropriata funzione *hash*.

Tuttavia, al di là di verificare che il documento sia integro – operazione matematica priva di criticità – in un contesto reale è importante soprattutto verificare che il sottoscrittore sia veramente chi dice di essere e che il suo certificato sia in corso di validità.

Un documento firmato elettronicamente contiene una copia del certificato di ogni sottoscrittore.
Quindi il sistema di verifica ha a portata di mano la chiave pubblica per eseguire la verifica di integrità sopra descritta.

Ma per verificare l'identità del sottoscrittore il sistema deve verificare se il certificato è autentico.
A tale scopo si deve verificare la firma digitale della CA, apposta al certificato stesso.

Per verificare questa firma occorre disporre del certificato della CA; questo di regola è possibile conservando, a disposizione del proprio sistema, una lista dei certificati delle CA di proprio interesse.
Nel caso in cui il certificato della CA sia stato emesso da un'altra CA di livello superiore occorre risalire tutta la "catena di certificazione" fino al livello più alto (cioè fino a quando si trova il certificato *self-signed*, si veda Il Certificatore).
Giunti a questo punto, per essere sicuri che questo certificato sia autentico, occorre contare su una copia locale veramente attendibile. Se un malintenzionato è in grado di farci considerare attendibile un certificato *self-signed*, può anche costruire facilmente una falsa catena di certificazione e simulare qualunque identità.

In un vero contesto di gestione di documenti informatici questo è il punto più delicato: l'attendibilità dei certificati delle CA. Vedremo come ***DigitalSign*** implementa per questo fine accorgimenti ad elevato livello di sicurezza, ma in questa sede ci limitiamo a portare il problema all'attenzione del lettore.

Dicevamo che oltre all'autenticità del certificato (ossia che sia stato veramente emesso da una CA considerata attendibile) occorre anche verificare che il certificato stesso sia in corso di validità.
Una prima verifica, banale, viene eseguita confrontando la data odierna con le date di emissione e scadenza registrate nel certificato stesso.

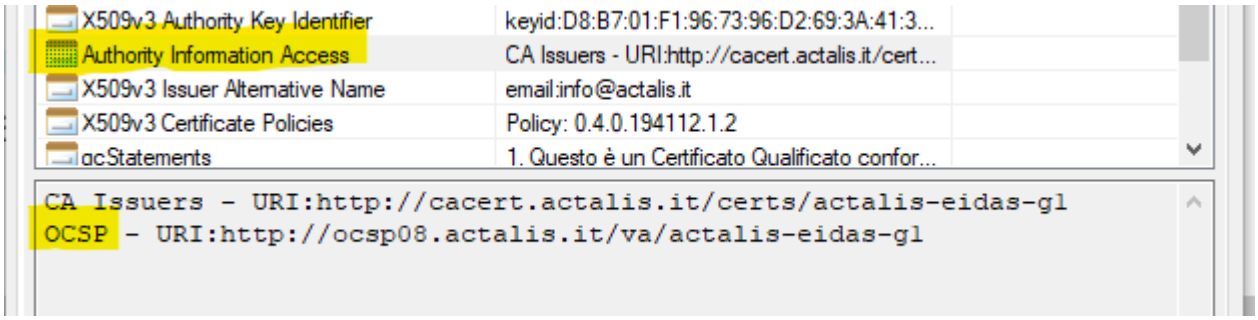
Ma, accertato che il certificato non sia scaduto, occorre verificare che il certificato non sia stato revocato.

In generale questo si può fare in due modi, ma non è detto che il singolo certificato sotto esame li consenta entrambi:

- Tramite OCSP
- Tramite CRL

3.8.3.1 Verifica dello stato di revoca tramite OCSP

Questo è possibile se il certificato sotto esame contiene, nell'attributo Authority Information Access, l'indirizzo di un servizio OCSP (Online Certificate Status Protocol):

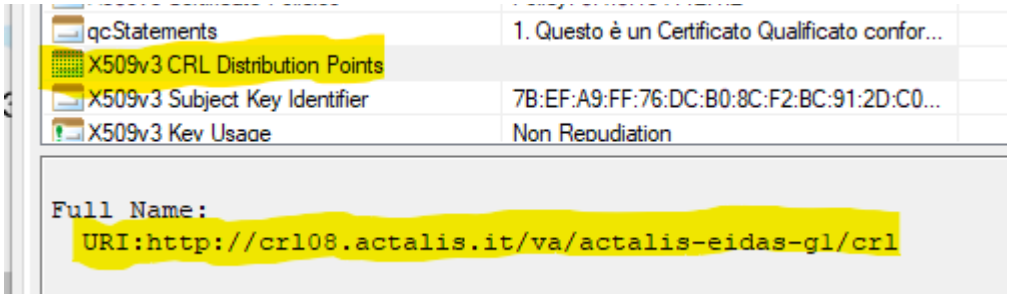


In tal caso il software di verifica contatta tale servizio e richiede informazioni sullo stato di revoca del certificato, individuato tramite il numero di serie.
Il server OCSP risponderà fornendo l'informazione richiesta, in generale che è tutto OK, oppure che il certificato è stato revocato per una qualche ragione.

3.8.3.2 Verifica dello stato di revoca tramite CLR

Il Certificatore mantiene una lista aggiornata dei numeri di serie dei certificati sospesi e revocati per ciascuna propria CA (CRL = Certificate Revocation List).

Questa lista (aggiornata frequentemente) è disponibile per il download ad un indirizzo Internet scritto all'interno del certificato stesso, nell'attributo CRL Distribution Point:



Per verificare lo stato di revoca il sistema di verifica esegue i seguenti passi:

1. estrazione, dal certificato, dell'indirizzo da cui scaricare la CRL (CRL Distribution Point)
2. scaricamento della CRL da tale indirizzo
3. verifica della firma della CA apposta alla CRL
4. verifica che la data ed ora attuali ricadano nell'intervallo tra la data ed ora di emissione e la data ed ora di prossimo aggiornamento pianificato della CRL
5. ricerca del numero di serie del certificato da verificare nella lista contenuta nella CRL

Naturalmente se la lista contiene effettivamente il numero di serie del certificato che stiamo verificando si deve concludere che il certificato, in questo momento, non è valido. E quindi nemmeno il documento che contiene una firma apposta mediante quel certificato, a meno che non sia possibile dimostrare che il documento era stato firmato in precedenza, anteriormente alla revoca.

3.8.3.3 Attendibilità dei Certificatori: le TSL e gli elenchi di certificati attendibili definiti dall'utente

Come introdotto nella sezione dedicata al processo di verifica, esiste la necessità di disporre di una fonte fidata per decidere sulla validità dei certificati delle CA e – di conseguenza – di quella dei certificati usati per firmare i documenti che andiamo a verificare.

A livello di Unione Europea il Regolamento eIDAS ha disposto un meccanismo per distribuire queste informazioni per tutti i Certificatori europei.
Ogni stato membro dell'Unione predispone e mantiene una lista (TSL = *Trust-Service Status List*) di certificati di CA attendibili perché accreditate all'interno di quello stato.
Inoltre, la lista contiene l'indirizzo Internet della TSL principale europea, la quale a sua volta contiene gli indirizzi di tutte le TSL degli altri stati membri.

La TSL Italiana è firmata digitalmente da AgID (Agenzia per l'Italia Digitale), l'Agenzia governativa che disciplina questa materia.
Il certificato che AgID usa per firmare la TSL è pubblicato nella Gazzetta Ufficiale: quindi se il software di verifica possiede una copia certa di questo certificato può verificare la TSL, da qui può verificare tutti i certificati di CA dei Certificatori, nonché tutti quelli delle CA accreditate in Unione Europea.

La TSL italiana non contiene soltanto i certificati delle CA che emettono certificati qualificati: contiene anche le CA che emettono i certificati per autenticazione contenuti nelle CNS (Carta Nazionale dei Servizi) e quelli delle TSA (le speciali Certification Authority che generano i certificati per le Marche Temporali), consentendo quindi una verifica automatica anche di queste tipologie di certificati.

Ma, come abbiamo visto, ***DigitalSign*** può essere usato per generare/verificare anche Firme Elettroniche Avanzate o Firme Elettroniche semplici, non basate su questi certificati "ufficiali". In questo caso è possibile creare (e distribuire) proprie liste di CA attendibili, firmandole con i propri certificati: il sistema evidenzierà – al momento di verificare una firma – che è stata generata con uno di questi certificati, indicando anche chi l'ha dichiarato attendibile.

3.8.4 Modulo di gestione del DB (locale) dei Certificati

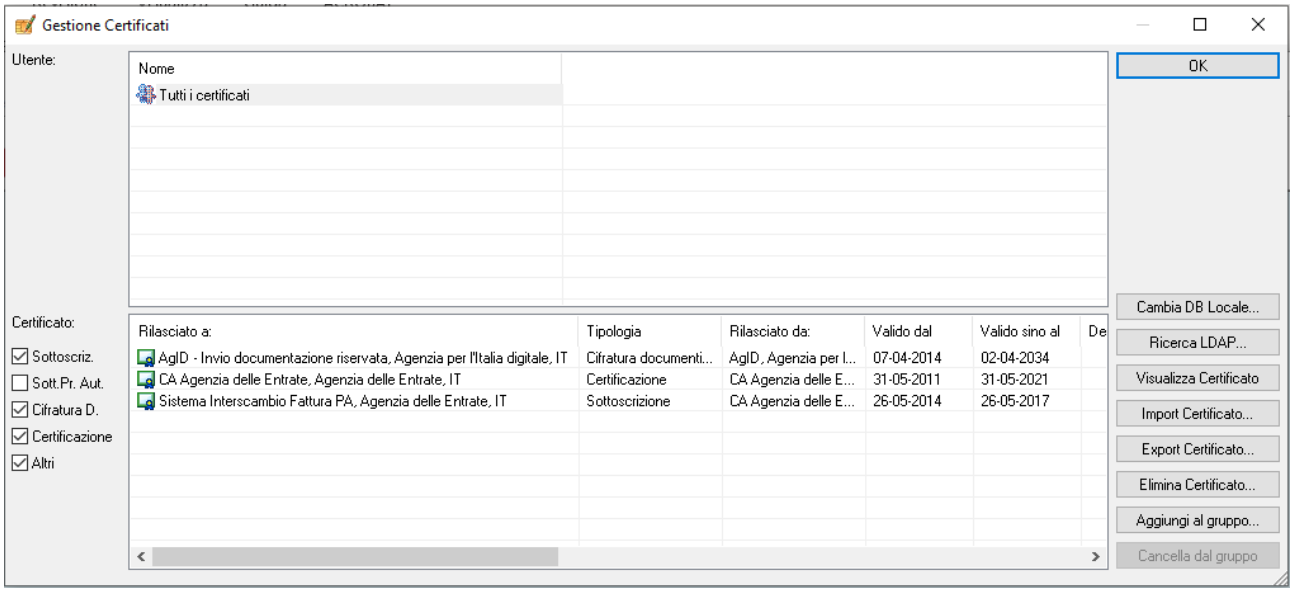
Il DB locale dei certificati è un archivio destinato, appunto, a contenere certificati.
Questo archivio può servire a diversi scopi, secondo che si operi in modalità di security **STRONG** oppure **SOFT** (si veda la sezione relativa).

- in modalità **STRONG *DigitalSign*** basa le verifiche dei certificati su una lista di CA dichiarate accreditate e/o attendibili tramite la firma digitale di AgID e – opzionalmente – tramite la firma di un ulteriore soggetto che si assume la responsabilità di dichiarare attendibili altre CA non accreditate.

  Quindi il DB locale non serve a contenere certificati di riferimento per le operazioni di verifica, ma di fatto funge solo da "rubrica" di certificati da utilizzare per le operazioni di crittografia. Come illustrato a proposito della cifratura dei documenti, l'utente che si accinge a codificare un contenuto sceglierà da questo archivio il soggetto o i soggetti abilitati a decifrarlo;

- in modalità **SOFT *DigitalSign*** verifica positivamente i certificati emessi da qualunque CA il cui certificato si trovi nel DB locale; quindi, il DB locale serve proprio a contenere i certificati delle CA considerate attendibili.

Il modulo di gestione si presenta come nella seguente figura:

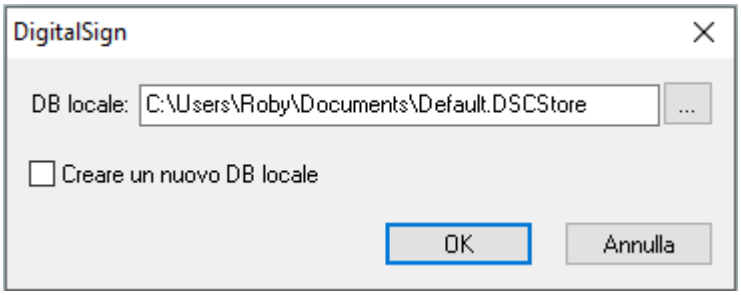


Il riquadro superiore contiene l'elenco dei **Gruppi** correntemente definiti: per default è sempre definito il gruppo speciale **Tutti gli utenti**.

Il riquadro inferiore contiene una lista dei certificati contenuti nel Gruppo correntemente selezionato nella finestra superiore; se nel riquadro superiore è selezionato il Gruppo **Tutti gli utenti** allora il riquadro inferiore mostra tutti i certificati dell'archivio.

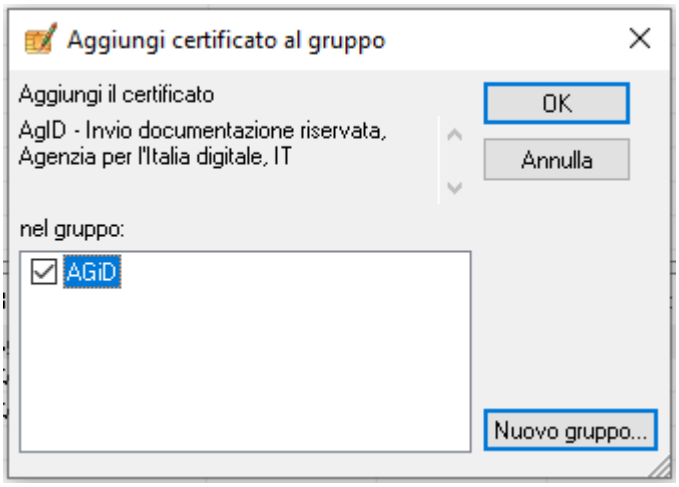
Sulla sinistra compare una batteria di *checkbox* che permette di abilitare o disabilitare la visualizzazione di diverse tipologie di certificato.

- Con il bottone **OK** si chiude la finestra
- Con il bottone **Cambia DB Locale** è possibile mettere in uso un diverso DB.
  Compare in tal caso una finestra di questo tipo:



  È possibile selezionare un diverso file, sfogliando con il bottone **[…]**, oppure crearne uno nuovo – vuoto – impostando il nome e selezionando l'apposito *checkbox*.

- Con il bottone **Ricerca LDAP** è possibile accedere al server LDAP gestito da un certificatore e ricercare certificati. La lista dei server disponibili per questa ricerca si gestisce attraverso il menu Strumenti -> Configurazione Servizi -> Elenchi in linea LDAP.
  La prossima sezione mostra come operare una effettiva ricerca LDAP per ottenere un certificato di cifratura.
- Con **Visualizza Certificato** si apre la finestra di visualizzazione del certificato selezionato.
- Con **Import Certificato** è possibile importare nel DB un certificato disponibile su file.
- Con **Export Certificato** è possibile esportare su file il certificato correntemente selezionato
- Con **Elimina certificato** si rimuove dal DB il certificato selezionato
- Con **Aggiungi a Gruppo** è possibile includere il certificato correntemente selezionato in un particolare Gruppo, eventualmente creato appositamente.
  Scopo principale dei Gruppi è predefinire delle "liste di destinatari" da utilizzare frequentemente per le operazioni di cifratura dei contenuti.
  Si apre una ulteriore finestra di dialogo:



  La finestra mostra i Gruppi già definiti (eventualmente vuota); se il gruppo a cui si intende aggiungere il certificato selezionato è già esistente è sufficiente fare click sulla casella corrispondente. Altrimenti è possibile creare subito un Nuovo Gruppo con il bottone corrispondente.

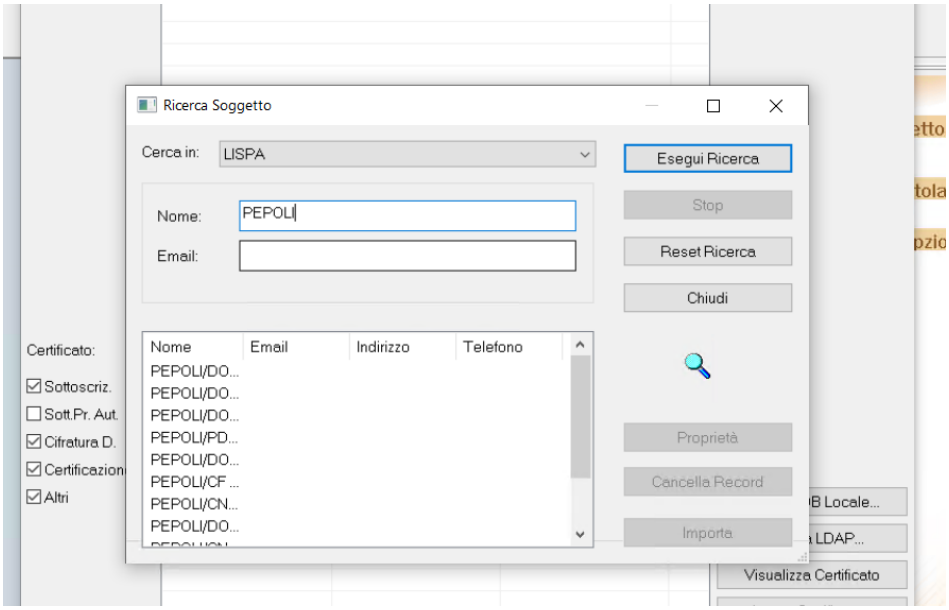
- Con **Rimuovi dal Gruppo** è possibile far sì che il certificato correntemente selezionato nel riquadro inferiore (e quindi appartenente al Gruppo selezionato nel riquadro superiore) venga eliminato dal gruppo stesso.

3.8.4.1 Ricerca di un certificato tramite LDAP

Come detto, una delle funzioni del DB locale dei certificati è fungere da rubrica per i certificati di cifratura dei soggetti a cui intendiamo trasmettere documenti crittografati.
In generale ci faremo trasmettere (via mail o in qualsiasi altro modo) una copia del certificato del nostro corrispondente, ma alcune organizzazioni possono contare su servizi di directory attraverso i quali è possibile reperire i certificati degli appartenenti all'organizzazione.

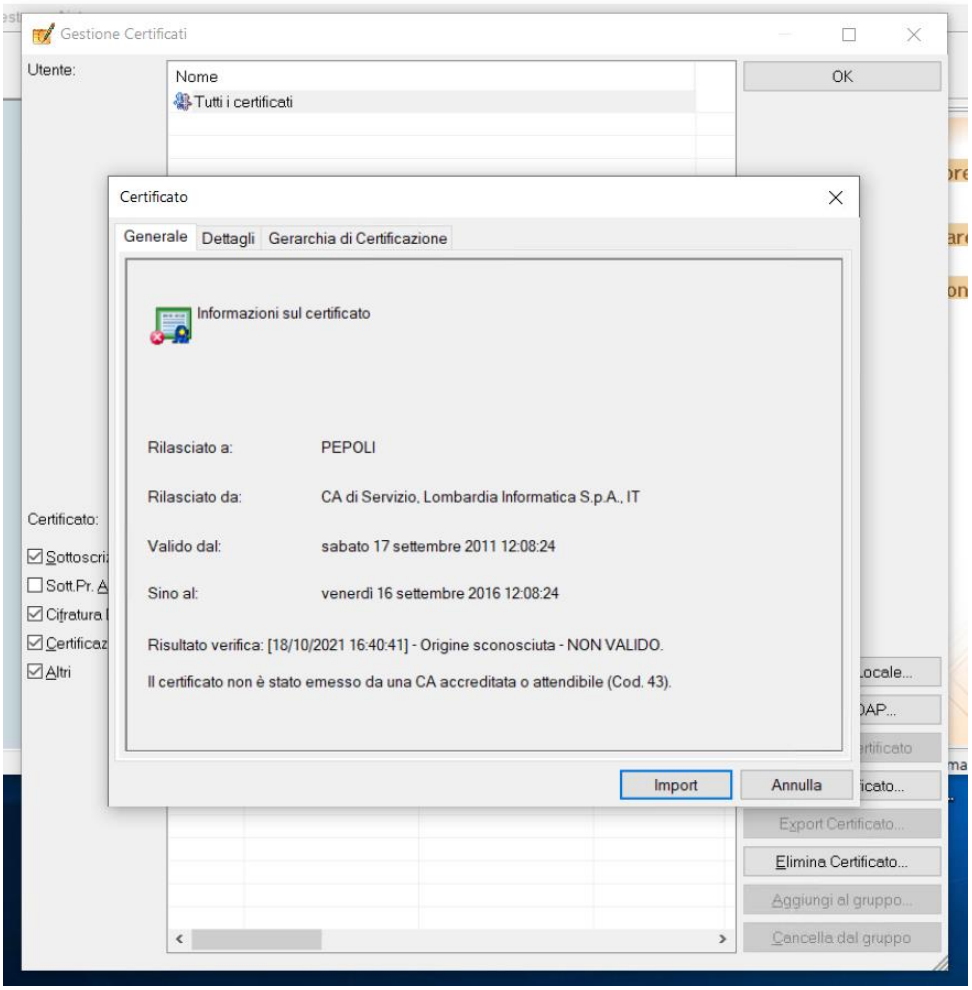
È il caso di Regione Lombardia: gli afferenti al sistema SISS sono registrati nell'archivio Intranet dei certificati e possono usare tale archivio per ricercare i corrispondenti.

Dopo aver fatto click sul bottone Ricerca LDAP si ottiene questa schermata:



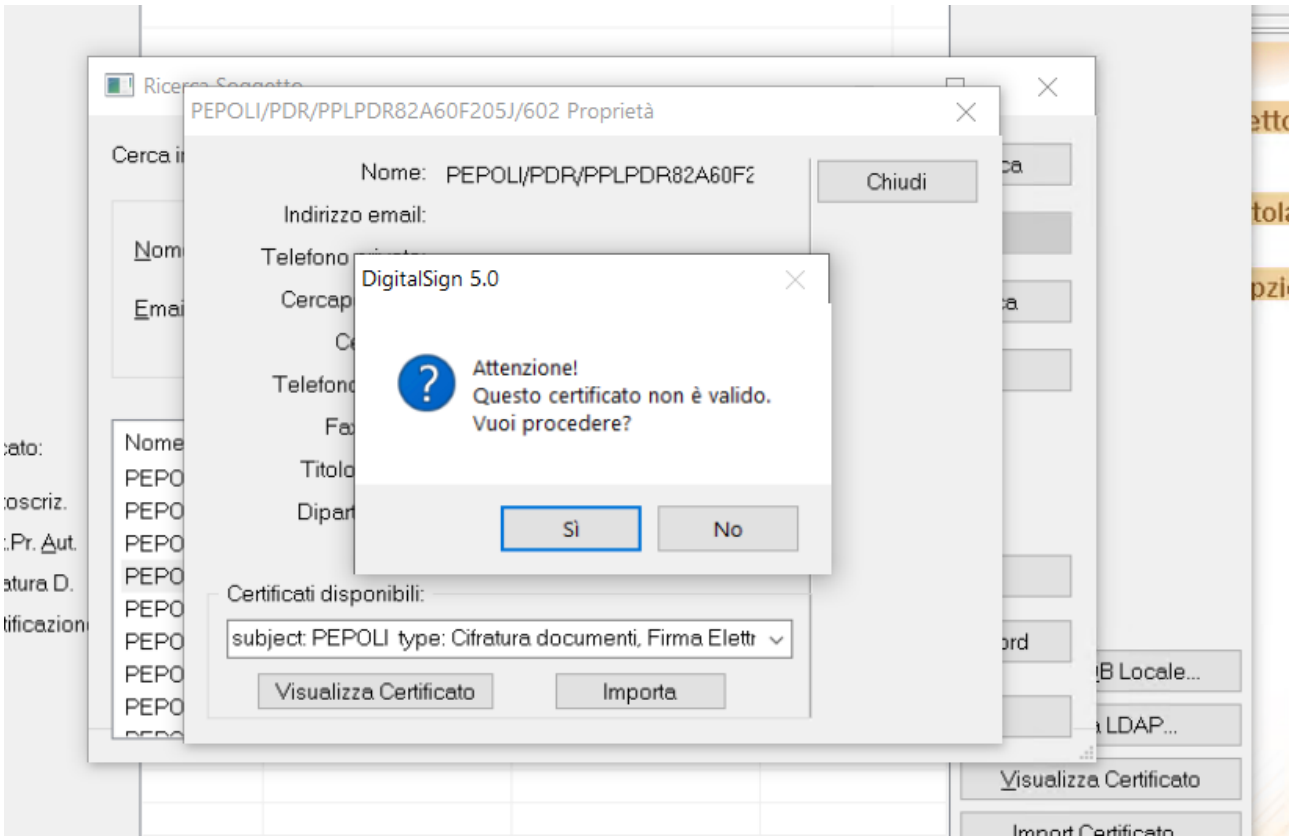
Digitando una parte del nominativo cercato e facendo click su Esegui Ricerca otterremo una lista di certificati intestati alla persona che stiamo cercando.

Se i certificati sono numerosi dovremo visionarli uno per uno alla ricerca di quello indicato, dopo di che potremo sceglierlo per l'importazione:



Si noti che un certificato può essere importato anche se non è "valido" agli effetti della verifica: in questo caso useremo un certificato scaduto ed emesso da una CA non dichiarata attendibile, ma per la cifratura dei contenuti questo non è un problema, in generale.

Con il bottone **Import** caricheremo il certificato nel DB, previa conferma che vogliamo importare un certificato non verificato:



3.8.5 Modulo di Gestione delle Liste di Sospensione e Revoca (CRL)

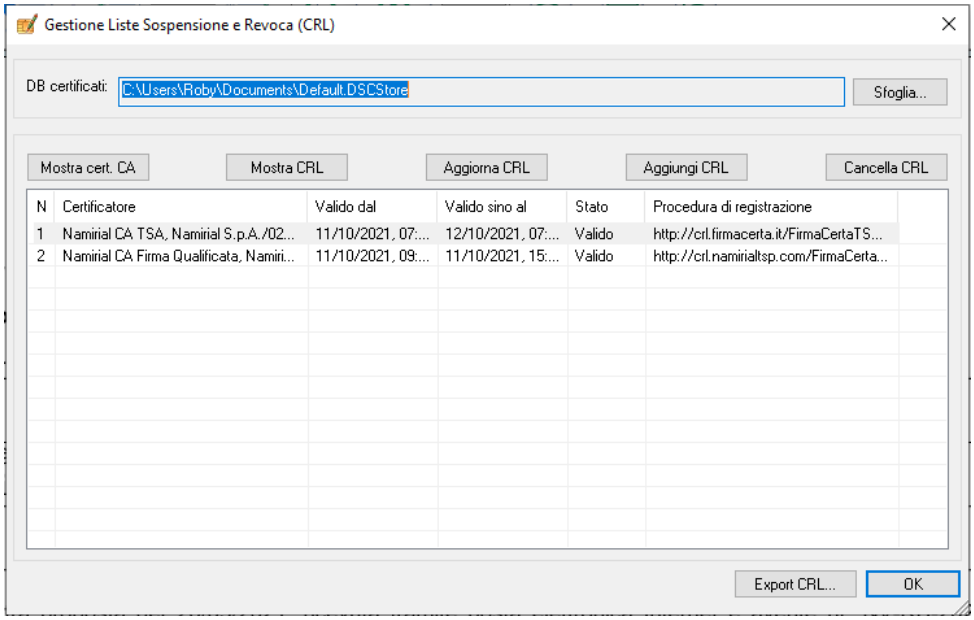
NOTA IMPORTANTE: in passato le Liste di Sospensione e Revoca erano l'unico strumento disponibile per consentire di verificare che il certificato usato per generare una firma non fosse in stato sospeso o revocato: il Certificatore emette periodicamente lista (firmata digitalmente) contenente tutti i numeri di serie dei certificati sospesi e revocati; il software scarica la lista e vi cerca il numero di serie del certificato sotto esame: se non lo trova deduce che il certificato è valido.

Oggi lo stato di quasi tutti i certificati qualificati di recente emissione può essere verificato mediante una richiesta diretta al Certificatore tramite il protocollo OCSP, senza necessità di scaricare tutta la lista.

Man mano che ***DigitalSign*** esegue operazioni di verifica di certificati mediante le liste CRL (se il certificato sotto esame non prevede un punto di erogazione del servizio OCSP o se è disabilitata la funzionalità OCSP in configurazione), accede ai server delle CA che hanno emesso i certificati e richiede il download di tali CRL (Liste di Sospensione e Revoca).
Si ricorda che l'indirizzo URL a cui si reperisce una CRL è scritto nel certificato stesso, nell'estensione standard CDP (CRL Distribution Point), protetta dalla firma del Certificatore stesso.

Ogni CRL scaricata viene automaticamente memorizzata all'interno dello stesso file che ospita anche il DB locale, sovrascrivendo l'eventuale copia più vecchia della stessa lista.

Il modulo di gestione delle CRL si presenta come in figura:



La lista presenta tutte le CRL correntemente presenti nell'archivio locale, con una organizzazione in colonne:

- **Certificatore**: il nominativo del certificatore che ha emesso la lista
- **Valido dal:** la data ed ora di inizio validità della lista. Coincide con la data ed ora di emissione da parte del certificatore
- **Valido sino al:** rappresenta il temine di validità della CRL, che dovrebbe coincidere con la pubblicazione del prossimo aggiornamento della CRL da parte del certificatore
- **Stato:** valido o non valido, in base al momento attuale ed alla finestra di validità dichiarata con i due campi "Valido dal" e "Valido sino al"

NOTA IMPORTANTE: una CRL compare nella lista solo se ***DigitalSign*** si è trovato a verificare un certificato che punta a tale lista. Il fatto poi che la copia in archivio sia "Valida" o "Scaduta" dipende dal fatto che tale verifica sia stata fatta di recente (cioè nel periodo di validità nominale) oppure più indietro nel tempo: se una CRL scade ma non serve a verificare un certificato ***DigitalSign*** non si preoccupa di aggiornarla automaticamente.

In alto compare il nome (completo di percorso) del file del DB locale certificati che contiene anche le CRL sotto osservazione. Con il bottone **Sfoglia** è possibile esplorare altri file dello stesso tipo.

- con il bottone **Mostra certificato di CA** si ottiene la visualizzazione del certificato della Certification Authority che ha emesso la CRL selezionata, tramite l'apposito viewer
- Con il bottone **Mostra CRL** si visualizza il contenuto della CRL correntemente selezionata, mediante un viewer specifico
- Con il bottone **Aggiorna CRL** si provoca l'immediata rilettura della CRL aggiornata dal server della CA. Si noti che questa funzione non è utilizzabile con tutte le CA: può funzionare solo nel caso in cui il certificato della CA contenga l'estensione CDP (CRL Distribution Point) e che alla URL così ottenuta sia presente la CRL corrispondente
- Con **Aggiungi CRL** è possibile caricare nell'archivio una CRL disponibile su un file, ottenuta con altri mezzi
- Con **Cancella CRL** si può eliminare dall'archivio la CRL selezionata.
- Con **Export CRL** è possibile esportare su un file la CRL selezionata
- Con il bottone **OK** si chiude la finestra

Per informazioni sulle strategie attuate da ***DigitalSign*** nell'utilizzo delle CRL per la verifica di firme e certificati si veda la sezione relativa.

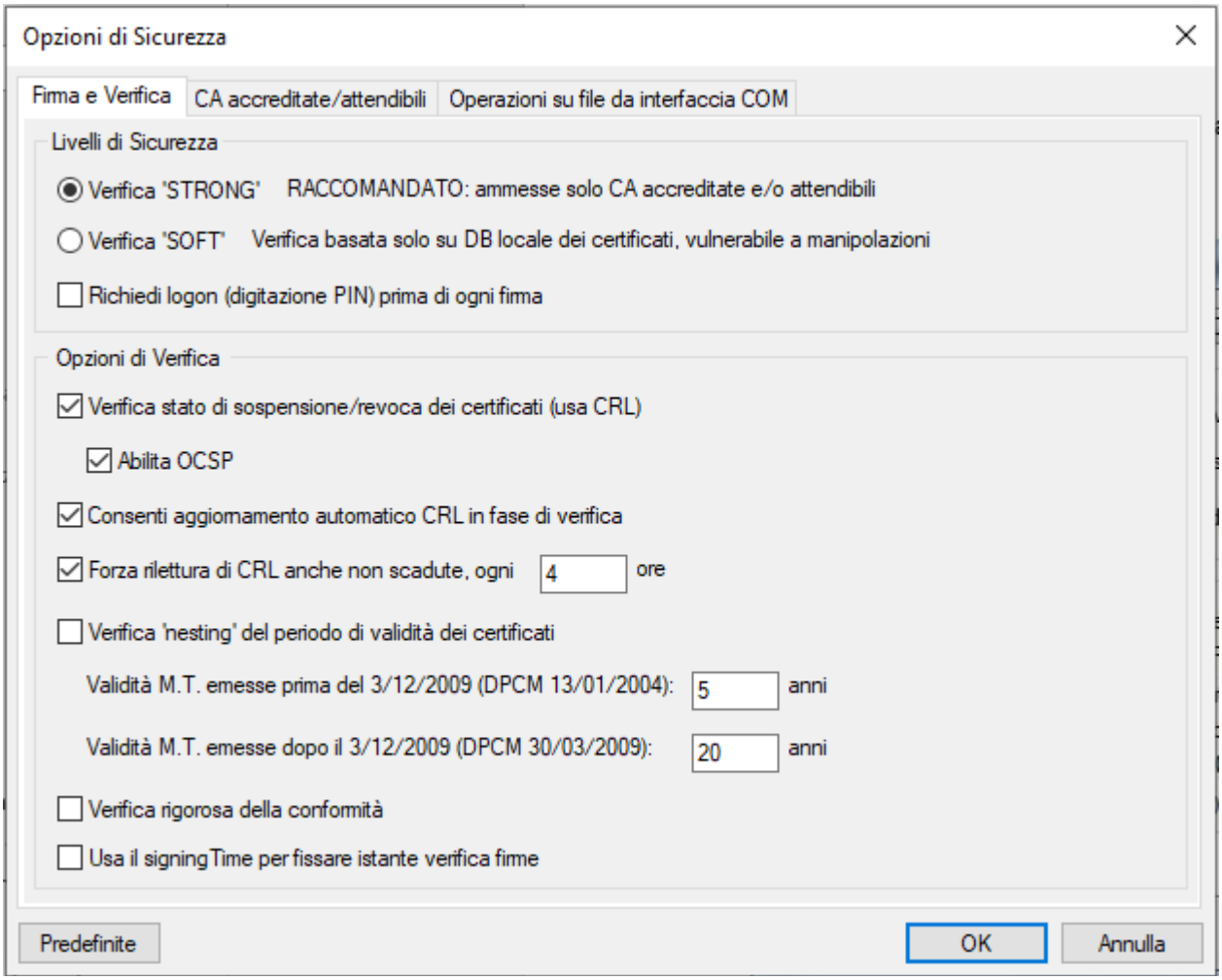
3.8.6 Modulo di Gestione delle Opzioni di Security

Questo modulo di configurazione presenta tre diverse cartelle per gestire altrettante serie di parametri.
Per tutte le cartelle sono disponibili i seguenti bottoni:

- **Predefinite** – ripristina i valori di default
- **OK** – salva le modifiche e chiude la finestra

- **Annulla** – chiude la finestra senza salvare le modifiche eventualmente apportate

3.8.6.1 Firma e verifica



Questo pannello consente di configurare la strategia di verifica ed il comportamento di ***DigitalSign*** in fase di verifica di documenti, firme, certificati.

Il riquadro superiore (**Livelli di Sicurezza**) permette di scegliere, per mezzo di una coppia di *radio button*, tra la modalità di verifica **STRONG** e la modalità **SOFT**.

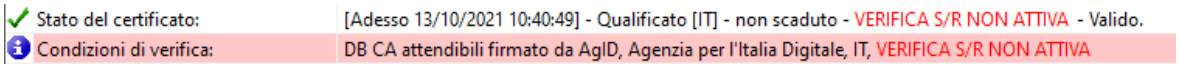
- in modalità **STRONG** ***DigitalSign*** considera attendibili soltanto i certificati emessi da una CA inclusa nella *'trust list'*.
  La trust list è un elenco di certificati di CA costituito da:
  - l'elenco ufficiale delle CA accreditate (TSL) pubblicato da AgID (contiene anche le CA che emettono certificati di tipo CNS per l'autenticazione);
  - l'elenco firmato di ulteriori CA attendibili (opzionale, si veda la prossima sezione)
  - i certificati di CA eventualmente contenuti nella smartcard inserita

  NOTA: in fase di verifica di un certificato o di una firma DigitalSign mostra esplicitamente in quale di questi sottoinsiemi ha trovato il certificato della CA pertinente.

- In modalità **SOFT** ***DigitalSign*** considera attendibili i certificati emessi da qualunque CA il cui certificato sia presente nel DB locale dei certificati. Questa modalità è comoda per test ed esperimenti, ma non dovrebbe essere usata in contesti di utilizzo effettivo.

Il riquadro sottostante (**Opzioni di Verifica**) presenta una serie di *checkbox* che controllano il comportamento in fase di verifica:

- **Verifica dello stato di sospensione/revoca dei certificati** – se attivo istruisce ***DigitalSign*** a verificare i certificati anche in merito all'eventuale stato di sospensione o revoca, tramite la relativa CRL (Lista di Sospensione o Revoca) o – si veda il punto successivo – tramite protocollo OCSP. Se questa opzione non è attiva ***DigitalSign*** mostra sempre un apposito messaggio di *warning* in occasione di ogni verifica:



- **Abilita OCSP** – ormai quasi tutti i certificati qualificati consentono la verifica dello stato di revoca in modo puntuale, chiedendo tale informazione direttamente al Certificatore tramite il protocollo OCSP *(Online Certification Status Protocol)*, senza necessità di scaricare ed analizzare la CRL.
  Abilitando questa opzione – nell'ipotesi che sia abilitata anche la precedente – il sistema usa OCSP anziché la CRL, purché questo sia disponibile per il certificato in esame.

- **Consenti aggiornamento automatico della CRL in fase di verifica** – se attivo consente a ***DigitalSign***, in occasione della verifica di un certificato mediante CRL, di scaricare automaticamente la relativa CRL nel caso non disponga di una copia sufficientemente aggiornata.
  Se questa opzione non è attiva ***DigitalSign*** chiede conferma prima di operare lo scaricamento.
  Naturalmente le CRL possono essere scaricate ed utilizzate solo se si dispone di un collegamento ad Internet.

- **Forza rilettura di CRL anche non scadute, ogni <*x*> ore** – ogni CRL viene pubblicata dalla CA corredata di informazioni sul periodo di validità (più esattamente sull'istante pianificato per il prossimo aggiornamento). Per le CA accreditate in Italia il periodo di validità varia da alcune ore sino a 24 ore; la normale strategia di verifica è quella di considerare valida una CRL per tutto il tempo di validità dichiarata: se si verificano più certificati emessi dalla stessa CA, in generale solo la prima verifica provocherà l'effettivo scaricamento della CRL, dopo di che si continua ad utilizzare la copia scaricata localmente.
  Attivando questo *checkbox*, tuttavia, si istruisce ***DigitalSign*** ad anticipare il nuovo scaricamento della CRL trascorso un certo tempo dall'ultima volta in cui la lista era stata effettivamente scaricata, anche se essa è ancora nominalmente valida. Questo accorgimento consente di beneficiare con la massima tempestività di eventuali pubblicazioni anticipate da parte dei Certificatori.
  Si noti che le verifiche di certificati eseguite puntualmente tramite OCSP non sono influenzate da questa opzione.

- **Verifica "nesting" del periodo di validità dei certificati** - questa opzione consente di attivare o disattivare una funzione di verifica soggetta a diverse interpretazioni da parte di diversi addetti ai lavori, che cerchiamo di spiegare.
  Si ricordi che un certificato intestato ad un soggetto è sempre emesso da un Certificatore, il quale lo firma utilizzando la propria chiave privata associata al proprio certificato di CA.
  Certa letteratura tecnica prescrive che in nessun caso un certificatore possa emettere un certificato il cui periodo di validità superi il periodo di validità del certificato di CA usato per firmarlo (ciò appare ragionevole, perché quando il certificato di CA sarà scaduto il certificato in questione sarebbe ancora valido, ma la verifica non potrà comunque essere complessivamente superata a causa della non validità del certificato di CA). Questo concetto è chiamato *nesting* del periodo di validità (l'intervallo di validità del certificato emesso è totalmente compreso - *nested* - nell'intervallo di validità dell'emittente).
  Tuttavia, non si tratta di una regola imposta dagli standard, quanto di un vincolo implementato nei sistemi più autorevoli e diffusi: alcuni certificatori non osservano (o almeno non osservavano) questa regola mettendo in circolazione certificati la cui validità sconfina dai limiti di validità del certificato di CA.
  Tornando alla configurazione di ***DigitalSign***, se si attiva questa opzione i certificati che violano il principio del *nesting* non saranno considerati validi, altrimenti il problema verrà ignorato (fintanto che sarà ancora valido il certificato di CA relativo!).

Seguono poi due parametri connessi con il periodo di validità legale delle Marche Temporali:

- **Validità Marche Temporali emesse prima del 3/12/2009 (ex DPCM 13/01/2004) <*x*> anni**
  Il DPCM 13/01/2004, all'art. 50, obbligava i certificatori a conservare copia di tutte le marche temporali emesse per un periodo minimo di 5 anni, oppure più a lungo a seguito di accordi con i

clienti. Lo stesso decreto chiariva poi che i documenti firmati digitalmente e corredati di una marca temporale – ovviamente corrispondente ad un istante di tempo in cui la firma fosse realmente valida – mantenessero la propria validità anche dopo la scadenza del certificato usato per la sottoscrizione.
Questo parametro consente di impostare il periodo di validità per le marche temporali in esame (per default 5 anni)

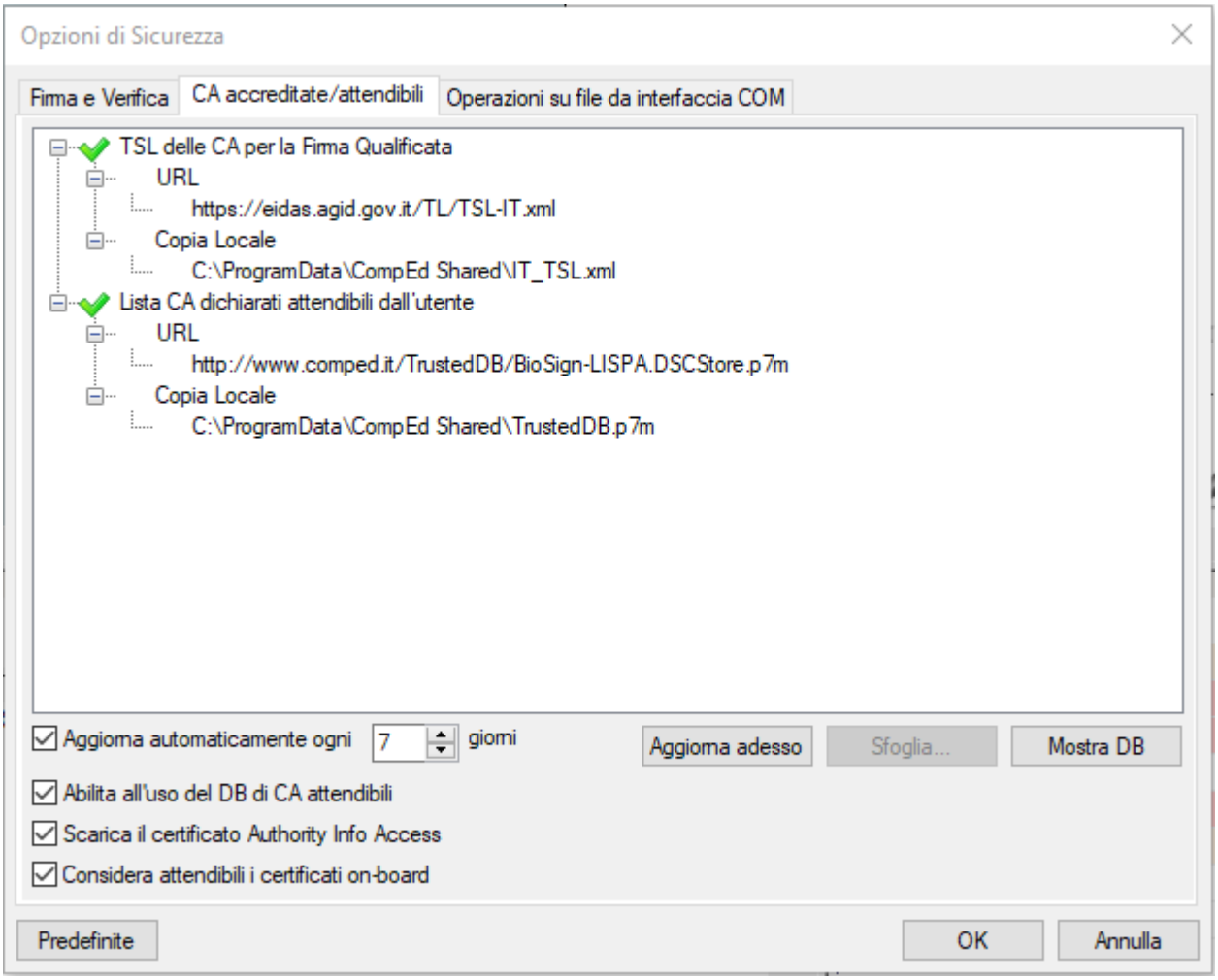
- **Validità Marche Temporali emesse dopo il 3/12/2009 (ex DPCM 30/03/2009) <*y*> anni**
  Il DPCM 30/03/2009, all'art. 49, modifica l'obbligo estendendolo a 20, ferma restando la facoltà di accordi certificatore-cliente per tempi di conservazione più lunghi.
  Il successivo DPCM 22/02/2013, all'art. 53, conferma identica disposizione.
  Questo parametro consente di impostare la durata di default pari a 20 anni o periodi ancora più lunghi.

  La data del 3/12/2009 è quella di entrata in vigore dell'obbligo di conservazione per 20 anni stabilito dal DPCM 30/3/2009.
  Quindi i parametri descritti servono a ***DigitalSign*** per decidere sulla durata effettiva della validità di una marca temporale rispetto all'emissione.
  Se una marca temporale era stata emessa oltre 5 anni prima del 3/12/2009 allora il 3 dicembre 2009 probabilmente la sua copia nell'archivio del certificatore non esiste più, dunque il documento non ha più il pieno valore probatorio.
  Ma se la marca fosse stata emessa, per esempio, il 10 dicembre 2004 allora il 3 dicembre 2009 la copia d'archivio esisteva ancora e quindi l'obbligo di conservazione si estende ad un totale di 20 anni; e quindi, per i successivi 15 anni, il documento è ancora valido.

- **Verifica rigorosa della conformità** – lo standard ETSI per i formati delle firme digitali prevede che gli attributi su cui calcolare l'impronta – e da questa la firma – siano disposti in un ordine preciso. Ma molte applicazioni di firma, specie se derivate da prodotti non europei, non rispettano questo vincolo. ***DigitalSign*** verifica anche il rispetto di tale ordine e in caso non sia rispettato segnala la circostanza in verifica.
  Tuttavia, proprio perché molte applicazioni considerate attendibili non lo rispettano, poiché si tratta di una non conformità lieve che non inficia l'attendibilità di una firma, è possibile disattivare questo controllo e ottenere una verifica positiva.

- **Usa il signing Tme per fissare l'istante di verifica firme** – una firma dovrebbe sempre essere corredata di un riferimento temporale che indica l'istante in cui la firma è stata generata; tale riferimento può essere una Marca Temporale – che ha valore di prova, se emessa da un Certificatore Accreditato – oppure il più semplice attributo *SigningTime* (normalmente ricavato dall'orologio del computer, che non ha, di per sé, valore di prova).
  Quando noi verifichiamo una firma, anche molto tempo dopo la sua generazione, il certificato usato per la firma potrebbe essere nel frattempo scaduto oppure revocato.
  Quindi la verifica, se fissata al momento attuale, potrebbe dare risultato negativo anche se il certificato era valido al momento della firma.
  DigitalSign, per default, fissa la verifica al momento in cui la firma è stata generata se il riferimento temporale è una Marca Temporale (perché ha valore di prova). Così facendo la verifica risulta positiva se il certificato non era scaduto o revocato all'epoca della firma.
  Il sistema, invece, fissa la verifica all'istante attuale – e non a quello testimoniato dal *SigningTime*, che non ha valore di prova – se non c'è una vera e propria Marca Temporale.
  Attivando questo checkbox si modifica questo comportamento di ***DigitalSign***, istruendolo a "fidarsi" anche del *SigningTime*.
  Si veda anche il concetto di Verifica alla data.

3.8.6.2 CA accreditate/attendibili



Questo pannello controlla i punti di riferimento utilizzati da ***DigitalSign*** per considerare attendibili i certificati sottoposti a verifica in modalità **STRONG**.

Nel pannello sono mostrati, in generale, due strutture ad albero:

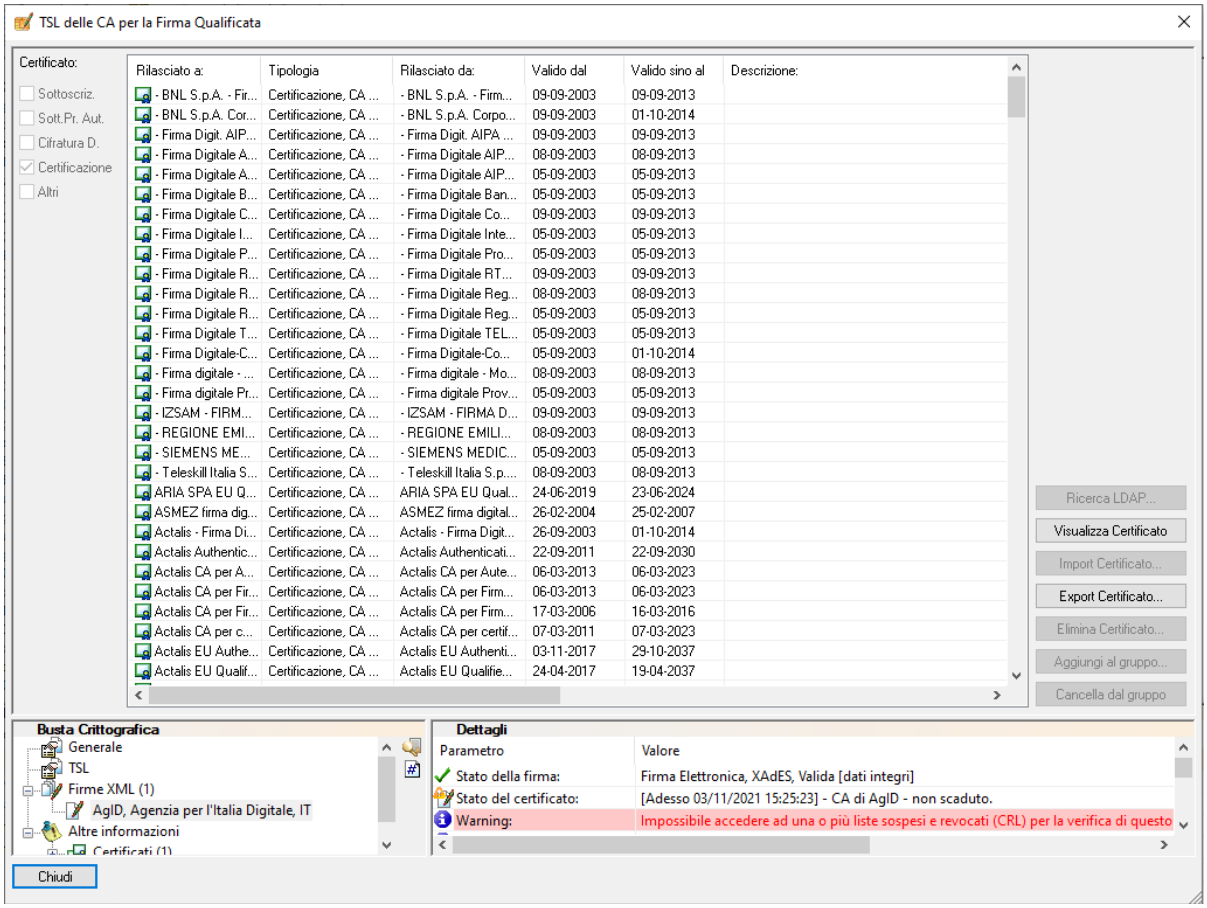
- **TSL delle CA per la Firma Qualificata** – si tratta di un file pubblicato dal Governo italiano, in conformità con il regolamento eIDAS, contenente la lista di tutti i certificati di CA riconosciuti attendibili in Italia.
  Si tratta delle CA che emettono certificati qualificati, certificati per i server di marcatura temporale, certificati CNS validi per l'autenticazione ai servizi della PA.
  La TSL contiene anche informazioni relative ai punti di pubblicazione di analoghe liste manutenute da altri stati membri dell'Unione Europea.
  La TSL è firmata digitalmente da AgID mediante un certificato la cui impronta è pubblicata in Gazzetta Ufficiale (DigitalSign contiene tale valore nel proprio codice e lo usa per verificare l'attendibilità dei certificati che contiene e – di conseguenza – quella di tutte le firme che si trova a verificare.
  Questo albero contiene un paio di "foglie" importanti:
  - La URL da cui scaricare la TSL – questo dato non è modificabile, è un indirizzo statico, pubblicato nella Gazzetta Ufficiale
  - La posizione della "copia locale" di questa TSL – anche questo è un dato *read-only* – ***DigitalSign*** scarica periodicamente o su richiesta manuale (vedere più avanti) la TSL e la copia localmente per poterla utilizzare

- **Lista certificati di CA dichiarati attendibili dall'utente** – qui abbiamo la possibilità di costruire una lista supplementare di certificati di CA che consideriamo attendibili. Ad esempio, può essere il caso di certificati per la Firma Elettronica Avanzata.
  Si veda l'appendice dedicata alla costruzione di un elenco personalizzato di CA attendibili.
  La URL da cui scaricare questo file è impostabile, facendo doppio click sull'indirizzo.

Anche questa lista prevede una "copia locale", la cui posizione è fissa.

I controlli sottostanti hanno le seguenti funzioni:

- Il checkbox **Controlla aggiornamento ogni <x> giorni** permette di impostare un aggiornamento automatico, con la periodicità desiderata, per entrambe le liste eventualmente impostate;
- Il bottone **Aggiorna adesso** consente di operare un aggiornamento manuale immediato dell'elenco selezionato
- Il bottone **Sfoglia** permette di modificare il percorso della copia locale della lista certificati di CA dichiarati attendibili dall'utente;
- Il bottone **Mostra DB** visualizza il contenuto dell'elenco correntemente selezionato:



Si noti che la visualizzazione, specie quella della TSL, può richiedere un'attesa di qualche decina di secondi: si tratta di un file XML contenente molti elementi e il sistema deve interpretarlo per costruire la lista visualizzabile e navigabile.

NOTA: la verifica della firma di AgID apposta a questo elenco mostra un warning relativo allo stato di revoca. Questo è dovuto al fatto che la CA di AgID, usata solo per questo scopo, ha un approccio non standard alla generazione della CRL (la firma con una CA diversa da quella che firma il certificato). Del resto, una vera e propria revoca di questo certificato è impossibile, nel caso AgID avesse problemi con la chiave relativa dovrebbe generare e dichiarare un diverso certificato.

Da questa finestra, oltre a ispezionare la busta crittografica e il suo contenuto, è solo possibile selezionare, visualizzare, esportare un singolo certificato.

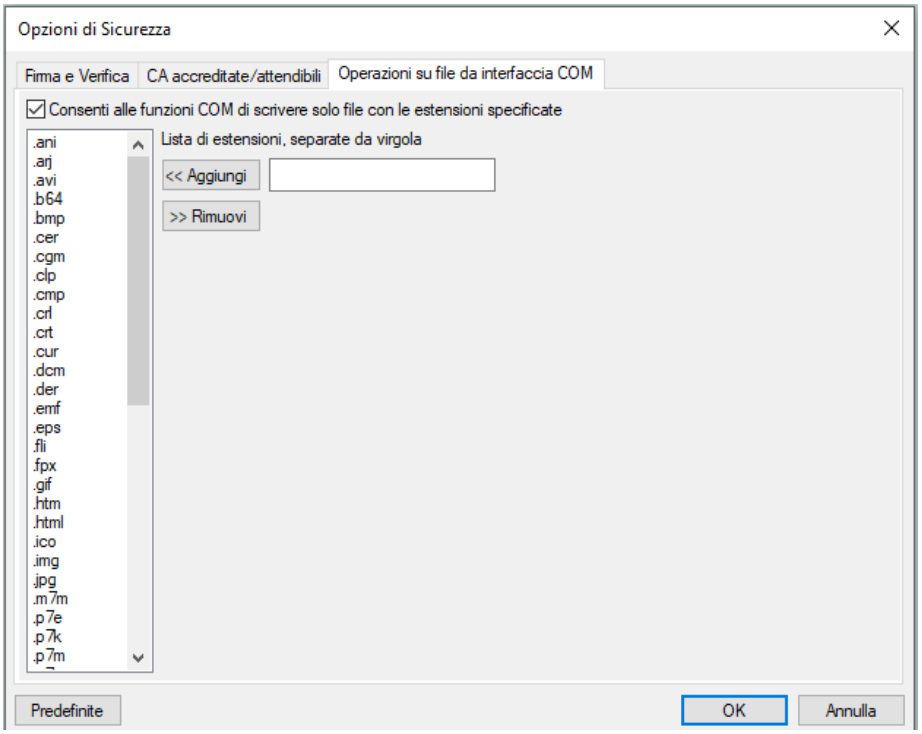
- Il checkbox **Abilita all'uso del DB di CA attendibili**, se selezionato, istruisce ***DigitalSign*** a considerare attendibili i certificati di CA contenuti in tale DB.

- Il checkbox **Scarica certificati indicati da Authority Info Access, se necessario**, agisce in taluni casi di verifiche di certificati esteri (comunque EU). In alcuni paesi europei non tutte le CA elencate

nella TSL di competenza emettono direttamente i certificati di firma degli utenti: talvolta ci sono CA intermedie che poi emettono tali certificati.
Ma poiché solo il certificato root compare in TSL, la verifica del certificato di una firma non è possibile senza disporre di quello intermedio.
Selezionando questo checkbox si autorizza ***DigitalSign***, all'occorrenza, a scaricare il certificato intermedio (indicato dall'attributo Authority Info Access, se presente) e completare la verifica. Il certificato intermedio, comunque, viene eliminato subito dopo l'operazione.

- Il checkbox **Considera attendibili i certificati on-board**, se abilitato, fa sì che i certificati di CA eventualmente contenuti nel dispositivo di firma correntemente inserito siano considerati attendibili anche se non compresi in alcuno degli elenchi sopra descritti. Questa funzione serve prevalentemente a semplificare le attività con firme elettroniche basate su certificati autoprodotti con la Personal Certification Authority, importando i certificati di CA nelle smartcard.

3.8.6.3 Operazioni su file da interfaccia COM



DigitalSign, come è noto, dispone di un'interfaccia (COM) tramite la quale altre applicazioni possono utilizzare i servizi di firma digitale, marcatura temporale, ecc. allo scopo di realizzare sistemi integrati.
Tuttavia, le funzioni di questa interfaccia potrebbero teoricamente essere utilizzate per introdurre nel sistema file eseguibili dannosi, come virus, trojans, e così via.
Questa finestra di dialogo consente di limitare la libertà di azione delle applicazioni client restringendo la loro possibilità di scrivere file.
Per attivare questa opzione di filtro occorre attivare il checkbox e cancellare/inserire le estensioni che si intende autorizzare.

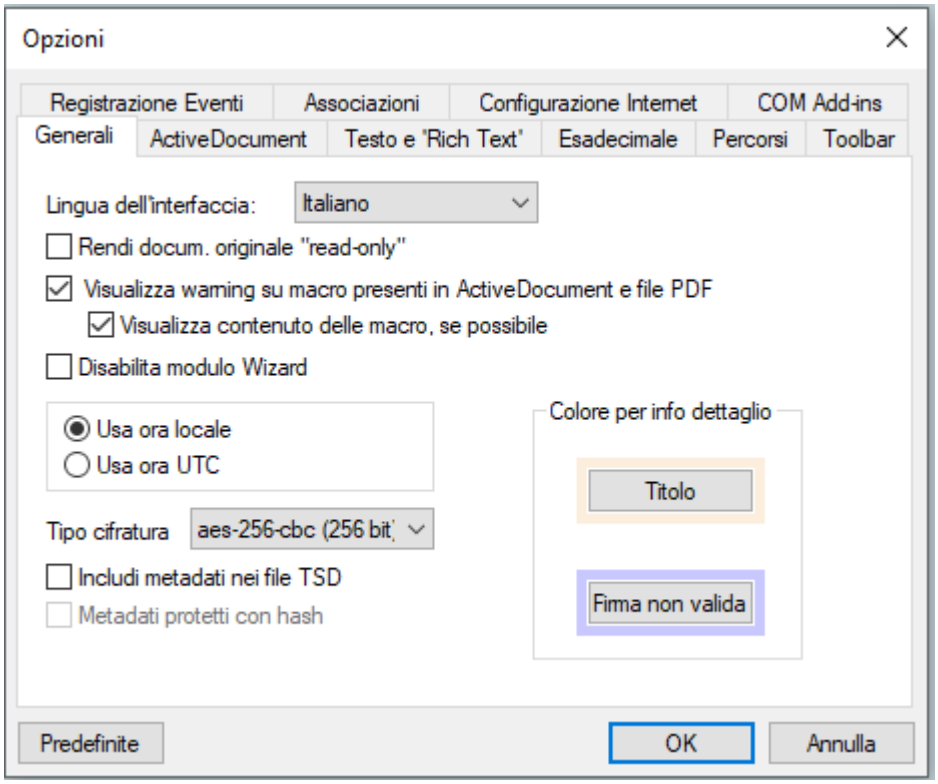
3.8.7 Modulo di Gestione delle Opzioni

Questo modulo di configurazione presenta diverse cartelle per gestire altrettante serie di parametri.
Per tutte le cartelle sono disponibili i seguenti bottoni:

- **Predefinite** – ripristina i valori di default
- **OK** – salva le modifiche e chiude la finestra
- **Annulla** – chiude la finestra senza salvare le modifiche eventualmente apportate

3.8.7.1 Generali

Questa finestra di dialogo consente il controllo di alcuni parametri generali:

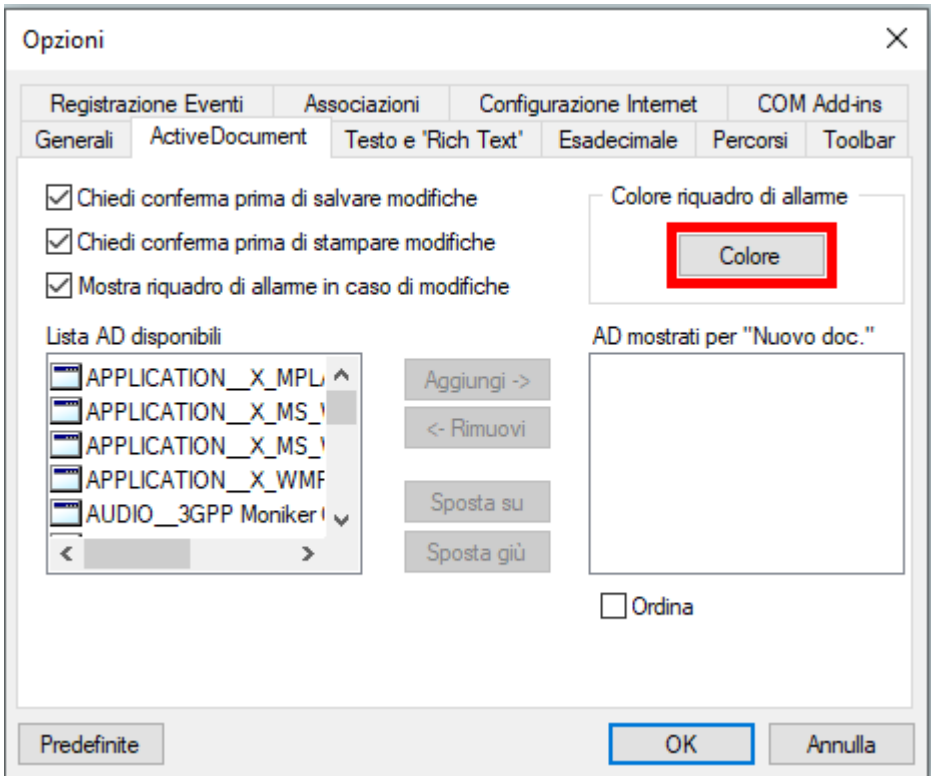


- **Lingua dell'interfaccia** – il selettore consente di scegliere tra Italiano e Inglese; per default viene impostata la lingua italiana, se la lingua del sistema operativo è l'Italiano, altrimenti l'Inglese. L'utente può forzare una delle due lingue attraverso questa opzione.
- **Rendi documento originale *read-only*** - se questo *checkbox* è attivato, i file corrispondenti ai documenti aperti da ***DigitalSign*** non verranno modificati da eventuali operazioni compiute nell'ambito della finestra documento associata (aggiunta o rimozione di firme digitali, di marche temporali, di destinatari di cifratura, ecc.). Occorrerà usare il comando del menu **File -> Salva documento con nome...**
- **Visualizza *warning* su macro presenti in doc. ActiveDocument e PDF -** se questo *checkbox* è attivo ***DigitalSign*** mostrerà, nel pannello dei dettagli della finestra documento, una riga di informazione sul rischio o sull'effettiva presenza di elementi variabili nel documento.
- **Visualizza contenuto delle macro, se possibile** - se questo *checkbox* è attivo (ed è attivo anche quello del punto precedente), nel caso il documento sia in un formato che ***DigitalSign*** è in grado di analizzare, il pannello dettagli della finestra documento mostrerà una lista esplicita delle macro rilevate.
- **Disabilita modulo Wizard** – questo checkbox consente di disabilitare l'avvio automatico del modulo Wizard se il documento PDF caricato contiene un riferimento ad una procedura.
- **Usa ora locale/ora UTC** – questa coppia di *radio button* permette di scegliere se la presentazione di date e ore deve avvenire usando il formato locale o quello UTC.
- **Scelta del tipo di cifratura** – il selettore, per default, mostra l'algoritmo `aes-256-cbc` a 256 bit, ossia una crittografia molto forte; è possibile scegliere altri algoritmi di crittografia del contenuto del documento. Si veda anche la sezione relativa alle modalità di cifratura.
- **Colore per informazioni dettaglio** - l'utente può controllare con questo bottone il colore in cui DigitalSign visualizza nell'area PKCS#7 della finestra documento i campi di informazione relativi a firme digitali la cui verifica non viene superata positivamente.
- **Includi metadati nel file TSD –** quando si appone una marca temporale a un documento già completo, si possono usare diverse modalità di salvataggio dei file: mantenere documento e marca separati (modalità "detached") oppure riunirli in un unico file mediante lo standard RFC5544 (documento in formato **.tsd**). Nel secondo caso lo standard permette di includere alcuni metadati standard.
- **Metadati protetti con hash –** questo checkbox, nel caso sia selezionato il precedente, istruisce DigitalSign a considerare i metadati nel calcolo dell'hash oggetto di marcatura temporale.

Scegliendo questa opzione, tuttavia, non sarà possibile convertire il documento all'altra modalità. Rinunciando ai metadati sarà possibile salvare il documento '.tsd' anche nel formato detached.

3.8.7.2 ActiveDocument

Questa finestra consente di controllare alcuni parametri relativi al comportamento di DigitalSign nella manipolazione di documenti aperti in una finestra documento tramite un viewer di tipo **ActiveDocument**.



NOTA IMPORTANTE: questa è da considerarsi una funzionalità "legacy", perché progettata in passato per l'utilizzo con i prodotti Microsoft Office 2003.
Le successive edizioni di Office hanno introdotto formati diversi per i documenti, per i quali non è più disponibile la proprietà **ActiveDocument**.

Tre *checkbox* controllano il comportamento in presenza di modifiche apportate durante l'editing:

- **Chiedi conferma prima di salvare modifiche**
- **Chiedi conferma prima di stampare modifiche** – riguarda l'esecuzione di stampe di documenti modificati dopo l'apertura
- **Mostra riquadro di allarme in caso di modifiche** – se questo checkbox è attivo, in caso il documento venga modificato in fase di editing evidentemente le firme digitali preesistenti non saranno più valide; un riquadro lampeggiante di allarme informerà l'utente di questa circostanza. Un bottone **colore riquadro allarme** permette di configurare il "look" del riquadro di allarme di cui al punto precedente.

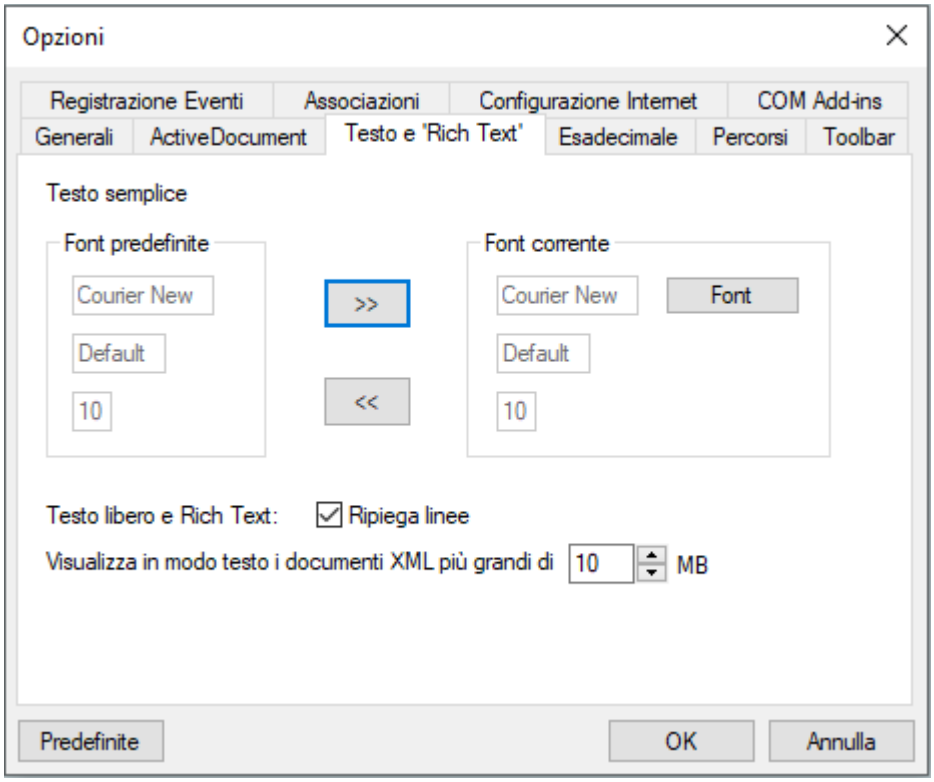
Nella parte bassa della finestra compaiono due riquadri tramite i quali è possibile configurare il sistema su quali applicazioni compatibili **ActiveDocument**, tra quelle installate nel sistema, sia possibile usare con ***DigitalSign***.
Il riquadro di sinistra mostra tutte le applicazioni ActiveDocument ancora disponibili, quello di destra mostra quali applicazioni sono già state abilitate all'uso come viewer ActiveDocument per ***DigitalSign***.

- Il bottone **Aggiungi** provoca il passaggio dell'applicazione correntemente selezionata nel riquadro di sinistra verso quello di destra (ossia inserimento tra le applicazioni abilitate)
- Il bottone **Rimuovi** provoca il passaggio dell'applicazione correntemente selezionata nel riquadro di sinistra verso quello di destra (ossia rimozione dalle applicazioni abilitate).
- Il bottone **Sposta su** provoca lo spostamento di una posizione verso l'alto dell'applicazione correntemente selezionata nel riquadro di destra.

- Il bottone **Sposta giù** provoca lo spostamento di una posizione verso il basso dell'applicazione correntemente selezionata nel riquadro di destra.

3.8.7.3 Testo e "Rich Text"

Questa finestra di dialogo controlla alcuni parametri relativi al comportamento del *viewer* per documenti di puro testo e per documenti *rich text.*

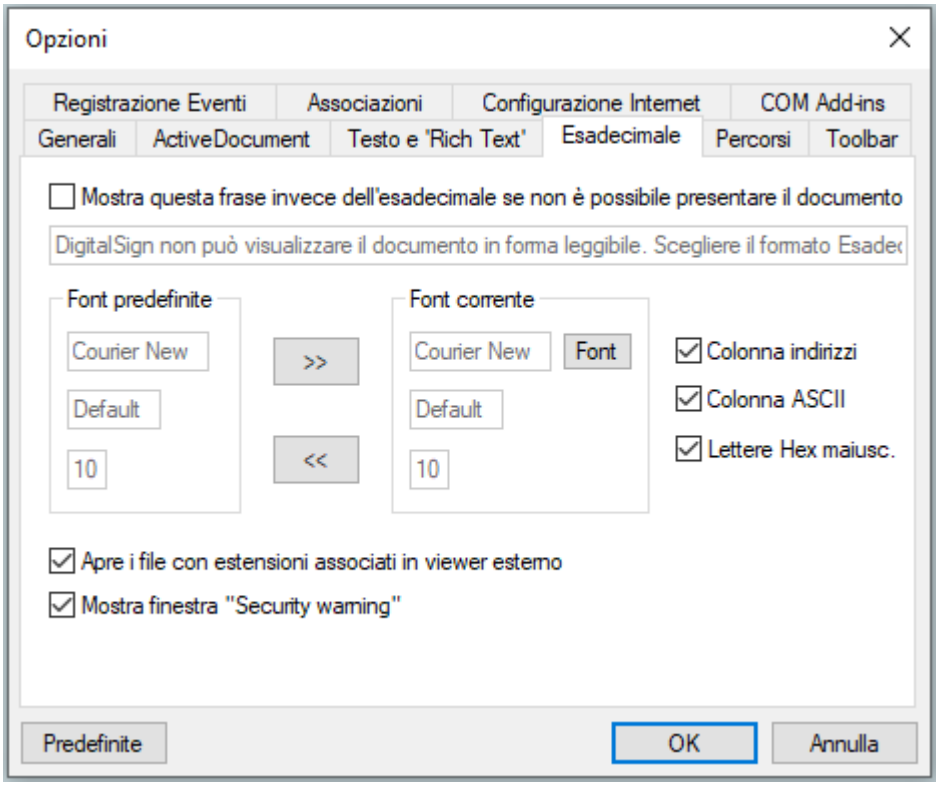


Due aree della finestra consentono di specificare un particolare font da utilizzare per la rappresentazione dei documenti di puro testo.
Il Font corrente è quello utilizzato per il documento correntemente aperto, il font di default è quello che verrà utilizzato per tutti i documenti di questo tipo.

- Tramite il bottone **[<<]** il font di default assume una configurazione identica a quella del font corrente.
- Tramite il bottone **[>>]** il font corrente viene riconfigurato in accordo con il font di default.
- Il *checkbox* **ripiega linee**, se attivo, istruisce DigitalSign a tagliare automaticamente le lunghe linee di testo che superano la larghezza della finestra e a riportarle su una linea successiva. Se il flag non è attivo l'utente dovrà agire sulla scroll-bar orizzontale per visualizzare tali linee lunghe.
- Il controllo **Visualizza in modo testo i documenti XML più grandi di <*x*> MB** serve a contrastare un limite di Internet Explorer (il *viewer* di default per i documenti XML) che provoca un abnorme consumo di memoria ed un conseguente progressivo decadimento delle prestazioni al crescere delle dimensioni dei documenti. Per ovviare a questo fenomeno ***DigitalSign*** limita l'uso di tale *viewer* ai file di dimensione contenuta, mostrando invece in formato di testo semplice quelli più grandi della soglia prefissata.

3.8.7.4 Esadecimale

Questa finestra di dialogo controlla alcuni parametri relativi al comportamento del *viewer* per dati binari di ***DigitalSign:***



Il *checkbox* **Mostra questa frase invece dell'esadecimale**, se attivo, fa sì che il viewer riporti semplicemente una frase informativa sull'impossibilità di manipolare il documento tramite un viewer specifico. Se il *checkbox* è disabilitato ***DigitalSign*** procede invece direttamente con la visualizzazione dei dati in formato esadecimale.
La frase specifica è impostabile dall'utente tramite l'*edit-box* sottostante.

Due riquadri sottostanti consentono di controllare il font da impiegare per la visualizzazione: Il font corrente è quello utilizzato per il documento correntemente aperto, il font predefinito è quello che verrà utilizzato per tutti i documenti di questo tipo.

- Tramite il bottone **[<<]** il font di default assume una configurazione identica a quella del font corrente.
- Tramite il bottone **[>>]** il font corrente viene riconfigurato in accordo con il font di default.

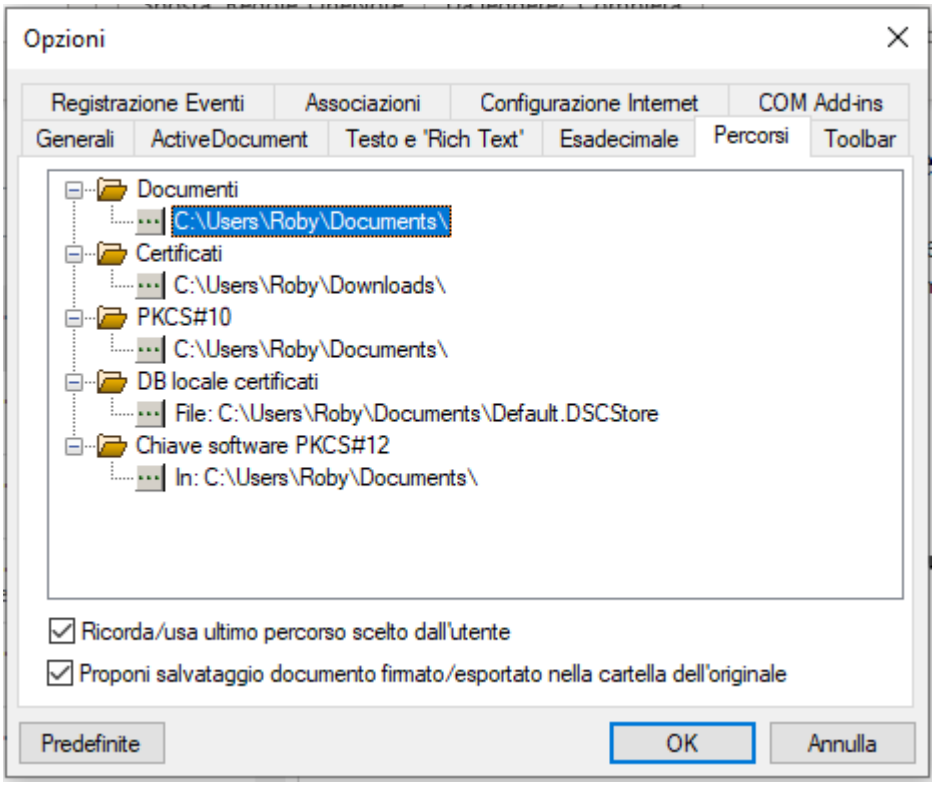
Tre *checkbox* consentono di abilitare o disabilitare individualmente la visualizzazione, rispettivamente, della **colonna degli indirizzi** (offset), della **colonna ASCII**, l'utilizzo delle **lettere maiuscole** nella presentazione dei dati esadecimali.

Il checkbox **Apre i file con estensioni registrate con l'applicazione predefinita**, se attivo, autorizza ***DigitalSign*** a mostrare i file con estensioni registrate presso il sistema operativo con l'applicazione associata, usata come viewer esterno. Se il checkbox è inattivo, invece, si utilizzerà la visualizzazione esadecimale.

Il checkbox **Mostra security warning**, se attivo, istruisce ***DigitalSign*** a mostrare, prima dell'attivazione di un viewer esterno, una schermata di avvertimento sul ridotto livello di sicurezza offerto da un viewer di questo tipo.

3.8.7.5 Percorsi

Questa finestra di dialogo consente di controllare le posizioni di default in cui ***DigitalSign*** colloca i file di diverso tipo.



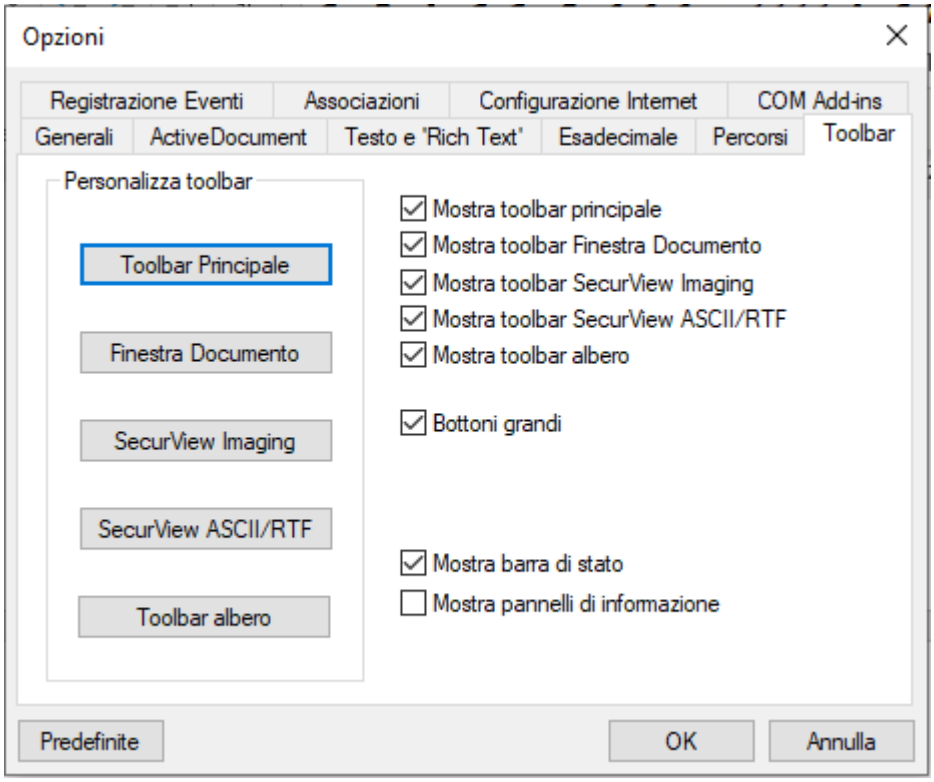
La finestra mostra alcuni elementi, corrispondenti ai diversi tipi di file a cui ***DigitalSign*** deve accedere: Documenti, Certificati, richieste PKCS#10, DB locale dei certificati, coppie di chiavi software in formato PKCS#12.

Per ognuna di queste tipologie è mostrato un percorso; normalmente il sistema aggiorna autonomamente questi valori, secondo le operazioni svolte o per effetto dell'esecuzione di varie operazioni. Ma agendo sul bottone … di ciascun percorso è possibile impostare manualmente un percorso specifico.

- Il *checkbox* **Ricorda/Usa ultimo percorso scelto dall'utente**, se attivo, fa sì che il percorso effettivamente scelto dall'utente in una delle operazioni menzionate, venga salvato come percorso di default per le successive operazioni dello stesso tipo.
- Il *checkbox* **Proponi salvataggio documento firmato/esportato nella cartella dell'originale**, se attivo, fa sì che il documento risultante da un'operazione di firma/export finisca – per default – nella stessa cartella di provenienza dell'originale.

3.8.7.6 Toolbar

Questa finestra di dialogo consente di personalizzare le barre strumenti (toolbar) che ***DigitalSign*** presenta nelle diverse situazioni.



Sul lato destro della finestra sono elencati alcuni *checkbox* per controllare se ***DigitalSign*** debba o meno mostrare toolbar specifiche:

- **Mostra Toolbar principale** (quella mostrata inizialmente da DigitalSign anche quando nessuna finestra documento è aperta)
- **Mostra Finestra documento** (la toolbar specifica delle funzioni di DigitalSign mostrata all'interno di ogni finestra documento)
- **Mostra Securview Imaging** (quella associata al viewer per immagini raster)
- **Mostra Securview ASCII/RTF** (quella associata al viewer per documenti di puro testo e al viewer RTF)
- **Mostra Toolbar Albero** (quella verticale che appare sul separatore tra il pannello proprietà della busta crittografica e l'area dettagli della finestra documento)

Altri *checkbox* controllano il comportamento di ***DigitalSign*** relativamente alle toolbar:

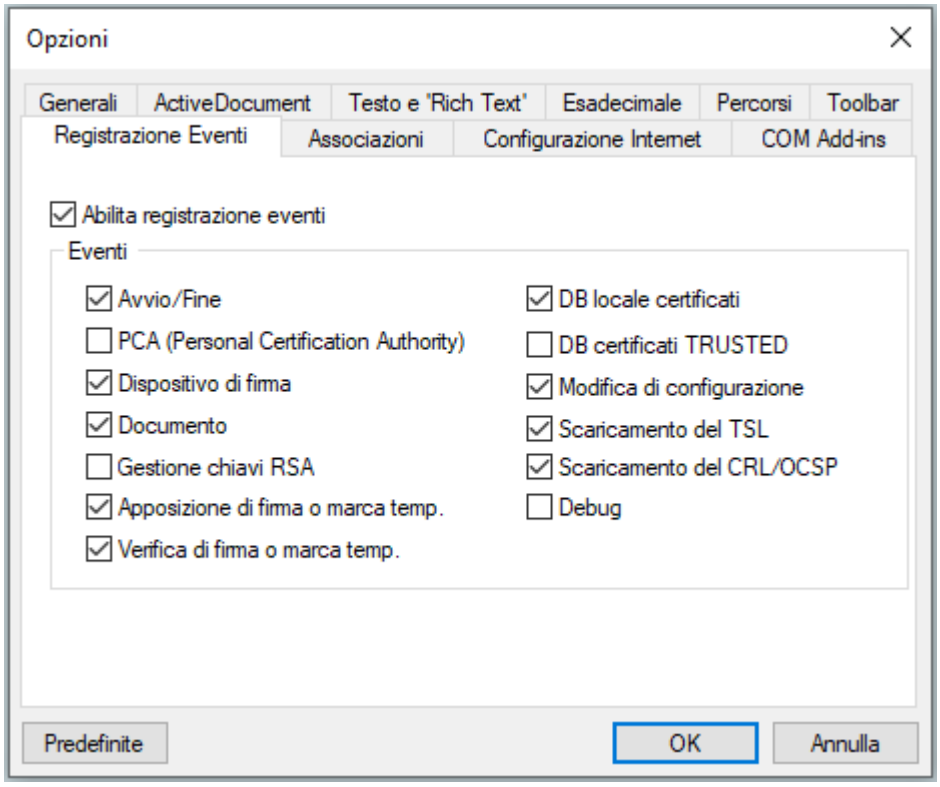
- **Bottoni grandi** - consente di controllare la dimensione dei bottoni delle toolbar
- **Mostra barra di stato** - controlla la visualizzazione della barra di stato in fondo alla finestra principale.
- **Mostra pannelli di informazione** - abilita o disabilita la visualizzazione dei pannelli informativi

Alcuni bottoni di comando permettono di personalizzare il contenuto delle diverse toolbar attraverso una specifica finestra di dialogo:

- **Toolbar principale** (quella mostrata inizialmente da ***DigitalSign*** anche quando nessuna finestra documento è aperta)
- **Finestra documento** (la toolbar specifica delle funzioni di ***DigitalSign*** mostrata all'interno di ogni finestra documento)
- **Securview Imaging** (quella associata al viewer per immagini raster)
- **Securview ASCII/RTF** (quella associata al viewer per documenti di puro testo e al viewer RTF)
- **Toolbar Albero** (quella verticale che appare sul separatore tra il pannello proprietà PKCS#7 e l'area dettagli della finestra documento)

3.8.7.7 Registrazione Eventi

Questa finestra di dialogo permette all'utente di attivare/disattivare la registrazione degli eventi e, nel caso tale funzione sia attivata, di controllare quali categorie di eventi includere nella registrazione.



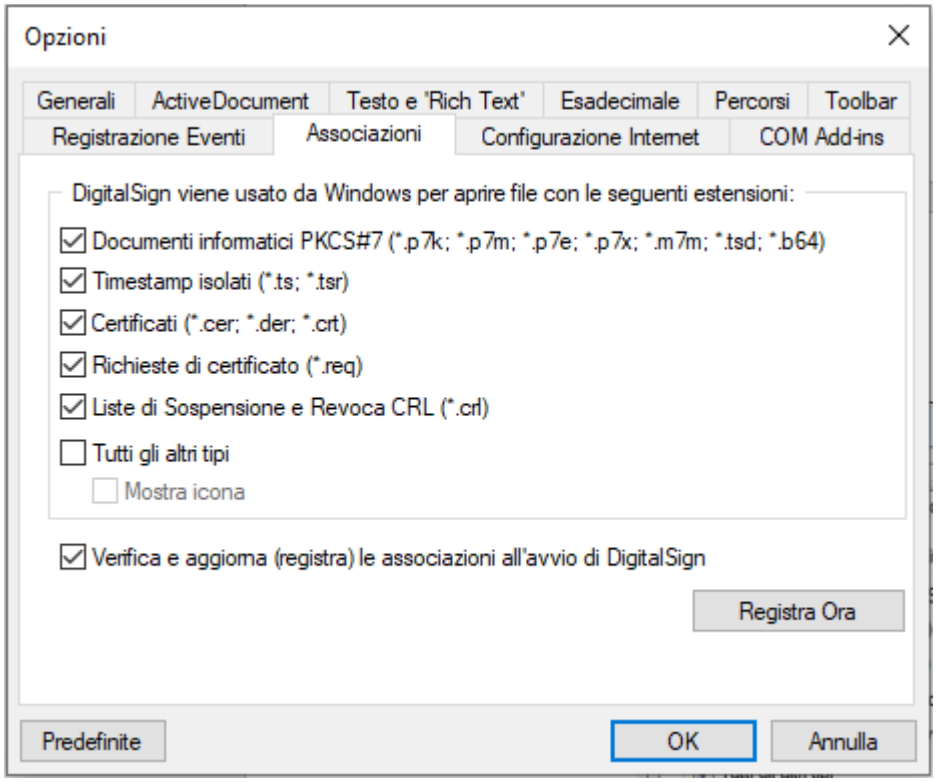
Il *checkbox* **Abilita registrazione eventi**, se attivo, fa sì che gli eventi significativi dell'attività di DigitalSign vengano effettivamente registrati.

Il riquadro sottostante, accessibile se il *checkbox* di abilitazione è attivo, consente di includere o escludere dalla registrazione le varie categorie di eventi disponibili.

NOTA: la categoria **Debug** merita particolare attenzione: se attivata provoca la scrittura di registrazioni molto dettagliate, soprattutto in materia di interfacciamento con le smartcard. L'effetto collaterale è che l'esecuzione rallenta significativamente, quindi va attivato solo in caso di necessità per analizzare situazioni problematiche.

3.8.7.8 Associazioni

Questa finestra di dialogo consente di configurare le modalità secondo cui Windows fa uso di ***DigitalSign*** per gestire i file dei tipi compatibili con ***DigitalSign*** stesso:



Il primo riquadro permette di controllare le associazioni vere e proprie di ***DigitalSign*** ai file con le diverse estensioni specifiche. Questo significa che, agendo con doppio click (da Windows) su un file appartenente ad uno dei tipi selezionati, l'apertura avverrà per default con ***DigitalSign***.

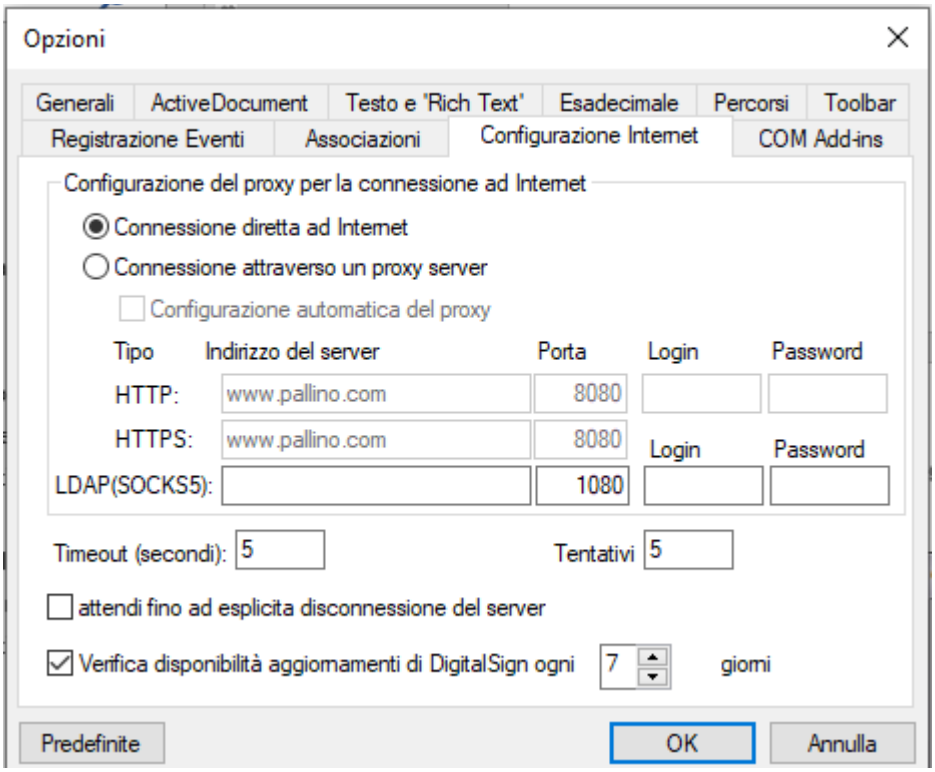
Esiste poi l'opzione **Tutti gli altri tipi**: quando questa è selezionata, se da una finestra di Windows Explorer si fa click con il tasto destro su un file di tipo generico, comparirà nel menu di apertura anche un **Apri con *DigitalSign***.
Se poi è attiva anche l'opzione **Mostra icona**: il menu presenterà anche la tipica icona di ***DigitalSign***.
Se l'operazione con il tasto destro viene effettuata a livello di una cartella invece che di un singolo file, si attiverà il meccanismo firma semiautomatica di file contenuti in una cartella dalla *shell* di Windows.

Fuori dal riquadro si trova un altro checkbox, **Verifica e registra all'avvio di DigitalSign:** se questo è attivo ***DigitalSign*** riesegue ad ogni avvio la configurazione a livello di registro di sistema per tutte le associazioni qui configurate (utile nel caso in cui altre applicazioni, nel frattempo, avessero modificato la configurazione)

Esiste un bottone di comando specifico, **Registra ora**, che provoca la registrazione immediata in Windows della configurazione appena completata.

3.8.7.9 Configurazione Internet

Questa finestra di dialogo consente di configurare la modalità in cui ***DigitalSign*** deve accedere ad Internet, per le operazioni che lo richiedono (marcatura temporale, scaricamento degli elenchi autenticati di certificati accreditati/attendibili, consultazione delle CRL, ...):



I *radio button* del primo riquadro consentono di scegliere tra una connessione diretta (nel caso di configurazioni di rete relativamente libere) o attraverso un *proxy* aziendale.
Nel secondo caso la scelta di operare una configurazione automatica (che eredita la configurazione di Internet Explorer) risolve la gran parte delle situazioni.

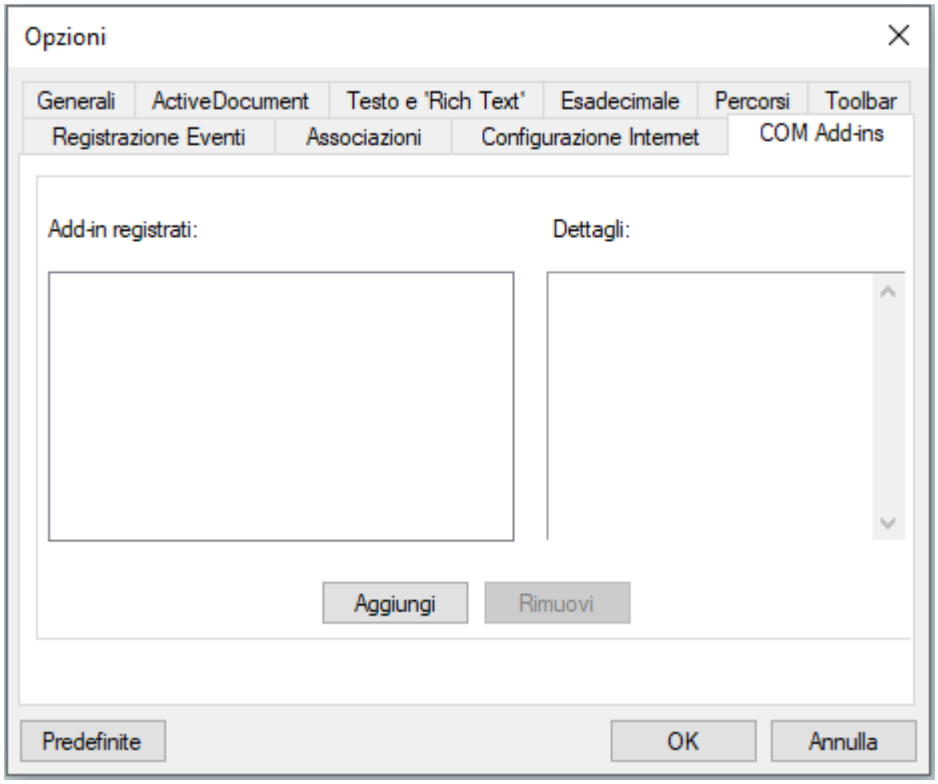
NOTA: l'eventuale configurazione del proxy ha effetto solo sulle connessioni via http e https, non sulle connessioni in LDAP.

Ove fosse necessario configurare parametri specifici, incluse le credenziali di accesso, può essere utile rivolgersi all'amministratore di sistema.

L'ultimo *checkbox* **Verifica disponibilità aggiornamenti di DigitalSign ogni <x> giorni** consente di mantenere aggiornata la propria installazione, tramite un accesso al server di CompEd.

3.8.7.10 COM Add-Ins

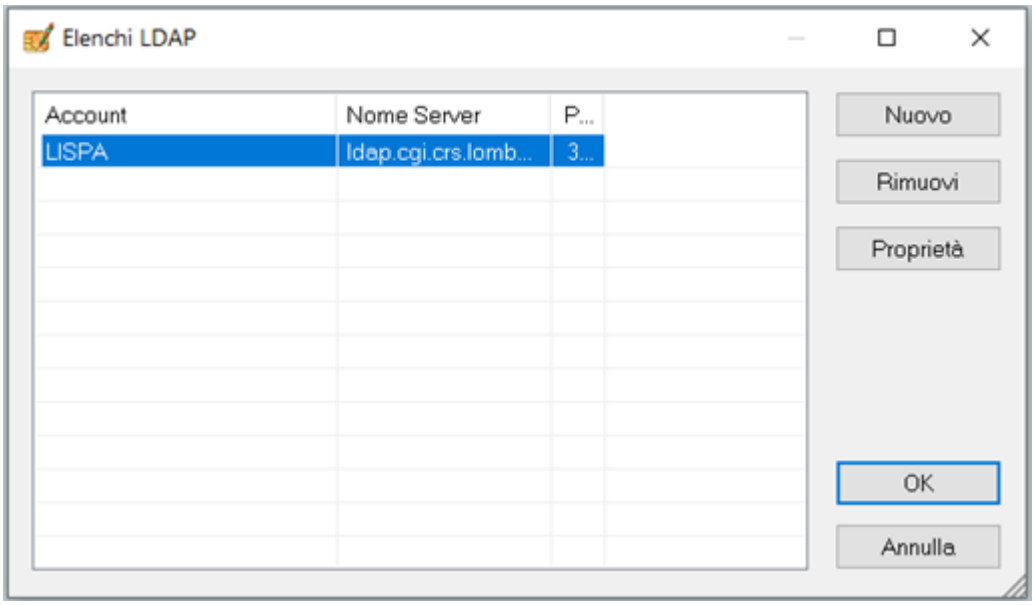
Questo pannello serve alla gestione di moduli Add-In per ***DigitalSign***.
In generale la presenta può presentarsi vuota oppure contenere la lista degli Add-in correntemente installati:



- Con il bottone **Aggiungi** è possibile installare un nuovo Add-in (si faccia riferimento alla documentazione specifica dell'add-in che si intende installare)
- Con il bottone **Rimuovi** si opera la disinstallazione dell'add-in selezionato dalla lista

3.8.8 Modulo di Configurazione dei servizi di accesso agli elenchi di certificati LDAP

Questa finestra di dialogo consente di configurare i servizi di consultazione degli elenchi di certificati in linea.



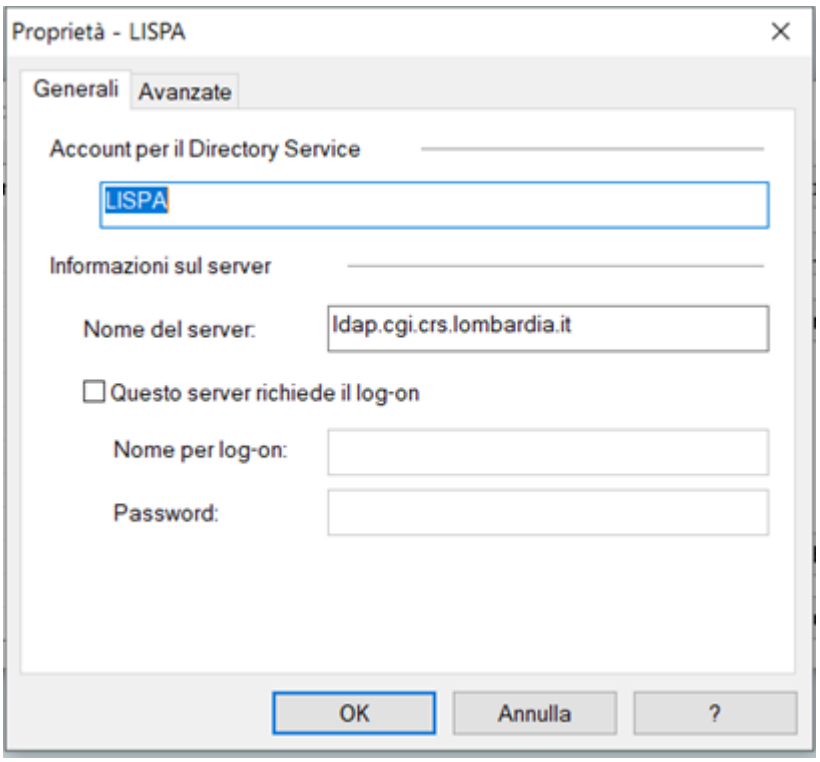
È possibile inserire diversi servizi, che corrispondono ad altrettanti server LDAP, in generale uno per ogni certificatore ritenuto di interesse.

- Il bottone **Nuovo** crea una nuova entry e conduce alla finestra di dialogo per la compilazione dei relativi parametri.
- Il bottone **Rimuovi** elimina il servizio selezionato
- Il bottone **Proprietà** conduce alla finestra di dialogo per la revisione dei parametri relativi al servizio selezionato

- Il bottone **OK** salva le modifiche apportate e chiude la finestra
- Il bottone **Annulla** chiude la finestra senza salvare le eventuali modifiche.

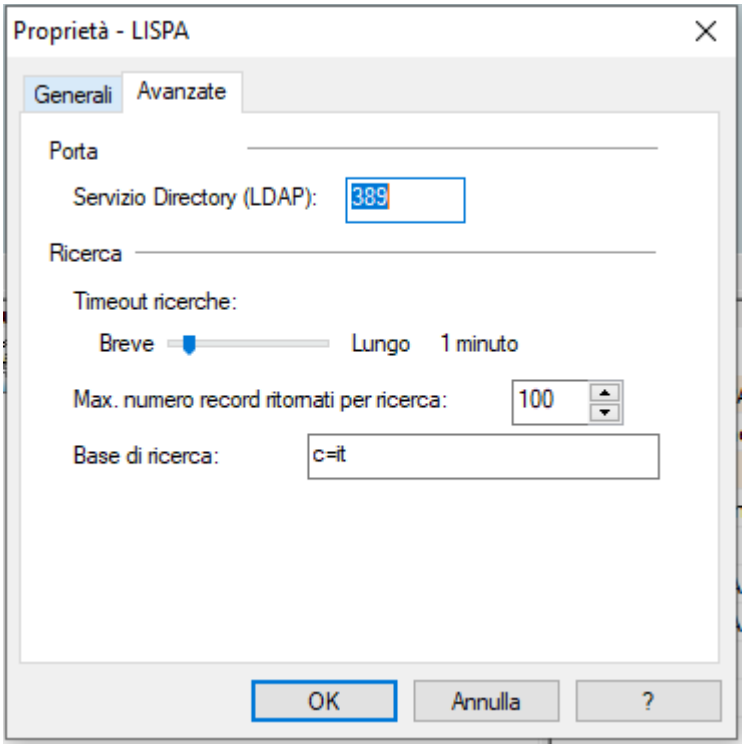
3.8.8.1 Finestra di configurazione di un servizio LDAP

Questa finestra di dialogo è in effetti organizzata in due distinte cartelle, la prima delle quali è **Generali**:



- Il **Nome Simbolico (Account per il Directory Service)** è un nome arbitrario deciso dall'utente un significato locale, per distinguere i vari servizi attivi in ***DigitalSign***. Tipicamente si usa il nome del certificatore che gestisce il server.
- Il **Nome del server** è in pratica l'indirizzo Internet a cui il server risponde. Questa informazione è pubblicata dal certificatore che gestisce ogni servizio
- Il *checkbox* **Questo server richiede logon** va attivato se il server in oggetto richiede che l'utente sia preventivamente registrato ed in tal caso occorre fornire anche il **nominativo** e la **password** necessari per l'accesso

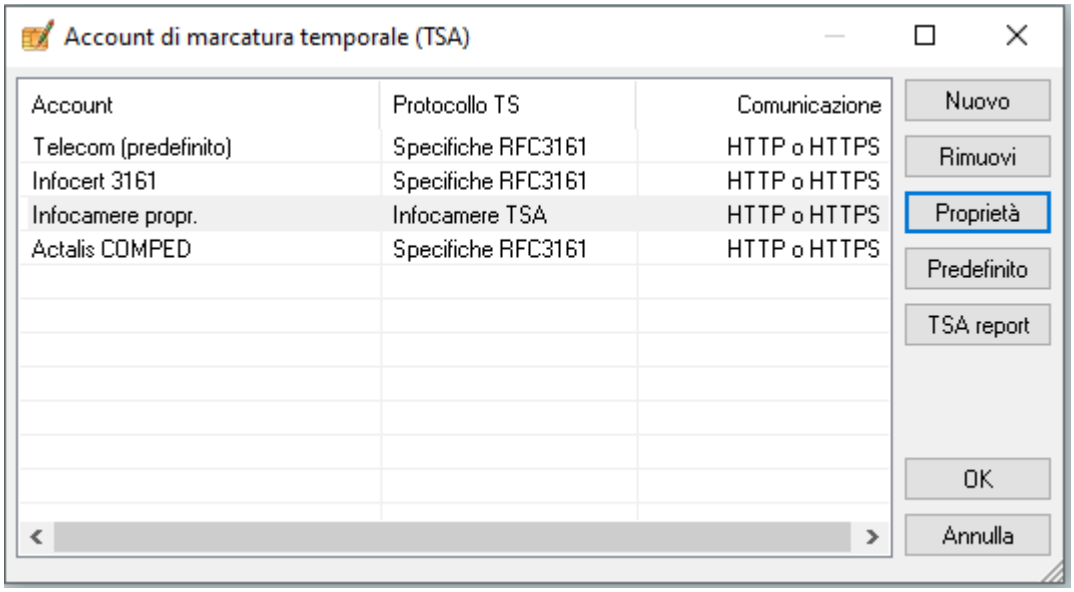
La cartella **Avanzate** si presenta come segue:



- Il **Servizio Directory** è in effetti il numero di porta, un parametro specifico del server. Il valore 389 è usato di norma da tutti i server LDAP, ma in casi particolari può essere necessario un valore diverso (consultare il gestore)
- Il **Timeout ricerche** indica il tempo massimo durante il quale ***DigitalSign*** attenderà una risposta prima di considerare la ricerca fallita. Si agisce spostando il cursore a destra o sinistra per allungare o abbreviare l'intervallo
- Il **Massimo numero record ritornati per ricerca** limita il flusso di informazioni trasferite nel caso si introduca una chiave di ricerca troppo ampia, soddisfatta da molti record. Da notare che molti server limitano comunque il numero di record ritornati
- La **Base di Ricerca** è una stringa usata per limitare la ricerca a record di una specifica categoria. I server gestiti dai certificatori accreditati AgID di norma esigono che la base di ricerca sia "**c=it**", altrimenti non ritornano alcun risultato.

3.8.9 Modulo di Configurazione dei servizi di Marcatura Temporale

Questo modulo permette di visualizzare, aggiungere od eliminare gli account di marcatura temporale utilizzabili.
DigitalSign consente di interagire con diversi *provider* di servizi di marcatura temporale, l'utente deve creare e configurare un *account* per ogni fornitore che intende utilizzare.
La schermata mostrata in figura visualizza tutti gli account correntemente configurati:



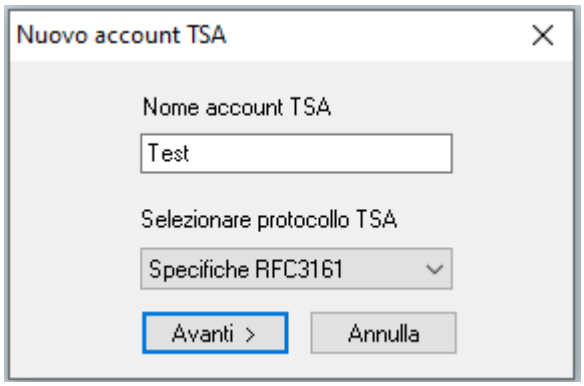
- Con il bottone **Nuovo** si passa all'inserimento di un nuovo account, per mezzo di una ulteriore finestra di dialogo
- Con il bottone **Rimuovi** è possibile eliminare l'account selezionato
- Il bottone **Proprietà** mostra le caratteristiche dell'account selezionato, con la possibilità di modificarle per mezzo di una ulteriore finestra di dialogo
- Il bottone **Predefinito** permette di indicare l'account selezionato come quello predefinito da utilizzare con tutti i comandi di marcatura temporale. Il bottone non è accessibile se l'account selezionato è già il predefinito (oppure l'unico disponibile). L'account attualmente predefinito viene indicato nella lista.
- Il bottone **TSA report** consente – per i servizi che supportano tale funzione, attualmente soltanto Infocamere – di ottenere un rapporto sul credito di marche temprale residuo (solo per gli account che supportano tale opzione)

- Il bottone **OK** chiude la finestra registrando le modifiche eventualmente apportare.
- Il bottone **Annulla** chiude la finestra senza salvare le modifiche.

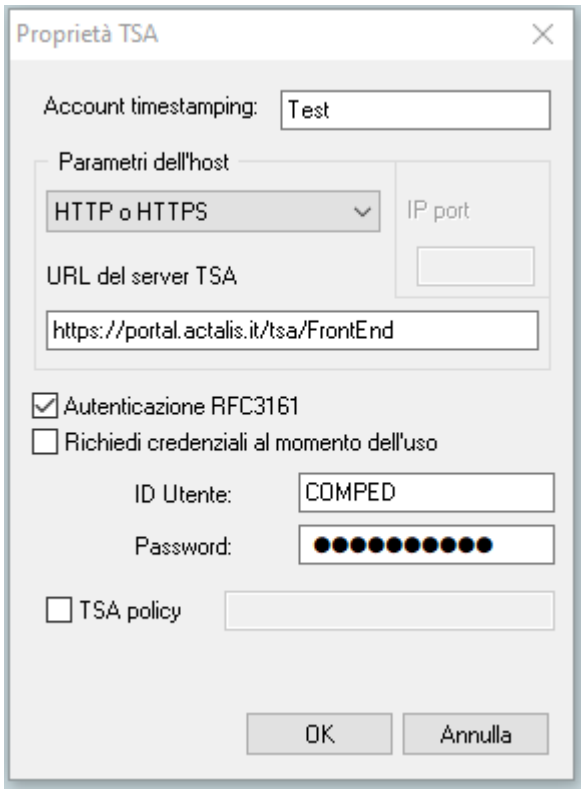
3.8.9.1 Finestra di configurazione per un account di Marcatura Temporale

Quando si richiede la creazione di un nuovo account di Marcatura Temporale occorre innanzitutto assegnare un nome all'account e scegliere il "protocollo".

Oggi tutti i certificatori devono erogare il servizio in modalità standard RFC3161, ma il sistema ancora supporta alcuni protocolli proprietari.



Al passo successivo (o in fase modifica) si passa direttamente ad intervenire sui dettagli:

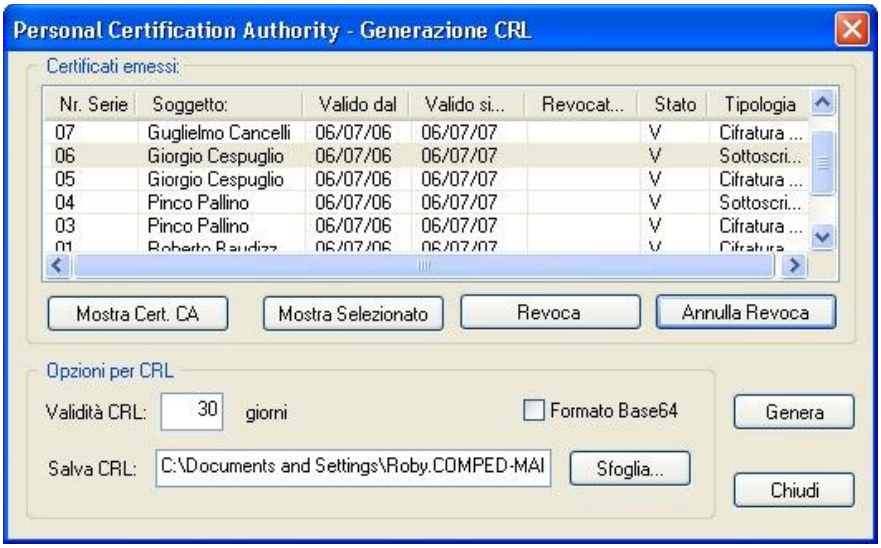


In generale si utilizzeranno i parametri di default: protocollo http o https e autenticazione RFC3161 attiva, in modo da poter fornire le credenziali di accesso.
Per compilare gli altri parametri, ove necessari, occorrono le indicazioni del provider.

3.8.10 Modulo per la generazione di una CRL

Questo modulo funzionale, appartenente alla Personal Certification Authority, consente di produrre una lista di revoca da utilizzare per la verifica di certificati prodotti appunto tramite la PCA.

La finestra di gestione, accessibile solo se è inserita – ed in stato di logon – una smartcard contenente un certificato di CA, si presenta come in figura:

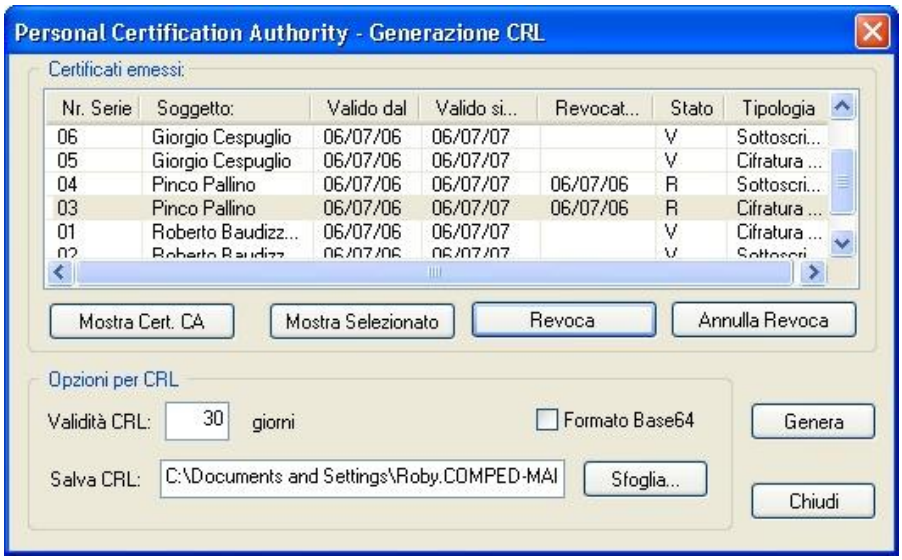


La tabella mostra tutti i certificati attualmente contenuti nel DB locale generati con il certificato di CA contenuto nel dispositivo di firma correntemente inserito.

La tabella contiene le seguenti colonne:

- numero di serie del certificato
- nominativo del titolare del certificato
- inizio validità nominale
- termine validità nominale
- data dell'eventuale sospensione/revoca
- indicatore dello stato del certificato (R=Revocato, V=Valido)

La prima volta che si accede a questo modulo la tabella mostrerà tutti i certificati in stato di validità; quando si accederà a questa funzione in seguito, dopo aver generato una lista contenente almeno un certificato in stato di revoca, la tabella continuerà a mostrare lo stato imposto in precedenza (naturalmente le informazioni vengono prelevate dall'ultima CRL caricata nel DB locale), per cui si potranno aggiornare i dati e quindi creare una nuova copia aggiornata della CRL
Si veda l'esempio corrispondente a due certificati revocati:



Alcuni bottoni comando situati sotto la tabella consentono di operare sulla tabella stessa:

- **Mostra Certificato di CA -** visualizza il certificato corrispondente alla chiave di certificazione contenuta nel dispositivo di firma per il quale si sta costruendo la CRL
- **Mostra selezionato** - mostra il certificato correntemente selezionato nella tabella
- **Revoca -** cambia lo stato del certificato selezionato
- **Annulla revoca** - ripristina lo stato di *attivo* per il certificato selezionato

Un altro riquadro consente di configurare alcune opzioni per la produzione del file che rappresenta la CRL:

- **Periodo di validità CRL <x> giorni**: tale termine viene registrato all'interno della CRL, così che in fase di consultazione sia possibile verificare se la lista è ancora attuale oppure se è obsoleta
- **Salva CRL**: l'utente deve dichiarare un nome per il file completo di percorso, eventualmente utilizzando il bottone **Sfoglia**
- **Formato Base64**: attivando questo checkbox la lista verrà esportata in tale formato

Il bottone **Genera** provoca la creazione della CRL, che conterrà i riferimenti a tutti i certificati che nella tabella riportano lo stato di revocato o sospeso. La lista verrà anche caricata nel database locale dei certificati, dal quale potrà poi essere gestita mediante l'apposito modulo di gestione.

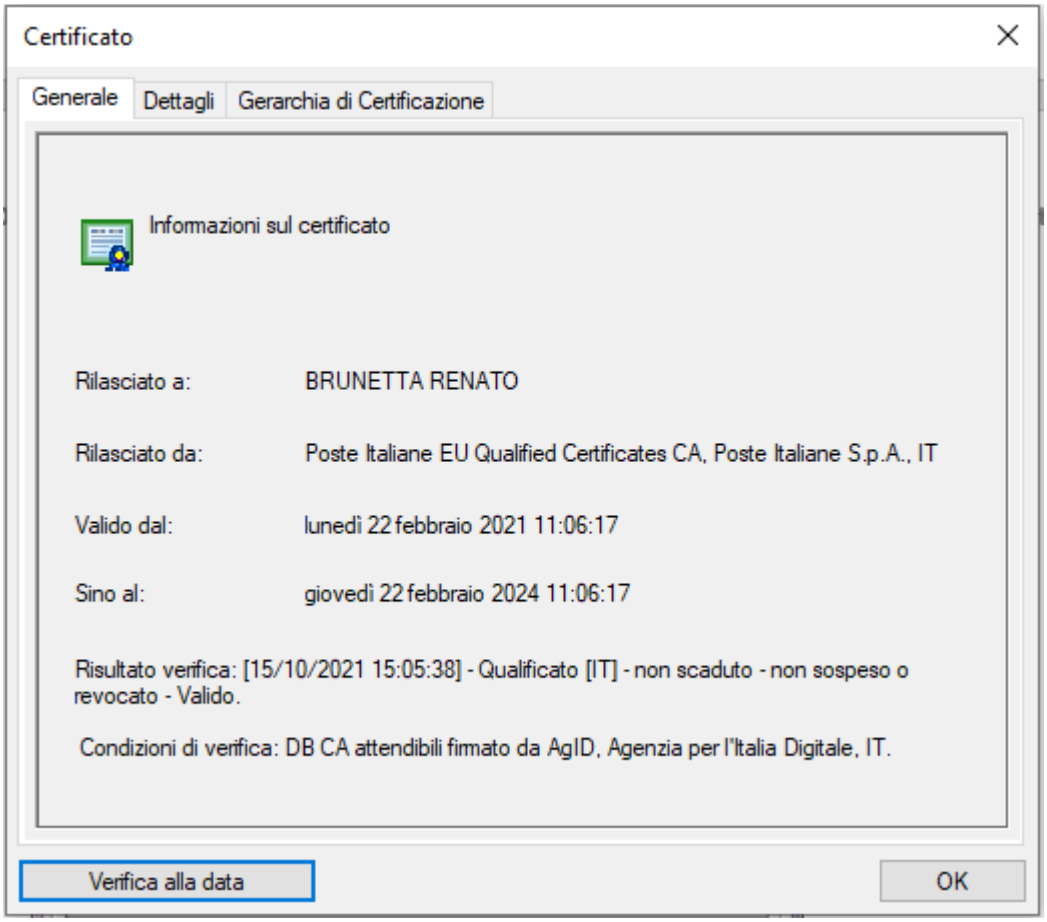
Si noti che per mettere in esercizio la CRL prodotta è necessario che essa venga poi resa accessibile alla URL scritta in tutti i certificati prodotti dalla CA in questione, cioè quello che si trova esplicitato nel file .INI, si vedano i dettagli a proposito della Personal Certification Authority.

Naturalmente è necessario ripetere questa operazione prima di ogni scadenza della validità della CRL, evitando che gli utenti trovino alla URL predefinita una CRL scaduta.

3.8.11 Modulo di visualizzazione di un Certificato

Questo viewer viene utilizzato per presentare il contenuto di un certificato o di una richiesta di certificato. Nel caso del certificato, in generale, la visualizzazione è organizzata in tre distinte cartelle:

Generale

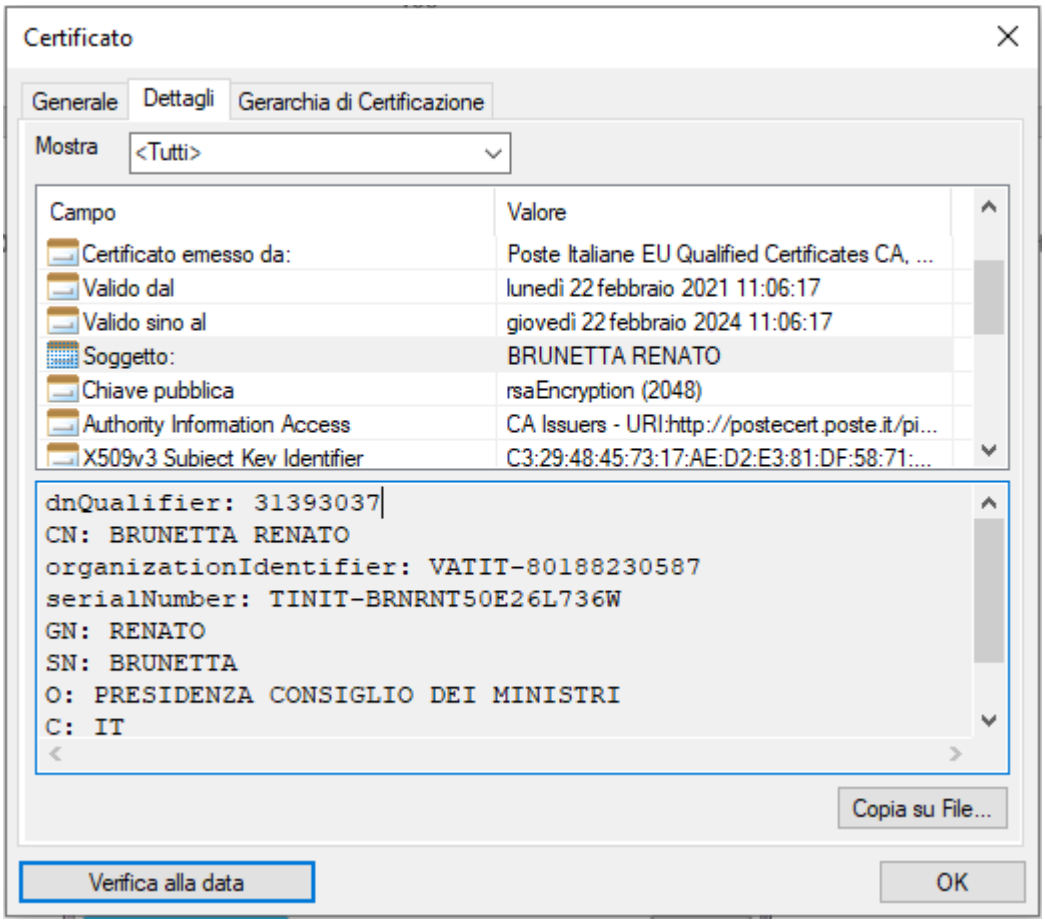


Le informazioni mostrate in questa finestra (che mostra un certificato estratto da un DPCM pubblicato su un sito istituzionale) sono:

- **Rilasciato a -** il titolare del certificato e quindi della relativa coppia di chiavi
- **Rilasciato da -** il fornitore di servizi di certificazione che lo ha rilasciato (eventualmente un organo interno all'organizzazione, qualora si operi mediante la Personal Certification Authority)
- **Valido dal -** l'inizio del periodo di validità, corrispondente al momento del rilascio
- **Sino al -** termine del periodo di validità, imposto dal Certificatore
- **Risultato Verifica -** lo stato di validità del certificato, in termini di verifica della relativa firma. Il caso più normale, come quello in figura, riporta la verifica superata positivamente, il fatto che il certificato in esame è stato emesso da una CA accreditata (presso AgID), il fatto che non sia sottoposto a revoca o sospensione.
- **Condizioni di verifica -** indica sommariamente la fonte di attendibilità in uso per il certificato: in questo caso la lista firmata da AgID.

Il bottone **Verifica alla data** consente di effettuare la verifica rispetto ad una data specifica, per verificare se il certificato era valido o meno (rispetto a scadenza o revoca).

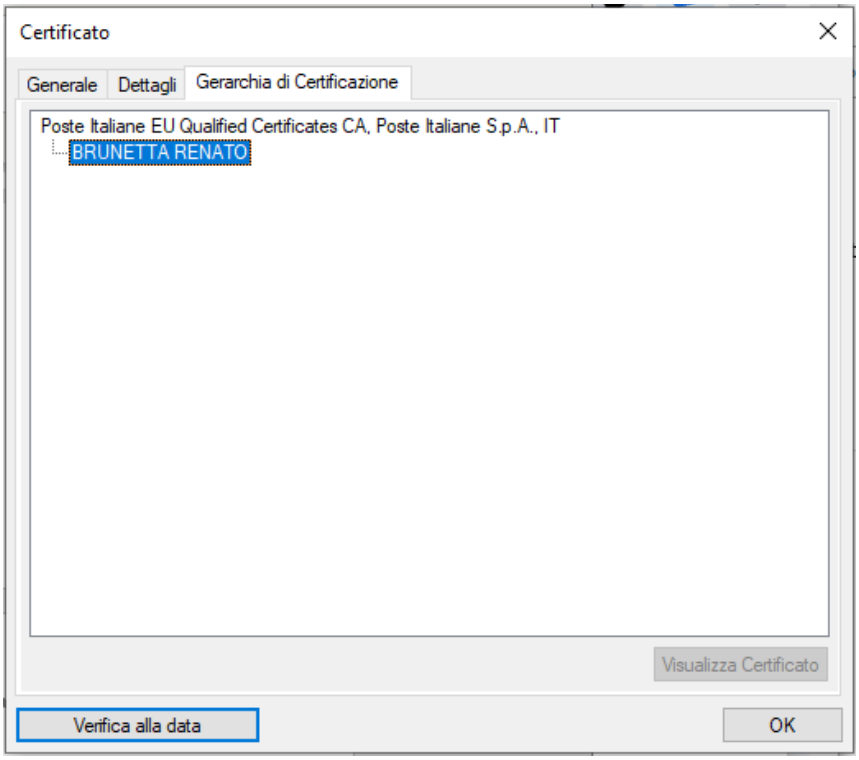
Dettagli



La finestra presenta in alto un campo con etichetta **Mostra** che permette di scegliere se la visualizzazione deve riguardare tutte le informazioni (per default) oppure le sole "proprietà".
Il riquadro sottostante contiene una tabella di entry, ciascuna delle quali rappresenta un campo del certificato ed il relativo valore. Poiché alcuni valori (per esempio la chiave pubblica) sono troppo grandi per essere contenuti nella colonna destra della tabella, la finestra contiene un ulteriore riquadro nel quale vengono riportate per esteso le informazioni contenute nel campo del certificato correntemente selezionato.

Il bottone **Copia su file** permette di esportare il certificato su un file (.CER) in formato X.509 (DER encoded) scelto dall'utente.

Gerarchia di Certificazione



Questa schermata mostra visivamente la catena di certificazione di un certificato di chiave pubblica.

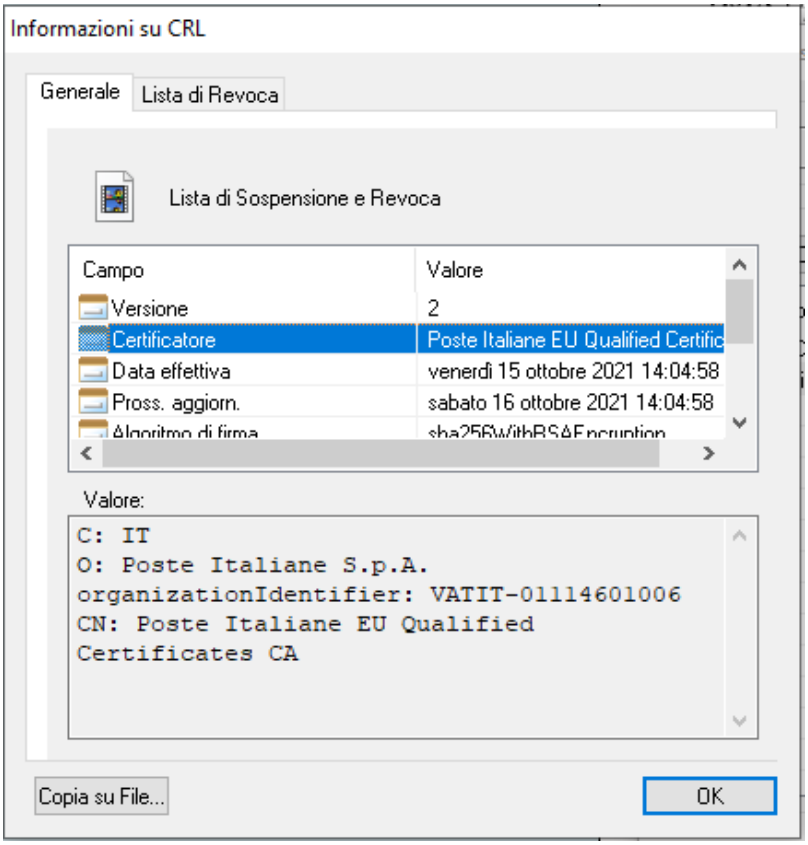
Ogni certificato deve infatti essere firmato digitalmente dalla Certification Authority che lo emette, il cui certificato deve a sua volta essere disponibile per la verifica e potrebbe a sua volta essere stato emesso da un altro soggetto di livello più elevato.
Si risale così una catena sino al raggiungimento di un certificato di livello root, firmato da se stesso.

Lo schema dell'infrastruttura italiana per i certificati qualificati prevede solo due livelli, come in figura.

Selezionando il certificato del livello superiore diventa disponibile il bottone **Visualizza Certificato**, che consente di esaminare il certificato della CA emittente.

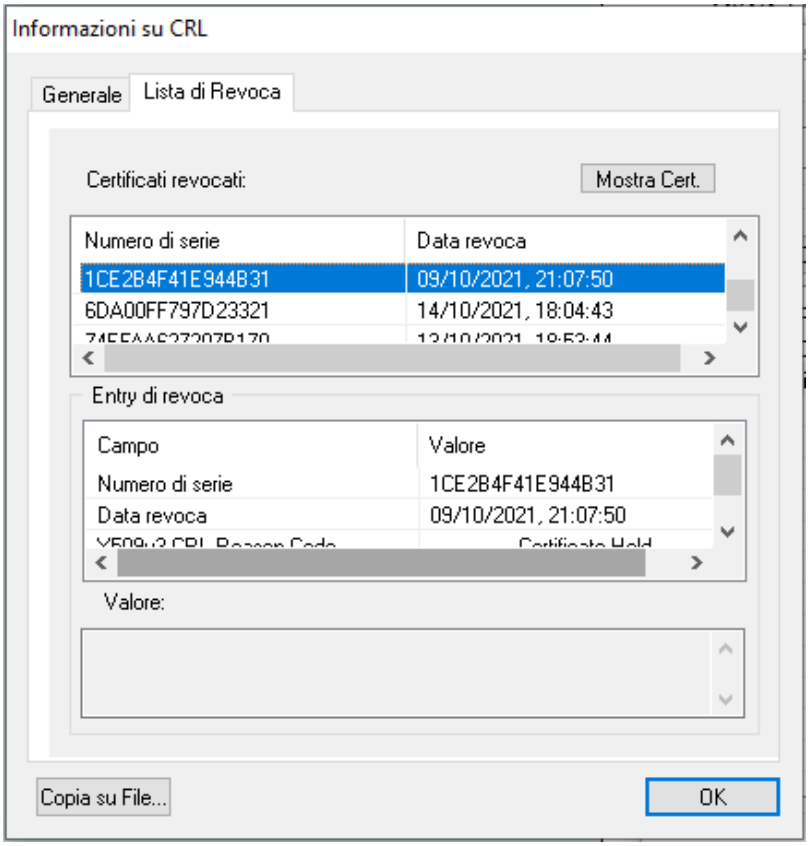
3.8.12 Modulo di visualizzazione di una Lista di Sospensione o Revoca

Questa finestra è organizzata in due cartelle, la prima della quale mostra le informazioni generali relative alla lista di revoca:



La tabella del primo riquadro mostra tutti gli elementi fondamentali della CRL, in particolare il nominativo della Certification Authority che l'ha emessa, la data effettiva di emissione, la data pianificata dal Certificatore per l'emissione del prossimo aggiornamento.
Il riquadro inferiore mostra gli eventuali dettagli disponibili per l'elemento del primo riquadro correntemente selezionato

La seconda cartella mostra invece il contenuto effettivo della lista:



Si noti che una CRL contiene unicamente i numeri di serie come riferimenti ai certificati veri e propri, non contiene i certificati completi. Quindi è possibile sapere, dato un certificato, se esso è incluso nella lista (ricercandone il numero di serie), ma non è possibile conoscere le identità dei titolari di tutti i certificati revocati semplicemente disponendo della lista.

Tuttavia, se nel DB locale è presente un certificato corrispondente alla entry correntemente selezionata, il bottone **Mostra Certificato** lo apre per la visualizzazione.

Il riquadro superiore contiene la lista effettiva: una tabella le cui colonne rappresentano, rispettivamente, i numeri di serie dei certificati e la data/ora di sospensione o revoca.

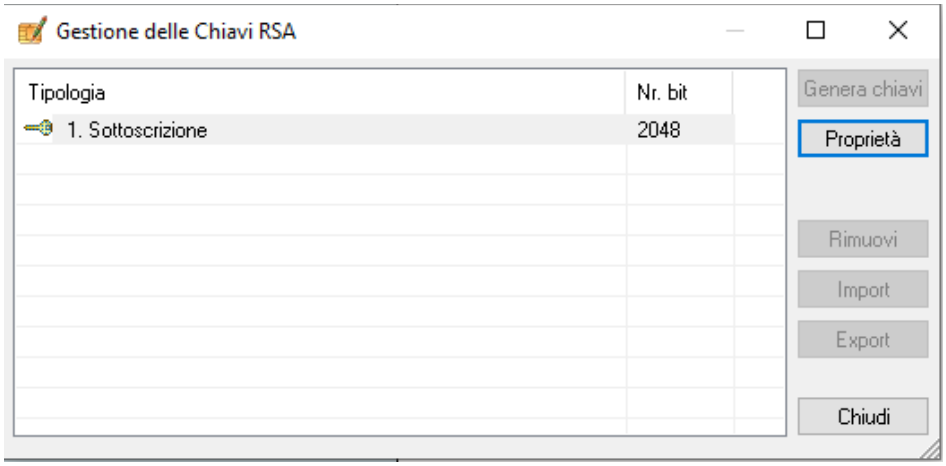
Il riquadro **Entry di revoca** mostra tutti i dettagli relativi alla riga della tabella superiore correntemente selezionata; numero di serie del certificato, data e ora della sospensione o revoca, il codice e descrizione dell'operazione impostato dal certificatore per quel certificato.

Il riquadro **Valore** mostra una ulteriore espansione del dettaglio correntemente selezionato nel riquadro delle entry di revoca.

Da entrambe le cartelle, con il bottone **Copia su File** è possibile esportare la CRL su un file esterno, con **OK** si chiude la finestra.

3.8.13 Modulo di gestione delle coppie di chiavi RSA

Questo modulo consente di operare sull'insieme di coppie di chiavi presenti in un dispositivo di firma:



La tabella mostra una riga per ogni coppia di chiavi disponibile nel dispositivo.

Per ognuna delle coppie di chiavi vengono visualizzate le seguenti informazioni:

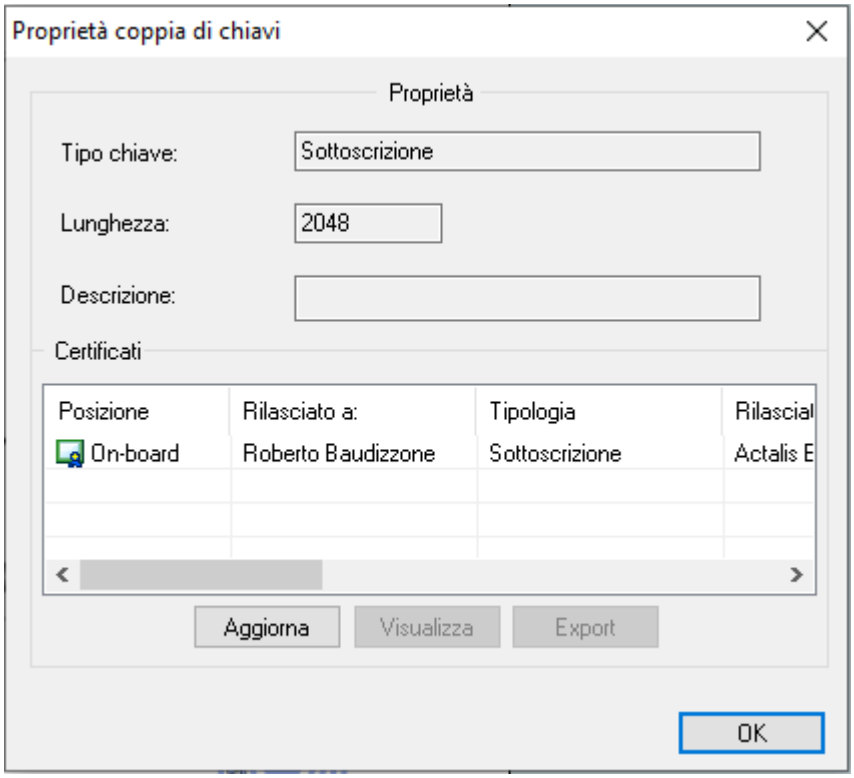
- l'icona che rappresenta la tipologia
- la tipologia in esteso
- l'eventuale identificatore della procedura automatica (solo per le coppie di chiavi di sottoscrizione mediante procedura automatica): questa colonna è mantenuta per compatibilità con dispositivi di firma personalizzati con vecchie edizioni di ***DigitalSign***
- la lunghezza delle chiavi, espressa in bit

Sono disponibili alcuni bottoni comando:

- **Genera chiavi -** conduce ad una finestra di dialogo che assiste alla creazione di una nuova coppia di chiavi. Questo comando è abilitato solo se si opera con un dispositivo che effettivamente consente la generazione.
- **Proprietà –** conduce ad una ulteriore finestra di dialogo che illustra proprietà di dettaglio della coppia di chiavi selezionata.
- **Import -** consente di importare da un file in formato PKCS#12 una coppia di chiavi di cifratura. In pratica è una operazione di *restore*, mentre l'export è assimilabile ad una operazione di *backup.*
  In generale questa funzione può non essere disponibile con le smartcard fornite dai Certificatori accreditati.
- **Export -** consente di esportare su un file in formato PKCS#12 una coppia di chiavi da utilizzare per la cifratura dei documenti (si noti che l'esportazione di una chiave privata per la firma digitale sarebbe del tutto illegale). Lo scopo di questa operazione è quello di eseguire un backup (definito *key recovery*) al fine di non perdere la possibilità di decifrare documenti crittografati in caso di perdita o distruzione del dispositivo di firma che contiene le relative chiavi.
  In generale questa funzione può non essere disponibile con le smartcard fornite dai Certificatori accreditati.
- **Chiudi** - chiude la finestra di dialogo

3.8.13.1 Proprietà di una coppia di chiavi

Viene mostrata una finestra di questo tipo:

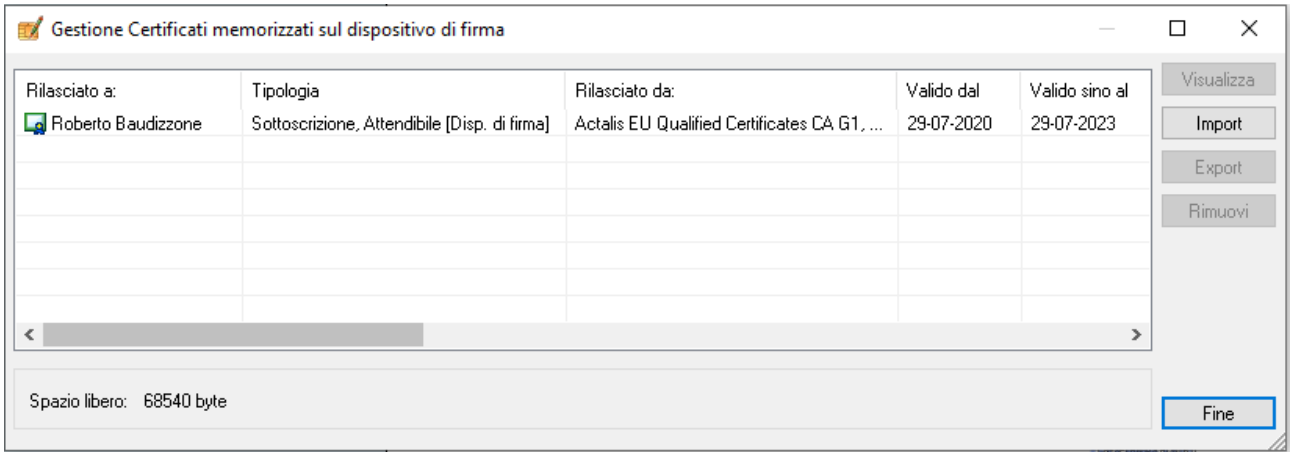


La tabella della finestra mostra il certificato o i certificati presenti nel sistema e che corrispondono alla coppia di chiavi.

- il bottone **Aggiorna** ripete la scansione degli archivi di ***DigitalSign*** alla ricerca dei certificati
- **Visualizza** apre la visualizzazione del certificato selezionato
- **Export** consente di esportare su un file esterno una copia del certificato selezionato

3.8.14 Modulo di Gestione dei Certificati 'on-board'

Questo modulo consente di esplorare i certificati contenuti a bordo del dispositivo di firma correntemente inserito.



Sono disponibili i seguenti bottoni comando:

- **Visualizza** - per visualizzare il contenuto del certificato, tramite l'apposito visualizzatore (4.8.9)
- **Import** - per caricare nel dispositivo un certificato disponibile su file. L'effettiva disponibilità di questa funzione dipende dalla configurazione del particolare dispositivo
- **Export** - per esportare su un file esterno il certificato correntemente selezionato

- **Rimuovi** - per cancellare dalla memoria della smartcard il certificato selezionato. L'effettiva disponibilità di questa funzione dipende dalla configurazione del particolare dispositivo.

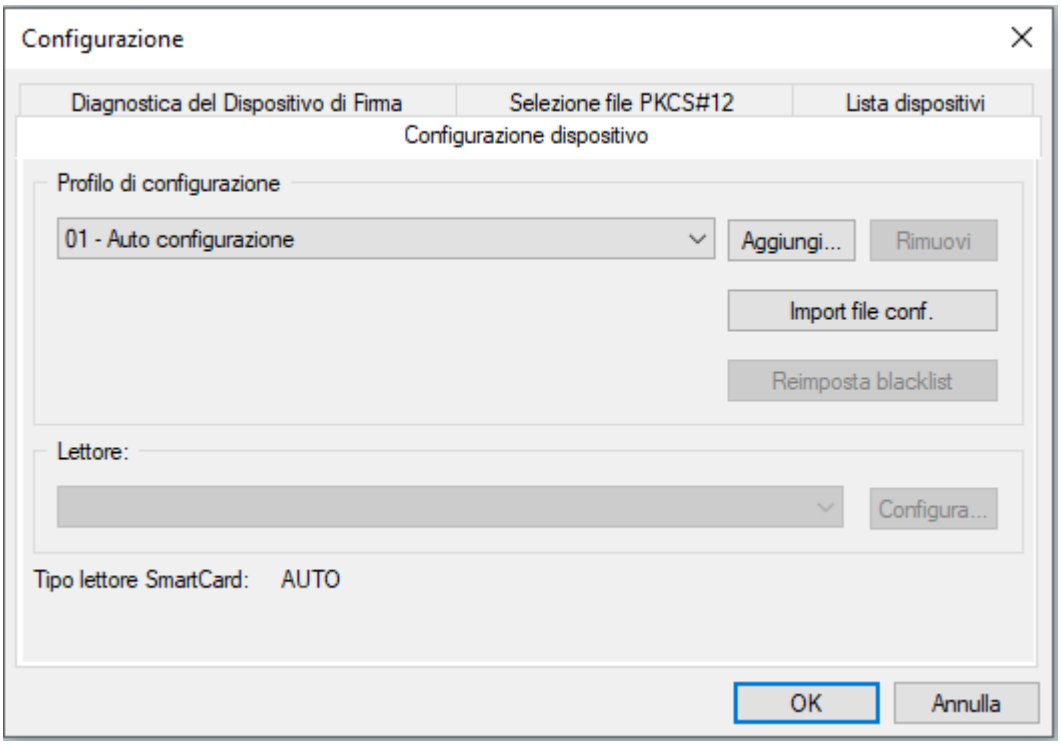
3.8.15 Modulo di Gestione della Configurazione del Dispositivo di Firma

DigitalSign può operare con una grande varietà di dispositivi di firma, a patto che siano correttamente interfacciati.
La gran parte delle smartcard e delle chiavette USB disponibili sul mercato – soprattutto quelli rilasciati dai Certificatori Accreditati AgID – viene interfacciata attraverso lo standard PKCS#11: ***DigitalSign*** deve collegarsi ad un modulo PKCS#11 (in ambiente Windows si tratta di una DLL) progettato per la particolare tipologia di smartcard che si intende usare.

Ovviamente l'utente può scegliere la DLL da impiegare e collegarla manualmente, ma in generale si sfrutterà la capacità di ***DigitalSign*** di trovare e collegare automaticamente la DLL appropriata.

3.8.15.1 Auto-configurazione

Avendo a che fare con una smartcard già pronta all'uso, contenente chiavi e certificati, il modo più semplice di procedere è quello di attuare la configurazione automatica.



In questa modalità l'utente non deve fare nulla, ma solo lasciare che ***DigitalSign*** risolva automaticamente il problema della configurazione.

Questo si ottiene impostando il profilo di configurazione **Auto configurazione**, come nella figura riportata qui sopra.

NOTA: è opportuno spendere qualche minuto per descrivere come funziona il meccanismo di riconoscimento automatico del dispositivo di firma.

Ogni serie smartcard o chiavetta USB (si noti che sono dispositivi molto simili: la chiavetta è un lettore di smartcard di formato particolare, al cui interno è montata una smartcard nel formato SIM) presenta un caratteristico codice ATR *(Answer To Reset)*; quando il chip della carta viene alimentato (o resettato), esso trasmette sul canale di comunicazione, attraverso il lettore, una specifica stringa di byte, denominata appunto ATR.

Il distributore di ogni carta (in generale un Certificatore, o un partner tecnico del Certificatore), quando adotta una certa tipologia di smartcard, mette anche a disposizione un modulo PKCS#11 in grado di far funzionare quelle smartcard.

DigitalSign opera con due tabelle:

i. **una lista di ATR di smartcard** – CompEd, nel tempo, incorpora in ***DigitalSign*** i codici ATR di tutte le smartcard di cui ha notizia, insieme al nome del modulo PKCS#11 appropriato per interfacciare ogni carta.
Questa lista è "cablata" all'interno del codice di ***DigitalSign***, anche se – all'occorrenza – l'utente ha facoltà di estenderla o sostituirla con una propria lista, si veda la sezione dedicata;

ii. **una lista di moduli PKCS#11** – questa tabella (scritta nel file devices.ini) contiene i nomi simbolici dei moduli PKCS#11 conosciuti e i nomi dei file (DLL) che li implementano; anche questa lista può essere estesa manualmente dall'utente, si veda la sezione dedicata;

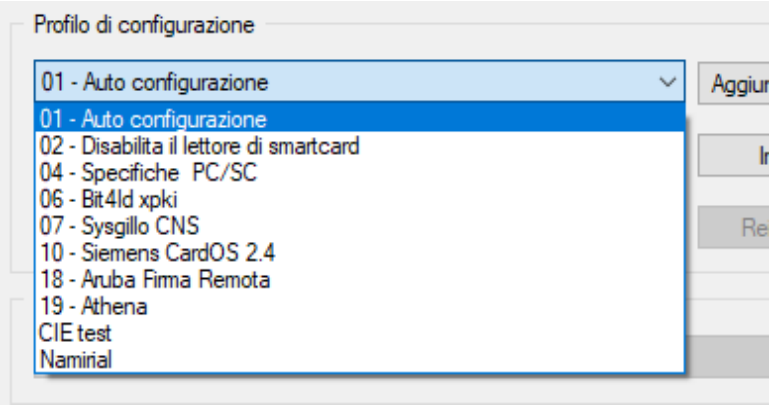
Quindi, all'inserimento di una nuova carta, ***DigitalSign***:

1) rileva il codice ATR della carta;
2) cerca, nella tabella degli ATR, il nome del modulo PKCS#11 da impiegare per quella tipologia di carta;
3) cerca, nel file devices.ini, la DLL corrispondente al modulo PKCS#11 così individuato;
4) se la DLL è presente viene collegata e le operazioni possono iniziare.

Se qualcosa va storto in questa sequenza (ad esempio se l'ATR è sconosciuto, se il modulo preassegnato non è installato sul computer, ecc.), allora ***DigitalSign*** tenta di montare, ciclicamente, tutti i moduli PKCS#11 trovati sul computer e a usarli per eseguire alcune operazioni sull'area pubblica della carta. E, infine, se almeno uno fornisce risultati positivi, monta quello.
Si noti che questa strategia di ripiego non necessariamente va a buon fine: l'accoppiamento di una carta con un modulo PKCS#11 può funzionare correttamente riguardo alla lettura di certificati dall'area pubblica, ma potrebbe non funzionare al momento di generare una firma (e lo si scopre solo al momento di tentare una firma). In caso di difficoltà occorre studiare la diagnostica del dispositivo.
Si veda anche l'appendice dedicata al troubleshooting.

3.8.15.2 Configurazione manuale

Se il modulo di configurazione automatica non riesce ad associare correttamente la smartcard a disposizione con un modulo PKCS#11 tra quelli installati nel sistema (può essere il caso di dispositivi diversi da quelli distrbuiti dai certificatori, di moduli PKCS#11 non reperibili nelle cartelle coperte dal PATH di sistema, oppure un servizio di Firma Remota) è possibile eseguire la configurazione manuale, forzando ***DigitalSign*** a colloquiare con il dispositivo utilizzando una modalità ben determinata ed uno specifico lettore.



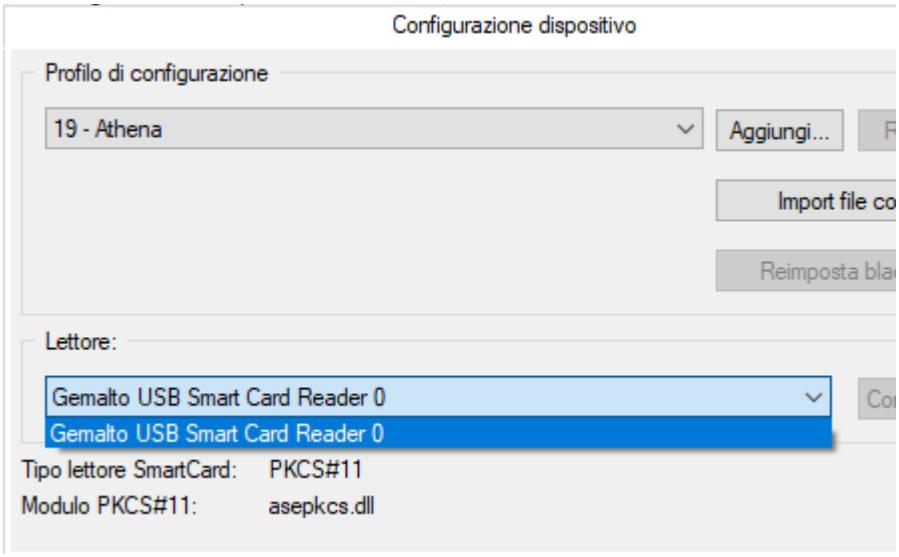
Innanzitutto, occorre scegliere il modulo da impiegare, dalla lista completa di tutte le opzioni disponibili (cioè i moduli effettivamente installati sul computer).

Si noti che i primi elementi della lista sono speciali:

- 01 – **Auto configurazione** – attiva il riconoscimento automatico
- 02 – **Disabilita il lettore di smartcard** – predispone ***DigitalSign*** ad operare senza dispositivo di firma, evitando i messaggi di errore relativi all'assenza di un lettore

- 04 – **Specifiche PC/SC** – predispone ***DigitalSign*** ad interfacciare la smartcard in modalità APDU, senza alcuna intermediazione di moduli PKCS#11. In questa modalità sarà possibile utilizzare solo un set ristretto di dispositivi ben identificati, per progetti speciali

Dopo la selezione della modalità occorre anche specificare in quale lettore si trova il dispositivo, nel caso la macchina disponga di più di un lettore:



Qualora il dispositivo a disposizione richiedesse, per l'interfacciamento, un modulo PKCS#11 diverso da tutti quelli noti a ***DigitalSign***, è comunque possibile aggiungere un nuovo profilo tramite il bottone **Aggiungi**, si veda la sezione dedicata.

NOTA: la configurazione manuale è l'unico modo di impostare un modulo PKCS#11 virtuale per collegare un servizio di Firma Remota, si veda l'appendice dedicata.

3.8.15.3 Lista dispositivi

Questa funzione consente di esplorare e di modificare la tabella di corrispondenza tra i dispositivi fisici (smartcard e simili), individuati tramite i loro codici ATR, e i moduli PKCS#11 da utilizzare per interfacciarli.

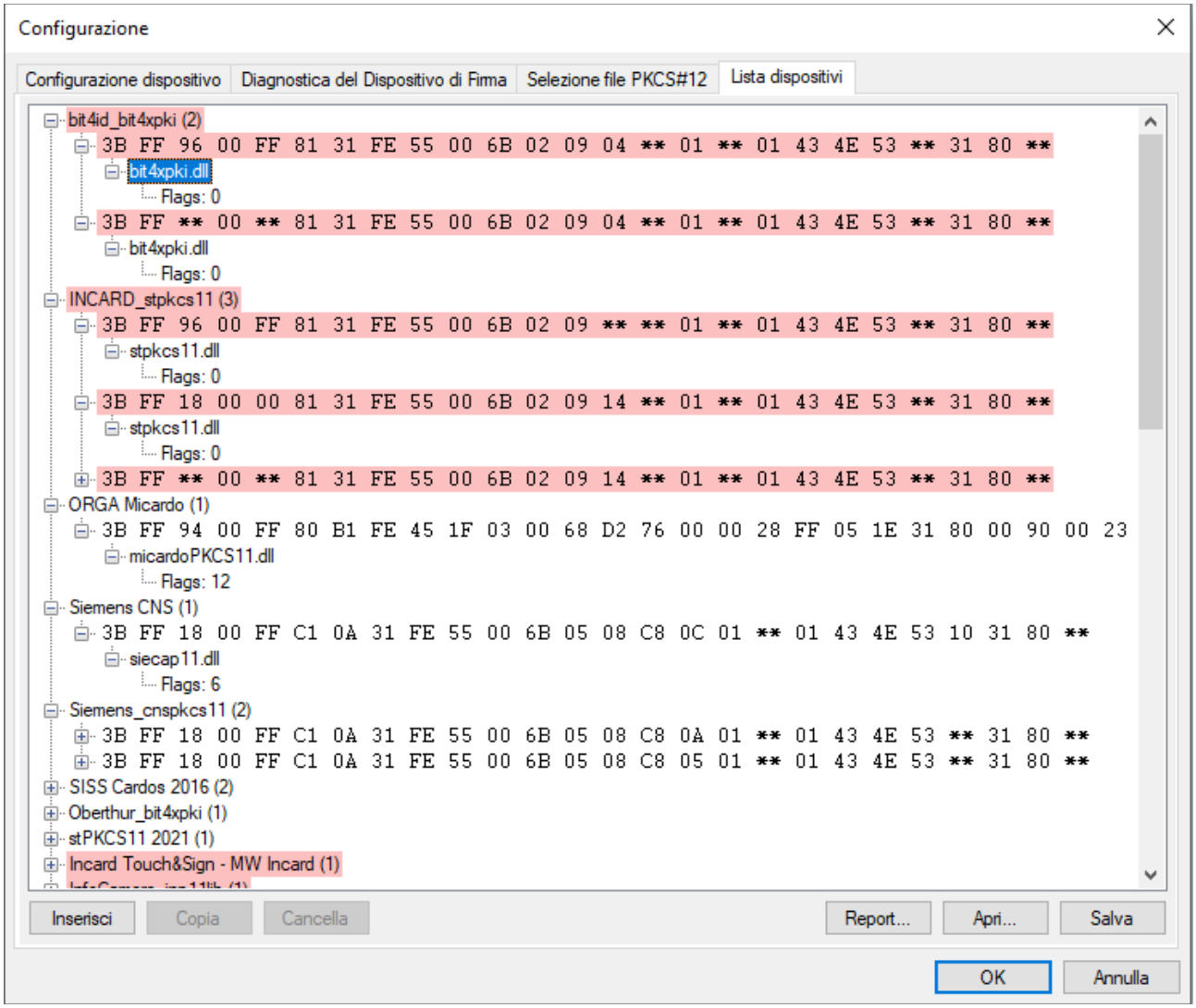
NOTA IMPORTANTE: ***DigitalSign*** ha una copia di questa tabella cablata nel proprio codice, mantenuta aggiornata da CompEd con le informazioni ricavate sul campo, nel tempo.
Questo modulo consente effettivamente agli addetti ai lavori di modificare la configurazione originale per risolvere qualche problema puntuale in attesa di avere una copia del software più aggiornata, ma dovrebbe essere usata con consapevolezza ed attenzione, perché una configurazione errata può provocare l'impossibilità, per ***DigitalSign***, di riconoscere correttamente i dispositivi di firma.

Si noti anche che ogni modifica apportata, ovviamente, non altera la copia cablata della tabella, ma può generare una versione alternativa della tabella, salvata nel file `ATRlist.txt` nella cartella `C:\ProgramData\CompEd Shared`

In qualunque momento si può tornare alle impostazioni originali semplicemente eliminando questo file.

Naturalmente è possibile fare una o più copie di questo file con nomi diversi, corrispondenti ad altrettante proprie configurazioni. Sarà poi possibile recuperare queste copie con il comando **Apri**, mentre con **Salva** le si renderanno operative.

Questa funzione mostra una pagina come questa (qui mostrata con gli alberi espansi, avendo fatto click sui pulsanti [+]:



Come precisato all'inizio di questa sezione, la tabella mostrata nella finestra può essere quella di default, cablata nel codice di ***DigitalSign***, oppure letta dal file `C:\ProgramData\CompEd Shared\ATRlist.txt` (se questo esiste).

Ogni albero corrisponde a un gruppo di smartcard, individuate con un nome affine a quello del modulo PKCS#11 da usare per interfacciarle. Si tratta però solo di un nome mnemonico per il gruppo.
Accanto al nome del gruppo è indicato il numero di dispositivi effettivamente contenuti nel gruppo.

Ogni dispositivo è rappresentato da una "maschera" ATR, ossia una stringa di byte mostrati in formato esadecimale.
Sotto ogni dispositivo è mostrato il nome di una DLL (l'effettivo modulo PKCS#11, corrispondente a una entry della lista Profili codificata nel file devices.ini) da collegare al dispositivo che presenta quel dato ATR.
Con le DLL è mostrato anche un indicatore "Flags", attualmente non utilizzato da ***DigitalSign***.

Si noti la prima maschera del modulo **bit4id_bitxpki**:

```
3B FF 96 00 FF 81 31 FE 55 00 6B 02 09 04 ** 01 ** 01 43 4E 53 ** 31 80 **
```

Si tratta di una stringa di byte (rappresentati in formato esadecimale), che presenta alcune posizioni **: queste ultime indicano "qualsiasi byte" (jolly); in altre parole una stringa di byte che corrisponda a questa maschera, contenente qualunque dato nelle posizioni ** è considerato corrispondente (match). E quindi una carta con un tale ATR è idonea ad essere interfacciata tramite il modulo `bit4xpki.dll`

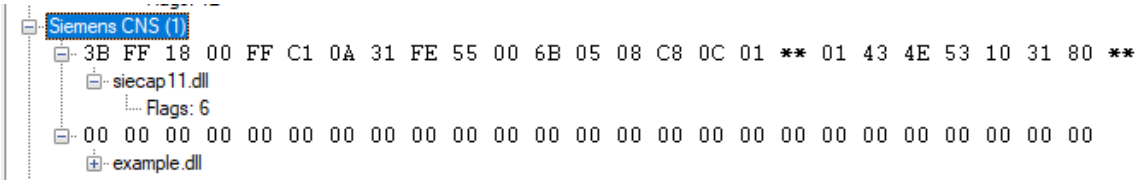
Si noti anche che alcuni moduli (come questo appena esaminato) sono evidenziati in colore rosa, mentre gli altri sono in fondo bianco.

Questo significa che c'è una sovrapposizione: per effetto dei byte mascherati con ** un effettivo codice ATR può corrispondere a più di un modulo.
In tal caso ***DigitalSign*** sceglierà il modulo PKCS#11 più specifico, ossia quello che corrisponde con meno byte jolly **.

Vediamo come intervenire per modificare la tabella: anticipiamo che le modifiche eventualmente apportate non hanno effetto fino a quando non si attiva il comando **Salva**.

- Facendo click su una maschera esistente possiamo editarne il contenuto:

- Con il bottone **Inserisci** si crea una nuova entry – costituita interamente da zeri – per un dispositivo appartenente al gruppo correntemente selezionato)



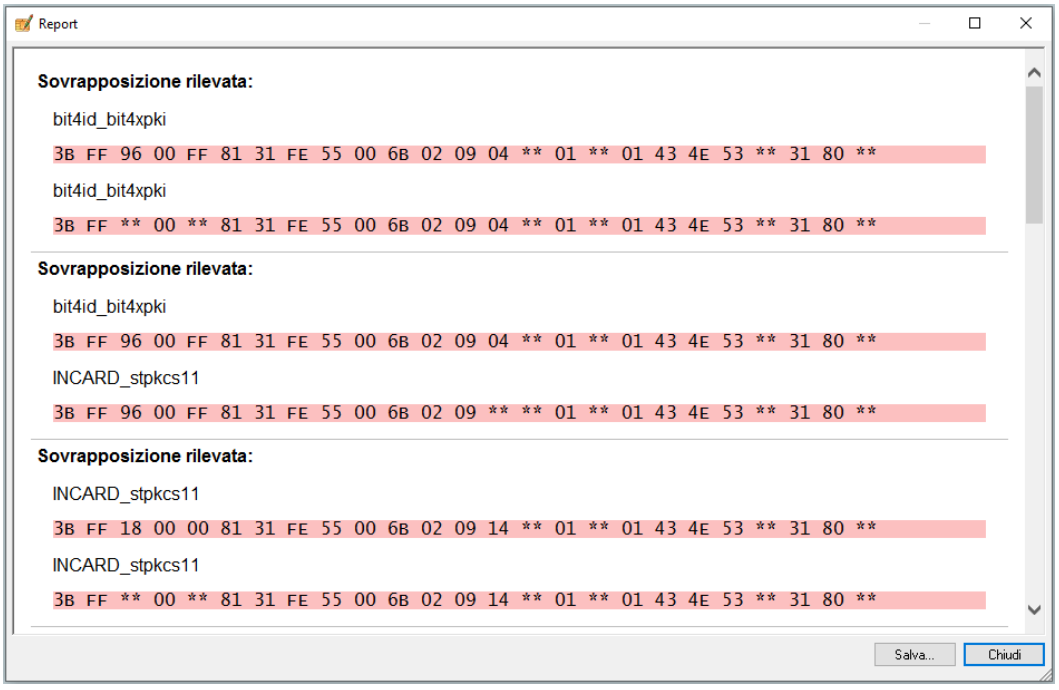
  Si noti che a questa nuova maschera è inizialmente assegnato un modulo fittizio chiamato `example.dll`, ma anche tale elemento può (deve) essere editato facendo click su di esso.

  Facendo un singolo click sulla maschera così inserita potremo editarne il contenuto.

- Con il bottone **Copia**, azionato dopo aver selezionato una entry, si produce una ulteriore entry uguale all'originale (con lo scopo di modificarne uno o più byte)

- Con il bottone **Cancella** si elimina la entry selezionata

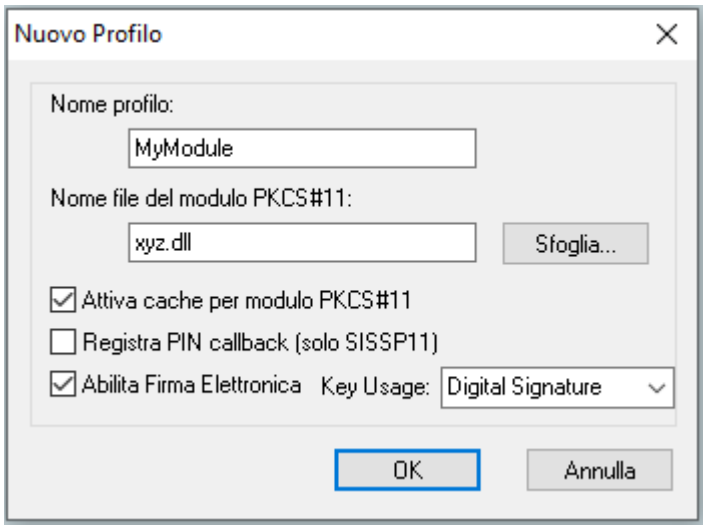
- Con il bottone **Report** si genera una schermata che evidenzia le sovrapposizioni rilevate:



- Il bottone **Salva** consente di salvare l'attuale configurazione sul file `C:\ProgramData\CompEd Shared\ATRlist.txt`: al successivo avvio ***DigitalSign*** caricherà il file così generato e utilizzerà le sue impostazioni (anziché quelle cablate all'interno dell'eseguibile)

- Il bottone **Apri** consente di caricare le impostazioni lette da un file specifico (si tratterà di una copia rinominata di un file ATRlist.txt ottenuto con **Salva**). Ovviamente le impostazioni così caricate saranno operative solo se useremo **Salva** per registrarle nel file `C:\ProgramData\CompEd Shared\ATRlist.txt`

3.8.15.4 Aggiunta di un Profilo di Configurazione



Questa finestra consente di registrare in ***DigitalSign*** un nuovo profilo di configurazione per dispositivi PKCS#11, oltre a quelli "di serie" predisposti da CompEd nel file `devices.ini` contenuto nella cartella dell'eseguibile.

I moduli aggiunti per questa via non verranno registrati nel file `devices.ini`, bensì in un file `devices_usr.ini` che si troverà nella cartella `C:\ProgramData\CompEd Shared`.
Si noti che questa cartella non è privata per l'utente corrente: si suppone che l'eventuale aggiunta di un modulo PKCS#11 sia potenzialmente utile per tutti gli utenti del computer.

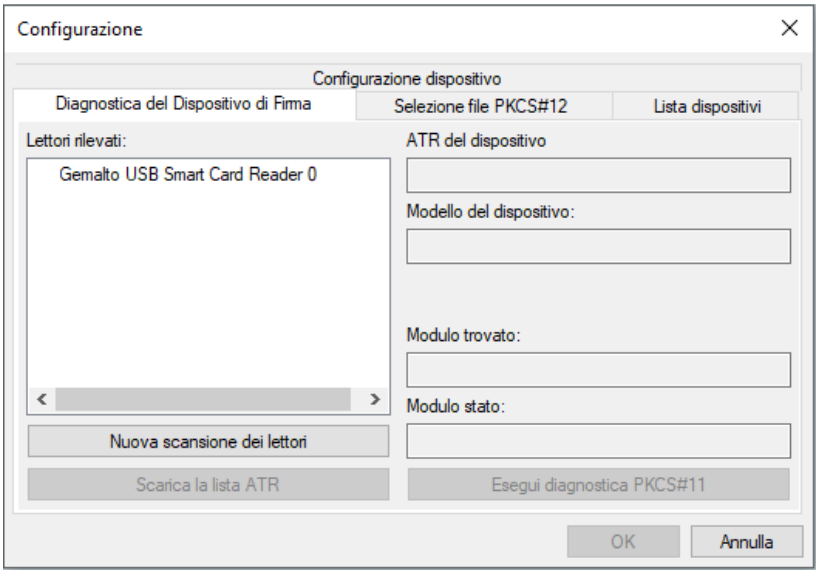
Questi i controlli disponibili:

- **Nome profilo** – è un campo editabile in cui va inserito il nome simbolico assegnato al nuovo modulo PKCS#11
- **Nome file del modulo PKCS#11** – è il nome della DLL che implementa il nuovo modulo. Si noti che inserendo il nome senza percorso esso verrà cercato nei percorsi coperti dal PATH di sistema
- **Sfoglia** – questo bottone consente di individuare la dll nel file system; in tal caso verrà salvato l'intero percorso in cui si trova la DLL
- **Attiva cache per il modulo PKCS#11** – se attivo fa sì che ***DigitalSign***, una volta collegato positivamente un dispositivo a questo modulo, registri l'associazione mediante l'ATR del dispositivo stesso, così che successivi inserimenti di dispositivi dello stesso tipo colleghino direttamente questo modulo se è attiva la modalità di auto-configurazione.
- **Registra PIN callback** – questa è una funzione speciale, riservata ad uno specifico modulo (SISSP11) e consente di gestire in modo automatico il PIN di firma, evitando la doppia richiesta del PIN. Si raccomanda di non attivare questa opzione se non su indicazioni del fornitore
- **Abilita Firma Elettronica** – questa opzione istruisce il sistema ad abilitare, per i dispositivi di firma interfacciati per tramite di questo modulo, la funzione di Firma Elettronica (firma debole). In caso di abilitazione di questo checkbox è anche necessario specificare quale *"key usage"* devono presentare i certificati da usare per questo scopo. Si raccomanda di usare **Digital Signature**, a meno di avere esplicite indicazioni diverse.

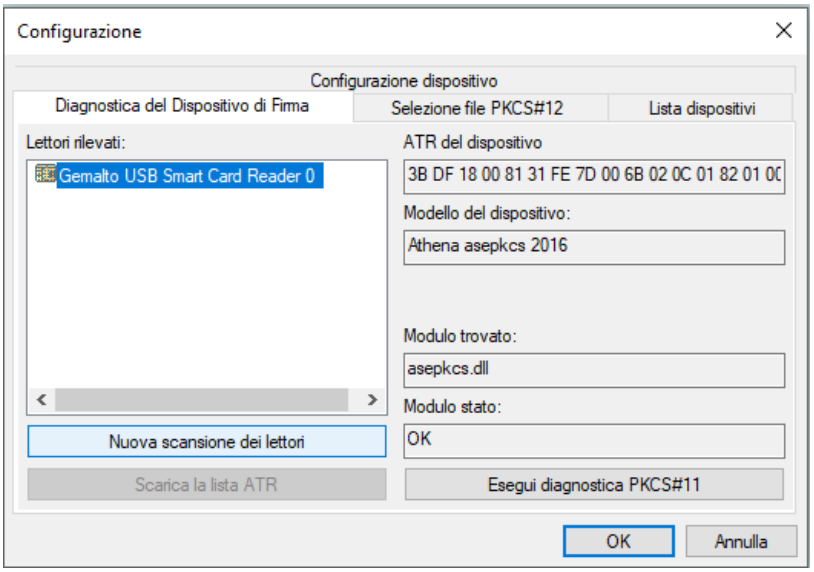
3.8.15.5 Diagnostica del dispositivo

Questo pannello consente di controllare i passi svolti da ***DigitalSign*** nella ricerca automatica di un modulo PKCS#11 adatto ad interfacciare un dispositivo di firma.

Se nessun dispositivo è inserito in un lettore il pannello può presentarsi come in figura:



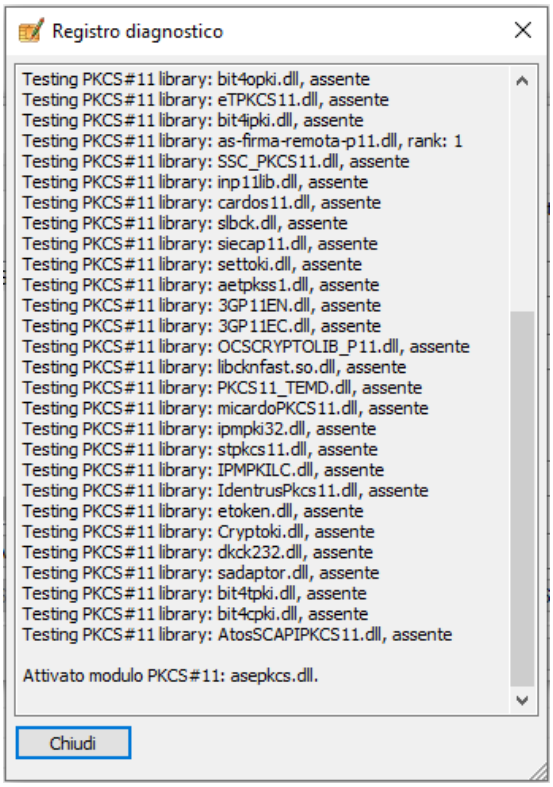
Il bottone **Nuova scansione dei lettori** forza il sistema a rileggere lo stato dei lettori, aggiornando la lista. Ma normalmente è sufficiente inserire una smartcard in un lettore per veder aggiornare la finestra in questo modo:



Il simbolo della smartcard appare accanto al nome del lettore, mentre nel riquadro a destra compare il codice ATR *(Answer To Reset)* del dispositivo.
Talvolta è disponibile anche una denominazione del modello del dispositivo.

Particolarmente importante è il bottone **Esegui diagnostica PKCS#11**: questo comando avvia un processo che ciclicamente prova a eseguire le funzioni di base (quelle accessibili senza PIN, sull'area pubblica) della smartcard con tutti i moduli PKCS#11 elencati nella tabella composta dal contenuto dei file `devices.ini` (la configurazione "di serie") e da quello eventuale del file `devices_usr-ini` (i moduli aggiunti dall'utente).

Il risultato viene riportato nella finestra di dialogo successiva:



Probabilmente la finestra non sarà abbastanza alta per contenere tutto il report. Le informazioni più importanti si trovano in testa…

```
DigitalSign 5.0 Edizione Professional - build 5,0,3,612.

ATR = 3B DF 18 00 81 31 FE 7D 00 6B 02 0C 01 82 01 00 01 43 4E 53 10 31 80 ED
Schema assegnato: ASECARD (asepkcs.dll)

Testing PKCS#11 library: asepkcs.dll, rank: 3
Testing PKCS#11 library: CIEPKI.dll, rank: 1
Testing PKCS#11 library: IPMPkiLU.dll, assente
Testing PKCS#11 library: bit4xpki.dll, rank: 3
```

… e, in fondo:

```
Testing PKCS#11 library: dkck232.dll, assente
Testing PKCS#11 library: sadaptor.dll, assente
Testing PKCS#11 library: bit4tpki.dll, assente
Testing PKCS#11 library: bit4cpki.dll, assente
Testing PKCS#11 library: AtosSCAPIPKCS11.dll, assente

Attivato modulo PKCS#11: asepkcs.dll.
```

In testa vediamo l'indicazione della versione completa di ***DigitalSign***, il codice ATR del dispositivo e – se trovato – il modulo PKCS#11 che corrisponde a tale carta in funzione del codice ATR.

Poi segue il risultato del testing con tutti i moduli, che può produrre:

- un risultato nullo, se il modulo PKCS#11 è assente nel sistema;
- un valore (*rank*) numerico, da 0 a 3, in funzione del numero di operazioni andate a buon fine (comunque solo operazioni di lettura dall'area pubblica della carta).

In fondo si legge quale modulo è stato attivato: se tutto va per il meglio il modulo coincide con lo schema assegnato indicato in alto (cioè se la carta è conosciuta, se il modulo previsto è installato sul computer e se il test ha prodotto *rank* = 3).

Altrimenti il sistema attiva il primo modulo tra quelli che hanno prodotto *rank* = 3: talvolta questa scelta funziona, ma spesso – al momento di firmare – l'operazione fallisce.

Questo report diagnostico – copiato dalla finestra e trasmesso integralmente a CompEd, può aiutare a diagnosticare un problema di interfacciamento del dispositivo di firma.

3.8.15.6 Caricamento file PKCS#12

Per ragioni di sicurezza e di aderenza alle normative ***DigitalSign*** è stato progettato per gestire chiavi private di firma contenute all'interno di dispositivi hardware, interfacciati attraverso lo standard PPKCS#11

Tuttavia, ***DigitalSign***, oltre che di firmare documenti, è anche in grado di operare la cifratura e decifratura dei contenuti (si veda l'appendice relativa).
In particolare, l'operazione di decifratura necessita di una chiave privata.

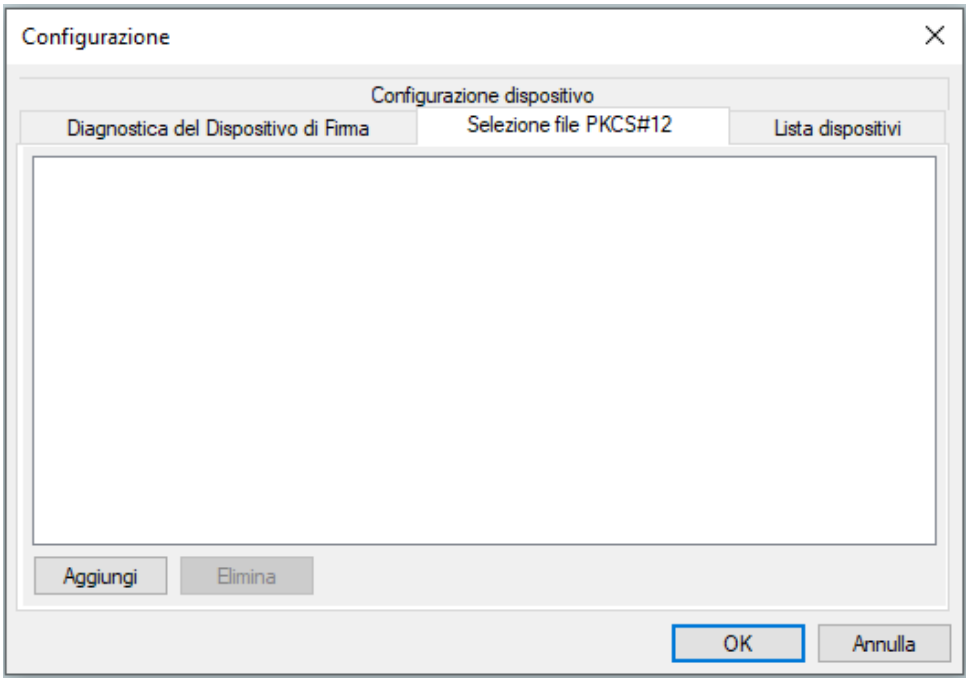
Si noti che, mentre è bene smettere di usare una chiave di firma trascorso un certo tempo dalla sua generazione (da cui la scadenza di un certificato), la decifratura di documenti criptati con una certa chiave pubblica avrà sempre bisogno della parte privata della coppia di chiavi, anche dopo la scadenza dei certificati.
Del resto, affidarsi totalmente a una smartcard per poter accedere a documenti confidenziali, anche a distanza di molti anni, può essere rischioso: se la smartcard smettesse di funzionare o non fosse più disponibile il software PKCS#11 per interfacciarla sotto una certa versione di sistema operativo, perderemmo l'accesso ai documenti.

È quindi opportuno, per questi scopi, poter usare chiavi e certificati gestiti via software.

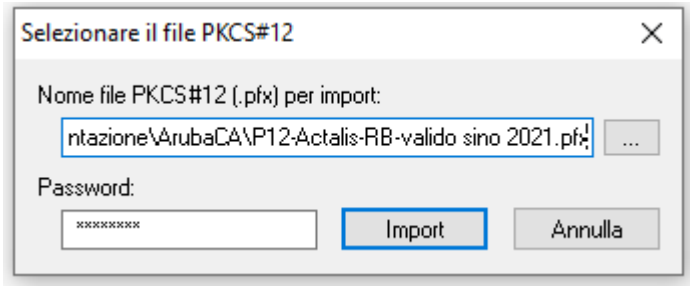
DigitalSign può utilizzare i container standard PKCS#12 per accedere alle chiavi private.

Ma poiché ***DigitalSign*** assume di lavorare con una smartcard, non direttamente con file PKCS#12, esso prevede che un file PKCS#12 sia associato ad una smartcard: opera una sorta di "importazione virtuale": tramite questa funzione è possibile importare il contenuto del file PKCS#12 e far sì che ***DigitalSign*** lo consideri, operativamente, come una chiave e un certificato contenuti nella smartcard montata.

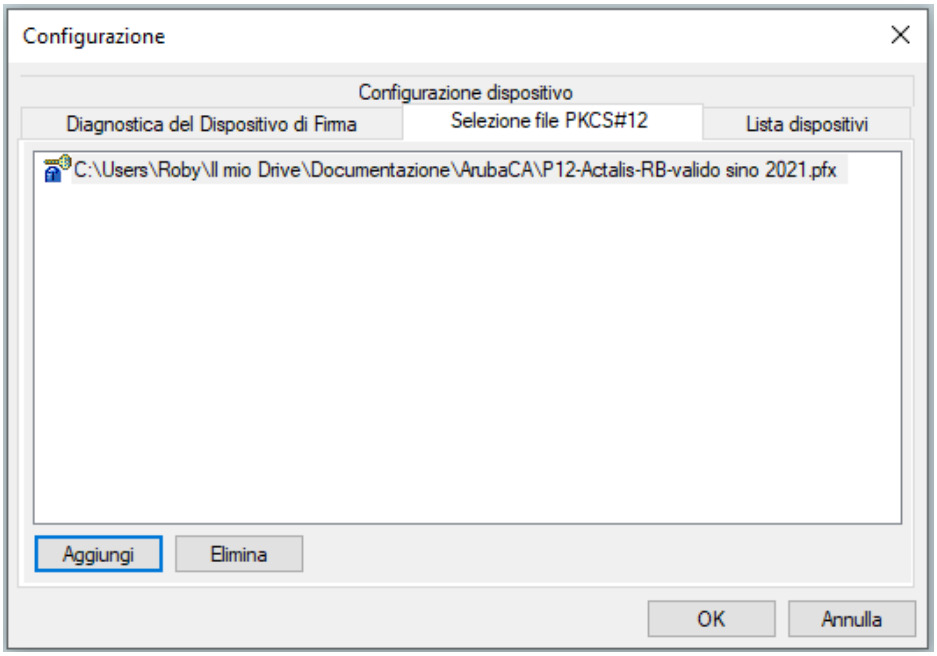
La finestra è inizialmente vuota:



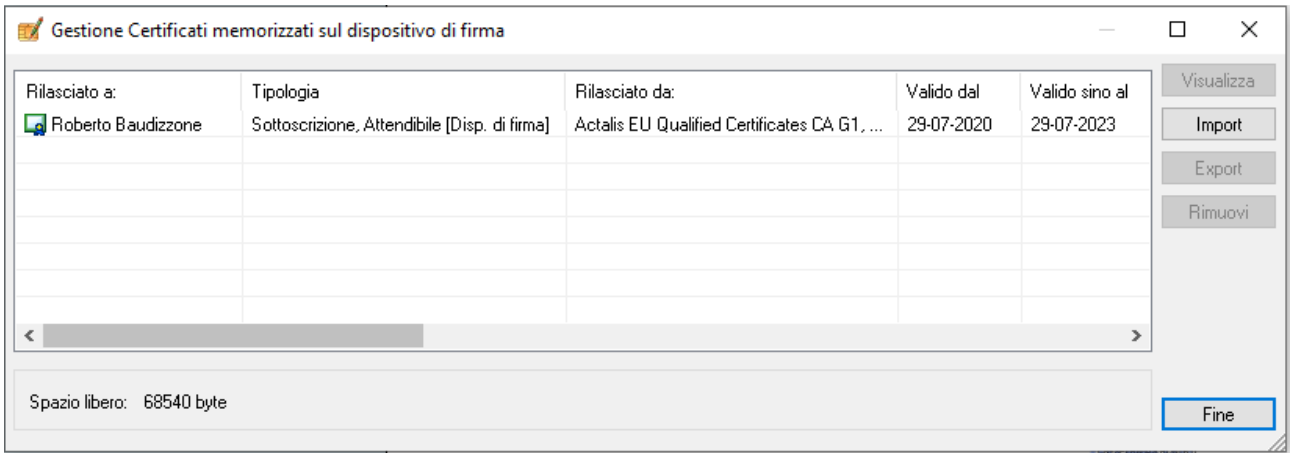
Con il bottone **Aggiungi** si apre una ulteriore finestra di dialogo per selezionare il file da importare e per inserire la password:



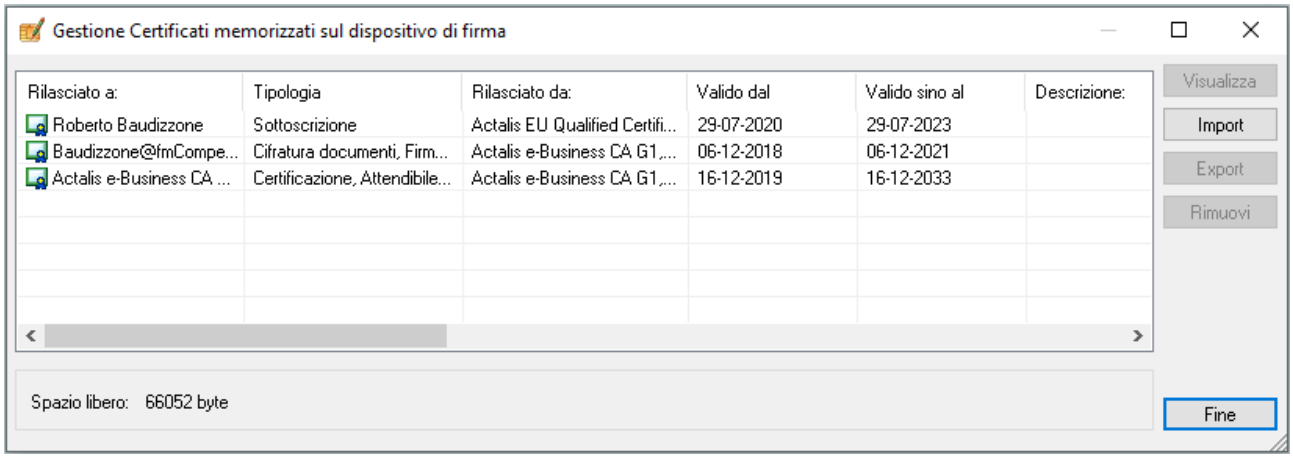
Con il bottone **Import** si opera l'effettiva importazione:



Ora possiamo verificare che i certificati contenuti in questo file siano visibili tra quelli on-board.
Se prima la nostra smartcard mostrava solo il certificato di firma effettivamente contenuto:



Ora vedremo anche il certificato di cifratura e il relativo certificato di CA caricati dal PKCS#12:



NOTA IMPORTANTE: si ribadisce inoltre che le chiavi ed i certificati importati dai file PKCS#12 specificati per tramite di questo ambiente di configurazione vengono utilizzati da ***DigitalSign*** – limitatamente alla funzione di decifratura documenti – come se le stesse chiavi e certificati fossero presenti nella smartcard correntemente inserita.
Questo significa anche che, se nessuna smartcard è inserita, non sarà possibile usare nemmeno gli oggetti software letti dai file PKCS#12: questo perché l'architettura interna di ***DigitalSign*** mette in funzione certe strutture solo quando un dispositivo di firma è correttamente interfacciato.

3.8.16 Verifica alla Data

Quando si verifica una firma apposta ad un documento in una data passata, ad esempio risalente ad alcuni anni fa, è probabile che il certificato con cui era stata apposta la firma sia ormai scaduto.
Quindi, verificando la firma oggi, avremo un risultato negativo.

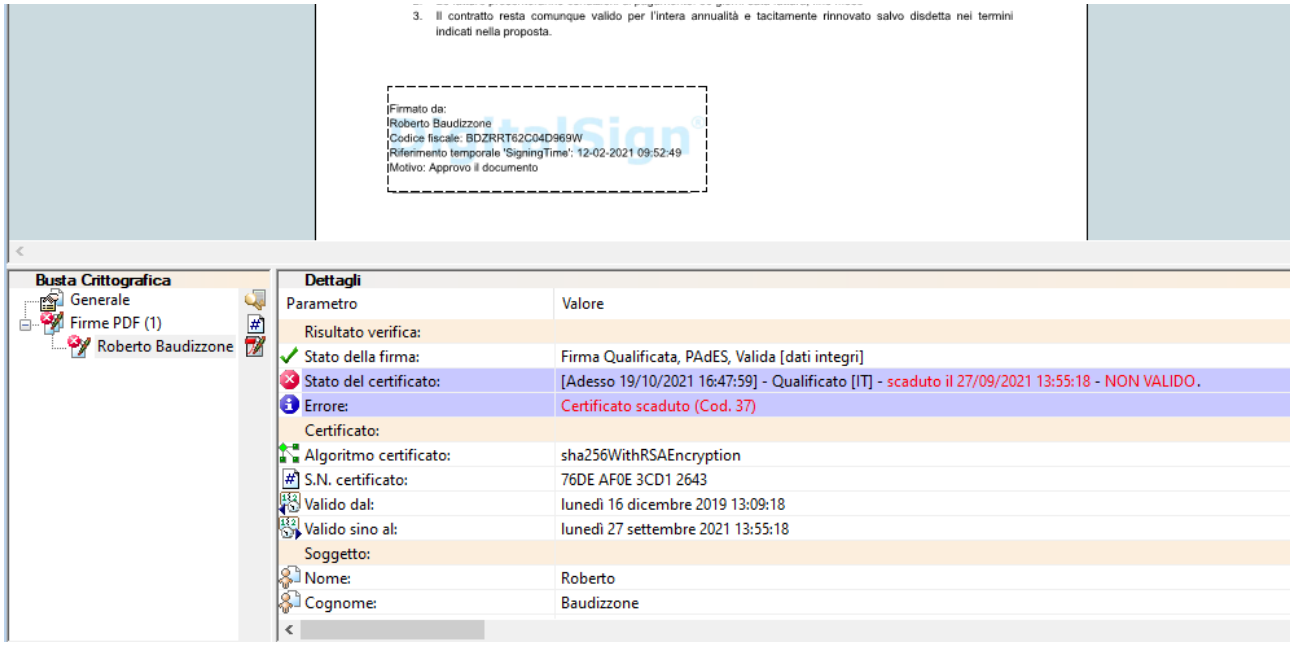
Se è nota la data in cui il documento è stato firmato è abbastanza semplice, esaminando il periodo di validità del certificato, determinare se in quel momento tale certificato fosse in corso di validità (ossia non scaduto).

Meno facile è stabilire se in quel momento il certificato fosse stato revocato: occorre esaminare la lista di revoca corrispondente al certificato sotto esame, ricercare il numero di serie e – nell'ipotesi di trovarlo – verificare se il provvedimento di revoca fosse anteriore o posteriore a quello della firma,

NOTA IMPORTANTE: la normativa attuale impone ai Certificatori di mantenere nelle proprie CRL le informazioni di revoca anche dopo la scadenza naturale di un certificato, quindi questa operazione è possibile. Ma questo non è scontato: la norma lo prevede solo dal 2009, prima di tale data la scadenza di un certificato implicava la perdita delle informazioni sulla revoca.
Altre autorità di certificazione, estranee all'infrastruttura della Firma Qualificata, potrebbero comportarsi in tal modo. Par assicurare la disponibilità di queste informazioni nel tempo si può ricorrere alla modalità LTV.

Tutte queste operazioni si possono eseguire automaticamente, mediante la "Verifica alla data".

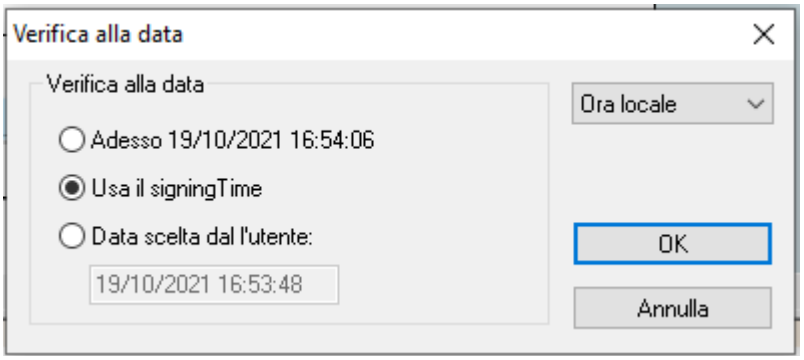
Ad esempio, proviamo ad aprire normalmente un documento firmato con un certificato ormai scaduto:



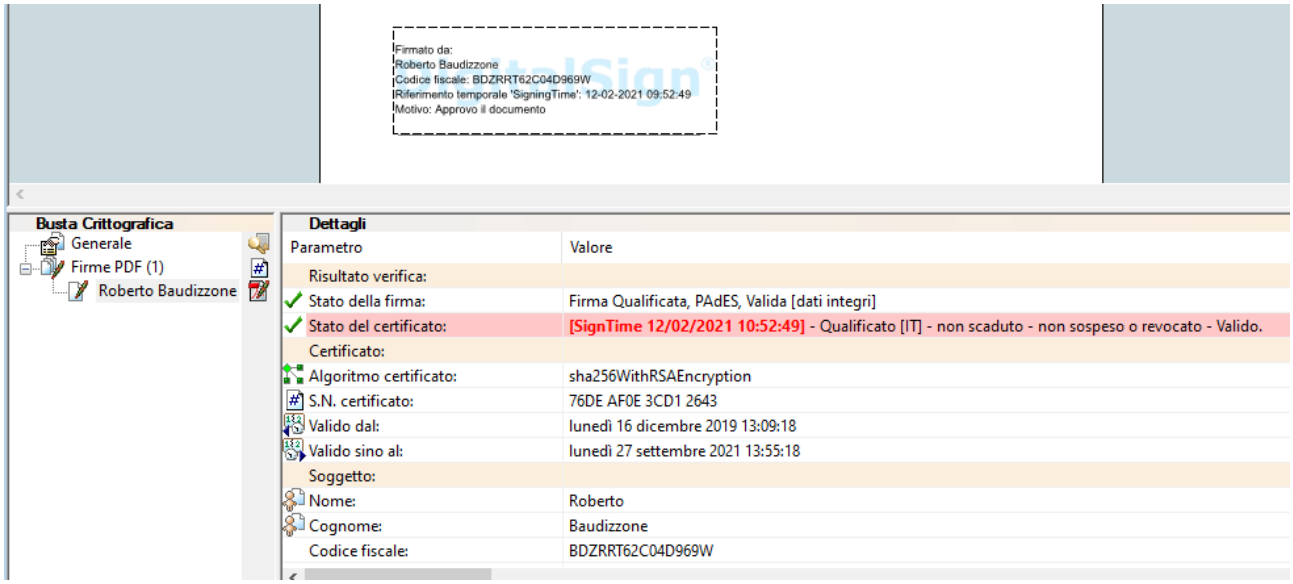
DigitalSign indica che la firma – esaminata "Adesso", il 19/10/2021, non è valida perché il certificato è scaduto da quasi un mese.

Ma, si veda l'istante della firma "SigningTime", tale firma era stata apposta il 12/02/2021.

Proviamo a richiamare la funzione del menu Documento -> Verifica alla data:



Scegliamo l'opzione **Usa il signingTime**, così il sistema centrerà automaticamente la verifica all'istante determinato da tale attributo della firma:

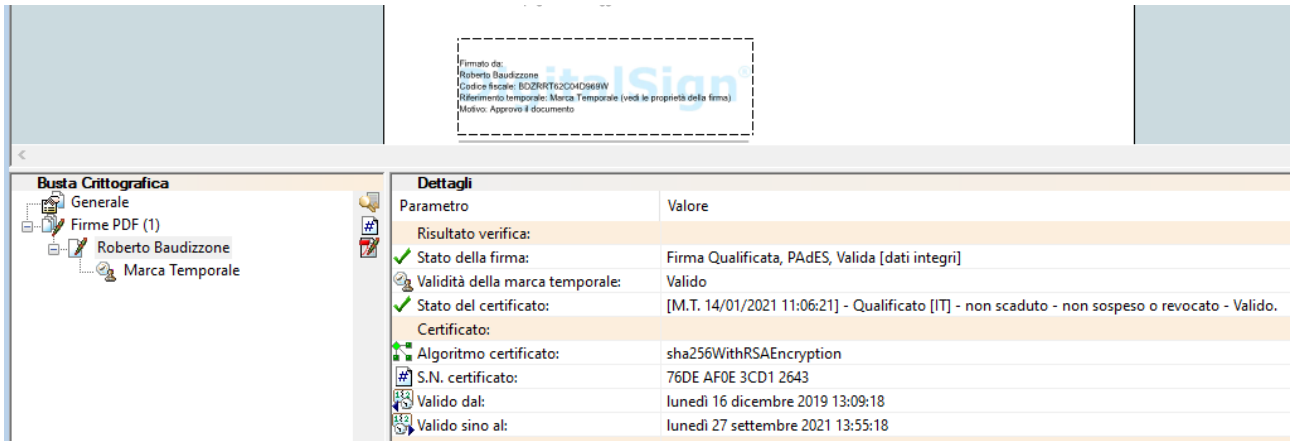


Ora la verifica è positiva, ma è evidenziato **(in rosso)** che la verifica si basa su un riferimento temporale non necessariamente attendibile (l'attributo signingTime non ha valore di prova, non è un riferimento temporale opponibile ai terzi, perché è facile impostarlo a proprio piacimento al momento della firma).

In ogni caso, se ci fidiamo di questo riferimento, il sistema riferisce che in quel momento il certificato non era scaduto e non era nemmeno stato revocato.

NOTA IMPORTANTE: poiché, come detto, il signingTime non ha valore di prova, ***DigitalSign*** non lo usa come riferimento nelle verifiche delle firme (a meno che l'utente non decida di farlo, impostando il checkbox **Usa il signingTime per fissare istante verifica firme** dalla finestra di dialogo delle Opzioni di Security).

Se invece una firma è stata generata aggiungendo – come riferimento temporale – una vera e propria Marca Temporale (che è un riferimento temporale opponibile ai terzi) allora ***DigitalSign*** esegue automaticamente la *verifica alla data* nell'istante testimoniato dalla M.T. senza bisogno di usare la funzione **Verifica alla Data**:



In questo caso lo stato del certificato è riportato "Valido", con la dicitura (non evidenziata in rosso, perché non c'è nulla di critico):

[M.T. 14/01/2021 11:06:21]

ad indicare che la verifica è centrata nella data e ora corrispondenti alla Marca Temporale a suo tempo associata alla firma.

3.9 Appendici

3.9.1 Troubleshooting: problemi di interfacciamento dei dispositivi di firma

La quasi totalità delle richieste di supporto tecnico a CompEd, riguardo a ***DigitalSign***, hanno per oggetto difficoltà di interfacciamento con smartcard e token USB.

In questa sezione cerchiamo di illustrare i dettagli di funzionamento del sistema e fornire suggerimenti per la risoluzione di questi problemi.

Assumiamo che il dispositivo sia correttamente interfacciato a livello hardware (ci sia un lettore di smartcard, oppure il token USB sia correttamente "visto" dal sistema operativo come un "Lettore di Smartcard").

I problemi di interfacciamento si possono manifestare in diverse forme, le quali hanno in comune l'impossibilità di generare una firma con la chiave privata associata al certificato qualificato presente nel dispositivo.

Qualche esempio:

1. La barra di stato non mostra correttamente il nome e cognome del titolare del certificato, a volte mostrando solo il suo codice fiscale. In questo caso non è possibile neppure iniziare un'operazione di firma, perché nella lista di opzioni per la scelta del certificato, al momento di confermare l'esecuzione della firma, non compare il certificato qualificato che sappiamo essere disponibile sulla smartcard.
2. In fase di firma otteniamo un **Errore Sconosciuto (601)**
3. In fase di firma vediamo un messaggio del tipo: **Il modulo PKCS#11 ha generato un errore e verrà reinizializzato (cod. 2088)**

In tutti questi casi la causa più probabile è che ***DigitalSign*** non stia usando il modulo PKCS#11 appropriato per interfacciare il dispositivo di firma correntemente inserito nel lettore.

Si veda anche la sezione dedicata agli strumenti di configurazione del dispositivo di firma per approfondire i dettagli di funzionamento.

Il concetto fondamentale è che i Certificatori mettono continuamente in circolazione nuovi dispositivi, con diversi "Card OS" (i sistemi operativi dei microcomputer a bordo delle carte), diverse versioni degli stessi. E di conseguenza rilasciano/aggiornano i cosiddetti "middleware", cioè i pacchetti software in grado di interfacciare questi dispositivi e che contengono anche i relativi moduli PKCS#11.

Affinché ***DigitalSign*** possa usare tutti i servizi di un dispositivo di firma, deve attivare la DLL giusta per quel dispositivo. E questo non è sempre un risultato scontato.

3.9.1.1 Il riconoscimento automatico del dispositivo

In quasi tutte le situazioni il problema si risolve in modo ottimale lasciando che il modulo di Auto Configurazione trovi e attivi la DLL giusta.
A tal fine si imposta la modalità Auto Configurazione e si lascia che ***DigitalSign*** faccia il resto.

Questo però può avvenire solo se si verificano certe condizioni:

i. il dispositivo inserito nel lettore (o il token USB inserito) presenta un codice ATR conosciuto per la copia di ***DigitalSign*** in esecuzione, così che quindi ***DigitalSign*** "sappia" quale DLL attivare per interfacciarlo;
ii. la DLL che implementa il modulo PKCS#11 è effettivamente installata e in versione aggiornata (una versione troppo vecchia del modulo teoricamente appropriato potrebbe non essere in grado di interfacciare un dispositivo introdotto di recente);
iii. la DLL in questione si trova in un percorso effettivamente raggiunto dal PATH di sistema.

Se una o più di queste condizioni non è soddisfatta è probabile che l'interfacciamento non vada a buon fine.
Il riconoscimento automatico tenta, in questi casi, di montare una DLL diversa da quella ottimale, ma quasi mai questo tentativo dà risultati soddisfacenti e non riusciremo ad apporre la firma.

3.9.1.2 Il report diagnostico

In caso di difficoltà la prima cosa da fare è eseguire la Diagnostica del Dispositivo:

Nelle situazioni in cui tutto funziona correttamente il report diagnostico si presenta più o meno così:

```
DigitalSign 5.0 Edizione Professional - build 5,0,3,621.

ATR = 3B FF 18 00 00 81 31 FE 45 00 6B 05 05 20 00 01 21 01 43 4E 53 10 31 80 79
Schema assegnato: InfoCamere_bit4xpki (bit4xpki.dll)

Testing PKCS#11 library: bit4xpki.dll, rank: 3
Testing PKCS#11 library: CIEPKI.dll, rank: 1
Testing PKCS#11 library: C:\Windows\SysWOW64\namirial-p11.dll, rank: 1
Testing PKCS#11 library: IPMPkiLU.dll, assente
<...>
Testing PKCS#11 library: bit4cpki.dll, assente
Testing PKCS#11 library: AtosSCAPIPKCS11.dll, assente
Testing PKCS#11 library: bit4p11.dll, assente

Attivato modulo PKCS#11: bit4xpki.dll.
```

Si noti che che:

a) per l'ATR ricavato dalla carta esiste uno **Schema assegnato**
b) la DLL corrispondente allo **Schema assegnato** è presente e, al *testing*, fornisce il risultato massimo (rank: 3)
c) il modulo attivato è proprio quello assegnato

Se siamo in questa situazione e abbiamo comunque difficoltà a firmare la causa può essere un modulo non aggiornato oppure la presenza di più copie della stessa DLL nel sistema.

NOTA: se l'utente non riesce a risolvere il problema in autonomia, seguendo le indicazioni delle prossime sezioni, può essere utile trasmettere a CompEd o al rivenditore una copia di questo report diagnostico.
È appena il caso di sottolineare che non sarà sufficiente fornire una *screenshot* della finestra che lo contiene, perché in genere è troppo piccola per contenere (e mostrare) sia la testa che la coda del report. Occorre selezionare l'intero testo, copiarlo e poi incollarlo nel corpo della mail di richiesta di supporto.

3.9.1.3 Carta di tipo sconosciuto

Questa situazione è rivelata da una diagnostica di questo tipo:

```
DigitalSign 5.0 Edizione Professional - build 5,0,3,538.

ATR = 3B FF 18 00 00 81 31 FE 55 00 6B 02 09 06 03 01 01 01 43 4E 53 10 31 80 67
Nessuno schema preassegnato a questo ATR.

Testing PKCS#11 library: IPMPkiLU.dll, assente
Testing PKCS#11 library: bit4xpki.dll, rank: 3
Testing PKCS#11 library: incryptoki2.dll, rank: 3
Testing PKCS#11 library: AtosSCAPIPKCS11.dll, assente
Testing PKCS#11 library: bit4p11.dll, assente
<…>
Attivato modulo PKCS#11: bit4xpki.dll.
```

La dicitura **Nessuno schema preassegnato a questo ATR** indica che il codice ATR letto dalla carta non corrisponde a nessun modello presente nella lista dei dispositivi conosciuti a ***DigitalSign***.

Quindi ***DigitalSign*** non può andare a colpo sicuro; esegue un test ciclico di test delle funzioni con tutti i moduli trovati, tentando di enumerare e leggere gli oggetti presenti nell'area pubblica del dispositivo, quindi assegnando un voto (rank) in funzione del risultato.
E infine monta la prima DLL della lista che raggiunge almeno rank = 2

Poiché la lista è ordinata secondo la "popolarità" dei diversi moduli (cioè il numero di diversi ATR effettivamente serviti da quel particolare modulo), è possibile che questa manovra permetta il regolare funzionamento.

Ma è anche possibile (anzi, probabile) che le funzioni attive (logon al dispositivo, generazione della firma) non funzionino.

Se ricadiamo in questa situazione possiamo:

1. procurarci una versione aggiornata di ***DigitalSign*** e verificare se il problema persiste (una versione più recente potrebbe "conoscere" l'ATR che la copia datata non conosceva);
2. consultare CompEd fornendo i dati così ricavati e, soprattutto, il Certificatore he ha rilasciato la carta;
3. se dal fornitore si ottiene un'indicazione precisa su quale modulo PKCS#11 va montato con questa carta è possibile configurarlo manualmente;
4. possiamo aggiungere questo codice ATR e l'indicazione della DLL usando le funzioni di Lista dispositivi: tuttavia, questa è un'operazione non banale e che resterebbe confinata al computer su cui viene effettuata, o – al più a quelli su cui riportiamo il file **ATRlist.txt** così ottenuto

Sia che risolviamo con (3) o con (4) si raccomanda di informare CompEd, così che un successivo aggiornamento di ***DigitalSign*** possa essere arricchito di questa nuova informazione e risolvere il problema alla radice.

3.9.1.4 DLL assente

È il caso in cui la carta è riconosciuta tramite il suo ATR, ma la DLL che servirebbe per interfacciarla è assente nel sistema.

La diagnostica si presenta più o meno così:

```
DigitalSign 5.0 Edizione Professional - build 5,0,3,538.

ATR = 3B DF 18 00 81 31 FE 7D 00 6B 02 0C 01 82 01 11 01 43 4E 53 10 31 80 FC
Schema assegnato: Athena_asepkcs (asepkcs.dll)

Testing PKCS#11 library: asepkcs.dll, assente
Testing PKCS#11 library: IPMPkiLU.dll, assente
Testing PKCS#11 library: bit4xpki.dll, assente
Testing PKCS#11 library: incryptoki2.dll, rank: 2
Testing PKCS#11 library: cnsPKCS11.dll, assente
Testing PKCS#11 library: SissP11.dll, assente
Testing PKCS#11 library: si_pkcs11.dll, assente
Testing PKCS#11 library: CardOS_PKCS11.dll, assente
Testing PKCS#11 library: sadaptor.dll, assente
<...>
Testing PKCS#11 library: bit4tpki.dll, assente
Testing PKCS#11 library: bit4cpki.dll, assente

Attivato modulo PKCS#11: incryptoki2.dll.
```

In questo caso esiste uno **Schema assegnato** per l'ATR rilevato, il quale richiederebbe il file `asepkcs.dll`.

Ma tale DLL non è stata trovata nel sistema: quindi il sistema attiva un modulo che, al test, abbia raggiunto almeno il risultato rank=2. Ma probabilmente non funzionerà.

NOTA IMPORTANTE: per verificare se un modulo PKCS#11 (una DLL) sia effettivamente presente nel sistema ***DigitalSign*** non può effettuare una ricerca massiva per tutto il file system del computer. Si limita a tentare l'attivazione della DLL. Questo può avvenire solo se la DLL si trova in una cartella inclusa nel PATH di sistema.
Quindi, se ***DigitalSign*** riporta che una DLL è assente, non significa necessariamente che non esiste, ma potrebbe essere in una cartella privata di una diversa applicazione. Si veda il problema del PATH di sistema.

Quindi, se ci troviamo in questa situazione, nella maggior parte dei casi sarà sufficiente procurarsi il middleware fornito dal Certificatore che ha rilasciato la carta e installarlo nel computer.

In taluni casi il middleware è fornito sotto forma di un package a sé stante (ad esempio Bit4Id), altre volte è integrato nel software di firma distribuito dal certificatore, obbligando quindi ad installarlo per risolvere il problema.

3.9.1.5 Modulo non aggiornato

Come accennato nella sezione introduttiva alla diagnosi, può capitare che la diagnostica riporti una situazione corretta (esiste uno schema assegnato, esiste una DLL con il nome corrispondente, ***DigitalSign*** la attiva), ma persistano errori in fase di firma.

La causa probabile di una situazione di questo tipo è che la DLL montata, anche se ha il nome giusto, non sia in versione aggiornata.

Specie nei tempi più recenti i produttori delle carte e i Certificatori tendono a distribuire middleware la cui DLL di interfaccia PKCS#11 è sempre la stessa, anche se vengono via via introdotti nuovi dispositivi: successive versioni del middleware includono il supporto delle carte più recenti.

Inoltre, capita che le carte pur simili adottate da diversi certificatori abbiano delle differenze di configurazione e richiedano versioni specifiche dello stesso middleware.

Questo problema si risolve richiedendo ed installando la versione più recente possibile del middleware al Certificatore che fornisce il dispositivo.

Talvolta si verifica anche il caso in cui diverse copie del middleware coesistano sullo stesso computer, si veda la prossima sezione.

3.9.1.6 Presenza di più copie della DLL nel sistema

Consideriamo ancora il caso, accennato nella sezione introduttiva alla diagnosi, in cui la diagnostica riporta una situazione corretta (esiste uno schema assegnato, esiste una DLL con il nome corrispondente, ***DigitalSign*** la attiva), ma persistano errori in fase di firma.

Talvolta si installano sul computer diverse copie, in versioni diverse, del middleware di una carta; ancora più frequentemente package diversi (tipicamente le basiche applicazioni di firma fornite da diversi certificatori) installano nel sistema la propria versione di un modulo PKCS#11 per una certa tipologia di carta.

Di solito il primo package installa queste DLL nelle cartelle predefinite a contenerle (`System32` o `SysWOW64`), ma non di rado gli installer, se trovano in tali posizioni copie preesistenti di queste DLL, evitano di sovrascriverle e installano le nuove in una propria cartella (ad esempio `C:\Users\`*`nomeutente`*`\AppData\Local\InfoCert\GoSign Desktop\RAO`).

Il risultato è che nel computer ci saranno diverse copie – a diversi livelli di aggiornamento – delle DLL necessarie a interfacciare le smartcard. Inoltre, la versione più recente, essendo installata più tardi, sarà quella relegata in una cartella proprietaria dell'applicazione che l'ha installata, anziché nella cartella predefinita di Windows.

Ma ***DigitalSign*** si limita a richiedere al sistema operativo l'attivazione di una DLL, dato il nome: quindi collegherà quella eventualmente presente nel primo percorso tra quelli listati nel PATH di sistema. La quale potrebbe essere vecchia e non idonea al nostro dispositivo di firma.

Quindi, in questa situazione vale la pena di ricercare la DLL richiesta (ricordiamo: è quella indicata dallo **Schema assegnato** nel report diagnostico) nel computer; nel caso se ne trovino più di una è bene esaminarle (con le proprietà di Windows Explorer) e considerare quella dal numero di versione maggiore.

Per verificare se tale DLL più recente è idonea si può provare a collegarla manualmente e provare un'operazione di firma.

In tal caso il problema si può risolvere modificando il PATH di sistema ed includendovi il percorso della cartella che contiene la nostra DLL. Si vedano le considerazioni sul problema del PATH di sistema.

Altrimenti può essere il caso di disinstallare i middleware trovati, procurarsi quello corretto dal fornitore della carta ed installarlo su una situazione "pulita".

3.9.1.7 Il problema del PATH di sistema e la procedura di troubleshooting

Come introdotto nelle precedenti sezioni (modulo non aggiornato e presenza di più copie di una DLL) capita, talvolta, che un modulo PKCS#11 raggiunto tramite Windows (che opera ricercandolo nei percorsi dichiarati nel PATH di sistema), nonostante abbia il nome atteso, non funzioni correttamente con la carta a disposizione.
Può anche capitare che tale modulo non si riesca a raggiungere perché si trova in una cartella non inclusa tra i percorsi dichiarati nel PATH di sistema.

La procedura da seguire per gestire questi problemi, una volta determinato (dall'indicazione **Schema assegnato** del report diagnostico) il nome della DLL necessaria, è la seguente:

1. ricercare tale DLL nel sistema; se non esiste => installare il middleware che la contiene, dal package fornito/indicato dal fornitore del dispositivo di firma;
2. se ne esiste una sola copia, ma il report diagnostico la dichiara **assente** allora => *verificare & risolvere* (vedere sotto)
3. se ne esiste una sola copia, il report diagnostico dice che è presente e attivata, ma non funziona => procurarsi il package aggiornato e installarlo sul computer, meglio disinstallando prima l'esistente;
4. se ne esistono più di una copia, ma quella montata non funziona => *verificare & risolvere* (vedere sotto)

Verificare & risolvere
Per verificare se una DLL funziona (ad esempio, una DLL che il report diagnostico dichiara assente, ma che abbiamo trovato sul computer in una cartella non standard, oppure una seconda o terza copia di una DLL mentre la prima non funziona) occorre collegarla manualmente e provare a firmare.
Se non funziona dobbiamo proprio cercare il middleware giusto, rivolgendoci al fornitore.

Una volta verificato che la DLL funziona abbiamo due opzioni:

a) la più elegante: disinstallare i package che contengono le DLL (nel dubbio: tutti gli altri package middleware, tutte le altre applicazioni di firma fornite dai certificatori) e installare solo quello raccomandato dal fornitore della smartcard, nella versione più recente possibile.
Questo dovrebbe far sì che la DLL in questione finisca in `Windows\System32` o `Windows\SywWOW64`, dove verrà raggiunta tramite il PATH di sistema. Ma se la DLL si troverà di nuovo in una posizione non standard occorrerà ricorrere all'opzione (b);

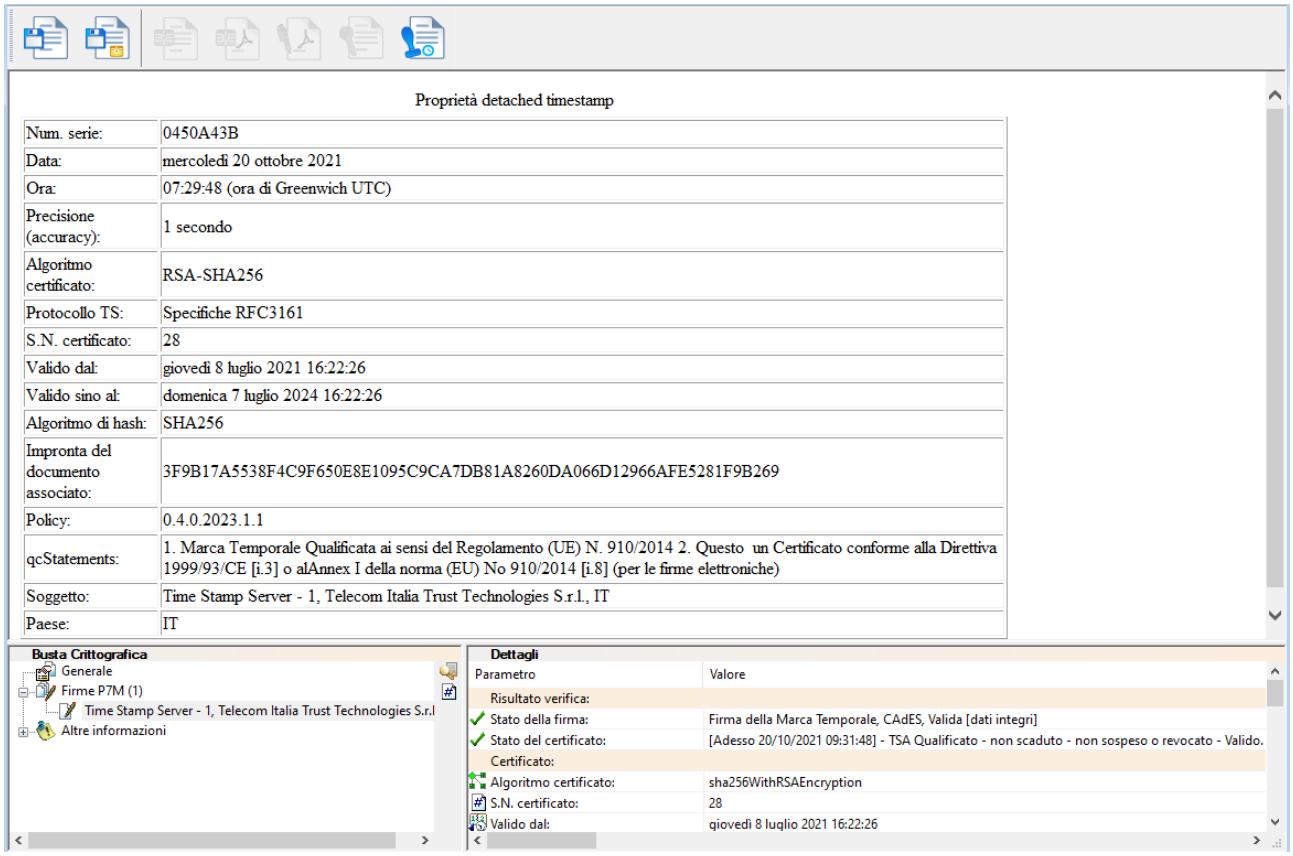
b) modificare il PATH di sistema in modo che includa il percorso in cui si trova la cartella.
ATTENZIONE: se lasciamo entrambe le copie e aggiungiamo il nuovo percorso in coda alla lista di percorsi dichiarati nel PATH, il sistema continuerà a trovare la prima DLL. O inseriamo il nuovo percorso in testa (il che non è ottimale per il normale funzionamento del sistema), oppure eliminiamo (meglio rinominare, per verificare che altre applicazioni non dipendano da quella specifica DLL) quella vecchia che non funziona con la nostra carta, in modo che venga collegata la seconda.

3.9.2 Marche temporali: contenuto e modalità di associazione ai documenti

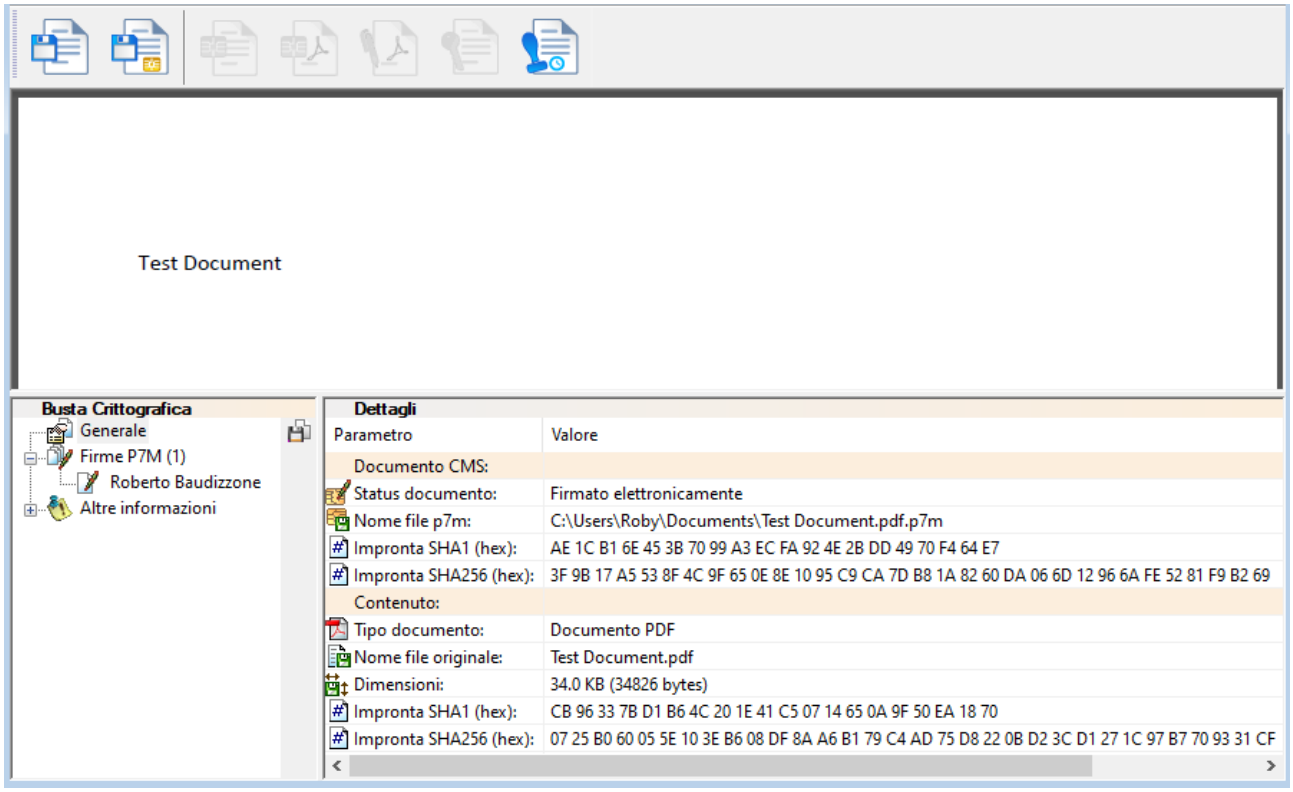
Se una Marca Temporale è associata ad un intero documento (quindi non ad una singola firma) costituisce un documento a sé stante, firmato digitalmente dal Provider di marcatura temporale.

Il suo scopo – essendo generato a partire dal valore dell'impronta dell'intero file a cui si riferisce – è dimostrare che tale documento e sistema all'istante testimoniato dalla data ed ora della marca stessa.

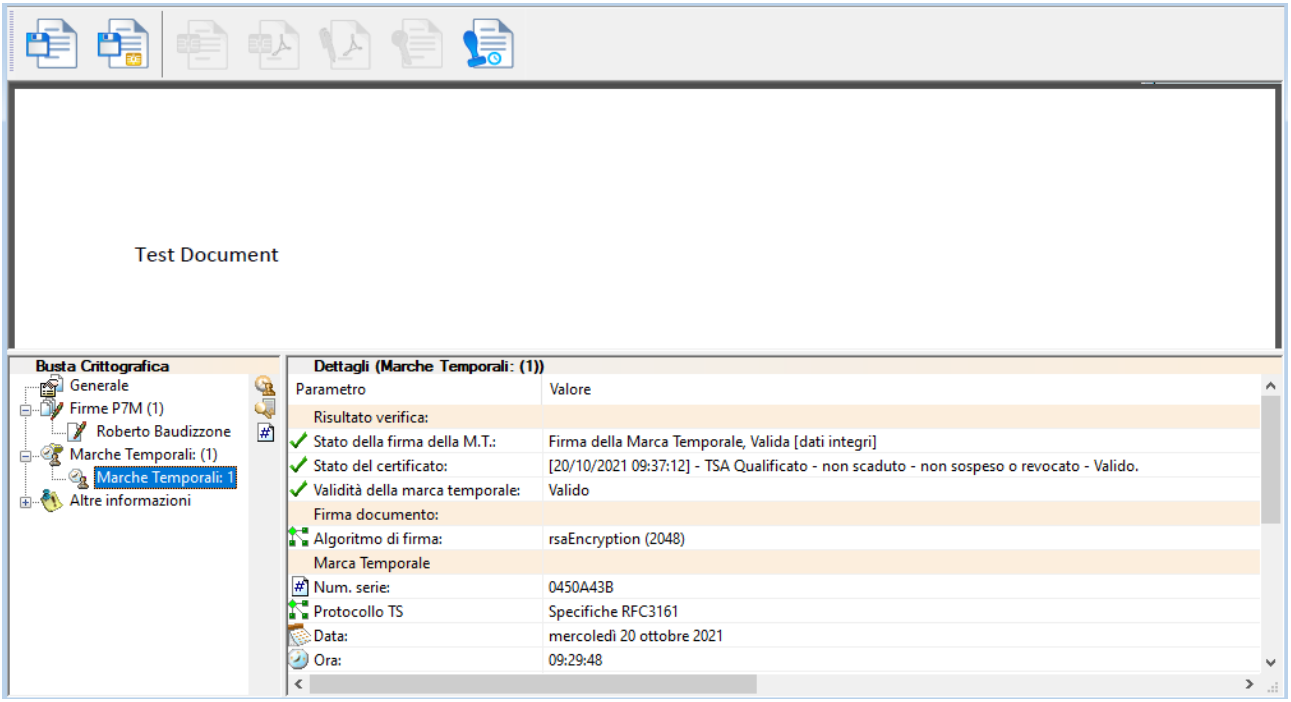
La figura qui sotto mostra il contenuto di una marca temporale esaminata separatamente dal documento cui è riferita:



Quest'altra mostra il documento a cui la marca era stata associata. Si noti la coincidenza dei valori di impronta:

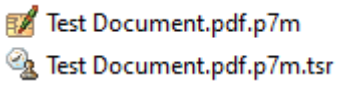


Naturalmente sarebbe troppo macchinoso per l'utente verificare visivamente l'identità dell'impronta del documento e quello dell'impronta oggetto della marca temporale; per questo ***DigitalSign*** apre la coppia di documenti insieme, mostrando il documento marcato temporalmente:



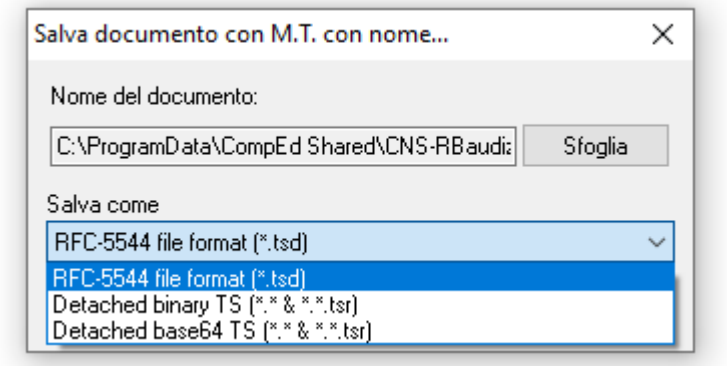
Ma per ottenere un tale obiettivo occorre individuare una modalità per associare i due oggetti.

Il modo più semplice è mantenere i due file (il documento e la marca temporale) nella stessa cartella, con lo stesso nome a meno dell'estensione:



In passato (2009) la normativa italiana aveva individuato uno standard (RFC 5544) che consentiva di riunire i due oggetti in un singolo file avente estensione **.tsd**
Purtroppo, il regolamento eIDAS non ha recepito questo standard, quindi l'unica modalità ufficiale per gestire questi file è quella *detached* (coppia di file distinti).

Ma poiché il formato '**.tsd'** è reversibile (avendo l'accortezza di NON abilitare l'inclusione dei metadati nel file .tsd, si veda la configurazione delle opzioni generali dal menu Strumenti -> Opzioni), possiamo tranquillamente salvare questi file in formato '.tsd' e – all'occorrenza – aprirli per salvarli nella modalità *detached*.



Le diverse modalità supportate sono le seguenti:

- **RFC-5544 file format (*.tsd)**

È lo standard previsto dalle regole tecniche 2009, poi tralasciato dal regolamento eIDAS. Comodo per evitare di gestire sempre coppie di file, reversibile se non si includono i metadati nel calcolo del hash.

- **Detached binary TS (*.* & *.tsr)**
  Il documento e la marca temporale vengono memorizzati separatamente, come due file PKCS#7 codificati in DER.
  La *naming convention* adottata prevede per il documento vero e proprio la denominazione prescritta da AgID (es. `mydoc.pdf.p7m`) e per la marca temporale lo stesso nome con l'ulteriore estensione .tsr (es. `mydoc.pdf.p7m.tsr`).
  Poiché i due file hanno lo stesso nome ***DigitalSign*** trova immediatamente la marca temporale al momento di aprire il file principale (ovviamente a condizione che i due file siano memorizzati nella stessa cartella).

- **Detached base64 TS (*.* & *.tsr)**
  Del tutto analoga alla modalità precedente, ma entrambi i file sono espressi in formato base64. I nomi dei file sono gli stessi del caso precedente.

3.9.3 La cifratura dei contenuti in DigitalSign

DigitalSign supporta la cifratura dei contenuti creando una specifica busta crittografica dedicata a questo scopo: un file con estensione '.p7e' contiene sia le informazioni specifiche per consentire la decifratura a chi dispone degli strumenti per farlo, sia il contenuto cifrato.

Il contenuto può essere un file di qualunque tipo, firmato o meno.

L'algoritmo di cifratura è di tipo misto:

- innanzitutto, viene generata, con un procedimento casuale, una chiave di crittografia simmetrica
- la chiave simmetrica viene usata per cifrare il contenuto del documento
- la stessa chiave simmetrica viene poi cifrata a sua volta usando la chiave pubblica del destinatario; nel caso siano previsti più destinatari questa operazione viene ripetuta per ciascuno di essi. La chiave pubblica di ogni destinatario viene estratta dal relativo certificato (si ricorda che la selezione dei destinatari di cifratura avviene selezionandone i relativi certificati)
- il documento viene confezionato inserendo nella busta crittografica il documento cifrato e tutte le copie cifrate della chiave simmetrica

Il destinatario potrà usare la propria chiave privata per decifrare la chiave simmetrica e quindi potrà usare quest'ultima per decodificare il documento.

NOTA: la crittografia simmetrica è basata sull'algoritmo selezionato a livello di opzioni tra una lista molto nutrita di alternative.
La crittografia asimmetrica attuata sulla chiave simmetrica viene invece eseguita con l'algoritmo supportato dalla chiave pubblica disponibile nel certificato prescelto (di solito RSA 1024 o 2048).

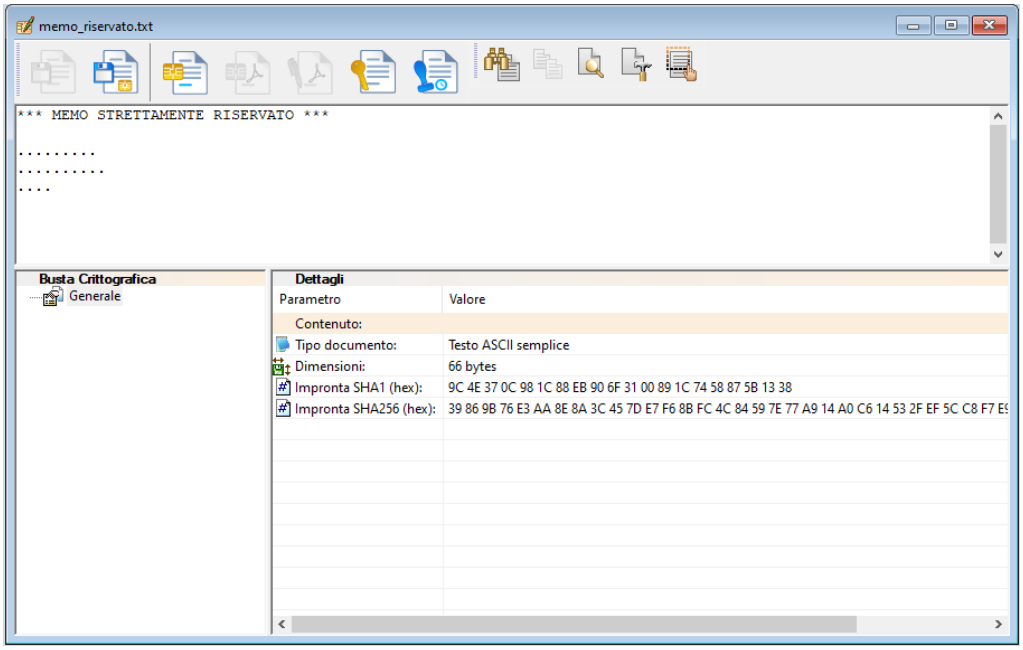
Vediamo un paio di esempi:

3.9.3.1 esempio: trasmissione documenti riservati

Alcuni enti richiedono che documenti confidenziali siano trasmessi in forma cifrata, mettendo a disposizione un loro certificato per la cifratura.

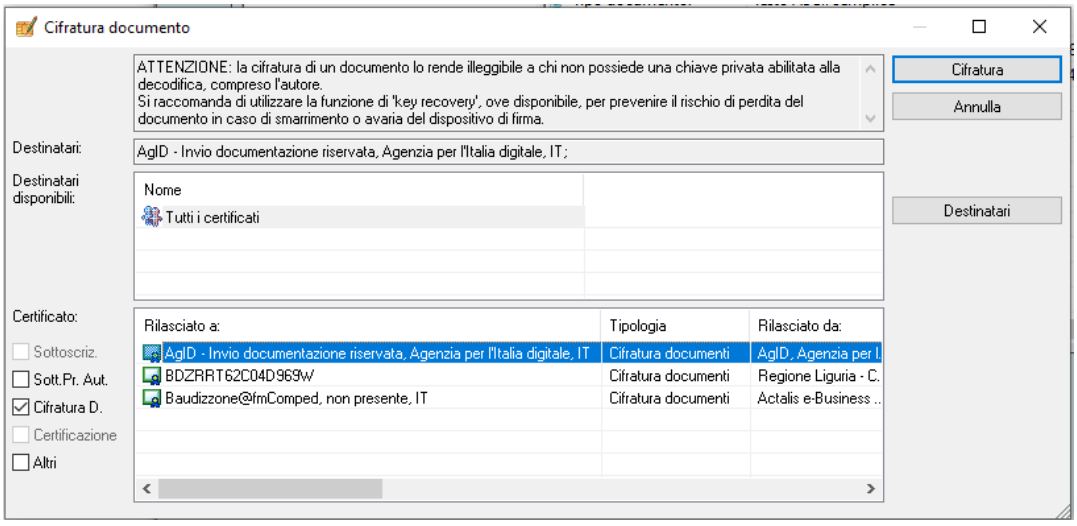
In precedenza, lo avremo importato nel DB dei certificati.

Inseriamo una smartcard che contenga un certificato idoneo alla cifratura (o carichiamo un PKCS#12, si veda la sezione dedicata), quindi apriamo il documento riservato:

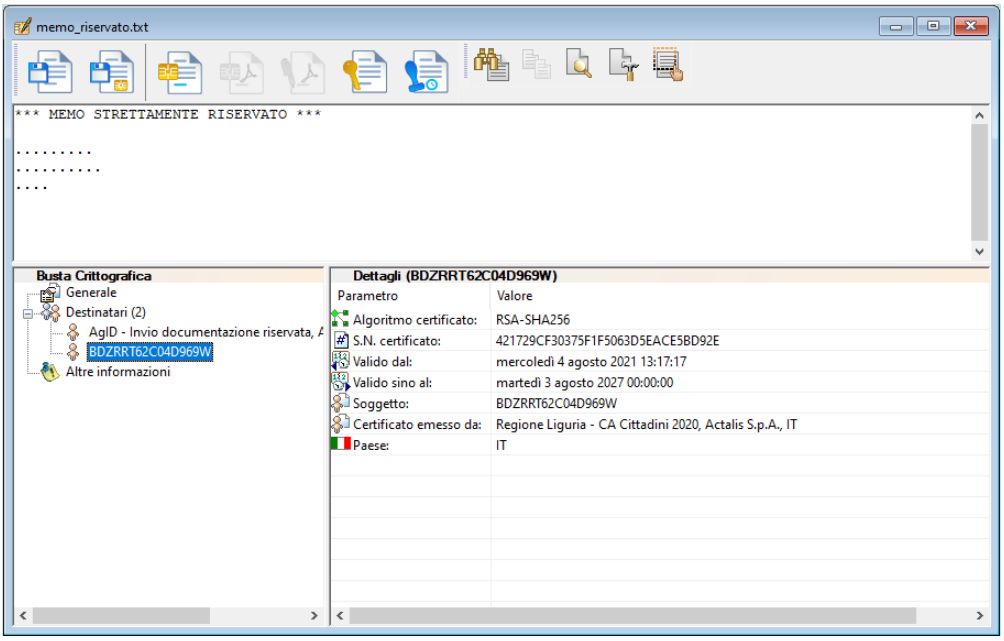


Ora facciamo click sul bottone  (corrispondente a Documento -> Destinatario cifratura)

Dalla finestra che si apre scegliamo il certificato da usare:



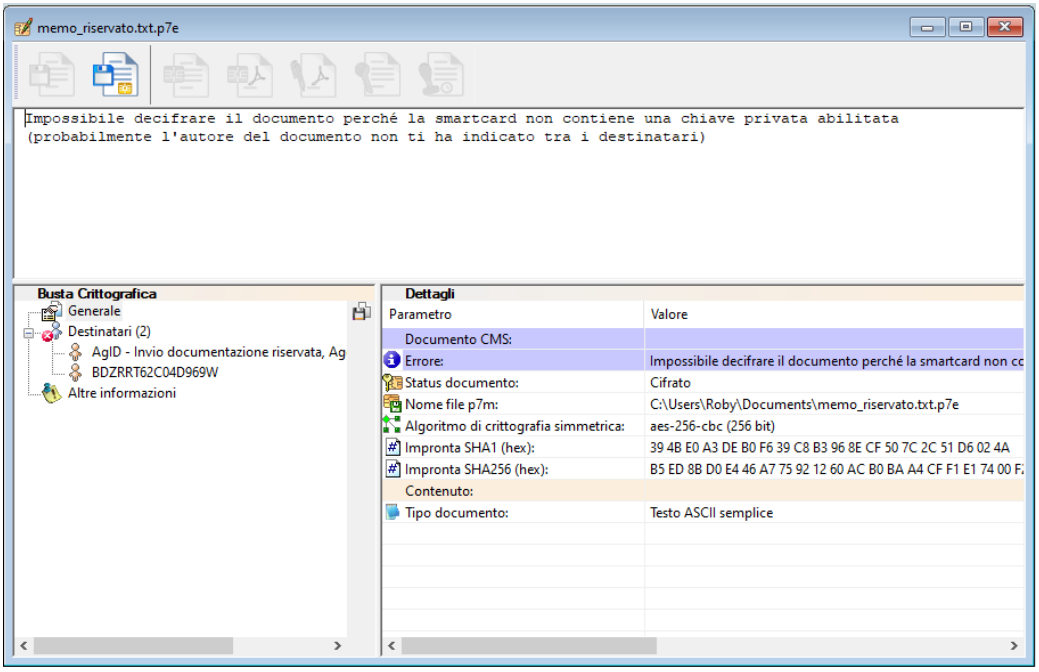
Confermando con il bottone **Cifratura** vedremo comporre la busta crittografica:



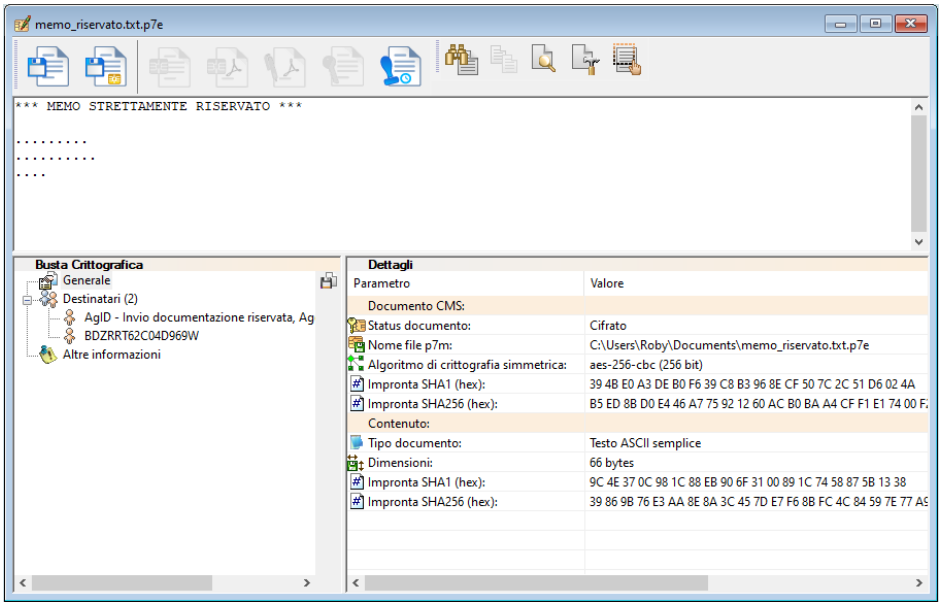
Si noti che, oltre al certificato che abbiamo appena scelto, il sistema include anche il nostro certificato (per questo dobbiamo effettuare questa operazione avendo inserito una smartcard contenente un certificato valido per la cifratura).
Questo serve ad evitare che, appena conclusa l'operazione, perdiamo la possibilità di leggere il contenuto.

Salviamo il documento, che si chiamerà `memo_riservato.txt.p7e`
Possiamo a questo punto trasmetterlo (via mail o per qualunque altro canale) al destinatario, senza rischiare che qualcuno possa leggerne il contenuto.

Se proveremo ad aprire questo documento SENZA una smartcard o con una smartcard diversa da quella usata per cifrarlo:



Ma se lo faremo con la smartcard corretta, dopo aver inserito il PIN:



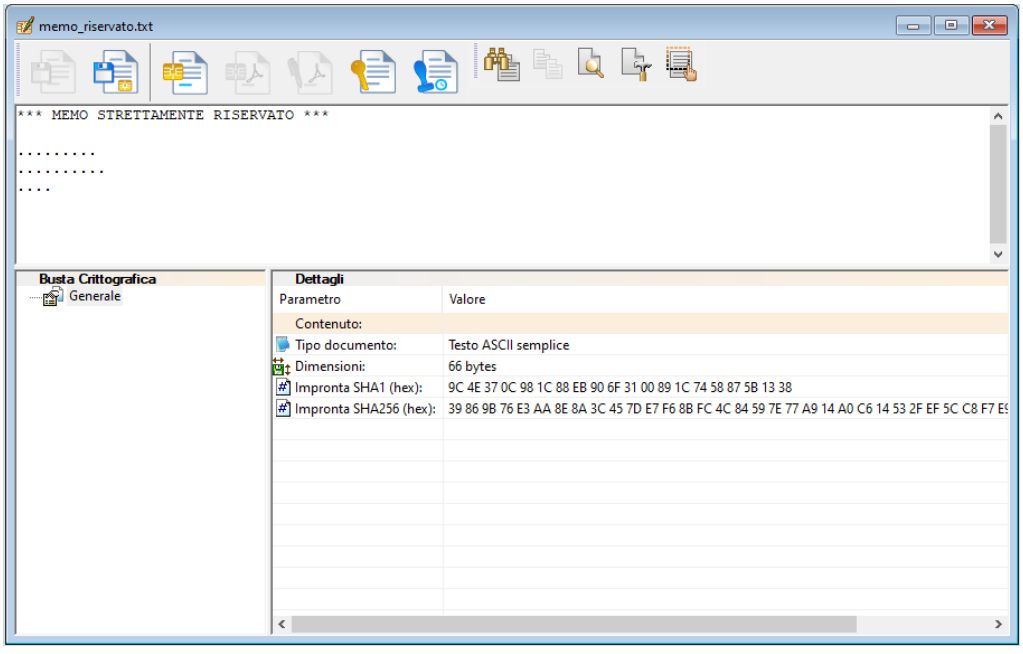
3.9.3.2 esempio: protezione di un nostro documento riservato

Supponiamo di voler mantenere, a lungo, alcuni documenti che consideriamo riservati.
Oltre all'ovvia protezione di tali documenti in termini di accesso, con le opportune misure a livello di file system, isolamento e quant'altro, possiamo cifrare il contenuto.

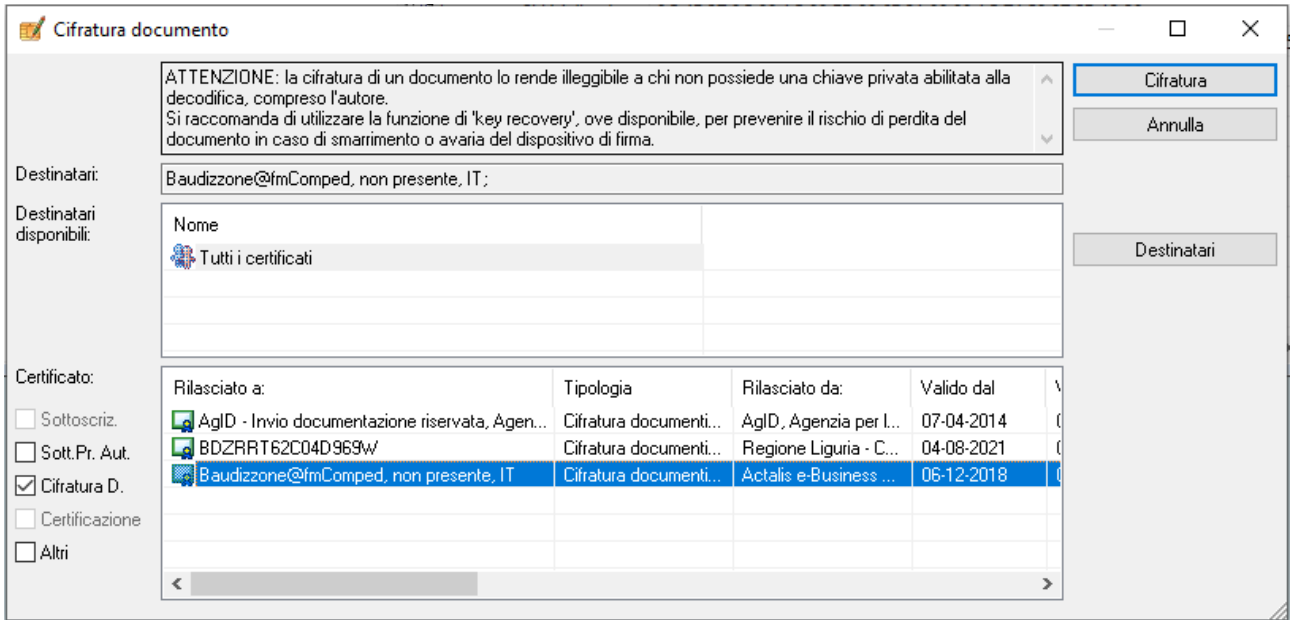
Poiché ci serve poter accedere ai documenti anche a distanza di molto tempo preferiamo evitare di usare una chiave contenuta in una smartcard, per decifrare, considerando che la smartcard potrebbe guastarsi o – tra qualche anno – potrebbe essere difficile interfacciarla su un computer dalle caratteristiche molto diverse da quelle odierne.

Usiamo allora un certificato e una chiave privata contenuti in un container PKCS#12, che provvediamo a importare nel sistema seguendo le istruzioni della sezione dedicata.

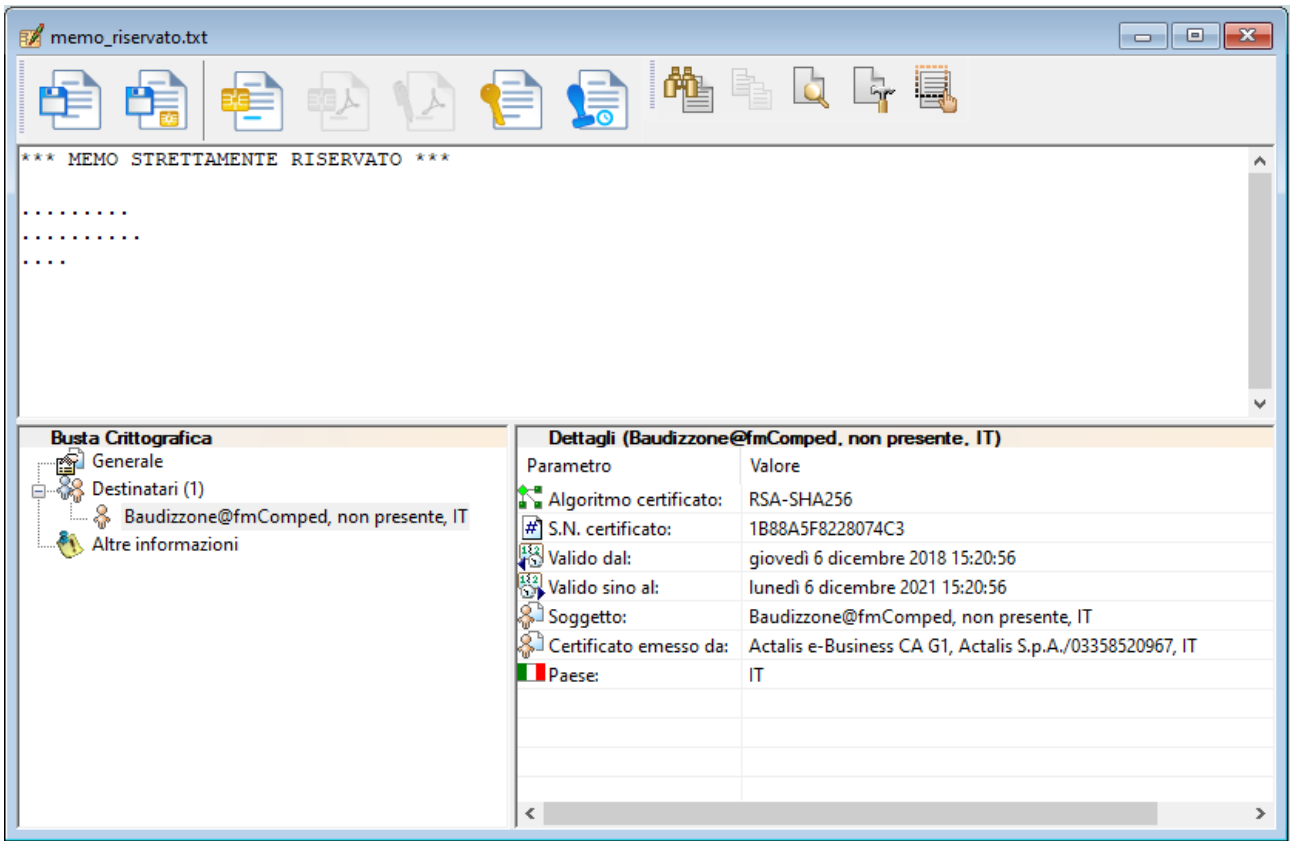
Come prima, apriamo il documento da cifrare:



Come prima, scegliamo il destinatario, ma stavolta selezioniamo il nostro certificato:



Questa volta vedremo una busta con un solo destinatario:



La ragione è che abbiamo selezionato come destinatario lo stesso certificato associato alla smartcard che stiamo usando.

Anche in questo caso salviamo il documento con un nome arbitrario: `memo_riservato_interno.txt.p7e`

Per riaprire il documento dovremo avere a disposizione la chiave privata che corrisponde al certificato prescelto. Ricordiamo che stavolta non era una chiave fisicamente memorizzata in una smartcard, ma solo caricata nel sistema tramite il Caricamento file PKCS#12.

Questo significa che, se il file è ancora caricato e stiamo operando sullo stesso computer, basterà inserire qualunque smartcard per poterlo aprire.
Altrimenti dovremo ripetere il caricamento dello stesso file PKCS#12, fornendo la relativa password.

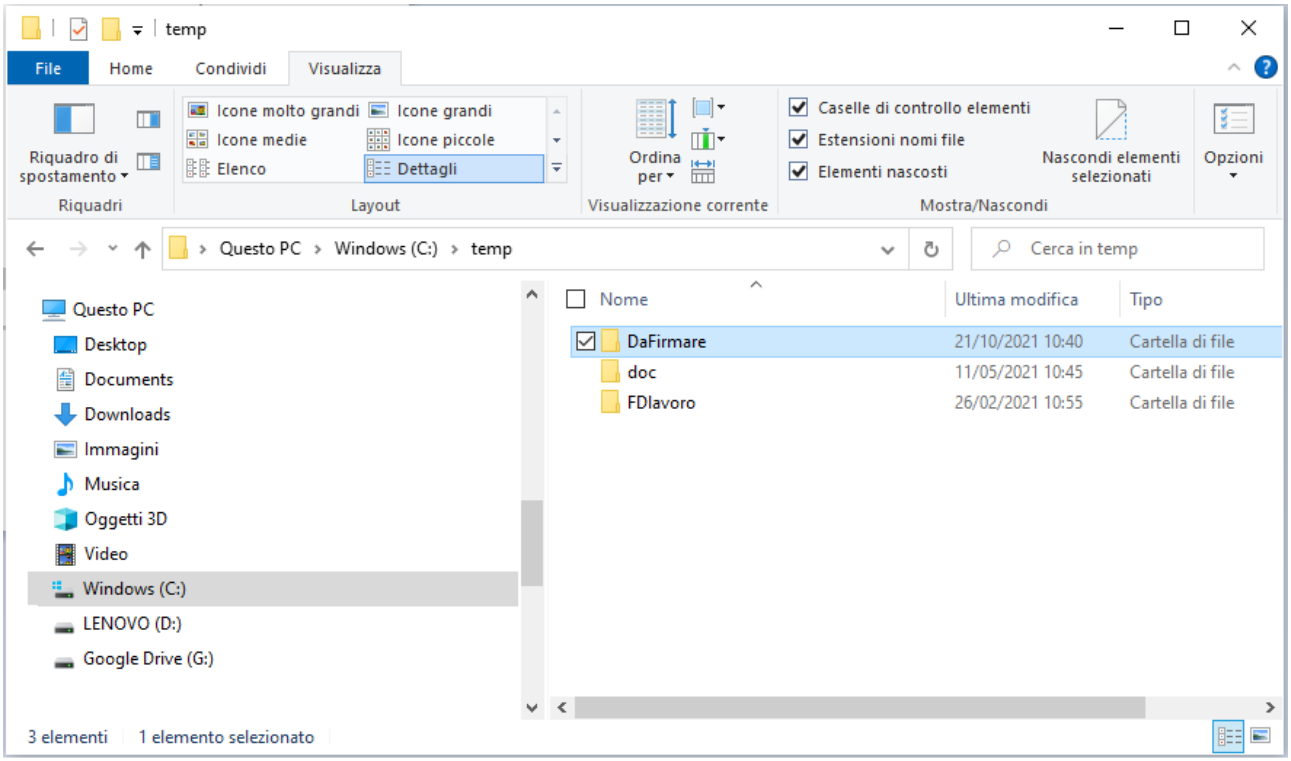
NOTA IMPORTANTE: cifrare un documento con ***DigitalSign*** significa che produciamo una nuova versione cifrata del documento stesso, ma la versione originale resta inalterata.

Dopo la cifratura è possibile usare la funzione Documento -> Wipe file per eliminare il documento di partenza.
Si legga la nota in calce alla sezione appena indicata per una discussione sui limiti di questo approccio.

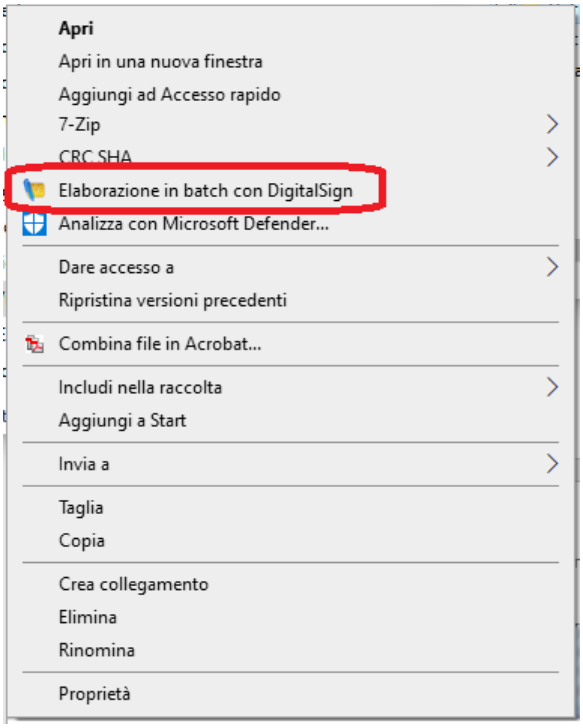
3.9.4 Firma semiautomatica dalla *shell* di Windows

Se dal menu di Strumenti -> Opzioni, dal tab Associazioni, viene opportunamente abilitata l'opzione **Tutti gli altri tipi**, ***DigitalSign*** offrirà dalla *shell* di Windows la possibilità di attivare direttamente la firma semiautomatica di tutti i documenti presenti in una data cartella, sfruttando la funzionalità di Elaborazione Automatica.

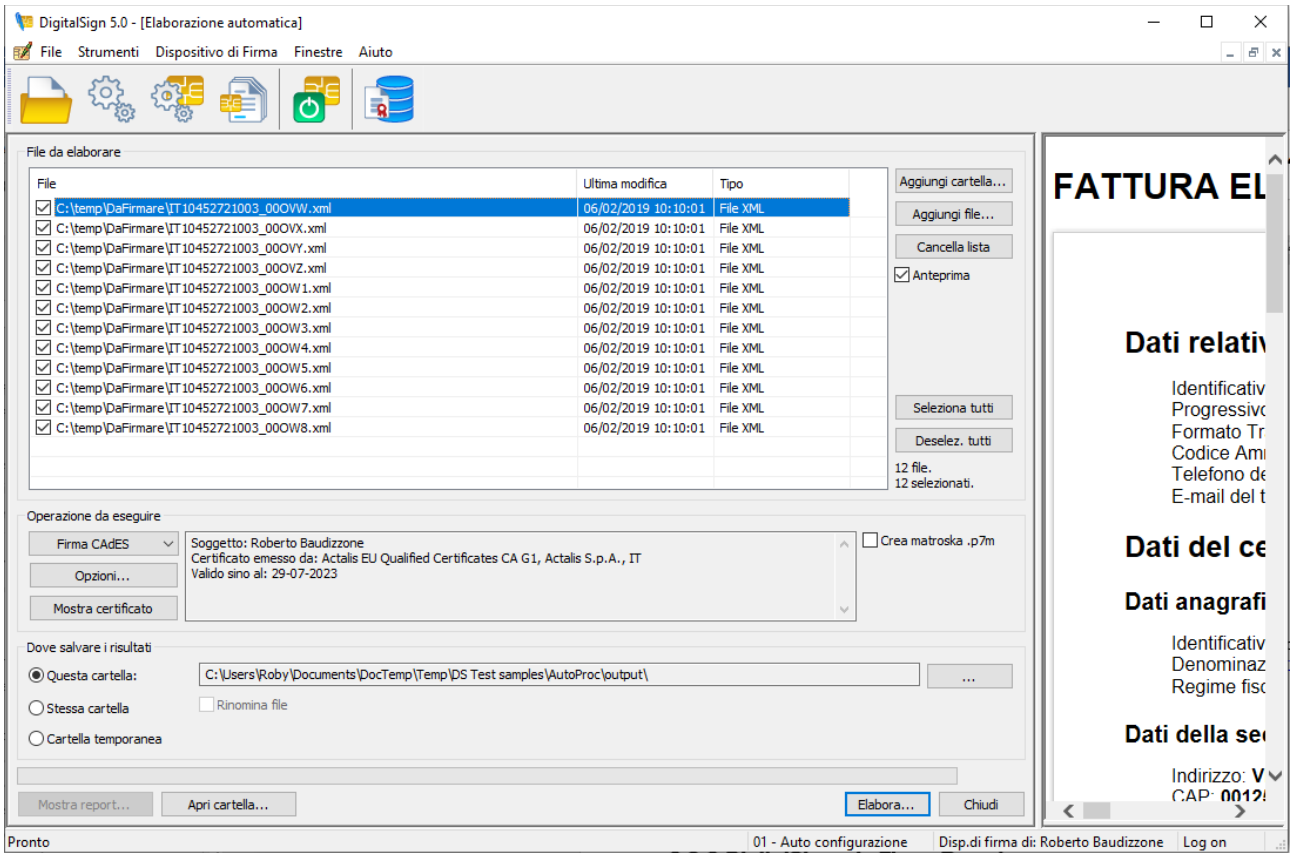
Operando da una normale visualizzazione di Windows Explorer, si localizzi la cartella su cui agire:



Quindi, facendo click con il tasto destro del mouse sulla cartella (nel nostro caso **Da Firmare**) si vedrà un menu proprio di Windows. Il contenuto effettivo del nostro menu dipende dalle applicazioni che abbiamo installato:



Selezionando ora **Elaborazione in batch con DigitalSign** si avvierà ***DigitalSign*** (se non è già attivo) e si passa automaticamente alla schermata corrispondente alla voce del menu File -> Elaborazione Automatica, con la selezione dei file su cui operare già completata:



3.9.5 Costruire un Elenco di CA attendibili definito dall'utente

Come illustrato a proposito del processo di verifica di una firma e delle Opzioni di Security -> Firma e Verifica, ***DigitalSign*** dovrebbe essere sempre configurato ad operare in modalità **STRONG** per la verifica di firme e certificati.
Questa scelta aumenta notevolmente il grado di attendibilità delle verifiche, ma richiede la disponibilità di un punto di riferimento (si veda il tab CA Accreditate e Attendibili delle stesse Opzioni di Security).

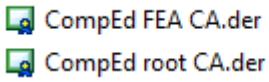
Fintanto che verifichiamo firme emesse con Certificati Qualificati o con i certificati contenuti nelle CNS possiamo contare, per questo, sull'infrastruttura delle TSL distribuite in Unione Europea.
Ma se dobbiamo usare/verificare certificati prodotti con CA private (ad esempio per la Firma Elettronica Avanzata o per la firma grafometrica) sarà necessario predisporre un DB di CA attendibili.

Tale DB deve presentare alcune caratteristiche fondamentali:

1. essere costruito nel formato '`.DSCStore`' (lo stesso del DB locale dei certificati);
2. essere firmato digitalmente in formato CAdES con un certificato qualificato;
3. essere pubblicato a un indirizzo web raggiungibile

In questa sezione illustriamo come procedere praticamente per raggiungere l'obiettivo (assumendo che si disponga di un server web e si abbia la possibilità di caricare il file risultante in una posizione raggiungibile)

Esempio: abbiamo predisposto un sistema di Firma Elettronica Avanzata basata sui servizi di ***DigitalSign Cloud***; tale sistema prevede una CA root a nome di CompEd e poi diversi "domini" per le organizzazioni clienti, ciascuna delle quali ha una propria CA intermedia, emessa dalla CA root (anche questo, nel nostro esempio, a nome di CompEd, ma altri clienti hanno questa CA intermedia a proprio nome):



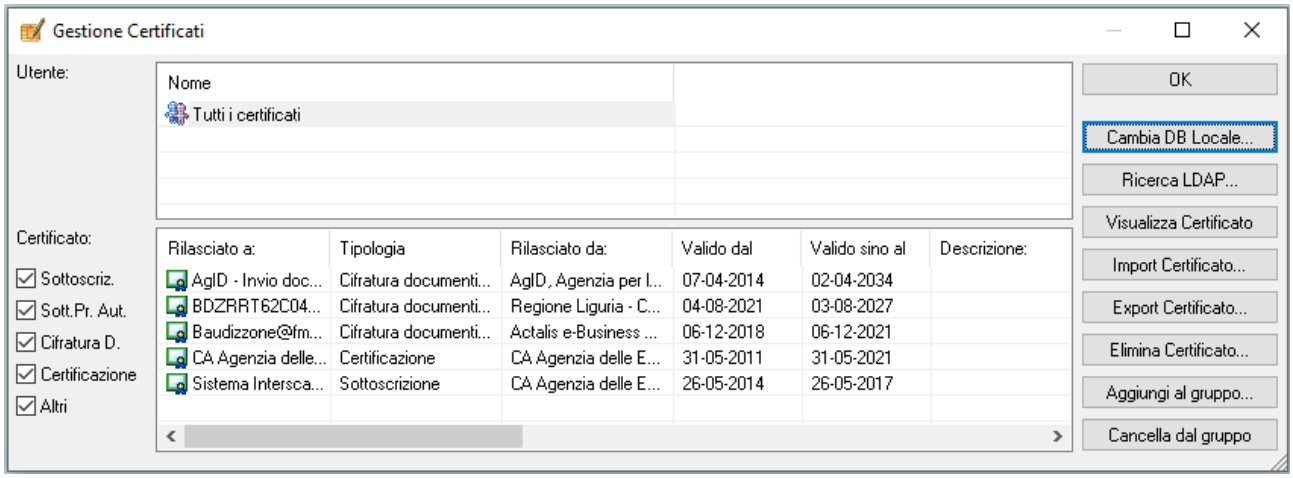
Al fine di verificare positivamente in ***DigitalSign*** le firme generate da tale sistema (quindi da parte di sottoscrittori in possesso di certificati FEA emessi dalla `CompEd FEA CA`, a sua volta emesso dalla `CompEd root CA`) occorre predisporre un DB contenente questi due certificati.

Procediamo:

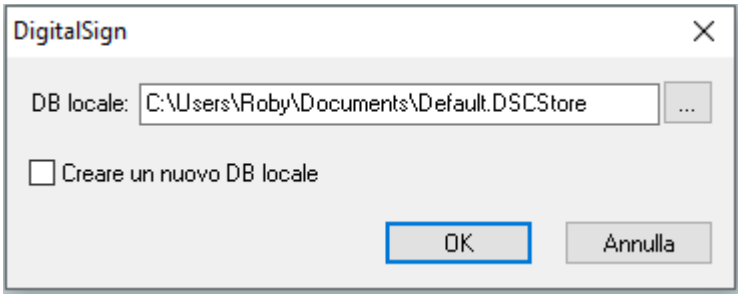
3.9.5.1 impostare un DB locale vuoto

Poiché il nostro DB autenticato dovrà avere lo stesso formato '.DSCStore' del DB locale dei certificati, sfruttiamo le funzioni di gestione di ***DigitalSign***.

Strumenti -> Gestione DB Locale

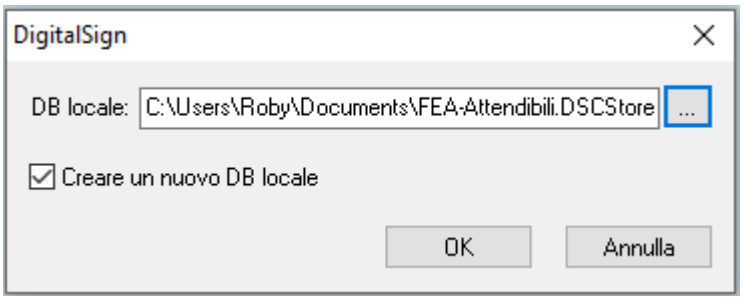


Da qui usiamo il bottone **Cambia DB Locale**:

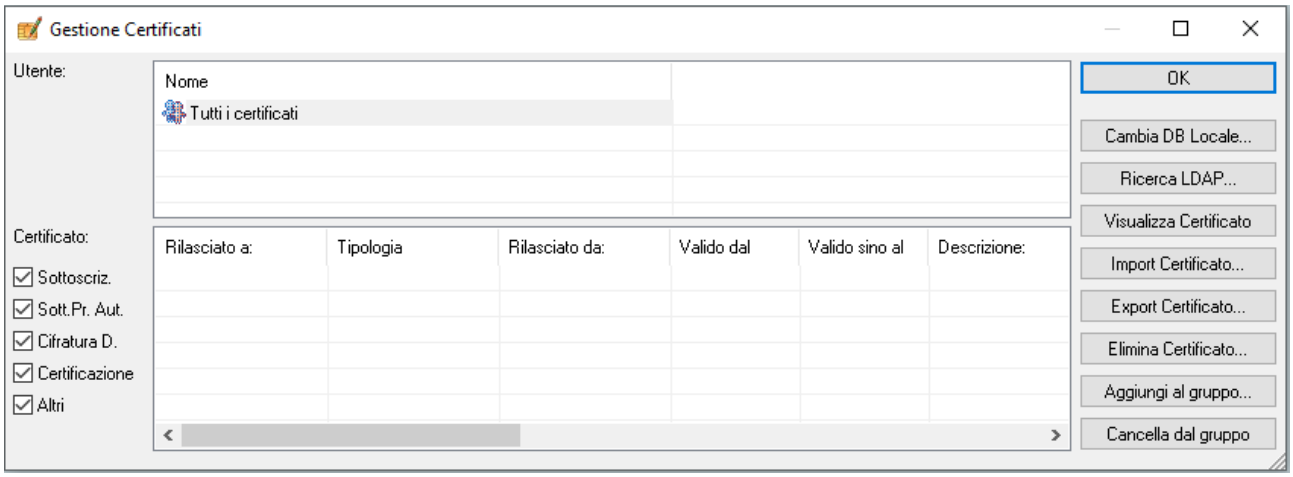


È **IMPORTANTE** annotare il percorso attuale del DB locale in uso, al fine di poterlo ripristinare a operazioni concluse.

Scegliamo un percorso e un nuovo nome (qui noi abbiamo scelto `FEA-Attendibili`), settando anche il checkbox **Creare un nuovo DB locale**:

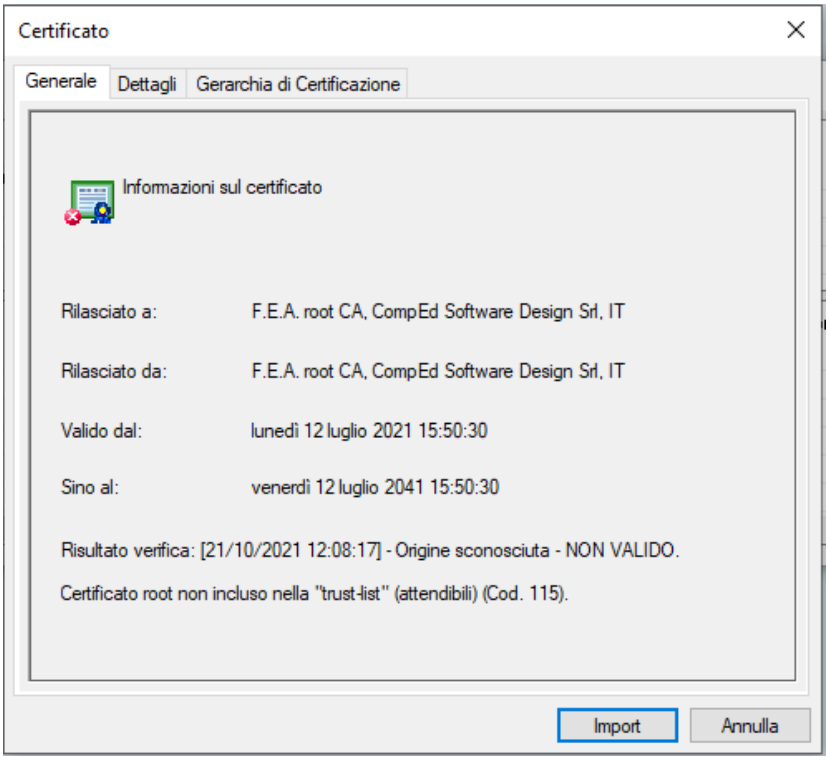


Premendo il bottone **OK** vediamo il nuovo DB vuoto:



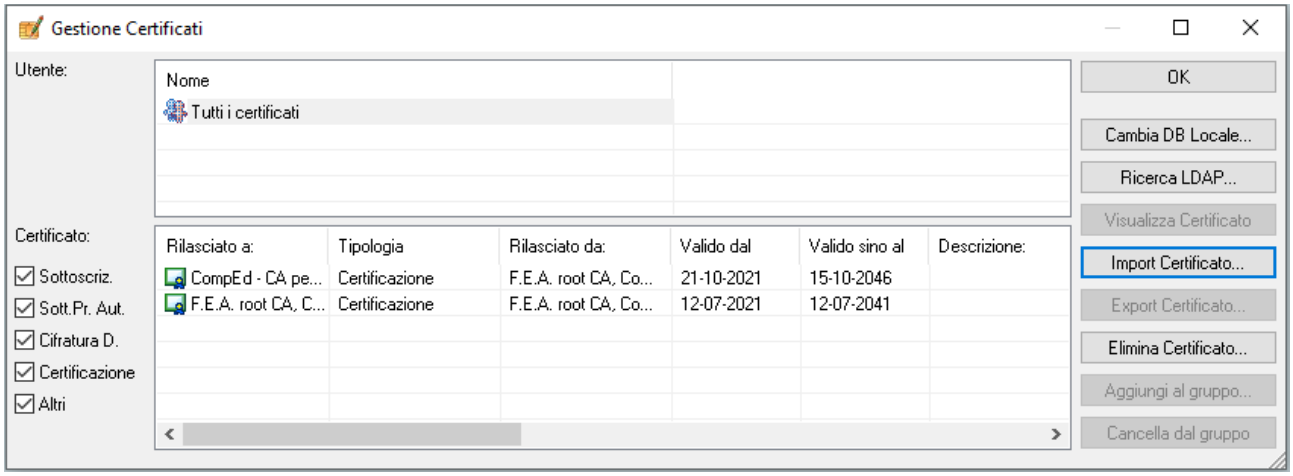
3.9.5.2 importare i certificati di CA

Ora usiamo il bottone Import certificato per importare, uno dopo l'altro i due certificati di CA:



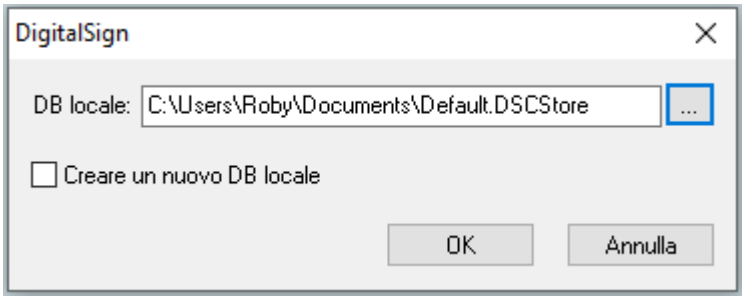
DigitalSign mostra il certificato che abbiamo chiesto di importare e segnala che non è valido perché non ne conosce l'origine (è corretto, stiamo insegnandogli ora a fidarsi di questo certificato). Premiamo **Import** e confermiamo di voler procedere anche se il certificato non è valido.

Dopo aver ripetuto l'operazione con entrambi i certificati avremo questa situazione:

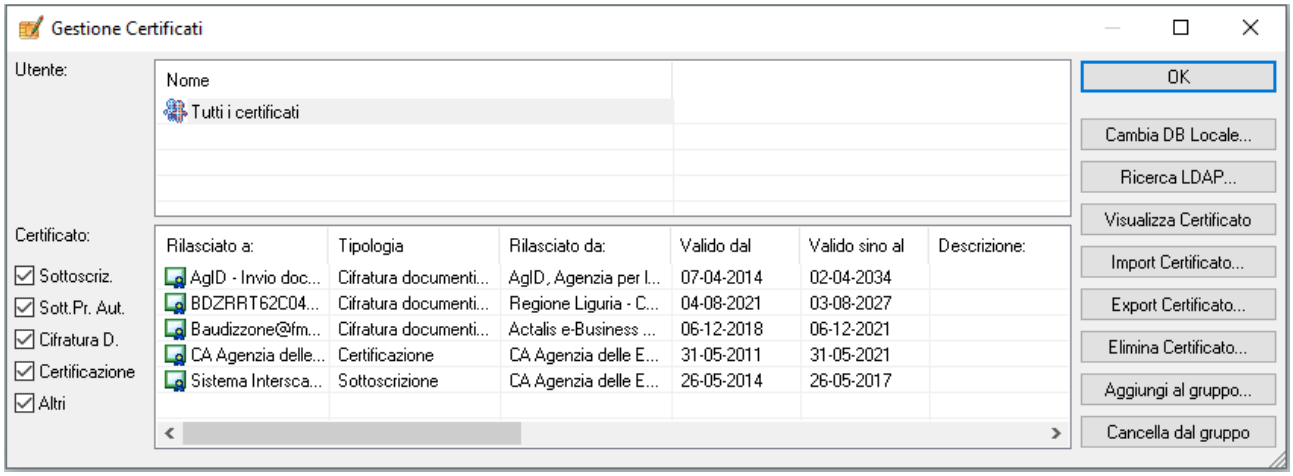


3.9.5.3 ripristino del DB locale originario

Abbiamo completato la predisposizione del DB, ora possiamo tornare al DB che usavamo in precedenza: usiamo il bottone **Cambia DB Locale** e selezioniamo il file di cui avevamo annotato il percorso, senza selezionare il checkbox **Creare un nuovo DB locale**:



Con **OK** torniamo alle condizioni precedenti:

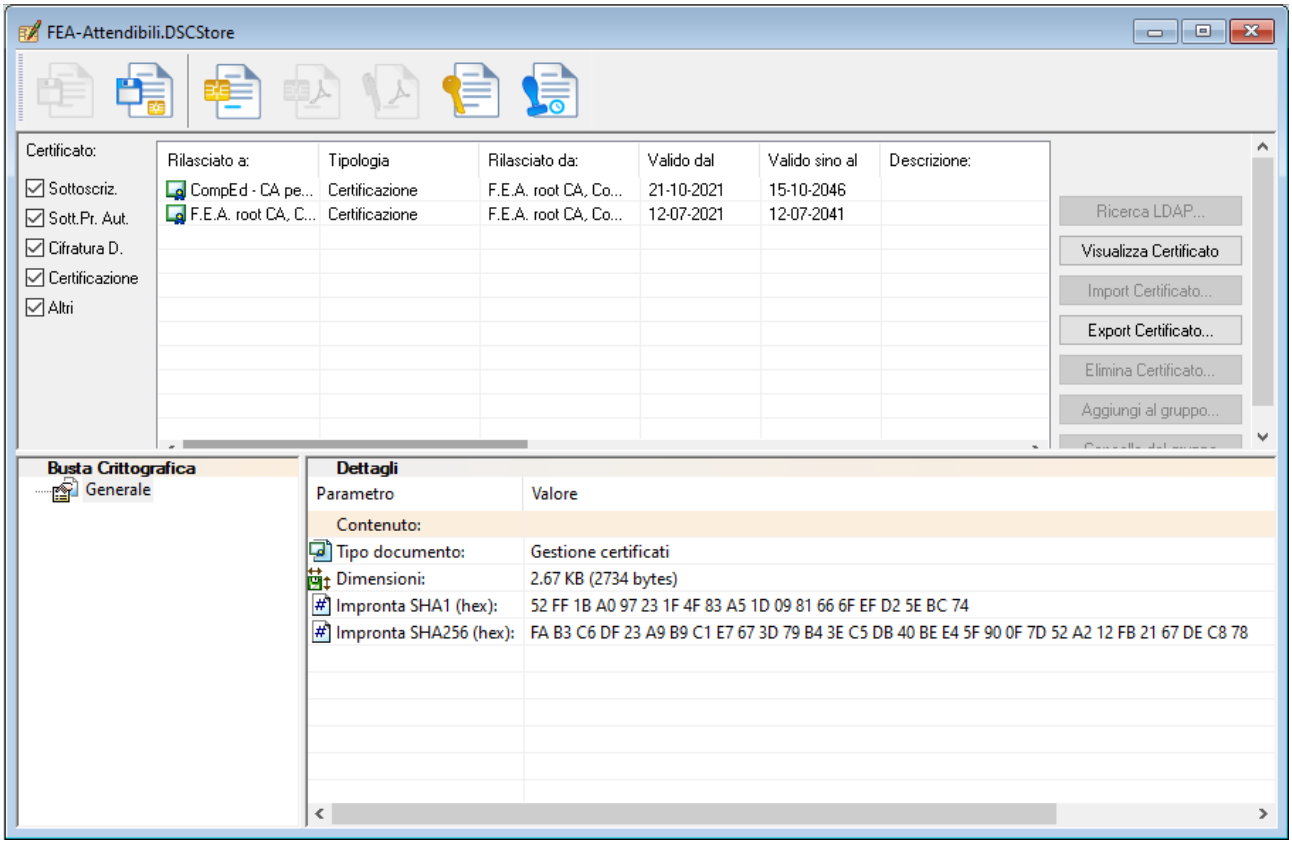


3.9.5.4 firmare digitalmente il DB

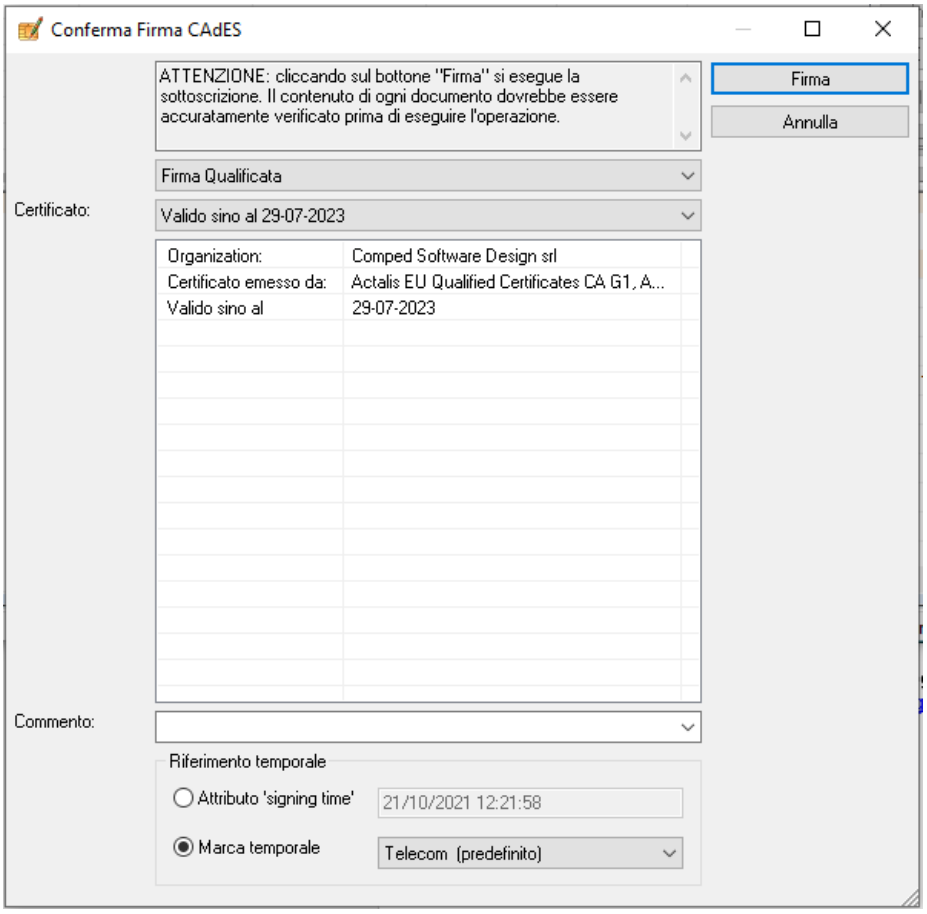
Per far sì che ***DigitalSign*** consideri attendibile un DB di CA occorre che tale DB sia firmato digitalmente con un certificato qualificato.

NOTA IMPORTANTE: Se lo scopo è quello di far considerare attendibile i certificati FEA ad un'intera organizzazione sarà opportuno che questa firma sia apposta da un responsabile di alto livello (un Amministratore Delegato, un Responsabile dei Sistemi Informativi…): ***DigitalSign*** dichiarerà sempre in modo esplicito il nominativo del soggetto che ha firmato il DB.

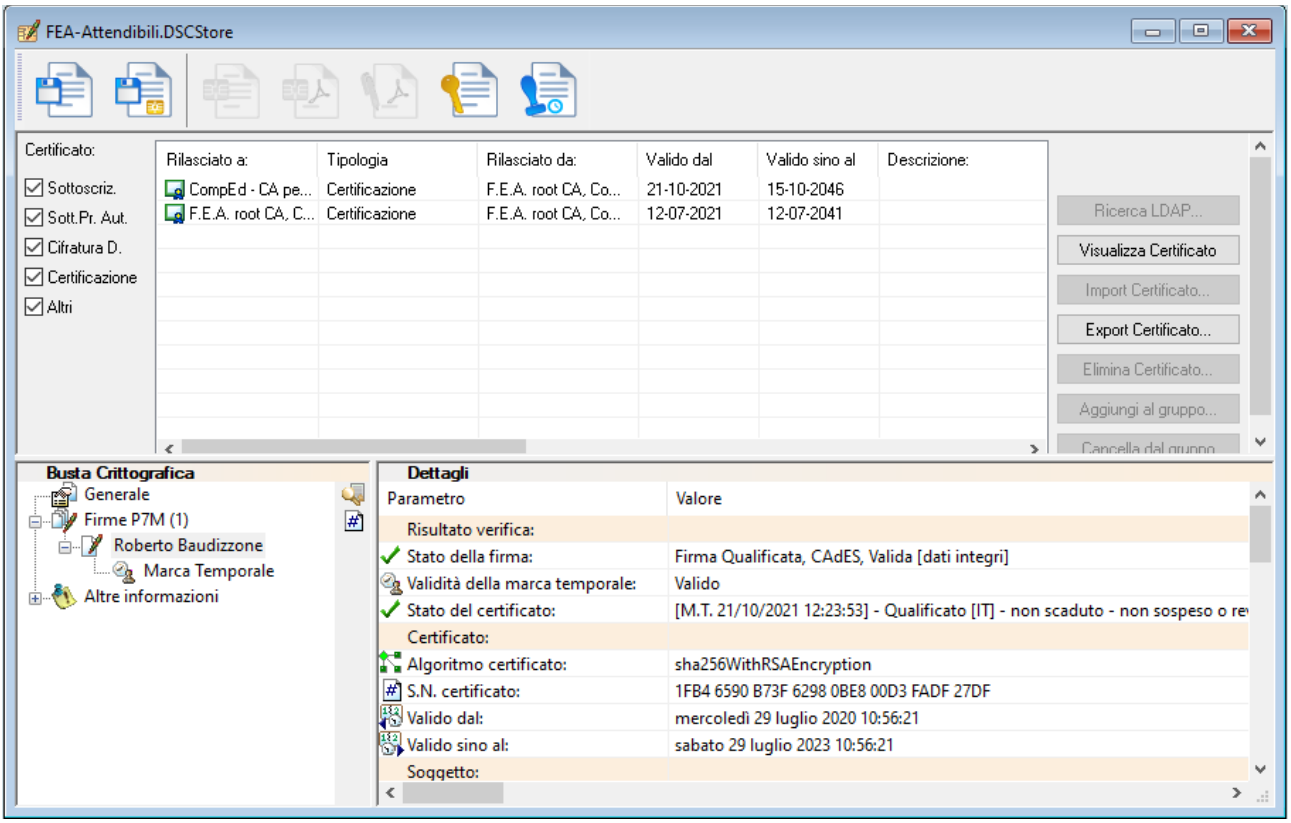
Usiamo la funzione File -> Apri Documento e selezioniamo il file `FEA-Attendibili.DSCStore` appena costruito:



DigitalSign ha già predisposto una busta crittografica, mostrandoci il contenuto del DB.
Usiamo la funzione del menu Documento -> Aggiungi firma CAdES:



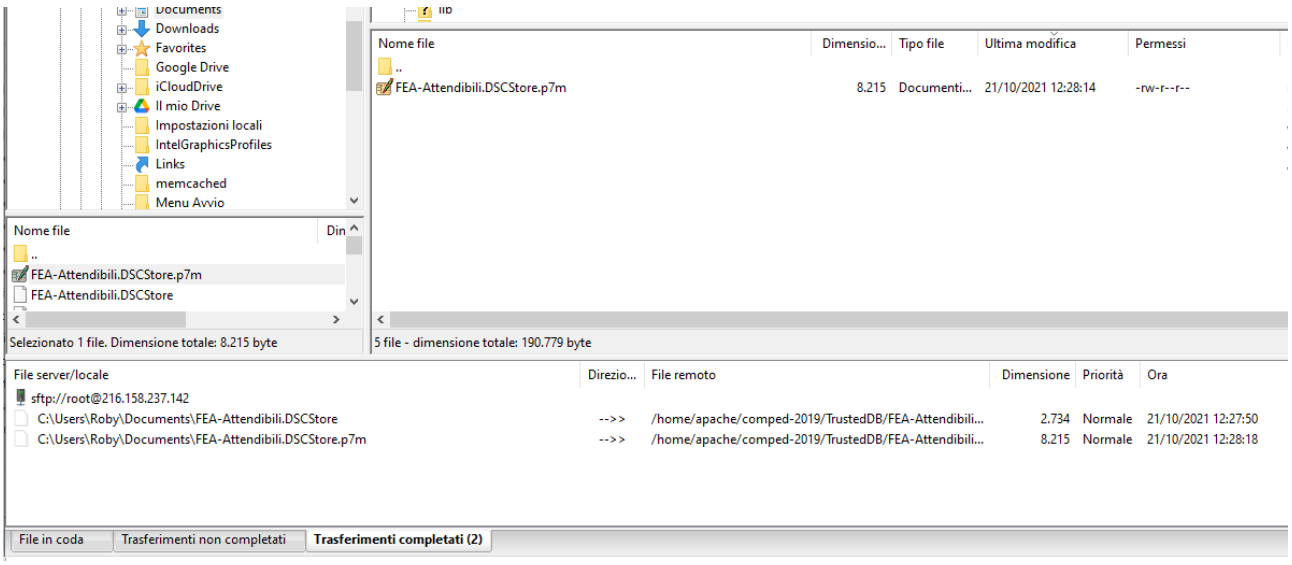
In questo caso è molto opportuno associare una Marca Temporale alla firma: così facendo il nostro DB sarà considerato attendibile per 20 anni, a prescindere dalla scadenza del certificato qualificato che stiamo usando per firmarlo:



Ora Salviamo il documento con il nome `FEA-Attendibili.DSCStore.p7m`

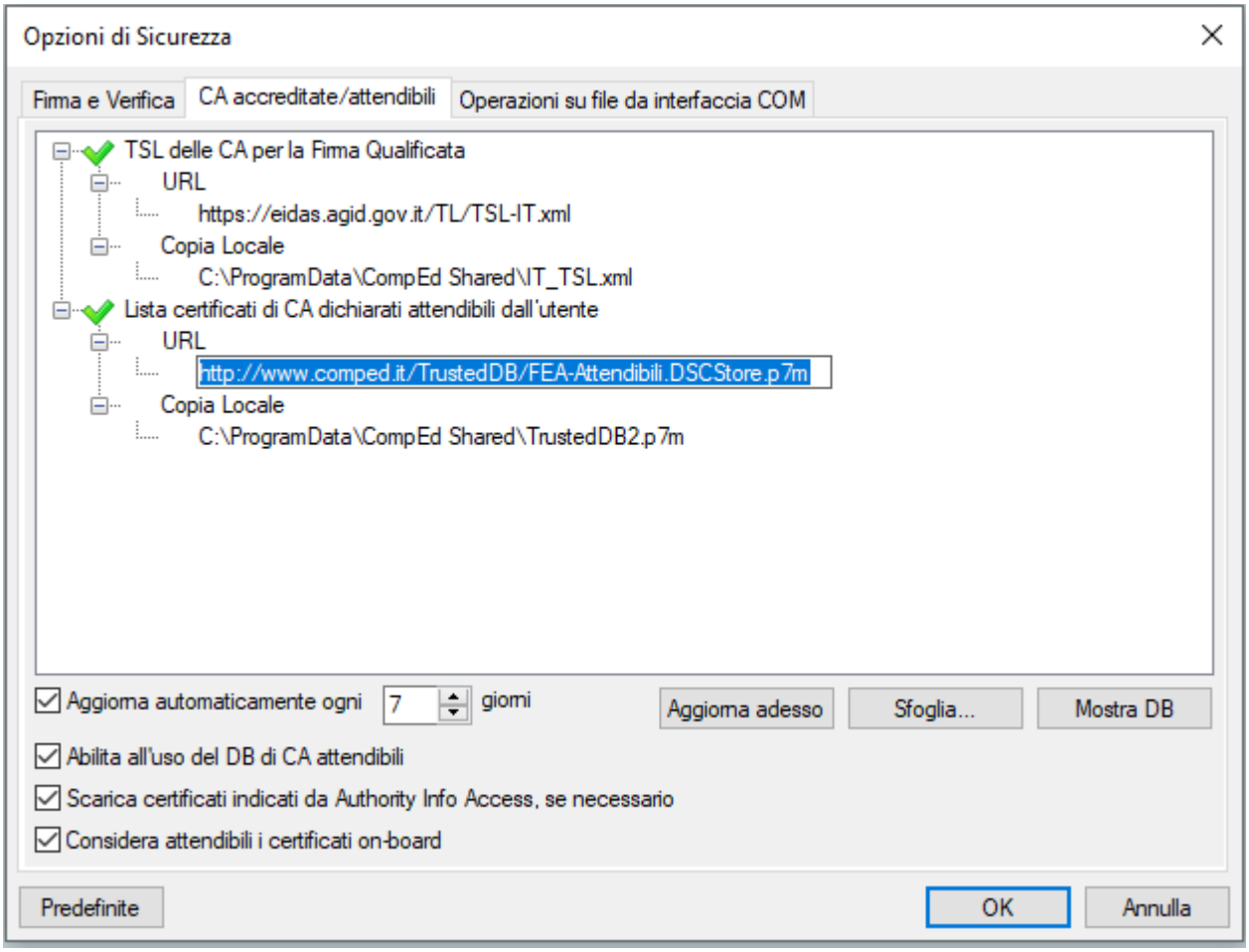
3.9.5.5 pubblicazione su sito web

Questa operazione dipende dalle modalità con cui gestiamo il nostro sito.
Nel nostro caso abbiamo una cartella dedicata www.comped.it/TrustedDB e usiamo un client FTP per pubblicarlo:



3.9.5.6 impostazione del DB di CA attendibili sulle copie interessate di DigitalSign

Dal menu Strumenti -> Opzioni di Security selezioniamo il tab CA Accreditate/Attendibili:

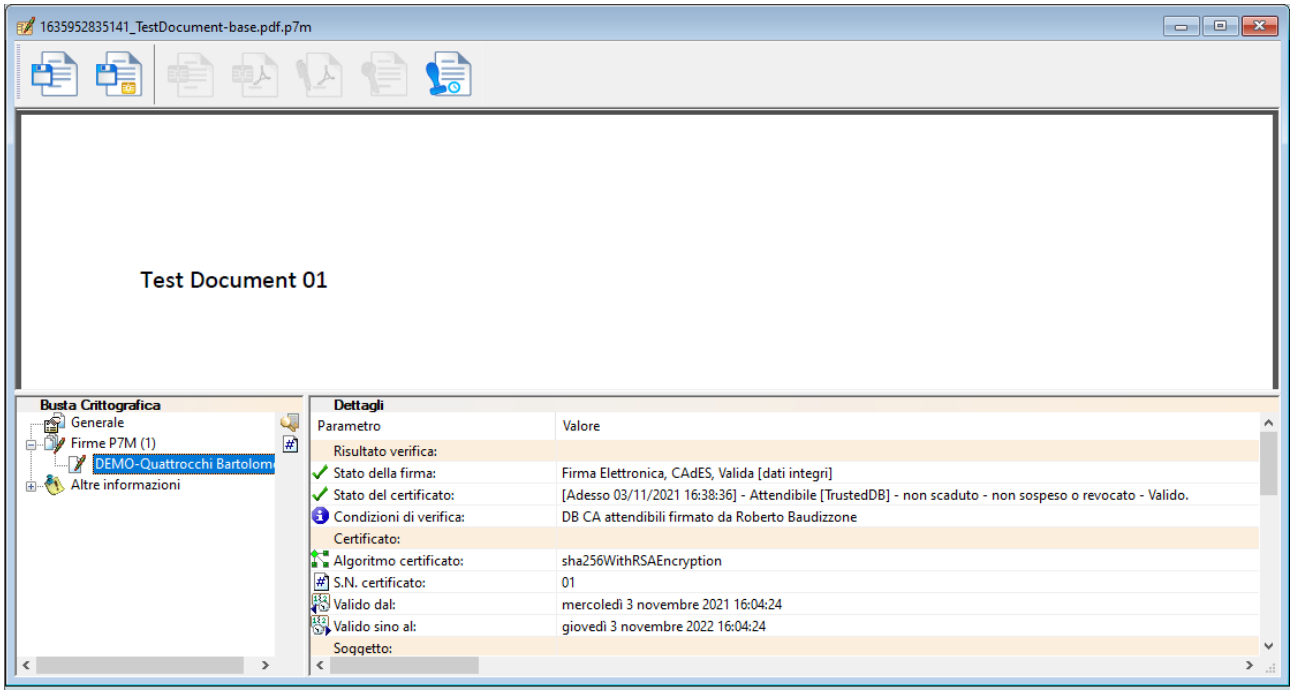


Qui selezioniamo il checkbox **Abilita all'uso del DB di CA attendibili**, quindi facciamo doppio click sulla URL e riportiamo l'indirizzo web del nostro file.

Con **Aggiorna Adesso** istruiamo ***DigitalSign*** a caricare l'elenco.
Con **Mostra DB** ne vediamo il contenuto.

3.9.5.7 Verifica di un documento firmato con un certificato emesso da questa CA

Se verifichiamo con ***DigitalSign*** un documento firmato con un certificato emesso da questa CA vedremo:



Qui vediamo che il certificato è dichiarato "Attendibile" tramite il TrustedDB. E che il DB delle CA attendibili è considerato tale perché firmato (con un certificato qualificato) da Roberto Baudizzone.

3.9.6 DigitalSign e la Firma Remota

DigitalSign è progettato per l'utilizzo combinato con dispositivi di firma pienamente conformi con la normativa sulla firma digitale qualificata, tutti compatibili con lo standard PKCS#11.
In ambiente Windows questo significa che l'applicazione di firma (***DigitalSign***, nel nostro caso) opera l'interfacciamento attivando una DLL che implementa l'interfaccia PKCS#11 per una certa tipologia di smartcard. Sarà poi la DLL, dall'altro lato, a convertire le azioni in comandi e interrogazioni compatibili con il "linguaggio" proprio della smartcard.

Oltre ai tradizionali dispositivi quali smartcard e token USB, oggi esistono sul mercato diversi servizi di "firma digitale remota", pensati per svincolare le attività di firma dal possesso fisico di un dispositivo elettronico personale.

Un servizio di questo genere si basa su un sistema server (gestito direttamente da un Certificatore), nel quale vengono concentrati un elevato numero di chiavi e certificati, corrispondenti ad altrettanti utenti, titolari dei certificati.
Un singolo utente si collegherà via Internet a questo server, si identificherà in modo sicuro, trasmetterà l'impronta del documento da firmare ed otterrà in ritorno la firma digitale calcolata dal server stesso.

Purtroppo, i diversi Certificatori non hanno ancora standardizzato le modalità di erogazione di questi servizi, offrendoli quasi tutti in una propria modalità proprietaria.

CompEd, su richiesta, rende possibile connettere ***DigitalSign*** a questo tipo di servizi – ove siano note le specifiche di collegamento e funzionamento – realizzando specifici moduli chiamati **Virtual P11**.

Un **Virtual P11** è un modulo software (una DLL) che può essere visto da ***DigitalSign*** al pari di qualunque altro modulo PKCS#11, ma svolge i propri servizi senza interconnettersi con alcun dispositivo hardware. Si collega invece via Internet – tramite un canale criptato – con il server remoto che eroga il servizio di firma remota.

Uno *slot* (che nel caso di un normale modulo PKCS#11 destinato a interfacciare smartcard corrisponderebbe ad un lettore nel quale possa essere inserita fisicamente una diversa carta), nel caso di un **Virtual P11**, corrisponde ad un diverso profilo, ossia un set di chiavi private/certificato utilizzabile dall'utente.

Un singolo utente del **Virtual P11** può disporre di molteplici slot, proprio come potrebbe avere diverse smartcard.

3.9.6.1 L'autenticazione: concetti fondamentali

La chiave privata per la firma digitale è un oggetto estremamente critico, sul piano della sicurezza. La normativa stessa impone che l'uso di tale oggetto (quindi la possibilità di apporre una firma) debba essere riservato esclusivamente al legittimo titolare.

Nell'ambito dei sistemi ad elevata sicurezza, si postula che un utente possa disporre in linea di principio di tre distinte qualità:

- ***qualcosa che sono*** *(elementi fisici dell'utente, rilevabili dai sistemi biometrici)*
- ***qualcosa che ho*** *(un oggetto ben identificabile nel possesso esclusivo dell'utente)*
- ***qualcosa che so*** *(un segreto personale, come una password o un PIN)*

Una autenticazione forte, ossia un riconoscimento attendibile per l'uso di un oggetto sensibile come la chiave privata di firma, deve basarsi su almeno due di queste qualità.

Nel caso di una smartcard l'autenticazione è basata su:

- il possesso della carta (*qualcosa che ho*)
- la conoscenza di un PIN (*qualcosa che so*)

Nel caso dei sistemi di Firma Remota, dove non è previsto che l'utente possieda direttamente la propria chiave privata contenuta in un dispositivo fisico come una smartcard, l'autenticazione richiede – oltre alla conoscenza di una password – l'introduzione di un codice numerico (OTP = *One Time Password*) ricavato da un altro genere dispositivo fisico in possesso del titolare: si può trattare di un "autenticatore hardware" (ossia un piccolo dispositivo che mostra sul proprio display un valore apparentemente casuale, ma dipendente dallo specifico dispositivo e dall'istante attuale) oppure dal proprio cellulare il cui numero è associato al certificato.

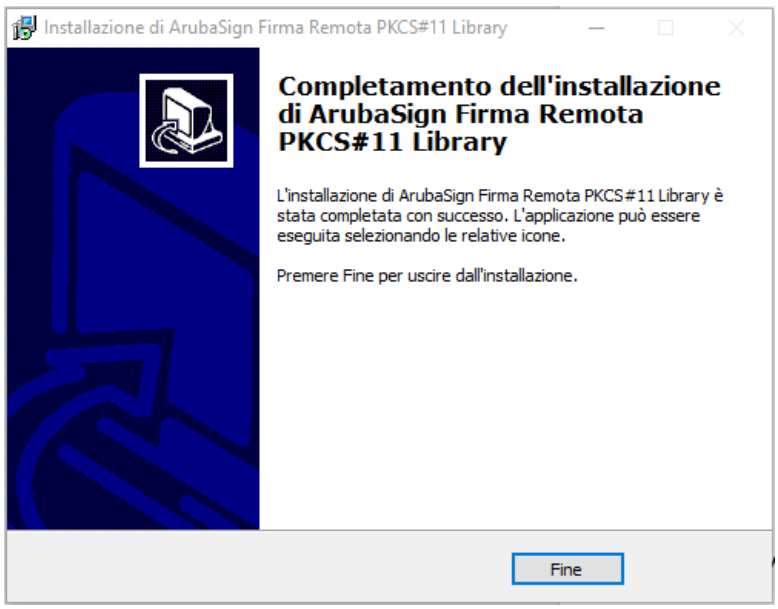
Quando trasmetteremo queste informazioni al server, quest'ultimo potrà verificare il codice OTP e determinare che l'utente è effettivamente in possesso del dispositivo (l'autenticatore hardware, oppure il telefono cellulare) associato all'utenza.

3.9.6.2 Virtual P11 ArubaSign: installazione

L'installazione avviene semplicemente lanciando l'apposito setup, che si presenta come un singolo eseguibile del tipo:

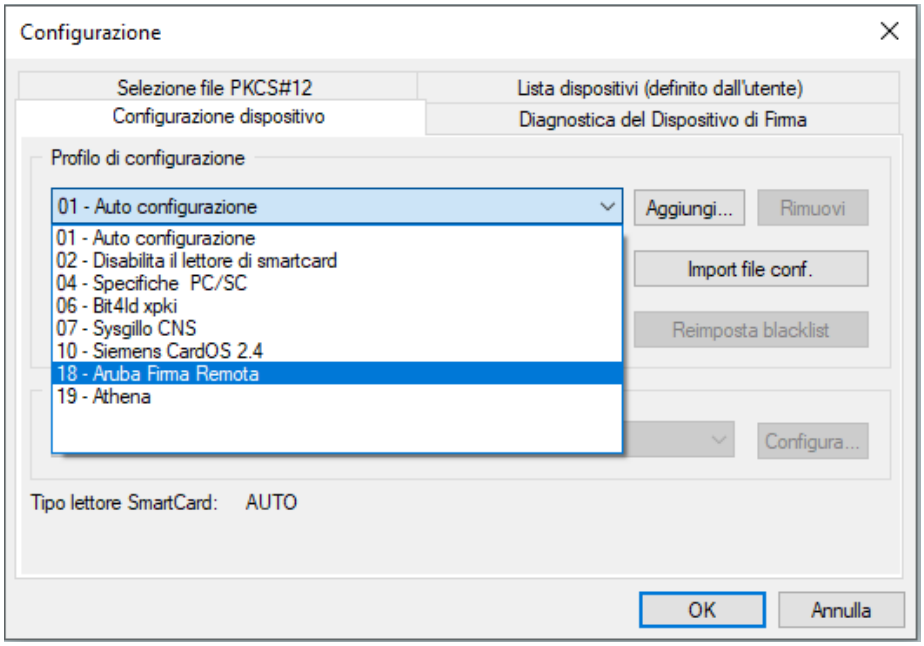
```
as-firma-remota-p11-R86.exe
```

Al termine dell'installazione il modulo sarà utilizzabile da parte di ***DigitalSign***:

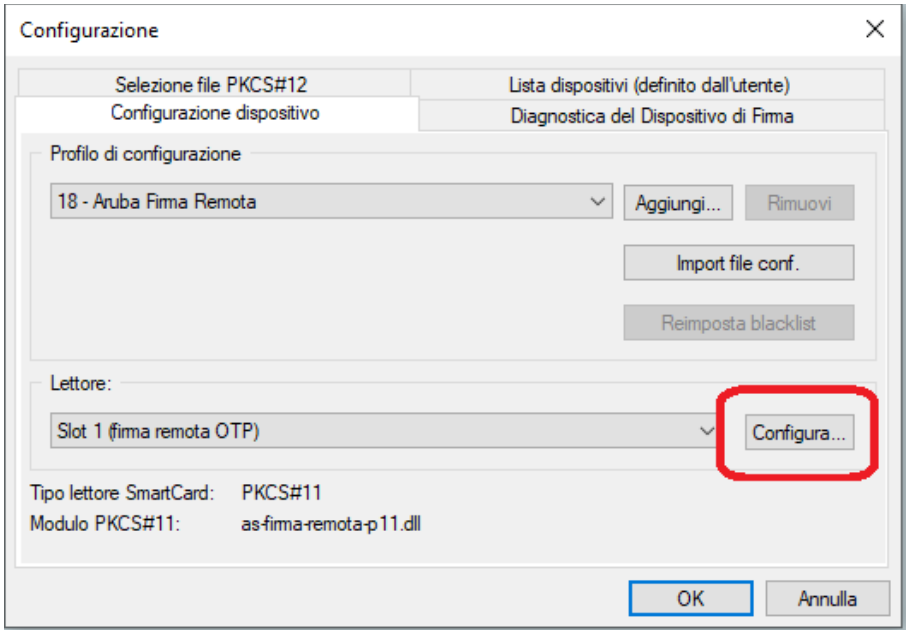


3.9.6.3 Virtual P11 ArubaSign: configurazione

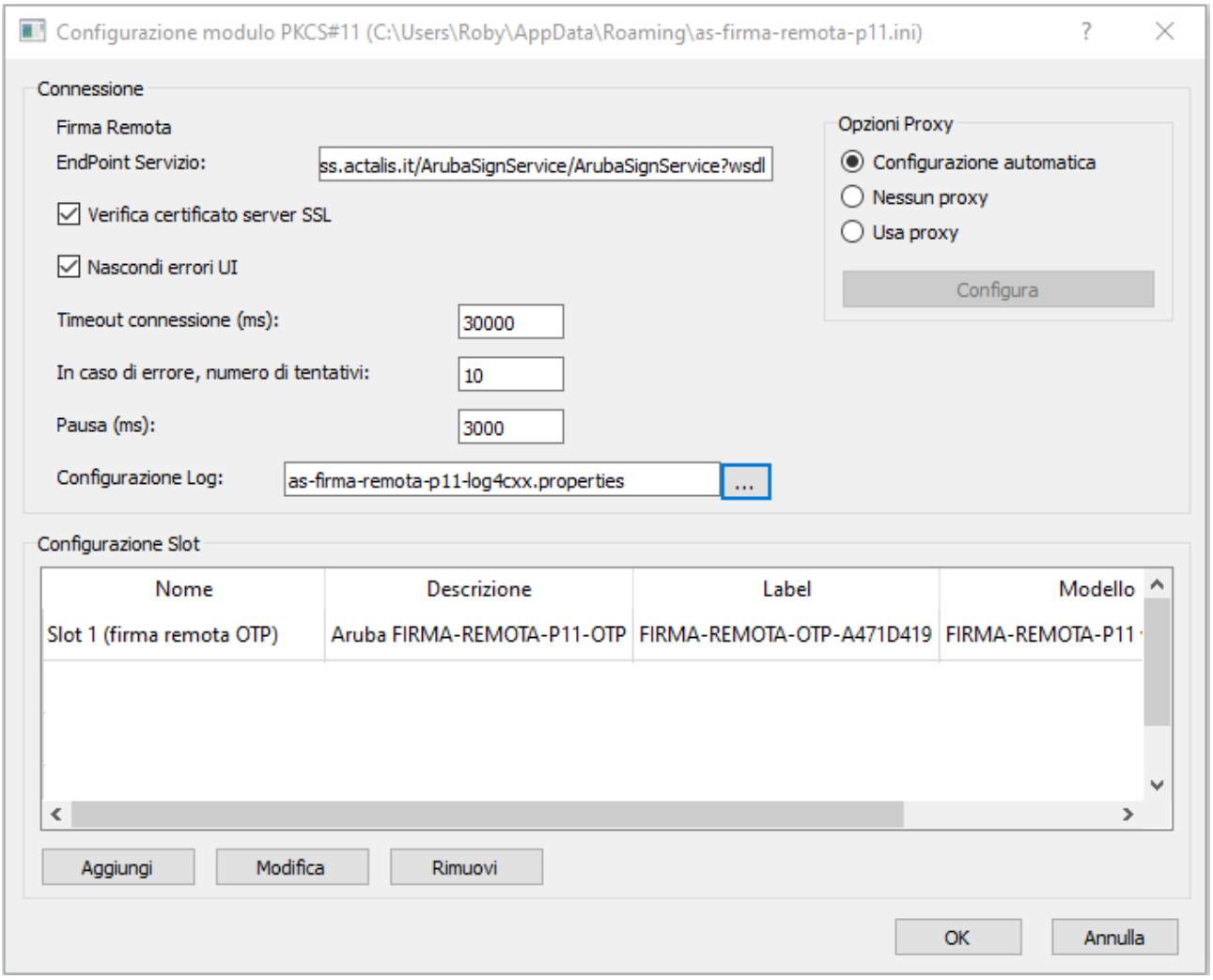
La configurazione del **Virtual P11** si opera direttamente da ***DigitalSign***: dal menu Dispositivo di firma -> Configurazione si accede alla finestra di dialogo per la configurazione del dispositivo, quindi si sceglie (manualmente) il modulo **Aruba Firma Remota**:



La finestra mostrerà la preselezione del primo slot, noi azioneremo il bottone Configura:



Si aprirà la schermata di configurazione propria del **Virtual P11**



Questa schermata consente di impostare diversi parametri:

- **Endpoint servizio** – è un indirizzo Internet che corrisponde al front-end del servizio a cui collegarsi. Va ottenuto dal fornitore del servizio: potrebbe essere un front-end pubblico di Aruba/Actalis, oppure un frontend ARSS privato dell'organizzazione di cui l'utente fa parte.
- **Verifica certificato server SSL** – istruisce il sistema a verificare la validità del certificato SSL del server cui ci si collega.
  Ovviamente la connessione tra il ***Virtual P11*** ed il server remoto avviene su un canale sicuro, attraverso il protocollo SSL; in condizioni normali questa opzione dovrebbe essere attivata, perché la verifica del certificato del server consente di assicurare l'originalità del server stesso. Tuttavia, i server di test in generale non montano certificati "ufficiali" e questa verifica non verrebbe superata.
  L'utente configurerà l'opzione in modo appropriato al contesto effettivo.
- **Nascondi Errori UI** – fa sì che i messaggi di errore generati dal sistema PKCS#11 non vengano presentati a video, ma soltanto tramite l'interfaccia programmatica. ***DigitalSign*** quindi interpreterà tali errori come se provenissero da un sottosistema smartcard, quindi probabilmente in modo non sempre coerente con il particolare contesto di utilizzo di un Virtual P11.
  Questa opzione dovrebbe essere selezionata solo nel caso in cui ***DigitalSign*** venga usato per tramite di applicazioni che ne usano l'interfaccia COM, le quali non potrebbero gestire i messaggi rivolti all'utente umano.
- **Timeout connessione (ms)** – è il valore del ritardo della risposta dal server tollerato prima di considerare fallito un tentativo di comunicazione. Il valore di default è pari a 30 secondi (espresso in millisecondi).
- **In caso di errore, numero di tentativi –** nel caso si verifichi un errore di comunicazione con il server possiamo programmare il numero di ripetizioni del tentativo, prima di abortire la sessione

- **Pausa (mS)** – in caso di errore e nel caso sia previsto di effettuare almeno un tentativo ripetuto, questo valore è la pausa (in millisecondi) di attesa prima di effettuare il nuovo tentativo.
- **Configurazione Log** – questo parametro consente di impostare un particolare file da cui il sistema deve leggere le opzioni di logging. Questo parametro va usato seguendo le indicazioni del supporto tecnico, questo manuale non documenta le opzioni disponibili per il logging.
- **Opzioni Proxy** – questo pannello permette di impostare la configurazione per il collegamento ad Internet: la *configurazione automatica* istruisce il sistema ad utilizzare la configurazione già effettuata per Internet Explorer; *nessun proxy* dispone alla connessione diretta ad Internet; *usa proxy* permette di accedere ad una ulteriore schermata di configurazione di un proxy aziendale (da operare secondo le istruzioni dell'amministratore di rete).

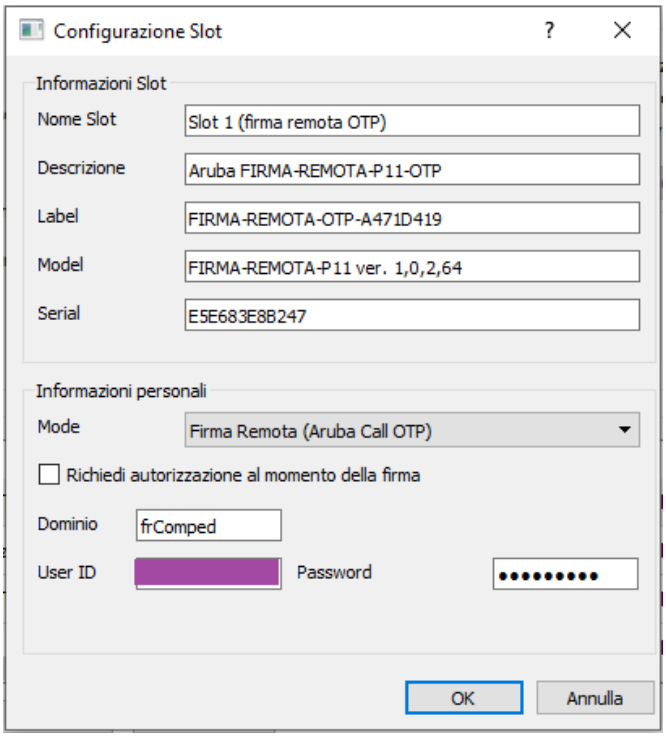
La schermata mostra poi una tabella contenente la lista degli *slot* già definiti. Nelle situazioni normali l'installazione propone uno slot pronto alla configurazione.

Uno *slot*, nell'ambito del PKCS#11, rappresenta un diverso dispositivo connesso allo stesso modulo di interfaccia. Per esempio, un computer che avesse due o più lettori di smartcard, potrebbe avere diverse carte inserite. I diversi *slot* corrisponderebbero ai diversi lettori capaci di accogliere diverse smartcard.
In questo contesto "virtuale", dove non esistono veri e propri lettori, usiamo il concetto di *slot* per gestire diversi profili, ciascuno dei quali corrisponde ad una coppia di chiavi e relativo certificato.
In generale ce ne basterà uno, ma non esiste un limite predefinito.

- Per creare uno slot si agisce sul bottone **Aggiungi**
- Per modificare i parametri dello slot selezionato si usa **Modifica**
- Per eliminare del tutto la configurazione di uno slot si usa **Rimuovi**

3.9.6.4 Virtual P11 ArubaSign: configurazione di uno slot

Quando dalla schermata di configurazione del Virtual P11, illustrata nella sezione precedente, si aziona il bottone **Aggiungi**, oppure **Modifica**, vedremo una finestra di questo tipo:



I campi riportati:

- **Nome** – è il nome simbolico assegnato allo slot, che ***DigitalSign*** mostrerà poi nella lista dei "lettori" disponibili. Si può usare qualunque nome, ma nel caso si pianifichi di avere più di uno slot sarà bene usare nomi significativi che consentano di distinguerli a colpo d'occhio.

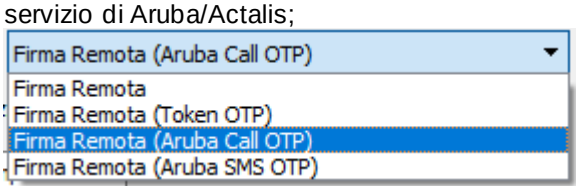
- **Descrizione** – in questo campo il sistema imposta automaticamente una descrizione del modulo PKCS#11 virtuale.

- **Label** – questo è un campo ispezionabile nell'ambito delle funzioni PKC#11; il sistema compone automaticamente un contenuto.

- **Model** – è un campo a sola lettura che identifica il modulo PKCS#11 in esecuzione

- **Serial** – anche questo è un campo ispezionabile nell'ambito delle funzioni PKC#11; il sistema compone automaticamente un contenuto; si raccomanda di lasciare il valore impostato automaticamente, anche se è possibile editare il valore, soprattutto a scopi di test e sperimentazione.

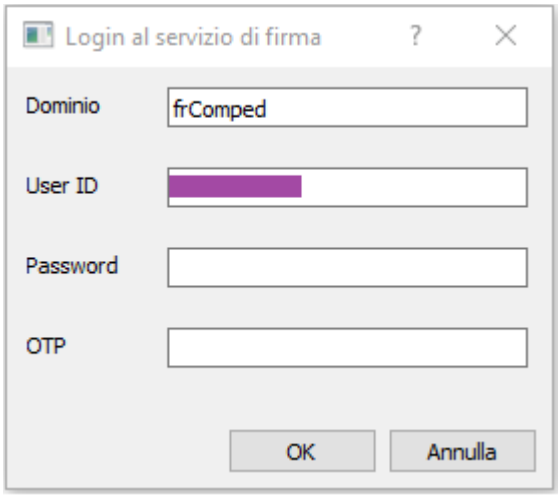
- **Mode** – è la modalità di funzionamento dello slot, in relazione alle diverse modalità supportate dal servizio di Aruba/Actalis;



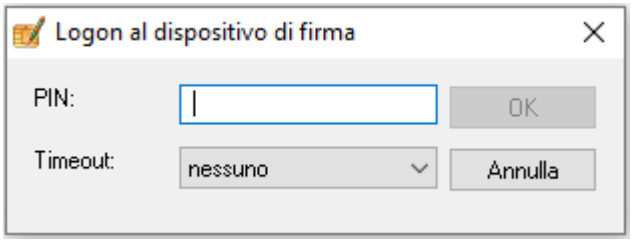
  - ✓ **Firma Remota** – si sottintende "automatica", si intende una modalità che NON RICHIEDE il codice OTP. Aruba offe un servizio che, sotto certe condizioni (pre-autorizzazione di un operatore, accesso solo da posizioni autorizzate, documentazione del processo) consente di firmare senza fornire un codice OTP per iniziare la sessione.
  - ✓ **Token OTP** – in questo caso il codice OTP proviene da un generatore hardware munito di display, oppure dall'app ***ArubaOTP***: l'utente legge il valore dal dispositivo e lo inserisce quando richiesto.
  - ✓ **Aruba Call OTP** – in questo caso il codice OTP è fornito dal servizio "Aruba Call": si riceve una chiamata automatica sul proprio telefono (il cui numero è registrato in fase di rilascio del certificato) da un numero di Aruba; le ultime 4 cifre del numero del chiamante rappresentano il codice OTP.
  - ✓ **Aruba SMS OTP** – analogo al precedente, ma il codice OTP viene ricevuto via SMS

  NOTA IMPORTANTE: l'utente, in generale, non è libero di scegliere a piacimento l'una o l'altra modalità; la modalità a disposizione è impostata in fase di rilascio del certificato.

- **Richiedi autorizzazione al momento della firma** – selezionando questa casella ***DigitalSign*** non consente di preimpostare la password nell'apposito campo (vedere sotto) e quindi, al momento della firma, l'utente dovrà inserire sia la password che l'OTP:



Se, invece, la casella NON è selezionata allora l'utente preimposterà la password in questa finestra di configurazione e DigitalSign presenterà solo la normale richiesta del PIN, in cui noi l'utente dovrà inserire l'OTP:



Si noti che solo la seconda opzione è totalmente compatibile con lo standard PKCS#11 (si comporta quindi come una normale smartcard) ed è quella da usare quando ***DigitalSign*** opera al servizio di altre applicazioni che lo richiamano attraverso l'interfaccia COM.

- **Dominio** – ad alcuni clienti di Aruba / Actalis si assegna un dominio, a cui appartiene l'utenza. Ad esempio, l'utente che appartiene a un dominio potrebbe essere **MarioRossi@myDominio**; In un caso come questo la parola scritta a destra della '@' è il dominio e va riportata in questo campo.
  I comuni utenti del servizio di firma Aruba appartengono invece al dominio generico "firma". É possibile lasciare vuoto questo campo, oppure scrivere **firma**.

- **UserID** – è il nome dell'utente. Nell'esempio appena riportato sarebbe **MarioRossi**

- **Password** – è la password di firma scelta dall'utente in fase di registrazione al servizio. Se la casella **Richiedi autorizzazione al momento della firma** è selezionata, allora questo campo non può essere impostato (la password verrà richiesta al momento della firma). Viceversa, NON impostando tale casella sarà obbligatorio immettere la password in questo campo, mentre al momento della firma verrà richiesto solo il codice OTP come se fosse il PIN di una smartcard.