BANCA D'ITALIA
EUROSISTEMA

Manuale Operativo per il servizio di certificazione delle chiavi pubbliche

Responsabile del documento: ***Fabio Bolognesi***
Firma

Sommario

1. INFORMAZIONI GENERALI

1.1. Premessa

Il presente Manuale definisce le procedure seguite dalla Banca d'Italia in qualità di Certificatore Accreditato (indicata di seguito anche come Certificatore o Ente certificatore) per l'emissione e l'utilizzo di certificati qualificati.

Esso è rivolto ai soggetti che entrano in relazione con il Certificatore in qualità di titolari dei certificati, terzi interessati o richiedenti la verifica delle firme.

I certificati sono rilasciati ai dipendenti della Banca d'Italia per esigenze connesse ai processi di lavoro e a specifiche categorie di soggetti terzi, pubblici o privati. I certificati rilasciati in favore dei terzi possono essere utilizzati soltanto nei rapporti con la Banca d'Italia.

1.2. Definizioni

Si riportano di seguito alcuni termini e concetti di uso corrente nell'attività di certificazione elettronica, non necessariamente contenuti nel presente Manuale.

CERTIFICATO ELETTRONICO: attestato elettronico che collega all'identità del titolare i dati utilizzati per verificare la firma elettronica.

CERTIFICATO QUALIFICATO: certificato elettronico conforme all'allegato I alla Direttiva europea 1999/93/CE e rilasciato da Certificatori che rispondono ai requisiti fissati dall'allegato II della stessa Direttiva.

CERTIFICATORE: soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.

CERTIFICATORE ACCREDITATO: certificatore che ha ottenuto da DigitPA il riconoscimento del possesso dei requisiti del livello più elevato in termini di qualità e sicurezza nonché in ordine alla solidità finanziaria e alla onorabilità.

CHIAVE PRIVATA: elemento della coppia di chiavi asimmetriche destinato a essere utilizzato soltanto dal titolare. Se facente parte di una coppia di chiavi di firma o certificazione è utilizzata per apporre una firma elettronica.

CHIAVE PUBBLICA: elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico. Se facente parte della coppia di chiavi di firma o

certificazione viene utilizzata per verificare la firma apposta con la corrispondente chiave privata.

CHIAVI ASIMMETRICHE: coppia di chiavi asimmetriche, una privata e una pubblica, correlate tra loro, da utilizzarsi nell'ambito di sistemi di firma, cifratura e autenticazione.

CHIAVI AUSILIARIE – CERTIFICATO AUSILIARIO: coppia di chiavi crittografiche, con relativo certificato, fornite al Titolare con il dispositivo di firma, in aggiunta a quelle di firma digitale, per utilizzi diversi dalla sottoscrizione.

CHIAVI DI CERTIFICAZIONE: coppia di chiavi utilizzate dal Certificatore per firmare i certificati e le liste dei certificati sospesi (CSL) e revocati (CRL).

CRITTOGRAFIA ASIMMETRICA: tipologia di operazione matematica mediante la quale, utilizzando apposite chiavi tra loro differenti e specifici algoritmi, dal risultato della cifratura di un file ottenuta con una chiave è possibile risalire al file originario unicamente applicando a tale risultato lo stesso algoritmo con l'utilizzo dell'altra chiave.

CRL (Certificate Revocation List): cfr. Lista dei certificati revocati.

CSL (Certificate Suspension List): cfr. Lista dei certificati sospesi.

DISPOSITIVO DI SICUREZZA: apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado di conservare in modo protetto le chiavi private e di generare al suo interno firme elettroniche.

FIRMA ELETTRONICA: l'insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

FIRMA ELETTRONICA QUALIFICATA: firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica che sia:

- creata con mezzi sui quali il firmatario può conservare un controllo esclusivo;
- collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
- basata su un certificato qualificato;
- realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica.

FIRMA DIGITALE: particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche (asimmetriche a coppia), 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 la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

FUNZIONE DI HASH: funzione matematica che genera, a partire da una generica sequenza di simboli binari, un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.

GIORNALE DI CONTROLLO: insieme delle registrazioni effettuate automaticamente dai dispositivi installati presso il Certificatore al verificarsi di condizioni predeterminate.

INFRASTRUTTURA A CHIAVI PUBBLICHE (PKI): insieme di macchine, software, persone e regole che consentono l'emissione e la gestione dei certificati elettronici e dei relativi dispositivi di firma.

LISTA DEI CERTIFICATI REVOCATI (CRL): elenco elettronico dei certificati che sono stati revocati dal Certificatore che li ha emessi. Tale elenco - che costituisce parte integrante del Registro dei certificati - è firmato, tenuto e aggiornato dal Certificatore.

LISTA DEI CERTIFICATI SOSPESI (CSL): elenco elettronico dei certificati che sono stati sospesi dal Certificatore che li ha emessi. Tale elenco - che costituisce parte integrante del Registro dei certificati - è firmato, tenuto e aggiornato dal Certificatore.

MANUALE OPERATIVO: documento che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività, stabilendo obblighi e responsabilità del Certificatore stesso, del titolare e degli altri destinatari del servizio di certificazione.

OCSP (ONLINE CERTIFICATE STATUS PROTOCOL): protocollo di rete, conforme alla specifica RFC 2560 e successive modificazioni, utilizzato per verificare la validità dei certificati elettronici.

MARCA TEMPORALE: evidenza informatica che consente la validazione temporale.

PASS-PHRASE: sequenza di caratteri alfanumerici e di punteggiatura, conosciuta solo dal titolare del certificato, il quale deve comunicarla al servizio di Help desk per chiedere la sospensione d'urgenza del certificato in caso di smarrimento, furto o compromissione della sicurezza della smartcard.

PIN (Personal Identification Number): codice di identificazione personale.

PKI (Public Key Infrastructure): cfr. Infrastruttura a chiavi pubbliche.

PUK (PIN unlock key): codice di sblocco del PIN.

REGISTRAZIONE: attività di acquisizione, verifica e archiviazione dei dati dei richiedenti i certificati. La registrazione costituisce condizione necessaria per l'accoglimento della domanda di certificazione.

REGISTRO DEI CERTIFICATI: registro contenente tutti i certificati emessi dal Certificatore, la lista dei certificati revocati e quella dei certificati sospesi.

REVOCA DEL CERTIFICATO: operazione con la quale il Certificatore annulla la validità del certificato da un dato momento in poi.

RICHIEDENTE: persona fisica che, anche su designazione del terzo interessato, chiede al Certificatore l'attribuzione di una coppia di chiavi (pubblica e privata) e il relativo certificato; una volta emesso il certificato, il richiedente ne diviene titolare.

RIFERIMENTO TEMPORALE: informazione contenente la data e l'ora che viene associata ad una evidenza informatica.

SMARTCARD: dispositivo di sicurezza sul quale risiedono la coppia di chiavi (pubblica e privata) e il certificato del titolare.

SOSPENSIONE DEL CERTIFICATO: operazione con cui il Certificatore sospende la validità del certificato per un periodo di tempo.

TERZO INTERESSATO: ente o persona giuridica che chiede l'emissione di un certificato in favore di un altro soggetto (titolare), da esso designato, a lui legato da un rapporto di rappresentanza o di lavoro.

TITOLARE: persona fisica che, anche su designazione del terzo interessato, ha richiesto e ottenuto dal Certificatore l'attribuzione di una coppia di chiavi (pubblica e privata) e quindi il relativo certificato.

VALIDAZIONE TEMPORALE: risultato della procedura informatica con cui si attribuisce ad uno o più documenti informatici un riferimento temporale opponibile ai terzi.

1.3. Riferimenti normativi

Direttiva 1999/93/CE	Direttiva 1999/93/CE del Parlamento e del Consiglio del 13.12.1999 relativa ad un quadro comunitario per le firme elettroniche, pubblicata nella Gazzetta Ufficiale delle Comunità europee 19 gennaio 2000, L 13.
Legge 59/1997 Art. 15,	Legge 15 marzo 1997, n. 59 "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione

comma 2	e per la semplificazione amministrativa" pubblicata nel S.O. 56/L alla Gazzetta Ufficiale n. 63 del 17 marzo 1997.
Legge 229/2003 Art. 10	Legge 29 luglio 2003, n. 229 "Interventi in materia di qualità della regolazione, riassetto normativo e codificazione – legge di semplificazione 2001", pubblicata nella Gazzetta Ufficiale n. 196 del 25 agosto 2003.
D. Lgs. 82/2005	Decreto legislativo 7 marzo 2005, n. 82. "Codice dell'amministrazione digitale", pubblicato nel S.O. N. 93/L alla Gazzetta Ufficiale n. 112 del 16 maggio 2005 [1].
D. Lgs. 159/2006	Decreto legislativo 4 aprile 2006, n. 159. "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale".
Circ. C.N.I.P.A./CR/48	Circolare C.N.I.P.A. 6 settembre 2005
DPCM 30.3.2009	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 "Regole tecniche in materia di generazione, apposizione e verifica delle firma digitali e validazione temporale dei documenti informatici", Pubblicato nella Gazzetta Ufficiale del 6 giugno 2009 n. 129.
Deliberaz. C.N.I.P.A. 45/2009	Deliberazione C.N.I.P.A. 45 del 21 maggio 2009 modificata dalla determinazione DigitPa n. 69 del 28 luglio 2010.

[1] Il "Codice", in vigore dal 1^ gennaio 2006, ha abrogato le previsioni in materia di firme elettroniche, documenti informatici, carta d'identità elettronica e sviluppo dei sistemi informativi delle PP.AA. contenute nel D.P.R. 28.12.2000, n. 445.

2. DATI IDENTIFICATIVI

2.1. Dati identificativi del Certificatore

Denominazione	Banca d'Italia
Indirizzo della sede legale	Via Nazionale, 91 – 00184 ROMA
Legale Rappresentante	Governatore pro tempore
e-mail	**pki@bancaditalia.it**
Indirizzo internet	**www.bancaditalia.it**
Telefono	06/47921
Fax	06/47928956

2.2. Dati identificativi del Manuale Operativo

Il presente documento costituisce la versione n. 1.2 del 07/06/2011 del Manuale Operativo per il servizio di certificazione delle chiavi pubbliche svolto dalla Banca d'Italia ed è consultabile per via telematica sul sito internet www.bancaditalia.it.

La versione è identificabile in calce ad ogni pagina.

Il presente Manuale operativo è referenziato dal seguente O.I.D. (Object Identifier Number):

- 1.3.76.38.1.1.1

2.3. Responsabile del Manuale Operativo

Il responsabile del Manuale Operativo è:

Nome	Fabio
Cognome	Bolognesi
Telefono	+39 06 4792 6237
e-mail	**fabio.bolognesi@bancaditalia.it**

3. OBBLIGHI DEL CERTIFICATORE, DEL TITOLARE, DEL TERZO INTERESSATO E DEI RICHIEDENTI LA VERIFICA DELLE FIRME

3.1. Obblighi del Certificatore

Il Certificatore:

1. adotta tutte le misure organizzative e tecniche idonee ad evitare danno a terzi;
2. identifica con certezza la persona che effettua la richiesta di certificazione;
3. si accerta dell'autenticità della richiesta;
4. rilascia, rende pubblico e gestisce il certificato qualificato nei modi stabiliti dalle regole tecniche di cui al DPCM 30.3.2009, e successive modificazioni e integrazioni, e nel rispetto del D. Lgs. 196/2003 e successive modificazioni;
5. specifica nel certificato qualificato, su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;
6. si attiene alle regole tecniche di cui al DPCM 30.3.2009 e successive modificazioni e integrazioni;
7. informa i richiedenti in modo compiuto e chiaro sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
8. non si rende depositario di dati per la creazione della firma del titolare;
9. procede alla tempestiva pubblicazione della revoca e della sospensione del certificato qualificato in caso di richiesta da parte del titolare o del terzo interessato, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui al DPCM 30.3.2009 e successive modificazioni e integrazioni;

10. garantisce un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;
11. assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
12. tiene la registrazione di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
13. non copia, né conserva le chiavi private di firma del Titolare del certificato;
14. predispone su mezzi di comunicazione durevoli e rende disponibili ai richiedenti il servizio di certificazione tutte le informazioni utili, tra cui in particolare gli esatti termini e condizioni relativi all'uso del certificato, compresa ogni limitazione dell'uso;
15. utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;
16. nel caso di cessazione della propria attività informa, almeno sessanta giorni prima, i titolari che tutti i certificati non scaduti al momento della cessazione saranno revocati e a tempo debito provvede alla loro effettiva revoca;
17. registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione; il momento della generazione dei certificati è attestato tramite riferimento temporale;
18. genera un certificato qualificato per ciascuna delle chiavi di firma elettronica utilizzate da DigitPA per la sottoscrizione dell'Elenco Pubblico dei certificatori e lo pubblica nel proprio registro dei certificati;
19. fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme e ne garantisce l'interoperabilità;
20. mantiene copia della lista, sottoscritta da DigitPA, dei certificati relativi alle chiavi di certificazione e la rende accessibile per via telematica;

21. revoca o sospende il certificato qualificato ove abbia notizia della compromissione della chiave privata o del dispositivo per la creazione della firma;
22. adotta le misure di sicurezza per il trattamento dei dati personali, ai sensi del D. Lgs. 196/2003;
23. garantisce l'interoperabilità del prodotto di verifica di cui all'art. 10 del DPCM 30.3.2009, e successive modificazioni e integrazioni, ai documenti informatici sottoscritti con firma digitale.

3.2. Obblighi del titolare

Il titolare è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri nonché a utilizzare personalmente il dispositivo di firma.

Il titolare del certificato deve altresì:

1. fornire tutte le informazioni richieste dall'Ente Certificatore, garantendone l'attendibilità sotto la propria responsabilità;
2. comunicare all'Ente Certificatore eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica (e-mail), ecc;
3. conservare con la massima diligenza e separatamente il dispositivo che contiene la chiave privata e i codici segreti (PIN, PUK e pass-phrase) ricevuti dall'Ente Certificatore, al fine di garantirne l'integrità e la massima riservatezza;
4. non utilizzare la coppia di chiavi per funzioni e finalità diverse da quelle per le quali il certificato è stato emesso;
5. inoltrare all'Ente Certificatore, secondo le modalità indicate nel presente Manuale, le richieste di sospensione, riattivazione e revoca;
6. richiedere immediatamente la sospensione dei certificati qualificati relativi alle chiavi contenute in dispositivi difettosi o di cui abbia perduto il possesso;
7. comunicare all'Ente Certificatore lo smarrimento o la sottrazione del dispositivo di sicurezza.

In definitiva, i titolari dei certificati sono responsabili del corretto utilizzo degli stessi e della custodia dei dispositivi che li contengono; devono farne uso solo per

le finalità per le quali sono stati rilasciati, mantenerli nel loro esclusivo possesso e informare la Banca d'Italia – con le modalità prescritte – di ogni evento che ne possa compromettere la funzionalità.

3.3. Obblighi del terzo interessato

Il terzo interessato ha l'obbligo di chiedere la revoca e la sospensione dei certificati, secondo le modalità indicate nel presente Manuale, ogniqualvolta vengano meno i presupposti in base ai quali il certificato è stato rilasciato al titolare ovvero in caso di cessazione della propria attività (per operazioni di fusione, liquidazione ecc.).

Inoltre - fermi restando gli obblighi e le responsabilità che fanno capo al titolare dei certificati - il terzo, in quanto soggetto nel cui interesse è svolto il servizio di certificazione, adotta tutte le cautele e le misure organizzative funzionali a un utilizzo dei certificati conforme alle prescrizioni previste dalla legge e dal presente Manuale.

Il terzo interessato ha altresì l'obbligo di comunicare tempestivamente al certificatore ogni modifica delle circostanze indicate al momento del rilascio del certificato rilevanti ai fini del suo utilizzo.

3.4. Obblighi dei richiedenti la verifica delle firme

I destinatari dei documenti informatici firmati digitalmente devono verificare:

1. la validità del certificato;
2. l'assenza del certificato dalla lista dei certificati revocati (CRL) e dalla lista dei certificati sospesi (CSL);
3. l'esistenza ed il rispetto di eventuali limitazioni all'uso del certificato utilizzato dal titolare.

4. RESPONSABILITÀ DEL CERTIFICATORE

4.1. Responsabilità del Certificatore

Il Certificatore è responsabile dell'adempimento di tutti gli obblighi previsti dalla legge e richiamati nel presente Manuale.

Il Certificatore è altresì responsabile, se non prova di aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:

- sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma contenute nel certificato alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;
- sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
- sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare nei casi in cui il certificatore generi entrambi.

Il Certificatore è inoltre responsabile dei danni provocati ai terzi per effetto della mancata o non tempestiva registrazione della revoca o della non tempestiva sospensione del certificato.

Il Certificatore non assume responsabilità:

- per le conseguenze derivanti dal mancato rispetto delle procedure e delle modalità operative specificate in questo Manuale da parte del titolare del certificato;
- per le conseguenze derivanti da un uso dei certificati diverso da quello consentito e in particolare per i danni derivanti dall'uso di un certificato che ecceda i limiti posti dallo stesso;
- per il mancato adempimento degli obblighi previsti a suo carico dovuto a cause ad esso non imputabili.

4.2. Limitazioni agli indennizzi e tariffe

Non sono previste limitazioni agli indennizzi né applicazione di tariffe.

5. MODALITA' DI IDENTIFICAZIONE E REGISTRAZIONE DEGLI UTENTI

In questo capitolo viene illustrata la procedura per la prima emissione dei certificati nel cui ambito si collocano la registrazione del richiedente e la sua identificazione.

Fermo il rispetto delle norme di legge, tale procedura può subire talune variazioni per i dipendenti della Banca d'Italia.

5.1. Presentazione della domanda di emissione

I soggetti esterni alla Banca d'Italia che richiedono l'emissione di certificati devono essere designati dagli enti (terzi interessati) per i quali operano in virtù di un rapporto di lavoro o di rappresentanza.

La nota di designazione - sottoscritta dal legale rappresentante dell'ente ovvero da altro soggetto a ciò delegato - deve:

- indicare le generalità del soggetto designato, la tipologia dei certificati da rilasciare (firma e ausiliari), le finalità per le quali vengono richiesti i certificati;
- contenere una dichiarazione nella quale il terzo attesti di conoscere il contenuto del presente Manuale e di impegnarsi al rispetto degli obblighi in esso previsti a suo carico;
- recare in allegato la richiesta di certificato, redatta e sottoscritta dal soggetto designato, che deve:
  a) indicare i dati anagrafici, il codice fiscale, il numero di telefono (di rete fissa o cellulare), l'indirizzo di posta elettronica del richiedente;
  b) contenere l'attestazione da parte del richiedente circa l'attendibilità delle informazioni fornite e l'impegno a comunicare ogni variazione delle stesse;
  c) contenere l'attestazione che il richiedente ha ricevuto l'informativa di cui all'art. 13 del D. Lgs. 196/2003;
  d) essere corredata di una copia di un valido documento di riconoscimento del richiedente nonché del tesserino contenente il codice fiscale.

La suddetta documentazione va inviata, anche via fax, alla Filiale della Banca d'Italia competente con riferimento al luogo in cui il richiedente risiede o ha il domicilio ovvero svolge la propria attività lavorativa; presso tale Filiale il titolare deve essere identificato e ritirare la smartcard e i codici segreti.

5.2. Registrazione degli utenti

La Filiale, effettuate le verifiche di competenza, inoltra la richiesta di certificati all'Amministrazione Centrale che provvede all'inserimento nell'archivio di registrazione di tutti i dati necessari all'emissione dei certificati.

L'eventuale mancato accoglimento dell'istanza è comunicato dalla Filiale al terzo interessato e al richiedente.

5.3. Identificazione e consegna agli utenti dei dispositivi di sicurezza

La Filiale - ricevute le buste[2] contenenti rispettivamente la smartcard e i codici segreti (PIN, PUK e pass-phrase)[3] - invita il titolare dei certificati a recarsi presso la Filiale stessa al fine di identificarlo; l'identificazione avviene sulla base di uno dei seguenti documenti, in corso di validità:

1) passaporto;
2) tessera personale di riconoscimento di cui all'art. 1 del DPR 28 luglio 1967, n. 851, rilasciata da amministrazioni statali ai propri dipendenti, civili e militari, in attività di servizio e in quiescenza nonché ai loro familiari;
3) libretto di licenza di porto d'armi;
4) tessera postale di riconoscimento;
5) patente di abilitazione alla guida di autoveicoli o motoveicoli;
6) carta d'identità;
7) tessera di riconoscimento rilasciata dai Paesi appartenenti alla UE;
8) patente nautica;
9) libretto di pensione;
10) patentino di abilitazione alla conduzione di impianti termici.

Effettuata l'identificazione, la Filiale consegna al richiedente le buste contenenti la smartcard e i codici segreti nonché rende disponibile copia del presente Manuale.

---

[2] Le buste sono trasmesse alla Filiale mediante vettori separati.

[3] Il PIN deve essere digitato per procedere alle operazioni di firma e alle altre connesse all'utilizzo dei certificati ausiliari e può essere variato dal titolare all'atto del primo utilizzo del dispositivo. Il PUK serve a sbloccare la smartcard dopo un numero prestabilito di tentativi errati di inserimento del PIN.

Le operazioni di consegna sono verbalizzate. Il verbale è redatto in duplice copia e sottoscritto dall'incaricato della consegna e dal titolare, al quale viene rilasciata una copia.

A seguito della consegna si procede all'attivazione dei certificati.

6. MODALITÀ DI GENERAZIONE DELLE CHIAVI

Le coppie di chiavi generate dal servizio di certificazione della Banca d'Italia appartengono alle seguenti tipologie:

- chiavi di certificazione;
- chiavi di firma;
- chiavi di marcatura temporale;
- chiavi ausiliarie[4].

La generazione della coppia di chiavi (pubblica e privata) è effettuata mediante dispositivi e procedure che garantiscono, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata. Il sistema di generazione delle chiavi assicura:

- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- l'equiprobabilità di generazione di tutte le coppie possibili;
- l'identificazione del soggetto che attiva la procedura di generazione.

La generazione delle coppie di chiavi di firma avviene all'interno del dispositivo di sicurezza e riguarda:

1. le chiavi di certificazione, cioè le chiavi utilizzate dall'Ente Certificatore per firmare elettronicamente i certificati dei titolari e le liste di revoca e sospensione dei certificati;
2. le chiavi del titolare, vale a dire le chiavi di firma attribuite dall'Ente Certificatore ai singoli titolari.

Ogni coppia di chiavi è utilizzabile unicamente per la tipologia di operazione per la quale è stata generata.

L'indicazione della tipologia di operazione che è possibile effettuare con la coppia di chiavi è riportata nel relativo certificato.

6.1. Lunghezza delle chiavi

La lunghezza delle chiavi di certificazione del Certificatore è di 2048 bit.

[4] Il processo di rilascio e gestione delle chiavi ausiliarie e dei relativi certificati non differisce, in linea di massima, da quello previsto per le chiavi e i certificati di firma, anche se la disciplina di legge riguarda esclusivamente questi ultimi.

La lunghezza delle chiavi di firma, di marcatura temporale e ausiliarie è di 1024 bit.

6.2. Algoritmi

Per la generazione e verifica delle firme digitali è utilizzato il seguente algoritmo:

- RSA (Rivest-Shamir-Adleman algorithm).

La funzione di hash utilizzata per la generazione dell'impronta è:

- SHA-256 (Dedicated Hash Function 4).

6.3. Chiavi di firma

Le coppie di chiavi di firma consentono di rendere manifesta la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Ciascuna coppia di chiavi è attribuita ad un solo titolare.

6.3.1. Dispositivo di sicurezza per le operazioni di firma

Le chiavi private di firma del titolare sono custodite all'interno del dispositivo di sicurezza (smartcard).

I certificati attribuiti ad un medesimo titolare risiedono su di un unico dispositivo di sicurezza e hanno una medesima data di scadenza.

Nelle operazioni di firma e nelle altre operazioni connesse all'utilizzo dei certificati ausiliari il dispositivo di sicurezza non comunica mai all'esterno le chiavi private del titolare.

L'accesso alla chiave privata da parte del titolare è protetto con un PIN.

La duplicazione delle chiavi private o dei dispositivi di sicurezza che le contengono è vietata.

I dispositivi di firma utilizzati dai titolari sono certificati Common Criteria EAL4+ (protection Profile CWA14169).

Tali dispositivi sono in grado di:

- generare al proprio interno coppie di chiavi asimmetriche con equiprobabilità di generazione di tutte le coppie possibili;
- proteggere la chiave privata da accessi non autorizzati; effettuare le elaborazioni crittografiche di cifra.

6.3.2. Personalizzazione del dispositivo di sicurezza per le operazioni di firma

Nell'ambito del processo di personalizzazione del dispositivo di sicurezza, si svolgono le seguenti operazioni:

- acquisizione dei dati identificativi del titolare nel dispositivo utilizzato e loro associazione al titolare;
- registrazione nel dispositivo dei dati identificativi del titolare presso l'Ente Certificatore;
- registrazione nel dispositivo del certificato relativo alle chiavi di firma del titolare.

6.4. Chiavi di certificazione

L'Ente Certificatore si avvale delle proprie chiavi di certificazione per firmare elettronicamente i certificati dei titolari e le liste dei certificati sospesi e revocati.

Il dispositivo che contiene la chiave privata di certificazione è conforme ai requisiti di sicurezza imposti dai criteri previsti dal livello di valutazione E4 e robustezza dei meccanismi HIGH dell'ITSEC.

Il certificato contenente la chiave pubblica di certificazione è generato nel formato ISO 9594-8 (1997) ed è registrato nel registro dei certificati con le modalità di seguito previste per i certificati dei titolari.

Le chiavi di certificazione hanno validità 10 anni. Con tali chiavi saranno sottoscritti certificati dei titolari con periodo di validità temporalmente inferiore alla validità delle chiavi di certificazione.

6.5. Estrazione della chiave privata dai dispositivi di sicurezza

Le chiavi private dei titolari non possono essere estratte, allo stato attuale della tecnologia, dai dispositivi di sicurezza (smart card) che le contengono.

Il processo di generazione delle chiavi di certificazione prevede la clonazione delle chiavi private su dispositivi di salvaguardia che detengono i medesimi profili autorizzativi dell'originale e sono custoditi in locali protetti.

Il loro impiego è previsto nelle circostanze in cui per guasti o inagibilità la continuità di servizio non può essere assicurata con i sistemi e gli impianti di produzione.

7. MODALITÀ DI EMISSIONE DEI CERTIFICATI

Il certificato associa la chiave pubblica di una coppia di chiavi asimmetriche ad un insieme d'informazioni che identificano un soggetto (titolare del certificato), il quale possiede la corrispondente chiave privata.

Tale associazione è garantita dalla firma apposta al certificato da parte dell'Ente Certificatore, mediante la propria chiave privata di certificazione.

7.1. Informazioni contenute nei certificati

Il certificato, conformemente alla Deliberazione CNIPA 45/2009 ove applicabile, contiene:

- l'indicazione che il certificato è qualificato;
- numero di serie o altro codice identificativo del certificato;
- denominazione dell'Ente Certificatore e stato nel quale è stabilito;
- codice identificativo del titolare presso l'Ente Certificatore;
- nome, cognome, codice fiscale (in mancanza, per i residenti all'estero, il codice fiscale rilasciato dall'Autorità fiscale del Paese di residenza o un analogo codice identificativo) del titolare del certificato;
- indicazione del termine iniziale e finale di validità del certificato;
- firma elettronica dell'Ente Certificatore;
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- algoritmo di firma del certificato;
- tipologia della coppia di chiavi in base all'uso cui sono destinate.

Il certificato qualificato può contenere, ove richiesto dal titolare o dal terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:

- le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
- limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui al punto precedente;
- limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere utilizzato.

Se il certificato è relativo a una coppia di chiavi di certificazione, è indicato l'uso delle chiavi stesse per la certificazione.

Fatto salvo quanto sopra esposto, l'individuazione del titolare avviene mediante l'uso del Distinguished name (DN) come previsto nello standard ISO 9594-1 (1997).

Le informazioni personali contenute nel certificato sono utilizzabili unicamente per identificare il titolare relativamente alle operazioni che è abilitato a compiere.

Il Certificatore custodisce le informazioni relative al certificato per un periodo non inferiore a 20 anni dalla data di scadenza o revoca del certificato.

7.2. Profilo del certificato

Il profilo dei certificati generati è conforme alla norma ISO/IEC 9594-8:2001 e successive evoluzioni.

7.3. Generazione del certificato e suo inserimento nel Registro dei certificati

Il certificato è generato presso i competenti Servizi dell'Amministrazione Centrale della Banca d'Italia con un sistema utilizzato esclusivamente per tale funzione, situato in locali adeguatamente protetti.

Al termine delle operazioni di generazione, il certificato è inserito nel Registro dei certificati; la data e l'ora di emissione del certificato vengono memorizzate nel giornale di controllo.

A conclusione del processo, sulla *smartcard* del titolare risultano registrati:

- i certificati richiesti e le relative chiavi private;
- i certificati relativi alle chiavi di certificazione del Certificatore.

I certificati sono consultabili secondo le modalità descritte nel presente Manuale.

7.4. Periodi di validità delle chiavi e dei relativi certificati

I certificati di firma rilasciati ai titolari hanno validità massima di 3 anni.

7.5. Accesso al sistema di generazione dei certificati

L'accesso al sistema di generazione dei certificati è consentito, limitatamente alle funzioni assegnate, ai soli operatori autorizzati.

8.TIPOLOGIA E MODALITA' DI EMISSIONE DEI CERTIFICATI

8.1. Tipologia

A partire dalle chiavi asimmetriche generate secondo le procedure descritte nei precedenti paragrafi si giunge alla generazione dei certificati digitali.

I certificati digitali emessi dalla Banca d'Italia sono firmati con proprie chiavi di certificazione e sono conformi allo standard X. 509 v3, che prevede una struttura dati con campi fissi e variabili in relazione all'utilizzo a cui il certificato digitale è destinato. Detti certificati sono inoltre conformi alla deliberazione CNIPA 45/2009 del 21.5.2009 sull'interoperabilità. In analogia alle tipologie di coppie di chiavi generate, i certificati si distinguono in:

- certificato di CA: relativo alla chiave di certificazione utilizzata per la firma dei certificati di sottoscrizione e delle CRL;
- certificato di ROOT-TSA: relativo alla chiave di certificazione utilizzata per la firma di certificati di marcatura temporale;
- certificati di marcatura temporale: relativi alle chiavi di marcatura temporale;
- certificati di sottoscrizione: relativi a chiavi per la firma digitale;
- certificati ausiliari: relativi a coppie di chiavi per altre finalità.

8.2. Modalità di emissione

Le generalità dei titolari dei certificati derivano dai dati di registrazione. Non è previsto l'uso di pseudonimi. Per ogni certificato deve essere specificato il tipo di operazione (certificazione, marcatura temporale, sottoscrizione, altre finalità) che è possibile eseguire con la coppia di chiavi ad esso associata. Non è consentito l'utilizzo di un certificato per scopi diversi da quelli per i quali il certificato è stato prodotto, scopi espressamente indicati sul certificato stesso.

I certificati sospesi/revocati sono riportati nelle liste di sospensione/revoca pubblicate sullo stesso sistema che implementa il Registro dei certificati.

I certificati digitali emessi dalla Banca d'Italia sono identificati in maniera univoca da un codice seriale progressivo, mentre i Titolari dei certificati sono identificati da un codice identificativo univoco (I.U.T.) .

9. MODALITA' DI SOSPENSIONE E REVOCA DEI CERTIFICATI

I certificati sono sospesi o revocati da parte dell'Ente Certificatore mediante inserimento del relativo numero identificativo (serial number) nelle liste dei certificati sospesi o revocati[5].

La sospensione e la revoca sono efficaci a partire dal momento dell'inserimento dei certificati nelle suddette liste.

La sospensione di un certificato comporta l'interruzione temporanea della sua validità.

La revoca di un certificato determina la cessazione anticipata della sua validità.

Nell'ipotesi di sospensione o revoca del certificato di firma, vengono parimenti sospesi o revocati gli eventuali certificati ausiliari residenti sul medesimo dispositivo di sicurezza.

La revoca, la sospensione e la successiva riattivazione dei certificati sono annotate nel giornale di controllo con l'indicazione della data e dell'ora di esecuzione dell'operazione.

I certificati possono essere sospesi o revocati dalla Banca d'Italia nei casi previsti dall'art. 36 del d.lgs. 82/2005.

9.1. Sospensione dei certificati

Il titolare o il terzo interessato possono chiedere alla competente Filiale della Banca d'Italia, la sospensione della validità del certificato al verificarsi delle causali riepilogate nella tabella che segue; per i dipendenti della Banca, la richiesta è avanzata dalla Struttura di appartenenza o dal dipendente stesso. Il Certificatore, qualora venga a conoscenza di sospetti abusi, falsificazioni, negligenze, si riserva la facoltà di sospendere i certificati previa comunicazione motivata, salvo i casi di urgenza, ai titolari stessi.

[5] Allo stato le due liste vengono presentate per la consultazione mediante un unico elenco in cui sono presenti sia i certificati sospesi sia quelli revocati, contraddistinti da diverse "causali".

RICHIEDENTE CAUSALE	TITOLARE (soggetto esterno o dipendente)	TERZO INTERESSATO (per i soggetti esterni)	BANCA D'ITALIA (dipendenti)
SMARRIMENTO DELLA SMARTCARD	X	--	--
FURTO DELLA SMARTCARD	X	--	--
COMPROMISSIONE DELLA SICUREZZA[6]	X	--	--
PROLUNGATA ASSENZA DEL TITOLARE	--	--	X
ALTRO[7]	X	X	X

Le richieste con causale "altro" devono essere adeguatamente motivate.

In caso di furto, smarrimento o compromissione della sicurezza della smartcard, il Titolare è tenuto a rivolgersi al servizio di Help desk per la sospensione d'urgenza, secondo le modalità descritte al par. 9.5.

Nell'ipotesi di ritrovamento della *smartcard* può essere richiesta la riattivazione del certificato sospeso.

Al contrario, qualora il furto o lo smarrimento vengano confermati, il titolare deve inoltrare richiesta di revoca, nei termini descritti al par. 9.3.

Negli altri casi la richiesta di sospensione deve essere trasmessa mediante posta elettronica[8] e sottoscritta con firma digitale.

Nel caso in cui non sia possibile l'utilizzo della posta elettronica, la richiesta deve essere presentata alla competente Filiale in forma cartacea, ovvero inviata per posta o tramite fax, e recare in allegato fotocopia di un valido documento di identificazione.

---

[6] Per compromissione della sicurezza deve intendersi il verificarsi di qualunque evento che faccia venire meno la certa riconducibilità al legittimo titolare dell'uso della smartcard (es. il PIN o il PUK sono conosciuti da altre persone).

[7] La causale "altro" comprende tutte le fattispecie non riconducibili a quelle espressamente individuate.

[8] La richiesta effettuata con tale modalità deve essere indirizzata alla casella funzionale della Filiale competente Non è necessario accludere alla richiesta copia di alcun documento se la stessa è avanzata dal Titolare.

Ove avanzata dal terzo interessato, la richiesta deve essere sottoscritta dal legale rappresentante dell'ente ovvero da altro soggetto a ciò delegato.

La Filiale che riceve la richiesta, verificata l'autenticità della stessa, provvede ad avviare il procedimento di sospensione.

La Filiale informa il titolare e il terzo interessato, ove possibile con e-mail, dell'avvenuta sospensione del certificato, specificando la data e l'ora a partire dalle quali il certificato non è più valido.

9.2. Riattivazione dei certificati sospesi

Il certificato sospeso è inserito nella Lista dei certificati sospesi, pubblicata nel Registro dei certificati.

La riattivazione del certificato va chiesta dallo stesso soggetto che ha avanzato l'istanza di sospensione mediante invio al Certificatore di apposita richiesta contenente i dati identificativi del titolare e del certificato.

La richiesta di riattivazione è avanzata con le modalità e osservando l'iter procedurale già descritto per le richieste di sospensione diverse da quelle di urgenza.

Il Certificatore procede alla riattivazione del certificato attraverso la cancellazione dello stesso dalla Lista dei certificati sospesi.

L'Ente Certificatore comunica al titolare e al terzo interessato l'avvenuta riattivazione del certificato, specificando la data e l'ora a partire dalle quali esso è nuovamente attivo.

Nel caso in cui, entro i 12 mesi successivi alla richiesta di sospensione, non venga chiesta, dallo stesso soggetto che ha chiesto la sospensione, l'attivazione o la revoca del certificato, quest'ultimo viene revocato d'ufficio.

9.3. Revoca dei certificati

Il titolare o il terzo interessato possono chiedere alla competente Filiale della Banca d'Italia la revoca del certificato al verificarsi delle causali riepilogate nella tabella che segue; per i dipendenti della Banca, la richiesta è avanzata dal dipendente stesso o dalla Struttura di appartenenza. Il Certificatore, qualora venga a conoscenza di sospetti abusi, falsificazioni, negligenze, si riserva la facoltà di revocare i certificati previa comunicazione motivata, salvo i casi di urgenza, ai titolari stessi.

RICHIEDENTE CAUSALE	TITOLARE (soggetto esterno o dipendente)	TERZO INTERESSATO	BANCA D'ITALIA (dipendenti)
SMARRIMENTO DELLA SMARTCARD (previa sospensione)	X	--	--
FURTO DELLA SMARTCARD (previa sospensione)	X	--	--
COMPROMISSIONE DELLA SICUREZZA (previa sospensione)	X	--	--
DETERIORAMENTO DELLA SMARTCARD	X	X	X
MODIFICA DELLA POSIZIONE TITOLARE[9]	--	X	X
ALTRO[10]	X	X	X

Le richieste con causale "altro" devono essere adeguatamente motivate.

La richiesta di revoca dovrà essere presentata alla competente Filiale anche per posta o tramite fax, corredata di copia del documento di identificazione del richiedente; laddove possibile, potrà essere inoltrata via posta elettronica, e sottoscritta con firma digitale[11].

Quando la richiesta è avanzata dal terzo interessato va sottoscritta dal legale rappresentante dell'ente ovvero da altro soggetto a ciò delegato.

La Filiale, verificata l'autenticità della stessa, provvede ad avviare il procedimento di revoca.

La Filiale informa il titolare e il terzo interessato dell'avvenuta revoca del certificato, specificando la data e l'ora a partire dalle quali il certificato non è più valido.

---

9 Causale da utilizzare ad esempio in caso di cessazione del titolare dall'attività lavorativa.

10 La causale "altro" comprende tutte le fattispecie non riconducibili a quelle espressamente individuate (es. va riferita a tale causale la richiesta di revoca che i terzi interessati devono avanzare in caso di cessazione delle attività per operazioni di fusione, liquidazione ecc.).

11 In caso di sottoscrizione con firma digitale non è richiesto alcun documento allegato.

Salvo i casi di smarrimento e furto, il titolare è tenuto a restituire o a far recapitare alla Filiale la smartcard in proprio possesso dopo averla resa inutilizzabile mediante taglio del microcircuito.

Qualora il titolare si rechi presso la Filiale, l'operazione di ritiro della smartcard viene verbalizzata. Il verbale viene redatto in duplice copia e sottoscritto dall'incaricato della Filiale e dal titolare; a quest'ultimo viene rilasciata una copia del verbale.

A seguito della revoca per smarrimento, furto, compromissione della sicurezza e deterioramento della smartcard, la Banca provvede d'ufficio all'avvio della procedura per il rinnovo del certificato.

9.4. Revoca dei certificati relativi alle chiavi dell'Ente Certificatore

L'Ente Certificatore procede alla revoca del certificato relativo alla coppia di chiavi di certificazione esclusivamente nei seguenti casi:

- compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza di quest'ultima;
- cessazione dell'attività.

La revoca avviene mediante inserimento del certificato nella Lista dei certificati revocati.

La revoca viene comunicata entro ventiquattro ore a DigitPA e a tutti i titolari di certificati qualificati emessi dall'Ente Certificatore firmati con la chiave privata appartenente alla coppia revocata.

Nel caso in cui la revoca discenda dalla compromissione della chiave privata dell'Ente Certificatore, vengono revocati d'ufficio tutti i certificati sottoscritti con detta chiave.

9.5. Disponibilità del servizio di sospensione

Il Certificatore garantisce, per ogni modalità di inoltro delle richieste di sospensione, una diversa disponibilità del servizio ad esse connesso:

- per le richieste di sospensione per furto, smarrimento e compromissione della sicurezza (richieste d'urgenza), da effettuare telefonicamente, il servizio di Help desk (tel. 06/47929341) è disponibile 24 ore su 24, tutti i giorni feriali e festivi;
- negli altri casi il servizio è disponibile negli orari di ufficio (8.30-16.30).

Ai fini della sospensione d'urgenza il titolare del certificato, su richiesta dell'operatore, dimostra la propria identità e comunica, a richiesta dell'operatore, la *pass-phrase*.

Qualora l'operazione di identificazione del richiedente non vada a buon fine, il certificato viene sospeso in via cautelativa. Entro le successive 24 ore il richiedente dovrà comunicare idonei elementi ai fini della sua identificazione.

9.6 Aggiornamento delle liste di revoca e di sospensione

Le liste di revoca e di sospensione sono aggiornate in seguito ad ogni richiesta.

La pubblicazione delle liste avviene al massimo ogni 24 ore.

9.7 Servizio OCSP

L'Ente Certificatore ha facoltà di rendere disponibili le informazioni sulla revoca e la sospensione dei certificati attraverso servizi OCSP, ai sensi dell'art. 19 della Deliberazione n. 45 del 21 maggio 2009.

10. MODALITA' DI SOSTITUZIONE DELLE CHIAVI

10.1. Sostituzione delle chiavi di firma del titolare

I certificati di firma hanno validità triennale; ove al titolare vengano rilasciati anche certificati ausiliari, tutti i certificati risiedono sul medesimo dispositivo di sicurezza.

In prossimità della scadenza dei certificati le Filiali provvedono a chiedere ai terzi interessati se, con riferimento a ciascun titolare, sia necessaria l'emissione di un set di certificati (firma e ausiliari) uguale a quello in scadenza (c.d. rinnovo).

In caso di risposta affermativa, il terzo interessato invia alla Filiale competente, via posta elettronica[12], una nota, sottoscritta con firma digitale dal legale rappresentante o da altro soggetto all'uopo delegato nella quale indica le generalità del titolare e le finalità per le quali viene richiesto il rinnovo; alla predetta nota il terzo interessato allega la richiesta di emissione dei certificati del titolare, da questi pure sottoscritta con firma digitale. In alternativa, il terzo interessato dovrà presentare la nota per posta o tramite fax, allegando la richiesta del titolare corredata di una copia del documento di identificazione.

Le richieste seguono l'iter procedurale descritto per la prima emissione, al termine del quale il titolare è invitato dalla Filiale competente a recarsi presso la Filiale stessa per la consegna della nuova smartcard, contenente i certificati rinnovati, e dei relativi codici segreti; nella circostanza viene ritirata la smartcard contenente i certificati in scadenza, dopo averla resa inutilizzabile mediante taglio del microcircuito.

Le suddette operazioni vengono verbalizzate; il verbale è redatto in duplice copia e sottoscritto dall'incaricato della Filiale e dal titolare, cui viene rilasciata una copia; l'avvenuta consegna della nuova smartcard e dei relativi codici segreti dà luogo alla successiva attivazione dei certificati.

10.2. Sostituzione delle chiavi di certificazione

Il Certificatore novanta giorni prima della scadenza del certificato relativo ad una chiave di certificazione avvia la procedura di sostituzione, generando una nuova coppia di chiavi (cfr. anche par.6.4).

[12] In tal caso la richiesta deve essere indirizzata alla casella funzionale della Filiale competente.

I certificati così generati sono inviati a DigitPA che provvede all'aggiornamento della lista dei certificati delle chiavi di certificazione contenuta nell'Elenco Pubblico dei certificatori.

10.3. Sostituzione delle chiavi di marcatura temporale

Le chiavi di marcatura temporale sono sostituite dopo non più di un mese di utilizzo, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato, in conformità a quanto stabilito dal DPCM 30.3.2009, art. 45, comma 2.

11. MODALITA' DI GESTIONE DEL REGISTRO DEI CERTIFICATI

Il registro dei certificati contiene:

- tutti i certificati emessi dal Certificatore;
- le liste dei certificati revocati e sospesi.

11.1. Gestione del Registro dei certificati

Del registro dei certificati (cd. directory master) esistono una o più copie operative (cd. directory shadow).

Tutte le operazioni che modificano il contenuto del registro sono riportate nel giornale di controllo.

Il registro è aggiornato ad ogni emissione, sospensione e revoca di certificati.

Le copie operative replicano il contenuto del directory master su più siti.

Almeno una copia è presente nel sito principale; ulteriori copie possono riportare completamente o in parte il contenuto del registro.

Le copie operative sono aggiornate ogni volta che viene aggiornato il directory master.

11.2. Accesso al Registro dei certificati

Il registro dei certificati è allocato su un sistema sicuro installato in locali protetti ed accessibile solo dal sistema di generazione dei certificati che vi registra i certificati emessi e le liste dei certificati revocati e sospesi.

L'accesso al registro dei certificati è consentito solo nella rete interna della Banca d'Italia.

L'accesso alla copia operativa del registro dei certificati avviene secondo il protocollo LDAP come definito nelle specifiche pubbliche RFC 1777 e successivi aggiornamenti, ovvero tramite indicazione della URL secondo quanto definito nella norma RFC 2255.

Per ciò che concerne le liste dei certificati revocati e sospesi, l'accesso è consentito sia con il protocollo HTTP sia con il protocollo LDAP.

12. MODALITÀ DI PROTEZIONE DELLA RISERVATEZZA

La Banca d'Italia garantisce la protezione della riservatezza dei dati trattati nell'ambito del servizio di certificazione.

Tutti i dati che risiedono nei database del sistema di certificazione sono protetti con modalità sicure.

Il trattamento dei dati è effettuato secondo processi prevalentemente automatizzati curati da operatori autorizzati che accedono ai dati sulla base di sistemi di autenticazione e di precise politiche di sicurezza.

Le misure di protezione adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali previste dal D. Lgs. 196/2003.

13. MODALITÀ PER L'APPOSIZIONE E LA DEFINIZIONE DEL RIFERIMENTO TEMPORALE

Il servizio di emissione di marche temporali da associare a documenti informatici reso disponibile dal Certificatore è riservato agli utenti in possesso di certificati di firma digitale emessi dalla Banca d'Italia.

La fruizione dei servizi di marcatura temporale da parte dei titolari dei certificati avviene mediante un'applicazione, fornita dal Certificatore e installata sulla postazione di lavoro dell'utente, e il sito Web della Banca raggiungibile tramite la rete Internet con protocollo sicuro. Il servizio è svolto con le seguenti modalità:

1. il titolare, tramite la predetta applicazione, produce la richiesta di marcatura temporale del documento informatico;
2. la richiesta viene trasmessa in modalità sicura al sistema del Certificatore;
3. il sistema del Certificatore verifica l'autenticità della richiesta e l'abilitazione del Titolare;
4. il sistema del Certificatore genera la marca temporale garantendo un tempo di risposta non superiore al minuto primo; l'emissione viene annotata nel Registro operativo;
5. la marca temporale viene restituita in modalità sicura al Titolare per il successivo utilizzo.

Il servizio di marcatura temporale consente anche la verifica delle marche temporali.

Lo strumento è realizzato in conformità a standard di qualità e sicurezza (ISO 9000). L'impronta del documento è generata con un algoritmo di hash corrispondente alla funzione SHA-256, in conformità all'art. 4, comma 3, della Deliberazione CNIPA n. 45 del 21 maggio 2009.

13.1. Chiavi di marcatura temporale

Le chiavi di marcatura temporale sono destinate alla generazione e alla verifica delle marche temporali (art. 4, comma 4, lett. C, del DPCM 30.3.2009).

La marca temporale è un'evidenza informatica, sottoposta a firma, contenente una serie di indicazioni (art. 44, DPCM 30.3.2009):

- identificativo dell'emittente;

- numero di serie della marca temporale;
- algoritmo di sottoscrizione della marca temporale;
- identificativo del certificato relativo alla chiave di verifica della marca;
- data e ora di generazione della marca;
- identificatore dell'algoritmo di hash (SHA-256) utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
- valore dell'impronta dell'evidenza informatica.

Ogni coppia di chiavi utilizzata per la validazione temporale è univocamente associata al sistema di validazione temporale (art. 45, comma 1, DPCM 30.3.2009).

13.2. Conservazione e validità della marca temporale

Tutte le marche temporali emesse dal sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni.

Le marche temporali sono valide per l'intero periodo di conservazione.

13.3. Riferimenti temporali apposti sul giornale di controllo

I riferimenti temporali apposti sul giornale di controllo derivano da un sistema alimentato da una sorgente esterna (ETS, External Time Source) fornita dal National Institute of Standards and Technology (NIST - Colorado, USA). Tali riferimenti corrispondono alla scala di tempo UTC(IEN) con una differenza non superiore al minuto primo.

14. VERIFICA DELLE FIRME DIGITALI

Il Certificatore, secondo quanto previsto dall'art. 10 del DPCM 30/03/2009, rende disponibile o indica ai titolari e agli utilizzatori un sistema che consente di effettuare la verifica delle firme digitali.

Il sistema per la verifica delle firme digitali, da utilizzare con una connessione internet attiva, consente di:

- verificare la validità del certificato del firmatario e la qualifica di certificatore accreditato dell'emittente;
- accertare l'integrità del documento firmato;
- verificare la validità della firma nel periodo di vigenza del corrispondente certificato, coerentemente con quanto previsto dalla Deliberazione CNIPA 45/2009. art. 27, comma 3.

Per l'effettuazione della descritta operazione di verifica della firma non è richiesta la disponibilità di dispositivi, quali smartcard e relativi lettori.

15. MODALITÀ OPERATIVE PER LA GENERAZIONE DELLA FIRMA DIGITALE

L'apposizione della firma digitale a un documento può essere sintetizzata nelle seguenti operazioni:

- calcolo dell'impronta del documento mediante una funzione matematica detta di *hash*;
- cifratura dell'impronta così ottenuta mediante un algoritmo asimmetrico RSA che utilizza la chiave privata del titolare contenuta nel dispositivo sicuro di firma (smartcard).

Il titolare svolge tali operazioni in maniera trasparente mediante il software di firma ricevuto dal Certificatore unitamente al dispositivo di firma[13].

Il software richiede la selezione del documento da firmare e ne consente la visualizzazione da parte del titolare prima dell'apposizione della firma.

Quando il titolare decida di firmare il documento, il software richiede in maniera esplicita di confermare la volontà di apporre la firma al documento elettronico visualizzato.

[13] Le istruzioni per l'utilizzo del software di firma sono riportate nell'allegato 1.

In caso di assenso, il software richiede la digitazione del codice PIN della smartcard, previo inserimento della stessa nel lettore, e procede quindi alla produzione del documento informatico.

15.1. Formato dei documenti

L'automazione di ufficio ha introdotto un largo uso di formati documentali che arricchiscono il "contenuto" del documento con macroistruzioni o codice eseguibile finalizzati ad incrementarne il riuso (es. modulistica, campi data, numerazione pagine, formattazione testo) o, ad esempio, ad effettuare calcoli matematici.

Occorre però tener conto che la presenza di elementi di codice interpretati dal software applicativo (ad esempio, Microsoft Office) potrebbe alterare il contenuto originario del documento, modificando "gli atti, i fatti o i dati rappresentati nel documento" (art. 3, comma 3, del DPCM 30.3.2009) al momento della sottoscrizione.

Pertanto si suggerisce l'uso di formati documentali statici quali ad esempio:

puro testo – ".txt";

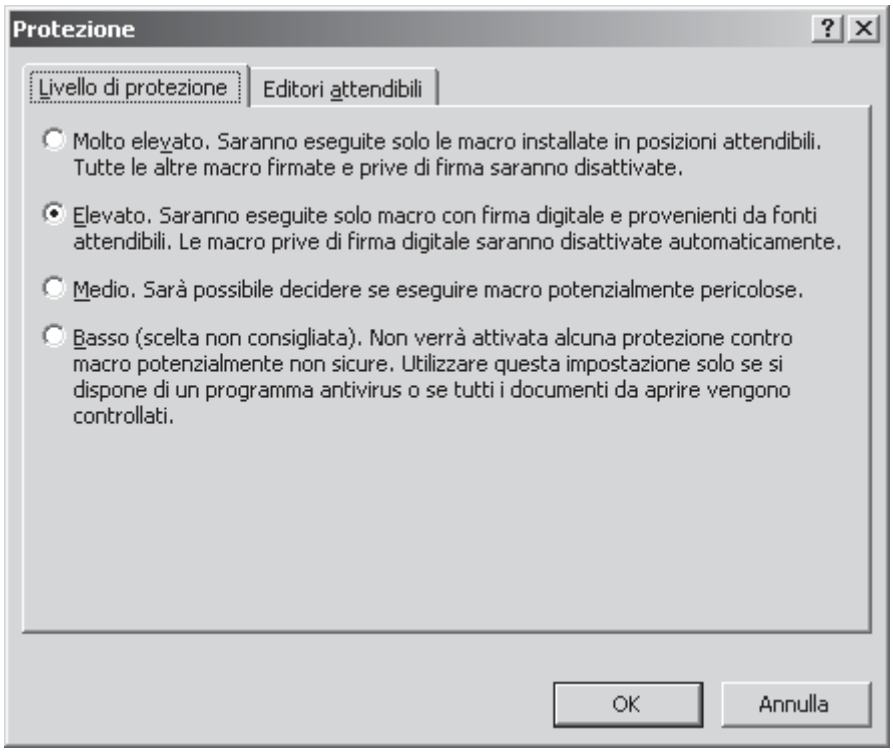
Portable Document Format – ".pdf" (se privo di campi modulo o javascript).

Nel caso in cui sia indispensabile l'utilizzo di formati quali ad esempio .doc, .dot, .rtf, .xls, prima di procedere alla sottoscrizione del documento è opportuno individuare la presenza di campi dinamici. Si riportano di seguito alcuni suggerimenti utili ai fini dell'individuazione di oggetti e campi variabili all'interno dei documenti.

15.1.1 Macro

Una **macro** è una procedura, codificata in un linguaggio di programmazione specifico, che è possibile utilizzare per automatizzare una sequenza di operazioni all'interno dei prodotti Microsoft Office®.

Per verificare il livello di protezione delle macro in MS Word® o MS Excel®, occorre aprire il menu **Strumenti**, selezionare **Macro**, quindi **Protezione**, in modo che compaia la finestra seguente:



Si precisa che scegliendo livelli di protezione elevati, le macro rimangono presenti nel documento anche se non eseguite.

15.1.2 Codici di campo

I **codici di campo** sono oggetti che consentono di inserire all'interno del documento valori dinamici come numeri di pagina, indici, riferimenti incrociati, ecc. Per visualizzare i codici di campo presenti in un documento, aprire il menu **Strumenti**, scegliere **Opzioni** e nella scheda **Visualizza** accertarsi che siano selezionate le caselle **Testo nascosto, Ancoraggi oggetti, Codici di campo** con **Ombreggiatura campo: sempre**.

Sarà possibile in tal modo visualizzare tutti i codici di controllo presenti nel documento per verificare se detti codici siano tali da modificarne il contenuto dopo la sua sottoscrizione.

I codici campo possono essere sostituiti in testo normale posizionandosi con il cursore sul campo e digitando la combinazione di tasti CTRL+SHIFT+F9. Tale operazione può essere effettuata sull'intero documento selezionando tutto il testo e premendo CTRL+SHIFT+F9.

15.1.3 Oggetti

Per visualizzare la presenza di collegamenti a oggetti esterni in un documento MS Word®, quali ad esempio un foglio elettronico MS Excel®, aprire il menu **Visualizza** e scegliere **Struttura**.

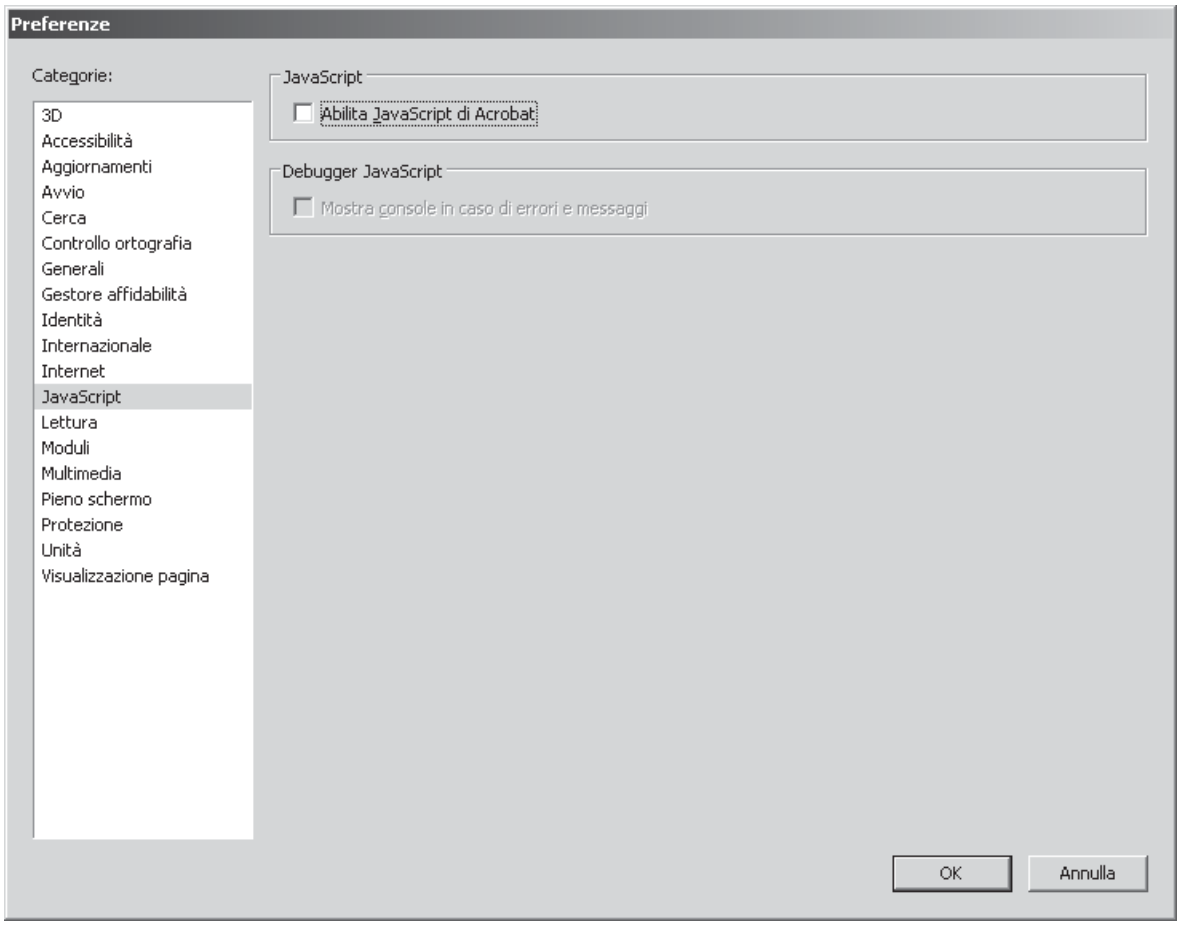
15.1.4 Formule

Per visualizzare le **Formule** in MS Excel®, aprire il menu **Strumenti**, scegliere **Opzioni** e nella scheda **Visualizza** spuntare la casella **Formule**.

15.1.5 Javascript

I documenti PDF possono contenere codice Javascript che aggiunge funzionalità dinamiche per la validazione dei moduli, l'accesso a basi dati locali e il controllo di oggetti multimediali.

L'esecuzione di codice Javascript in Adobe® Reader è abilitata per default; per disabilitarla, occorre aprire il menu **Modifica**, scegliere **Preferenze**, quindi la categoria **Javascript** nella colonna di sinistra e deselezionare la casella **Abilita Javascript di Acrobat**. (la figura seguente si riferisce alla versione 7 di Adobe® Reader).


Preferenze
Categorie:
3D
Accessibilità
Aggiornamenti
Avvio
Cerca
Controllo ortografia
Generali
Gestore affidabilità
Identità
Internazionale
Internet
JavaScript
Lettura
Moduli
Multimedia
Pieno schermo
Protezione
Unità
Visualizzazione pagina
JavaScript
Abilita JavaScript di Acrobat
Debugger JavaScript
Mostra console in caso di errori e messaggi
OK
Annulla

ALLEGATO 1 Manuale di utilizzo del software di firma

BANCA D'ITALIA

EUROSISTEMA

MANUALE DI UTILIZZO DEL SOFTWARE DI FIRMA

Introduzione

Il software di firma consente la firma digitale, la marcatura temporale di file di ogni tipo e dimensione, nel rispetto della normativa vigente e degli standard tecnici di riferimento.

Molto versatile e di facile uso, l'applicazione è disponibile per ambiente Windows, MacOS X e Linux.

Questa guida fornisce le informazioni essenziali per l'uso dell'applicazione.

Concetti di base

Firma digitale

La firma digitale è un'operazione con la quale si genera un codice crittografico che dimostra l'**identità** e l'**integrità** di un documento. In altre parole, la firma digitale permette di verificare che il documento:

- è stato firmato da una ben precisa persona
- successivamente, non ha subito modifiche

La firma digitale si basa su algoritmi crittografici che richiedono il possesso, da parte dell'utente, di una **chiave privata** e di un corrispondente **certificato**. La chiave privata ed il certificato sono normalmente memorizzati su un dispositivo elettronico simile ad una carta di credito, chiamato **smartcard**, oppure su un **token USB** (in entrambi i casi si tratta di microchip con funzionalità crittografiche):

Smartcard

Token USB

In fase di generazione della firma, è necessario digitare il **PIN** della propria smartcard o dispositivo USB.

Il certificato è un piccolo file contenente informazioni essenziali per la verifica della firma:

- il nome ed il codice fiscale dell'utente titolare (es. Mario Rossi)
- il nome dell'azienda di appartenenza, se applicabile
- il nome dell'ente certificatore (es. Banca d'Italia)
- la data di inizio e la data di fine validità
- la **chiave pubblica** del titolare
- altre informazioni di servizio

Il certificato viene rilasciato all'utente da un ente terzo fidato, detto **certificatore** (Certification Authority, CA).

Dopo aver generato una firma digitale, questa viene solitamente salvata in un file detto **busta crittografica**; la busta contiene normalmente anche il documento di partenza ed il certificato del firmatario, così da tenere insieme tutte le informazioni necessarie per la verifica.

Esistono diversi formati di busta crittografica; il più diffuso è quello conosciuto come PKCS#7 (in tal caso il file ha l'estensione **P7M**).

Affinché la firma digitale abbia un pieno valore legale (in tal caso si parla di firma **qualificata**), devono essere rispettate diverse norme di legge che stabiliscono requisiti relativi alle chiavi, al certificato, alla smartcard, al certificatore, al formato della busta crittografica, eccetera.

La icona di un documento firmato con l'applicazione assume il seguente aspetto:

Marcatura temporale

La **marcatura temporale** (time-stamping) di un documento è un'operazione con la quale si ottiene, da un ente terzo fidato, un piccolo file chiamato marca temporale;

questa permette di dimostrare che il documento di partenza effettivamente esisteva non più tardi di un dato momento (data e ora), così da poter risolvere eventuali contestazioni al riguardo. La marcatura temporale di un documento può essere molto importante in diverse situazioni, come ad esempio:

- trasmissione di documenti entro una data-limite
- invio di offerte in risposta a gare d'appalto
- deposito di contratti di qualsiasi genere
- sottomissione di richieste di brevetto

Inoltre, la marcatura temporale di un documento firmato permette di accertare la data-ora in cui la firma digitale è stata effettivamente apposta, quando tale informazione non sia ottenibile in altro modo.

La marca temporale (time-stamp token) si ottiene inviando una opportuna richiesta attraverso Internet ad un ente detto **Time-Stamping Authority** (TSA). La richiesta contiene l'impronta (digest) del documento. La TSA risponde generando la marca temporale ed inviandola all'utente. La marca temporale contiene:

- data e ora certa di generazione
- impronta (digest) del documento
- nome della TSA
- firma digitale della TSA
- altre informazioni di servizio

Affinché la marcatura temporale abbia un pieno valore legale, essa deve essere ottenuta da un certificatore accreditato che opera nel rispetto delle norme vigenti. Il ruolo di TSA è dunque svolto da un certificatore.

La icona di una marca temporale ottenuta con l'applicazione assume il seguente aspetto:

Firmare un file

Per poter firmare un file, dovete avere almeno un certificato valido di firma sulla vostra smartcard. Se ne avete più di uno, in fase di firma dovrete scegliere il certificato desiderato.

Si può avviare la firma digitale di un file in tre modi diversi, descritti di seguito:

- dall'esterno dell'applicazione, attraverso il menu contestuale di Windows Explorer
- dall'esterno dell'applicazione, mediante "drag-and-drop"
- dall'interno dell'applicazione di firma

Il **primo metodo**, disponibile al momento solo in ambiente Windows, consiste nel cliccare sull'icona del file desiderato con il tasto destro del mouse, per visualizzare il menu contestuale; qui selezionare la voce "**Firma con File Protector**" per avviare l'applicazione e firmare il file. Vi verrà richiesto il PIN della smartcard. La firma digitale verrà salvata nella stessa cartella del documento di partenza, con estensione P7M. Per esempio, la firma del file contratto.pdf verrà salvata in un file di nome contratto.pdf.p7m.

Il **secondo metodo** è particolarmente comodo se l'applicazione è già avviata. In tal caso, la firma di un file si può avviare trascinando l'icona del file desiderato sopra l'area-bersaglio.

Come **terzo metodo**, se l'applicazione è già avviata, per avviare la firma di un file si può anche:

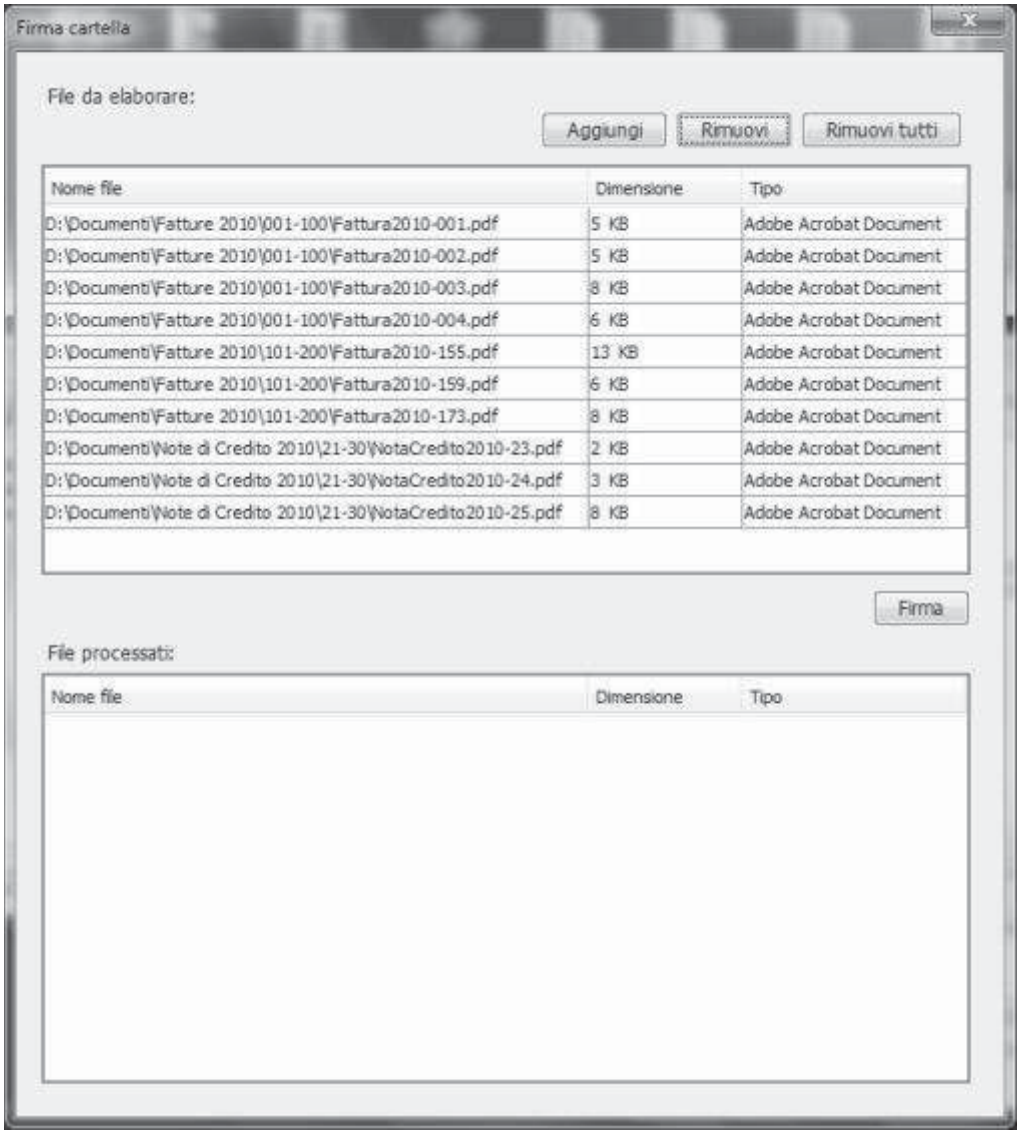
- selezionare la voce "**Firma**" dal menu "**File**"
- oppure cliccare sul bottone "**Firma**" della toolbar

In entrambi i casi verrà visualizzata una finestra di selezione file per consentirvi di scegliere il file desiderato.

Avviando la firma dall'interno dell'applicazione, è possibile eseguire anche una *firma multipla* (vedere la sezione relativa).

Firma in unica soluzione

Selezionando la voce di menu "**Firma in unica soluzione**" (oppure cliccando sul bottone corrispondente) appare una finestra di dialogo che permette di firmare "in un'unica soluzione" un insieme qualsiasi di file, anche residenti in cartelle diverse:



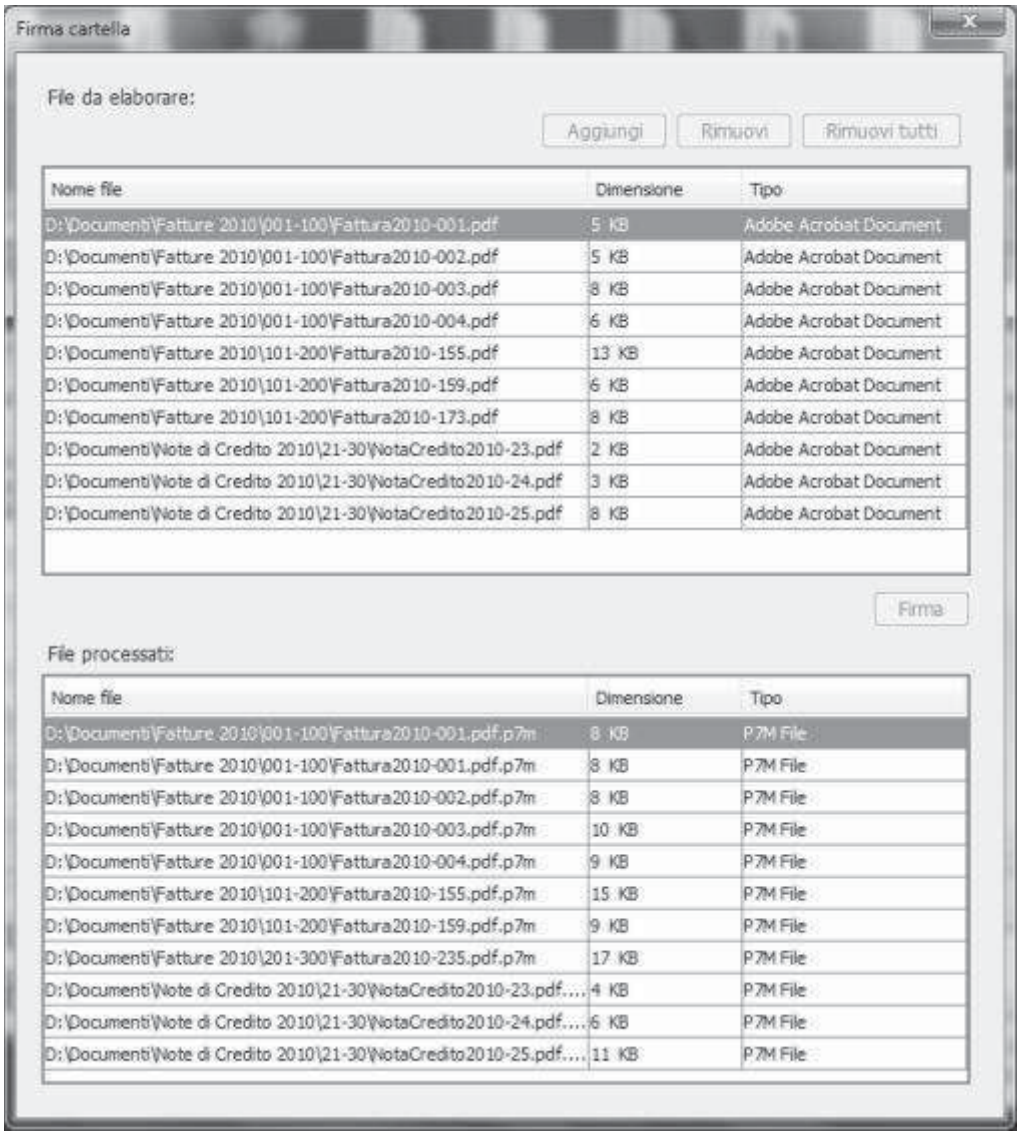
La parte superiore della finestra ("basket") elenca i file che verranno firmati. L'elenco può essere compilato sia cliccando sul bottone "**Aggiungi**" e selezionando un file, sia *trascinando* l'icona del file desiderato sull'elenco stesso

(drag and drop). Possono essere aggiunti al basket anche file già firmati (in questo caso verrà aggiunta ad essi una ulteriore firma).

Come si può intuire, i bottoni "Rimuovi" e "Rimuovi tutti" permettono di eliminare dal basket il file selezionato oppure tutti quanti.

Volendo controllare un documento prima della firma, è sufficiente fare doppio-clic sulla voce corrispondente nell'elenco "da elaborare": il file sarà aperto nell'applicazione associata (per es. nel caso di un documento PDF si aprirà tipicamente Adobe Reader).

Cliccando infine sul bottone "**Firma**", verrà avviato il processo di firma digitale (in formato P7M) di tutti i file dell'elenco. Le buste P7M risultanti, elencate nella parte inferiore della finestra, vengono salvate nella stessa cartella del documento di origine:



Al termine, per dismettere la finestra premere il tasto ESC oppure cliccare sull'icona di chiusura.

Firmare una cartella

Con l'applicazione è possibile firmare tutti i file presenti in una cartella con una singola operazione.

Sono disponibili due modalità di firma di una cartella:

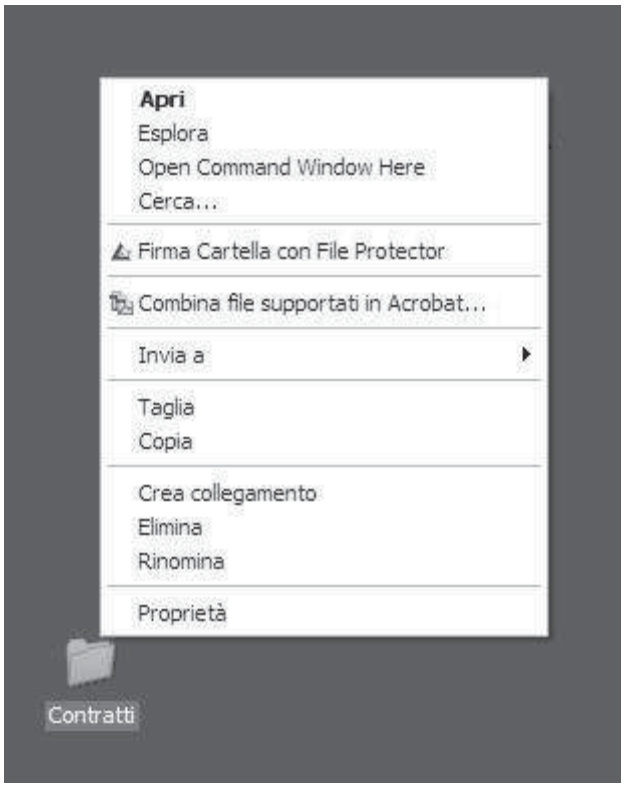
- firma individuale di ciascun file
- firma di un elenco delle impronte dei file

Nel primo caso vengono prodotte tante buste crittografiche P7M quanti sono i file presenti nella cartella di input. Nel secondo caso, invece, viene prodotta una singola busta crittografica in formato XML. Il secondo metodo è più veloce e consente un forte risparmio di spazio su disco, quando la cartella di input contiene molti documenti.

Come nel caso della firma di un singolo file, si può avviare la firma di una cartella in tre modi diversi:

- dall'esterno dell'applicazione, attraverso il menu contestuale di Windows Explorer
- dall'esterno dell'applicazione, mediante "drag-and-drop"
- dall'interno dell'applicazione

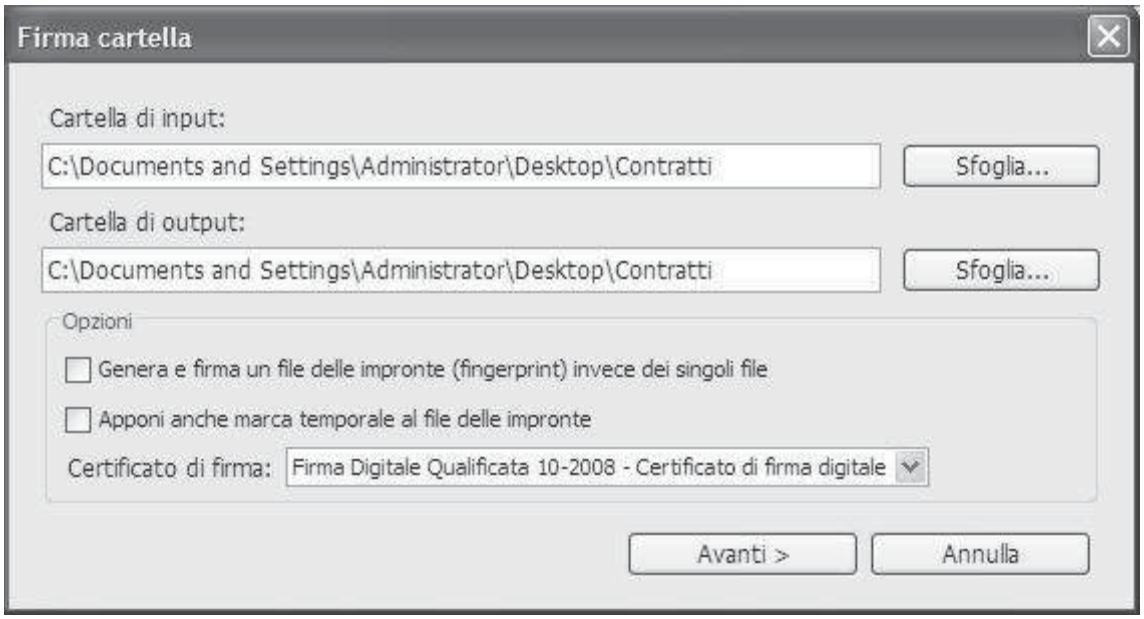
Il **primo metodo**, disponibile al momento solo in ambiente Windows, consiste nel cliccare sull'icona della cartella desiderata con il tasto destro del mouse, per visualizzare il menu contestuale; qui selezionare la voce "**Firma Cartella con File Protector**" per avviare l'applicazione ed avviare il processo di firma.



Il **secondo metodo** è particolarmente comodo se l'applicazione è già avviata. In tal caso, la firma di una cartella si può avviare trascinando l'icona della cartella desiderata sopra l'area-bersaglio (vedere la figura).

Il **terzo metodo**, utilizzabile se l'applicazione è già avviata, consiste nel selezionare la voce "**Firma Cartella**" dal menu "**File**".

Qualunque sia il metodo scelto per avviare la firma di una cartella, apparirà la seguente finestra di dialogo:



In questa finestra occorre scegliere la modalità di firma desiderata e le relative opzioni. Dopodiché, cliccando sul bottone "**Avanti>**" il processo di firma avrà inizio.

Firmare in modalità PDF

In un documento PDF (Portable Document Format) è possibile inserire una o più firme digitali senza necessità di produrre una busta crittografica separata. L'applicazione è in grado di generare anche firme in standard PDF; l'utente può quindi scegliere tra la firma classica (P7M) oppure la firma PDF, secondo necessità.

La firma in standard PDF ha il vantaggio di poter essere verificata col visualizzatore Adobe Reader, di ampia diffusione, e di poter avere una rappresentazione grafica che la rende più facilmente confrontabile con la firma tradizionale (autografa). Per contro, la firma in standard PDF è per adesso meno diffusa ed accettata della firma P7M, pur avendo lo stesso valore dal punto di vista tecnico e legale, ed è applicabile solo ai documenti in formato PDF.

Esistono due tipi di firma PDF dal punto di vista "grafico":

- firma *invisibile* (senza rappresentazione grafica)
- firma *visibile* (con rappresentazione grafica)

L'applicazione è sempre in grado di produrre una firma PDF "invisibile", mentre per produrre una firma visibile è necessario che il documento PDF contenga un **campo firma** apprositamente predisposto. Ad ogni firma apposta al documento corrisponde una "revisione" del documento stesso.

Le firme PDF si differenziano poi in:

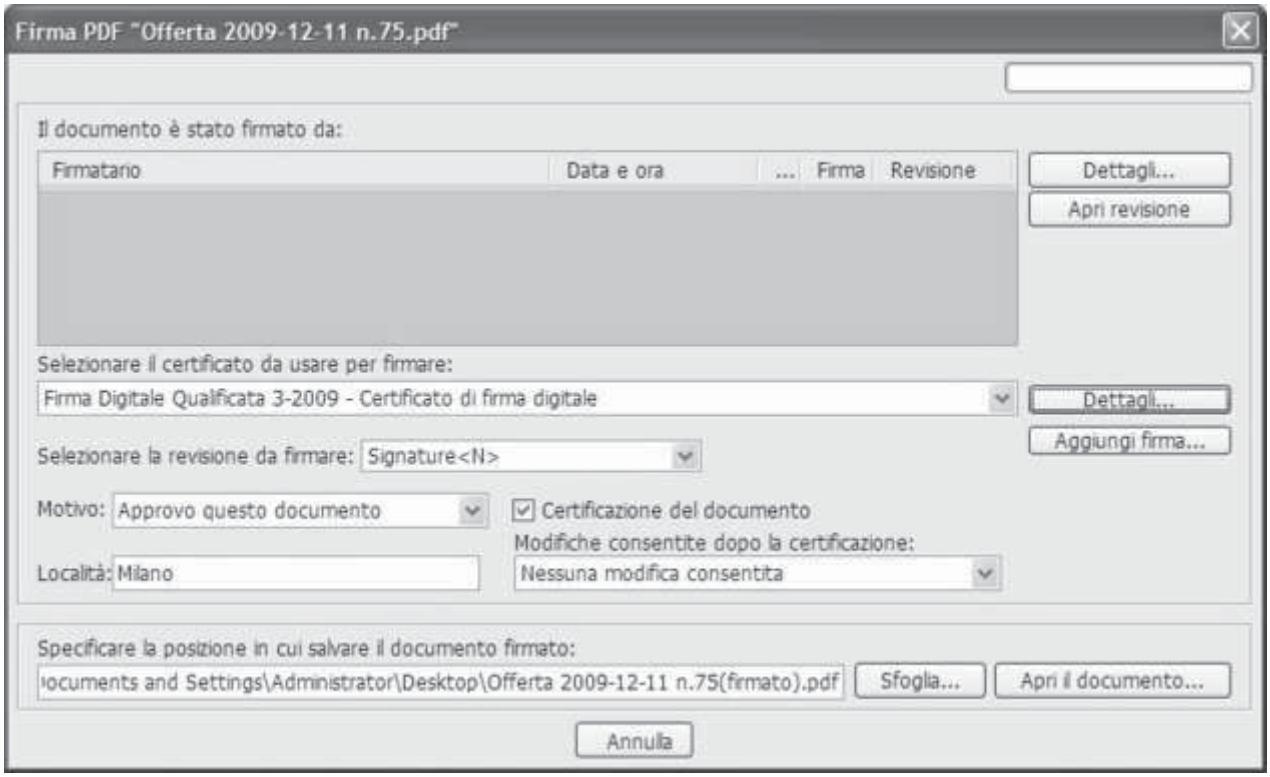
- firma di *certificazione*
- firme di *approvazione*

La "firma di approvazione" è quella che generalmente si appone su un documento prodotto da altri e non ha altri effetti se non quello di attestare l'identità del firmatario e l'integrità del documento.

La "firma di certificazione", invece, consente anche di impostare permessi sul documento che limitano le successive modifiche. Solitamente, chi appone una firma di certificazione è l'autore o responsabile del documento. Inoltre, una firma di certificazione viene *sempre evidenziata* dalle applicazioni Adobe, anche se non apposta in un campo firma.

Entrambi i tipi di firma sono supportati dall'applicazione.

Per firmare un documento in standard PDF si deve selezionare la voce "**Firma PDF**" dal menu "**File**". Dopo aver selezionato il documento desiderato, compare la seguente finestra di dialogo:



Volendo apporre una firma di certificazione, selezionare la casella corrispondente e scegliere dal menu a discesa i permessi desiderati.

È possibile, opzionalmente, compilare i campi "Motivo" e "Località"; in tal caso, tali informazioni saranno anch'esse firmate.

Infine, per aggiungere una firma al documento basta scegliere il certificato desiderato e cliccare sul bottone "**Aggiungi firma**".

* * *

È anche possibile avviare il processo di firma PDF dal menu contestuale di Windows, cliccando col tasto destro del mouse sul documento desiderato e poi selezionando la voce di menu "**Firma PDF con File Protector**"

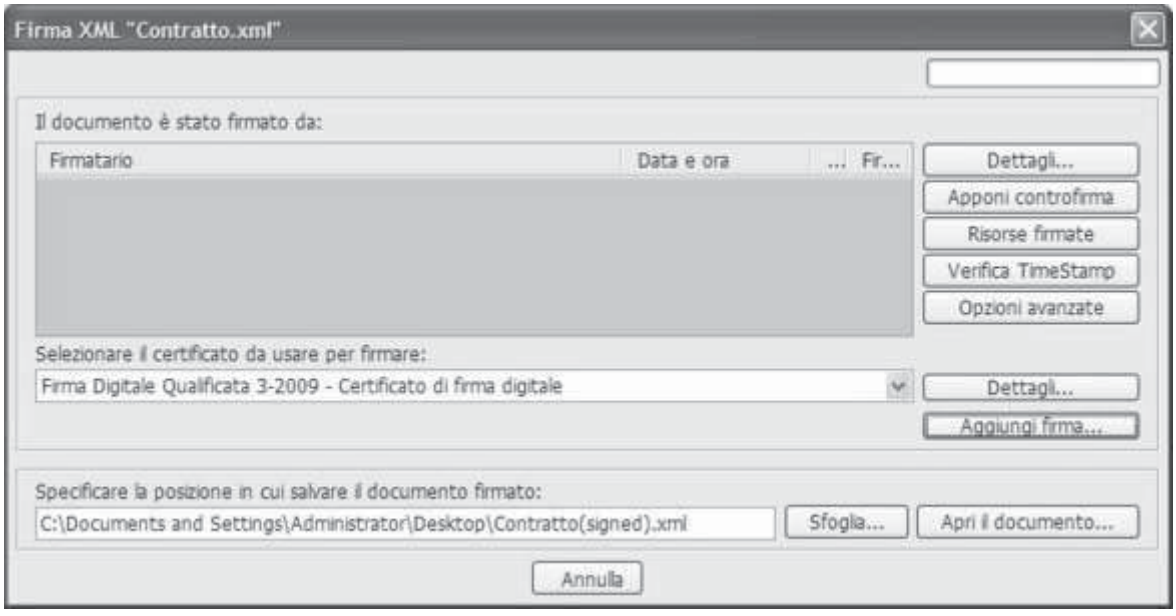
Firmare in modalità XML

In alternativa ai formati P7M e PDF, la firma digitale può anche avere una codifica di tipo XML (eXtended Markup Language). La firma in modalità XML è particolarmente adatta ai documenti che sono essi stessi in formato XML, ma può essere applicata a documenti di qualsiasi tipo.

La firma in standard XML non è ancora molto diffusa, essendo usata prevalentemente nell'ambito sanitario e bancario; tuttavia, la firma XML ha lo stesso valore tecnico e legale degli altri formati (P7M e PDF).

Rispetto alla firma P7M, la firma in modalità XML è più flessibile ma anche più "tecnica": può infatti assumere tre diverse forme (*enveloped*, *enveloping*, *detached*) e prevede numerose opzioni che in questa guida, per brevità, non approfondiamo.

Per firmare un documento in modalità XML, selezionare la voce "**Firma XML**" dal menu "**File**"; dopo aver selezionato il documento desiderato, apparirà la seguente finestra di dialogo:



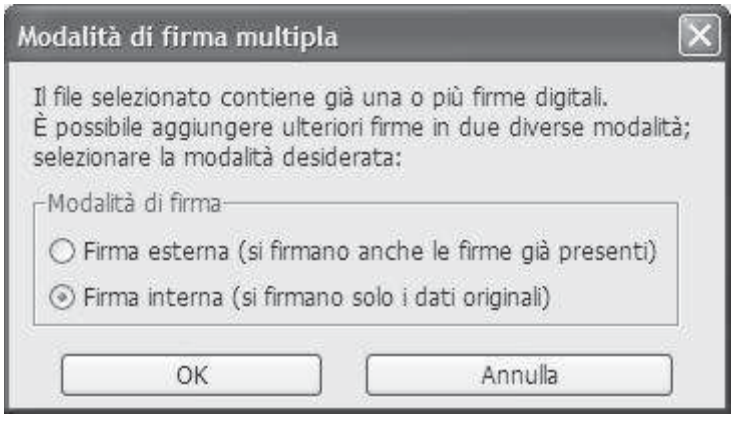
Eseguire firme multiple

Ad un medesimo documento possono essere apposte più firme digitali; si parla in tal caso di "firme multiple". Questo consente di dimostrare che più persone hanno assunto la paternità e/o la responsabilità del documento, eventualmente in momenti diversi, così come spesso avviene nel caso della tradizionale firma autografa (basti pensare ai contratti, ai bilanci, ecc).

Esistono tre tipologie di firme multiple:

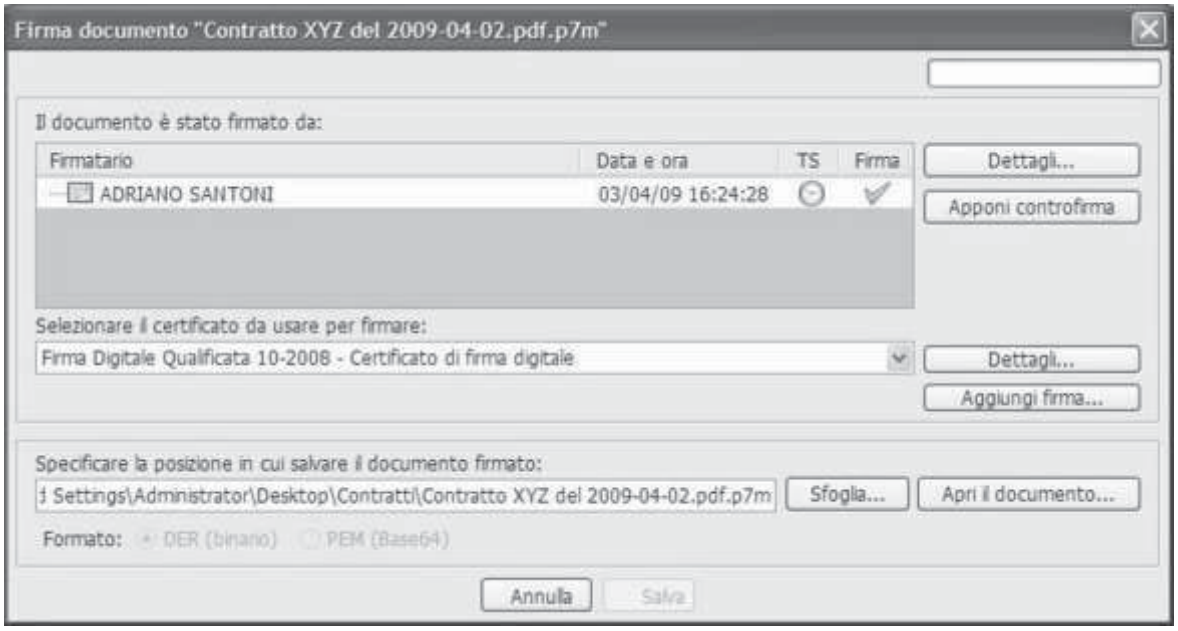
- firme "a matrioska"
- firme parallele (anche dette *indipendenti*)
- contro-firme (anche dette *annidate*)

Il primo tipo si ottiene semplicemente firmando una busta crittografica P7M (che contiene un documento già firmato). Questa operazione digitale equivale, nel mondo della carta, a firmare una busta che contiene un documento firmato, ciò che in effetti a volte viene fatto (si pensi alle buste che contengono le offerte in risposta a bandi di gara). Per effettuare una firma "a matrioska" con l'applicazione, occorre agire dall'interno dell'applicazione, cliccando sul bottone "**Firma**" oppure selezionando la corrispondente voce di menu. Quando l'applicazione si accorge che il documento selezionato è in effetti una busta P7M, visualizza la seguente finestra di dialogo:

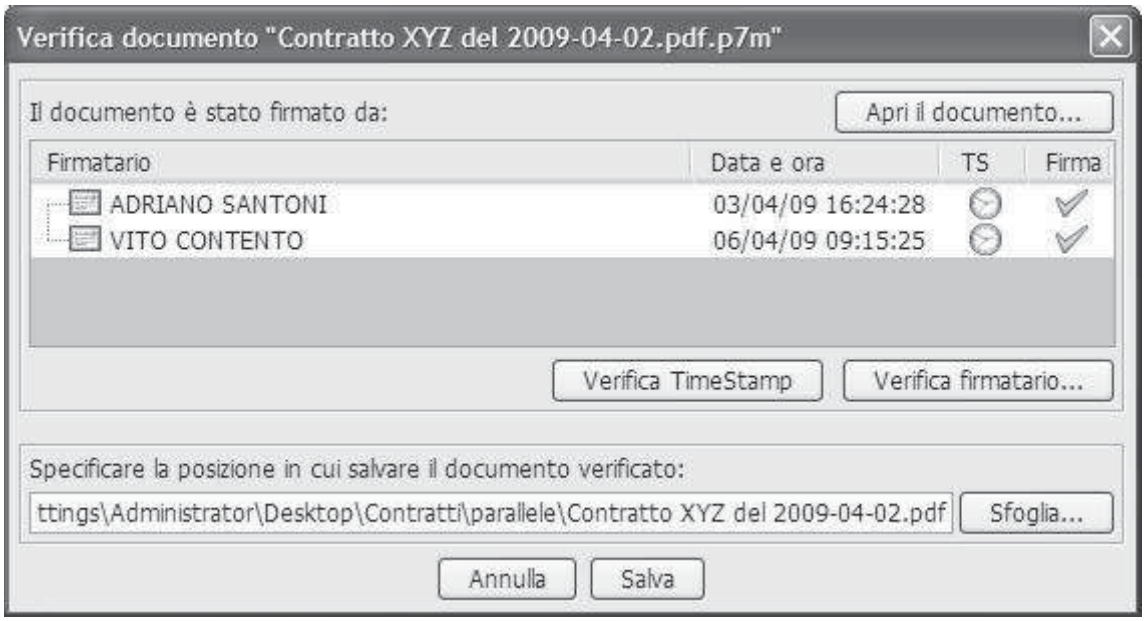


A questo punto, per fare una firma multipla "a matrioska" si deve selezionare la voce "**Firma esterna**".

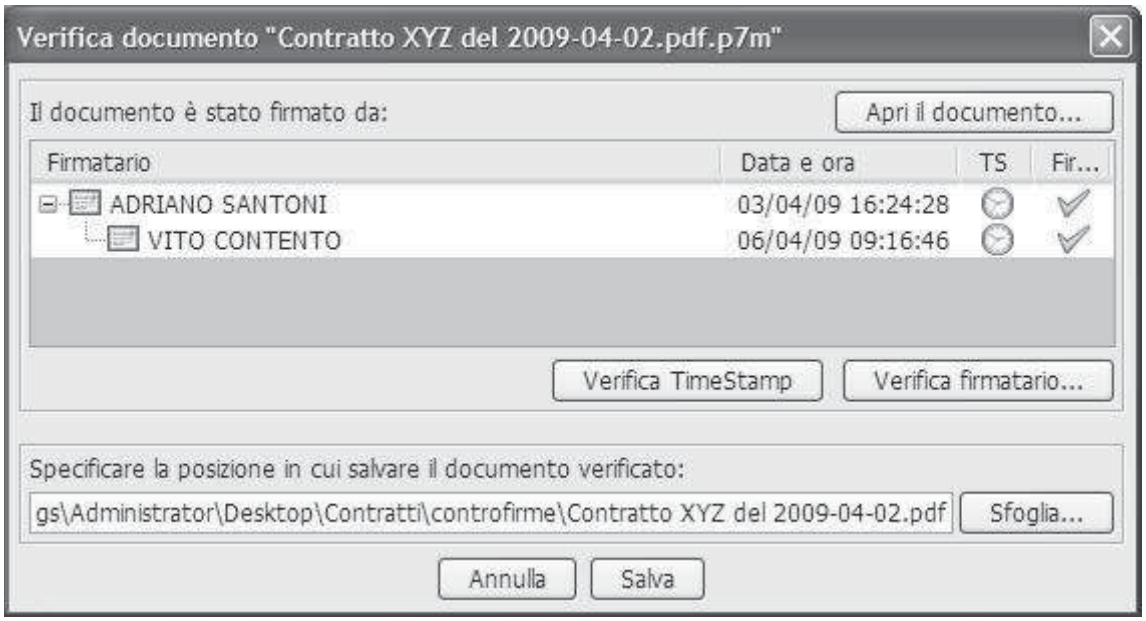
Selezionando invece la voce "**Firma interna**", sarà possibile eseguire firme multiple del secondo e del terzo tipo; apparirà a questo punto la seguente finestra di dialogo:



Il secondo tipo di firma multipla (detta *parallela* o *indipendente*) consiste nell'aggiungere ulteriori firme "a fianco" della prima, dove ciascuna firma mantiene la sua indipendenza (ogni firmatario firma gli stessi dati che firmano gli altri). Questa operazione digitale equivale, nel mondo della carta, ad apporre più firme, da parte di persone diverse, in calce al medesimo documento. Per aggiungere una firma indipendente, cliccare sul bottone "**Aggiungi firma...**" nella finestra mostrata sopra. In fase di verifica, si potrà constatare che il documento contiene le firme aggiunte:



Il terzo tipo di firma multipla (detta *controfirma* o *annidata*) si ottiene firmando una firma già esistente, e conservando il risultato (detto contro-firma) all'interno della medesima busta. Facendo questo, il secondo firmatario in pratica approva o "convalida" la prima firma. A sua volta, la seconda firma può essere firmata da una terza persona, e così via. Per aggiungere una controfirma, selezionare la firma desiderata poi cliccare sul bottone "**Apponi controfirma**" nella finestra mostrata sopra. In fase di verifica, si potrà constatare che il documento contiene la contro-firma (notare la rappresentazione ad albero):

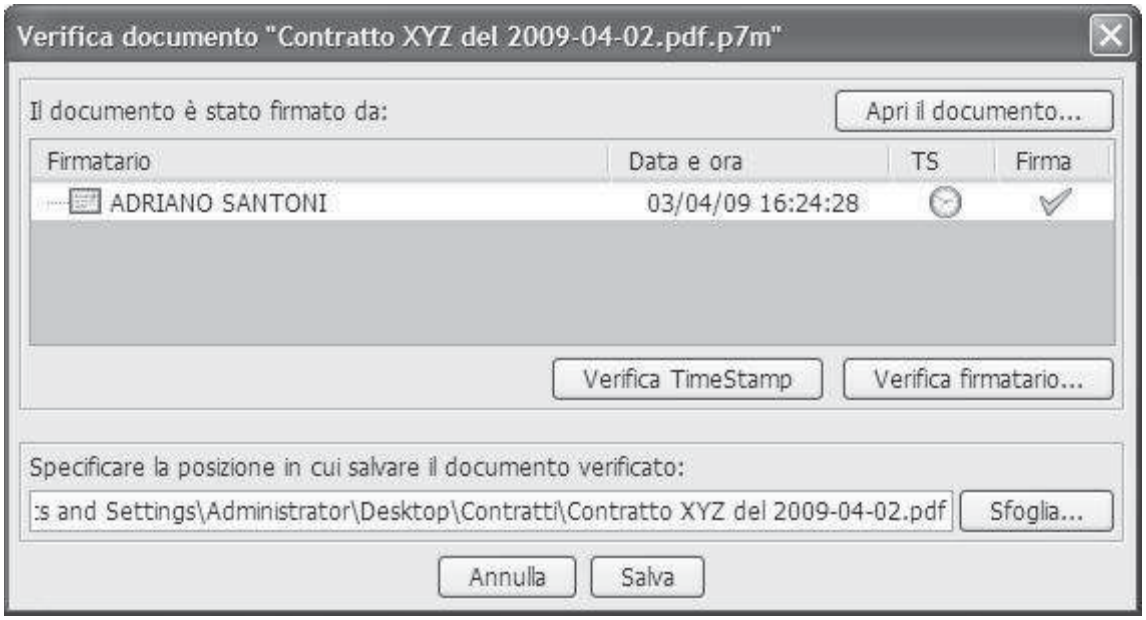

Verifica documento "Contratto XYZ del 2009-04-02.pdf.p7m"
Il documento è stato firmato da:
Apri il documento...
Firmatario
Data e ora
TS
Fir...
ADRIANO SANTONI
03/04/09 16:24:28
VITO CONTENTO
06/04/09 09:16:46
Verifica TimeStamp
Verifica firmatario...
Specificare la posizione in cui salvare il documento verificato:
gs\Administrator\Desktop\Contratti\controfirme\Contratto XYZ del 2009-04-02.pdf
Sfoglia...
Annulla
Salva

Verificare

La verifica di un documento firmato in standard P7M si può avviare in cinque modi diversi:

- facendo "doppio-clic" sul file da verificare
- attraverso il menu contestuale di Windows Explorer (selezionare la voce "**Verifica con File Protector**")
- mediante "drag-and-drop" (trascinamento del documento sull'area bersaglio)
- cliccando sul bottone "**Verifica**" oppure selezionando la voce di menu "**File**" > "**Verifica**"

Al termine della verifica, apparirà la seguente finestra:



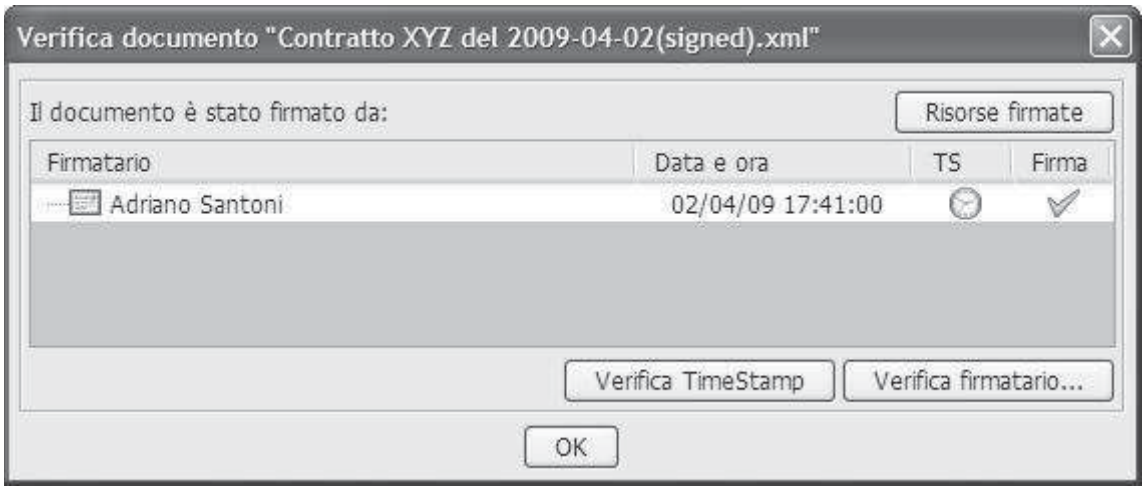
Da questa finestra è possibile:

- verificare la validità della firma
- verificare la validità del certificato di ogni firmatario
- visualizzare il documento fimato, estrarlo e salvarlo su file
- visualizzare e verificare la marca temporale (se presente) associata alla firma

La verifica di un documento firmato in standard XML si può avviare in due modi diversi:

- dall'esterno dell'applicazione, attraverso il menu contestuale di Windows Explorer (come sopra)
- dall'interno dell'applicazione (come sopra)

Al termine della verifica, apparirà la seguente finestra:



Da questa finestra è possibile:

- verificare la validità della firma
- verificare la validità del certificato di ogni firmatario
- visualizzare l'elenco delle risorse fimate ed eventualmente salvarle su file
- visualizzare e verificare la marca temporale (se presente) associata alla firma

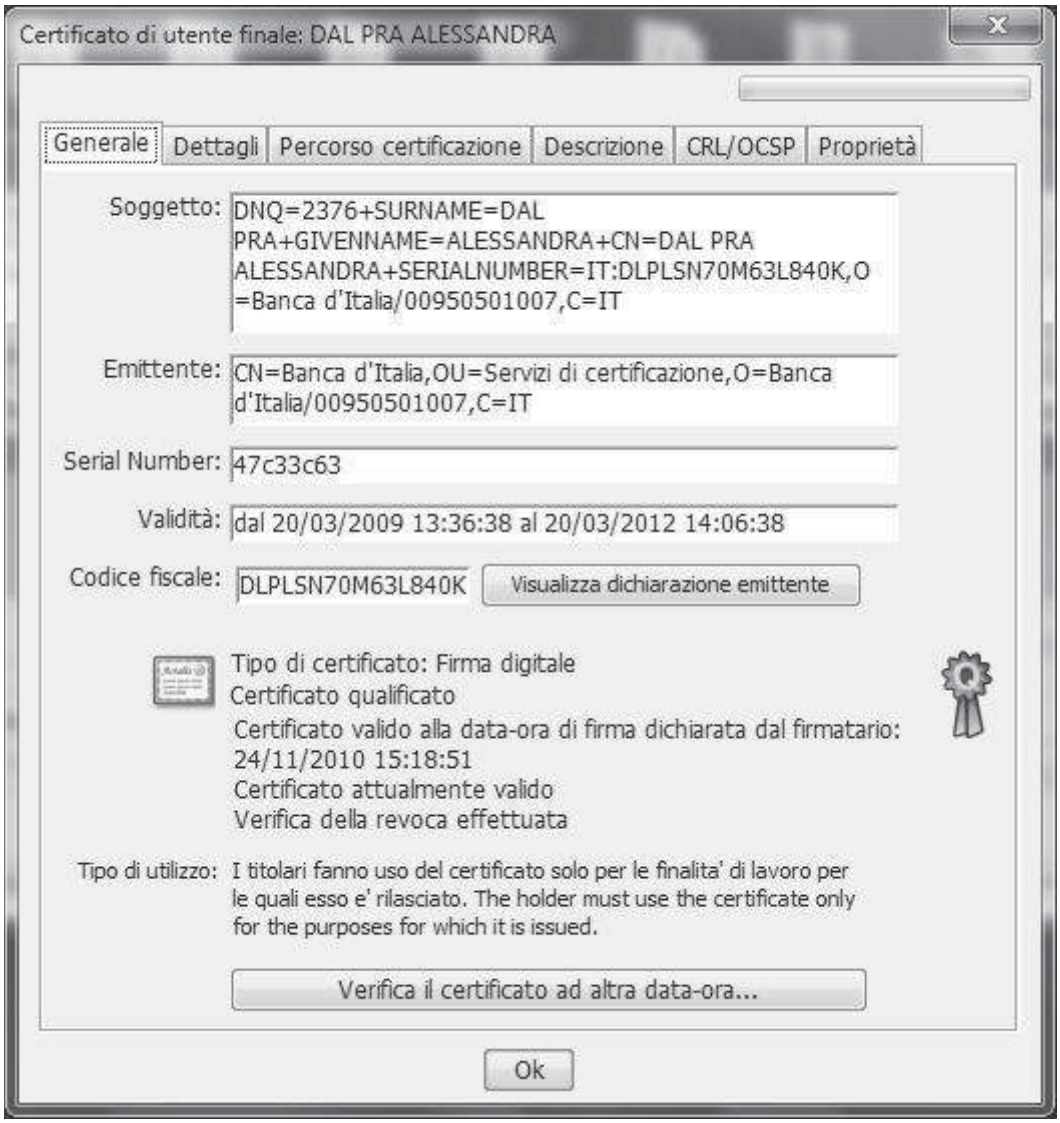
Nel caso di un documento firmato in standard PDF, si procede esattamente allo stesso modo.

Verifica del firmatario

La verifica *completa* di una firma digitale richiede sempre due passi:

1. verifica della firma in se stessa (verifica di integrità)
2. verifica del certificato del firmatario

Nella sezione precedente abbiamo descritto come effettuare il primo passo. Per effettuare il secondo passo, di fondamentale importanza, si deve cliccare sul bottone "**Verifica firmatario**" presente nella finestra riepilogativa delle firme. Dopo qualche istante, apparirà una finestra del tipo seguente che mostra il risultato delle verifiche svolte:



È importante notare che la verifica del certificato viene sempre svolta alla data-ora di firma, la quale viene determinata nel modo seguente:

- la data-ora estratta dalla marca temporale associata alla firma (se presente)
- altrimenti, la data-ora estratta dall'attributo signingTime (se presente)
- altrimenti, la data-ora corrente del sistema operativo

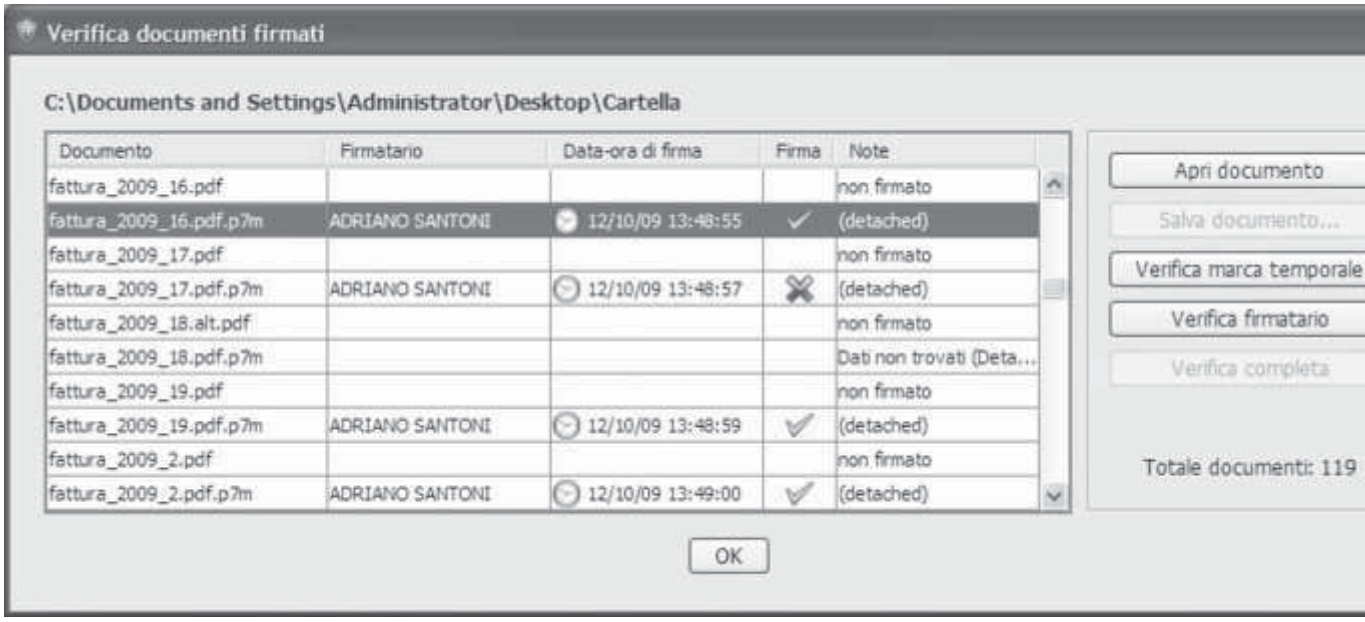
Per effettuare la verifica del certificato ad una data-ora diversa, di propria scelta, cliccare sul bottone "**Verifica il certificato ad altra data-ora**"; apparirà la seguente finestra di dialogo:

Da qui, usando gli appositi selettori, è possibile impostare la data e ora desiderate per la verifica del certificato. Cliccando sul bottone "**Oggi**" la data-ora viene reimpostata alla data-ora corrente del sistema operativo.

Verificare una cartella

Se una cartella è stata firmata col metodo elenco delle impronte, per la verifica si procede come nel caso di una normale verifica di firma XML, avendo l'accortezza di selezionare il file di nome "**signature.xml**" presente nella cartella firmata.

Se invece sono stati firmati i singoli file contenuti in una cartella, è possibile svolgere una "verifica massiva" selezionando la voce "**Verifica cartella**" dal menu "File" dell'applicazione. Dopo aver selezionato la cartella di input (quella che contiene i documenti firmati da verificare) apparirà una finestra di dialogo di questo tipo:



Nel caso in cui il documento selezionato presenti una firma singola - come avviene di norma nel caso della firma cartella - la finestra mostra le informazioni principali risultanti dalla verifica: il nome del firmatario (estratto dal certificato), la data e ora di firma (se presente, eventualmente attestata da una marca temporale), la validità della firma e le eventuali note aggiuntive in caso di errore. Per completare la verifica, cliccare sul bottone "**Verifica firmatario**" e sul bottone "**Verifica marca temporale**" (se presente).

Nel caso in cui, invece, il file selezionato presenti più firme, si dovrà cliccare sul bottone "**Verifica completa**".

Se il documento è contenuto nel file firmato, è possibile visualizzarlo ed eventualmente salvarlo cliccando sul bottone "**Apri documento**".

La funzione di "verifica cartella" supporta tutti i tipi di firma gestiti dall'applicazione: P7M/CMS, PDF, XML.

Marcatura temporale

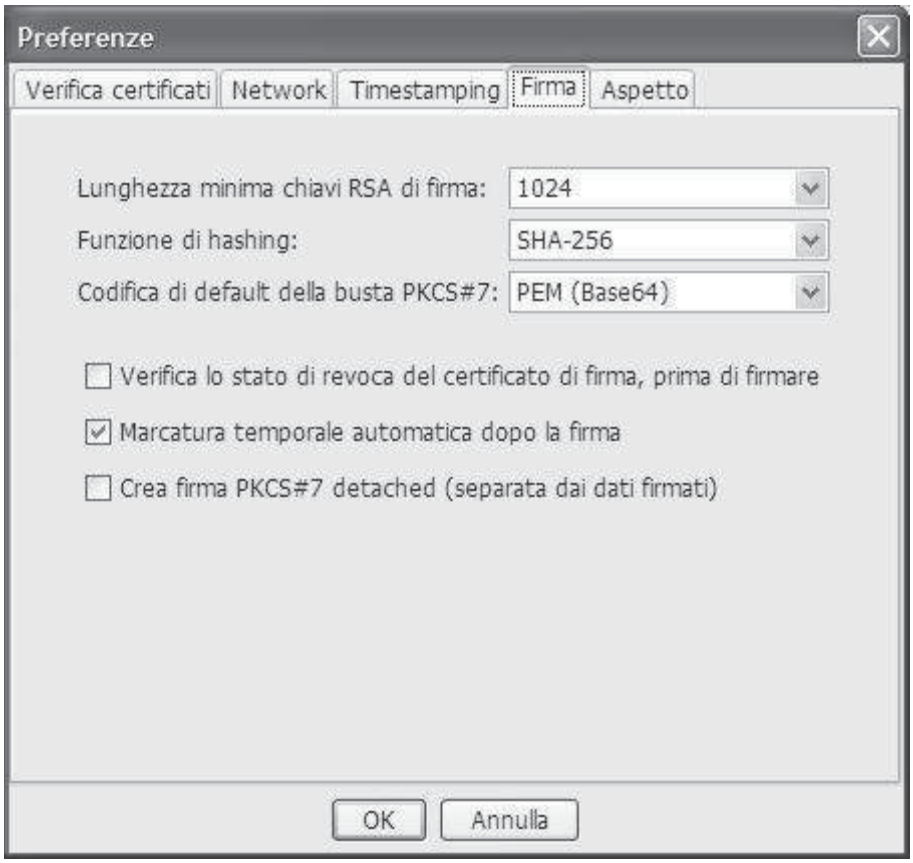
L'applicazione permette di apporre la marca temporale (time-stamp) in due modi:

- marca temporale di una singola firma digitale
- marca temporale di un intero documento

Marcatura della singola firma digitale

Si può ottenere una marca temporale che attesta la data/ora di apposizione di una specifica firma digitale (si tenga presente la possibilità di firma multipla). Questa marca viene quindi associata alla firma digitale, restando così all'interno della busta crittografica. In questo modo, è possibile garantire - a chi dovrà in seguito verificare la firma - che quella particolare firma è stata apposta alla data/ora indicata dalla marca temporale.

Per attivare questa funzionalità, per quanto riguarda la firma in formato **P7M** e **PDF**, accedere alla finestra delle preferenze di firma e selezionare la casella "**Marcatura temporale automatica dopo la firma**":



Per quanto riguarda la firma XML, questa funzionalità è attivabile caso per caso, cliccando sul bottone "**Opzioni avanzate**" (cfr. la figura).

Le marche temporali associate alle singole firme sono visualizzabili e verificabili in fase di verifica di un documento firmato.

Marcatura di un intero documento

Si può anche ottenere una marca temporale che attesta la data/ora di esistenza di un intero documento, indipendentemente da quante firme digitali contiene (ma può anche trattarsi di un documento non firmato). Questa operazione si attiva cliccando sul bottone "**Marca temporale**" nella finestra principale, oppure selezionando la voce corrispondente nel menu "**File**".

La marca temporale ottenuta per un intero documento può essere salvata in due modi diversi:

1. come file separato (con estensione TSR)

2. insieme al documento di riferimento, all'interno di una "busta marcata" (con estensione TSD)

La "busta marcata" è una busta conforme alla specifica pubblica TimeStampedData che racchiude:

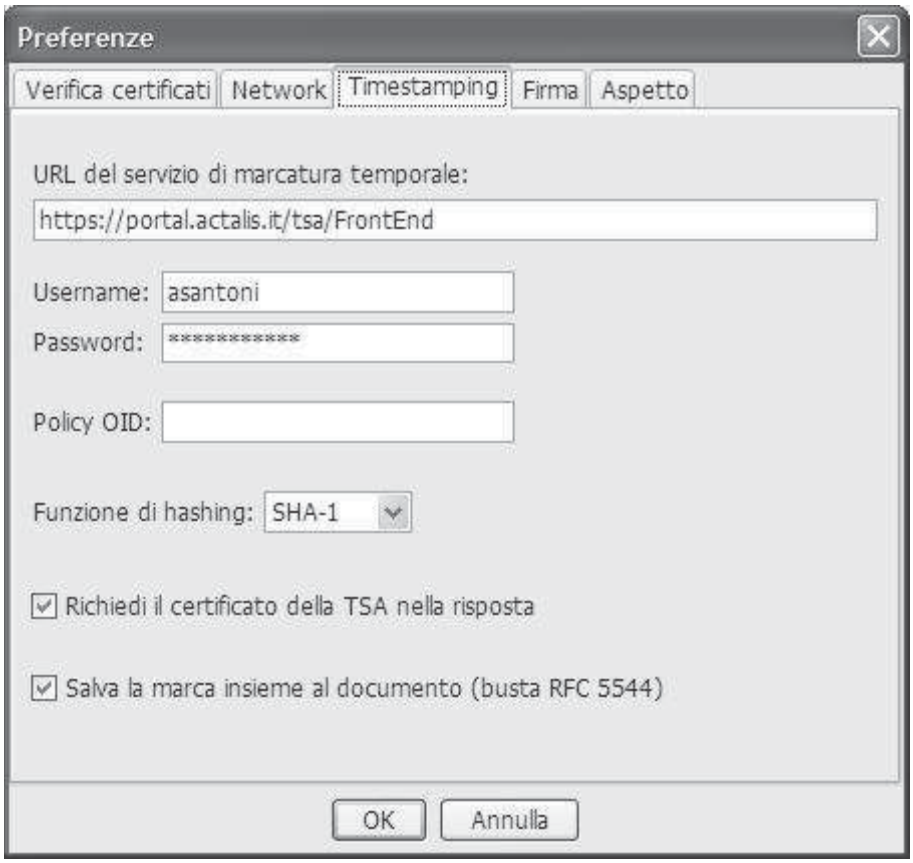
- un documento o file qualsiasi (non necessariamente firmato)
- opzionalmente, dei metadati riferiti al documento (per es. il nome)
- una o più marche temporali

Le marche temporali sono associate al documento nel modo seguente:

- la prima marca temporale (tempo T1) è calcolata sul documento di riferimento ed eventualmente sui metadati
- la seconda marca temporale (tempo T2) è calcolata sulla prima (e ne attesta l'esistenza al tempo T1)
- la terza marca temporale (tempo T3) è calcolata sulla seconda (e ne attesta l'esistenza al tempo T2)
- eccetera...

La busta marcata, dunque, oltre alla convenienza di contenere il documento di riferimento, consente di *estendere a piacere* l'attestazione di esistenza del documento al tempo T1, anche molto tempo dopo che la prima marca temporale è scaduta.

La scelta tra le due opzioni (marca temporale separata o imbustata) può essere fatta dal pannello delle Preferenze, attraverso la casella "**Salva la marca insieme al documento**":



* * *

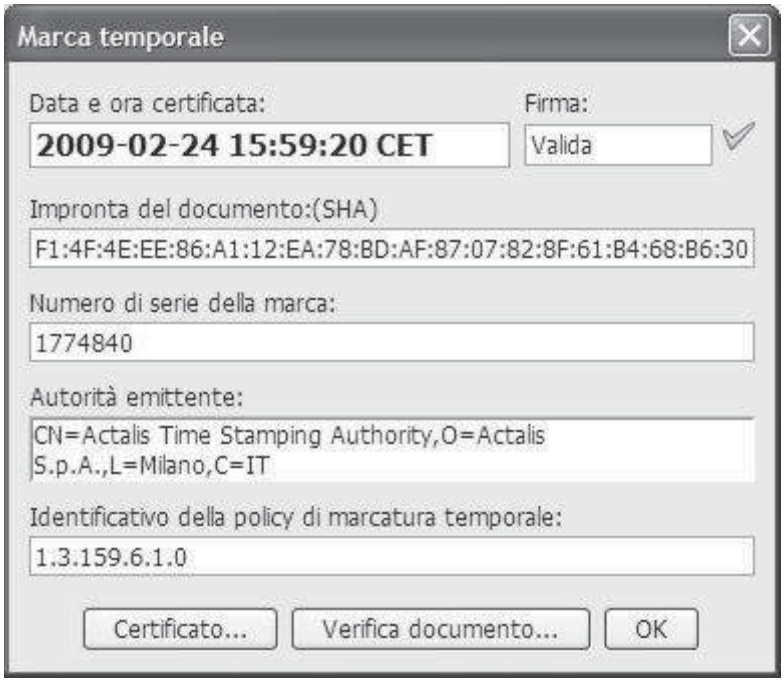
Per ottenere marche temporali, in entrambi i casi sopra descritti, è necessario avere accesso ad un servizio di marcatura temporale ed impostare l'indirizzo del servizio e le credenziali di accesso nella finestra delle **Preferenze** (cliccare sul corrispondente bottone nella finestra principale, quindi selezionare la scheda "**Timestamping**").

Verifica marca temporale

È possibile verificare sia marche temporali "sciolte" sia buste marcate; in entrambi i casi, la verifica può essere fatta in 4 modi diversi:

- facendo "doppio-clic" col mouse sul file desiderato (con estensione TSR o TSD)
- cliccando sul file desiderato col tasto destro del mouse e quindi selezionando la voce "**Verifica con File Protector**"
- trascinando il file desiderato sull'area-bersaglio
- selezionando la voce di menu "**Verifica marca temporale**"

Verificando una marca temporale "sciolta" (file con estensione .TSR) compare una finestra di questo tipo:



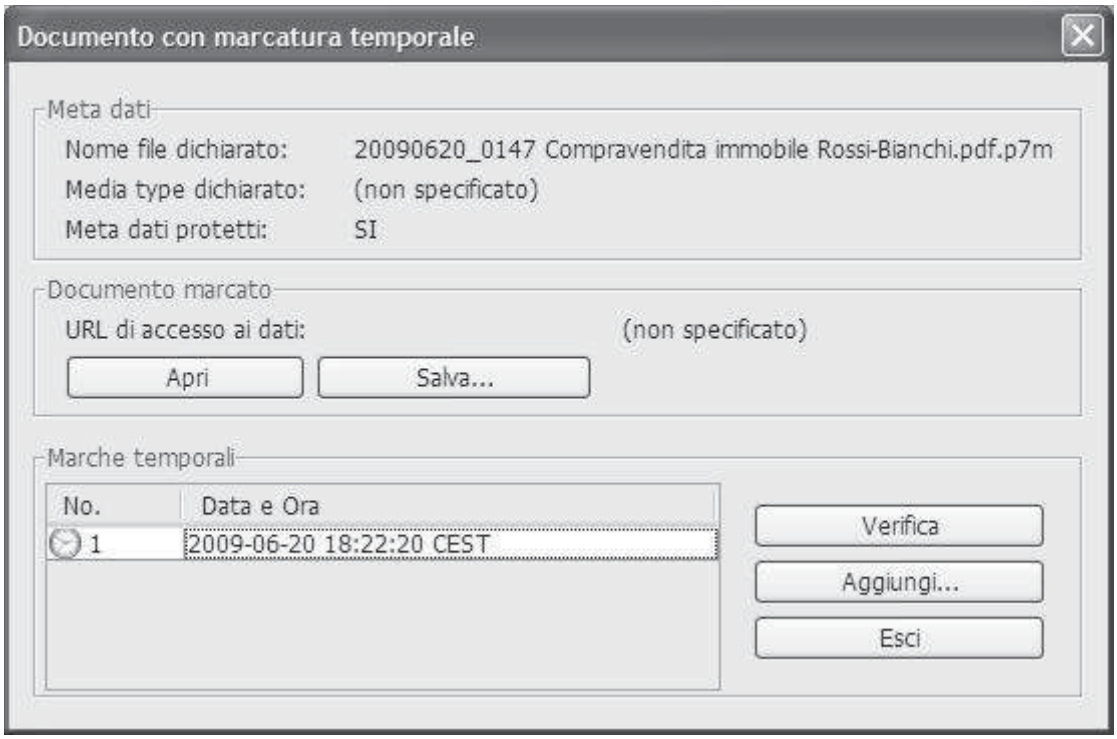
Questa finestra mostra una serie di importanti informazioni, tra cui:

- la data e ora in cui è stata emessa la marca temporale
- la validità della firma della TSA sulla marca temporale
- l'autorità (TSA) che ha emesso la marca temporale

Cliccando sul bottone "**Verifica documento**..." è possibile selezionare il documento di riferimento e controllare che corrisponda effettivamente alla marca temporale in esame (ossia che l'impronta ricalcolata del documento coincida con l'impronta contenuta nella marca).

Cliccando sul bottone "**Certificato**..." vengono visualizzati tutti i dettagli sul certificato della TSA.

Quando invece si verifica una "busta marcata", compare anzitutto una finestra di questo tipo:

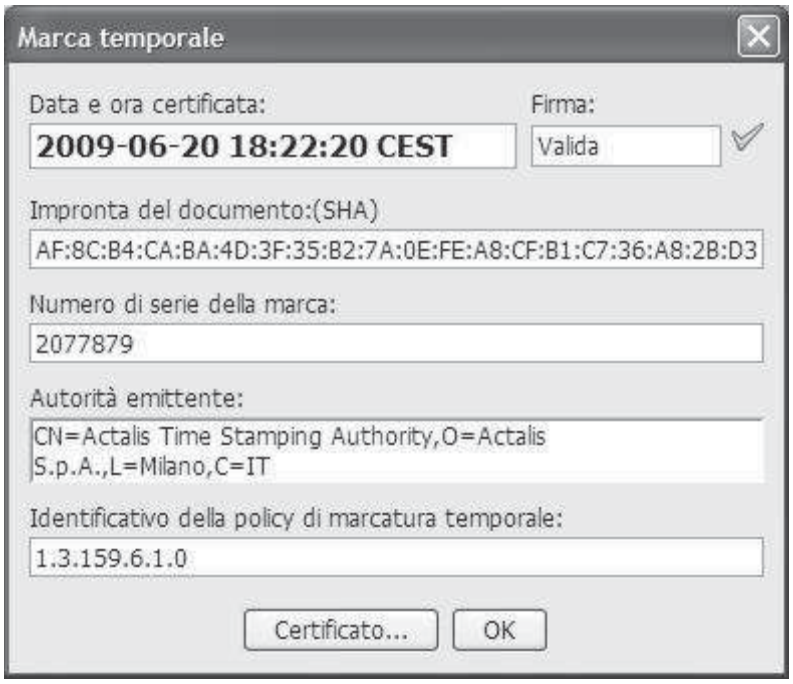


Questa finestra mostra le principali informazioni sulla busta in esame:

- metadati (tra cui, solitamente, il nome del documento contenuto nella busta)
- elenco delle marche temporali ottenute per il documento

Sono inoltre presenti due bottoni "**Apri**" e "**Salva**" che consentono rispettivamente di visualizze e salvare il documento contenuto nella busta.

Per verificare le singole marche temporali, selezionare dall'elenco quella desiderata e cliccare sul bottone "**Verifica**"; apparirà una finestra di questo tipo:



In questo caso non è presente il bottone "**Verifica documento**" in quanto la verifica viene fatta automaticamente rispetto al documento contenuto nella busta.

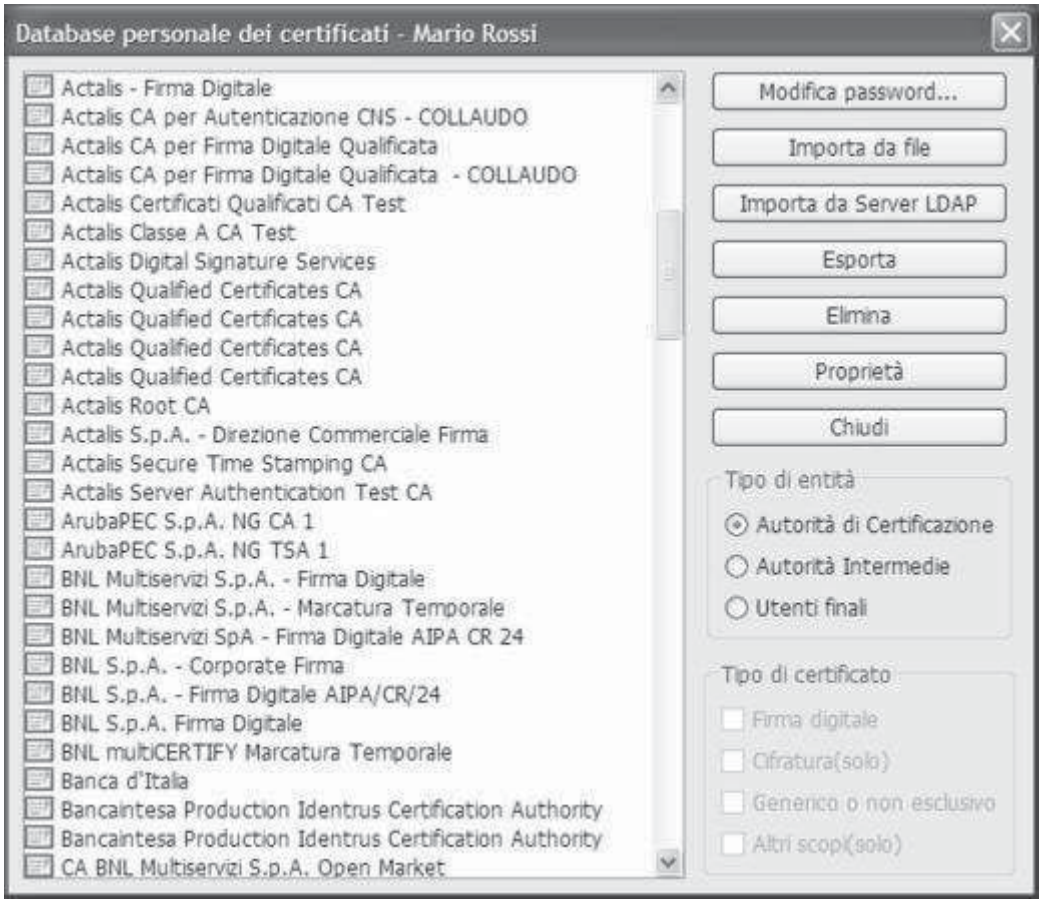
Cliccando sul bottone "**Aggiungi**..." nella finestra di verifica di una busta marcata, verrà aggiunta una marca temporale a quelle esistenti, secondo la logica descritta nella sezione precedente. Questa operazione è utile se il documento deve essere conservato per un lungo periodo di tempo, al di là della data di scadenza della marca temporale corrente.

Gestione dei certificati

L'applicazione permette di gestire un database personale dei certificati delle CA (necessari per verificare la validità dei certificati degli utenti) e degli utenti;

Il database è protetto con la password di accesso al profilo.

È possibile aggiungere, rimuovere e visualizzare i certificati attraverso la finestra di gestione dei certificati, alla quale si accede selezionando la voce "**Database certificati**" dal menu "**Strumenti e opzioni**":

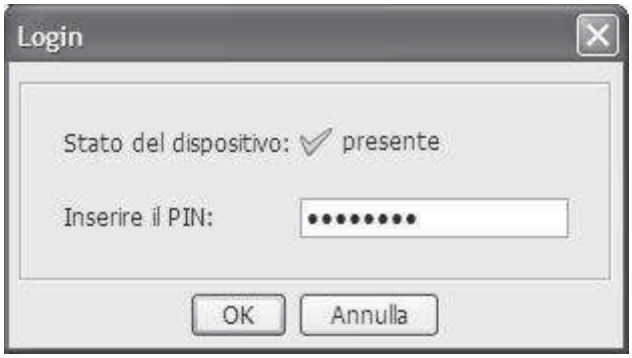


Per impostare il server LDAP da utilizzare nella ricerca dei certificati, selezionare la voce "**Elenco server LDAP**" dal menu "**Strumenti e opzioni**" nella finestra principale dell'applicazione, quindi aggiungere o modificare la voce desiderata in modo che la casella "**Usa per ricerca**..." sia abilitata (possono essere configurati

diversi server LDAP, ma solo quello contrassegnato sarà poi utilizzabile nelle ricerche):

Gestione del PIN

Il dispositivo di firma (smartcard o altro dispositivo equivalente) è protetto da un codice segreto detto **PIN.** Durante una sessione di lavoro, per poter svolgere operazioni di firma dovete digitare il PIN della vostra smartcard almeno una volta (cliccare sul bottone "**Login**" nella finestra principale); in alcuni casi, l'applicazione vi chiede automaticamente di inserire il PIN se necessario:



Al termine di una sessione di lavoro, se preferite lasciare attiva l'applicazione, raccomandiamo di cliccare sul bottone "**Logout**" in modo da impedire ad altri l'uso indebito della vostra smartcard.

Senza conoscere il vostro PIN, non è possibile apporre la vostra firma digitale, perciò è molto importante che il vostro PIN sia noto solo a voi e che sia difficile da indovinare.

La smartcard viene di solito consegnata all'utente con un adeguato PIN preimpostato; tuttavia potete impostare il PIN al valore desiderato selezionando la voce "**Cambio PIN**" dal menu "**Dispositivo**", nella finestra principale.

Per ragioni di sicurezza, se si inserisce il PIN in modo errato più di un certo numero di volte (solitamente 3), la smartcard si blocca e non è più possibile utilizzarla fino a quando non viene sbloccata. Per **sbloccare** la vostra smartcard, dovete conoscere un secondo codice segreto detto **PUK**. In tal caso, selezionate la voce "**Sblocco PIN**" dal menu "**Dispositivo**", nella finestra principale.

Si faccia attenzione a digitare correttamente il PUK, perché anche questo è soggetto al blocco in caso di errori ripetuti. In caso di blocco del PUK, non è più possibile ripristinare il normale funzionamento della smartcard.